NetScaler Gateway 13.1

Machine translated content

Disclaimer

Contents

Notes de mise à jour de NetScaler Gateway

January 26, 2024

Les notes de mise à jour décrivent comment le logiciel a changé dans une version particulière, et les problèmes connus pour exister dans cette version.

Le document des notes de version comprend tout ou partie des sections suivantes :

- **Nouveautés** : les améliorations et autres modifications publiées dans la version.
- **Problèmes résolus** : Problèmes résolus dans la version.
- **Problèmes connus** : problèmes qui existent dans la version.
- **Points à noter** : Les aspects importants à garder à l'esprit lors de l'utilisation de la version.
- **Limitations** : les limitations qui existent dans la version.

> **Important :** Les notes de mise à jour de NetScaler Gateway sont couvertes dans les notes de mise à jour d'ADC.
> Pour des informations détaillées sur les améliorations de NetScaler Gateway 13.1, les problèmes connus et les corrections de bogues, consultez la page des notes de mise à jour.

Remarque :

- Les étiquettes [# XXXXXX] figurant dans les descriptions des problèmes sont des identifiants de suivi internes utilisés par l'équipe NetScaler.
- Ces notes de publication ne documentent pas les correctifs liés à la sécurité. Pour obtenir la liste des correctifs et des conseils relatifs à la sécurité, consultez le bulletin de sécurité.

À propos de NetScaler Gateway

March 27, 2024

NetScaler Gateway est facile à déployer et à administrer. La configuration de déploiement la plus courante consiste à localiser l'appliance NetScaler Gateway dans la zone démilitarisée. Vous pouvez installer plusieurs appliances NetScaler Gateway sur le réseau pour des déploiements plus complexes.

La première fois que vous démarrez NetScaler Gateway, vous pouvez effectuer la configuration initiale à l'aide d'une console série, de l'assistant de configuration de l'utilitaire de configuration ou du protocole DHCP (Dynamic Host Configuration Protocol). Sur l'appliance MPX, vous pouvez utiliser le clavier LCD situé sur le panneau avant de l'appliance pour effectuer la configuration initiale. Vous

pouvez configurer des paramètres de base spécifiques à votre réseau interne, tels que l'adresse IP, le masque de sous-réseau, l'adresse IP de la passerelle par défaut et l'adresse DNS (Domain Name System). Après avoir configuré les paramètres réseau de base, vous configurez les paramètres spécifiques au fonctionnement de NetScaler Gateway, tels que les options d'authentification, d'autorisation, de ressources réseau, de serveurs virtuels, de stratégies de session et de stratégies de point de terminaison.

Avant d'installer et de configurer NetScaler Gateway, consultez les rubriques de cette section pour obtenir des informations sur la planification de votre déploiement. La planification du déploiement peut inclure la détermination de l'emplacement d'installation de l'appliance, la compréhension de la procédure d'installation de plusieurs appliances dans la zone démilitarisée et les exigences de licence. Vous pouvez installer NetScaler Gateway dans n'importe quelle infrastructure réseau sans modifier le matériel ou les logiciels existants exécutés sur le réseau sécurisé. NetScaler Gateway prend en charge d'autres produits réseau, tels que les équilibreurs de charge pour serveurs, les moteurs de cache, les pare-feux, les routeurs et les périphériques sans fil IEEE 802.11.

Vous pouvez écrire vos paramètres dans la liste de contrôle de pré-installation à avoir sous la main avant de configurer NetScaler Gateway.

Appliances NetScaler Gateway	Fournit des informations sur les appliances NetScaler Gateway et les instructions d'installation des appliances.
Check-list d'installation	Fournit des informations de planification à consulter et une liste des tâches à effectuer avant d'installer NetScaler Gateway sur votre réseau.
Déploiements courants	Fournit des informations sur le déploiement de NetScaler Gateway dans la zone démilitarisée du réseau, dans un réseau sécurisé sans zone démilitarisée et avec d'autres appliances pour prendre en charge l'équilibrage de charge et le basculement. Fournit également des informations sur le déploiement de NetScaler Gateway avec Citrix Virtual Apps and Desktops.
Licensing	Fournit des informations sur l'installation des licences sur l'appliance. Fournit également des informations sur l'installation de licences sur plusieurs appliances NetScaler Gateway.

Architecture NetScaler Gateway

Les principaux composants de NetScaler Gateway sont les suivants :

- **Serveurs**virtuels. Le serveur virtuel NetScaler Gateway est une entité interne représentative de tous les services configurés disponibles pour les utilisateurs. Le serveur virtuel est également le point d'accès par lequel les utilisateurs accèdent à ces services. Vous pouvez configurer plusieurs serveurs virtuels sur une seule appliance, ce qui permet à une appliance NetScaler Gateway de servir plusieurs communautés d'utilisateurs ayant des exigences d'authentification et d'accès aux ressources différentes.
- **Authentification, autorisation et audit**. Vous pouvez configurer l'authentification, l'autorisation et la comptabilité pour permettre aux utilisateurs de se connecter à NetScaler Gateway avec des informations d'identification reconnues par NetScaler Gateway ou par des serveurs d'authentification situés sur le réseau sécurisé, tels que LDAP ou RADIUS. Les stratégies d'autorisation définissent les autorisations des utilisateurs, déterminant les ressources auxquelles un utilisateur donné est autorisé à accéder. Pour plus d'informations sur l'authentification et l'autorisation, consultez Configuration de l'authentification et de l'autorisation. Les serveurs d'audit conservent les données relatives à l'activité de NetScaler Gateway, notamment les événements de connexion des utilisateurs, les instances d'accès aux ressources et les erreurs opérationnelles. Ces informations sont stockées sur NetScaler Gateway ou sur un serveur externe. Pour plus d'informations sur l'audit, voir Configuration de l'audit sur NetScaler Gateway
- **Connexions utilisateur**. Les utilisateurs peuvent se connecter à NetScaler Gateway en utilisant les méthodes d'accès suivantes :
  - Le client Citrix Secure Access pour Windows est un logiciel installé sur un ordinateur Windows. Les utilisateurs ouvrent une session en cliquant avec le bouton droit de la souris sur une icône dans la zone de notification d'un ordinateur Windows. Si les utilisateurs utilisent un ordinateur sur lequel le client Citrix Secure Access n'est pas installé, ils peuvent se connecter à l'aide d'un navigateur Web pour télécharger et installer le plug-in. Si l'application Citrix Workspace est installée sur les utilisateurs, ils ouvrent une session avec le client Citrix Secure Access à partir de l'application Citrix Workspace. Lorsque l'application Citrix Workspace et le client Citrix Secure Access sont installés sur la machine utilisateur, l'application Citrix Workspace ajoute automatiquement le client Citrix Secure Access.
  - Le client Citrix Secure Access pour macOS X qui permet aux utilisateurs exécutant macOS X de se connecter. Il possède les mêmes caractéristiques et fonctions que le client Citrix Secure Access pour Windows. Vous pouvez fournir un support d'analyse des points de terminaison pour cette version du plug-in en installant NetScaler Gateway 10.1, Build 120.1316.e.
  - Application Citrix Workspace qui permet aux utilisateurs de se connecter aux applications

publiées et aux bureaux virtuels dans une batterie de serveurs à l'aide de l'interface Web ou de Citrix StoreFront.

- Application Citrix Workspace, Secure Hub, WorxMail et WorxWeb qui permettent aux utilisateurs d'accéder aux applications Web et SaaS, aux applications mobiles iOS et Android et aux données ShareFile hébergées dans Citrix Endpoint Management.
- Les utilisateurs peuvent se connecter à partir d'un appareil Android qui utilise l'adresse Web de NetScaler Gateway. Lorsque les utilisateurs démarrent une application, la connexion utilise Micro VPN pour acheminer le trafic réseau vers le réseau interne. Si les utilisateurs se connectent depuis un appareil Android, vous devez configurer les paramètres DNS sur NetScaler Gateway. Pour plus d'informations, consultez Prise en charge des requêtes DNS à l'aide de suffixes DNS pour les appareils Android.
- Les utilisateurs peuvent se connecter à partir d'un appareil iOS qui utilise l'adresse Web de NetScaler Gateway. Vous configurez la Secure Browse soit globalement, soit dans un profil de session. Lorsque les utilisateurs démarrent une application sur leur appareil iOS, une connexion VPN démarre et la connexion est acheminée via NetScaler Gateway.
- Accès sans client qui fournit aux utilisateurs l'accès dont ils ont besoin sans installer de logiciel sur la machine utilisateur.

  Lors de la configuration de NetScaler Gateway, vous pouvez créer des stratégies pour configurer la manière dont les utilisateurs se connectent. Vous pouvez également restreindre l'ouverture de session des utilisateurs en créant des stratégies d'analyse de session et de point de terminaison.

- **Ressources réseau**. Il s'agit notamment de tous les services réseau auxquels les utilisateurs accèdent via NetScaler Gateway, tels que les serveurs de fichiers, les applications et les sites Web.
- **Adaptateur**virtuel. L'adaptateur virtuel NetScaler Gateway prend en charge les applications qui nécessitent une usurpation d'adresse IP. L'adaptateur virtuel est installé sur la machine utilisateur lorsque le client Citrix Secure Access est installé. Lorsque les utilisateurs se connectent au réseau interne, la connexion sortante entre NetScaler Gateway et les serveurs internes utilise l'adresse IP de l'intranet comme adresse IP source. Le client Citrix Secure Access reçoit cette adresse IP du serveur dans le cadre de la configuration.

  Si vous activez le split tunneling sur NetScaler Gateway, tout le trafic intranet est acheminé via l'adaptateur virtuel. Lors de l'interception du trafic lié à l'intranet, la carte virtuelle intercepte les requêtes DNS de type d'enregistrement A et AAAA tout en laissant toutes les autres requêtes DNS intactes. Le trafic réseau qui n'est pas lié au réseau interne est acheminé via la carte réseau installée sur la machine utilisateur. Les connexions Internet et LAN privé (LAN) restent ouvertes et connectées. Si vous désactivez le split tunneling, toutes les connexions sont routées via

l'adaptateur virtuel. Toutes les connexions existantes sont déconnectées et l'utilisateur doit rétablir la session.

Si vous configurez une adresse IP intranet, le trafic vers le réseau interne est falsifié avec l'adresse IP intranet via la carte virtuelle.

Fonctionnent des connexions utilisateur

Les utilisateurs peuvent se connecter à leurs e-mails, partages de fichiers et autres ressources réseau à partir d'un emplacement distant. Les utilisateurs peuvent se connecter aux ressources réseau internes à l'aide des logiciels suivants :

- Client Citrix Secure Access
- Application Citrix Workspace
- WorxMail et WorxWeb
- Appareils mobiles Android et iOS

Connectez-vous au client Citrix Secure Access

Le client Citrix Secure Access permet aux utilisateurs d'accéder aux ressources du réseau interne en procédant comme suit :

1. Un utilisateur se connecte à NetScaler Gateway pour la première fois en saisissant l'adresse Web dans un navigateur Web. La page de connexion apparaît et l'utilisateur est invité à entrer un nom d'utilisateur et un mot de passe. Si des serveurs d'authentification externes sont configurés, NetScaler Gateway contacte le serveur et les serveurs d'authentification vérifient les informations d'identification de l'utilisateur. Si l'authentification locale est configurée, NetScaler Gateway procède à l'authentification de l'utilisateur.
2. Si vous configurez une stratégie de préauthentification, lorsque l'utilisateur saisit l'adresse Web de NetScaler Gateway dans un navigateur Web sur un ordinateur Windows ou macOS X, NetScaler Gateway vérifie si des stratégies de sécurité basées sur le client sont en place avant l'affichage de la page de connexion. Les vérifications de sécurité vérifient que la machine utilisateur répond aux conditions de sécurité, telles que les mises à jour du système d'exploitation, la protection antivirus et un pare-feu correctement configuré. Si la machine utilisateur échoue au contrôle de sécurité, NetScaler Gateway empêche l'utilisateur de se connecter. Un utilisateur qui ne peut pas ouvrir de session doit télécharger les mises à jour ou packages nécessaires et les installer sur la machine utilisateur. Lorsque la machine utilisateur passe la stratégie de pré-authentification, la page d'ouverture de session s'affiche et l'utilisateur peut entrer les informations d'identification de connexion. Vous pouvez utiliser Advanced Endpoint Analysis sur un ordinateur macOS X si vous installez NetScaler Gateway 10.1, build 120.1316.e.

3. Lorsque NetScaler Gateway authentifie correctement l'utilisateur, NetScaler Gateway lance le tunnel VPN. NetScaler Gateway invite l'utilisateur à télécharger et à installer le client Citrix Secure Access pour Windows ou le client Citrix Secure Access pour macOS X.
4. Si vous configurez un scan post-authentification, une fois qu'un utilisateur s'est connecté avec succès, NetScaler Gateway analyse la machine utilisateur à la recherche des stratégies de sécurité client requises. Vous pouvez exiger les mêmes conditions de sécurité que pour une stratégie de pré-authentification. Si la machine utilisateur échoue à l'analyse, la stratégie n'est pas appliquée ou l'utilisateur est placé dans un groupe de quarantaine et l'accès de l'utilisateur aux ressources réseau est limité.
5. Lorsque la session est établie, l'utilisateur est dirigé vers une page d'accueil de NetScaler Gateway où il peut sélectionner les ressources auxquelles il souhaite accéder. La page d'accueil incluse dans NetScaler Gateway s'appelle l'interface d'accès. Si l'utilisateur ouvre une session à l'aide du client Citrix Secure Access pour Windows, une icône dans la zone de notification sur le bureau Windows indique que la machine utilisateur est connectée et que l'utilisateur reçoit un message indiquant que la connexion est établie. L'utilisateur peut également accéder aux ressources du réseau sans utiliser l'interface d'accès, par exemple en ouvrant Microsoft Outlook et en récupérant des e-mails.
6. Si la demande de l'utilisateur passe les contrôles de sécurité avant et après authentification, NetScaler Gateway contacte alors la ressource demandée et établit une connexion sécurisée entre la machine utilisateur et cette ressource.
7. L'utilisateur peut fermer une session active en cliquant avec le bouton droit sur l'icône NetScaler Gateway dans la zone de notification d'un ordinateur Windows, puis en cliquant sur Déconnexion. La session peut également être dépassé en raison d'une inactivité. Lorsque la session est fermée, le tunnel est arrêté et l'utilisateur n'a plus accès aux ressources internes. L'utilisateur peut également saisir l'adresse Web de NetScaler Gateway dans un navigateur. Lorsque l'utilisateur appuie sur Entrée, l'interface d'accès apparaît à partir de laquelle les utilisateurs peuvent se déconnecter.

Remarque : si vous déployez Citrix Endpoint Management sur votre réseau interne, un utilisateur qui se connecte depuis l'extérieur du réseau interne doit d'abord se connecter à NetScaler Gateway. Lorsque l'utilisateur établit la connexion, il peut accéder aux applications Web et SaaS, aux applications mobiles Android et iOS et aux données ShareFile hébergées sur Citrix Endpoint Management. Un utilisateur peut se connecter au client Citrix Secure Access via un accès sans client ou à l'aide de l'application Citrix Workspace ou de Secure Hub.

Connectez-vous avec l'application Citrix Workspace

Les utilisateurs peuvent se connecter à l'application Citrix Workspace pour accéder à leurs applications Windows et à leurs bureaux virtuels. Les utilisateurs peuvent également accéder aux applications depuis Endpoint Management. Pour se connecter à distance, les utilisateurs installent égale-

ment le client Citrix Secure Access sur leur appareil. L'application Citrix Workspace ajoute automatiquement le client Citrix Secure Access à sa liste de plug-ins. Lorsque les utilisateurs se connectent à l'application Citrix Workspace, ils peuvent également se connecter au client Citrix Secure Access. Vous pouvez également configurer NetScaler Gateway pour effectuer une authentification unique au client Citrix Secure Access lorsque les utilisateurs se connectent à l'application Citrix Workspace.

Connectez-vous avec des appareils iOS et Android

Les utilisateurs peuvent se connecter à partir d'un appareil iOS ou Android à l'aide de Secure Hub. Les utilisateurs peuvent accéder à leur messagerie en utilisant Secure Mail et se connecter à des sites Web avec WorxWeb.

Lorsque les utilisateurs se connectent depuis l'appareil mobile, les connexions passent par NetScaler Gateway pour accéder aux ressources internes. Si les utilisateurs se connectent à iOS, vous activez la Secure Browse dans le cadre du profil de session. Si les utilisateurs se connectent à Android, la connexion utilise automatiquement le Micro VPN. De plus,
Secure Mail et WorxWeb utilisent Micro VPN pour établir des connexions via NetScaler Gateway. Il n'est pas nécessaire de configurer Micro VPN sur NetScaler Gateway.

Déploiements courants de NetScaler Gateway

January 26, 2024

vous pouvez déployer NetScaler Gateway en périphérie du réseau interne de votre organisation (ou intranet) afin d'offrir un point d'accès unique et sécurisé aux serveurs, applications et autres ressources réseau hébergées sur votre réseau interne. Tous les utilisateurs distants doivent se connecter à NetScaler Gateway avant de pouvoir accéder aux ressources du réseau interne.

NetScaler Gateway est le plus souvent installé aux emplacements suivants d'un réseau :

- Dans la zone démilitarisée du réseau
- Réseau sécurisé dans DMZ

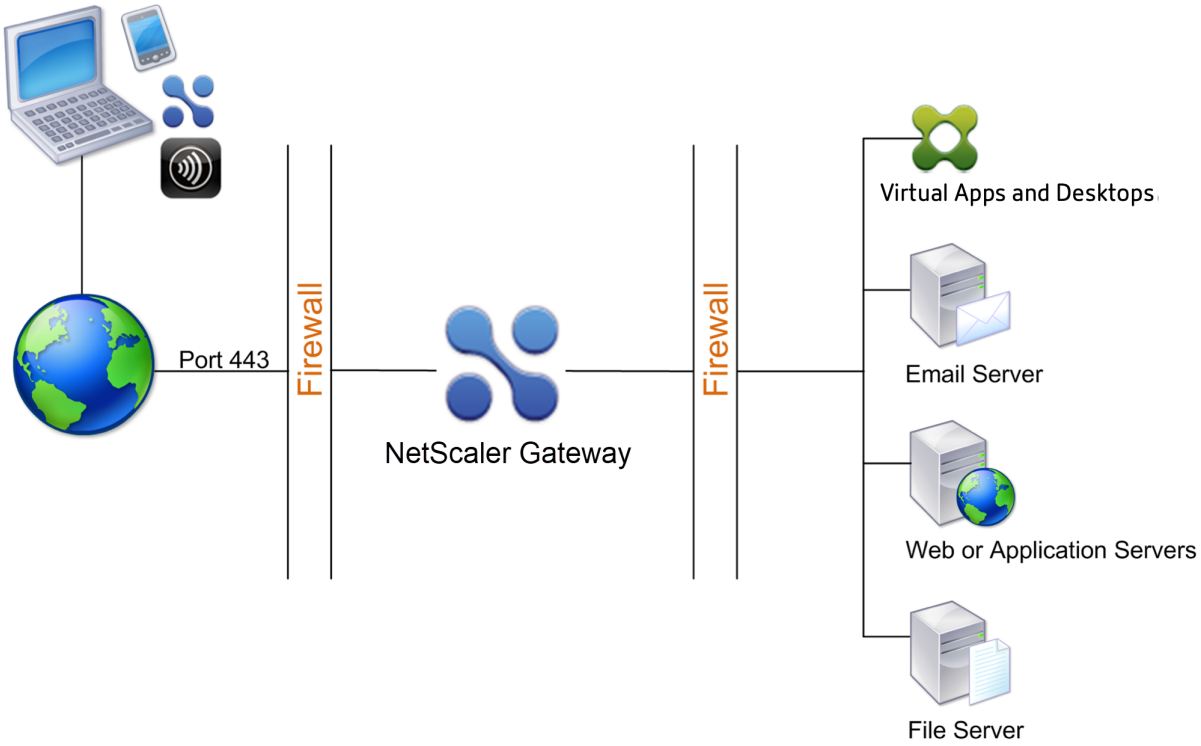
Vous pouvez également déployer NetScaler Gateway avec Citrix Virtual Apps, Citrix Virtual Desktops, StoreFront et Citrix Endpoint Management pour permettre aux utilisateurs d'accéder à leurs applications Windows, Web, mobiles et SaaS. Si votre déploiement inclut Citrix Virtual Apps, StoreFront et Desktops 7, vous pouvez déployer NetScaler Gateway dans une configuration DMZ à saut unique ou à double saut. Un déploiement à double saut n'est pas pris en charge avec les versions antérieures de Citrix Virtual Desktops ou de Citrix Endpoint Management.

Pour plus d'informations sur l'extension de votre installation NetScaler Gateway avec ces solutions et d'autres solutions NetScaler prises en charge, consultez la rubrique Intégration aux produits NetScaler.

Déployer NetScaler Gateway dans une zone démilitarisée

De nombreuses entreprises protègent leur réseau interne avec une zone démilitarisée. Une zone démilitarisée est un sous-réseau situé entre le réseau interne sécurisé d'une organisation et Internet (ou tout autre réseau externe). Lorsque vous déployez NetScaler Gateway dans la zone démilitarisée, les utilisateurs se connectent à l'application Citrix Secure Access pour Windows ou Citrix Workspace.

Figure 1. NetScaler Gateway déployé dans la zone démilitarisée



Dans la configuration présentée dans la figure précédente, vous installez NetScaler Gateway dans la zone démilitarisée et le configurez pour qu'il se connecte à la fois à Internet et au réseau interne.

Connectivité NetScaler Gateway dans une zone démilitarisée

Lorsque vous déployez NetScaler Gateway dans la zone démilitarisée, les connexions utilisateur doivent traverser le premier pare-feu pour se connecter à NetScaler Gateway. Par défaut, les connexions utilisateur utilisent SSL sur le port 443 pour établir cette connexion. Pour permettre aux connexions utilisateur d'atteindre le réseau interne, vous devez autoriser SSL sur le port 443 via le premier pare-feu.

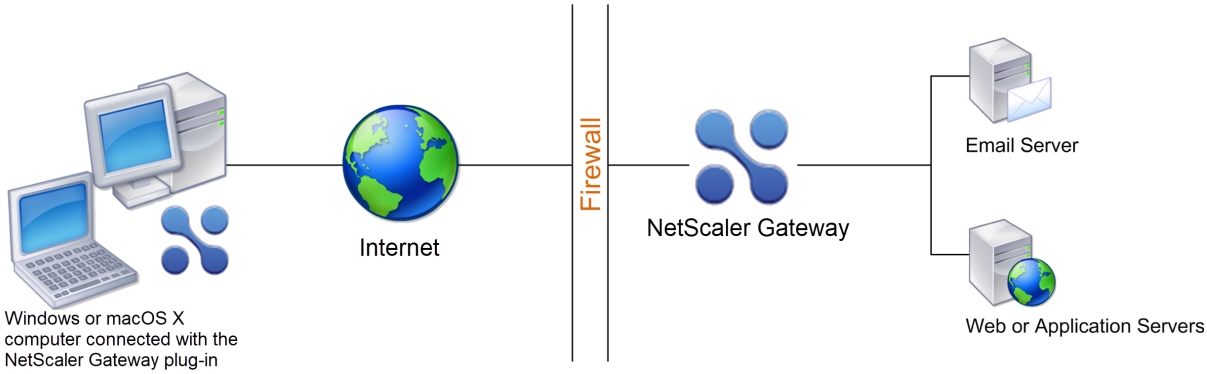
NetScaler Gateway déchiffre les connexions SSL de la machine utilisateur et établit une connexion au nom de l'utilisateur aux ressources réseau situées derrière le second pare-feu. Les ports qui doivent être ouverts via le deuxième pare-feu dépendent des ressources réseau auxquelles vous autorisez les utilisateurs externes à accéder.

Par exemple, si vous autorisez des utilisateurs externes à accéder à un serveur Web du réseau interne et que ce serveur écoute les connexions HTTP sur le port 80, vous devez autoriser HTTP sur le port 80 via le deuxième pare-feu. NetScaler Gateway établit la connexion via le second pare-feu au serveur HTTP du réseau interne pour le compte des machines utilisateur externes.

Déployez NetScaler Gateway dans un réseau sécurisé

Vous pouvez installer NetScaler Gateway sur le réseau sécurisé. Dans ce scénario, un pare-feu se trouve entre Internet et le réseau sécurisé. NetScaler Gateway réside à l'intérieur du pare-feu pour contrôler l'accès aux ressources du réseau.

Figure 1. NetScaler Gateway déployé dans le réseau sécurisé



Lorsque vous déployez NetScaler Gateway sur le réseau sécurisé, connectez une interface de NetScaler Gateway à Internet et l'autre interface aux serveurs s'exécutant sur le réseau sécurisé. L'intégration de NetScaler Gateway au réseau sécurisé permet aux utilisateurs locaux et distants d'y accéder. Comme cette configuration ne comporte qu'un seul pare-feu, le déploiement est moins sécurisé pour les utilisateurs qui se connectent depuis un emplacement distant. Bien que NetScaler Gateway intercepte le trafic en provenance d'Internet, celui-ci entre dans le réseau sécurisé avant que les utilisateurs ne soient authentifiés. Lorsque NetScaler Gateway est déployé dans une zone démilitarisée, les utilisateurs sont authentifiés avant que le trafic réseau n'atteigne le réseau sécurisé.

Lorsque NetScaler Gateway est déployé sur le réseau sécurisé, les connexions Citrix Secure Access pour Windows doivent traverser le pare-feu pour se connecter à NetScaler Gateway. Par défaut, les connexions utilisateur utilisent le protocole SSL sur le port 443 pour établir cette connexion. Pour prendre en charge cette connectivité, vous devez ouvrir le port 443 sur le pare-feu.

Configuration logicielle requise du client

March 27, 2024

NetScaler Gateway prend en charge les connexions utilisateur à l'aide du client Citrix Secure Access. Lorsque les utilisateurs ouvrent une session avec le plug-in, il établit un tunnel VPN complet. Avec le client Citrix Secure Access, les utilisateurs peuvent se connecter aux ressources réseau auxquelles vous autorisez l'accès.

Si les stratégies relatives aux terminaux sont configurées sur NetScaler Gateway, NetScaler Gateway télécharge et installe automatiquement le client Citrix EPA sur la machine utilisateur lorsque l'utilisateur ouvre une session.

Configuration système requise pour le client Citrix Secure Access

Le client Citrix Secure Access établit une connexion sécurisée entre l'ordinateur client et l'appliance NetScaler Gateway.

Le plug-in est distribué sous la forme d'une application de bureau pour les systèmes d'exploitation Microsoft Windows, macOS X et Linux. Une fois que vous vous êtes authentifié auprès de l'URL sécurisée de l'appliance NetScaler Gateway à l'aide de votre navigateur Web, le plug-in est téléchargé et installé automatiquement sur votre machine.

Le plug-in est configuré en tant qu'application mobile pour les appareils Android et iOS.

> **Remarque :**
>
> - Pour installer le plug-in, des privilèges admin/root sont requis sur le système d'exploitation.
> - Les navigateurs qui prennent en charge le client Citrix Secure Access prennent également en charge le VPN sans client.

Le client Citrix Secure Access en tant qu'application de bureau est pris en charge pour les systèmes d'exploitation et navigateurs Web suivants.

Système d'exploitation	Navigateurs compatibles
macOS X (10.9 et versions ultérieures)	Safari 7.1 ou version ultérieure ; Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 30 ou ultérieure
Windows 11	Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 24 ou ultérieure ; Edge Chromium

Système d'exploitation	Navigateurs compatibles
Windows 10 (x86 et x64)	Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 24 ou ultérieure ; Edge Chromium
Linux ; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox Release 44 et versions ultérieures ; Google Chrome 50 et versions ultérieures

> **Remarque :**
>
> Actuellement, les clients Citrix Secure Access et Citrix EPA pour Ubuntu ne prennent en charge que le gestionnaire d'affichage GNOME par défaut.

Si les packages de dépendances requis sont manquants, la commande les répertorie et l'installation du plug-in échoue. Ces packages de dépendances doivent être installés manuellement. Les administrateurs peuvent installer un package manquant en tapant la commande suivante à l'aide de l'interface de ligne de commande.

```
apt-get install <dependency package>
<!--NeedCopy-->
```

Le client Citrix Secure Access en tant qu'application mobile est pris en charge pour les systèmes d'exploitation suivants.

Appli VPN	Systèmes d'exploitation pris en charge
Android	Android 7.0 et versions ultérieures
iOS	iOS 12.0 et versions ultérieures

> **Remarque :**
>
> Si vous utilisez les dernières versions du système d'exploitation Apple, telles que macOS 14/iOS 17 et versions ultérieures, nous vous recommandons de passer à la version 23.09.1 ou ultérieure de Citrix Secure Access Client/Citrix SSO.

Configuration requise pour Endpoint Analysis

NetScaler Gateway installe le client Citrix EPA sur la machine utilisateur. Le client Citrix EPA analyse la machine utilisateur pour vérifier les exigences de sécurité des terminaux que vous avez configurées sur NetScaler Gateway. Les exigences incluent des informations, telles que le système d'exploitation, l'antivirus ou les versions du navigateur Web.

Lorsque les utilisateurs se connectent à NetScaler Gateway à l'aide du navigateur pour la première fois, le portail demande l'installation du client Citrix EPA. Lors des tentatives de connexion suivantes, le client Citrix EPA vérifie la configuration du contrôle de mise à niveau pour confirmer si la mise à niveau du client Citrix EPA est nécessaire. Si nécessaire, l'utilisateur est invité à télécharger et à installer la dernière version du client Citrix EPA. Le client Citrix EPA pour Windows est installé en tant qu'application Windows 32 bits. Le client Citrix EPA pour macOS est installé en tant qu'application 64 bits. Aucun privilège spécial n'est requis pour installer ou utiliser le client Citrix EPA, sauf lorsque vous utilisez EPA pour accéder aux certificats des appareils. Pour plus d'informations sur l'utilisation de l'EPA pour l'authentification par certificat d'appareil, voir Utiliser des certificats d'appareil pour l'authentification.

Les infobulles de la console de l'interface utilisateur d'administration expliquent en détail les analyses. Pour plus d'informations sur les bibliothèques EPA, reportez-vous à la section https://www.citrix.com/en-in/downloads/citrix-gateway/epa-libraries/.

> **Important :**
>
> - Les navigateurs qui prennent en charge l'EPA prennent également en charge le VPN sans client.
> - Lors de l'analyse des points de terminaison avant l'authentification, l'utilisateur ne peut pas se connecter avec le client Citrix Secure Access s'il n'installe pas le plug-in Endpoint Analysis ou ignore l'analyse.
> - Dans l'analyse des points de terminaison post-authentification, l'utilisateur peut accéder aux ressources pour lesquelles une analyse n'est pas nécessaire en utilisant un accès sans client ou en utilisant l'application Citrix Workspace.
> - Pour les analyses liées à OPSWAT, vous devez installer le package binaire `epaPackage.exe` sur la machine cliente.

Les logiciels suivants sont requis sur les machines utilisateur pour utiliser le plug-in Endpoint Analysis :

Système d'exploitation	Navigateurs compatibles
macOS (10.9 et versions ultérieures)	Safari 7.1 ou version ultérieure ; Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 30 ou ultérieure
Windows 11	Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 24 ou ultérieure ; Edge Chromium
Windows 10	Google Chrome version 30 ou ultérieure ; Mozilla Firefox version 24 ou ultérieure ; Edge Chromium

Système d'exploitation	Navigateurs compatibles
Linux ; Ubuntu 18.04 LTS, 20.04 LTS, 22.04 LTS.	Mozilla Firefox Release 44 et versions ultérieures ; Google Chrome 50 et versions ultérieures

Remarque :

- Toutes les éditions des variantes du système d'exploitation mentionnées précédemment sont prises en charge.
- Windows 10 et Windows 11 en modes S ne sont pas pris en charge.
- Pour les éditions Windows, tous les Service Packs et mises à jour critiques doivent être installés.
- Pour les versions de Mozilla Firefox, Endpoint Analysis doit être activé pour les plug-ins. La version minimale requise est 3.0.

Compatibilité de NetScaler Gateway avec les produits NetScaler

March 27, 2024

Le tableau suivant présente les produits NetScaler et les versions avec lesquels NetScaler Gateway 13.1 est compatible.

> **Remarque :**
>
> les fonctionnalités de NetScaler Gateway sont disponibles sur NetScaler VPX.

Produits NetScaler et versions prises en charge

Produit NetScaler	Version de sortie
Citrix SD-WAN	10.2, 11.0
Plateformes NetScaler	Tous les modèles MPX et VPX actuels, y compris les appliances conformes à la norme FIPS.
StoreFront	Toutes les versions StoreFront actuellement prises en charge.
Citrix Virtual Apps and Desktops	7.15, 1808, 1811, 1903, 1906, 1909, 2003, 2009, 2112, 1912 LTSR, 2203 LTSR
XenMobile	10.5, 10.6, 10.7, 10.8, 10.9, 10.10, 10.11, 10.12

Produit NetScaler	Version de sortie

Applications Citrix Workspace, applications de productivité mobiles Citrix et plug-ins

*La première version prise en charge pour chaque version logicielle est répertoriée dans le tableau suivant. Toutes les versions suivantes sont prises en charge, sauf indication contraire. Pour plus d'informations sur le cycle de vie des versions, reportez-vous à lamatrice des produits.

Application ou plug-in Citrix Workspace	Version minimale prise en charge*
Client Citrix Secure Access pour macOS X	3.1.8
Client Citrix Secure Access pour Windows	12.0
Client Citrix Secure Access pour iOS	3.1.4
Client Citrix Secure Access pour Android	2.0.14
Application Citrix Workspace pour Android	3.11
Application Citrix Workspace pour iOS	7.1.3
Application Citrix Workspace pour Mac	12.4
Application Citrix Workspace pour Windows	4.4
Application Citrix Workspace pour Linux	13.4
Application Citrix Workspace pour HTML5	2.3
Application Citrix Workspace pour Chrome	2.3
Secure Hub pour iOS	10.5
Secure Hub pour Android	10.5
Secure Mail pour iOS	10.5
SecureWeb pour iOS	10.5
Secure Mail pour Android	10.5
SecureWeb pour Android	10.5

> **Remarque :**
>
> - Pour plus de détails sur certaines des fonctionnalités couramment utilisées prises en

> charge pour chaque client VPN, consultez la section Clients VPN NetScaler Gateway et fonctionnalités prises en charge.

Licence NetScaler Gateway

March 27, 2024

Après avoir installé NetScaler Gateway, vous pouvez obtenir vos fichiers de licence Platform ou Universal auprès de Citrix. Vous ouvrez une session sur le site Web Citrix pour accéder à vos licences disponibles et générer un fichier de licences. Une fois le fichier de licence généré, vous le téléchargez sur un ordinateur. Lorsque le fichier de licence se trouve sur l'ordinateur, vous le chargez ensuite vers NetScaler Gateway. Pour plus d'informations sur les licences Citrix, consultez la section Système de licences Citrix.

Avant d'obtenir vos fichiers de licence, assurez-vous de configurer le nom d'hôte de l'appliance à l'aide de l'Assistant d'installation, puis de redémarrer l'appliance.

Pour obtenir vos licences, accédez à la page Web Activer, mettre à niveau et gérer les licences NetScaler. Sur cette page, vous pouvez obtenir votre nouvelle licence et activer, mettre à niveau et gérer les licences NetScaler.

Important :

> - Vous devez installer des licences sur NetScaler Gateway. L'appliance n'obtient pas de licences auprès du serveur de licences NetScaler.
> - Citrix vous recommande de conserver une copie locale de tous les fichiers de licences que vous recevez. Lorsque vous enregistrez une copie de sauvegarde du fichier de configuration, elle inclut tous les fichiers de licences téléchargés. Si vous devez réinstaller le logiciel de l'appliance NetScaler Gateway et que vous ne disposez pas d'une sauvegarde de la configuration, vous avez besoin des fichiers de licence d'origine.

Avant d'installer des licences sur NetScaler Gateway, définissez le nom d'hôte de l'appliance, puis redémarrez NetScaler Gateway. Vous utilisez l'Assistant d'installation pour configurer le nom d'hôte. Lorsque vous générez la licence universelle pour NetScaler Gateway, le nom d'hôte est utilisé dans la licence.

Types de licences NetScaler Gateway

NetScaler Gateway nécessite une licence de plateforme. La licence Platform autorise un nombre illimité de connexions à Citrix Virtual Apps, Citrix Virtual Desktops ou StoreFront à l'aide du proxy ICA.

Pour autoriser les connexions VPN au réseau à partir du client Citrix Secure Access, d'un point de connexion SmartAccess ou de Secure Hub, WorxWeb ou Secure Mail, vous devez également ajouter une licence universelle. NetScaler Gateway VPX est fourni avec la licence de plate-forme.

La licence de plate-forme est prise en charge sur les versions suivantes de NetScaler Gateway :

- NetScaler Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1
- NetScaler Gateway 11.0
- NetScaler Gateway 10.5
- NetScaler Gateway 10.1
- Access Gateway 10
- NetScaler VPX

> **Important :** Citrix vous recommande de conserver une copie locale de tous les fichiers de licences que vous recevez. Lorsque vous enregistrez une copie de sauvegarde du fichier de configuration, tous les fichiers de licence téléchargés sont inclus dans la sauvegarde. Si vous devez réinstaller le logiciel de l'appliance NetScaler Gateway et que vous ne disposez pas d'une sauvegarde de la configuration, vous avez besoin des fichiers de licence d'origine.

La licence Platform

La licence Platform autorise des connexions utilisateur illimitées aux applications publiées sur Citrix Virtual Apps ou aux bureaux virtuels depuis Citrix Virtual Desktops. Les connexions à l'aide de Citrix Receiver n'utilisent pas de licence universelle NetScaler Gateway. Ces connexions n'ont besoin que de la licence Platform. La licence de plate-forme est délivrée électroniquement avec toutes les nouvelles commandes NetScaler Gateway, qu'elles soient physiques ou virtuelles. Si vous possédez déjà une appliance couverte par un contrat de garantie ou de maintenance, vous pouvez obtenir la licence Platform sur le site Web de Citrix.

La licence universelle

La licence universelle NetScaler Gateway limite le nombre de sessions utilisateur simultanées au nombre de licences achetées. Si vous achetez 100 licences, vous pouvez avoir 100 sessions simultanées à tout moment. Si vous achetez une licence Standard Edition, vous pouvez avoir 500 sessions simultanées à tout moment. Lorsqu'un utilisateur met fin à une session, cette licence est libérée pour l'utilisateur suivant. Un utilisateur qui se connecte à NetScaler Gateway à partir de plusieurs ordinateurs occupe une licence pour chaque session.

Si toutes les licences sont occupées, aucune connexion supplémentaire ne peut être ouverte tant qu'un utilisateur ne met pas fin à une session ou que l'administrateur ne met fin à la session à l'aide de l'

utilitaire de configuration. Lorsqu'une connexion est fermée, la licence est libérée et peut être utilisée pour un nouvel utilisateur.

Lorsque vous recevez votre appliance NetScaler Gateway, l'attribution des licences s'effectue dans l'ordre suivant :

- Vous recevez le code d'accès à la licence (clé de licence) dans un e-mail.
- Vous utilisez l'assistant de configuration pour configurer NetScaler Gateway avec le nom d'hôte.
- Vous attribuez les licences NetScaler Gateway depuis le site Web de Citrix. Utilisez le nom d'hôte pour lier les licences à l'appliance pendant le processus d'allocation.
- Vous installez le fichier de licence sur NetScaler Gateway.

La licence universelle prend en charge les fonctionnalités suivantes :

- Tunnel VPN complet
- Micro VPN
- Analyse des points de terminaison
- SmartAccess basé sur des règles
- Accès sans client aux sites Web et aux partages de fichiers

Obtention de la licence universelle Vous devez disposer des informations suivantes avant d'accéder au site Web Citrix pour obtenir la licence universelle.

- L'ID utilisateur et le mot de passe de votre compte Citrix.

  Inscrivez-vous sur le site Web de Citrix (https://www.citrix.com/welcome/create-account/) pour recevoir votre ID utilisateur et votre mot de passe.
  Remarque : Si vous ne trouvez pas le code de licence ou votre ID utilisateur et votre mot de passe, contactez le service client Citrix.

- Le nom d'hôte de
  NetScaler Gateway

  Le champ de saisie de ce nom sur le site Web de Citrix fait la distinction entre majuscules et minuscules. Veillez donc à copier le nom d'hôte exactement tel qu'il est configuré sur l'appliance NetScaler.

- Le nombre de licences que vous souhaitez inclure dans le fichier de licences

  vous n'êtes pas obligés de télécharger toutes vos licences en une seule fois. Par exemple, si votre entreprise a acheté 100 licences, vous pouvez choisir d'en télécharger 50. Vous pourrez allouer le reste dans un autre fichier de licence ultérieurement. Plusieurs fichiers de licence peuvent être installés sur
  NetScaler Gateway.

Remarque : Avant d'obtenir vos licences, assurez-vous de configurer le nom d'hôte de l'appliance NetScaler à l'aide de l'assistant de configuration, puis redémarrez l'appliance.

Pour obtenir votre licence universelle

1. Connectez-vous au site Web Citrix (https://www.citrix.com/en-in/account/) à l'aide de vos informations d'identification Citrix.
2. Sous **Citrix Manage Licenses se trouve ici**, suivez les instructions pour obtenir votre fichier de licence.

Installation de la licence universelle Pour installer la licence, reportez-vous à la section « Installation de la licence ». Après l'installation, vérifiez que la licence a été installée correctement.

Vérification de l'installation de la licence universelle Avant de continuer, vérifiez que votre licence universelle est correctement installée.

Pour vérifier l'installation de la licence universelle à l'aide de l'interface de ligne de commande

1. Ouvrez une connexion SSH à l'appliance NetScaler à l'aide d'un client SSH, tel que PuTTY.
2. Connectez-vous à l'appliance NetScaler à l'aide des informations d'identification de l'administrateur.
3. Utilisez la commande show license pour vérifier que « VPN SSL = OUI » et que le nombre maximal d'utilisateurs est passé de 5 au nombre attendu d'utilisateurs simultanés.

Pour vérifier l'installation de la licence universelle à l'aide de l'interface graphique

1. Dans un navigateur Web, tapez l'adresse IP de l'appliance NetScaler, par exemple. `http://192.168.100.1`
2. Dans Nom d'utilisateur et Mot de passe, tapez les informations d'identification de l'administrateur.
3. Dans le volet de navigation, développez Système, puis cliquez sur Licences.
4. Dans le volet Licences, une coche verte s'affiche en regard de **. Le champ Nombre maximum d'utilisateurs autorisés de NetScaler Gateway affiche le nombre de sessions utilisateur simultanées sous licence sur l'appliance NetScaler.

Ressources connexes

- Système de licences Citrix

- Fiche technique NetScaler
- Types de licences NetScaler et NetScaler Gateway

Installation d'une licence sur NetScaler Gateway

March 27, 2024

Après avoir correctement téléchargé le fichier de licence sur votre ordinateur, vous pouvez l'installer sur NetScaler Gateway. La licence est installée dans le répertoire /nsconfig/license.

Si vous avez utilisé l'assistant de configuration pour configurer les paramètres initiaux de NetScaler Gateway, le fichier de licence est installé lorsque vous exécutez l'assistant. Si vous allouez une partie de vos licences et que, plus tard, vous attribuez un numéro supplémentaire, vous pouvez installer les licences sans utiliser l'Assistant d'installation.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système**, puis cliquez sur **Licences**.
2. Dans le volet d'informations, cliquez sur **Gérer les licences**.
3. Cliquez sur **Ajouter une nouvelle licence**, puis sur **Parcourir**, accédez au fichier de licence, puis cliquez sur **OK**.

   Un message s'affiche dans l'utilitaire de configuration indiquant que vous devez redémarrer NetScaler Gateway. Cliquez sur Reboot.

Définir le nombre maximal d'utilisateurs

Après avoir installé la licence sur l'appliance, vous devez définir le nombre maximal d'utilisateurs autorisés à se connecter à l'appliance. Vous devez définir le nombre maximal d'utilisateurs dans la stratégie d'authentification globale.

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous Paramètres, cliquez sur **Modifier les paramètres d'authentification AAA**.
3. Dans Nombre maximal d'utilisateurs, tapez le nombre total d'utilisateurs, puis cliquez sur **OK**.

   Le nombre indiqué dans ce champ correspond au nombre de licences contenues dans le fichier de licence. Ce nombre doit être inférieur ou égal au nombre total de licences installées sur l'appliance. Par exemple, vous installez une licence qui contient 100 licences utilisateur et une

seconde qui contient 400 licences utilisateur. Le nombre total de licences est égal à 500. Le nombre maximal d'utilisateurs pouvant ouvrir une session est égal ou inférieur à 500. Si 500 utilisateurs sont connectés, tous les utilisateurs qui tentent de se connecter au-delà de ce nombre se voient refuser l'accès jusqu'à ce qu'un utilisateur ferme sa session ou que vous mettiez fin à une session.

Vérifier l'installation de la licence universelle

Avant de continuer, vérifiez que votre licence universelle est correctement installée.

Pour vérifier l'installation de la licence universelle à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Licences.

   Dans le volet Licences, une coche verte apparaît à côté de NetScaler Gateway. Le champ Nombre maximum d'utilisateurs autorisés de NetScaler Gateway affiche le nombre de sessions utilisateur simultanées sous licence sur l'appliance.

Pour vérifier l'installation de la licence universelle à l'aide de l'interface de ligne de commande

1. Ouvrez une connexion Secure Shell (SSH) à l'appliance à l'aide d'un client SSH, tel que PuTTY.
2. Ouvrez une session sur l'appliance à l'aide des informations d'identification de l'administrateur.
3. À l'invite de commandes, tapez :

```
show license
<!--NeedCopy-->
```

La licence est correctement installée si le paramètre VPN SSL est égal à Oui et le paramètre Nombre maximal d'utilisateurs est égal au nombre de licences.

FAQ sur les licences NetScaler Gateway

March 27, 2024

Comment obtenir de l'aide concernant les licences d'essai ou de démonstration ?

La plupart des produits NetScaler sont désormais proposés sous forme d'expériences de démonstration individuelles complètes et privées, animées par des experts. Nos experts Citrix personnalisent la démonstration en fonction de vos besoins, de vos cas d'utilisation et de vos projets actifs. Aucun téléchargement, aucune licence ou installation n'est nécessaire. Vous avez besoin d'une configuration minimale pour voir une démonstration instantanée. Après la démonstration, pour procéder à une validation de concept ou à l'essai d'une solution Citrix qui s'applique à vos services, contactez des experts Citrix. Pour les démonstrations, cliquez sur https://demo.citrix.com/.

Comment installer les licences ?

Pour plus d'informations sur l'installation des licences, voir Pour installer une licence sur NetScaler Gateway.

Quels sont les différents types de licences Gateway ?

La licence Platform autorise un nombre illimité de connexions à Citrix Virtual Apps, Citrix Virtual Desktops ou StoreFront à l'aide du proxy ICA.
La licence universelle est une licence complémentaire qui s'ajoute aux licences de la plateforme NetScaler. Cela permet les connexions VPN au réseau à partir du client Citrix Secure Access, d'un point de connexion SmartAccess ou de Secure Hub, Secure Web ou Secure Mail. Pour plus de détails, consultez la section Types de licence NetScaler Gateway.

Combien de sessions utilisateur simultanées sont prises en charge ?

Les sessions prises en charge dépendent du type de licence de passerelle. Pour plus de détails, consultez la section Types de licence NetScaler Gateway.

Un autre facteur à prendre en compte est la capacité du matériel sous-jacent lui-même. Reportez-vous à la fiche technique de NetScaler MPX/SDX ou à la fiche technique de NetScaler VPX pour les considérations relatives aux performances.

Comment vérifier les sessions utilisateur simultanées sous licence actuelle ?

Dans l'utilitaire de configuration de l'onglet Configuration, développez **Système**, puis cliquez sur **Licences**.
Dans le volet **Licences**, une coche verte apparaît à côté de NetScaler Gateway. Le champ **Nombre maximum d'utilisateurs autorisés de NetScaler Gateway** affiche le nombre de sessions utilisateur simultanées sous licence sur l'appliance.

Comment vérifier si la limite de débit sous licence est atteinte ?

Vous pouvez extraire le débit en temps réel à l'aide de `newnslog`. Par exemple, si le débit de licence est de 500 Mbps, vous pouvez extraire le débit en temps réel supérieur à 500 à l'aide de la commande suivante.

```
nsconmsg -K newnslog -g mbits -d past -s disptime=1 -s ratecount=500 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Mon Feb  5 13:47:13 2018
 Index    rtime totalcount-val      delta rate/sec symbol-name&device-no&time
    12     7000      801130681       3701      528 allnic_tot_rx_mbits  Mon Feb  5 13:47:55 2018
    13        0      460776045       3682      526 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:47:55 2018
    14     7000      801134437       3756      536 allnic_tot_rx_mbits  Mon Feb  5 13:48:02 2018
    15        0      460779784       3739      534 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:02 2018
    16     7000      801138166       3729      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:09 2018
    17        0      460783497       3713      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:09 2018
    18     7000      801141896       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:16 2018
    19        0      460787213       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:16 2018
    20     7000      801145623       3727      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:23 2018
    21        0      460790929       3716      530 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:23 2018
    22     7000      801149353       3730      532 allnic_tot_rx_mbits  Mon Feb  5 13:48:30 2018
    23        0      460794646       3717      531 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:30 2018
    24     7000      801153067       3714      530 allnic_tot_rx_mbits  Mon Feb  5 13:48:37 2018
    25        0      460798342       3696      528 nic_tot_rx_mbits interface(0/2) Mon Feb  5 13:48:37 2018
```

Comment vérifier si les paquets sont abandonnés à la suite de l'atteinte du débit de licences ?

Vous pouvez utiliser la commande suivante pour vérifier si des paquets sont supprimés.

```
nsconmsg -K newnslog -d current -g nic_err_rl_pkt_drops -s disptime=1 |
    more
<!--NeedCopy-->
```

```
reltime:mili second between two records Fri Feb  2 00:12:38 2018
 Index    rtime    totalcount-val      delta rate/sec symbol-name&device-no&time
     0 1966993        23723602        478       68 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:38 2018
     1        0        48048402        465       66 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:38 2018
     2        0      8307679782     145475    20782 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:38 2018
     3     7000        23723933        331       47 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:45 2018
     4        0        48048712        310       44 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:45 2018
     5        0      8307787105     107323    15331 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:45 2018
     6     7000        23723941          8        1 nic_err_rl_pkt_drops interface(1/2) Fri Feb  2 00:12:52 2018
     7        0        48048735         23        3 nic_err_rl_pkt_drops interface(1/1) Fri Feb  2 00:12:52 2018
     8        0      8307811163      24058     3436 nic_err_rl_pkt_drops interface(0/2) Fri Feb  2 00:12:52 2018
```

Comment puis-je savoir quel est le débit autorisé pour une appliance NetScaler ?

Exécutez la commande `show license` à partir de l'interface de ligne de commande, puis utilisez le numéro de modèle pour obtenir le débit de la fiche technique MPX, SDX et VPX ADC ou passerelle.


```
> sh license
       License status:
                          Web Logging: YES
                     Surge Protection: YES
                       Load Balancing: YES
                    Content Switching: YES
                    Cache Redirection: YES
                         Sure Connect: YES
                  Compression Control: YES
                    Delta Compression: NO
                     Priority Queuing: YES
                       SSL Offloading: YES
          Global Server Load Balancing: YES
                       GSLB Proximity: YES
                  Http DoS Protection: YES
                      Dynamic Routing: YES
                    Content Filtering: YES
                   Integrated Caching: YES
                              SSL VPN: YES   (Maximum users = 5)   (Maximum ICA u
sers = 0)
                                  AAA: YES
                          OSPF Routing: YES
                           RIP Routing: YES
                           BGP Routing: YES
                              Rewrite: YES
              IPv6 protocol translation: YES
                   Application Firewall: YES
                             Responder: YES
                        HTML Injection: YES
                        NetScaler Push: YES
                  Web Interface on NS: YES
                               AppFlow: YES
                           CloudBridge: YES
                       Model Number ID: 5500
 Done
> 
```

CITRIX

Citrix NetScaler | Datasheet

NetScaler platform	MPX 9500	MPX 7500	MPX 5500	VPX 10/200/1000/3000
Platform attributes				
Processor	Intel Xeon L5410 (4 cores total)	Intel Xeon L5410 (4 cores total)	Intel Xeon E5205 (2 cores total)	Minimum Server Req.:[1] Dual core server with Intel® VTx or AMD-V™
Memory	8 GB	8 GB	4 GB	
Ethernet ports	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	8x 10/100/1000 BASE-T OR 4x 10/100/1000 BASE-T AND 4x 1000BASE-X SFP (fiber or copper)	4x 10/100/1000 BASE-T	• Citrix® XenServer® 5 (update 3 or better) • Windows Server 2008 R2 with Hyper-V role • VMWare ESX/ESXi 3.5 or higher • 4G RAM/20 GB hard drive • Hypervisor supported NIC
Transceivers support	SX, LX	SX, LX		
Software upgradable performance		Upgrade option to MPX 9500		Upgrade options to VPX 200, VPX 1000 and VPX 3000
Platform performance				
System throughput, Gbps	3	1	0.5	Up to 3.0[2]
HTTP requests/sec	200,000	100,000	50,000	Up to 100,000
SSL transactions/sec	20,000	10,000	5,000	Up to 500
SSL throughput, Gbps	3	1	0.5	Up to 1.0
Compression throughput, Gbps	2	1	0.5	Up to 0.75
SSL VPN: concurrent users	10,000	10,000	5,000	Up to 300[3]

Comment ajouter d'autres utilisateurs aux licences Gateway existantes ?

Vous pouvez installer une licence universelle supplémentaire. Par exemple, supposons que vous ayez installé une licence universelle contenant 100 licences utilisateur. Si vous installez la deuxième licence universelle qui contient 400 licences utilisateur, le nombre total de licences utilisateur est égal à 500.

Avant de commencer

March 27, 2024

Avant d'installer NetScaler Gateway, vous devez évaluer votre infrastructure et collecter des informations afin de planifier une stratégie d'accès qui réponde aux besoins spécifiques de votre organisation. Lorsque vous définissez votre stratégie d'accès, vous devez prendre en compte les implications en matière de sécurité et effectuer une analyse des risques. Vous devez également déterminer les réseaux auxquels les utilisateurs sont autorisés à se connecter et décider des stratégies qui autorisent les connexions utilisateur.

Outre la planification des ressources disponibles pour les utilisateurs, vous devez également planifier votre scénario de déploiement. NetScaler Gateway est compatible avec les produits NetScaler suivants :

- Citrix Endpoint Management
- Citrix Virtual Apps
- Citrix Virtual Desktops
- StoreFront
- Interface Web
- Citrix SD-WAN

Pour plus d'informations sur le déploiement de NetScaler Gateway, voir Déploiements courantset Intégrationaux produits NetScaler

Lorsque vous préparez votre stratégie d'accès, effectuez les étapes préliminaires suivantes :

- Identifiez les ressources. Répertoriez les ressources réseau auxquelles vous souhaitez fournir un accès, telles que le Web, le SaaS, les applications mobiles ou publiées, les bureaux virtuels, les services et les données que vous avez définis dans votre analyse des risques.
- Développez des scénarios d'accès. Créez des scénarios d'accès qui décrivent comment les utilisateurs accèdent aux ressources réseau. Un scénario d'accès est défini par le serveur virtuel utilisé pour accéder au réseau, aux résultats de l'analyse des points de terminaison, au type d'authentification ou à une combinaison des deux. Vous pouvez également définir la façon dont les utilisateurs ouvrent une session sur le réseau.

- Identifiez le logiciel client. Vous pouvez fournir un accès VPN complet avec le client Citrix Secure Access, en demandant aux utilisateurs de se connecter avec l'application Citrix Workspace, Secure Hub ou en utilisant un accès sans client. Vous pouvez également restreindre l'accès à la messagerie à Outlook Web App ou WorxMail. Ces scénarios d'accès déterminent également les actions que les utilisateurs peuvent effectuer lorsqu'ils y accèdent. Par exemple, vous pouvez spécifier si les utilisateurs peuvent modifier des documents à l'aide d'une application publiée ou en se connectant à un partage de fichiers.
- Associez des stratégies à des utilisateurs, des groupes ou des serveurs virtuels. Les stratégies que vous créez sur NetScaler Gateway s'appliquent lorsque l'individu ou l'ensemble d'utilisateurs répond à des conditions spécifiées. Vous déterminez les conditions en fonction des scénarios d'accès que vous créez. Vous créez ensuite des stratégies qui étendent la sécurité de votre réseau en contrôlant les ressources auxquelles les utilisateurs peuvent accéder et les actions que les utilisateurs peuvent effectuer sur ces ressources. Vous associez les stratégies aux utilisateurs, groupes, serveurs virtuels appropriés ou globalement.

Cette section inclut les rubriques suivantes pour vous aider à planifier votre stratégie d'accès :

- Planning for Security inclut des informations sur l'authentification et les certificats.
- Conditions préalables qui définissent le matériel et les logiciels réseau dont vous pourriez avoir besoin.
- La liste de contrôle préalable à l'installation que vous pouvez utiliser pour noter vos paramètres avant de configurer NetScaler Gateway.

Conditions préalables à l'installation de NetScaler Gateway

Avant de configurer les paramètres sur NetScaler Gateway, vérifiez les prérequis suivants :

- NetScaler Gateway est physiquement installé sur votre réseau et y a accès. NetScaler Gateway est déployé dans la zone démilitarisée ou sur le réseau interne derrière un pare-feu. Vous pouvez également configurer NetScaler Gateway dans une zone démilitarisée à double saut et configurer les connexions à une batterie de serveurs. Citrix recommande de déployer l'appliance dans la zone démilitarisée.
- Vous configurez NetScaler Gateway avec une passerelle par défaut ou avec des routes statiques vers le réseau interne afin que les utilisateurs puissent accéder aux ressources du réseau. NetScaler Gateway est configuré pour utiliser des routes statiques par défaut.
- Les serveurs externes utilisés pour l'authentification et l'autorisation sont configurés et en cours d'exécution. Pour plus d'informations, consultez la section Authentification et autorisation.
- Le réseau dispose d'un serveur de noms de domaine (DNS) ou d'un serveur Windows Internet Naming Service (WINS) pour la résolution des noms afin de fournir les fonctionnalités utilisateur correctes de NetScaler Gateway.

- Vous avez téléchargé les licences universelles pour les connexions utilisateur avec le client Citrix Secure Access depuis le site Web de Citrix et les licences sont prêtes à être installées sur NetScaler Gateway.
- NetScaler Gateway possède un certificat signé par une autorité de certification (CA) approuvée. Pour de plus amples informations, consultez la section Installation et gestion des certificats.

Avant d'installer NetScaler Gateway, utilisez la liste de contrôle de pré-installation pour noter vos paramètres.

Planification de la sécurité

Lorsque vous planifiez votre déploiement de NetScaler Gateway, vous devez comprendre les problèmes de sécurité de base associés aux certificats, ainsi qu'à l'authentification et à l'autorisation.

Configuration de la gestion sécurisée des certificats

Par défaut, NetScaler Gateway inclut un certificat de serveur SSL (Secure Sockets Layer) autosigné qui permet à l'appliance d'établir des liaisons SSL. Les certificats autosignés sont adéquats pour les tests ou pour des exemples de déploiements, mais NetScaler ne recommande pas de les utiliser pour les environnements de production. Avant de déployer NetScaler Gateway dans un environnement de production, Citrix vous recommande de demander et de recevoir un certificat de serveur SSL signé auprès d'une autorité de certification (CA) connue et de le télécharger sur NetScaler Gateway.

Si vous déployez NetScaler Gateway dans un environnement où NetScaler Gateway doit fonctionner en tant que client dans le cadre d'une liaison SSL (établir des connexions cryptées avec un autre serveur), vous devez également installer un certificat racine fiable sur NetScaler Gateway. Par exemple, si vous déployez NetScaler Gateway avec Citrix Virtual Apps et l'interface Web, vous pouvez chiffrer les connexions entre NetScaler Gateway et l'interface Web à l'aide du protocole SSL. Dans cette configuration, vous devez installer un certificat racine approuvé sur NetScaler Gateway.

Assistance pour l'authentification

Vous pouvez configurer NetScaler Gateway pour authentifier les utilisateurs et contrôler le niveau d'accès (ou d'autorisation) dont disposent les utilisateurs aux ressources réseau du réseau interne.

Avant de déployer NetScaler Gateway, votre environnement réseau doit disposer des répertoires et des serveurs d'authentification nécessaires à la prise en charge de l'un des types d'authentification suivants :

- LDAP
- RADIUS

- TACACS+
- Certificat client avec prise en charge de l'audit et de la carte à puce
- Configuration RSA avec RADIUS
- Authentification SAML

Si votre environnement ne prend en charge aucun de ces types d'authentification ou si vous avez une petite population d'utilisateurs distants, vous pouvez créer une liste d'utilisateurs locaux sur NetScaler Gateway. Vous pouvez ensuite configurer NetScaler Gateway pour authentifier les utilisateurs par rapport à cette liste locale. Avec cette configuration, vous n'avez pas besoin de gérer les comptes d'utilisateurs dans un répertoire externe distinct.

Sécurisez votre déploiement de NetScaler Gateway

Différents déploiements peuvent nécessiter différentes considérations de sécurité. Les directives de déploiement sécurisé de NetScaler fournissent des conseils de sécurité généraux pour vous aider à choisir un déploiement sécurisé approprié en fonction de vos exigences de sécurité spécifiques.

Pour plus de détails, consultez les directives de déploiement sécurisé de NetScaler.

Liste de contrôle de pré-installation de la passer

January 26, 2024

La liste de contrôle comprend une liste de tâches et d'informations de planification que vous devez effectuer avant d'installer NetScaler Gateway.

De l'espace est prévu pour que vous puissiez cocher chaque tâche au fur et à mesure que vous la terminez et que vous prenez des notes. Citrix vous recommande de prendre note des valeurs de configuration que vous devez saisir pendant le processus d'installation et lors de la configuration de NetScaler Gateway.

Pour savoir comment installer et configurer NetScaler Gateway, consultez la section Installationde NetScaler Gateway.

Machines utilisateur

- Assurez-vous que les machines utilisateur répondent aux conditions d'installation décrites dans la section Configuration système requise pour Citrix Secure Access
- Identifiez les appareils mobiles auxquels les utilisateurs se connectent. **Remarque** : Si les utilisateurs se connectent à un appareil iOS, vous devez activer la Secure Browse dans un profil de session.

Connectivité réseau de base de NetScaler Gateway

Citrix vous recommande d'obtenir des licences et des certificats de serveur signés avant de commencer à configurer l'appliance.

- Identifiez et prenez note du nom d'hôte de NetScaler Gateway. **Remarque** : Il ne s'agit pas du nom de domaine complet (FQDN). Le nom de domaine complet est contenu dans le certificat de serveur signé qui est lié au serveur virtuel.
- Obtenez des licences universelles sur le site Web Citrix
- Générez une demande de signature de certificat (CSR) et envoyez-la à une autorité de certification (CA). Entrez la date à laquelle vous envoyez le CSR à l'autorité de certification.
- Notez l'adresse IP du système et le masque de sous-réseau.
- Notez l'adresse IP du sous-réseau et le masque de sous-réseau.
- Notez le mot de passe administrateur. Le mot de passe par défaut fourni avec NetScaler Gateway est. `nsroot`
- Notez le numéro de port sur lequel NetScaler Gateway écoute les connexions utilisateur sécurisées. La valeur par défaut est le port TCP 443. Ce port doit être ouvert sur le pare-feu entre le réseau non sécurisé (Internet) et la zone démilitarisée.
- Notez l'adresse IP de la passerelle par défaut.
- Notez l'adresse IP et le numéro de port du serveur DNS. Le numéro de port par défaut est 53. En outre, si vous ajoutez directement le serveur DNS, vous devez également configurer ICMP (ping) sur l'appliance.
- Notez la première adresse IP et le nom d'hôte du premier serveur virtuel.
- Notez l'adresse IP et le nom d'hôte du deuxième serveur virtuel (le cas échéant).
- Notez l'adresse IP du serveur WINS (le cas échéant).

Réseaux internes accessibles via NetScaler Gateway

- Notez les réseaux internes auxquels les utilisateurs peuvent accéder via NetScaler Gateway. Exemple : 10.10.0.0/24
- Entrez tous les réseaux internes et les segments de réseau auxquels les utilisateurs doivent accéder lorsqu'ils se connectent via NetScaler Gateway à l'aide du client Citrix Secure Access.

Haute disponibilité

Si vous possédez deux appliances NetScaler Gateway, vous pouvez les déployer dans une configuration haute disponibilité dans laquelle un NetScaler Gateway accepte et gère les connexions, tandis qu'un second NetScaler Gateway surveille le premier dispositif. Si le premier NetScaler Gateway cesse d'accepter les connexions pour une raison quelconque, le second NetScaler Gateway prend le relais et commence à accepter activement les connexions.

- Notez le numéro de version du logiciel NetScaler Gateway.
- Le numéro de version doit être le même sur les deux appliances NetScaler Gateway.
- Notez le mot de passe administrateur (`nsroot`). Le mot de passe doit être le même sur les deux solutions matérielles-logicielles.
- Notez l'adresse IP et l'ID principaux de NetScaler Gateway. Le numéro d'identification maximal est de 64.
- Notez l'adresse IP et l'ID de NetScaler Gateway secondaires.
- Obtenez et installez la licence universelle sur les deux appliances.
- Installez la même licence universelle sur les deux appliances.
- Notez le mot de passe du nœud RPC.

Authentification et autorisation

NetScaler Gateway prend en charge différents types d'authentification et d'autorisation qui peuvent être utilisés selon différentes combinaisons. Pour plus d'informations sur l'authentification et l'autorisation, consultez la section Authentification et autorisation.

Authentification LDAP

Si votre environnement inclut un serveur LDAP, vous pouvez utiliser LDAP pour l'authentification.

- Notez l'adresse IP et le port du serveur LDAP.

  Si vous autorisez les connexions non sécurisées au serveur LDAP, le port par défaut est 389. Si vous chiffrez les connexions au serveur LDAP avec SSL, le port par défaut est 636.

- Notez le type de sécurité.

  Vous pouvez configurer la sécurité avec ou sans chiffrement.

- Notez le nom unique de liaison de l'administrateur.

  Si votre serveur LDAP nécessite une authentification, entrez le nom distinctif de l'administrateur que NetScaler Gateway doit utiliser pour s'authentifier lors de l'envoi de requêtes à l'annuaire LDAP. Un exemple est cn=administrator, CN=Users, dc=ace, dc=com.

- Notez le mot de passe administrateur.

  Le mot de passe est associé au nom unique de liaison de l'administrateur.

- Notez le nom unique de base.

  DN (ou niveau répertoire) sous lequel se trouvent les utilisateurs ; par exemple, ou=users, dc=ace, dc=com.

- Notez l'attribut du nom d'ouverture de session du serveur.

  Entrez l'attribut d'objet personne de l'annuaire LDAP qui spécifie le nom d'ouverture de session d'un utilisateur. La valeur par défaut est SAMAccountName. Si vous n'utilisez pas Active Directory, les valeurs communes de ce paramètre sont cn ou uid.
  Pour plus d'informations sur les paramètres de l'annuaire LDAP, consultez Configuration de l'authentification LDAP

- Notez l'attribut de groupe.
  Entrez l'attribut d'objet personne de l'annuaire LDAP qui spécifie les groupes auxquels appartient un utilisateur. La valeur par défaut est MemberOf. Cet attribut permet à NetScaler Gateway d'identifier les groupes d'annuaires auxquels appartient un utilisateur.

- Notez le nom du sous-attribut.

Authentification et autorisation RADIUS

Si votre environnement inclut un serveur RADIUS, vous pouvez utiliser RADIUS pour l'authentification.
L'authentification RADIUS inclut les produits RSA SecurID, SafeWord et Gemalto Protiva.

- Notez l'adresse IP et le port du serveur RADIUS principal. Le port par défaut est 1812.
- Notez le secret du serveur RADIUS principal (secret partagé).
- Notez l'adresse IP et le port du serveur RADIUS secondaire. Le port par défaut est 1812.
- Notez le secret du serveur RADIUS secondaire (secret partagé).
- Notez le type de codage du mot de passe (PAP, CHAP, MS-CHAP v1, MSCHAP v2).

Authentification SAML

Le langage SAML (Security Assertion Markup Language) est une norme XML pour l'échange d'authentification et d'autorisation entre les fournisseurs d'identité (IdP) et les fournisseurs de services.

- Obtenez et installez sur NetScaler Gateway un certificat IdP sécurisé.
- Notez l'URL de redirection.
- Notez le champ utilisateur.
- Notez le nom du certificat de signature.
- Notez le nom de l'émetteur SAML.
- Notez le groupe d'authentification par défaut.

Ouverture de ports via les pare-feu (DMZ à saut unique)

Si votre organisation protège le réseau interne à l'aide d'une seule zone démilitarisée et que vous déployez NetScaler Gateway dans la zone démilitarisée, ouvrez les ports suivants via les pare-feux. Si vous installez deux appliances NetScaler Gateway dans un déploiement DMZ à double saut, consultez la section Ouverture des ports appropriés sur les pare-feux.

Sur le pare-feu entre le réseau non sécurisé et la zone démilitarisée

- Ouvrez un port TCP/SSL (443 par défaut) sur le pare-feu entre Internet et NetScaler Gateway. Les machines utilisateur se connectent à NetScaler Gateway sur ce port.

Sur le pare-feu entre le réseau sécurisé

- Ouvrez un ou plusieurs ports appropriés sur le pare-feu entre la zone démilitarisée et le réseau sécurisé. NetScaler Gateway se connecte à un ou plusieurs serveurs d'authentification ou à des ordinateurs exécutant Citrix Virtual Apps and Desktops sur le réseau sécurisé sur ces ports.
- Notez les ports d'authentification.

  Ouvrez uniquement le port correspondant à votre configuration NetScaler Gateway.

  - Pour les connexions LDAP, la valeur par défaut est le port TCP 389.
  - Pour une connexion RADIUS, la valeur par défaut est le port UDP 1812. Notez les ports Citrix Virtual Apps and Desktops.

- Si vous utilisez NetScaler Gateway avec Citrix Virtual Apps and Desktops, ouvrez le port TCP 1494. Si vous activez la fiabilité de session, ouvrez le port TCP 2598 au lieu de 1494. Citrix recommande de garder ces deux ports ouverts.

Citrix Virtual Desktops, Citrix Virtual Apps, l'interface Web ou StoreFront

Effectuez les tâches suivantes si vous déployez NetScaler Gateway pour fournir un accès à Citrix Virtual Apps and Desktops via l'interface Web ou StoreFront. Le client Citrix Secure Access n'est pas requis pour ce déploiement. Les utilisateurs accèdent aux applications et aux bureaux publiés via NetScaler Gateway en utilisant uniquement des navigateurs Web et Citrix Receiver.

- Notez le nom de domaine complet ou l'adresse IP du serveur exécutant l'interface Web ou StoreFront.
- Notez le nom de domaine complet ou l'adresse IP du serveur exécutant la Secure Ticket Authority (STA) (pour l'interface Web uniquement).

Citrix Endpoint Management

Effectuez les tâches suivantes si vous déployez Citrix Endpoint Management sur votre réseau interne. Si les utilisateurs se connectent à Endpoint Management depuis un réseau externe, tel qu'Internet, ils doivent se connecter à NetScaler Gateway avant d'accéder aux applications mobiles, Web et SaaS.

- Notez le nom de domaine complet ou l'adresse IP d'Endpoint Management.
- Identifiez les applications Web, SaaS et mobiles iOS ou Android auxquelles les utilisateurs peuvent accéder.

Déploiement DMZ à double saut avec Citrix Virtual Apps

Effectuez les tâches suivantes si vous déployez deux appliances NetScaler Gateway dans une configuration DMZ à double saut pour prendre en charge l'accès aux serveurs exécutant Citrix Virtual Apps.

NetScaler Gateway dans la première zone démilitarisée

La première zone démilitarisée est la zone démilitarisée située à la périphérie de votre réseau interne (la plus proche d'Internet ou d'un réseau non sécurisé). Les clients se connectent à NetScaler Gateway dans la première zone démilitarisée via le pare-feu qui sépare Internet de la zone démilitarisée. Collectez ces informations avant d'installer NetScaler Gateway dans la première zone démilitarisée.

- Complétez les éléments de la section Connectivité réseau de base de NetScaler Gateway de cette liste de contrôle pour ce NetScaler Gateway.

  Lorsque vous complétez ces éléments, l'interface 0 connecte ce NetScaler Gateway à Internet et l'interface 1 connecte ce NetScaler Gateway à NetScaler Gateway dans la deuxième zone démilitarisée.

- Configurez les informations de la deuxième appliance DMZ sur l'appliance principale.

  Pour configurer NetScaler Gateway comme premier saut dans la zone démilitarisée à double saut, vous devez spécifier le nom d'hôte ou l'adresse IP de NetScaler Gateway dans la deuxième zone démilitarisée sur l'appliance située dans la première zone démilitarisée. Après avoir spécifié quand le proxy NetScaler Gateway est configuré sur l'appliance lors du premier saut, liez-le à NetScaler Gateway globalement ou à un serveur virtuel.

- Notez le protocole de connexion et le port entre les appliances.

  Pour configurer NetScaler Gateway comme premier saut dans la double DMZ, vous devez spécifier le protocole de connexion et le port sur lequel NetScaler Gateway de la seconde DMZ écoute les connexions. Le protocole de connexion et le port sont SOCKS avec SSL (port 443 par défaut). Le protocole et le port doivent être ouverts via le pare-feu qui sépare la première DMZ de la deuxième DMZ.

NetScaler Gateway dans la deuxième zone démilitarisée

La deuxième zone démilitarisée est la zone démilitarisée la plus proche de votre réseau interne et sécurisé. NetScaler Gateway déployé dans la seconde zone démilitarisée sert de proxy pour le trafic ICA, qui traverse la seconde zone démilitarisée entre les machines utilisateur externes et les serveurs du réseau interne.

- Effectuez les tâches décrites dans la section Connectivité réseau de base de NetScaler Gateway de cette liste de contrôle pour ce NetScaler Gateway.

  Lorsque vous complétez ces éléments, l'interface 0 connecte ce NetScaler Gateway à NetScaler Gateway dans la première zone démilitarisée. L'interface 1 connecte ce NetScaler Gateway au réseau sécurisé.

Installation et configuration de l'appliance NetScaler Gateway

January 26, 2024

Lorsque vous recevez votre appliance NetScaler Gateway, vous devez la déballer et préparer le site et le rack. Une fois que vous avez déterminé que l'emplacement où vous installez votre appliance répond aux normes environnementales et que le rack de serveur est en place conformément aux instructions, vous installez le matériel. Après avoir monté l'appliance, vous la connectez au réseau, à une source d'alimentation et au terminal de console que vous utilisez pour la configuration initiale. Après avoir mis l'appliance sous tension, vous effectuez la configuration initiale et vous attribuez des adresses IP de gestion et de réseau. Veillez à respecter les mises en garde et les avertissements énumérés avec les instructions d'installation.

Lors de l'installation d'un dispositif virtuel NetScaler VPX, vous devez d'abord acquérir l'image du dispositif virtuel et l'installer sur un hyperviseur ou un autre moniteur de machine virtuelle.

Citrix recommande d'utiliser la rubrique Liste de contrôle de pré-installation de NetScaler Gateway afin de prendre note de vos paramètres avant de tenter de configurer un dispositif NetScaler Gateway. La liste de contrôle inclut des informations sur l'installation de NetScaler Gateway et d'un dispositif.

Configurer l'appliance NetScaler Gateway à l'aide d'assistants

March 27, 2024

NetScaler Gateway possède les six assistants suivants que vous pouvez utiliser pour configurer les paramètres de l'appliance :

- L'assistant de première configuration s'affiche lorsque vous vous connectez à l'appliance NetScaler Gateway pour la première fois.
- L'assistant de configuration rapide vous aide à configurer les stratégies, expressions et paramètres appropriés pour les connexions à Citrix Endpoint Management, StoreFront et l'interface Web.
- L'assistant NetScaler Gateway vous aide à configurer les paramètres spécifiques à NetScaler Gateway.
- L'assistant de configuration vous aide à configurer les paramètres de base de NetScaler Gateway pour la première fois.
- La configuration intégrée de Citrix Endpoint Management vous aide à configurer votre environnement NetScaler Gateway et Citrix Endpoint Management.
- L'assistant Applications publiées vous aide à configurer les paramètres des connexions utilisateur à l'aide de l'application Citrix Workspace.

Assistant de première installation

Lorsque vous avez terminé d'installer et de configurer les paramètres initiaux sur l'appliance NetScaler Gateway, lorsque vous vous connectez à l'utilitaire de configuration pour la première fois, l'assistant de première installation s'affiche si les conditions suivantes ne sont pas remplies :

- Vous n'avez pas installé de licence sur l'appliance.
- Vous n'avez pas configuré de sous-réseau ou d'adresse IP mappée.
- Si l'adresse IP par défaut des appliances est 192.168.100.1.

Configurer NetScaler Gateway à l'aide de l'assistant de première configuration

Pour configurer NetScaler Gateway (l'appliance physique ou l'appliance virtuelle VPX) pour la première fois, vous avez besoin d'un ordinateur administratif configuré sur le même réseau que l'appliance.

Attribuez une adresse IP NetScaler Gateway (NSIP) comme adresse IP de gestion de votre appliance et une adresse IP de sous-réseau (SNIP) à laquelle vos serveurs peuvent se connecter. Vous attribuez un masque de sous-réseau qui s'applique à la fois aux adresses NetScaler Gateway et SNIP. Configurez également un fuseau horaire. Si vous attribuez un nom d'hôte, vous pouvez accéder à l'appliance en spécifiant son nom au lieu de l'adresse NSIP.

L'Assistant Première installation comporte deux sections. Dans la première section, vous configurez les paramètres système de base de l'appliance NetScaler Gateway, notamment :

Adresse NSIP, adresse SNIP et masque de sous-réseau Nom d'hôte de
l'appliance Serveurs

DNS Fuseau
horaire Mot de passe
administrateur
Dans la deuxième section, vous installez les licences. Si vous spécifiez l'adresse d'un serveur DNS, vous pouvez utiliser le numéro de série matériel (HSN) ou la clé de licence pour attribuer vos licences, au lieu de télécharger vos licences depuis un ordinateur local vers l'appliance.

Remarque : Citrix recommande d'enregistrer vos licences sur votre ordinateur local.

Lorsque vous avez terminé de configurer ces paramètres, NetScaler Gateway vous invite à redémarrer l'appliance. Lorsque vous ouvrez une nouvelle session sur l'appliance, vous pouvez utiliser d'autres assistants et l'utilitaire de configuration pour configurer d'autres paramètres.

Assistant de configuration rapide

L'assistant de configuration rapide vous permet de configurer plusieurs serveurs virtuels sur NetScaler Gateway. Vous pouvez ajouter, modifier et supprimer des serveurs virtuels.

L'assistant de configuration rapide permet une configuration transparente pour les déploiements suivants :

- Connexions de l'interface Web à Citrix Virtual Apps and Desktops, avec la possibilité de configurer plusieurs instances de la Secure Ticket Authority (STA)
- Citrix Endpoint Management uniquement
- StoreFront uniquement
- Citrix Endpoint Management et StoreFront ensemble

L'assistant de configuration rapide vous permet de configurer les paramètres suivants sur l'appliance :

- Nom du serveur virtuel, adresse IP et port
- Redirection d'un port non sécurisé vers un port sécurisé
- serveur LDAP
- Serveur RADIUS
- Certificats
- Serveur DNS
- Citrix Endpoint Management et Citrix Virtual Apps and Desktops

  Remarque : Pour activer l'authentification unique, vous devez activer manuellement l'option d'**authentification unique pour les applications Web** dans l'onglet **Créer un profil de session NetScaler Gateway > Expérience client pour l'action de session**.

NetScaler Gateway prend en charge les connexions utilisateur directement à Citrix Endpoint Management, ce qui permet aux utilisateurs d'accéder à leurs applications Web, SaaS et mobiles, ainsi qu'à ShareFile. Vous pouvez également configurer les paramètres de StoreFront, ce qui permet aux utilisateurs d'accéder à leurs applications Windows et à leurs bureaux virtuels.

Lorsque vous exécutez l'assistant de configuration rapide, les stratégies suivantes sont créées en fonction de vos paramètres Citrix Endpoint Management, StoreFront et de l'interface Web :

- Stratégies de session, y compris les stratégies et les profils pour Receiver, Receiver pour Web, le client Citrix Secure Access et le Program Neighborhood Agent
- Accès sans client
- Authentification LDAP et RADIUS

Configuration des paramètres à l'aide de l'assistant de configuration rapide

Vous pouvez configurer les paramètres dans NetScaler Gateway pour permettre la communication avec Citrix Endpoint Management, StoreFront ou Web Interface à l'aide de l'assistant de configuration rapide. Lorsque vous avez terminé la configuration, l'assistant crée les stratégies appropriées pour la communication entre NetScaler Gateway, Endpoint Management, StoreFront ou l'interface Web. Ces stratégies incluent les stratégies d'authentification, de session et d'accès sans client. Lorsque l'Assistant est terminé, les stratégies sont liées au serveur virtuel.

Lorsque vous avez terminé l'assistant de configuration rapide, NetScaler Gateway peut communiquer avec Endpoint Management ou StoreFront, et les utilisateurs peuvent accéder à leurs applications Windows, à leurs bureaux virtuels et à leurs applications Web, SaaS et mobiles. Les utilisateurs peuvent ensuite se connecter directement à Endpoint Management.

Au cours de l'assistant, vous configurez les paramètres suivants :

- Nom du serveur virtuel, adresse IP et port
- Redirection d'un port non sécurisé vers un port sécurisé
- Certificats
- serveur LDAP
- Serveur RADIUS
- Certificat client pour l'authentification (uniquement pour l'authentification à deux facteurs)
- Endpoint Management, StoreFront ou Interface Web

L'assistant de configuration rapide prend en charge l'authentification par certificat LDAP, RADIUS et client. Vous pouvez configurer l'authentification à deux facteurs dans l'assistant en suivant ces instructions :

- Si vous sélectionnez LDAP comme type d'authentification principal, vous pouvez configurer RADIUS en tant que type d'authentification secondaire.

- Si vous sélectionnez RADIUS comme type d'authentification principal, vous pouvez configurer LDAP en tant que type d'authentification secondaire.
- Si vous sélectionnez des certificats clients comme type d'authentification principal, vous pouvez configurer LDAP ou RADIUS comme type d'authentification secondaire.

Vous ne pouvez pas créer plusieurs stratégies d'authentification LDAP à l'aide de l'assistant de configuration rapide. Par exemple, vous souhaitez configurer une stratégie qui utilise SAMAccountName dans le champ **Attribut de nom d'ouverture de session du serveur** et une deuxième stratégie LDAP qui utilise le nom principal d'utilisateur (UPN) dans le champ **Attribut du nom d'ouverture de session du serveur**. Pour configurer ces stratégies distinctes, utilisez l'utilitaire de configuration NetScaler Gateway pour créer les stratégies d'authentification. Pour plus d'informations, consultez la section Configuration de l'authentification LDAP.

Vous pouvez configurer des certificats pour NetScaler Gateway dans l'assistant de configuration rapide en utilisant les méthodes suivantes :

- Sélectionnez un certificat installé sur l'appliance.
- Installez un certificat et une clé privée.
- Sélectionnez un certificat de test.
  Remarque : Si vous utilisez un certificat de test, vous devez ajouter le nom de domaine complet (FQDN) figurant dans le certificat.

Vous pouvez ouvrir l'**assistant de configuration rapide** de l'une des deux manières suivantes :

- Lorsque vous êtes sur la page d'ouverture de session de NetScaler Gateway et que vous sélectionnez **NetScaler Gateway** dans **Type de déploiement**, l'onglet **Accueil** apparaît. Si vous sélectionnez une autre option dans **Type de déploiement**, l'onglet **Accueil** n'apparaît pas.
- À partir du lien **Créer/Surveiller NetScaler Gateway dans le volet de détails de NetScaler Gateway**. Le lien apparaît si vous installez une licence qui active les fonctionnalités de NetScaler. Si vous accordez une licence à l'appliance pour NetScaler Gateway uniquement, le lien ne s'affiche pas.

Après l'exécution initiale de l'Assistant, vous pouvez l'exécuter à nouveau pour créer davantage de serveurs et de paramètres virtuels.

Important : si vous utilisez l'assistant de configuration rapide pour configurer un serveur virtuel NetScaler Gateway supplémentaire, vous devez utiliser une adresse IP unique. Vous ne pouvez pas utiliser la même adresse IP que celle utilisée sur un serveur virtuel existant. Par exemple, vous disposez d'un serveur virtuel avec l'adresse IP 192.168.10.5 avec un numéro de port 80. Vous exécutez l'assistant de configuration rapide pour créer un deuxième serveur virtuel avec l'adresse IP 192.168.10.5 avec le numéro de port 443. Lorsque vous essayez d'enregistrer la configuration, une erreur se produit.

Pour configurer les paramètres à l'aide de l'assistant de configuration rapide

1. Dans l'utilitaire de configuration, effectuez l'une des opérations suivantes :

    a) Si l'appliance possède une licence pour NetScaler Gateway uniquement, cliquez sur l'onglet **Accueil**.
    b) Si l'appliance est autorisée à inclure les fonctionnalités de NetScaler, dans l'onglet Configuration, dans le volet de navigation, cliquez sur **NetScaler Gateway**, puis dans le volet de détails, sous **Mise en route**, cliquez sur **Configurer NetScaler Gateway** pour Enterprise Store.

2. Dans le tableau de bord, cliquez sur **Créer un nouveau NetScaler Gateway**.
3. Dans les **paramètres de NetScaler Gateway**, configurez les éléments suivants :

    a) Dans **Nom**, tapez le nom du serveur virtuel.
    b) Dans la **zone Adresse IP**, tapez l'adresse IP du serveur virtuel.
    c) Dans **Port**, tapez le numéro de port. Le numéro de port par défaut est 443.
    d) Sélectionnez Rediriger les demandes du port 80 vers le port sécurisé pour permettre aux connexions utilisateur du port 80 d'accéder au port 443.

4. Cliquez sur **Continuer**.
5. Sur la page Certificat, effectuez l'une des opérations suivantes :

    a) Cliquez sur **Choisir un certificat**, puis dans Certificat, sélectionnez le certificat.
    b) Cliquez sur **Installer le certificat,** puis dans **Choisir un certificat** et dans **Choisir une clé**, cliquez sur **Parcourir** pour accéder au certificat et à la clé privée.
    c) Cliquez sur **Utiliser le certificat de test**, puis dans Certificat FQDN, entrez le nom de domaine complet (FQDN) contenu dans le certificat de test.

6. Cliquez sur **Continuer**.
7. Dans les paramètres d'authentification, procédez comme suit :

    a) Dans **Authentification principale**, sélectionnez LDAP, RADIUS ou Cert.
    b) Sélectionnez un serveur d'authentification ou configurez les paramètres du type d'authentification sélectionné à l'étape précédente. Si vous sélectionnez Cert, sélectionnez le certificat client ou installez un nouveau certificat client.
    c) Dans **Authentification secondaire**, sélectionnez le type d'authentification, puis configurez les paramètres du serveur d'authentification.

8. Cliquez sur **Continuer**.

Lorsque vous avez terminé de configurer les paramètres réseau et d'authentification, vous pouvez ensuite configurer les paramètres Citrix Endpoint Management ou Citrix Virtual Apps and Desktops (StoreFront ou Interface Web).

Configuration des paramètres du magasin d'entreprise NetScaler Gateway prend en charge l'accès des utilisateurs aux applications Web, SaaS et mobiles et à ShareFile uniquement via Endpoint Management. Si vous déployez également StoreFront ou l'interface Web, les utilisateurs ont accès aux applications Windows et aux bureaux virtuels. Vous pouvez configurer les paramètres des options suivantes :

- Endpoint Management uniquement
- StoreFront uniquement
- Endpoint Management et StoreFront ensemble
- Interface Web uniquement

Lorsque vous cliquez sur **Continuer** dans la procédure précédente, vous pouvez ensuite configurer les paramètres de votre scénario de déploiement. Les procédures suivantes démarrent sur la page Paramètres d'intégration Citrix.

Une fois le serveur virtuel créé, la modification du serveur virtuel dans l'assistant de configuration rapide ne vous permet pas de modifier les paramètres Citrix Endpoint Management ou Citrix Virtual Apps and Desktops.

Par exemple, si vous annulez la configuration d'un serveur virtuel à n'importe quel stade avant de configurer les paramètres de **Citrix Enterprise Store**, l'Assistant sélectionne automatiquement l'interface Web sans configurer de paramètres. Lorsque cette situation se produit, vous pouvez modifier les détails du serveur virtuel pour configurer l'interface Web, mais vous ne pouvez pas passer à Citrix Endpoint Management. Pour basculer, vous devez créer un nouveau serveur virtuel et ne pas annuler l'Assistant à aucun moment pendant la configuration. Si vous n'avez pas besoin du serveur virtuel de l'interface Web, vous pouvez le supprimer à l'aide de l'assistant de configuration rapide.

Pour configurer les paramètres de StoreFront uniquement

1. Cliquez sur **Citrix Virtual Apps and Desktops**.
2. Dans **Deployment Type**, sélectionnez **StoreFront**.
3. Dans le nom de domaine **complet StoreFront**, entrez le nom de domaine complet (FQDN) du serveur StoreFront.
4. Dans **Receiver pour Web Path**, conservez le chemin par défaut ou entrez votre propre chemin.
5. Sélectionnez **HTTPS** pour sécuriser les connexions utilisateur.
6. Dans **Domaine d'authentification unique**, saisissez le domaine de StoreFront.
7. Dans **URL STA**, entrez l'adresse IP complète ou le nom de domaine complet du serveur exécutant la Secure Ticket Authority (STA) si vous déployez StoreFront et fournissez un accès aux applications publiées à partir de Citrix Virtual Apps ou de bureaux virtuels à partir de Citrix Virtual Desktops.
8. Cliquez sur **Terminé**.

Lorsque les utilisateurs se connectent via NetScaler Gateway à StoreFront, ils peuvent démarrer leurs applications et leurs postes de travail depuis Receiver pour Web ou Receiver.

Pour configurer les paramètres pour Endpoint Management uniquement

1. Cliquez sur **Citrix Endpoint Management**.
2. Dans le nom de **domaine complet d'App Controller**, saisissez le nom de domaine complet pour Endpoint Management.
3. Cliquez sur **Terminé**.

Pour configurer les paramètres de l'interface Web

1. Dans l'assistant de configuration rapide, cliquez sur **Citrix Virtual Apps and Desktops**.
2. Dans **Type de déploiement**, sélectionnez **Interface Web**, puis configurez les éléments suivants :

    a) Dans l'**URL du site Citrix Virtual Apps**, tapez l'adresse IP complète ou le nom de domaine complet de l'interface Web.
    b) Dans l'**URL du site Citrix Virtual Apps Services**, saisissez l'adresse IP complète ou le nom de domaine complet de l'interface Web avec le chemin de l'application Citrix Workspace. Vous pouvez entrer le chemin d'accès par défaut ou le vôtre.
    c) Dans **Domaine d'authentification unique**, saisissez le domaine à utiliser.
    d) Dans **URL STA**, saisissez l'adresse IP complète ou le nom de domaine complet du serveur exécutant la STA.

3. Cliquez sur **Terminé**.

Assistant NetScaler Gateway

Vous utilisez l'assistant NetScaler Gateway pour configurer les paramètres suivants sur l'appliance :

- Serveurs virtuels
- Certificats
- Fournisseurs de services de noms
- Authentification
- Authorization
- Redirection des ports
- Accès sans client
- Accès sans client pour SharePoint

Configuration des paramètres à l'aide de l'assistant NetScaler Gateway

Après avoir exécuté l'assistant de configuration, vous pouvez exécuter l'assistant NetScaler Gateway pour configurer d'autres paramètres sur NetScaler Gateway. Vous exécutez l'assistant NetScaler Gateway à partir de l'utilitaire de configuration.

NetScaler Gateway est fourni avec un certificat de test. Si vous ne possédez pas de certificat signé par une autorité de certification (CA), vous pouvez utiliser le certificat de test lorsque vous utilisez l'assistant NetScaler Gateway. Lorsque vous recevez le certificat signé, vous pouvez supprimer le certificat de test et installer le certificat signé. Citrix recommande d'obtenir le certificat signé avant de mettre NetScaler Gateway à la disposition du public pour les utilisateurs.

Remarque : Vous pouvez créer une demande de signature de certificat (CSR) depuis l'assistant NetScaler Gateway. Si vous utilisez l'assistant NetScaler Gateway pour créer le CSR, vous devez quitter l'assistant puis redémarrer l'assistant lorsque vous recevez le certificat signé de l'autorité de certification. Pour plus d'informations sur les certificats, consultez la section Installation et gestion des certificats.

Vous pouvez configurer les connexions utilisateur pour le protocole Internet version 6 (IPv6) dans l'assistant NetScaler Gateway lorsque vous configurez un serveur virtuel. Pour plus d'informations sur l'utilisation d'IPv6 pour les connexions utilisateur, consultez Configuration d'IPv6 pour les connexions utilisateur.

Pour démarrer l'assistant NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur NetScaler Gateway.
2. Dans le volet d'informations, sous Getting Started, cliquez sur l'assistant NetScaler Gateway.
3. Cliquez sur Suivant, puis suivez les instructions de l'assistant.

Assistant d'installation

Vous utilisez l'Assistant d'installation pour configurer les paramètres initiaux suivants sur l'appliance :

- Adresse IP système et masque de sous-réseau
- Adresse IP et masque de sous-réseau mappés
- Nom d'hôte
- passerelle par défaut
- Licences

Remarque : Avant d'exécuter l'Assistant d'installation, téléchargez vos licences depuis le site Web de Citrix. Pour plus d'informations, consultez
Licensing NetScaler Gateway

Assistant Applications publiées

Vous utilisez l'assistant d'applications publiées pour configurer NetScaler Gateway afin de vous connecter aux serveurs exécutant Citrix Virtual Apps and Desktops sur le réseau interne. Avec l'assistant Applications publiées, vous pouvez :

- Sélectionnez un serveur virtuel pour les connexions à la batterie de serveurs.
- Configurez les paramètres des connexions utilisateur pour l'interface Web ou StoreFront, l'authentification unique et l'Secure Ticket Authority.
- Créez ou sélectionnez des stratégies de session pour SmartAccess.

Dans l'assistant, vous pouvez également créer des expressions de stratégie de session pour les connexions utilisateur. Pour plus d'informations sur la configuration de NetScaler Gateway pour se connecter à une batterie de serveurs, consultez la section Fournir un accès aux applications publiées et aux bureaux virtuels via l'interface Web.

Configuration intégrée de Citrix Endpoint Management

Vous pouvez déployer NetScaler Gateway avec Citrix Endpoint Management MDM, qui permet d'évoluer, de garantir la haute disponibilité des applications et de maintenir la sécurité. Pour utiliser la configuration Citrix Endpoint Management, vous devez installer la version 10.1, Build 120.1316.e.

La configuration intégrée de Citrix Endpoint Management crée les éléments suivants :

- Serveurs d'équilibrage de charge pour Device Manager.
- Serveurs d'équilibrage de charge pour Microsoft Exchange avec filtrage des e-mails.
- Serveurs d'équilibrage de charge pour ShareFile.

Pour plus d'informations sur la création de paramètres avec la configuration intégrée de Citrix Endpoint Management, consultez Configuration des paramètres pour votre environnement Citrix Endpoint Management

Configurer NetScaler Gateway

March 27, 2024

Après avoir configuré les paramètres réseau de base sur NetScaler Gateway, vous configurez les paramètres détaillés afin que les utilisateurs puissent se connecter aux ressources réseau du réseau sécurisé. Ces paramètres sont les suivants :

- Serveurs virtuels. Vous pouvez configurer plusieurs serveurs virtuels sur NetScaler Gateway, ce qui vous permet de créer différentes stratégies en fonction du scénario utilisateur que vous devez implémenter. Chaque serveur virtuel possède sa propre adresse IP, son propre certificat et son propre jeu de stratégies. Par exemple, vous pouvez configurer un serveur virtuel et restreindre les utilisateurs aux ressources réseau du réseau interne en fonction de leur appartenance à des groupes et des stratégies que vous liez aux serveurs virtuels. Vous pouvez créer des serveurs virtuels en utilisant les méthodes suivantes :
  - Assistant de configuration rapide
  - Assistant NetScaler Gateway
  - utilitaire de configuration
- Haute disponibilité. Vous pouvez configurer la haute disponibilité lorsque vous déployez deux appliances NetScaler Gateway sur votre réseau. Si les appliances principales tombent en panne, l'appliance secondaire peut prendre le relais sans affecter les sessions utilisateur.
- Certificats. Vous pouvez utiliser des certificats pour sécuriser les connexions des utilisateurs à NetScaler Gateway. Lorsque vous créez une demande de signature de certificat (CSR), vous ajoutez le nom de domaine complet au certificat. Vous pouvez lier des certificats à des serveurs virtuels.
- Authentification. NetScaler Gateway prend en charge plusieurs types d'authentification, notamment le LDAP local, le RADIUS, le SAML, les certificats clients et TACACS+. De plus, vous pouvez configurer l'authentification en cascade et l'authentification à deux facteurs.
  Remarque : Si vous utilisez RSA, Safeword ou Gemalto Protiva pour l'authentification, vous configurez ces types à l'aide de RADIUS.
- Connexions utilisateur. Vous pouvez configurer les connexions utilisateur à l'aide de profils de session. Dans le profil, vous pouvez déterminer les plug-ins auxquels les utilisateurs peuvent se connecter, ainsi que les restrictions que les utilisateurs peuvent avoir besoin. Vous pouvez ensuite créer une stratégie avec un seul profil. Vous pouvez lier des stratégies de session aux utilisateurs, aux groupes et aux serveurs virtuels.
- Page d'accueil. Vous pouvez utiliser l'interface d'accès par défaut comme page d'accueil ou créer une page d'accueil personnalisée. La page d'accueil s'affiche lorsque les utilisateurs se connectent correctement à NetScaler Gateway.
- Analyse des points de terminaison. Vous pouvez configurer des stratégies sur NetScaler Gateway qui vérifient la présence de logiciels, de fichiers, d'entrées de registre, de processus et de systèmes d'exploitation sur la machine utilisateur lorsque les utilisateurs ouvrent une session. L'analyse des points de terminaison vous permet d'accroître la sécurité de votre réseau en exigeant que la machine utilisateur dispose du logiciel requis.

Utilisation de l'utilitaire de configuration

L'utilitaire de configuration vous permet de configurer la plupart des paramètres de NetScaler Gateway. Vous utilisez un navigateur Web pour accéder à l'utilitaire de configuration.

Ouvrez une session sur l'utilitaire de configuration

1. Dans un navigateur Web, saisissez l'adresse IP système de NetScaler Gateway, par exemple. `http://192.168.100.1`
   Remarque : NetScaler Gateway est préconfiguré avec une adresse IP par défaut 192.168.100.1 et un masque de sous-réseau 255.255.0.0.
2. Dans Nom d'utilisateur et mot de passe, tapez `nsroot`.
3. Dans Type de déploiement, sélectionnez NetScaler Gateway, puis cliquez sur Connexion.

Lorsque vous ouvrez une session sur l'utilitaire de configuration pour la première fois, le tableau de bord s'ouvre par défaut sous l'onglet **Accueil**. Dans l'onglet **Accueil**, vous pouvez utiliser l'assistant Configuration rapide pour configurer les paramètres d'un serveur virtuel, l'authentification, les certificats et Citrix Endpoint Management. Vous pouvez également configurer les paramètres de StoreFront ou de l'interface Web dans l'assistant de configuration rapide.

Pour plus d'informations sur la configuration de NetScaler Gateway, consultez :

- Configuration des paramètres initiaux à l'aide de l'assistant d'installation.
- Configuration des paramètres avec l'assistant de configuration rapide
- Configuration des paramètres à l'aide de l'assistant NetScaler Gateway.

Créer des serveurs virtuels

March 27, 2024

Un serveur virtuel est un point d'accès auquel les utilisateurs ouvrent une session. Chaque serveur virtuel possède sa propre adresse IP, son propre certificat et son propre jeu de stratégies. Un serveur virtuel consiste en une combinaison d'une adresse IP, d'un port et d'un protocole qui accepte le trafic entrant. Les serveurs virtuels contiennent les paramètres de connexion lorsque les utilisateurs ouvrent une session sur l'appliance. Vous pouvez configurer les paramètres suivants sur les serveurs virtuels :

- Certificats
- Authentification

- Stratégies
- Signets
- Pools d'adresses (également appelés pools d'adresses IP ou IP intranet)
- Déploiement de DMZ à double saut avec NetScaler Gateway
- Secure Ticket Authority
- Transfert de session proxy ICA SmartAccess

Si vous exécutez l'assistant NetScaler Gateway, vous pouvez créer un serveur virtuel au cours de l'assistant. Vous pouvez configurer d'autres serveurs virtuels de l'une des manières suivantes :

- **Depuis le nœud des serveurs virtuels**. Ce nœud se trouve dans le volet de navigation de l'utilitaire de configuration. Vous pouvez ajouter, modifier et supprimer des serveurs virtuels à l'aide de l'utilitaire de configuration.
- **Avec l'assistant de configuration rapide**. Si vous déployez Citrix Endpoint Management, StoreFront ou l'interface Web dans votre environnement, vous pouvez utiliser l'assistant de configuration rapide pour créer le serveur virtuel et toutes les stratégies nécessaires à votre déploiement.

Si vous souhaitez que les utilisateurs ouvrent une session et utilisent un type d'authentification spécifique, tel que RADIUS, vous pouvez configurer un serveur virtuel et attribuer au serveur une adresse IP unique. Lorsque les utilisateurs ouvrent une session, ils sont dirigés vers le serveur virtuel, puis invités à entrer leurs informations d'identification RADIUS.

Vous pouvez également configurer la manière dont les utilisateurs se connectent à NetScaler Gateway. Vous pouvez utiliser une stratégie de session pour configurer le type de logiciel utilisateur, la méthode d'accès et la page d'accueil affichée par les utilisateurs après la connexion.

Pour créer des serveurs virtuels

Vous pouvez ajouter, modifier, activer ou désactiver et supprimer des serveurs virtuels à l'aide de l'interface graphique de NetScaler Gateway ou de l'assistant de configuration rapide. Pour plus d'informations sur la configuration d'un serveur virtuel à l'aide de l'assistant de configuration rapide, consultez
Configuration des paramètres à l'aide de l'assistant de configuration rapide.

> **Remarque :**
>
> Le serveur virtuel VPN prend en charge la version 1.0 de DTLS par défaut. Pour activer la version 1.2 de DTLS, voir Configurer le serveur virtuel VPN DTLS à l'aide d'un serveur virtuel VPN SSL.

Pour créer un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.

2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Configurez les paramètres en fonction de vos besoins.
4. Cliquez sur **Create**, puis cliquez sur **Close**.

Pour créer un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
add vpn vserver <name> <serviceType> [<IPAddress> [<port>]
<!--NeedCopy-->
```

Exemple :

```
add vpn vserver gatewayserver SSL 1.1.1.1 443
<!--NeedCopy-->
```

Points à noter lors de la liaison d'un profil réseau au serveur virtuel VPN

Vous pouvez créer des profils réseau (profils réseau) pour configurer l'appliance pour qu'elle utilise une adresse IP source spécifiée et lie le profil réseau au serveur virtuel VPN. Toutefois, notez les points suivants lorsque vous liez un profil réseau au serveur virtuel VPN.

- Lorsque vous liez un profil réseau à un serveur virtuel NetScaler Gateway, le profil réseau ne sélectionne pas de SNIP spécifique à utiliser par le serveur virtuel ou le service pour le trafic vers les serveurs principaux. Au lieu de cela, l'appliance de passerelle ignore la liaison du profil réseau et utilise la méthode Round Robin pour sélectionner les SNIP.
- Le profil réseau ne fonctionne pas pour les services générés dynamiquement (STA, moniteur SF). Pour STA et d'autres services générés dynamiquement, vous pouvez lier directement le profil réseau à ces moniteurs et ces moniteurs sont utilisés à ce stade. Toutefois, si vous disposez de plusieurs passerelles sur le même dispositif, toutes les passerelles utilisent le même profil réseau pour les moniteurs configurés.

Pour plus d'informations sur le profil réseau, consultez Utiliser une adresse IP source spécifiée pour la communicationprincipale.

Utilisateurs actuels et nombre total d'utilisateurs connectés sur le serveur virtuel

Utilisateurs actuels : nombre d'utilisateurs connectés à un serveur virtuel spécifique. Il est recommandé de surveiller les utilisateurs actuels pour le suivi des CCU.

Nombre**total d'utilisateurs connectés :** nombre d'utilisateurs disposant d'une ou de plusieurs connexions actives via le serveur virtuel spécifique. Le nombre total d'utilisateurs connectés est principalement utilisé dans le proxy ICA.

Vous pouvez utiliser le compteur du nombre total d'utilisateurs connectés dans les scénarios suivants :

- Considérez qu'une connexion ICA est établie mais qu'aucune session d'authentification, d'autorisation et d'audit correspondante n'est établie. Dans ce scénario, un utilisateur lance une application ou un bureau, ferme le navigateur et continue de travailler sur l'application ou le bureau lancé. La session d'authentification, d'autorisation et d'audit est dépassé, mais la connexion est toujours active. Le nombre total d'utilisateurs connectés peut être utilisé pour identifier les utilisateurs qui sont toujours connectés.
- Dans le routage optimal HDX, la passerelle d'authentification et la passerelle ICA peuvent se trouver sur différentes appliances. Dans ce cas, le nombre total d'utilisateurs connectés peut être utilisé pour identifier le nombre d'utilisateurs connectés sur la passerelle ICA.

Points à noter :

- Les utilisateurs actuels dépassent le nombre total d'utilisateurs connectés lorsqu'il y a des sessions actives (pas encore dépassées) mais qu'il n'y a pas de connexion active sur ces sessions. Par exemple, un utilisateur a lancé une application ou un bureau et l'a fermé immédiatement, mais ne s'est pas déconnecté de la session d'authentification, d'autorisation et d'audit.
- Le nombre total d'utilisateurs connectés dépasse le nombre d'utilisateurs actuels si les sessions d'authentification, d'autorisation et d'audit expirent, mais que les connexions ICA sont toujours actives.
- Dans une configuration VPN pure (aucune ICA n'est impliquée), le nombre d'utilisateurs actuels et le nombre total d'utilisateurs connectés sont égaux.

Configuration des types de connexion sur le serveur virtuel

Lorsque vous créez et configurez un serveur virtuel, vous pouvez configurer les options de connexion suivantes :

- Connexions avec l'application Citrix Workspace uniquement à Citrix Virtual Apps and Desktops sans SmartAccess, analyse des points de terminaison ou fonctionnalités de tunneling de la couche réseau.
- Connexions avec le client Citrix Secure Access et SmartAccess, qui permettent d'utiliser SmartAccess, l'analyse des points de terminaison et les fonctions de tunneling de la couche réseau.
- Connexions avec Secure Hub qui établit une connexion micro VPN entre des appareils mobiles et NetScaler Gateway.

- Connexions parallèles effectuées via le protocole de session ICA par un utilisateur à partir de plusieurs appareils. Les connexions sont migrées vers une session unique pour empêcher l'utilisation de plusieurs licences universelles.

Si vous souhaitez que les utilisateurs ouvrent une session sans logiciel utilisateur, vous pouvez configurer une stratégie d'accès sans client et la lier au serveur virtuel.

Pour configurer les connexions Basic ou SmartAccess sur un serveur virtuel

1. Accédez à **NetScaler Gateway**, puis cliquez sur **Virtual Servers**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom du serveur virtuel.
4. Dans **Adresse IP** et **port**, tapez l'adresse IP et le numéro de port du serveur virtuel.
5. Procédez comme suit :
    - Pour autoriser uniquement les connexions ICA, cliquez sur **Mode de base**.
    - Pour autoriser les utilisateurs à se connecter avec Secure Hub, le client Citrix Secure Access et SmartAccess, cliquez sur Mode **SmartAccess**.
    - Pour permettre à SmartAccess de gérer les sessions de proxy ICA pour plusieurs connexions utilisateur, cliquez sur **Migration de session de proxy ICA**.
6. Configurez les autres paramètres du serveur virtuel, cliquez sur **Créer**, puis sur **Fermer**.

Configurer une stratégie d'écoute pour les serveurs virtuels génériques

Vous pouvez configurer les serveurs virtuels NetScaler Gateway pour restreindre la capacité d'un serveur virtuel à écouter sur un VLAN spécifique. Vous pouvez créer un serveur virtuel générique avec une stratégie d'écoute qui le limite au traitement du trafic sur le VLAN spécifié.

Les paramètres de configuration sont les suivants :

Paramètre	Description
Nom	Le nom du serveur virtuel. Le nom est obligatoire et vous ne pouvez pas le modifier après avoir créé le serveur virtuel. Le nom ne peut pas dépasser 127 caractères et le premier caractère doit être un chiffre ou une lettre. Vous pouvez également utiliser les caractères suivants : symbole arobase (@), trait de soulignement (_), tiret (-), point (.), deux-points (:), signe dièse (#) et espace.
Adresse IP	L'adresse IP du serveur virtuel. Pour un serveur virtuel générique lié au VLAN, la valeur est toujours *.
Type	Le comportement du service. Vous avez le choix entre HTTP, SSL, FTP, TCP, SSL_TCP, UDP, SSL_BRIDGE, NNTP, DNS, ANY, SIP-UDP, DNS-TCP et RTSP.
Port	Port sur lequel le serveur virtuel écoute les connexions des utilisateurs. Le numéro de port doit être compris entre 0 et 65535. Pour le serveur virtuel générique lié à un VLAN, la valeur est généralement *.
Priorité écoute	Priorité attribuée à la stratégie d'écoute. La priorité est évaluée dans l'ordre inverse ; plus le nombre est bas, plus la priorité attribuée à la stratégie d'écoute est élevée.
Règle de stratégie d'écoute	La règle de stratégie à utiliser pour identifier le VLAN que le serveur virtuel doit écouter. La règle est la suivante : CLIENT.VLAN.ID.EQ (<ipaddressat>) Pour,<ipaddressat> remplacez le numéro d'ID attribué au VLAN.

Pour créer un serveur virtuel générique avec une stratégie d'écoute

1. Dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Serveurs virtuels**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom du serveur virtuel.

4. Dans **Protocole**, sélectionnez le protocole.
5. Dans **Adresse IP**, tapez l'adresse IP du serveur virtuel.
6. Dans **Port**, tapez le port du serveur virtuel.
7. Dans l'onglet **Avancé**, sous Stratégie d'écoute, dans **Priorité d'écoute**, tapez la priorité de la stratégie d'écoute.
8. En regard de Règle de stratégie d'écoute, cliquez sur **Configurer**.
9. Dans la boîte de dialogue **Créer une expression**, cliquez sur **Ajouter**, configurez l'expression, puis cliquez sur **OK**.
10. Cliquez sur **Create**, puis cliquez sur **Close**.

Configurer les adresses IP sur NetScaler Gateway

January 26, 2024

Vous pouvez configurer des adresses IP pour ouvrir une session à l'utilitaire de configuration et pour les connexions utilisateur. NetScaler Gateway est configuré avec une adresse IP par défaut 192.168.100.1 et un masque de sous-réseau 255.255.0.0 pour l'accès de gestion. L'adresse IP par défaut est utilisée chaque fois qu'une valeur configurée par l'utilisateur pour l'adresse IP système (NSIP) est absente.

- Adresse NSIP. Adresse IP de gestion de NetScaler Gateway qui est utilisée pour tous les accès liés à la gestion à l'appliance. NetScaler Gateway utilise également l'adresse NSIP pour l'authentification.
- **Passerelle par défaut**. Le routeur qui transfère le trafic provenant de l'extérieur du réseau sécurisé vers NetScaler Gateway.
- **Adresse IP du sous-réseau (SNIP)**. Adresse IP qui représente la machine utilisateur en communiquant avec un serveur sur un réseau secondaire.

L'adresse SNIP utilise les ports 1024 à 64000.

Comment NetScaler Gateway utilise les adresses IP

NetScaler Gateway génère le trafic à partir d'adresses IP en fonction de la fonction en cours. La liste suivante décrit plusieurs fonctions ainsi que la manière dont NetScaler Gateway utilise les adresses IP pour chacune d'entre elles, à titre indicatif :

- **Authentification.** L'adresse IP utilisée par NetScaler Gateway dépend du type de serveur d'authentification.

  - Serveurs LDAP/RADIUS/TACACS. Si AAAD communique directement avec le serveur virtuel d'authentification, l'adresse NSIP est utilisée.
  - Si un équilibreur de charge est utilisé comme proxy, il utilise l'adresse SNIP pour l'authentification. AAAD utilise l'adresse NSIP pour communiquer avec l'équilibreur de charge. L'adresse IP utilisée par NetScaler dépend de l'entité qui communique avec le serveur virtuel d'authentification.
  - Serveurs SAML/OAUTH/WEBAUTH : Ces serveurs communiquent à l'aide de l'adresse SNIP.

- **Transferts de fichiers depuis la page d'accueil.** NetScaler Gateway utilise l'adresse SNIP.
- **Requêtes DNS et WINS.** NetScaler Gateway utilise l'adresse SNIP.
- **Trafic réseau vers les ressources du réseau sécurisé.** NetScaler Gateway utilise l'adresse SNIP ou le pool d'adresses IP, selon la configuration de NetScaler Gateway.
- **Paramètre de proxy ICA.** NetScaler Gateway utilise l'adresse SNIP.

Adresses IP de sous-réseau

L'adresse IP du sous-réseau permet à l'utilisateur de se connecter à NetScaler Gateway à partir d'un hôte externe résidant sur un autre sous-réseau. Lorsque vous ajoutez une adresse IP de sous-réseau, une entrée de route correspondante est créée dans la table de routage. Une seule entrée est créée par sous-réseau. L'entrée de route correspond à la première adresse IP ajoutée dans le sous-réseau.

Contrairement à l'adresse IP du système et à l'adresse IP mappée, il n'est pas obligatoire de spécifier l'adresse IP du sous-réseau lors de la configuration initiale de NetScaler Gateway.

L'adresse IP mappée et les adresses IP de sous-réseau utilisent les ports 1024 à 64000.

Pour ajouter une adresse IP de sous-réseau

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système \ > Réseau**, puis cliquez sur **IP**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer une adresse IP, dans Adresse IP, tapez l'adresse IP.
4. Dans Masque de réseau, tapez le masque de sous-réseau.
5. Sous Type d'adresse IP, sélectionnez IP de sous-réseau, cliquez sur **Fermer,** puis sur **Créer**.

Configurer IPv6 pour les connexions utilisateur

Vous pouvez configurer NetScaler Gateway pour qu'il écoute les connexions des utilisateurs à l'aide du protocole Internet version 6 (IPv6). Lorsque vous configurez l'un des paramètres suivants, vous pouvez activer la case à cocher IPv6, puis entrer l'adresse IPv6 dans la boîte de dialogue :

- Paramètres globaux - Applications publiées - Proxy ICA
- Authentification globale - RADIUS
- Authentification globale - LDAP
- Authentification globale - TACACS
- Profil de session - Applications publiées - ICA Proxy
- Serveurs virtuels NetScaler Gateway
- Créer un serveur d'authentification - RADIUS
- Créer un serveur d'authentification - LDAP
- Créer un serveur d'authentification - TACACS
- Créer un serveur d'audit
- Configuration de la haute disponibilité
- Lier/délier les moniteurs de routage pour une haute disponibilité
- Serveur virtuel (équilibrage de charge)

Lorsque vous configurez le serveur virtuel NetScaler Gateway pour écouter sur une adresse IPv6, les utilisateurs peuvent se connecter uniquement avec l'application Citrix Workspace. Les connexions utilisateur avec le client Citrix Secure Access ne sont pas prises en charge avec IPv6.

Vous pouvez utiliser les instructions suivantes pour configurer IPv6 sur NetScaler Gateway :

- Citrix Virtual Apps et interface Web. Lorsque vous configurez IPv6 pour les connexions utilisateur et si une adresse IP mappée utilise IPv6, les serveurs Citrix Virtual Apps et Web Interface peuvent également utiliser IPv6. L'interface Web doit être installée derrière NetScaler Gateway. Lorsque les utilisateurs se connectent via NetScaler Gateway, l'adresse IPv6 est traduite en IPv4. Lorsque la connexion revient, l'adresse IPv4 est traduite en IPv6.
- Serveurs virtuels. Vous pouvez configurer IPv6 pour un serveur virtuel lorsque vous exécutez l'assistant NetScaler Gateway. Dans l'assistant NetScaler Gateway sur la page Serveurs virtuels, cliquez sur IPv6 et entrez l'adresse IP. Vous pouvez uniquement configurer une adresse IPv6 pour un serveur virtuel à l'aide de l'assistant NetScaler Gateway.
- Autres. Pour configurer IPv6 pour le proxy ICA, l'authentification, l'audit et la haute disponibilité, activez la case à cocher IPv6 dans la boîte de dialogue, puis tapez l'adresse IP.

Résoudre les serveurs DNS situés dans le réseau sécurisé

January 26, 2024

Si votre serveur DNS se trouve dans le réseau sécurisé derrière un pare-feu et que le pare-feu bloque le trafic ICMP, vous ne pouvez pas tester les connexions au serveur car le pare-feu bloque la demande. Vous pouvez résoudre ce problème en procédant comme suit :

- Création d'un service DNS avec un moniteur DNS personnalisé qui se résout en un nom de domaine complet (FQDN) connu.
- Création d'un serveur virtuel DNS non directement adressable sur NetScaler Gateway.
- Liaison du service au serveur virtuel.

Remarque :

- Configurez un serveur virtuel DNS et un service DNS uniquement si votre serveur DNS se trouve derrière un pare-feu.
- Si vous installez une licence d'équilibrage de charge NetScaler sur l'appliance, le nœud Virtual Servers and Services n'apparaît pas dans le volet de navigation. Vous pouvez effectuer cette procédure en développant Équilibrage de charge, puis en cliquant sur Serveurs virtuels.

Pour configurer un service DNS et un moniteur DNS

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Serveurs et services virtuels, puis cliquez sur Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom, tapez le nom du service.
4. Dans Protocole, sélectionnez DNS.
5. Dans Adresse IP, tapez l'adresse IP du serveur DNS.
6. Dans Port, tapez le numéro de port.
7. Dans l'onglet Services, cliquez sur Ajouter.
8. Sous l'onglet Moniteurs, sous Disponible, sélectionnez DNS, cliquez sur Ajouter, sur Créer, puis sur Fermer.
9. Dans la boîte de dialogue Créer un serveur virtuel (équilibrage de charge), cliquez sur Créer, puis sur Fermer.

Ensuite, créez le serveur virtuel DNS à l'aide de la procédure Pour configurer un serveur virtuel DNS, puis liez le service DNS au serveur virtuel.

Pour lier un service DNS à un serveur virtuel DNS

1. Dans la boîte de dialogue Configurer le service virtuel (équilibrage de charge), sous l'onglet Services, cliquez sur Ajouter, sélectionnez le service DNS, cliquez sur Créer, puis cliquez sur Fermer.

Configurer les serveurs virtuels DNS

January 26, 2024

Pour configurer un serveur virtuel DNS, vous devez spécifier un nom et une adresse IP. Comme pour le serveur virtuel NetScaler Gateway, vous devez attribuer une adresse IP au serveur virtuel DNS. Toutefois, cette adresse IP doit se trouver du côté interne du réseau ciblé pour que les machines utilisateur résolvent toutes les adresses internes. Spécifiez également le port DNS.

Remarque : Si vous installez une licence d'équilibrage de charge NetScaler sur l'appliance, le nœud Virtual Servers and Services n'apparaît pas dans le volet de navigation. Vous pouvez configurer cette fonctionnalité à l'aide du serveur virtuel d'équilibrage de charge. Pour plus d'informations, consultez la documentation de NetScaler dans la documentation du produit NetScaler.

Pour configurer un serveur virtuel DNS

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Serveurs et services virtuels, puis cliquez sur Serveurs virtuels.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom, tapez le nom du serveur virtuel.
4. Dans Adresse IP, tapez l'adresse IP du serveur DNS.
5. Dans Port, tapez le port sur lequel le serveur DNS écoute.
6. Dans Protocole, sélectionnez DNS, puis cliquez sur Créer.

Enfin, associez le serveur virtuel DNS à NetScaler Gateway via l'une des deux méthodes suivantes, en fonction des besoins de votre déploiement :

- Liez le serveur globalement à NetScaler Gateway.
- Liez le serveur virtuel DNS par serveur virtuel.

Si vous déployez le serveur virtuel DNS globalement, tous les utilisateurs y ont accès. Vous pouvez ensuite restreindre les utilisateurs en liant le serveur virtuel DNS au serveur virtuel.

Configuration des fournisseurs de services de noms

March 27, 2024

NetScaler Gateway utilise des fournisseurs de services de noms pour convertir les adresses Web en adresses IP.

Lorsque vous exécutez l'assistant NetScaler Gateway, vous pouvez configurer un serveur DNS ou un serveur WINS. Vous pouvez utiliser l'utilitaire de configuration pour configurer également d'autres serveurs DNS ou WINS.

Pour ajouter un serveur DNS à NetScaler Gateway

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Configuration réseau, cliquez sur Ajouter.
4. Dans la boîte de dialogue Insérer un serveur de noms, dans Adresse IP, tapez l'adresse IP du serveur DNS, cliquez sur Créer, puis cliquez sur Fermer.
5. Cliquez sur OK dans l'utilitaire de configuration.

Pour ajouter un serveur WINS à NetScaler Gateway

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Sous l'onglet Configuration réseau, dans IP du serveur WINS, tapez l'adresse IP du serveur WINS, puis cliquez sur OK.

Ensuite, spécifiez le nom et l'adresse IP du serveur virtuel DNS. Comme pour le serveur virtuel NetScaler Gateway, une adresse IP doit être attribuée au serveur virtuel. Toutefois, cette adresse IP doit se trouver du côté interne du réseau ciblé pour que les machines utilisateur résolvent correctement toutes les adresses internes. Vous devez également spécifier le port DNS.

Si vous configurez un serveur DNS et un serveur WINS pour la résolution des noms, vous pouvez ensuite utiliser l'assistant NetScaler Gateway pour sélectionner le serveur qui effectue la recherche de noms en premier.

Pour spécifier la priorité de recherche de noms

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur NetScaler Gateway.
2. Dans le volet d'informations, sous Getting Started, cliquez sur l'assistant NetScaler Gateway.
3. Cliquez sur Suivant pour accepter les paramètres actuels jusqu'à ce que vous arriviez à la page Name Service Providers.
4. Dans Priorité de recherche de noms, sélectionnez WINS ou DNS, puis continuez jusqu'à la fin de l'assistant.

Configuration des connexions initiées par le serveur

March 27, 2024

Pour chaque utilisateur connecté à NetScaler Gateway avec les adresses IP activées, le suffixe DNS est ajouté au nom d'utilisateur et un enregistrement d'adresse DNS est ajouté au cache DNS de l'appliance. Cette technique permet de fournir aux utilisateurs un nom DNS plutôt que leurs adresses IP.

Lorsqu'une adresse IP est attribuée à la session d'un utilisateur, il est possible de se connecter à l'appareil de l'utilisateur à partir du réseau interne. Par exemple, les utilisateurs qui se connectent au Bureau à distance ou à un client VNC (Virtual Network Computing) peuvent accéder à la machine utilisateur pour diagnostiquer une application problématique. Il est également possible pour deux utilisateurs de NetScaler Gateway possédant une adresse IP réseau interne et connectés à distance de communiquer entre eux via NetScaler Gateway. Le fait d'autoriser la découverte des adresses IP réseau internes des utilisateurs connectés sur l'appliance facilite cette communication.

Un utilisateur distant peut utiliser la commande ping suivante pour découvrir l'adresse IP réseau interne d'un utilisateur qui peut alors se connecter à NetScaler Gateway :

```
ping \<username.domainname\>
```

Un serveur peut établir une connexion à une machine utilisateur de différentes manières :

- Connexions TCP ou UDP. Les connexions peuvent provenir d'un système externe du réseau interne ou d'un autre ordinateur connecté à NetScaler Gateway. L'adresse IP du réseau interne attribuée à chaque machine utilisateur connectée à NetScaler Gateway est utilisée pour ces connexions. Les différents types de connexions initiées par le serveur pris en charge par NetScaler Gateway sont décrits.
  Pour les connexions initiées par le serveur TCP ou UDP, le serveur dispose de connaissances préalables sur l'adresse IP et le port de la machine utilisateur et établit une connexion avec celle-ci. NetScaler Gateway intercepte cette connexion.

  Ensuite, le dispositif utilisateur établit une connexion initiale avec le serveur et le serveur se connecte au dispositif utilisateur sur un port connu ou dérivé du premier port configuré.

  Dans ce scénario, la machine utilisateur établit une connexion initiale au serveur, puis échange des ports et des adresses IP avec le serveur à l'aide d'un protocole spécifique à l'application dans lequel ces informations sont intégrées. Cela permet à NetScaler Gateway de prendre en charge des applications, telles que les connexions FTP actives.
- Commande de port. Il est utilisé dans un FTP actif et dans certains protocoles Voice over IP.
- Connexions entre les plug-ins. NetScaler Gateway prend en charge les connexions entre les plug-ins à l'aide des adresses IP du réseau interne.

Avec ce type de connexion, deux machines utilisateur NetScaler Gateway qui utilisent le même NetScaler Gateway peuvent établir des connexions entre elles. Un exemple de ce type est l'utilisation d'applications de messagerie instantanée, telles que Office Communicator ou Yahoo ! Messenger.

Si un utilisateur se déconnecte de NetScaler Gateway et que la demande de fermeture de session n'est pas parvenue à l'appliance, il peut se reconnecter en utilisant n'importe quel appareil et remplacer la session précédente par une nouvelle session. Cette fonctionnalité peut s'avérer utile dans les déploiements où une adresse IP est attribuée par utilisateur.

Lorsqu'un utilisateur se connecte à NetScaler Gateway pour la première fois, une session est créée et une adresse IP est attribuée à l'utilisateur. Si l'utilisateur ferme sa session mais que la demande de fermeture de session est perdue ou que la machine utilisateur ne parvient pas à effectuer une fermeture de session propre, la session est maintenue sur le système. Si l'utilisateur tente de se connecter à nouveau à partir du même appareil ou d'un autre appareil, une fois l'authentification réussie, une boîte de dialogue d'ouverture de session de transfert apparaît. Si l'utilisateur choisit de transférer l'ouverture de session, la session précédente sur NetScaler Gateway est fermée et une nouvelle session est créée. Le transfert d'ouverture de session n'est actif que deux minutes après la fermeture de session, et si la connexion est tentée à partir de plusieurs appareils simultanément, la dernière tentative de connexion remplace la session d'origine.

Configurer la plage de ports privés pour les connexions initiées par le serveur

À partir de la version 23.10.1.7 du client Citrix Secure Access, vous pouvez configurer un port privé compris entre 49152 et 64535 pour les connexions initiées par le serveur (SIC). La configuration des ports privés permet d'éviter les conflits qui peuvent survenir lorsque vous utilisez des ports pour créer des sockets entre le client Citrix Secure Access et des applications tierces sur les machines clientes. Cela ne s'applique que si le pilote WFP est en cours d'utilisation.

Vous pouvez configurer les ports privés à l'aide du `SicBeginPort`registre VPN Windows. Vous pouvez également configurer la plage de ports privés à l'aide d'un fichier JSON de personnalisation du plug-in VPN sur NetScaler.

Si un serveur établit une connexion, le client Citrix Secure Access utilise les 1 000 premiers ports à partir du `SicBeginPort`registre VPN Windows pour créer les sockets. Si le registre est configuré sur un ordinateur client, le paramètre de registre a priorité sur le paramètre NetScaler JSON.

Voici un exemple de configuration JSON du plug-in VPN sur NetScaler :

```
root@ADC# cat /var/netscaler/gui/vpn/pluginCustomization.json

{
 "SicBeginPort" : 51000 }

```



```
<!--NeedCopy-->
```

Pour plus d'informations sur les paramètres du registre, consultez la section Clés de registre du client VPN Windows NetScaler Gateway.

> **Remarque :**
>
> La plage de ports par défaut utilisée pour créer des sockets est comprise entre 62 500 et 63 500.

Configurer le routage sur NetScaler Gateway

March 27, 2024

Pour fournir un accès aux ressources du réseau interne, NetScaler Gateway achemine les données vers vos réseaux internes sécurisés. Par défaut, NetScaler Gateway utilise une route statique.

Les réseaux vers lesquels NetScaler Gateway peut acheminer les données sont déterminés par la façon dont vous configurez la table de routage NetScaler Gateway et la passerelle par défaut que vous spécifiez pour NetScaler Gateway.

La table de routage NetScaler Gateway doit contenir les routes nécessaires pour acheminer les données vers toute ressource réseau interne à laquelle un utilisateur peut avoir besoin d'accéder.

NetScaler Gateway prend en charge les protocoles de routage suivants :

- Protocole d'information de routage (RIP v1 et v2)
- Ouvrir le chemin le plus court en premier (OSPF)
- Border Gateway Protocol (BGF)

Configurer un itinéraire statique

Lorsque vous configurez la communication avec un autre hôte ou un autre réseau, vous devez configurer un itinéraire statique entre NetScaler Gateway et la nouvelle destination si vous n'utilisez pas le routage dynamique.

Pour configurer un itinéraire statique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système > Réseau > Avancé**, puis cliquez sur **Itinéraires**.
2. Dans le volet d'informations, sous l'onglet Basic, cliquez sur **Ajouter**.
3. Configurez les paramètres de l'itinéraire, puis cliquez sur **Créer**.

Pour tester une route statique

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **Système,** puis cliquez sur **Diagnostics**.
2. Dans le volet d'informations, sous Utilitaires, cliquez sur **Ping**.
3. Sous Paramètres, dans Nom d'hôte, tapez le nom du périphérique.
4. Sous Avancé, dans Adresse IP source, tapez l'adresse IP de l'appareil, puis cliquez sur **Exécuter**.

   Si vous parvenez à communiquer avec l'autre appareil, les messages indiquent que le même nombre de paquets a été transmis et reçu, et qu'aucun paquet n'a été perdu.

   Si vous ne communiquez pas avec l'autre appareil, les messages d'état indiquent qu'aucun paquet n'a été reçu et que tous les paquets ont été perdus. Pour corriger ce manque de communication, répétez la procédure pour ajouter une route statique.

Pour arrêter le test, dans la boîte de dialogue **Ping**, cliquez sur **Arrêter,** puis sur **Fermer**.

Configurer la négociation automatique

March 27, 2024

Par défaut, l'appliance est configurée pour utiliser la négociation automatique, dans laquelle NetScaler Gateway transmet le trafic réseau dans les deux sens simultanément et détermine la vitesse d'adaptateur appropriée. Si vous conservez le paramètre par défaut sur Négociation automatique, NetScaler Gateway utilise le mode duplex intégral, dans lequel l'adaptateur réseau est capable d'envoyer des données dans les deux sens simultanément.

Si vous désactivez la négociation automatique, NetScaler Gateway utilise le mode semi-duplex, dans lequel l'adaptateur peut envoyer des données dans les deux sens entre deux nœuds, mais l'adaptateur ne peut utiliser que l'un ou l'autre sens à la fois.

Pour la première installation, Citrix vous recommande de configurer NetScaler Gateway pour utiliser la négociation automatique pour les ports connectés à l'appliance. Après avoir ouvert une session initiale et configuré NetScaler Gateway, vous pouvez désactiver la négociation automatique. Vous ne pouvez pas configurer la négociation automatique globalement. Vous devez activer ou désactiver le paramètre pour chaque interface.

Pour activer ou désactiver la négociation automatique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système \ > Réseau,** puis cliquez sur **Interfaces**.

2. Dans le volet d'informations, sélectionnez l'interface, puis cliquez sur **Ouvrir**.
3. Effectuez l'une des opérations suivantes dans la boîte de dialogue **Configurer l'interface** :

    - Pour activer la négociation automatique, cliquez sur **Oui** en regard de Négociation automatique, puis cliquez sur **OK**.
    - Pour désactiver la négociation automatique, cliquez sur **Non** en regard de Négociation automatique, puis cliquez sur **OK**.

Configurer le nom d'hôte et le FQDN sur NetScaler Gateway

March 27, 2024

Le nom d'hôte est le nom de l'appliance NetScaler Gateway associée au fichier de licence. Le nom d'hôte est unique à l'appliance et est utilisé lorsque vous téléchargez la licence universelle. Vous définissez le nom d'hôte lorsque vous exécutez l'assistant de configuration pour configurer NetScaler Gateway pour la première fois.

Le nom de domaine complet (FQDN) est inclus dans le certificat signé lié à un serveur virtuel. Vous ne configurez pas le FQDN sur NetScaler Gateway. Un dispositif peut avoir un nom de domaine complet unique attribué à chaque serveur virtuel configuré sur NetScaler Gateway à l'aide de certificats.

Vous pouvez trouver le nom de domaine complet d'un certificat en consultant les détails du certificat. Le nom de domaine complet se trouve dans le champ Objet du certificat.

Pour afficher le nom de domaine complet d'un certificat

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **SSL,** puis cliquez sur **Certificats**.
2. Dans le volet d'informations, sélectionnez un certificat, cliquez sur **Action,** puis sur **Détails**.
3. Dans la boîte de dialogue Détails du certificat, cliquez sur **Objet**. Le nom de domaine complet du certificat apparaît dans la liste.

Stratégies et profils sur NetScaler Gateway

March 27, 2024

Les stratégies et les profils de NetScaler Gateway vous permettent de gérer et de mettre en œuvre les paramètres de configuration selon des scénarios ou des conditions spécifiques. Une stratégie indi-

viduelle indique ou définit les paramètres de configuration qui entrent en vigueur lorsqu'un ensemble de conditions spécifié est rempli. Chaque stratégie a un nom unique et peut avoir un profil lié à la stratégie.

Fonctionnent des stratégies

Une stratégie se compose d'une condition booléenne et d'un ensemble de paramètres appelés profil. La condition est évaluée au moment de l'exécution pour déterminer si la stratégie doit être appliquée.

Un profil est un ensemble de paramètres utilisant des paramètres spécifiques. Le profil peut porter n'importe quel nom et vous pouvez le réutiliser dans plusieurs stratégies. Vous pouvez configurer plusieurs paramètres dans le profil, mais vous ne pouvez inclure qu'un seul profil par stratégie.

Vous pouvez lier des stratégies, avec les conditions et profils configurés, à des serveurs virtuels, des groupes, des utilisateurs ou globalement. Les stratégies sont désignées par le type de paramètres de configuration qu'elles contrôlent. Par exemple, dans une stratégie de session, vous pouvez contrôler la façon dont les utilisateurs ouvrent une session et le nombre de fois où les utilisateurs peuvent rester connectés.

Si vous utilisez NetScaler Gateway avec Citrix Virtual Apps, les noms de stratégie NetScaler Gateway sont envoyés à Citrix Virtual Apps sous forme de filtres. Lorsque vous configurez NetScaler Gateway pour qu'il soit compatible avec Citrix Virtual Apps et SmartAccess, vous configurez les paramètres suivants dans Citrix Virtual Apps :

- Nom du serveur virtuel configuré sur l'appliance. Le nom est envoyé à Citrix Virtual Apps en tant que nom de batterie de serveurs NetScaler Gateway.
- Les noms des stratégies de pré-authentification ou de session sont envoyés sous forme de noms de filtres.

Pour plus d'informations sur la configuration de NetScaler Gateway pour qu'il soit compatible avec Citrix Endpoint Management, consultez lasection Configuration des paramètres de votre environnement Citrix Endpoint Management.

Pour plus d'informations sur la configuration de NetScaler Gateway pour qu'il soit compatible avec Citrix Virtual Apps and Desktops, consultezAccès aux ressources Citrix Virtual Apps et Citrix Virtual Desktops via l'interface WebetIntégration à Citrix Endpoint Management ou StoreFront.

Pour plus d'informations sur les stratégies de pré-authentification, consultez Configuration des stratégies de point de terminaison.

Stratégies conditionnelles

Lorsque vous configurez des stratégies, vous pouvez utiliser n'importe quelle expression booléenne pour exprimer la condition de l'application de la stratégie. Lorsque vous configurez des stratégies conditionnelles, vous pouvez utiliser n'importe laquelle des expressions système disponibles, telles que les suivantes :

- chaînes de sécurité client
- Informations sur le réseau
- En-têtes et cookies HTTP
- Heure de la journée
- Valeurs des certificats clients

Vous pouvez également créer des stratégies à appliquer uniquement lorsque la machine utilisateur répond à des critères spécifiques, tels qu'une stratégie de session pour SmartAccess.

Un autre exemple de configuration d'une stratégie conditionnelle consiste à modifier la stratégie d'authentification des utilisateurs. Par exemple, vous pouvez demander aux utilisateurs qui se connectent au client Citrix Secure Access depuis l'extérieur du réseau interne, par exemple depuis leur ordinateur personnel ou à l'aide du Micro VPN depuis un appareil mobile, d'être authentifiés à l'aide de LDAP et aux utilisateurs qui se connectent via le WAN d'être authentifiés à l'aide de RADIUS.

Remarque : Vous ne pouvez pas utiliser de conditions de politique basées sur les résultats de l'analyse des terminaux si la règle de politique est configurée dans le cadre des paramètres de sécurité d'un profil de session.

Priorités des stratégies

Les stratégies sont priorisées et évaluées dans l'ordre dans lequel elles sont liées.

Les deux méthodes suivantes déterminent la priorité de la stratégie :

- Niveau auquel la stratégie est liée : globalement, serveur virtuel, groupe ou utilisateur. Les niveaux de stratégie sont classés du plus haut au plus bas comme suit :
  - Utilisateur (priorité la plus élevée)
  - Groupe
  - Serveur virtuel
  - Global (priorité la plus basse)
- La priorité numérique est prioritaire quel que soit le niveau auquel la stratégie est liée. Si une stratégie liée globalement a un numéro de priorité de l'un et qu'une autre stratégie liée à un utilisateur a un numéro de priorité de deux, la stratégie globale est prioritaire. Un numéro de priorité inférieur donne à la stratégie une priorité plus élevée.

Création de stratégies sur NetScaler Gateway

Vous pouvez utiliser l'utilitaire de configuration pour créer des stratégies. Après avoir créé une stratégie, vous liez la stratégie au niveau approprié : utilisateur, groupe, serveur virtuel ou global. Lorsque vous liez une stratégie à l'un de ces niveaux, les utilisateurs reçoivent les paramètres du profil si les conditions de la stratégie sont remplies. Chaque stratégie et profil porte un nom unique.

Si Citrix Endpoint Management ou StoreFront font partie de votre déploiement, vous pouvez utiliser l'assistant de configuration rapide pour configurer les paramètres de ce déploiement. Pour plus d'informations sur l'assistant, consultez Configuration des paramètres à l'aide de l'assistant de configuration rapide.

Configuration des expressions système

March 27, 2024

Une expression système spécifie les conditions dans lesquelles la stratégie est appliquée. Par exemple, les expressions d'une stratégie de pré-authentification sont appliquées lorsqu'un utilisateur se connecte. Les expressions d'une stratégie de session sont évaluées et appliquées une fois que l'utilisateur est authentifié et connecté à NetScaler Gateway.

Les expressions de NetScaler Gateway incluent :

- Expressions générales qui limitent les objets que les utilisateurs peuvent utiliser lors de l'établissement d'une connexion à NetScaler Gateway. Par exemple, voir :
  - Stratégies de session
- Expressions de sécurité client qui définissent les logiciels, les fichiers, les processus ou les valeurs de registre qui doivent être installés et exécutés sur la machine utilisateur. Par exemple, voir :
  - Stratégies Endpoint
- Expressions basées sur le réseau qui limitent l'accès en fonction des paramètres réseau. Par exemple, voir :
  - Stratégies de trafic
  - Stratégies d'autorisation

NetScaler Gateway peut également être utilisé comme appliance NetScaler. Certaines expressions de l'appliance sont plus applicables à NetScaler. Les expressions générales et basées sur le réseau sont couramment utilisées avec NetScaler et ne le sont généralement pas avec NetScaler Gateway. Les

expressions de sécurité du client sont utilisées sur NetScaler Gateway pour déterminer si les éléments appropriés sont installés sur la machine utilisateur.

Configuration des expressions de sécurité client

Les expressions sont un composant d'une stratégie. Une expression représente une condition unique évaluée par rapport à une demande ou à une réponse. Vous pouvez créer une chaîne de sécurité d'expression simple pour vérifier les conditions, telles que :

- Système d'exploitation de la machine utilisateur, y compris les service packs
- Version du logiciel antivirus et définitions de virus
- Fichiers
- Processus
- Valeurs du registre
- Certificats utilisateur

Gestion des certificats sur NetScaler Gateway

January 26, 2024

Sur NetScaler Gateway, vous utilisez des certificats pour créer des connexions sécurisées et authentifier les utilisateurs.

Pour établir une connexion sécurisée, un certificat de serveur est requis à une extrémité de la connexion. Un certificat racine de l'autorité de certification (CA) qui a émis le certificat de serveur est requis à l'autre extrémité de la connexion.

- Certificat serveur. Un certificat de serveur certifie l'identité du serveur. NetScaler Gateway nécessite ce type de certificat numérique.
- Certificat racine. Un certificat racine identifie l'autorité de certification qui a signé le certificat de serveur. Le certificat racine appartient à l'autorité de certification. Une machine utilisateur a besoin de ce type de certificat numérique pour vérifier le certificat de serveur.

Lors de l'établissement d'une connexion sécurisée avec un navigateur Web sur la machine utilisateur, le serveur envoie son certificat à l'appareil.

Lorsque la machine utilisateur reçoit un certificat de serveur, le navigateur Web, tel qu'Internet Explorer, vérifie quelle autorité de certification a émis le certificat et si l'autorité de certification est approuvée par la machine utilisateur. Si l'autorité de certification n'est pas approuvée ou s'il s'agit d'un certificat de test, le navigateur Web invite l'utilisateur à accepter ou à refuser le certificat (en acceptant ou en refusant la possibilité d'accéder au site).

NetScaler Gateway prend en charge les trois types de certificats suivants :

- Certificat de test lié à un serveur virtuel et pouvant également être utilisé pour les connexions à une batterie de serveurs. NetScaler Gateway est fourni avec un certificat de test préinstallé.
- Certificat au format PEM ou DER signé par une autorité de certification et associé à une clé privée.
- Certificat au format PKCS #12 utilisé pour stocker ou transporter le certificat et la clé privée. Le certificat PKCS #12 est généralement exporté à partir d'un certificat Windows existant sous forme de fichier PFX, puis installé sur NetScaler Gateway.

Citrix recommande d'utiliser un certificat signé par une autorité de certification approuvée, telle que Thawte ou Verisign.

Créer une demande de signature de certificat

March 27, 2024

Pour fournir des communications sécurisées via SSL ou TLS, un certificat de serveur est requis sur NetScaler Gateway. Avant de pouvoir charger un certificat sur NetScaler Gateway, vous devez générer une demande de signature de certificat (CSR) et une clé privée. Vous utilisez la demande de création de certificat incluse dans l'assistant NetScaler Gateway ou l'utilitaire de configuration pour créer le CSR. La demande de création de certificat crée un fichier .csr qui est envoyé par e-mail à l'autorité de certification (CA) pour signature et une clé privée qui reste sur l'appliance. L'autorité de certification signe le certificat et vous le renvoie à l'adresse e-mail que vous avez fournie. Lorsque vous recevez le certificat signé, vous pouvez l'installer sur NetScaler Gateway. Lorsque vous recevez le certificat de la part de l'autorité de certification, vous associez le certificat à la clé privée.

Important : lorsque vous utilisez l'assistant NetScaler Gateway pour créer le CSR, vous devez quitter l'assistant et attendre que l'autorité de certification vous envoie le certificat signé. Lorsque vous recevez le certificat, vous pouvez réexécuter l'assistant NetScaler Gateway pour créer les paramètres et installer le certificat. Pour plus d'informations sur l'assistant NetScaler Gateway, voir Configuration des paramètres à l'aide de l'assistant NetScaler Gateway.

Créez un CSR à l'aide de l'assistant NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Getting Started, cliquez sur l'assistant **NetScaler Gateway**.
3. Suivez les instructions de l'assistant jusqu'à ce que vous arriviez à la page Spécifier un certificat de serveur.

4. Cliquez sur **Créer une demande de signature de certificat** et remplissez les champs.
   Remarque : Le nom de domaine complet (FQDN) ne doit pas nécessairement être le même que le nom d'hôte NetScaler Gateway. Le nom de domaine complet est utilisé pour l'ouverture de session de l'utilisateur.
5. Cliquez sur **Créer** pour enregistrer le certificat sur votre ordinateur, puis cliquez sur **Fermer**.
6. Quittez l'assistant NetScaler Gateway sans enregistrer vos paramètres.

Création d'un CSR à l'aide de l'interface graphique NetScaler

Vous pouvez également utiliser l'interface graphique de NetScaler pour créer un CSR, sans exécuter l'assistant NetScaler Gateway.

1. Accédez à **Gestiondu trafic**>**SSL > Fichiers SSL**et sélectionnez**Créer une demande de signature de certificat (CSR)**.
2. Renseignez les paramètres du certificat, puis cliquez sur **Créer**.

Après avoir créé le certificat et la clé privée, envoyez le certificat par e-mail à l'autorité de certification, telle que Thawte ou Verisign.

Pour obtenir une procédure détaillée, consultez la section Créer une demande de signature de certificat.

Installation du certificat signé sur NetScaler Gateway

Lorsque vous recevez le certificat signé de l'autorité de certification (CA), associez-le à la clé privée de l'appliance, puis installez le certificat sur NetScaler Gateway.

Jumeler le certificat signé avec une clé privée à l'aide de l'interface graphique

1. Copiez le certificat vers NetScaler Gateway dans le dossier nsconfig/ssl à l'aide d'un programme Secure Shell (SSH) tel que WinSCP.
2. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **SSL > Certificats**.
3. Dans la page **Certificat SSL**, cliquez sur **Démarrer**.
4. Dans le volet d'informations, cliquez sur **Installer**.
5. Dans **Nom de la paire de clés** de certificat, tapez le nom du certificat.
6. Dans **Nom du fichier de certificat**, cliquez sur **Appliance**.
7. Accédez au certificat, cliquez sur **Sélectionner**, puis sur **Ouvrir**.
8. Dans **Nom du fichier clé**, cliquez sur **Appliance**. Le nom de la clé privée est identique à celui de la demande de signature de certificat (CSR). La clé privée se trouve sur NetScaler Gateway dans le répertoire \ nsconfig \ ssl.

9. Choisissez la clé privée, puis cliquez sur **Ouvrir**.
10. Si le certificat est au format PEM, dans Mot de **passe**, saisissez le mot de passe de la clé privée.
11. Si vous souhaitez configurer la notification pour la date d'expiration du certificat, sélectionnez **Notifier lorsque le certificat expire**.
12. Dans **Période de notification**, tapez le nombre de jours, cliquez sur **Créer**, puis sur **Fermer**.

Liez le certificat et la clé privée à un serveur virtuel à l'aide de l'interface graphique

Après avoir créé et lié une paire de certificats et de clés privées, liez-la à un serveur virtuel.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet Certificats, sous **Disponible**, sélectionnez un certificat, cliquez sur **Ajouter**, puis sur **OK**.

Liez le certificat et la clé privée à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
1 bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
     Mandatory | Optional )
2 <!--NeedCopy-->
```

Exemple :

```
1 bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
     ocspCheck Mandatory
2 <!--NeedCopy-->
```

Remarque : OSCPCheck est facultatif si la vérification OCSP n'est pas requise pour le certificat de périphérique.

Délier les certificats de test du serveur virtuel à l'aide de l'interface graphique

Après avoir installé le certificat signé, déliez tous les certificats de test liés au serveur virtuel. Vous pouvez délier les certificats de test à l'aide de l'utilitaire de configuration.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.

3. Dans l'onglet Certificats, sous **Configuré**, sélectionnez le certificat de test, puis cliquez sur **Supprimer**.

Configuration des certificats intermédiaires

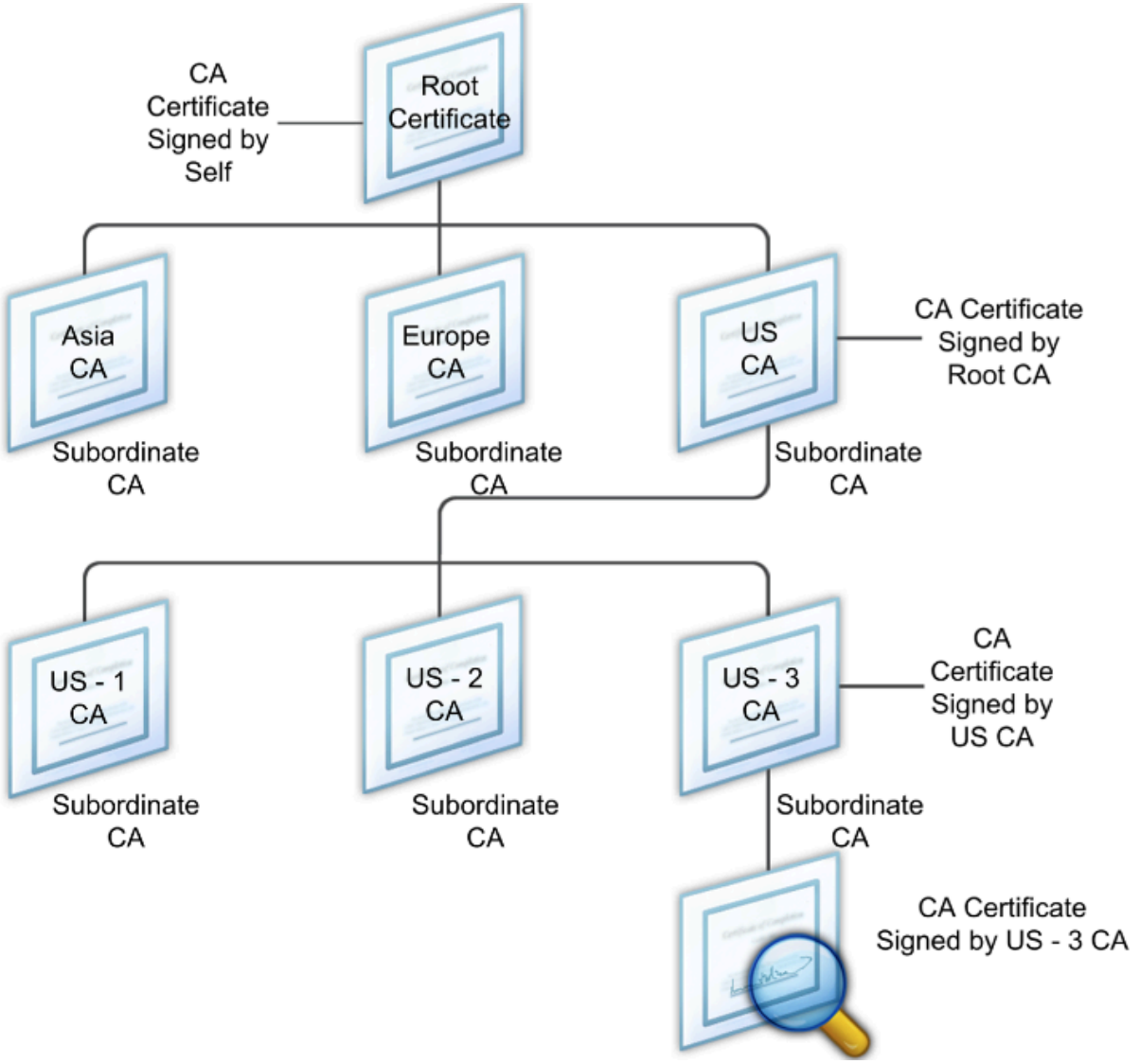
January 26, 2024

Un certificat intermédiaire est un certificat qui fait le lien entre NetScaler Gateway (le certificat du serveur) et un certificat racine (installé sur la machine utilisateur). Un certificat intermédiaire fait partie d'une chaîne.

Certaines organisations délèguent l'émission des certificats pour résoudre les problèmes liés à la dispersion géographique de leurs unités ou pour appliquer des stratégies d'émission différentes selon leurs secteurs d'activité.

La responsabilité de l'émission des certificats peut être déléguée en configurant des autorités de certification (CA) subordonnées. Les autorités de certification peuvent signer leurs propres certificats (c'est-à-dire qu'elles sont auto-signées) ou elles peuvent être signées par une autre autorité de certification. La norme X.509 inclut un modèle de mise en place d'une hiérarchie de CA. Dans ce modèle, comme illustré dans la figure suivante, l'autorité de certification racine se trouve en haut de la hiérarchie et est un certificat auto-signé par l'autorité de certification. Les autorités de certification qui sont directement subordonnées à l'autorité de certification racine possèdent des certificats d'autorité de certification signés par l'autorité de certification racine. Les CA situées sous les CA subordonnées dans la hiérarchie disposent de certificats signés par les CA subordonnées.

Figure 1. Modèle X.509 illustrant la structure hiérarchique d'une chaîne de certificats numériques classique



Si un certificat de serveur est signé par une autorité de certification avec un certificat auto-signé, la chaîne de certificats est composée exactement de deux certificats : le certificat d'entité finale et l'autorité de certification racine. Si un certificat d'utilisateur ou de serveur est signé par une autorité de certification intermédiaire, la chaîne de certificats est plus longue.

La figure suivante montre que les deux premiers éléments sont le certificat d'entité finale (dans ce cas, gwy01.company.com) et le certificat de l'autorité de certification intermédiaire, dans cet ordre. Le certificat de l'autorité de certification intermédiaire est suivi du certificat de son autorité de certification. Cette liste se poursuit jusqu'à ce que le dernier certificat de la liste soit destiné à une autorité de certification racine. Chaque certificat de la chaîne atteste de l'identité du certificat précédent.

Figure 2. Chaîne de certificats numériques classique

Installer un certificat intermédiaire

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Certificats.
2. Dans le volet d'informations, cliquez sur Installer.
3. Dans Nom de la paire de clés de certificat, tapez le nom du certificat.
4. Sous Détails, dans Nom du fichier de certificat, cliquez sur Parcourir (Appliance) et dans la liste, sélectionnez Local ou Appliance.
5. Accédez au certificat sur votre ordinateur (local) ou sur NetScaler Gateway (Appliance).
6. Dans Format de certificat, sélectionnez PEM.
7. Cliquez sur Installer, puis sur Fermer.

Lorsque vous installez un certificat intermédiaire sur NetScaler Gateway, vous n'avez pas besoin de spécifier de clé privée ni de mot de passe.

Une fois le certificat installé sur l'appliance, il doit être lié au certificat du serveur.

Lier un certificat intermédiaire à un certificat de serveur

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Certificats.
2. Dans le volet d'informations, sélectionnez le certificat du serveur, puis dans Action, cliquez sur Lier.
3. En regard de Nom du certificat de l'autorité de certification, sélectionnez le certificat intermédiaire dans la liste, puis cliquez sur OK.

Utiliser des certificats d'appareil pour l'authentification

March 27, 2024

NetScaler Gateway prend en charge la vérification du certificat de l'appareil qui vous permet de lier l'identité de l'appareil à la clé privée d'un certificat. La vérification du certificat de l'appareil peut

être configurée dans le cadre de stratégies EPA (Endpoint Analysis) classiques ou avancées. Dans les stratégies EPA classiques, le certificat d'appareil ne peut être configuré que pour l'EPA de pré-authentification.

NetScaler Gateway vérifie le certificat de l'appareil avant l'exécution de l'analyse des terminaux ou avant l'affichage de la page de connexion. Si vous configurez l'analyse des points de terminaison, l'analyse des points de terminaison est exécutée pour vérifier la machine utilisateur. Lorsque l'appareil passe l'analyse et que NetScaler Gateway a vérifié le certificat de l'appareil, les utilisateurs peuvent se connecter à NetScaler Gateway.

> **Important :**
>
> - Par défaut, Windows impose des privilèges d'administrateur pour accéder aux certificats d'appareil.
> - Pour ajouter une vérification de certificat d'appareil pour les utilisateurs non administrateurs, vous devez installer le plug-in VPN. La version du plug-in VPN doit être la même que celle du plug-in EPA sur l'appareil.
> - Vous pouvez ajouter plusieurs certificats d'autorité de certification à la passerelle et valider le certificat de l'appareil.
> - Si vous installez deux certificats d'appareils ou plus sur NetScaler Gateway, les utilisateurs doivent sélectionner le bon certificat lorsqu'ils commencent à se connecter à NetScaler Gateway ou avant l'exécution de l'analyse des terminaux.
> - Lorsque vous créez le certificat de périphérique, il doit s'agir d'un certificat X.509.
> - Si vous disposez d'un certificat de périphérique émis par une autorité de certification intermédiaire, les certificats d'autorité de certification intermédiaire et racine doivent être liés.
> - Le client EPA a besoin que l'utilisateur dispose de droits d'administrateur local pour pouvoir accéder au magasin de certificats de la machine. C'est rarement le cas. Par conséquent, une solution de contournement consiste à installer le plug-in NetScaler Gateway complet qui peut accéder au magasin local.

Pour plus d'informations sur la création de certificats d'appareil, consultez les sections suivantes :

- Network Device Enrollment Service (NDES) dans les services de certificats Active Directory (AD CS) sur le site Web de Microsoft.
- Comment demander un certificat à une autorité de certification Microsoft à l'aide de DCE/RPC et de la charge utile du profil de certificat Active Directory sur le site Web d'assistance Apple.
- Émissionde certificats iPad ou iPhone sur le blog de support Microsoft Ask the Directory Services Team.
- Configuration du service d'inscription des appareils réseau sur le site Web Windows IT Pro.
- Exemple pas à pas de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008 ? RedirectedFrom=MSDN) sur le site Web de Microsoft System

Center.

Étapes de configuration des certificats d'appareils

Pour configurer un certificat d'appareil, vous devez effectuer les étapes suivantes :

- Installez le certificat d'autorité de certification de l'émetteur du certificat de l'appareil sur NetScaler Gateway. Pour plus de détails, consultez la section Installation du certificat signé sur NetScaler Gateway.
- Liez le certificat d'autorité de certification de l'émetteur du certificat de l'appareil au serveur virtuel NetScaler Gateway et activez la vérification OCSP. Pour plus de détails, consultez la section Installation du certificat signé sur NetScaler Gateway.
- Créez et liez OCSP (répondeur) sur le certificat d'autorité de certification de l'émetteur du certificat de périphérique. Pour plus d'informations, consultez la section Surveiller l'état des certificats avec OCSP.

Activez la vérification des certificats de périphérique sur le serveur virtuel et ajoutez le certificat d'autorité de certification de l'émetteur du certificat de périphérique à la liste de vérification des certificats de périphérique. Pour plus d'informations, consultez la section Activer la vérification des certificats de périphériques sur un serveur virtuel pour la stratégie EPA classique.

Terminez la configuration côté client et la vérification du certificat de périphérique sur la machine Windows. Pour plus d'informations, consultez la section Vérification du certificat de périphérique sur un ordinateur Windows.

> **Remarque :**
>
> Le certificat de périphérique doit être installé dans le magasin de certificats système de la machine pour tous les clients destinés à bénéficier de la vérification EPA du certificat de périphérique.

Activer la vérification des certificats de périphériques sur un serveur virtuel pour la stratégie EPA classique

Après avoir créé le certificat de l'appareil, vous l'installez sur NetScaler Gateway en suivant la procédure d'importation et d'installation d'un certificat existant dans NetScaler Gateway.

1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Virtual Servers**.
2. Sur la page **Serveurs virtuels NetScaler Gateway**, sélectionnez un serveur virtuel existant et cliquez sur **Modifier**.
3. Sur la page **Serveurs virtuels VPN**, dans la section **Paramètres de base**, cliquez sur **Modifier**.
4. Décochez la case **Activer l'authentification** pour désactiver l'authentification.

5. Cochez la case **Activer le certificat de périphérique** pour activer le certificat de périphérique
6. Cliquez sur **Ajouter** pour ajouter le nom du certificat d'autorité de certification d'un émetteur de certificat de périphérique disponible à la liste.
7. Pour lier un certificat d'autorité de certification au serveur virtuel, cliquez sur **Certificat d'autorité de certification** dans la section **Certificat d'autorité de certification pour périphérique**, cliquez sur **Ajouter**, sélectionnez le certificat, puis cliquez sur **+**.

> **Remarque :**
>
> Pour plus d'informations sur l'activation et la liaison de certificats de périphériques sur un serveur virtuel pour une stratégie EPA avancée, consultez la section Certificat de périphérique dans nFactor en tant que composant EPA.

Vérification du certificat de l'appareil sur une machine Windows

1. Ouvrez un navigateur et accédez au FQDN de NetScaler Gateway.
2. Autorisez l'exécution du client Citrix End Point Analysis (EPA). Si ce n'est pas déjà fait, installez l'EPA.

   Citrix EPA exécute et valide le certificat de périphérique et redirige vers la page d'authentification si le contrôle EPA du certificat de périphérique est réussi, sinon il vous redirige vers la page d'erreur EPA. Dans le cas où vous disposez d'autres contrôles EPA, les résultats de l'analyse EPA dépendent des contrôles EPA configurés.

Pour un débogage plus poussé sur le client, examinez les journaux EPA suivants sur le client :
C:\Users <User name>\ AppData \ Local \ Citrix \ AGEE \ nsepa.txt

Remarque :

> La vérification du certificat d'appareil avec la liste de réexamen de certificats n'est pas prise

Importation et installation d'un certificat existant

March 27, 2024

Vous pouvez importer un certificat existant à partir d'un ordinateur Windows exécutant Internet Information Services (IIS) ou d'un ordinateur exécutant Secure Gateway.

Lorsque vous exportez le certificat, veillez à exporter également la clé privée. Parfois, vous ne pouvez pas exporter la clé privée, ce qui signifie que vous ne pouvez pas installer le certificat sur NetScaler

Gateway. Si cela se produit, utilisez la demande de signature de certificat (CSR) pour créer un certificat. Pour plus d'informations, consultez la section Création d'une demande de signature de certificat.

Lorsque vous exportez un certificat et une clé privée depuis Windows, l'ordinateur crée un fichier d'échange d'informations personnelles (.pfx). Ce fichier est ensuite installé sur NetScaler Gateway en tant que certificat PKCS #12.

Si vous remplacez le Secure Gateway par NetScaler Gateway, vous pouvez exporter le certificat et la clé privée depuis le Secure Gateway. Si vous effectuez une migration sur place de Secure Gateway vers NetScaler Gateway, le nom de domaine complet (FQDN) de l'application et de l'appliance doit être identique. Lorsque vous exportez le certificat depuis Secure Gateway, vous retirez immédiatement le Secure Gateway, vous installez le certificat sur NetScaler Gateway, puis vous testez la configuration. Secure Gateway et NetScaler Gateway ne peuvent pas s'exécuter simultanément sur votre réseau s'ils possèdent le même nom de domaine complet.

Si vous utilisez Windows Server 2003 ou Windows Server 2008, vous pouvez utiliser la console de gestion Microsoft pour exporter le certificat. Pour plus d'informations, consultez l'aide en ligne de Windows.

Conservez les valeurs par défaut pour toutes les autres options, définissez un mot de passe et enregistrez le fichier .pfx sur votre ordinateur. Lorsque le certificat est exporté, vous l'installez ensuite sur NetScaler Gateway.

Pour installer le certificat et la clé privée sur NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Getting Started, cliquez sur **l'assistant NetScaler Gateway**.
3. Cliquez sur **Suivant**, sélectionnez un serveur virtuel existant, puis cliquez sur **Suivant**.
4. Dans **Options de certificat**, sélectionnez **Installer un fichier PKCS #12 (.pfx)**.
5. Dans **Nom de fichier PKCS #12**, cliquez sur **Parcourir**, accédez au certificat, puis cliquez sur **Sélectionner**.
6. Dans ((Mot de passe)), tapez le mot de passe de la clé privée.

   Il s'agit du mot de passe que vous avez utilisé lors de la conversion du certificat au format PEM.
7. Cliquez sur **Suivant** pour terminer l'assistant NetScaler Gateway sans modifier aucun autre paramètre.

Lorsque le certificat est installé sur NetScaler Gateway, il apparaît dans l'utilitaire de configuration dans le nœud **SSL \ > Certificats**.

Pour créer une clé privée

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, cliquez sur **SSL**.
2. Dans le volet d'informations, sous **Clés SSL**, cliquez sur **Créer une clé RSA**.
3. Dans Nom du**fichier clé**, tapez le nom de la clé privée ou cliquez sur Parcourir pour accéder à un fichier existant.
4. Dans**Taille de la clé (bits)**, tapez la taille de la clé privée.
5. Dans**Valeur de l'exposant public**, sélectionnez F4 ou 3.

   La valeur de l'exposant public de la clé RSA. Cela fait partie de l'algorithme de chiffrement et est nécessaire à la création de la clé RSA. Les valeurs sont F4 (Hex : 0x10001) ou 3 (Hex : 0x3). La valeur par défaut est F4.
6. Dans**Format de clé**, sélectionnez PEM ou DER. Citrix recommande le format PEM pour le certificat.
7. Dans **Algorithme de codage PEM**, sélectionnez DES ou DES3.
8. Dans**Phrase de passe PEM**et**Verify Passphrase**, tapez le mot de passe, cliquez sur **Créer**, puis cliquez sur **Fermer**.

   Remarque : Pour attribuer une phrase de passe, le format de clé doit être PEM et vous devez sélectionner l'algorithme de codage.

Pour créer une clé privée DSA dans l'utilitaire de configuration, cliquez sur**Créer une clé DSA** et suivez les étapes de création de la clé privée RSA.

Listes de révocation des certificats

March 27, 2024

De temps en temps, les autorités de certification (CA) émettent des listes de révocation de certificats (CRL). Les CRL contiennent des informations sur les certificats qui ne peuvent plus être approuvés. Par exemple, supposons qu'Ann quitte XYZ Corporation. L'entreprise peut placer le certificat d'Ann sur une CRL pour l'empêcher de signer des messages avec cette clé.

De même, vous pouvez révoquer un certificat si une clé privée est compromise ou si ce certificat a expiré et qu'un nouveau certificat est en cours d'utilisation. Avant d'approuver une clé publique, assurez-vous que le certificat n'apparaît pas sur une liste de révocation de certificats.

NetScaler Gateway prend en charge les deux types de CRL suivants :

- Liste des listes de révocation de certificats qui répertorient les certificats révoqués ou qui ne sont plus valides
- Online Certificate Status Protocol (OSCP), un protocole Internet utilisé pour obtenir l'état de révocation des certificats X.509

Pour ajouter une liste de récrl :

Avant de configurer la CRL sur l'appliance NetScaler Gateway, assurez-vous que le fichier CRL est stocké localement sur l'appliance. Dans le cas d'une configuration à haute disponibilité, le fichier CRL doit être présent sur les deux appliances NetScaler Gateway et le chemin du répertoire vers le fichier doit être le même sur les deux appliances.

Si vous devez actualiser la CRL, vous pouvez utiliser les paramètres suivants :

- Nom de la CRL : nom de la CRL ajoutée sur NetScaler. 31 caractères maximum.
- Fichier CRL : nom du fichier CRL ajouté sur NetScaler. NetScaler recherche le fichier CRL dans le répertoire /var/netscaler/ssl par défaut. 63 caractères maximum.
- URL : 127 caractères maximum
- DN de base : 127 caractères maximum
- Bind DN : 127 caractères maximum
- Mot de passe : 31 caractères maximum
- Nombre de jours : 31 jours maximum

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez SSL, puis cliquez sur CRL.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Add CRL, spécifiez les valeurs des éléments suivants :

    - Nom de la CRL
    - Fichier CRL
    - Format (facultatif)
    - Certificat CA (facultatif)

4. Cliquez sur **Create**, puis cliquez sur **Close**. Dans le volet de détails de la CRL, sélectionnez la CRL que vous avez configurée et vérifiez que les paramètres qui apparaissent en bas de l'écran sont corrects.

Pour configurer l'actualisation automatique des LCR à l'aide de LDAP ou de HTTP dans l'interface graphique, procédez comme suit :

Une liste de révocation de certificats est générée et publiée par une autorité de certification périodiquement ou, parfois, immédiatement après la révocation d'un certificat particulier. Citrix vous recommande de mettre régulièrement à jour les CRL sur l'appliance NetScaler Gateway pour vous protéger contre les clients qui tentent de se connecter avec des certificats non valides.

L'appliance NetScaler Gateway peut actualiser les CRL à partir d'un emplacement Web ou d'un annuaire LDAP. Lorsque vous spécifiez des paramètres d'actualisation et un emplacement Web ou un serveur LDAP, il n'est pas nécessaire que la CRL soit présente sur le disque dur local au moment de l'exécution de la commande. La première actualisation stocke une copie sur le disque dur local, dans le chemin spécifié par le paramètre Fichier CRL. Le chemin d'accès par défaut pour le stockage de la CRL est /var/netscaler/ssl.

Paramètres d'actualisation CRL

- **Nom de la CRL**

  Le nom de la CRL en cours d'actualisation sur NetScaler Gateway.

- **Activer l'actualisation automatique des LCR**

  Activez ou désactivez l'actualisation automatique des LCR.

- **Certificat CA**

  Le certificat de l'autorité de certification qui a émis la CRL. Ce certificat d'autorité de certification doit être installé sur l'appliance. NetScaler ne peut mettre à jour les CRL qu'à partir des autorités de certification dont les certificats y sont installés.

- **Méthode**

  Protocole permettant d'obtenir l'actualisation de la liste de rétention de certificat à partir d'un serveur Web (HTTP) ou d'un serveur LDAP. Valeurs possibles : HTTP, LDAP. Par défaut : HTTP.

- **Étendue**

  L'étendue de l'opération de recherche sur le serveur LDAP. Si la portée spécifiée est Base, la recherche est au même niveau que le nom unique de base. Si la portée spécifiée est One, la recherche s'étend jusqu'à un niveau inférieur au DN de base.

- **Server IP**

  Adresse IP du serveur LDAP à partir duquel la CRL est récupérée. Sélectionnez IPv6 pour utiliser une adresse IP IPv6.

- **Port**

  Numéro de port sur lequel le serveur LDAP ou HTTP communique.

- **Adresse URL**

  URL de l'emplacement Web à partir duquel la CRL est récupérée.

- **DN de base**

  DN de base utilisé par le serveur LDAP pour rechercher l'attribut CRL.
  Remarque : Citrix recommande d'utiliser l'attribut DN de base au lieu du nom de l'émetteur du

certificat de l'autorité de certification pour rechercher la liste de rétention de certificats dans le serveur LDAP. Le champ Issuer-Name peut ne pas correspondre exactement au nom unique de la structure d'annuaire LDAP.

- **DN de liaison**

  L'attribut Bind DN est utilisé pour accéder à l'objet CRL dans le référentiel LDAP. Les attributs de nom unique de liaison sont les informations d'identification de l'administrateur du serveur LDAP. Configurez ce paramètre pour limiter l'accès non autorisé aux serveurs LDAP.

- **Mot de passe**

  Mot de passe administrateur utilisé pour accéder à l'objet CRL dans le référentiel LDAP. Un mot de passe est requis si l'accès au référentiel LDAP est restreint, c'est-à-dire que l'accès anonyme n'est pas autorisé.

- **Intervalle**

  Intervalle auquel l'actualisation de la LCR doit être effectuée. Pour une actualisation instantanée des LCR, spécifiez l'intervalle sur MAINTENANT. Valeurs possibles : MENSUEL, QUOTIDIEN, HEBDOMADAIRE, MAINTENANT, AUCUN.

- **Jours**

  Le jour où l'actualisation de la LCR doit être effectuée. Cette option n'est pas disponible si l'intervalle est défini sur QUOTIDIEN.

- **Heure**

  Heure exacte, au format 24 heures, à laquelle l'actualisation de la LCR doit être effectuée.

- **Binaire**

  Définissez le mode de récupération de la liste de révocation de révocation de révocation de révocation de révocation Valeurs possibles : OUI, NON. Par défaut : NON.

1. Dans le volet de navigation, développez SSL, puis cliquez sur CRL.
2. Sélectionnez la CRL configurée pour laquelle vous souhaitez mettre à jour les paramètres d'actualisation, puis cliquez sur Ouvrir.
3. Sélectionnez l'option Activer l'actualisation automatique des LCR.
4. Dans le groupe Paramètres d'actualisation automatique de la LCR, spécifiez les valeurs des paramètres suivants :
   Remarque : Un astérisque (*) indique un paramètre obligatoire.

   - Méthode
   - Binaire
   - Étendue
   - Server IP

- Port*
- Adresse URL
- DN de base*
- DN de liaison
- Mot de passe
- Intervalle
- Jours
- Heure

5. Cliquez sur Créer. Dans le volet CRL, sélectionnez la CRL que vous avez configurée et vérifiez que les paramètres qui apparaissent en bas de l'écran sont corrects.

Surveiller l'état des certificats avec OCSP

Le protocole OCSP (Online Certificate Status Protocol) est un protocole Internet utilisé pour déterminer l'état d'un certificat SSL client. NetScaler Gateway prend en charge l'OCSP tel que défini dans la RFC 2560. OCSP offre des avantages significatifs par rapport aux listes de révocation de certificats (CRL) en termes d'informations en temps opportun. Le statut de révocation à jour d'un certificat client est particulièrement utile dans les transactions impliquant des sommes d'argent importantes et des transactions boursières de grande valeur. Il utilise également moins de ressources système et réseau. L'implémentation d'OCSP par NetScaler Gateway inclut le traitement par lots des demandes et la mise en cache des réponses.

Implémentation d'OCSP par NetScaler Gateway

La validation OCSP sur une appliance NetScaler Gateway commence lorsque NetScaler Gateway reçoit un certificat client lors d'une liaison SSL. Pour valider le certificat, NetScaler Gateway crée une demande OCSP et la transmet au répondeur OCSP. Pour ce faire, NetScaler Gateway extrait l'URL du répondeur OCSP à partir du certificat client ou utilise une URL configurée localement. La transaction est suspendue jusqu'à ce que NetScaler Gateway évalue la réponse du serveur et détermine s'il faut autoriser la transaction ou la rejeter. Si la réponse du serveur est retardée au-delà de la durée configurée et qu'aucun autre répondeur n'est configuré, NetScaler Gateway autorise la transaction ou affiche une erreur, selon que vous avez défini le contrôle OCSP sur facultatif ou obligatoire. NetScaler Gateway prend en charge le traitement par lots des requêtes OCSP et la mise en cache des réponses OCSP afin de réduire la charge sur le répondeur OCSP et de fournir des réponses plus rapides.

traitement par lots de demandes OCSP

Chaque fois que NetScaler Gateway reçoit un certificat client, il envoie une demande au répondeur OCSP. Pour éviter de surcharger le répondeur OCSP, NetScaler Gateway peut demander l'état de

plusieurs certificats clients dans la même demande. Pour que le traitement par lots de demandes fonctionne efficacement, vous devez définir un délai d'expiration afin que le traitement d'un seul certificat ne soit pas retardé pendant l'attente de la formation d'un lot.

Mise en cache des réponses OCSP

La mise en cache des réponses reçues du répondeur OCSP permet de répondre plus rapidement à l'utilisateur et de réduire la charge sur le répondeur OCSP. Dès réception de l'état de révocation d'un certificat client de la part du répondeur OCSP, NetScaler Gateway met la réponse en cache localement pendant une durée prédéfinie. Lorsqu'un certificat client est reçu lors d'une connexion SSL, NetScaler Gateway vérifie d'abord dans son cache local une entrée pour ce certificat. Si une entrée est toujours valide (dans la limite du délai d'expiration du cache), elle est évaluée et le certificat client est accepté ou rejeté. Si aucun certificat n'est trouvé, NetScaler Gateway envoie une demande au répondeur OCSP et stocke la réponse dans son cache local pendant une durée configurée.

Configurer l'état du certificat OCSP

La configuration d'un protocole OCSP (Online Certificate Status Protocol) implique l'ajout d'un répondeur OCSP, la liaison du répondeur OCSP à un certificat signé d'une autorité de certification (CA) et la liaison du certificat et de la clé privée à un serveur virtuel SSL (Secure Sockets Layer). Si vous devez lier un certificat et une clé privée différents à un répondeur OCSP que vous avez déjà configuré, vous devez d'abord délier le répondeur, puis lier le répondeur à un autre certificat.

Pour configurer OCSP

1. Sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Répondeur OCSP.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom, saisissez le nom du profil.
4. Dans URL, tapez l'adresse Web du répondeur OCSP.

   Ce champ est obligatoire. L'adresse Web ne peut pas dépasser 32 caractères.
5. Pour mettre en cache les réponses OCSP, cliquez sur Cache et dans Time-out, tapez le nombre de minutes pendant lesquelles NetScaler Gateway conserve la réponse.
6. Sous Request Batching, cliquez sur Activer.
7. Dans la zone Délai de traitement par lots, spécifiez la durée, en millisecondes, autorisée pour le traitement par lots d'un groupe de demandes OCSP.

Les valeurs peuvent être comprises entre 0 et 10000. La valeur par défaut est 1.

8. Dans Produced At Time Skew, tapez le temps que NetScaler Gateway peut utiliser pendant lequel l'appliance doit vérifier ou accepter la réponse.
9. Sous Vérification des réponses, sélectionnez Réponses de confiance si vous souhaitez désactiver les vérifications de signature par le répondeur OCSP.

   Si vous activez les réponses d'approbation, ignorez les étapes 8 et 9.
10. Dans Certificat, sélectionnez le certificat utilisé pour signer les réponses OCSP.

    Si aucun certificat n'est sélectionné, l'autorité de certification à laquelle le répondeur OCSP est lié est utilisée pour vérifier les réponses.
11. Dans la zone Délai d'expiration de la demande, tapez le nombre de millisecondes d'attente d'une réponse OCSP.

    Cette durée inclut le délai de traitement par lots. Les valeurs peuvent être comprises entre 0 et 120000. La valeur par défaut est 2000.
12. Dans Signing Certificate, sélectionnez le certificat et la clé privée utilisés pour signer les demandes OCSP. Si vous ne spécifiez pas de certificat et de clé privée, les demandes ne sont pas signées.
13. Pour activer le numéro utilisé une fois, (`nonce`) `extension` sélectionnez Nonce.
14. Pour utiliser un certificat client, cliquez sur Insertion de certificat client.
15. Cliquez sur Create, puis cliquez sur Close.

Gérer les paramètres de configuration de NetScaler Gateway

January 26, 2024

Lorsque vous apportez des modifications à la configuration de NetScaler Gateway, les modifications sont enregistrées dans des fichiers journaux. Vous pouvez afficher plusieurs types de paramètres de configuration :

- Configuration enregistrée. Vous pouvez consulter les paramètres que vous avez enregistrés sur NetScaler Gateway.
- Configuration en cours d'exécution. Vous pouvez afficher les paramètres actifs, tels qu'un serveur virtuel ou une stratégie d'authentification, que vous avez configurés mais que vous n'avez pas enregistrés en tant que configuration enregistrée dans NetScaler Gateway.
- Configuration en cours d'exécution et configuration enregistrée. Vous pouvez comparer côte à côte la configuration en cours et la configuration enregistrée sur NetScaler Gateway.

Vous pouvez également effacer les paramètres de configuration sur NetScaler Gateway.

Important : si vous choisissez d'effacer les paramètres de NetScaler Gateway, les certificats, les serveurs virtuels et les stratégies sont supprimés. Citrix recommande de ne pas effacer la configuration.

Enregistrez la configuration de NetScaler Gateway

Vous pouvez enregistrer votre configuration actuelle sur NetScaler Gateway sur un ordinateur de votre réseau, afficher la configuration en cours d'exécution et comparer les configurations enregistrées et en cours d'exécution.

Pour enregistrer la configuration sur NetScaler Gateway

1. Dans l'utilitaire de configuration, au-dessus du volet d'informations, cliquez sur l'icône Enregistrer, puis sur Oui.

Pour afficher et enregistrer le fichier de configuration sur NetScaler Gateway

La configuration enregistrée est celle qui est enregistrée dans un fichier journal sur NetScaler Gateway, tels que les paramètres des serveurs virtuels, des stratégies, des adresses IP, des utilisateurs, des groupes et des certificats.

Lorsque vous configurez les paramètres sur NetScaler Gateway, vous pouvez les enregistrer dans un fichier sur votre ordinateur. Si vous devez réinstaller le logiciel NetScaler Gateway ou si vous supprimez accidentellement certains paramètres, vous pouvez utiliser ce fichier pour restaurer votre configuration. Si vous devez restaurer les paramètres, vous pouvez copier le fichier sur NetScaler Gateway et redémarrer l'appliance à l'aide de l'interface de ligne de commande ou d'un programme, tel que WinSCP, pour copier le fichier vers NetScaler Gateway.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Diagnostics.
2. Dans le volet d'informations, sous Afficher la configuration, cliquez sur Configuration enregistrée.
3. Dans la boîte de dialogue Configuration enregistrée, cliquez sur Enregistrer le texte de sortie dans un fichier, nommez le fichier, puis cliquez sur Enregistrer.
   Remarque : Citrix recommande d'enregistrer le fichier sous le nom de fichier ns.conf.

Pour afficher la configuration en cours d'exécution

Toute modification apportée à NetScaler Gateway sans effort pour l'enregistrer est appelée configuration en cours d'exécution. Ces paramètres sont actifs sur NetScaler Gateway, mais ne sont pas enregistrés sur l'appliance. Si vous avez configuré des paramètres supplémentaires, tels qu'une stratégie, un serveur virtuel, des utilisateurs ou des groupes, vous pouvez afficher ces paramètres dans la configuration en cours d'exécution.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Diagnostics.
2. Dans le volet d'informations, sous Afficher la configuration, cliquez sur Configuration en cours d'exécution.

Pour comparer la configuration enregistrée et en cours d'exécution

Vous pouvez voir quels paramètres sont enregistrés sur l'appliance et comparer ces paramètres à la configuration en cours d'exécution. Vous pouvez choisir d'enregistrer la configuration en cours d'exécution ou d'apporter des modifications à la configuration.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Diagnostics.
2. Dans le volet d'informations, sous Afficher la configuration, cliquez sur Enregistrer v/s en cours d'exécution.

Effacez la configuration de NetScaler Gateway

Vous pouvez effacer les paramètres de configuration sur NetScaler Gateway. Vous pouvez choisir parmi les trois niveaux de paramètres suivants à effacer :

Important : Citrix recommande d'enregistrer votre configuration avant d'effacer les paramètres de configuration de NetScaler Gateway.

- Basique. Efface tous les paramètres de l'appliance, à l'exception de l'adresse IP du système, de la passerelle par défaut, des adresses IP mappées, des adresses IP de sous-réseau, des paramètres DNS, des paramètres réseau, des paramètres de haute disponibilité, du mot de passe administratif et des paramètres de fonctionnalité et de mode.
- Étendu. Efface tous les paramètres à l'exception de l'adresse IP du système, des adresses IP mappées, des adresses IP de sous-réseau, des paramètres DNS et des définitions de haute disponibilité.
- Complet. Restaure la configuration aux paramètres d'usine d'origine, à l'exclusion de l'adresse IP du système (NSIP) et de la route par défaut, qui sont nécessaires pour maintenir la connectivité réseau avec l'appliance.

Lorsque vous effacez tout ou partie de la configuration, les paramètres des fonctionnalités sont définis sur les paramètres d'usine par défaut.

Lorsque vous effacez la configuration, les fichiers stockés sur NetScaler Gateway, tels que les certificats et les licences, ne sont pas supprimés. Le fichier ns.conf n'est pas modifié. Si vous souhaitez enregistrer la configuration avant d'effacer la configuration, enregistrez-la d'abord sur votre ordinateur. Si vous enregistrez la configuration, vous pouvez restaurer le fichier ns.conf sur NetScaler Gateway. Après avoir restauré le fichier sur l'appliance et redémarré NetScaler Gateway, tous les paramètres de configuration de ns.conf sont restaurés.

Les modifications apportées aux fichiers de configuration, tels que rc.conf, ne sont pas annulées.

Si vous disposez d'une paire haute disponibilité, les deux appliances NetScaler Gateway sont modifiées de la même manière. Par exemple, si vous effacez la configuration de base d'une appliance, les modifications sont propagées vers la seconde appliance.

Pour effacer les paramètres de configuration de NetScaler Gateway

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Diagnostics.
2. Dans le volet d'informations, sous Maintenance, cliquez sur Effacer la configuration.
3. Dans Niveau de configuration, sélectionnez le niveau à effacer, puis cliquez sur Exécuter.

Gestion des certificats sur NetScaler Gateway

January 26, 2024

Sur NetScaler Gateway, vous utilisez des certificats pour créer des connexions sécurisées et authentifier les utilisateurs.

Pour établir une connexion sécurisée, un certificat de serveur est requis à une extrémité de la connexion. Un certificat racine de l'autorité de certification (CA) qui a émis le certificat de serveur est requis à l'autre extrémité de la connexion.

- Certificat serveur. Un certificat de serveur certifie l'identité du serveur. NetScaler Gateway nécessite ce type de certificat numérique.
- Certificat racine. Un certificat racine identifie l'autorité de certification qui a signé le certificat de serveur. Le certificat racine appartient à l'autorité de certification. Une machine utilisateur a besoin de ce type de certificat numérique pour vérifier le certificat de serveur.

Lors de l'établissement d'une connexion sécurisée avec un navigateur Web sur la machine utilisateur, le serveur envoie son certificat à l'appareil.

Lorsque la machine utilisateur reçoit un certificat de serveur, le navigateur Web, tel qu'Internet Explorer, vérifie quelle autorité de certification a émis le certificat et si l'autorité de certification est approuvée par la machine utilisateur. Si l'autorité de certification n'est pas approuvée ou s'il s'agit d'un certificat de test, le navigateur Web invite l'utilisateur à accepter ou à refuser le certificat (en acceptant ou en refusant la possibilité d'accéder au site).

NetScaler Gateway prend en charge les trois types de certificats suivants :

- Certificat de test lié à un serveur virtuel et pouvant également être utilisé pour les connexions à une batterie de serveurs. NetScaler Gateway est fourni avec un certificat de test préinstallé.
- Certificat au format PEM ou DER signé par une autorité de certification et associé à une clé privée.
- Certificat au format PKCS #12 utilisé pour stocker ou transporter le certificat et la clé privée. Le certificat PKCS #12 est généralement exporté à partir d'un certificat Windows existant sous forme de fichier PFX, puis installé sur NetScaler Gateway.

Citrix recommande d'utiliser un certificat signé par une autorité de certification approuvée, telle que Thawte ou Verisign.

Créer une demande de signature de certificat

March 27, 2024

Pour fournir des communications sécurisées via SSL ou TLS, un certificat de serveur est requis sur NetScaler Gateway. Avant de pouvoir charger un certificat sur NetScaler Gateway, vous devez générer une demande de signature de certificat (CSR) et une clé privée. Vous utilisez la demande de création de certificat incluse dans l'assistant NetScaler Gateway ou l'utilitaire de configuration pour créer le CSR. La demande de création de certificat crée un fichier .csr qui est envoyé par e-mail à l'autorité de certification (CA) pour signature et une clé privée qui reste sur l'appliance. L'autorité de certification signe le certificat et vous le renvoie à l'adresse e-mail que vous avez fournie. Lorsque vous recevez le certificat signé, vous pouvez l'installer sur NetScaler Gateway. Lorsque vous recevez le certificat de la part de l'autorité de certification, vous associez le certificat à la clé privée.

Important : lorsque vous utilisez l'assistant NetScaler Gateway pour créer le CSR, vous devez quitter l'assistant et attendre que l'autorité de certification vous envoie le certificat signé. Lorsque vous recevez le certificat, vous pouvez réexécuter l'assistant NetScaler Gateway pour créer les paramètres et installer le certificat. Pour plus d'informations sur l'assistant NetScaler Gateway, voir Configuration des paramètres à l'aide de l'assistant NetScaler Gateway.

Créez un CSR à l'aide de l'assistant NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Getting Started, cliquez sur l'assistant **NetScaler Gateway**.
3. Suivez les instructions de l'assistant jusqu'à ce que vous arriviez à la page Spécifier un certificat de serveur.
4. Cliquez sur **Créer une demande de signature de certificat** et remplissez les champs.
   Remarque : Le nom de domaine complet (FQDN) ne doit pas nécessairement être le même que le nom d'hôte NetScaler Gateway. Le nom de domaine complet est utilisé pour l'ouverture de session de l'utilisateur.
5. Cliquez sur **Créer** pour enregistrer le certificat sur votre ordinateur, puis cliquez sur **Fermer**.
6. Quittez l'assistant NetScaler Gateway sans enregistrer vos paramètres.

Création d'un CSR à l'aide de l'interface graphique NetScaler

Vous pouvez également utiliser l'interface graphique de NetScaler pour créer un CSR, sans exécuter l'assistant NetScaler Gateway.

1. Accédez à **Gestiondu trafic**>**SSL > Fichiers SSL**et sélectionnez**Créer une demande de signature de certificat (CSR)**.
2. Renseignez les paramètres du certificat, puis cliquez sur **Créer**.

Après avoir créé le certificat et la clé privée, envoyez le certificat par e-mail à l'autorité de certification, telle que Thawte ou Verisign.

Pour obtenir une procédure détaillée, consultez la section Créer une demande de signature de certificat.

Installation du certificat signé sur NetScaler Gateway

Lorsque vous recevez le certificat signé de l'autorité de certification (CA), associez-le à la clé privée de l'appliance, puis installez le certificat sur NetScaler Gateway.

Jumeler le certificat signé avec une clé privée à l'aide de l'interface graphique

1. Copiez le certificat vers NetScaler Gateway dans le dossier nsconfig/ssl à l'aide d'un programme Secure Shell (SSH) tel que WinSCP.
2. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **SSL > Certificats**.

3. Dans la page **Certificat SSL**, cliquez sur **Démarrer**.
4. Dans le volet d'informations, cliquez sur **Installer**.
5. Dans **Nom de la paire de clés** de certificat, tapez le nom du certificat.
6. Dans **Nom du fichier de certificat**, cliquez sur **Appliance**.
7. Accédez au certificat, cliquez sur **Sélectionner**, puis sur **Ouvrir**.
8. Dans **Nom du fichier clé**, cliquez sur **Appliance**. Le nom de la clé privée est identique à celui de la demande de signature de certificat (CSR). La clé privée se trouve sur NetScaler Gateway dans le répertoire \ nsconfig \ ssl.
9. Choisissez la clé privée, puis cliquez sur **Ouvrir**.
10. Si le certificat est au format PEM, dans Mot de **passe**, saisissez le mot de passe de la clé privée.
11. Si vous souhaitez configurer la notification pour la date d'expiration du certificat, sélectionnez **Notifier lorsque le certificat expire**.
12. Dans **Période de notification**, tapez le nombre de jours, cliquez sur **Créer**, puis sur **Fermer**.

Liez le certificat et la clé privée à un serveur virtuel à l'aide de l'interface graphique

Après avoir créé et lié une paire de certificats et de clés privées, liez-la à un serveur virtuel.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet Certificats, sous **Disponible**, sélectionnez un certificat, cliquez sur **Ajouter**, puis sur **OK**.

Liez le certificat et la clé privée à un serveur virtuel à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

Exemple :

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA -
    ocspCheck Mandatory
<!--NeedCopy-->
```

Remarque : OSCPCheck est facultatif si la vérification OCSP n'est pas requise pour le certificat de périphérique.

Délier les certificats de test du serveur virtuel à l'aide de l'interface graphique

Après avoir installé le certificat signé, déliez tous les certificats de test liés au serveur virtuel. Vous pouvez délier les certificats de test à l'aide de l'utilitaire de configuration.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet Certificats, sous **Configuré**, sélectionnez le certificat de test, puis cliquez sur **Supprimer**.

Configuration des certificats intermédiaires

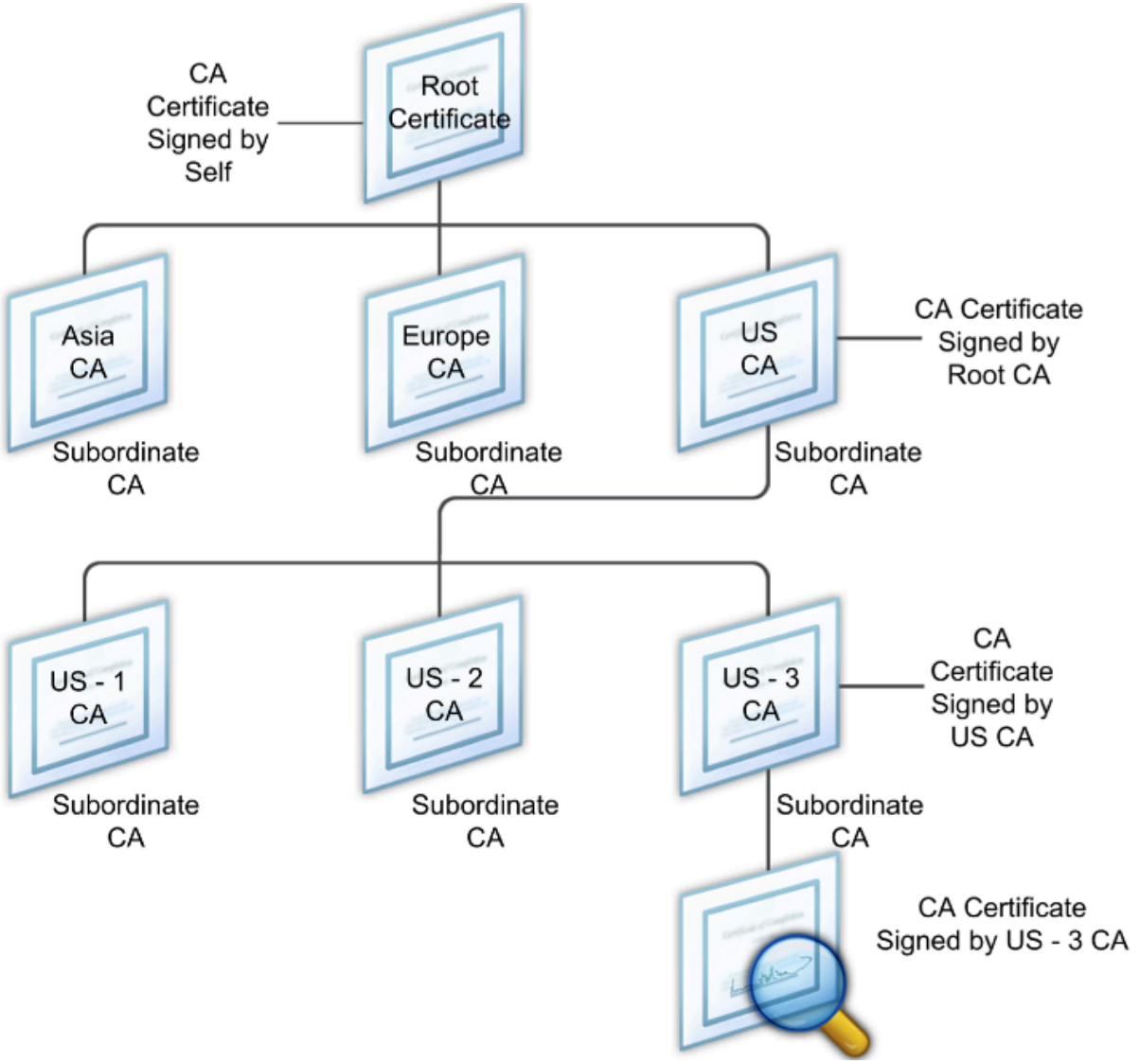
January 26, 2024

Un certificat intermédiaire est un certificat qui fait le lien entre NetScaler Gateway (le certificat du serveur) et un certificat racine (installé sur la machine utilisateur). Un certificat intermédiaire fait partie d'une chaîne.

Certaines organisations délèguent l'émission des certificats pour résoudre les problèmes liés à la dispersion géographique de leurs unités ou pour appliquer des stratégies d'émission différentes selon leurs secteurs d'activité.

La responsabilité de l'émission des certificats peut être déléguée en configurant des autorités de certification (CA) subordonnées. Les autorités de certification peuvent signer leurs propres certificats (c'est-à-dire qu'elles sont auto-signées) ou elles peuvent être signées par une autre autorité de certification. La norme X.509 inclut un modèle de mise en place d'une hiérarchie de CA. Dans ce modèle, comme illustré dans la figure suivante, l'autorité de certification racine se trouve en haut de la hiérarchie et est un certificat auto-signé par l'autorité de certification. Les autorités de certification qui sont directement subordonnées à l'autorité de certification racine possèdent des certificats d'autorité de certification signés par l'autorité de certification racine. Les CA situées sous les CA subordonnées dans la hiérarchie disposent de certificats signés par les CA subordonnées.

Figure 1. Modèle X.509 illustrant la structure hiérarchique d'une chaîne de certificats numériques classique



Si un certificat de serveur est signé par une autorité de certification avec un certificat auto-signé, la chaîne de certificats est composée exactement de deux certificats : le certificat d'entité finale et l'autorité de certification racine. Si un certificat d'utilisateur ou de serveur est signé par une autorité de certification intermédiaire, la chaîne de certificats est plus longue.

La figure suivante montre que les deux premiers éléments sont le certificat d'entité finale (dans ce cas, gwy01.company.com) et le certificat de l'autorité de certification intermédiaire, dans cet ordre. Le certificat de l'autorité de certification intermédiaire est suivi du certificat de son autorité de certification. Cette liste se poursuit jusqu'à ce que le dernier certificat de la liste soit destiné à une autorité de certification racine. Chaque certificat de la chaîne atteste de l'identité du certificat précédent.

Figure 2. Chaîne de certificats numériques classique

Installer un certificat intermédiaire

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Certificats.
2. Dans le volet d'informations, cliquez sur Installer.
3. Dans Nom de la paire de clés de certificat, tapez le nom du certificat.
4. Sous Détails, dans Nom du fichier de certificat, cliquez sur Parcourir (Appliance) et dans la liste, sélectionnez Local ou Appliance.
5. Accédez au certificat sur votre ordinateur (local) ou sur NetScaler Gateway (Appliance).
6. Dans Format de certificat, sélectionnez PEM.
7. Cliquez sur Installer, puis sur Fermer.

Lorsque vous installez un certificat intermédiaire sur NetScaler Gateway, vous n'avez pas besoin de spécifier de clé privée ni de mot de passe.

Une fois le certificat installé sur l'appliance, il doit être lié au certificat du serveur.

Lier un certificat intermédiaire à un certificat de serveur

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Certificats.
2. Dans le volet d'informations, sélectionnez le certificat du serveur, puis dans Action, cliquez sur Lier.
3. En regard de Nom du certificat de l'autorité de certification, sélectionnez le certificat intermédiaire dans la liste, puis cliquez sur OK.

Utiliser des certificats d'appareil pour l'authentification

March 27, 2024

NetScaler Gateway prend en charge la vérification du certificat de l'appareil qui vous permet de lier l'identité de l'appareil à la clé privée d'un certificat. La vérification du certificat de l'appareil peut

être configurée dans le cadre de stratégies EPA (Endpoint Analysis) classiques ou avancées. Dans les stratégies EPA classiques, le certificat d'appareil ne peut être configuré que pour l'EPA de pré-authentification.

NetScaler Gateway vérifie le certificat de l'appareil avant l'exécution de l'analyse des terminaux ou avant l'affichage de la page de connexion. Si vous configurez l'analyse des points de terminaison, l'analyse des points de terminaison est exécutée pour vérifier la machine utilisateur. Lorsque l'appareil passe l'analyse et que NetScaler Gateway a vérifié le certificat de l'appareil, les utilisateurs peuvent se connecter à NetScaler Gateway.

> **Important :**
>
> - Par défaut, Windows impose des privilèges d'administrateur pour accéder aux certificats d'appareil.
> - Pour ajouter une vérification de certificat d'appareil pour les utilisateurs non administrateurs, vous devez installer le plug-in VPN. La version du plug-in VPN doit être la même que celle du plug-in EPA sur l'appareil.
> - Vous pouvez ajouter plusieurs certificats d'autorité de certification à la passerelle et valider le certificat de l'appareil.
> - Si vous installez deux certificats d'appareils ou plus sur NetScaler Gateway, les utilisateurs doivent sélectionner le bon certificat lorsqu'ils commencent à se connecter à NetScaler Gateway ou avant l'exécution de l'analyse des terminaux.
> - Lorsque vous créez le certificat de périphérique, il doit s'agir d'un certificat X.509.
> - Si vous disposez d'un certificat de périphérique émis par une autorité de certification intermédiaire, les certificats d'autorité de certification intermédiaire et racine doivent être liés.
> - Le client EPA a besoin que l'utilisateur dispose de droits d'administrateur local pour pouvoir accéder au magasin de certificats de la machine. C'est rarement le cas. Par conséquent, une solution de contournement consiste à installer le plug-in NetScaler Gateway complet qui peut accéder au magasin local.

Pour plus d'informations sur la création de certificats d'appareil, consultez les sections suivantes :

- Network Device Enrollment Service (NDES) dans les services de certificats Active Directory (AD CS) sur le site Web de Microsoft.
- Comment demander un certificat à une autorité de certification Microsoft à l'aide de DCE/RPC et de la charge utile du profil de certificat Active Directory sur le site Web d'assistance Apple.
- Émissionde certificats iPad ou iPhone sur le blog de support Microsoft Ask the Directory Services Team.
- Configuration du service d'inscription des appareils réseau sur le site Web Windows IT Pro.
- Exemple pas à pas de déploiement des certificats PKI pour Configuration Manager : Autorité de certification Windows Server 2008 ? RedirectedFrom=MSDN) sur le site Web de Microsoft System

Center.

Étapes de configuration des certificats d'appareils

Pour configurer un certificat d'appareil, vous devez effectuer les étapes suivantes :

- Installez le certificat d'autorité de certification de l'émetteur du certificat de l'appareil sur NetScaler Gateway. Pour plus de détails, consultez la section Installation du certificat signé sur NetScaler Gateway.
- Liez le certificat d'autorité de certification de l'émetteur du certificat de l'appareil au serveur virtuel NetScaler Gateway et activez la vérification OCSP. Pour plus de détails, consultez la section Installation du certificat signé sur NetScaler Gateway.
- Créez et liez OCSP (répondeur) sur le certificat d'autorité de certification de l'émetteur du certificat de périphérique. Pour plus d'informations, consultez la section Surveiller l'état des certificats avec OCSP.

Activez la vérification des certificats de périphérique sur le serveur virtuel et ajoutez le certificat d'autorité de certification de l'émetteur du certificat de périphérique à la liste de vérification des certificats de périphérique. Pour plus d'informations, consultez la section Activer la vérification des certificats de périphériques sur un serveur virtuel pour la stratégie EPA classique.

Terminez la configuration côté client et la vérification du certificat de périphérique sur la machine Windows. Pour plus d'informations, consultez la section Vérification du certificat de périphérique sur un ordinateur Windows.

> **Remarque :**
>
> Le certificat de périphérique doit être installé dans le magasin de certificats système de la machine pour tous les clients destinés à bénéficier de la vérification EPA du certificat de périphérique.

Activer la vérification des certificats de périphériques sur un serveur virtuel pour la stratégie EPA classique

Après avoir créé le certificat de l'appareil, vous l'installez sur NetScaler Gateway en suivant la procédure d'importation et d'installation d'un certificat existant dans NetScaler Gateway.

1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Virtual Servers**.
2. Sur la page **Serveurs virtuels NetScaler Gateway**, sélectionnez un serveur virtuel existant et cliquez sur **Modifier**.
3. Sur la page **Serveurs virtuels VPN**, dans la section **Paramètres de base**, cliquez sur **Modifier**.
4. Décochez la case **Activer l'authentification** pour désactiver l'authentification.

5. Cochez la case **Activer le certificat de périphérique** pour activer le certificat de périphérique
6. Cliquez sur **Ajouter** pour ajouter le nom du certificat d'autorité de certification d'un émetteur de certificat de périphérique disponible à la liste.
7. Pour lier un certificat d'autorité de certification au serveur virtuel, cliquez sur **Certificat d'autorité de certification** dans la section **Certificat d'autorité de certification pour périphérique**, cliquez sur **Ajouter**, sélectionnez le certificat, puis cliquez sur **+**.

> **Remarque :**
>
> Pour plus d'informations sur l'activation et la liaison de certificats de périphériques sur un serveur virtuel pour une stratégie EPA avancée, consultez la section Certificat de périphérique dans nFactor en tant que composant EPA.

Vérification du certificat de l'appareil sur une machine Windows

1. Ouvrez un navigateur et accédez au FQDN de NetScaler Gateway.
2. Autorisez l'exécution du client Citrix End Point Analysis (EPA). Si ce n'est pas déjà fait, installez l'EPA.

   Citrix EPA exécute et valide le certificat de périphérique et redirige vers la page d'authentification si le contrôle EPA du certificat de périphérique est réussi, sinon il vous redirige vers la page d'erreur EPA. Dans le cas où vous disposez d'autres contrôles EPA, les résultats de l'analyse EPA dépendent des contrôles EPA configurés.

Pour un débogage plus poussé sur le client, examinez les journaux EPA suivants sur le client :
C:\Users <User name>\ AppData \ Local \ Citrix \ AGEE \ nsepa.txt

Remarque :

> La vérification du certificat d'appareil avec la liste de réexamen de certificats n'est pas prise

Importation et installation d'un certificat existant

March 27, 2024

Vous pouvez importer un certificat existant à partir d'un ordinateur Windows exécutant Internet Information Services (IIS) ou d'un ordinateur exécutant Secure Gateway.

Lorsque vous exportez le certificat, veillez à exporter également la clé privée. Parfois, vous ne pouvez pas exporter la clé privée, ce qui signifie que vous ne pouvez pas installer le certificat sur NetScaler

Gateway. Si cela se produit, utilisez la demande de signature de certificat (CSR) pour créer un certificat. Pour plus d'informations, consultez la section Création d'une demande de signature de certificat.

Lorsque vous exportez un certificat et une clé privée depuis Windows, l'ordinateur crée un fichier d'échange d'informations personnelles (.pfx). Ce fichier est ensuite installé sur NetScaler Gateway en tant que certificat PKCS #12.

Si vous remplacez le Secure Gateway par NetScaler Gateway, vous pouvez exporter le certificat et la clé privée depuis le Secure Gateway. Si vous effectuez une migration sur place de Secure Gateway vers NetScaler Gateway, le nom de domaine complet (FQDN) de l'application et de l'appliance doit être identique. Lorsque vous exportez le certificat depuis Secure Gateway, vous retirez immédiatement le Secure Gateway, vous installez le certificat sur NetScaler Gateway, puis vous testez la configuration. Secure Gateway et NetScaler Gateway ne peuvent pas s'exécuter simultanément sur votre réseau s'ils possèdent le même nom de domaine complet.

Si vous utilisez Windows Server 2003 ou Windows Server 2008, vous pouvez utiliser la console de gestion Microsoft pour exporter le certificat. Pour plus d'informations, consultez l'aide en ligne de Windows.

Conservez les valeurs par défaut pour toutes les autres options, définissez un mot de passe et enregistrez le fichier .pfx sur votre ordinateur. Lorsque le certificat est exporté, vous l'installez ensuite sur NetScaler Gateway.

Pour installer le certificat et la clé privée sur NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Getting Started, cliquez sur **l'assistant NetScaler Gateway**.
3. Cliquez sur **Suivant**, sélectionnez un serveur virtuel existant, puis cliquez sur **Suivant**.
4. Dans **Options de certificat**, sélectionnez **Installer un fichier PKCS #12 (.pfx)**.
5. Dans **Nom de fichier PKCS #12**, cliquez sur **Parcourir**, accédez au certificat, puis cliquez sur **Sélectionner**.
6. Dans ((Mot de passe)), tapez le mot de passe de la clé privée.

   Il s'agit du mot de passe que vous avez utilisé lors de la conversion du certificat au format PEM.
7. Cliquez sur **Suivant** pour terminer l'assistant NetScaler Gateway sans modifier aucun autre paramètre.

Lorsque le certificat est installé sur NetScaler Gateway, il apparaît dans l'utilitaire de configuration dans le nœud **SSL \ > Certificats**.

Pour créer une clé privée

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, cliquez sur **SSL**.
2. Dans le volet d'informations, sous **Clés SSL**, cliquez sur **Créer une clé RSA**.
3. Dans Nom du**fichier clé**, tapez le nom de la clé privée ou cliquez sur Parcourir pour accéder à un fichier existant.
4. Dans**Taille de la clé (bits)**, tapez la taille de la clé privée.
5. Dans**Valeur de l'exposant public**, sélectionnez F4 ou 3.

   La valeur de l'exposant public de la clé RSA. Cela fait partie de l'algorithme de chiffrement et est nécessaire à la création de la clé RSA. Les valeurs sont F4 (Hex : 0x10001) ou 3 (Hex : 0x3). La valeur par défaut est F4.
6. Dans**Format de clé**, sélectionnez PEM ou DER. Citrix recommande le format PEM pour le certificat.
7. Dans **Algorithme de codage PEM**, sélectionnez DES ou DES3.
8. Dans**Phrase de passe PEM**et**Verify Passphrase**, tapez le mot de passe, cliquez sur **Créer**, puis cliquez sur **Fermer**.

   Remarque : Pour attribuer une phrase de passe, le format de clé doit être PEM et vous devez sélectionner l'algorithme de codage.

Pour créer une clé privée DSA dans l'utilitaire de configuration, cliquez sur**Créer une clé DSA** et suivez les étapes de création de la clé privée RSA.

Listes de révocation des certificats

March 27, 2024

De temps en temps, les autorités de certification (CA) émettent des listes de révocation de certificats (CRL). Les CRL contiennent des informations sur les certificats qui ne peuvent plus être approuvés. Par exemple, supposons qu'Ann quitte XYZ Corporation. L'entreprise peut placer le certificat d'Ann sur une CRL pour l'empêcher de signer des messages avec cette clé.

De même, vous pouvez révoquer un certificat si une clé privée est compromise ou si ce certificat a expiré et qu'un nouveau certificat est en cours d'utilisation. Avant d'approuver une clé publique, assurez-vous que le certificat n'apparaît pas sur une liste de révocation de certificats.

NetScaler Gateway prend en charge les deux types de CRL suivants :

- Liste des listes de révocation de certificats qui répertorient les certificats révoqués ou qui ne sont plus valides
- Online Certificate Status Protocol (OSCP), un protocole Internet utilisé pour obtenir l'état de révocation des certificats X.509

Pour ajouter une liste de récrl :

Avant de configurer la CRL sur l'appliance NetScaler Gateway, assurez-vous que le fichier CRL est stocké localement sur l'appliance. Dans le cas d'une configuration à haute disponibilité, le fichier CRL doit être présent sur les deux appliances NetScaler Gateway et le chemin du répertoire vers le fichier doit être le même sur les deux appliances.

Si vous devez actualiser la CRL, vous pouvez utiliser les paramètres suivants :

- Nom de la CRL : nom de la CRL ajoutée sur NetScaler. 31 caractères maximum.
- Fichier CRL : nom du fichier CRL ajouté sur NetScaler. NetScaler recherche le fichier CRL dans le répertoire /var/netscaler/ssl par défaut. 63 caractères maximum.
- URL : 127 caractères maximum
- DN de base : 127 caractères maximum
- Bind DN : 127 caractères maximum
- Mot de passe : 31 caractères maximum
- Nombre de jours : 31 jours maximum

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez SSL, puis cliquez sur CRL.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans la boîte de dialogue Add CRL, spécifiez les valeurs des éléments suivants :

    - Nom de la CRL
    - Fichier CRL
    - Format (facultatif)
    - Certificat CA (facultatif)

4. Cliquez sur **Create**, puis cliquez sur **Close**. Dans le volet de détails de la CRL, sélectionnez la CRL que vous avez configurée et vérifiez que les paramètres qui apparaissent en bas de l'écran sont corrects.

Pour configurer l'actualisation automatique des LCR à l'aide de LDAP ou de HTTP dans l'interface graphique, procédez comme suit :

Une liste de révocation de certificats est générée et publiée par une autorité de certification périodiquement ou, parfois, immédiatement après la révocation d'un certificat particulier. Citrix vous recommande de mettre régulièrement à jour les CRL sur l'appliance NetScaler Gateway pour vous protéger contre les clients qui tentent de se connecter avec des certificats non valides.

L'appliance NetScaler Gateway peut actualiser les CRL à partir d'un emplacement Web ou d'un annuaire LDAP. Lorsque vous spécifiez des paramètres d'actualisation et un emplacement Web ou un serveur LDAP, il n'est pas nécessaire que la CRL soit présente sur le disque dur local au moment de l'exécution de la commande. La première actualisation stocke une copie sur le disque dur local, dans le chemin spécifié par le paramètre Fichier CRL. Le chemin d'accès par défaut pour le stockage de la CRL est /var/netscaler/ssl.

Paramètres d'actualisation CRL

- **Nom de la CRL**

  Le nom de la CRL en cours d'actualisation sur NetScaler Gateway.

- **Activer l'actualisation automatique des LCR**

  Activez ou désactivez l'actualisation automatique des LCR.

- **Certificat CA**

  Le certificat de l'autorité de certification qui a émis la CRL. Ce certificat d'autorité de certification doit être installé sur l'appliance. NetScaler ne peut mettre à jour les CRL qu'à partir des autorités de certification dont les certificats y sont installés.

- **Méthode**

  Protocole permettant d'obtenir l'actualisation de la liste de rétention de certificat à partir d'un serveur Web (HTTP) ou d'un serveur LDAP. Valeurs possibles : HTTP, LDAP. Par défaut : HTTP.

- **Étendue**

  L'étendue de l'opération de recherche sur le serveur LDAP. Si la portée spécifiée est Base, la recherche est au même niveau que le nom unique de base. Si la portée spécifiée est One, la recherche s'étend jusqu'à un niveau inférieur au DN de base.

- **Server IP**

  Adresse IP du serveur LDAP à partir duquel la CRL est récupérée. Sélectionnez IPv6 pour utiliser une adresse IP IPv6.

- **Port**

  Numéro de port sur lequel le serveur LDAP ou HTTP communique.

- **Adresse URL**

  URL de l'emplacement Web à partir duquel la CRL est récupérée.

- **DN de base**

  DN de base utilisé par le serveur LDAP pour rechercher l'attribut CRL.
  Remarque : Citrix recommande d'utiliser l'attribut DN de base au lieu du nom de l'émetteur du

certificat de l'autorité de certification pour rechercher la liste de rétention de certificats dans le serveur LDAP. Le champ Issuer-Name peut ne pas correspondre exactement au nom unique de la structure d'annuaire LDAP.

- **DN de liaison**

  L'attribut Bind DN est utilisé pour accéder à l'objet CRL dans le référentiel LDAP. Les attributs de nom unique de liaison sont les informations d'identification de l'administrateur du serveur LDAP. Configurez ce paramètre pour limiter l'accès non autorisé aux serveurs LDAP.

- **Mot de passe**

  Mot de passe administrateur utilisé pour accéder à l'objet CRL dans le référentiel LDAP. Un mot de passe est requis si l'accès au référentiel LDAP est restreint, c'est-à-dire que l'accès anonyme n'est pas autorisé.

- **Intervalle**

  Intervalle auquel l'actualisation de la LCR doit être effectuée. Pour une actualisation instantanée des LCR, spécifiez l'intervalle sur MAINTENANT. Valeurs possibles : MENSUEL, QUOTIDIEN, HEBDOMADAIRE, MAINTENANT, AUCUN.

- **Jours**

  Le jour où l'actualisation de la LCR doit être effectuée. Cette option n'est pas disponible si l'intervalle est défini sur QUOTIDIEN.

- **Heure**

  Heure exacte, au format 24 heures, à laquelle l'actualisation de la LCR doit être effectuée.

- **Binaire**

  Définissez le mode de récupération de la liste de révocation de révocation de révocation de révocation de révocation Valeurs possibles : OUI, NON. Par défaut : NON.

1. Dans le volet de navigation, développez SSL, puis cliquez sur CRL.
2. Sélectionnez la CRL configurée pour laquelle vous souhaitez mettre à jour les paramètres d'actualisation, puis cliquez sur Ouvrir.
3. Sélectionnez l'option Activer l'actualisation automatique des LCR.
4. Dans le groupe Paramètres d'actualisation automatique de la LCR, spécifiez les valeurs des paramètres suivants :
   Remarque : Un astérisque (*) indique un paramètre obligatoire.

   - Méthode
   - Binaire
   - Étendue
   - Server IP

- Port*
- Adresse URL
- DN de base*
- DN de liaison
- Mot de passe
- Intervalle
- Jours
- Heure

5. Cliquez sur Créer. Dans le volet CRL, sélectionnez la CRL que vous avez configurée et vérifiez que les paramètres qui apparaissent en bas de l'écran sont corrects.

Surveiller l'état des certificats avec OCSP

Le protocole OCSP (Online Certificate Status Protocol) est un protocole Internet utilisé pour déterminer l'état d'un certificat SSL client. NetScaler Gateway prend en charge l'OCSP tel que défini dans la RFC 2560. OCSP offre des avantages significatifs par rapport aux listes de révocation de certificats (CRL) en termes d'informations en temps opportun. Le statut de révocation à jour d'un certificat client est particulièrement utile dans les transactions impliquant des sommes d'argent importantes et des transactions boursières de grande valeur. Il utilise également moins de ressources système et réseau. L'implémentation d'OCSP par NetScaler Gateway inclut le traitement par lots des demandes et la mise en cache des réponses.

Implémentation d'OCSP par NetScaler Gateway

La validation OCSP sur une appliance NetScaler Gateway commence lorsque NetScaler Gateway reçoit un certificat client lors d'une liaison SSL. Pour valider le certificat, NetScaler Gateway crée une demande OCSP et la transmet au répondeur OCSP. Pour ce faire, NetScaler Gateway extrait l'URL du répondeur OCSP à partir du certificat client ou utilise une URL configurée localement. La transaction est suspendue jusqu'à ce que NetScaler Gateway évalue la réponse du serveur et détermine s'il faut autoriser la transaction ou la rejeter. Si la réponse du serveur est retardée au-delà de la durée configurée et qu'aucun autre répondeur n'est configuré, NetScaler Gateway autorise la transaction ou affiche une erreur, selon que vous avez défini le contrôle OCSP sur facultatif ou obligatoire. NetScaler Gateway prend en charge le traitement par lots des requêtes OCSP et la mise en cache des réponses OCSP afin de réduire la charge sur le répondeur OCSP et de fournir des réponses plus rapides.

traitement par lots de demandes OCSP

Chaque fois que NetScaler Gateway reçoit un certificat client, il envoie une demande au répondeur OCSP. Pour éviter de surcharger le répondeur OCSP, NetScaler Gateway peut demander l'état de

plusieurs certificats clients dans la même demande. Pour que le traitement par lots de demandes fonctionne efficacement, vous devez définir un délai d'expiration afin que le traitement d'un seul certificat ne soit pas retardé pendant l'attente de la formation d'un lot.

Mise en cache des réponses OCSP

La mise en cache des réponses reçues du répondeur OCSP permet de répondre plus rapidement à l'utilisateur et de réduire la charge sur le répondeur OCSP. Dès réception de l'état de révocation d'un certificat client de la part du répondeur OCSP, NetScaler Gateway met la réponse en cache localement pendant une durée prédéfinie. Lorsqu'un certificat client est reçu lors d'une connexion SSL, NetScaler Gateway vérifie d'abord dans son cache local une entrée pour ce certificat. Si une entrée est toujours valide (dans la limite du délai d'expiration du cache), elle est évaluée et le certificat client est accepté ou rejeté. Si aucun certificat n'est trouvé, NetScaler Gateway envoie une demande au répondeur OCSP et stocke la réponse dans son cache local pendant une durée configurée.

Configurer l'état du certificat OCSP

La configuration d'un protocole OCSP (Online Certificate Status Protocol) implique l'ajout d'un répondeur OCSP, la liaison du répondeur OCSP à un certificat signé d'une autorité de certification (CA) et la liaison du certificat et de la clé privée à un serveur virtuel SSL (Secure Sockets Layer). Si vous devez lier un certificat et une clé privée différents à un répondeur OCSP que vous avez déjà configuré, vous devez d'abord délier le répondeur, puis lier le répondeur à un autre certificat.

Pour configurer OCSP

1. Sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Répondeur OCSP.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom, saisissez le nom du profil.
4. Dans URL, tapez l'adresse Web du répondeur OCSP.

   Ce champ est obligatoire. L'adresse Web ne peut pas dépasser 32 caractères.
5. Pour mettre en cache les réponses OCSP, cliquez sur Cache et dans Time-out, tapez le nombre de minutes pendant lesquelles NetScaler Gateway conserve la réponse.
6. Sous Request Batching, cliquez sur Activer.
7. Dans la zone Délai de traitement par lots, spécifiez la durée, en millisecondes, autorisée pour le traitement par lots d'un groupe de demandes OCSP.

Les valeurs peuvent être comprises entre 0 et 10000. La valeur par défaut est 1.

8. Dans Produced At Time Skew, tapez le temps que NetScaler Gateway peut utiliser pendant lequel l'appliance doit vérifier ou accepter la réponse.
9. Sous Vérification des réponses, sélectionnez Réponses de confiance si vous souhaitez désactiver les vérifications de signature par le répondeur OCSP.

   Si vous activez les réponses d'approbation, ignorez les étapes 8 et 9.
10. Dans Certificat, sélectionnez le certificat utilisé pour signer les réponses OCSP.

    Si aucun certificat n'est sélectionné, l'autorité de certification à laquelle le répondeur OCSP est lié est utilisée pour vérifier les réponses.
11. Dans la zone Délai d'expiration de la demande, tapez le nombre de millisecondes d'attente d'une réponse OCSP.

    Cette durée inclut le délai de traitement par lots. Les valeurs peuvent être comprises entre 0 et 120000. La valeur par défaut est 2000.
12. Dans Signing Certificate, sélectionnez le certificat et la clé privée utilisés pour signer les demandes OCSP. Si vous ne spécifiez pas de certificat et de clé privée, les demandes ne sont pas signées.
13. Pour activer le numéro utilisé une fois, (`nonce`) `extension` sélectionnez Nonce.
14. Pour utiliser un certificat client, cliquez sur Insertion de certificat client.
15. Cliquez sur Create, puis cliquez sur Close.

Tester la configuration de NetScaler Gateway

March 27, 2024

Après avoir configuré les paramètres initiaux sur NetScaler Gateway, vous pouvez tester vos paramètres en vous connectant à l'appliance.

Pour tester les paramètres de NetScaler Gateway, créez un compte utilisateur local. Ensuite, à l'aide de l'adresse IP du serveur virtuel ou du nom de domaine complet (FQDN) de l'appliance, ouvrez un navigateur Web et saisissez l'adresse Web. Par exemple, dans la barre d'adresse, tapez `https://my.company.com` ou `https://192.168.96.183`.

Sur l'écran d'ouverture de session, saisissez le nom d'utilisateur et le mot de passe du compte utilisateur que vous avez créé précédemment. Une fois connecté, vous êtes invité à télécharger et à installer le client Citrix Secure Access.

Une fois que vous avez installé le client Citrix Secure Access puis que vous vous y êtes connecté, l'interface d'accès apparaît. L'interface d'accès est la page d'accueil par défaut de NetScaler Gateway.

Créer un compte utilisateur à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway \ > Administration des utilisateurs**, puis cliquez sur Utilisateurs **AAA**.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom d'utilisateur, tapez le nom d'utilisateur.
4. Si vous utilisez l'authentification locale, désactivez la case à cocher Authentification externe. L'authentification des utilisateurs avec des types d'authentification externes, tels que LDAP ou RADIUS, est la valeur par défaut. Si vous désactivez cette case à cocher, NetScaler Gateway authentifie les utilisateurs.
5. Dans Mot de passe et confirmation du mot de passe, tapez le mot de passe de l'utilisateur, cliquez sur Créer, puis sur Fermer.

Lorsque vous ajoutez des utilisateurs à l'aide de l'utilitaire de configuration, vous pouvez lier les stratégies suivantes à l'utilisateur :

- Authorization
- Trafic, session et audit
- Signets
- Applications Intranet
- Adresses IP Intranet

Si vous rencontrez des problèmes pour ouvrir une session avec le compte d'utilisateur de test, vérifiez les points suivants :

- Si vous recevez un avertissement de certificat, un certificat de test ou un certificat non valide est installé sur NetScaler Gateway. Si un certificat signé par une autorité de certification (CA) est installé sur l'appliance, assurez-vous qu'il existe un certificat racine correspondant sur la machine utilisateur.
- Si vous avez utilisé un certificat signé par une autorité de certification, vérifiez que vous avez correctement généré le certificat de site à l'aide de la demande de signature de certificat (CSR) signée et que les données de nom unique (DN) saisies dans la demande de signature de certificat sont exactes. Le problème peut également être dû au fait que le nom d'hôte ne correspond pas à l'adresse IP figurant sur le certificat signé. Vérifiez que le nom commun du certificat configuré correspond aux informations d'adresse IP du serveur virtuel configuré.
- Si l'écran d'ouverture de session n'apparaît pas ou si un autre message d'erreur s'affiche, passez en revue le processus de configuration et confirmez que vous avez effectué toutes les étapes correctement et que vous avez saisi tous les paramètres avec précision.

Mettre à niveau le logiciel NetScaler Gateway

March 27, 2024

Vous pouvez mettre à niveau le logiciel qui se trouve sur NetScaler Gateway lorsque de nouvelles versions sont disponibles. Vous pouvez rechercher des mises à jour sur le site Web de Citrix. Vous pouvez effectuer une mise à niveau vers une nouvelle version uniquement si vos licences NetScaler Gateway sont incluses dans le programme Subscription Advantage lorsque la mise à jour est publiée. Vous pouvez renouveler Subscription Advantage à tout moment. Pour plus d'informations, consultez le site Web de support de NetScaler.

Le chemin de mise à niveau et les informations sur les produits compatibles sont également disponibles dans le Guide de mise à niveau Citrix.

Pour plus d'informations sur la dernière version de maintenance de NetScaler Gateway, consultez le Centre de connaissances Citrix.

Rechercher les mises à jour logicielles

1. Accédez au site Web Citrix.
2. Cliquez sur **My Account (Se connecter)** et connectez-vous.
3. Cliquez sur **Téléchargements**.
4. Sous Rechercher des téléchargements, sélectionnez **NetScaler Gateway**.
5. Dans **Select Download Type (Sélectionnez téléchargement)**, sélectionnez **Product Software (Composants)**, puis cliquez sur **Find (Rechercher)**.
   Vous pouvez également sélectionner **Virtual Appliances** pour télécharger NetScaler VPX. Lorsque vous sélectionnez cette option, vous recevez une liste des logiciels pour la machine virtuelle pour chaque hyperviseur.
6. Sur la page NetScaler Gateway, développez **NetScaler Gateway ou Access Gateway**.
7. Cliquez sur la version du logiciel de l'appliance que vous souhaitez télécharger.
8. Sur la page du logiciel du dispositif correspondant à la version que vous souhaitez télécharger, sélectionnez le dispositif virtuel, puis cliquez sur **Télécharger**.
9. Suivez les instructions à l'écran pour télécharger le logiciel.

Lorsque le logiciel est téléchargé sur votre ordinateur, vous pouvez utiliser l'assistant de mise à niveau ou l'invite de commande pour installer le logiciel.

Mettez à niveau NetScaler Gateway à l'aide de l'assistant de mise à niveau

1. Dans l'utilitaire de configuration, sous l'**onglet Configuration**, dans le volet de navigation, cliquez sur Système.

2. Dans le volet d'informations, cliquez sur **Assistant de mise à niveau**.
3. Cliquez sur **Suivant**, puis suivez les instructions de l'assistant.

Mettez à niveau NetScaler Gateway à l'aide d'une invite de commande

1. Pour charger le logiciel sur NetScaler Gateway, utilisez un client FTP sécurisé, tel que WinSCP, pour vous connecter à l'appliance.
2. Copiez le logiciel depuis votre ordinateur vers le`nsinstall` répertoire /var/ de l'appliance.
3. Utilisez un client Secure Shell (SSH), tel que PuTTY, pour ouvrir une connexion SSH avec l'appliance.
4. Connectez-vous à NetScaler Gateway.
5. À l'invite de commande, tapez : `shell`
6. Pour accéder au `nsinstall` répertoire, à l'invite de commandes, tapez : `cd /var/nsinstall`
7. Pour afficher le contenu du répertoire, tapez : `ls`
8. Pour décompresser le logiciel, tapez : tar —xvzf build_x_xx.tgz, où BUILD_X_XX.tgz est le nom de la version vers laquelle vous souhaitez effectuer la mise à niveau.
9. Pour démarrer l'installation, à l'invite de commandes, tapez : `./installns`
10. Lorsque l'installation est terminée, redémarrez NetScaler Gateway.

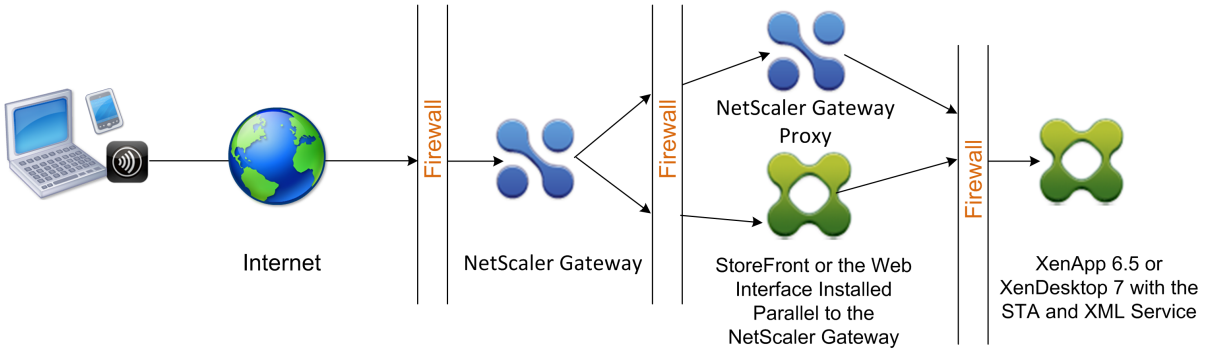
Après le redémarrage de NetScaler Gateway, lancez l'utilitaire de configuration pour vérifier la réussite de l'installation. La version de NetScaler Gateway qui se trouve sur l'appliance apparaît dans le coin supérieur droit.

Déployer NetScaler Gateway dans une zone démilitarisée à double saut

March 27, 2024

Certaines organisations utilisent trois pare-feu pour protéger leurs réseaux internes. Les trois pare-feu divisent la DMZ en deux phases afin d'offrir une couche supplémentaire de sécurité pour le réseau interne. Cette configuration réseau est appelée une DMZ double-hop.

Figure 1. Appliances NetScaler Gateway déployées dans une zone démilitarisée à double saut



> **Remarque :**
>
> À des fins d'illustration, l'exemple précédent décrit une configuration à double saut utilisant trois pare-feu avec StoreFront, l'Interface Web et Citrix Virtual Apps. Toutefois, vous pouvez également disposer d'une zone démilitarisée à double saut avec une appliance dans la zone démilitarisée et une appliance dans le réseau sécurisé. Si vous configurez une configuration à double saut avec une appliance dans la zone démilitarisée et une autre dans le réseau sécurisé, vous pouvez ignorer les instructions d'ouverture des ports sur le troisième pare-feu.

Vous pouvez configurer une zone démilitarisée à double saut pour prendre en charge Citrix StoreFront ou l'interface Web installée parallèlement au proxy NetScaler Gateway. Les utilisateurs se connectent à l'aide de l'application Citrix Workspace.

> **Remarque :**
>
> si vous déployez NetScaler Gateway dans une zone démilitarisée à double saut avec StoreFront, l'application AutoDiscovery pour Citrix Workspace basée sur le courrier électronique ne fonctionne pas.

Fonctionnement d'un déploiement à double saut

Vous pouvez déployer des appliances NetScaler Gateway dans une zone démilitarisée à double saut pour contrôler l'accès aux serveurs exécutant Citrix Virtual Apps. Les connexions dans un déploiement à double saut se déroulent comme suit :

- Les utilisateurs se connectent à NetScaler Gateway dans la première zone démilitarisée à l'aide d'un navigateur Web et de l'application Citrix Workspace pour sélectionner une application publiée.
- L'application Citrix Workspace démarre sur la machine utilisateur. L'utilisateur se connecte à NetScaler Gateway pour accéder à l'application publiée exécutée dans la batterie de serveurs du réseau sécurisé.

  Remarque : Secure Hub et le client Citrix Secure Access pour Windows ne sont pas pris en

charge dans un déploiement DMZ à double saut. Seule l'application Citrix Workspace est utilisée pour les connexions utilisateur.

- NetScaler Gateway situé dans la première zone démilitarisée gère les connexions des utilisateurs et exécute les fonctions de sécurité d'un VPN SSL. Ce NetScaler Gateway chiffre les connexions utilisateur, détermine la manière dont les utilisateurs sont authentifiés et contrôle l'accès aux serveurs du réseau interne.
- NetScaler Gateway situé dans la seconde zone démilitarisée sert de périphérique proxy NetScaler Gateway. Ce NetScaler Gateway permet au trafic ICA de traverser la deuxième zone démilitarisée pour terminer les connexions des utilisateurs au parc de serveurs. Les communications entre NetScaler Gateway dans la première DMZ et la Secure Ticket Authority (STA) dans le réseau interne sont également transmises par proxy via NetScaler Gateway dans la seconde DMZ.

NetScaler Gateway prend en charge les connexions IPv4 et IPv6. Vous pouvez utiliser l'utilitaire de configuration pour configurer l'adresse IPv6.

Le tableau suivant suggère la prise en charge du déploiement à double saut pour les différentes fonctionnalités ICA :

Fonctionnalité ICA	Prise en charge du double-hop
SmartAccess	Oui
SmartControl	Oui
Enlightened Data Transport (EDT)	Oui
HDX Insight	Oui
Fiabilité de session ICA (port 2598)	Oui
Migration de session ICA	Oui
Délai d'expiration de session ICA	Oui
ICA Multi-Stream	Oui (TCP uniquement)
Framehawk	Non
audio UDP	Non

Préparation à un déploiement DMZ à double saut

Lors de la configuration d'un déploiement DMZ à double saut, vous devez répondre aux questions suivantes :

- Voulez-vous prendre en charge l'équilibrage de charge ?

- Quels ports dois-je ouvrir sur les pare-feu ?
- De combien de certificats SSL ai-je besoin ?
- De quels composants ai-je besoin avant de commencer le déploiement ?

Les rubriques de cette section contiennent des informations qui vous aideront à répondre à ces questions en fonction de votre environnement.

Composants nécessaires au démarrage du déploiement

Avant de commencer un déploiement DMZ à double saut, vérifiez que vous disposez des composants suivants :

- Au minimum, deux appliances NetScaler Gateway doivent être disponibles (une pour chaque zone démilitarisée).
- Les serveurs exécutant Citrix Virtual Apps doivent être installés et opérationnels sur le réseau interne.
- L'interface Web ou StoreFront doit être installé dans la deuxième zone démilitarisée et configuré pour fonctionner avec la batterie de serveurs du réseau interne.
- Au minimum, un certificat de serveur SSL doit être installé sur NetScaler Gateway dans la première zone démilitarisée. Ce certificat garantit que les connexions du navigateur Web et des utilisateurs à NetScaler Gateway sont cryptées.

  Vous avez besoin de certificats supplémentaires si vous souhaitez chiffrer les connexions qui se produisent entre les autres composants d'un déploiement DMZ à double saut.

Flux de communication dans un déploiement DMZ à double saut

January 26, 2024

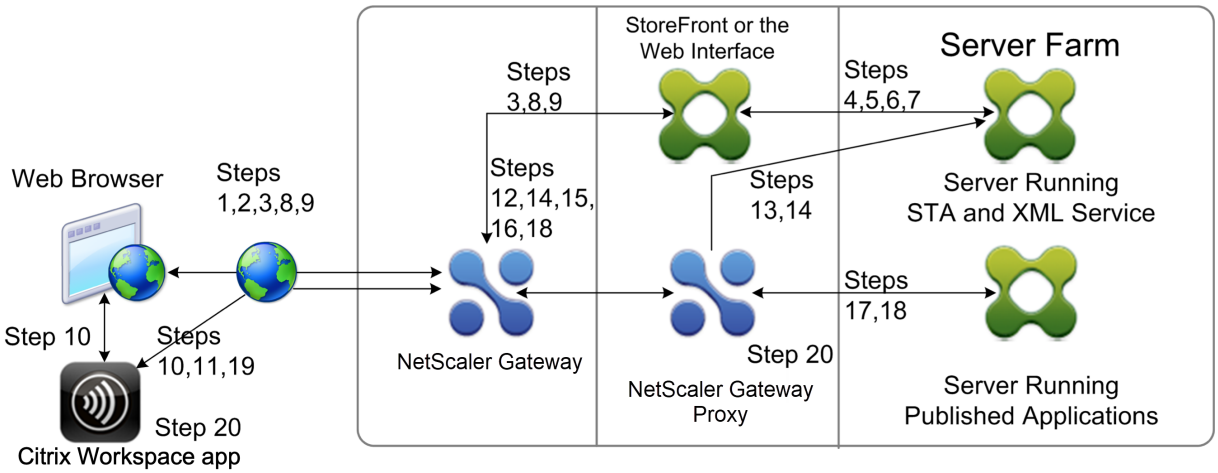
Pour comprendre les problèmes de configuration liés à un déploiement de DMZ à double saut, vous devez avoir une compréhension de base de la façon dont les différents composants NetScaler Gateway et Citrix Virtual Apps d'un déploiement DMZ à double saut communiquent pour prendre en charge une connexion utilisateur. Le processus de connexion de StoreFront et de l'interface Web est identique.

Bien que le processus de connexion utilisateur se déroule dans un flux continu, les étapes de haut niveau suivantes sont impliquées dans le processus.

- Authentification des utilisateurs
- Créer un ticket de session

- Démarrez l'application Citrix Workspace
- Terminez la connexion

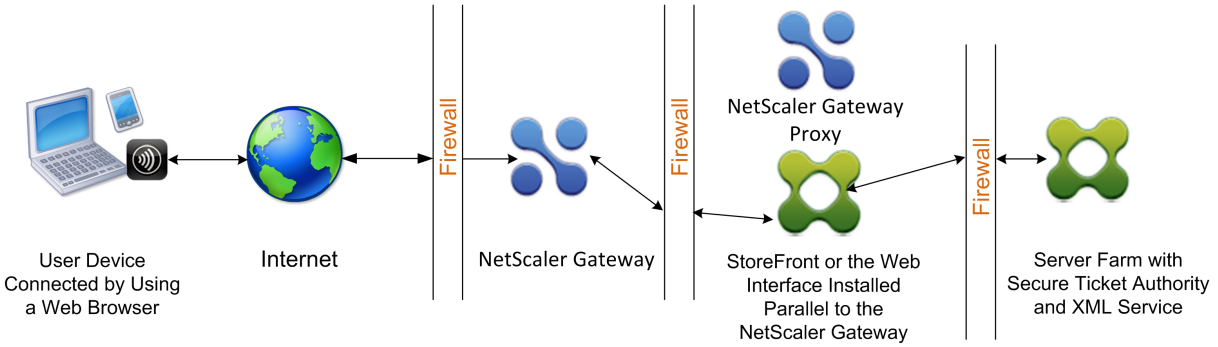
La figure suivante illustre les étapes du processus de connexion utilisateur à StoreFront ou à l'interface Web. Dans le réseau sécurisé, les ordinateurs exécutant Citrix Virtual Apps exécutent également la Secure Ticket Authority (STA), le service XML et les applications publiées.



Procédure de connexion

L'authentification des utilisateurs est la première étape du processus de connexion utilisateur dans un déploiement DMZ à double saut.

La figure suivante illustre le processus de connexion des utilisateurs dans ce déploiement.



Au cours de la phase d'authentification de l'utilisateur, le processus de base suivant se produit :

1. Un utilisateur saisit l'adresse de NetScaler Gateway, par exemple https://www.ng.wxyco.com dans un navigateur Web pour se connecter à NetScaler Gateway dans la première zone démilitarisée. Si vous avez activé l'authentification par page de connexion sur NetScaler Gateway, NetScaler Gateway authentifie l'utilisateur.
2. NetScaler Gateway situé dans la première zone démilitarisée reçoit la demande.

3. NetScaler Gateway redirige la connexion du navigateur Web vers l'interface Web.
4. L'interface Web envoie les informations d'identification de l'utilisateur au service Citrix XML exécuté dans la batterie de serveurs du réseau interne.
5. Le service XML Citrix authentifie l'utilisateur.
6. Le service XML crée une liste des applications publiées auxquelles l'utilisateur est autorisé à accéder et envoie cette liste à l'interface Web.

   Remarque :

   - Si vous activez l'authentification sur NetScaler Gateway, l'appliance envoie la page d'ouverture de session de NetScaler Gateway à l'utilisateur. L'utilisateur entre les informations d'identification d'authentification sur la page d'ouverture de session et l'appliance authentifie l'utilisateur. NetScaler Gateway renvoie ensuite les informations d'identification de l'utilisateur à l'interface Web.
   - Si vous n'activez pas l'authentification, NetScaler Gateway n'effectue pas d'authentification. L'appliance se connecte à l'interface Web, récupère la page d'ouverture de session de l'interface Web et envoie la page d'ouverture de session de l'interface Web à l'utilisateur. L'utilisateur saisit les informations d'authentification sur la page d'ouverture de session de l'interface Web et NetScaler Gateway transmet les informations d'identification de l'utilisateur à l'interface Web.

   La création du ticket de session est la deuxième étape du processus de connexion utilisateur dans un déploiement DMZ à double saut.

   Au cours de l'étape de création du ticket de session, le processus de base suivant se produit :

7. L'interface Web communique à la fois avec le service XML et la Secure Ticket Authority (STA) du réseau interne pour produire des tickets de session pour chacune des applications publiées auxquelles l'utilisateur est autorisé à accéder. Le ticket de session contient une adresse d'alias pour l'ordinateur exécutant Citrix Virtual Apps qui héberge une application publiée.
8. La STA enregistre les adresses IP des serveurs qui hébergent les applications publiées. La STA envoie ensuite les tickets de session demandés à l'interface Web. Chaque ticket de session inclut un alias qui représente l'adresse IP du serveur qui héberge l'application publiée, mais pas l'adresse IP réelle.
9. L'interface Web génère un fichier ICA pour chacune des applications publiées. Le fichier ICA contient le ticket émis par la STA. L'interface Web crée et remplit ensuite une page Web avec une liste de liens vers les applications publiées et envoie cette page Web au navigateur Web de la machine utilisateur.

   Le démarrage de l'application Citrix Workspace est la troisième étape du processus de connexion utilisateur dans un déploiement DMZ à double saut. Le processus de base est le suivant :

10. L'utilisateur clique sur un lien vers une application publiée dans l'interface Web. L'interface Web envoie le fichier ICA de cette application publiée au navigateur de la machine utilisateur.

    Le fichier ICA contient des données qui indiquent au navigateur Web de démarrer Receiver.

    Le fichier ICA contient également le nom de domaine complet (FQDN) ou le nom du système de noms de domaine (DNS) de NetScaler Gateway dans la première zone démilitarisée.

11. Le navigateur Web démarre Receiver et l'utilisateur se connecte à NetScaler Gateway dans la première zone démilitarisée en utilisant le nom de NetScaler Gateway dans le fichier ICA. La première connexion SSL/TLS a lieu pour établir l'identité du serveur exécutant NetScaler Gateway.

    L'achèvement de la connexion est la quatrième et dernière étape du processus de connexion utilisateur dans un déploiement DMZ à double saut.

    Au cours de l'étape d'achèvement de la connexion, le processus de base suivant se produit :

    - L'utilisateur clique sur un lien vers une application publiée dans l'interface Web.
    - Le navigateur Web reçoit le fichier ICA généré par l'interface Web et démarre l'application Citrix Workspace.
      Remarque : Le fichier ICA contient du code qui indique au navigateur Web de démarrer l'application Citrix Workspace.
    - L'application Citrix Workspace initie une connexion ICA à NetScaler Gateway dans la première zone démilitarisée.
    - NetScaler Gateway situé dans la première zone démilitarisée communique avec la Secure Ticket Authority (STA) du réseau interne pour convertir l'adresse alias du ticket de session en l'adresse IP réelle d'un ordinateur exécutant Citrix Virtual Apps ou StoreFront. Cette communication est transmise par proxy via la seconde zone démilitarisée par le proxy NetScaler Gateway.
    - NetScaler Gateway situé dans la première zone démilitarisée complète la connexion ICA à l'application Citrix Workspace.
    - L'application Citrix Workspace peut désormais communiquer via les deux appliances NetScaler Gateway avec l'ordinateur exécutant Citrix Virtual Apps sur le réseau interne.

    Les étapes détaillées pour terminer le processus de connexion utilisateur sont les suivantes :

12. L'application Citrix Workspace envoie le ticket STA pour l'application publiée à NetScaler Gateway dans la première zone démilitarisée.

13. Dans la première zone démilitarisée, NetScaler Gateway contacte la STA du réseau interne pour la validation des tickets. Pour contacter la STA, NetScaler Gateway établit une connexion SOCKS ou SOCKS avec SSL avec le proxy NetScaler Gateway dans la deuxième zone démilitarisée.

14. Le proxy NetScaler Gateway situé dans la deuxième zone démilitarisée transmet la demande de validation du ticket à la STA du réseau interne. La STA valide le ticket et le mappe sur l'ordinateur

exécutant Citrix Virtual Apps qui héberge l'application publiée.

15. La STA envoie une réponse au proxy NetScaler Gateway dans la seconde DMZ, qui est transmise à NetScaler Gateway dans la première DMZ. Cette réponse termine la validation du ticket et inclut l'adresse IP de l'ordinateur qui héberge l'application publiée.
16. NetScaler Gateway dans la première DMZ intègre l'adresse du serveur Citrix Virtual Apps dans le paquet de connexion utilisateur et envoie ce paquet au proxy NetScaler Gateway dans la seconde DMZ.
17. Le proxy NetScaler Gateway situé dans la deuxième zone démilitarisée envoie une demande de connexion au serveur spécifié dans le paquet de connexion.
18. Le serveur répond au proxy NetScaler Gateway dans la seconde zone démilitarisée. Le proxy NetScaler Gateway situé dans la deuxième zone démilitarisée transmet cette réponse à NetScaler Gateway dans la première zone démilitarisée afin d'établir la connexion entre le serveur et NetScaler Gateway dans la première zone démilitarisée.
19. NetScaler Gateway situé dans la première zone démilitarisée conclut l'établissement de liens SSL/TLS avec la machine utilisateur en transmettant le paquet de connexion final à la machine utilisateur. La connexion entre la machine utilisateur et le serveur est établie.
20. Le trafic ICA circule entre la machine utilisateur et le serveur via NetScaler Gateway dans la première DMZ et le proxy NetScaler Gateway dans la seconde DMZ.

Installation et configuration de NetScaler Gateway dans une zone démilitarisée à double saut

March 27, 2024

Vous devez effectuer plusieurs étapes pour déployer NetScaler Gateway dans une zone démilitarisée à double saut. Les étapes comprennent l'installation des appliances dans les deux zones démilitarisées et la configuration des appliances pour les connexions des machines utilisateur.

Installation de NetScaler Gateway dans la première zone démilitarisée

Pour installer NetScaler Gateway dans la première zone démilitarisée, suivez les instructions de la section Installerle matériel.

Si vous installez plusieurs appliances NetScaler Gateway dans la première zone démilitarisée, vous pouvez les déployer derrière un équilibreur de charge.

Configurer NetScaler Gateway dans la première zone démilitarisée

Dans un déploiement de zone démilitarisée à double saut, il est obligatoire de configurer chaque NetScaler Gateway dans la première zone démilitarisée pour rediriger les connexions vers StoreFront ou l'interface Web de la seconde zone démilitarisée.

La redirection vers StoreFront ou l'interface Web s'effectue au niveau du serveur global ou virtuel de NetScaler Gateway. Pour se connecter à l'interface Web via NetScaler Gateway, un utilisateur doit être associé à un groupe d'utilisateurs NetScaler Gateway pour lequel la redirection vers l'interface Web est activée.

Installation de NetScaler Gateway dans la deuxième zone démilitarisée

L'appliance NetScaler Gateway située dans la deuxième zone démilitarisée est appelée proxy NetScaler Gateway car elle transmet le trafic ICA et Secure Ticket Authority (STA) via la seconde zone démilitarisée.
Installez le matériel nécessaire pour installer chaque appliance NetScaler Gateway dans la seconde zone démilitarisée.

Vous pouvez utiliser cette procédure d'installation pour installer d'autres appliances dans la deuxième zone démilitarisée.

Après avoir installé les appliances NetScaler Gateway dans la deuxième zone démilitarisée, vous configurez les paramètres suivants :

- Configurer un serveur virtuel sur le proxy NetScaler Gateway.
- Configurer des appliances NetScaler Gateway dans la première et deuxième DMZ pour qu'elles puissent communiquer entre elles.
- Associer le NetScaler Gateway dans la seconde DMZ globalement ou à un serveur virtuel.
- Configurer la STA sur l'appliance dans la première DMZ.
- Ouvrir des ports dans les pare-feu séparant la DMZ.
- Installer des certificats sur les appliances.

Configurer les paramètres sur les serveurs virtuels du proxy NetScaler Gateway

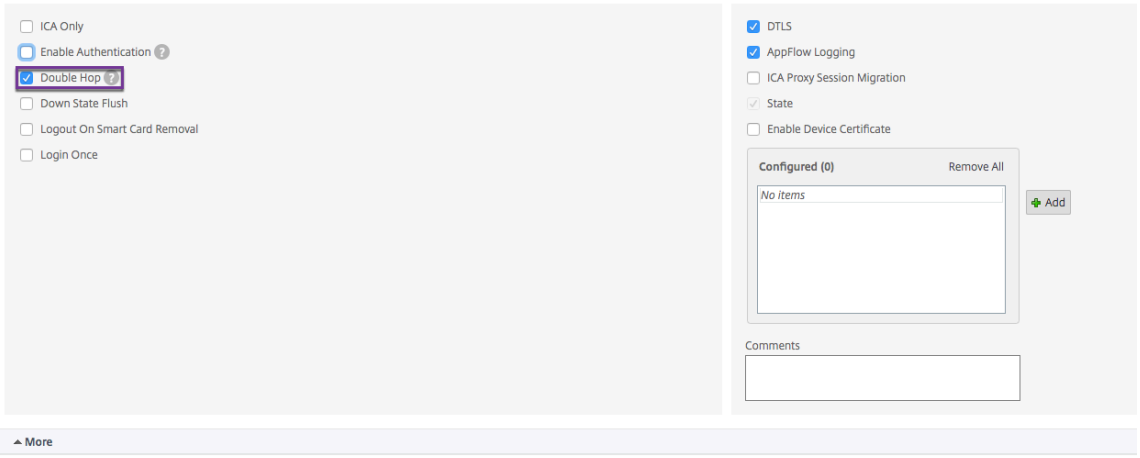
January 26, 2024

Pour autoriser le transfert des connexions entre les appliances NetScaler Gateway, vous activez le double saut dans le serveur virtuel sur le proxy NetScaler Gateway.

Lorsque les utilisateurs se connectent, l'appliance NetScaler Gateway authentifie les utilisateurs, puis transmet la connexion à l'appliance proxy. Sur NetScaler Gateway dans la première zone démilitarisée, configurez le serveur virtuel pour qu'il communique avec NetScaler Gateway dans la deuxième zone démilitarisée. Ne configurez pas l'authentification ou les stratégies sur le proxy NetScaler Gateway. Citrix recommande de désactiver l'authentification sur le serveur virtuel.

Pour activer le double saut sur le serveur virtuel sur le proxy NetScaler Gateway à l'aide de l'interface graphique

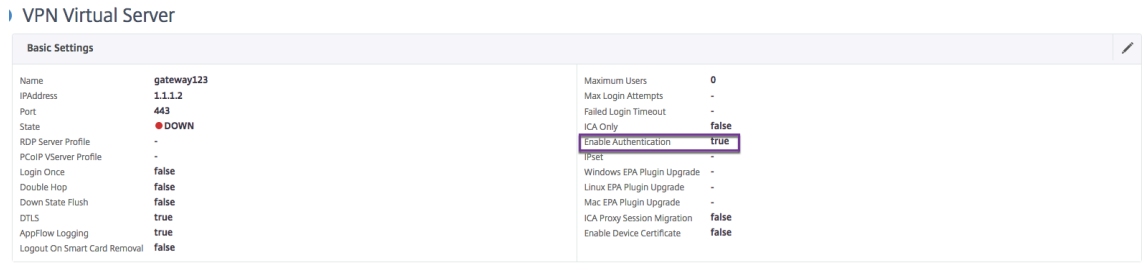
1. Accédez à **Configuration > NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône Modifier, puis sur **Plus**.
4. Sélectionnez **Double Hop**.



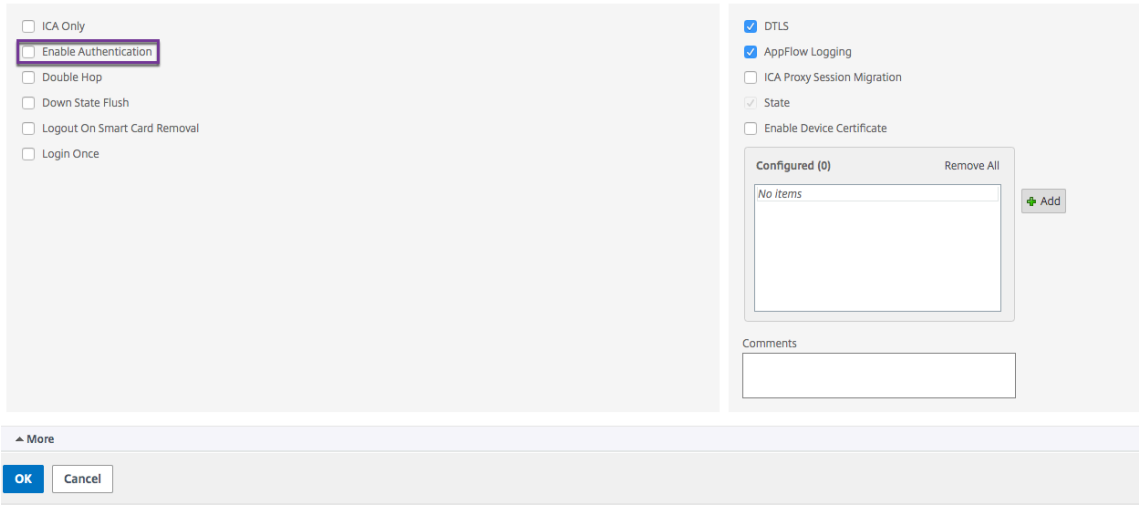
5. Cliquez sur **OK**.

Pour désactiver l'authentification sur le serveur virtuel sur le proxy NetScaler Gateway à l'aide de l'interface graphique

1. Accédez à **Configuration > NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.
3. Dans la section **Paramètres de base**, cliquez sur l'icône Modifier, puis sur **Plus**.



4. Désactivez la case à cocher **Activer l'authentification**.



5. Cliquez sur **OK**.

Configurer l'appliance pour qu'elle communique avec le proxy de l'appliance

January 26, 2024

Lorsque vous déployez NetScaler Gateway dans une zone démilitarisée à double saut, vous devez configurer NetScaler Gateway dans la première zone démilitarisée pour communiquer avec le proxy NetScaler Gateway dans la seconde zone démilitarisée.

Si vous déployez plusieurs appliances dans la deuxième zone démilitarisée, vous configurez chaque appliance de la première zone démilitarisée pour communiquer avec chaque appliance proxy de la seconde zone démilitarisée.

Remarque : Si vous souhaitez utiliser IPv6, vous configurez le serveur de saut suivant à l'aide de l'utilitaire de configuration. Pour ce faire, ouvrez
NetScaler Gateway > Ressources, puis cliquez sur

Next Hop Servers. Suivez les étapes de la procédure suivante, puis activez la case à cocher IPv6.

Pour configurer NetScaler Gateway afin qu'il communique avec le proxy NetScaler Gateway

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez NetScaler Gateway > Resources, puis cliquez sur Next Hop Servers.
2. Dans le volet d'informations, cliquez sur Ajouter.
3. Dans Nom, tapez le nom du premier NetScaler Gateway.
4. Dans Adresse IP, tapez l'adresse IP du serveur virtuel du proxy NetScaler Gateway dans la seconde zone démilitarisée.
5. Dans Port, tapez le numéro de port, cliquez sur Créer, puis sur Fermer. Si vous utilisez un port sécurisé, tel que 443, sélectionnez Sécurisé.

Vous devez configurer chaque NetScaler Gateway installé dans la première zone démilitarisée pour communiquer avec tous les dispositifs proxy NetScaler Gateway installés dans la seconde zone démilitarisée.

Après avoir configuré les paramètres du proxy NetScaler Gateway, liez la stratégie aux serveurs Next Hop dans NetScaler Gateway Global ou à un serveur virtuel.

Pour lier le serveur Next Hop de NetScaler Gateway de manière globale

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez NetScaler Gateway > Resources, puis cliquez sur Next Hop Servers.
2. Dans le volet d'informations, sélectionnez un serveur de saut suivant, puis dans Action, sélectionnez Liaisons globales.
3. Dans la boîte de dialogue Configurer la liaison globale du serveur de saut suivant, dans Nom du serveur de saut suivant, sélectionnez l'appliance proxy, puis cliquez sur OK.

Pour lier le serveur Next Hop de NetScaler Gateway à un serveur virtuel

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur Ouvrir.
3. Dans l'onglet Applications publiées, sous Serveurs de saut suivant, cliquez sur un élément, puis sur OK.

Vous pouvez également ajouter un serveur de saut suivant à partir de l'onglet Applications publiées.

Configurer NetScaler Gateway pour gérer le trafic STA et ICA

March 27, 2024

Lorsque vous déployez NetScaler Gateway dans une zone démilitarisée à double saut, vous devez configurer NetScaler Gateway dans la première zone démilitarisée pour gérer correctement les communications avec la Secure Ticket Authority (STA) et le trafic ICA. Le serveur exécutant la STA peut être lié globalement ou à un serveur virtuel.

Après avoir configuré la STA, vous pouvez la lier globalement ou à un serveur virtuel.

Pour configurer et lier la STA globalement :

1. Dans l'interface graphique, sous l'onglet Configuration, développez **NetScaler Gateway**, puis cliquez sur **Paramètres globaux**.
2. Dans le volet d'informations, sous **Serveurs,** cliquez sur Lind**/Unbind STA Servers à utiliser par la Secure Ticket Authority**.
3. **Dans la boîte de dialogue**Lier/dissocier les serveurs STA**, cliquez sur Ajouter.**
4. Dans la boîte de dialogue **Configurer le serveur STA**, dans **URL**, tapez le chemin d'accès au serveur exécutant le STA, par exemple http://mycompany.com ou, http://ipAddress puis cliquez sur **Créer**.

Pour configurer et lier la STA à un serveur virtuel, procédez comme suit :

1. Dans l'interface graphique, sous l'onglet Configuration, développez **NetScaler Gateway**, puis cliquez sur **Serveurs virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet **Applications publiées**, sous **Secure Ticket Authority**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Configurer le serveur STA**, dans URL, tapez le chemin d'accès au serveur exécutant le STA, par exemple ouhttp://mycompany.comhttp://ipAddress, puis cliquez sur **Créer**.

Remarque :

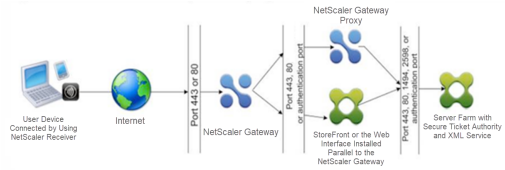
Si les serveurs virtuels VPN partagent le même serveur virtuel de saut suivant et les mêmes serveurs STA, la connexion est réinitialisée lorsque le serveur STA commun est indépendant d'un serveur virtuel qui partage le même serveur virtuel de saut suivant.

Ouvrir les ports appropriés sur les pare-feu

January 26, 2024

Vous devez vous assurer que les ports appropriés sont ouverts sur les pare-feu pour prendre en charge les différentes connexions qui se produisent entre les différents composants impliqués dans un déploiement DMZ à double saut. Pour plus d'informations sur le processus de connexion, consultez Flux de communication dans un déploiement DMZ à double saut.

La figure suivante montre les ports courants pouvant être utilisés dans un déploiement DMZ à double saut.



Le tableau suivant présente les connexions effectuées via le premier pare-feu et les ports qui doivent être ouverts pour prendre en charge les connexions.

Connexions via le premier pare-feu	Ports utilisés
Le navigateur Web d'Internet se connecte à NetScaler Gateway dans la première zone démilitarisée. **Remarque :** NetScaler Gateway inclut une option permettant de rediriger les connexions établies sur le port 80 vers un port sécurisé. Si vous activez cette option sur NetScaler Gateway, vous pouvez ouvrir le port 80 via le premier pare-feu. Lorsqu'un utilisateur établit une connexion non cryptée à NetScaler Gateway sur le port 80, NetScaler Gateway redirige automatiquement la connexion vers un port sécurisé.	Ouvrez le port TCP 443 via le premier pare-feu.
L'application Citrix Workspace depuis Internet se connecte à NetScaler Gateway dans la première zone démilitarisée.	Ouvrez le port TCP 443 via le premier pare-feu.

Le tableau suivant présente les connexions effectuées via le deuxième pare-feu et les ports qui doivent être ouverts pour prendre en charge les connexions.

Connexions via le deuxième pare-feu	Ports utilisés
NetScaler Gateway de la première zone démilitarisée se connecte à l'interface Web de la deuxième zone démilitarisée.	Ouvrez le port TCP 80 pour une connexion non sécurisée ou le port TCP 443 pour une connexion sécurisée via le deuxième pare-feu.
NetScaler Gateway de la première zone démilitarisée se connecte à NetScaler Gateway de la deuxième zone démilitarisée.	Ouvrez le port TCP 443 pour une connexion SOCKS sécurisée via le deuxième pare-feu.
Si vous avez activé l'authentification sur NetScaler Gateway dans la première zone démilitarisée, cette appliance devra peut-être se connecter à un serveur d'authentification du réseau interne.	Ouvrez le port TCP sur lequel le serveur d'authentification écoute les connexions. Par exemple, le port 1812 pour RADIUS et le port 389 pour LDAP.

Le tableau suivant présente les connexions effectuées via le troisième pare-feu et les ports qui doivent être ouverts pour prendre en charge les connexions.

Connexions via le troisième pare-feu	Ports utilisés
StoreFront ou l'interface Web de la deuxième zone démilitarisée se connecte au service XML hébergé sur un serveur du réseau interne.	Ouvrez le port 80 pour une connexion non sécurisée ou le port 443 pour une connexion sécurisée via le troisième pare-feu.
StoreFront ou l'interface Web de la deuxième zone démilitarisée se connecte à la Secure Ticket Authority (STA) hébergée sur un serveur du réseau interne.	Ouvrez le port 80 pour une connexion non sécurisée ou le port 443 pour une connexion sécurisée via le troisième pare-feu.
Dans la deuxième zone démilitarisée, NetScaler Gateway se connecte à la STA résidant dans le réseau sécurisé.	Ouvrez le port 80 pour une connexion non sécurisée ou le port 443 pour une connexion sécurisée via le troisième pare-feu.
NetScaler Gateway situé dans la deuxième zone démilitarisée établit une connexion ICA à une application publiée ou à un bureau virtuel sur un serveur du réseau interne.	Ouvrez le port TCP 1494 pour prendre en charge les connexions ICA via le troisième pare-feu. Si vous avez activé la fiabilité de session sur Citrix Virtual Apps, ouvrez le port TCP 2598 au lieu de 1494.
Si vous avez activé l'authentification sur NetScaler Gateway dans la première zone démilitarisée, cette appliance devra peut-être se connecter à un serveur d'authentification du réseau interne.	Ouvrez le port TCP sur lequel le serveur d'authentification écoute les connexions. Par exemple, le port 1812 pour RADIUS et le port 389 pour LDAP.

Maintenance et surveillance du système

January 26, 2024

Une fois que vous avez terminé la configuration de votre NetScaler Gateway, vous devez gérer et surveiller l'appliance. Vous pouvez le faire de l'une des manières suivantes :

- Vous pouvez mettre à niveau NetScaler Gateway vers la dernière version du logiciel. Lorsque vous vous connectez au site Web de Citrix, vous pouvez accéder au site de téléchargement de NetScaler Gateway et télécharger le logiciel. Vous trouverez le fichier Lisez-moi pour les versions de maintenance dans le centre de connaissances Citrix.
- Vous pouvez attribuer des tâches de configuration et de gestion de NetScaler Gateway à différents membres de votre groupe. Grâce à l'administration déléguée, vous pouvez attribuer des niveaux d'accès à des personnes qui les limitent à l'exécution de tâches spécifiques sur NetScaler Gateway.
- Vous pouvez enregistrer la configuration de NetScaler Gateway sur l'appliance ou dans un fichier sur votre ordinateur. Vous pouvez comparer la configuration en cours d'exécution et la configuration enregistrée. Vous pouvez également effacer la configuration depuis NetScaler Gateway.
- Vous pouvez afficher, actualiser et mettre à jour les sessions des utilisateurs finaux dans l'utilitaire de configuration de NetScaler Gateway.
- Vous pouvez configurer la journalisation sur NetScaler Gateway. Les journaux fournissent des informations importantes sur l'appliance et sont utiles en cas de problème.

Configuration des administrateurs délégués

January 26, 2024

NetScaler Gateway possède un nom d'utilisateur et un mot de passe d'administrateur par défaut. Le nom d'utilisateur et le mot de passe par défaut sont `nsroot`. Lorsque vous exécutez l'Assistant d'installation pour la première fois, vous pouvez modifier le mot de passe administrateur.

Vous pouvez créer d'autres comptes d'administrateur et attribuer à chaque compte différents niveaux d'accès à NetScaler Gateway. Ces comptes supplémentaires sont appelés administrateurs délégués. Par exemple, une personne est chargée de surveiller les connexions et les journaux de NetScaler Gateway et une autre personne est chargée de configurer des paramètres spécifiques sur NetScaler Gateway. Le premier administrateur dispose d'un accès en lecture seule et le deuxième administrateur dispose d'un accès limité à l'appliance.

Pour configurer un administrateur délégué, vous utilisez des stratégies de commande et des utilisateurs et groupes système.

Lorsque vous configurez un administrateur délégué, le processus de configuration est le suivant :

- Ajoutez un utilisateur système. Un utilisateur système est un administrateur doté de privilèges spécifiés. Tous les administrateurs héritent des stratégies des groupes auxquels ils appartiennent.
- Ajoutez un groupe de systèmes. Un groupe de systèmes contient des utilisateurs système dotés de privilèges spécifiques. Les membres du groupe système héritent des stratégies du ou des groupes auxquels ils appartiennent.
- Créez une stratégie de commande. Les stratégies de commande vous permettent de définir les parties de la configuration de NetScaler Gateway auxquelles un utilisateur ou un groupe est autorisé à accéder et à modifier. Vous pouvez également définir les commandes, telles que les groupes de commandes, les serveurs virtuels et les autres éléments que les administrateurs et les groupes sont autorisés à configurer.
- Liez la stratégie de commande à l'utilisateur ou au groupe en définissant la priorité. Lorsque vous configurez l'administration déléguée, attribuez des priorités à l'administrateur ou au groupe afin que NetScaler Gateway puisse déterminer quelle stratégie est prioritaire.

NetScaler Gateway dispose d'une stratégie de commande du système de refus par défaut. Les stratégies de commande ne peuvent pas être liées globalement. Liez les stratégies directement aux administrateurs système (utilisateurs) ou aux groupes. Si les utilisateurs et les groupes ne disposent pas d'une stratégie de commande associée, la stratégie de refus par défaut est appliquée et les utilisateurs ne peuvent exécuter aucune commande ni configurer NetScaler Gateway.

Vous pouvez configurer des stratégies de commande personnalisées pour définir un niveau de détail plus élevé pour les attributions de droits utilisateur. Par exemple, vous pouvez autoriser une personne à ajouter des stratégies de session à NetScaler Gateway, mais ne pas autoriser l'utilisateur à effectuer une autre configuration.

Configuration des stratégies de commande pour les administrateurs délégués

January 26, 2024

NetScaler Gateway possède quatre stratégies de commande intégrées que vous pouvez utiliser pour l'administration déléguée :

- La**lecture seule** permet un accès en lecture seule pour afficher toutes les commandes, à l'exception du groupe de commandes système et `ns.conf show` des commandes.

- **L'opérateur autorise l'** accès en lecture seule et permet également d'activer et de désactiver les commandes sur les services. Cette stratégie permet également d'accéder aux services et serveurs définis comme « accès hors service ».
- **Le réseau** permet un accès presque complet au système, à l'exclusion des commandes système et de la commande shell.
- **Le superutilisateur** accorde des privilèges système complets, tels que les privilèges accordés à l'administrateur par défaut `nsroot`.

Les stratégies de commande contiennent des expressions intégrées. Utilisez l'utilitaire de configuration pour créer des utilisateurs système, des groupes système, des stratégies de commande et pour définir des autorisations.

Pour créer un utilisateur administratif sur NetScaler Gateway

1. Dans l'utilitaire de configuration, dans le volet de navigation, sous l'onglet **Configuration**, développez **Système** > **Administration des utilisateurs**, puis cliquez sur **Utilisateurs système**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom d'utilisateur**, saisissez un nom d'utilisateur.
4. Dans les champs **Mot de passe** et **Confirmer le mot** de passe, entrez le mot de passe
5. Pour ajouter des utilisateurs à un groupe, dans **Membre de**, cliquez sur **Ajouter**.
6. Dans **Disponible**, sélectionnez un groupe, puis cliquez sur la flèche droite.
7. Cliquez sur **Stratégies de commande > Action > Insérer**.
8. Dans la boîte de dialogue Insérer des stratégies de commande, sélectionnez la commande, cliquez sur **OK > Créer > Fermer**.

Création de groupes d'administration

Les groupes d'administration contiennent des utilisateurs disposant de privilèges d'administration sur NetScaler Gateway. Vous pouvez créer des groupes d'administration dans l'utilitaire de configuration.

Pour configurer un groupe d'administration à l'aide de l'utilitaire de configuration

1. Dans l'utilitaire de configuration, dans le volet de navigation, sous l'onglet **Configuration**, développez **Système** > **Administration des utilisateurs**, puis cliquez sur **Groupes système**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom du groupe**, saisissez un nom pour le groupe.
4. Pour ajouter un utilisateur existant au groupe, dans **Membres**, cliquez sur **Ajouter**.

5. Sous **Disponible**, sélectionnez un utilisateur, puis cliquez sur la flèche droite.
6. Sous **Stratégies de commande**, dans **Action**, cliquez sur **Insérer**, sélectionnez une ou plusieurs stratégies, cliquez sur **OK**, cliquez sur **Créer**, puis cliquez sur **Fermer**.

Configuration des stratégies de commande personnalisées pour les administrateurs délégués

March 27, 2024

Lorsque vous configurez une stratégie de commande personnalisée, vous fournissez un nom de stratégie, puis configurez les composants de stratégie pour créer la spécification de commande. Avec la spécification de commande, vous pouvez limiter les commandes que les administrateurs sont autorisés à utiliser. Par exemple, vous souhaitez refuser aux administrateurs la possibilité d'utiliser la commande de suppression. Lors de la configuration de la stratégie, définissez l'action sur Refuser, puis configurez les paramètres.

Vous pouvez configurer une stratégie de commande simple ou avancée. Lorsque vous configurez une stratégie simple, vous configurez un composant sur l'appliance, tel que NetScaler Gateway et l'authentification. Lorsque vous configurez une stratégie avancée, vous sélectionnez le composant, appelé groupe d'entités, puis sélectionnez les commandes que les administrateurs sont autorisés à exécuter dans le groupe.

Pour créer une stratégie de commande personnalisée simple

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez **Système** > **Administration des utilisateurs**, puis cliquez sur **Stratégies de commande.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**
3. Dans **Nom de la stratégie**, tapez le nom de la stratégie.
4. Dans **Action**, sélectionnez **Autoriser** ou **Refuser**.
5. Sous **Spécification de commande**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter une commande**, sous l'onglet **Simple**, dans Opération, sélectionnez l'action que les administrateurs délégués peuvent effectuer.
7. Sous **Groupe d'entités**, sélectionnez un ou plusieurs groupes.

   Vous pouvez appuyer sur la touche CTRL pour sélectionner plusieurs groupes.
8. Cliquez sur **Create**, puis cliquez sur **Close**.

Pour créer une stratégie de commande personnalisée avancée

1. Dans l'utilitaire de configuration, dans le volet de navigation, sous l'onglet **Configuration**, développez **Système** > **Administration des utilisateurs**, puis cliquez sur **Stratégies de commande**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom de la stratégie**, tapez le nom de la stratégie.
4. Dans **Action**, sélectionnez **Autoriser** ou **Refuser**.
5. Sous **Spécification de commande**, cliquez sur **Ajouter**.
6. Dans la boîte de dialogue **Ajouter une commande**, cliquez sur l'onglet **Avancé**.
7. Dans **Groupe d'entités**, sélectionnez le groupe auquel la commande appartient, comme l'authentification ou la haute disponibilité.
8. Sous **Entité**, sélectionnez la stratégie.

   Vous pouvez appuyer sur la touche CTRL pour sélectionner plusieurs éléments dans la liste.
9. Dans **Opération**, sélectionnez la commande, cliquez sur **Créer,** puis sur **Fermer**.

   Vous pouvez appuyer sur la touche CTRL pour sélectionner plusieurs éléments dans la liste.
10. Cliquez sur **Créer,** puis sur **Fermer**.
11. Dans la boîte de dialogue **Créer une stratégie de commande**, cliquez sur **Créer,** puis sur **Fermer**.

Lorsque vous cliquez sur **Créer**, l'expression apparaît sous Spécification de commande dans la boîte de dialogue **Créer une politique de commande** .

Après avoir créé la stratégie de commande personnalisée, vous pouvez la lier à un utilisateur ou à un groupe.

> **Remarque :** Vous ne pouvez lier des stratégies de commande personnalisées qu'aux utilisateurs ou aux groupes que vous créez. Vous ne pouvez pas lier une stratégie de commande personnalisée à l'utilisateur `nsroot`.

Pour lier une stratégie de commande personnalisée à un utilisateur ou à un groupe

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez **Système** > **Administration** des **utilisateurs, puis cliquez sur Utilisateurs système** ou sur **Groupes de systèmes**.
2. Dans le volet d'informations, sélectionnez un utilisateur ou un groupe dans la liste, puis cliquez sur **Ouvrir**.

3. Sous **Stratégies de commande**, sélectionnez la stratégie, puis cliquez sur **OK**.

Configuration de l'audit sur NetScaler Gateway

January 26, 2024

NetScaler Gateway vous permet de consigner les états et les informations d'état que l'appliance collecte. Vous pouvez utiliser les journaux d'audit pour afficher l'historique des événements dans l'ordre chronologique. Les messages contenus dans les journaux contiennent des informations sur l'événement qui a généré le message, un horodatage, le type de message, ainsi que des niveaux de consignation et des informations de message prédéfinis. Vous pouvez configurer des paramètres qui déterminent les informations consignées et l'emplacement de stockage des messages.

NetScaler Gateway prend actuellement en charge deux formats de journaux : un format de journal propriétaire pour les journaux locaux et le format syslog à utiliser avec les serveurs syslog. Vous pouvez configurer les journaux d'audit pour fournir les informations suivantes :

Niveau	Description
URGENCE	Consigne uniquement les erreurs majeures. Les entrées du journal indiquent que NetScaler Gateway rencontre un problème critique qui le rend inutilisable.
ALERTE	Enregistre les problèmes susceptibles d'entraîner le mauvais fonctionnement de NetScaler Gateway, mais qui ne sont pas critiques pour son fonctionnement. Des mesures correctives peuvent être prises dès que possible pour éviter que NetScaler Gateway ne rencontre un problème critique.
CRITIQUE	Enregistre les conditions critiques qui ne limitent pas le fonctionnement de NetScaler Gateway, mais qui peuvent dégénérer en un problème plus important.
ERROR	Consigne les entrées résultant de l'échec d'une opération sur NetScaler Gateway.
AVERTISSEMENT	Consigne les problèmes potentiels pouvant entraîner une erreur ou une erreur critique.

Niveau	Description
REMARQUE	Consigne les problèmes plus approfondis que le journal de niveau information, mais sert le même objectif que la notification.
INFORMATION	Enregistrez les actions effectuées par NetScaler Gateway. Ce niveau s'avère utile pour résoudre les problèmes rencontrés.

Le journal d'audit de NetScaler Gateway stocke également les statistiques de compression pour NetScaler Gateway si vous configurez la compression TCP. Le taux de compression obtenu pour différentes données est enregistré dans le fichier journal de chaque session utilisateur.

NetScaler Gateway utilise la signature du journal SessionID. Cela vous permet de suivre les journaux par session plutôt que par utilisateur. Les journaux générés dans le cadre d'une session ont le même ID de session. Si un utilisateur établit deux sessions à partir de la même machine utilisateur avec la même adresse IP, chaque session possède un ID de session unique.

> **Important :** Si vous avez écrit des scripts d'analyse de journaux personnalisés, vous devez effectuer cette modification de signature dans les scripts d'analyse personnalisés.

Configuration des journaux sur NetScaler Gateway

March 27, 2024

Lorsque vous configurez la journalisation sur NetScaler Gateway, vous pouvez choisir de stocker les journaux d'audit sur NetScaler Gateway ou de les envoyer à un serveur syslog. Vous utilisez l'utilitaire de configuration pour créer des stratégies d'audit et configurer des paramètres pour stocker les journaux d'audit.

Pour créer une stratégie d'audit

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway** > **Stratégies** > **Audit**.
2. Dans **Nom**, tapez le nom de la politique.
3. Sélectionnez l'une des options suivantes :
    - Syslog si vous souhaitez envoyer les journaux à un serveur Syslog.
    - `Nslog` pour stocker les journaux sur NetScaler Gateway.

> **Remarque :** Si vous sélectionnez cette option, les journaux sont stockés dans le dossier /var/log de l'appliance.

4. Dans le volet d'informations, cliquez sur **Ajouter**.
5. Saisissez les informations suivantes pour les informations du serveur sur lesquelles les journaux sont stockés :
   - Dans Nom, tapez le nom du serveur.
   - Sous Serveur, tapez le nom ou l'adresse IP du serveur de journaux.
6. Cliquez sur Créer, puis sur Fermer.

Après avoir créé la stratégie d'audit, vous pouvez la lier à n'importe quelle combinaison des éléments suivants :

- Globalement
- Serveurs virtuels
- Groups
- Utilisateurs

Pour lier une stratégie d'audit à l'échelle mondiale

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway** > **Stratégies** > **Audit**.
2. Sélectionnez l'un **`Syslog`** ou l'autre **`Nslog`**.
3. Dans le volet d'informations, cliquez sur **Action**, puis sur **Liaisons globales**.
4. Dans la **boîte de dialogue Lier/délier les stratégies d'audit** à la stratégie **globale**, sous **Détails**, cliquez sur **Insérer une stratégie**.
5. Sous **Nom de la stratégie**, sélectionnez une stratégie, puis cliquez sur **OK**.

Pour modifier une stratégie d'audit

Vous pouvez modifier une stratégie d'audit existante pour modifier le serveur vers lequel les journaux sont envoyés.

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, développez **NetScaler Gateway** > **Stratégies** > **Audit**
2. Sélectionnez l'un **`Syslog`** ou l'autre **`Nslog`**.
3. Dans le volet d'informations, cliquez sur une stratégie, puis cliquez sur **Ouvrir**.
4. Dans Serveur, sélectionnez le nouveau serveur, puis cliquez sur **OK**.

Pour supprimer une stratégie d'audit

Vous pouvez supprimer une stratégie d'audit de NetScaler Gateway. Lorsque vous supprimez une stratégie d'audit, celle-ci est automatiquement déliée.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway** > **Stratégies** > **Audit**.
2. Sélectionnez **Syslog** ou **Nslog**.
3. Dans le volet d'informations, cliquez sur une stratégie, puis sur **Supprimer**.

Configuration de la journalisation de l'ACL

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour consigner les détails des paquets qui correspondent à une liste de contrôle d'accès étendue (ACL). Outre le nom de la liste de contrôle d'accès, les détails consignés incluent des informations spécifiques au paquet, telles que les adresses IP source et de destination. Les informations sont stockées dans un journal système ou dans un `nslog` fichier, selon le type de journalisation (Syslog ou `nslog`) que vous activez.

Vous pouvez activer la journalisation au niveau global et au niveau ACL. Toutefois, pour activer la journalisation au niveau de l'ACL, vous devez également l'activer au niveau global. Le paramètre global est prioritaire.

Pour optimiser la journalisation, lorsque plusieurs paquets du même flux correspondent à une ACL, seuls les détails du premier paquet sont consignés. Le compteur est incrémenté pour tous les autres paquets appartenant au même flux. Un flux est défini comme un ensemble de paquets qui ont les mêmes valeurs pour les paramètres suivants :

- IP source
- IP destination
- Port source
- Port de destination
- Protocole (TCP ou UDP)

Si le paquet ne provient pas du même flux ou si la durée est supérieure à la durée moyenne, un nouveau flux est créé. Le temps moyen est le temps pendant lequel les paquets d'un même flux ne génèrent pas de messages supplémentaires (bien que le compteur soit incrémenté).

> **Remarque :** Le nombre total de flux différents pouvant être enregistrés à un moment donné est limité à 10 000.

Le tableau suivant décrit les paramètres avec lesquels vous pouvez configurer la journalisation des listes de contrôle d'accès au niveau de la règle pour les listes de contrôle d'accès étendues.

Nom du paramètre	Description
`Logstate`	État de la fonctionnalité de journalisation de l'ACL. Valeurs possibles : ENABLED et DISABLED. Par défaut : DÉSACTIVÉ.
`Ratelimit`	Nombre de messages de journal qu'une liste de contrôle d'accès spécifique peut générer. Par défaut : 100.

Pour configurer la journalisation des ACL à l'aide de l'utilitaire de configuration

Vous pouvez configurer la journalisation d'une liste de contrôle d'accès et spécifier le nombre de messages de journal que la règle peut générer.

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **Système** > **Réseau**, puis cliquez sur ACL.
2. Dans le volet d'informations, cliquez sur l'onglet **ACL étendues**, puis cliquez sur Ajouter.
3. Dans la boîte de dialogue **Créer une liste de contrôle d'accès étendue**, dans Nom, tapez un nom pour la stratégie.
4. Activez la case à cocher **État du journal**.
5. Dans la zone de texte **Limite de taux de journalisation**, tapez la limite de taux que vous souhaitez spécifier pour la règle, puis cliquez sur **Créer**.

Après avoir configuré la journalisation des ACL, vous pouvez l'activer sur NetScaler Gateway. Créez une stratégie d'audit, puis liez-la à un utilisateur, un groupe, un serveur virtuel ou globalement.

Pour activer la journalisation ACL ou TCP sur NetScaler Gateway

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **NetScaler Gateway** > **Stratégies** > **Audit**.
2. Sélectionnez Syslog ou `nslog`.
3. Sous l'onglet **Serveurs**, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer un serveur d'audit**, dans **Nom**, tapez un nom pour le serveur, puis configurez les paramètres du serveur.
5. Cliquez sur **Journalisation ACL ou JournalisationTCP**, puis cliquez sur**Créer**.

Activer la journalisation Citrix Secure Access

March 27, 2024

Vous pouvez configurer le client Citrix Secure Access pour consigner toutes les erreurs dans des fichiers texte stockés sur la machine utilisateur. Les utilisateurs peuvent configurer le client Citrix Secure Access pour définir le niveau de journalisation sur la machine utilisateur afin d'enregistrer des activités utilisateur spécifiques. Lorsque les utilisateurs configurent la journalisation, le plug-in crée les deux fichiers suivants sur la machine utilisateur :

- hooklog<num>.txt, qui enregistre les messages d'interception générés par le client Citrix Secure Access.
- nssslvpn.txt, qui répertorie les erreurs associées au plug-in.

> **Remarque :** Les fichiers hooklog.txt ne sont pas supprimés automatiquement. Citrix recommande de supprimer régulièrement les fichiers.

Les journaux utilisateur se trouvent dans les répertoires suivants de Windows sur la machine utilisateur :

- Windows XP (tous les utilisateurs) : %SystemDrive% :\Documents and Settings\All Users\Application Data\Citrix\AGEE
- Windows XP (spécifique à l'utilisateur) : %SystemDrive% :\Documents and Settings\%username%\Local Settings\Application Data\Citrix\AGEE
- Windows Vista (tous les utilisateurs) : %SystemDrive% :\ProgramData\Citrix\AGEE
- Windows Vista (spécifique à l'utilisateur) : %SystemDrive% :\Users\%username%\AppData\Local\Citrix\AGE
- Windows 7 (tous les utilisateurs) : %SystemDrive% :\ProgramData\Citrix\AGEE
- Windows 7 (spécifique à l'utilisateur) : %SystemDrive% :\Users\%username%\AppData\Local\Citrix\AGEE
- Windows 8 (tous les utilisateurs) : %SystemDrive% :\ProgramData\Citrix\AGEE
- Windows 8 (spécifique à l'utilisateur) : %SystemDrive% :\Users\%username%\AppData\Local\Citrix\AGEE

Vous pouvez utiliser ces fichiers journaux pour dépanner le client Citrix Secure Access. Les utilisateurs peuvent envoyer les fichiers journaux par e-mail au support technique.

Dans la boîte de dialogue Configuration, les utilisateurs peuvent définir le niveau de journalisation pour le client Citrix Secure Access. Les niveaux de consignation sont les suivants :

- Enregistrer les messages d'erreur
- Enregistrer les messages d'événements
- Enregistrer les statistiques du client Citrix Secure Access
- Enregistrer toutes les erreurs, les messages d'événements et les statistiques

Pour plus d'informations sur la fonctionnalité de journalisation du client Citrix Secure Access pour Windows, consultez la section Collecte améliorée des journaux pour le client Windows.

Pour surveiller les connexions ICA

March 27, 2024

Vous pouvez surveiller les sessions utilisateur actives sur votre batterie de serveurs à l'aide de la boîte de dialogue Connexions
ICA. Cette boîte de dialogue fournit les informations suivantes :

- Nom d'utilisateur de la personne qui se connecte à la batterie de serveurs
- Nom de domaine de la batterie de serveurs
- Adresse IP de la machine utilisateur
- Numéro de port de la machine utilisateur
- Adresse IP du serveur exécutant Citrix Virtual Apps and Desktops
- Numéro de port du serveur exécutant Citrix Virtual Apps and Desktops

1. Accédez à **Configuration > NetScaler Gateway**.
2. Dans la section **Surveiller les connexions**, cliquez sur **Connexions ICA**.

Journaux de session ICA

Le fichier `ns.log` imprime les journaux de session ICA au format suivant :

```
May  2 09:29:02 <local0.info> 10.106.40.223  05/02/2023:09:29:02 GMT
    0-PPE-1 : default ICA Message 141327 0 :  "[Remote ip =
    10.10.99.86:514] [EDT] [CGP][ICAUUID=0006ab3454-d7de-1450-9678-
    c6333447a76] Received response from STA server {
 sta-server=10.11.40.222:80,type=ResponseData }
 "
<!--NeedCopy-->
```

À partir de la version 13.1 build 50.x, les améliorations suivantes sont apportées aux journaux ICA :

- Affiche les types de connexion tels que TCP, EDT, CGP et SOCKS.
- Affiche l'identifiant unique universel (UUID) de l'ICA.
- Tous les journaux STA sont affichés sous forme de journaux de niveau informatif.

Authentification et autorisation

March 27, 2024

NetScaler Gateway utilise une conception d'authentification flexible qui permet une personnalisation poussée de l'authentification des utilisateurs pour NetScaler Gateway. Vous pouvez utiliser des serveurs d'authentification conformes aux normes du secteur et configurer NetScaler Gateway pour authentifier les utilisateurs auprès des serveurs. NetScaler Gateway prend également en charge l'authentification basée sur les attributs présents dans un certificat client. L'authentification NetScaler Gateway est conçue pour prendre en charge des procédures d'authentification simples qui utilisent une source unique pour l'authentification des utilisateurs, et des procédures d'authentification en cascade plus complexes qui reposent sur plusieurs types d'authentification.

L'authentification NetScaler Gateway intègre l'authentification locale pour la création d'utilisateurs et de groupes locaux. Cette conception est centrée sur l'utilisation de stratégies pour contrôler les procédures d'authentification que vous configurez. Les stratégies que vous créez peuvent être appliquées au niveau global ou virtuel de NetScaler Gateway et peuvent être utilisées pour définir les paramètres du serveur d'authentification de manière conditionnelle en fonction du réseau source de l'utilisateur.

Étant donné que les stratégies sont liées globalement ou à un serveur virtuel, vous pouvez également attribuer des priorités à vos stratégies pour créer une cascade de plusieurs serveurs d'authentification dans le cadre de l'authentification.

NetScaler Gateway prend en charge les types d'authentification suivants.

- Stockage local
- LDAP (Lightweight Directory Access Protocol)
- RADIUS
- SAML
- TACACS+
- Authentification du certificat client (incluant l'authentification par carte à puce)

NetScaler Gateway prend également en charge RSA SecurID, Gemalto Protiva et SafeWord. Vous utilisez un serveur RADIUS pour configurer ces types d'authentification.

Alors que l'authentification permet aux utilisateurs de se connecter à NetScaler Gateway et de se connecter au réseau interne, l'autorisation définit les ressources du réseau sécurisé auxquelles les utilisateurs ont accès. Vous configurez l'autorisation à l'aide de stratégies LDAP et RADIUS.

Configuration des types d'authentification globale par défaut

March 27, 2024

Lorsque vous avez installé NetScaler Gateway et exécuté l'assistant NetScaler Gateway, vous avez configuré l'authentification dans l'assistant. Cette stratégie d'authentification est automatiquement liée au niveau global de NetScaler Gateway. Le type d'authentification que vous configurez dans l'assistant NetScaler Gateway est le type d'authentification par défaut. Vous pouvez modifier le type d'autorisation par défaut en exécutant à nouveau l'assistant NetScaler Gateway ou vous pouvez modifier les paramètres d'authentification globaux dans l'utilitaire de configuration.

Si vous devez ajouter des types d'authentification supplémentaires, vous pouvez configurer des stratégies d'authentification sur NetScaler Gateway et lier les stratégies à NetScaler Gateway à l'aide de l'utilitaire de configuration. Lorsque vous configurez l'authentification globalement, vous définissez le type d'authentification, configurez les paramètres et définissez le nombre maximal d'utilisateurs pouvant être authentifiés.

Après avoir configuré et lié la stratégie, vous pouvez définir la priorité pour définir le type d'authentification prioritaire. Par exemple, vous configurez les stratégies d'authentification LDAP et RADIUS. Si la stratégie LDAP a un numéro de priorité de 10 et que la stratégie RADIUS a un numéro de priorité de 15, la stratégie LDAP est prioritaire, quel que soit l'endroit où vous liez chaque stratégie. C'est ce qu'on appelle l'authentification en cascade.

Vous pouvez choisir de fournir des pages de connexion depuis le cache en mémoire de NetScaler Gateway ou depuis le serveur HTTP exécuté sur NetScaler Gateway. Si vous choisissez de diffuser la page de connexion à partir du cache en mémoire, la diffusion de la page de connexion à partir de NetScaler Gateway est nettement plus rapide qu'à partir du serveur HTTP. Le choix de fournir la page d'ouverture de session à partir du cache en mémoire réduit le temps d'attente lorsqu'un grand nombre d'utilisateurs ouvrent une session en même temps. Vous pouvez uniquement configurer la remise des pages d'ouverture de session à partir du cache dans le cadre d'une stratégie d'authentification globale.

Vous pouvez également configurer l'adresse IP NAT (Network Address Translation) qui est une adresse IP spécifique pour l'authentification. Cette adresse IP est unique pour l'authentification et ne correspond pas au sous-réseau NetScaler Gateway, aux adresses IP mappées ou virtuelles. Ce paramètre est facultatif.

Remarque : Vous ne pouvez pas utiliser l'assistant NetScaler Gateway pour configurer l'authentification SAML.

Vous pouvez utiliser l'assistant de configuration rapide pour configurer l'authentification par certificat LDAP, RADIUS et client. Lorsque vous exécutez l'assistant, vous pouvez sélectionner un serveur LDAP ou RADIUS existant configuré sur NetScaler Gateway. Vous pouvez également configurer les

paramètres de LDAP ou de RADIUS. Si vous utilisez l'authentification à deux facteurs, Citrix recommande d'utiliser LDAP comme type d'authentification principal.

Pour configurer l'authentification à l'échelle mondiale

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres d'authentification.
3. Dans Nombre maximum d'utilisateurs, tapez le nombre d'utilisateurs qui peuvent être authentifiés à l'aide de ce type d'authentification.
4. Dans Adresse IP NAT, saisissez l'adresse IP unique pour l'authentification.
5. Sélectionnez Activer la miseen cache statique pour diffuser les pages d'ouverture de session plus rapidement.
6. Sélectionnez Activer les commentaires sur l'authentification améliorée pour envoyer un message aux utilisateurs en cas d'échec de l'authentification. Le message que les utilisateurs reçoivent inclut des erreurs de mot de passe, un compte désactivé ou verrouillé, ou l'utilisateur est introuvable, pour n'en nommer que quelques-uns.
7. Dans Type d'authentification par défaut, sélectionnez le type d'authentification.
8. Configurez les paramètres de votre type d'authentification, puis cliquez sur OK.

Configuration de l'authentification sans autorisation

January 26, 2024

L'autorisation définit les ressources auxquelles les utilisateurs sont autorisés à se connecter via NetScaler Gateway. Vous configurez les stratégies d'autorisation en utilisant une expression, puis en définissant la stratégie pour qu'elle soit autorisée ou refusée. Vous pouvez configurer NetScaler Gateway pour qu'il utilise uniquement l'authentification, sans autorisation.

Lorsque vous configurez l'authentification sans autorisation, NetScaler Gateway n'effectue pas de vérification d'autorisation de groupe. Les stratégies que vous configurez pour l'utilisateur ou le groupe sont attribuées à l'utilisateur.

Pour plus d'informations sur la configuration de l'autorisation, consultez Configuration de l'autorisation.

Configuration de l'autorisation

January 26, 2024

L'autorisation spécifie les ressources réseau auxquelles les utilisateurs ont accès lorsqu'ils se connectent à NetScaler Gateway. Le paramètre par défaut de l'autorisation consiste à refuser l'accès à toutes les ressources réseau. Citrix recommande d'utiliser le paramètre global par défaut, puis de créer des stratégies d'autorisation pour définir les ressources réseau auxquelles les utilisateurs peuvent accéder.

Vous configurez l'autorisation sur NetScaler Gateway à l'aide d'une stratégie et d'expressions d'autorisation. Après avoir créé une stratégie d'autorisation, vous pouvez la lier aux utilisateurs ou aux groupes que vous avez configurés sur l'appliance.

Configuration des stratégies d'autorisation

March 27, 2024

Lorsque vous configurez une stratégie d'autorisation, vous pouvez la définir pour autoriser ou refuser l'accès aux ressources réseau du réseau interne. Par exemple, pour autoriser les utilisateurs à accéder au réseau 10.3.3.0, utilisez l'expression suivante :

CLIENT.IP.DST.IN_SUBNET(10.3.0.0/16)

Les stratégies d'autorisation sont appliquées aux utilisateurs et aux groupes. Une fois qu'un utilisateur est authentifié, NetScaler Gateway effectue une vérification d'autorisation de groupe en obtenant les informations de groupe de l'utilisateur auprès d'un serveur RADIUS, LDAP ou TACACS+. Si les informations de groupe sont disponibles pour l'utilisateur, NetScaler Gateway vérifie les ressources réseau autorisées pour le groupe.

Pour contrôler les ressources auxquelles les utilisateurs peuvent accéder, vous devez créer des stratégies d'autorisation. Si vous n'avez pas besoin de créer des stratégies d'autorisation, vous pouvez configurer l'autorisation globale par défaut.

Si vous créez une expression dans la stratégie d'autorisation qui refuse l'accès à un chemin d'accès au fichier, vous ne pouvez utiliser que le chemin d'accès au sous-répertoire et non le répertoire racine. Par exemple, utilisez fs.path contient "\\dir1\\dir2""au lieu de fs.path contient "\\rootdir\\dir1\\dir2. Si vous utilisez la deuxième version de cet exemple, la stratégie échoue.

Après avoir configuré la stratégie d'autorisation, vous la liez à un utilisateur ou à un groupe, comme indiqué dans les tâches ci-dessous.

Par défaut, les stratégies d'autorisation sont d'abord validées par rapport aux stratégies que vous liez au serveur virtuel, puis par rapport aux stratégies liées globalement. Si vous liez une stratégie globalement et que vous souhaitez qu'elle soit prioritaire sur une stratégie que vous liez à un utilisateur, un groupe ou un serveur virtuel, vous pouvez modifier le numéro de priorité de la stratégie. Les numéros de priorité commencent à zéro. Un numéro de priorité inférieur donne à la stratégie une priorité plus élevée.

Par exemple, si la stratégie globale a un numéro de priorité et que l'utilisateur a une priorité de deux, la stratégie d'authentification globale est appliquée en premier.

> **Important :**
>
> - Les stratégies d'autorisation classiques sont appliquées uniquement au trafic TCP.
> - La stratégie d'autorisation avancée peut être appliquée à tous les types de trafic (TCP/UDP/ICMP/DNS).
>   - To apply policy on UDP/ICMP/DNS traffic, policies must be bound at type UDP_REQUEST, ICMP_REQUEST, and DNS_REQUEST respectively.
>   - While binding, if "type"is not explicitly mentioned or "type"is set to REQUEST, the behavior does not change from earlier builds, that is these policies are applied only to TCP traffic.
>   - The policies bound at UDP_REQUEST do not apply for DNS traffic. For DNS, policies must be explicitly bound to DNS_REQUEST TCP_DNS is similar to other TCP requests.

Pour plus d'informations sur les stratégies d'autorisation avancées, consultez l'article https://support.citrix.com/article/CTX232237.

Exemples d'expressions de stratégie d'autorisation

Voici des exemples d'expressions de stratégies d'autorisation :

- `add authorization policy athzPol1 "HTTP.REQ.USER.IS_MEMBER_OF(\"allowedGroup\")"ALLOW`
- `add authorization policy athzPol2 "CLIENT.IP.DST.BETWEEN(10.102.75.10,10.1 "DENY`
- `add authorization policy athzPol3 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv")|| CLIENT.IP.DST.IN_SUBNET(10.102.75.0/25)"ALLOW`

Pour configurer une stratégie d'autorisation à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Stratégies > Autorisation**.

2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. Dans **Action**, sélectionnez **Autoriser** ou **Refuser**.
5. Dans **Expression**, cliquez sur **Expression Editor**.
6. Pour commencer à configurer l'expression, cliquez sur **Sélectionner** et choisissez les éléments nécessaires.
7. Cliquez sur **Terminé** lorsque votre expression est terminée.
8. Cliquez sur **Créer**.

Pour lier une stratégie d'autorisation à un utilisateur à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Administration des utilisateurs.**
2. Cliquez sur **Utilisateurs AAA**.
3. Dans le volet d'informations, sélectionnez un utilisateur, puis cliquez sur **Modifier**.
4. Dans les **paramètres avancés**, cliquez sur **Stratégies d'autorisation**.
5. Dans **la page Liaison** de stratégie, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Pour lier une stratégie d'autorisation à un groupe à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway**> Administration des utilisateurs.
2. Cliquez sur **AAA Groups**.
3. Dans le volet d'informations, sélectionnez un groupe, puis cliquez sur **Modifier**.
4. Dans les **paramètres avancés**, cliquez sur **Stratégies d'autorisation**.
5. Dans **la page Liaison** de stratégie, sélectionnez une stratégie ou créez une stratégie.
6. Dans **Priorité**, définissez le numéro de priorité.
7. Dans **Type**, sélectionnez le type de demande, puis cliquez sur **OK**.

Définition de l'autorisation globale par défaut

March 27, 2024

Pour définir les ressources auxquelles les utilisateurs ont accès sur le réseau interne, vous pouvez configurer l'autorisation globale par défaut. Vous configurez l'autorisation globale en autorisant ou en refusant l'accès aux ressources réseau globalement sur le réseau interne.

Toute action d'autorisation globale que vous créez est appliquée à tous les utilisateurs auxquels aucune stratégie d'autorisation n'est déjà associée, soit directement, soit par l'intermédiaire d'un

groupe. Une stratégie d'autorisation d'utilisateur ou de groupe remplace toujours l'action d'autorisation globale. Si l'action d'autorisation par défaut est définie sur Refuser, vous devez appliquer des stratégies d'autorisation pour tous les utilisateurs ou groupes afin de rendre les ressources réseau accessibles à ces utilisateurs ou groupes. Cette exigence contribue à améliorer la sécurité.

Pour définir l'autorisation globale par défaut :

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Sécurité, en regard de Action d'autorisation par défaut, sélectionnez Autoriser ou Refuser, puis cliquez sur OK.

Désactivation de l'authentification

March 27, 2024

Si votre déploiement ne nécessite pas d'authentification, vous pouvez le désactiver. Vous pouvez désactiver l'authentification pour chaque serveur virtuel qui ne nécessite pas d'authentification.

Important : Citrix recommande de désactiver l'authentification avec prudence. Si vous n'utilisez pas de serveur d'authentification externe, créez des utilisateurs et des groupes locaux pour permettre à NetScaler Gateway d'authentifier les utilisateurs. La désactivation de l'authentification arrête l'utilisation des fonctionnalités d'authentification, d'autorisation et de comptabilité qui contrôlent et surveillent les connexions à NetScaler Gateway. Lorsque les utilisateurs saisissent une adresse Web pour se connecter à NetScaler Gateway, la page de connexion ne s'affiche pas.

Pour désactiver l'authentification

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis sur Ouvrir.
3. Dans l'onglet Authentification, sous Authentification de l'utilisateur, cliquez pour désactiver Activer l'authentification.

Configuration de l'authentification pour des heures spécifiques

March 27, 2024

Vous pouvez configurer une stratégie d'authentification afin que les utilisateurs soient autorisés à accéder au réseau interne à des moments précis, par exemple pendant les heures de travail normales. Lorsque les utilisateurs tentent de se connecter à un autre moment, l'ouverture de session est refusée.

Pour restreindre le moment où les utilisateurs se connectent à NetScaler Gateway, créez une expression dans la stratégie d'authentification, puis liez-la à un serveur virtuel ou à l'échelle mondiale.

Pour configurer l'authentification pour l'heure, la date ou le jour de la semaine

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Sous Authentification, sélectionnez le type d'authentification.
3. Dans le volet d'informations, cliquez sur l'onglet Stratégies, sélectionnez une stratégie d'authentification, puis cliquez sur Ouvrir.
4. Dans la boîte de dialogue Configurer la stratégie d'authentification, sous Expression, en regard de Correspondance avec n'importe quelle expression, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une expression, dans Type d'expression, sélectionnez Date/heure.
6. Dans Qualificatif, sélectionnez l'une des options suivantes :

   - TIME pour configurer l'heure à laquelle les utilisateurs ne peuvent pas ouvrir de session.
   - DATE pour configurer la date à laquelle les utilisateurs ne peuvent pas ouvrir de session.
   - DAYOFWEEK pour configurer le jour où les utilisateurs ne peuvent pas ouvrir de session.

   Exemple : HEURE : 2020-10-12-02:30:00 GMT DATE : 2020-10-12 DAYOFWEEK : Lundi
7. Dans Opérateur, sélectionnez la valeur.
8. Dans Valeur, cliquez sur le calendrier en regard de la zone de texte, puis sélectionnez le jour, la date ou l'heure.
9. Cliquez deux fois sur OK, cliquez sur Fermer, puis sur OK.

Fonctionnent des stratégies d'authentification

January 26, 2024

Lorsque les utilisateurs se connectent à NetScaler Gateway, ils sont authentifiés conformément à une stratégie que vous créez. La stratégie définit le type d'authentification. Une stratégie d'authentification unique peut être utilisée pour des besoins d'authentification simples et est généralement liée au niveau global. Vous pouvez également utiliser le type d'authentification par défaut, qui est local. Si vous configurez l'authentification locale, vous devez également configurer les utilisateurs et les groupes sur NetScaler Gateway.

Vous pouvez configurer plusieurs stratégies d'authentification et les lier pour créer une procédure d'authentification détaillée et des serveurs virtuels. Par exemple, vous pouvez configurer l'authentification en cascade et à deux facteurs en configurant plusieurs stratégies. Vous pouvez également définir la priorité des stratégies d'authentification afin de déterminer quels serveurs et l'ordre dans lequel NetScaler Gateway vérifie les informations d'identification des utilisateurs. Une stratégie d'authentification inclut une expression et une action. Par exemple, si vous définissez l'expression sur la valeur True, lorsque les utilisateurs ouvrent une session, l'action évalue l'ouverture de session utilisateur sur True, puis les utilisateurs ont accès aux ressources réseau.

Après avoir créé une stratégie d'authentification, vous liez la stratégie au niveau global ou aux serveurs virtuels. Lorsque vous liez au moins une stratégie d'authentification à un serveur virtuel, les stratégies d'authentification que vous avez liées au niveau global ne sont pas utilisées lorsque les utilisateurs ouvrent une session sur le serveur virtuel, à moins que le type d'authentification globale ait une priorité supérieure à la stratégie liée au serveur virtuel.

Lorsqu'un utilisateur se connecte à NetScaler Gateway, l'authentification est évaluée dans l'ordre suivant :

- Le serveur virtuel est vérifié pour détecter toute stratégie d'authentification liée.
- Si les stratégies d'authentification ne sont pas liées au serveur virtuel, NetScaler Gateway vérifie les stratégies d'authentification globales.
- Si une stratégie d'authentification n'est pas liée à un serveur virtuel ou globalement, l'utilisateur est authentifié via le type d'authentification par défaut.

Si vous configurez des stratégies d'authentification LDAP et RADIUS et que vous souhaitez lier les stratégies globalement pour l'authentification à deux facteurs, vous pouvez sélectionner la stratégie dans l'utilitaire de configuration, puis choisir si la stratégie est le type d'authentification principal ou secondaire. Vous pouvez également configurer une stratégie d'extraction de groupe.

Configuration des profils d'authentification

March 27, 2024

Vous pouvez créer un profil d'authentification à l'aide de l'assistant NetScaler Gateway ou de l'utilitaire de configuration. Le profil contient tous les paramètres de la stratégie d'authentification. Vous configurez le profil lorsque vous créez la stratégie d'authentification.

Avec l'assistant NetScaler Gateway, vous pouvez utiliser le type d'authentification choisi pour configurer l'authentification. Si vous souhaitez configurer des stratégies d'authentification supplémentaires après l'exécution de l'assistant, vous pouvez utiliser l'utilitaire de configuration. Pour plus d'informations sur l'assistant NetScaler Gateway, voir Configuration des paramètres à l'aide de l'assistant NetScaler Gateway.

Pour créer une stratégie d'authentification à l'aide de l'utilitaire de configuration

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
4. Si vous utilisez un type d'authentification externe, cliquez sur Nouveau en regard de Serveur.
5. Dans la boîte de dialogue Créer un serveur d'authentification, configurez les paramètres de votre type d'authentification, cliquez sur Créer, puis sur Fermer.
6. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez Valeur vraie, cliquez sur Ajouter une expression, sur Créer, puis sur Fermer. Remarque : Lorsque vous sélectionnez un type d'authentification et que vous enregistrez le profil d'authentification, vous ne pouvez pas modifier le type d'authentification. Pour utiliser un autre type d'authentification, vous devez créer une nouvelle stratégie.

Pour modifier une stratégie d'authentification à l'aide de l'utilitaire de configuration

Vous pouvez modifier les stratégies et profils d'authentification configurés, tels que l'adresse IP du serveur d'authentification ou l'expression.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Serveurs, sélectionnez un serveur, puis cliquez sur Ouvrir.

Pour supprimer une stratégie d'authentification

Si vous avez modifié ou supprimé un serveur d'authentification de votre réseau, supprimez la stratégie d'authentification correspondante de NetScaler Gateway.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Dans le volet de navigation, sous Authentification, sélectionnez un type d'authentification.
3. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez une stratégie, puis cliquez sur Supprimer.

Liaison des stratégies d'authentification

March 27, 2024

Après avoir configuré les stratégies d'authentification, vous les liez globalement ou à un serveur virtuel. Vous pouvez utiliser l'utilitaire de configuration pour lier une stratégie d'authentification.

Pour lier une stratégie d'authentification globalement à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Cliquez sur un type d'authentification.
3. Dans le volet d'informations, sous **l'onglet Stratégies**, cliquez sur un serveur, puis dans **Action**, cliquez sur **Liaisons globales**.
4. Dans l'onglet **Principal ou Secondaire**, sous **Détails**, cliquez sur **Insérer une stratégie**.
5. Sous **Nom de la stratégie**, sélectionnez la stratégie, puis cliquez sur **OK**.

   Remarque : Lorsque vous sélectionnez la stratégie, NetScaler Gateway définit automatiquement l'expression sur la valeur True.

Pour délier une stratégie d'authentification globale à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Dans l'onglet **Stratégies**, dans **Action**, cliquez sur **Liaisons globales**.
3. Dans la boîte de dialogue **Lier/délier les stratégies d'authentification à Global**, sous l'onglet **Principal ou Secondaire**, dans **Nom de la stratégie**, sélectionnez la stratégie, cliquez sur **Dissocier la stratégie**, puis cliquez sur **OK**.

Définition des priorités des stratégies d'authentification

March 27, 2024

Par défaut, les stratégies d'authentification sont d'abord validées par rapport aux stratégies que vous liez au serveur virtuel, puis par rapport aux stratégies liées globalement. Si vous liez une stratégie d'authentification globalement et que vous souhaitez que la stratégie globale soit prioritaire sur une stratégie que vous liez à un serveur virtuel, vous pouvez modifier le numéro de priorité de la stratégie. Les numéros de priorité commencent à zéro. Un numéro de priorité inférieur donne à la stratégie d'authentification une priorité plus élevée.

Par exemple, si la stratégie globale a un numéro de priorité et que le serveur virtuel a une priorité de deux, la stratégie d'authentification globale est appliquée en premier.

Pour définir ou modifier la priorité des stratégies d'authentification globale

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Sous l'onglet Stratégies, dans Action, cliquez sur Liaisons globales.
3. Dans la boîte de dialogue Stratégies globales d'authentification de liaison/déliaison, sous l'onglet Primaire ou Secondaire, sous Priorité, tapez le numéro, puis cliquez sur OK.

Pour modifier la priorité d'une stratégie d'authentification liée à un serveur virtuel

Vous pouvez également modifier une stratégie d'authentification liée à un serveur virtuel.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Sélectionnez un serveur virtuel, puis cliquez sur Ouvrir.
3. Cliquez sur l'onglet Authentification, puis sélectionnez Primaire ou Secondaire.
4. Sélectionnez la stratégie et, dans Priorité, tapez le numéro de la priorité, puis cliquez sur OK.

Configuration des utilisateurs locaux

March 27, 2024

Vous pouvez créer des comptes utilisateurs localement sur NetScaler Gateway pour compléter les utilisateurs sur les serveurs d'authentification. Par exemple, vous pouvez créer des comptes d'utilisa-

teurs locaux pour des utilisateurs temporaires, tels que des consultants ou des visiteurs, sans créer d'entrée pour ces utilisateurs sur le serveur d'authentification.

Si vous utilisez l'authentification locale, créez des utilisateurs, puis ajoutez-les aux groupes que vous créez sur NetScaler Gateway. Après avoir configuré les utilisateurs et les groupes, vous pouvez appliquer des stratégies d'autorisation et de session, créer des signets, spécifier des applications et spécifier l'adresse IP des partages de fichiers et des serveurs auxquels les utilisateurs ont accès.

Pour créer des utilisateurs locaux

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et, dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Users.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom d'utilisateur**, tapez le nom d'utilisateur.
4. Si vous utilisez l'authentification locale, désactivez **Authentification externe**.
   Remarque : sélectionnez **Authentification externe** pour que les utilisateurs s'authentifient auprès d'un serveur d'authentification externe, tel que LDAP ou RADIUS. Décochez la case pour que NetScaler Gateway s'authentifie auprès de la base de données utilisateur locale.
5. Dans **Mot** de passe et **confirmation du mot** de passe, tapez le mot de passe de l'utilisateur, cliquez sur **Créer**, puis sur **Fermer**.

Pour modifier le mot de passe d'un utilisateur

Après avoir créé un utilisateur local, vous pouvez modifier le mot de passe de l'utilisateur ou configurer le compte d'utilisateur pour qu'il soit authentifié par rapport à un serveur d'authentification externe.

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et, dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Users.**
2. Dans le volet d'informations, sélectionnez un utilisateur, puis cliquez sur **Ouvrir**.
3. Dans **Mot de passe** et **confirmation du mot de passe**, tapez le nouveau mot de passe de l'utilisateur, puis cliquez sur **OK**.

Pour modifier la méthode d'authentification d'un utilisateur

Si vous avez des utilisateurs configurés pour l'authentification locale, vous pouvez remplacer l'authentification par un serveur d'authentification externe. Pour ce faire, activez l'authentification externe.

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et, dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Users.**

2. Dans le volet d'informations, sélectionnez un utilisateur, puis cliquez sur **Ouvrir**.
3. Sélectionnez **Authentification externe**, puis cliquez sur **OK**.

Pour supprimer un utilisateur

Vous pouvez également supprimer un utilisateur de NetScaler Gateway.

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et, dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Users.**
2. Dans le volet d'informations, sélectionnez un utilisateur, puis cliquez sur **Supprimer**.

Lorsque vous supprimez un utilisateur de NetScaler Gateway, toutes les stratégies associées sont également supprimées du profil utilisateur.

Configuration des groupes

January 26, 2024

Vous pouvez avoir des groupes sur NetScaler Gateway qui sont des groupes locaux et peuvent authentifier les utilisateurs à l'aide d'une authentification locale. Si vous utilisez des serveurs externes pour l'authentification, les groupes de NetScaler Gateway sont configurés pour correspondre aux groupes configurés sur les serveurs d'authentification du réseau interne. Lorsqu'un utilisateur ouvre une session et est authentifié, si le nom d'un groupe correspond à celui d'un groupe sur un serveur d'authentification, l'utilisateur hérite des paramètres du groupe sur NetScaler Gateway.

Après avoir configuré les groupes, vous pouvez appliquer des stratégies d'autorisation et de session, créer des signets, spécifier des applications et spécifier l'adresse IP des partages de fichiers et des serveurs auxquels l'utilisateur a accès.

Si vous utilisez l'authentification locale, créez des utilisateurs et ajoutez-les aux groupes configurés sur NetScaler Gateway. Les utilisateurs héritent ensuite des paramètres de ce groupe.

Important : si les utilisateurs sont membres d'un groupe Active Directory, le nom du groupe sur NetScaler Gateway doit être identique à celui du groupe Active Directory.

Pour créer un groupe

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Groups.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom du groupe**, tapez le nom du groupe, cliquez sur **Créer**, puis sur **Fermer**.

Pour supprimer un groupe

Vous pouvez également supprimer des groupes d'utilisateurs de NetScaler Gateway.

1. **Dans l'utilitaire de configuration, cliquez sur l'onglet**Configuration**et dans le volet de navigation, développez**NetScaler Gateway > User Administration**, puis cliquez sur AAA Groups.**
2. Dans le volet d'informations, sélectionnez le groupe, puis cliquez sur **Supprimer**.

Ajout d'utilisateurs aux groupes

March 27, 2024

Vous pouvez ajouter des utilisateurs à un groupe pendant la création du groupe ou ultérieurement. Vous pouvez ajouter des utilisateurs à plusieurs groupes afin que les utilisateurs puissent hériter des stratégies et des paramètres liés à ces groupes.

Pour ajouter des utilisateurs à des groupes :

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration et, dans le volet de navigation, développez **NetScaler Gateway > User Administration**, puis cliquez sur **AAA Users**.
2. Dans le volet d'informations, sélectionnez un groupe, puis cliquez sur **Ouvrir**.
3. Dans l'onglet **Utilisateurs**, sous **Utilisateurs disponibles**, sélectionnez les utilisateurs, cliquez sur **Ajouter**, puis sur **OK**.

Configuration des stratégies avec des groupes

January 26, 2024

Après avoir configuré des groupes, vous pouvez utiliser la boîte de dialogue Groupe pour appliquer des stratégies et des paramètres qui spécifient l'accès utilisateur. Si vous utilisez l'authentification locale, vous créez des utilisateurs et vous les ajoutez à des groupes configurés sur NetScaler Gateway. Les utilisateurs héritent ensuite des paramètres de ce groupe.

Vous pouvez configurer les stratégies ou paramètres suivants pour un groupe d'utilisateurs dans la boîte de dialogue Groupe :

- Utilisateurs
- Stratégies d'autorisation
- Stratégies d'audit
- Stratégies de session

- Stratégies de trafic
- Signets
- Applications Intranet
- Adresses IP Intranet

Dans votre configuration, certains utilisateurs peuvent appartenir à plusieurs groupes. En outre, chaque groupe peut avoir une ou plusieurs stratégies de session liées, avec différents paramètres configurés. Les utilisateurs appartenant à plusieurs groupes héritent des stratégies de session attribuées à tous les groupes auxquels ils appartiennent. Pour vous assurer que l'évaluation de la stratégie de session est prioritaire sur l'autre, vous devez définir la priorité de la stratégie de session.

Par exemple, le groupe1 est lié à une stratégie de session configurée avec la page d'accueil www.homepage1.com. Group2 est lié à une stratégie de session configurée avec la page d'accueil www.homepage2.com. Lorsque ces stratégies sont liées à des groupes respectifs sans numéro de priorité ou avec le même numéro de priorité, la page d'accueil qui apparaît aux utilisateurs appartenant aux deux groupes dépend de la stratégie traitée en premier. En définissant un numéro de priorité inférieur, qui donne une priorité plus élevée, pour la stratégie de session avec la page d'accueil www.homepage1.com, vous pouvez vous assurer que les utilisateurs appartenant aux deux groupes reçoivent la page d'accueil www.homepage1.com.

Si aucun numéro de priorité n'est attribué aux stratégies de session ou n'ont pas le même numéro de priorité, la priorité est évaluée dans l'ordre suivant :

- Utilisateur
- Groupe
- Serveur virtuel
- Global

Si les stratégies sont liées au même niveau, sans numéro de priorité ou si les stratégies ont le même numéro de priorité, l'ordre d'évaluation est celui de l'ordre de liaison des stratégies. Les stratégies qui sont liées en premier à un niveau sont prioritaires par rapport aux stratégies liées ultérieurement.

Si nous avons un utilisateur lié à plusieurs groupes avec chaque groupe lié à l'IIP, l'utilisateur peut obtenir une adresse IP gratuite de n'importe quel groupe lié.

Configuration de l'authentification LDAP

January 26, 2024

Vous pouvez configurer NetScaler Gateway pour authentifier l'accès des utilisateurs à un ou plusieurs serveurs LDAP.

L'autorisation LDAP nécessite des noms de groupe identiques dans Active Directory, sur le serveur LDAP et sur NetScaler Gateway. Les caractères et la casse doivent également correspondre.

Par défaut, l'authentification LDAP est sécurisée à l'aide de Secure Sockets Layer (SSL) ou de Transport Layer Security (TLS). Il existe deux types de connexions LDAP sécurisées. Avec un type, le serveur LDAP accepte les connexions SSL ou TLS sur un port distinct du port utilisé par le serveur LDAP pour accepter les connexions LDAP claires. Une fois que les utilisateurs ont établi les connexions SSL ou TLS, le trafic LDAP peut être envoyé via la connexion.

Les numéros de port des connexions LDAP sont les suivants :

- 389 pour les connexions LDAP non sécurisées
- 636 pour les connexions LDAP sécurisées
- 3268 pour les connexions LDAP non sécurisées Microsoft
- 3269 pour les connexions LDAP sécurisées Microsoft

Le deuxième type de connexions LDAP sécurisées utilise la commande StartTLS et utilise le numéro de port 389. Si vous configurez les numéros de port 389 ou 3268 sur NetScaler Gateway, le serveur essaie d'utiliser StartTLS pour établir la connexion. Si vous utilisez un autre numéro de port, le serveur tente d'établir des connexions en utilisant SSL ou TLS. Si le serveur ne peut pas utiliser StartTLS, SSL ou TLS, la connexion échoue.

Si vous spécifiez le répertoire racine du serveur LDAP, NetScaler Gateway recherche l'attribut utilisateur dans tous les sous-répertoires. Dans les grands répertoires, cette approche peut affecter les performances. Pour cette raison, Citrix vous recommande d'utiliser une unité d'organisation spécifique.

Le tableau suivant contient des exemples de champs d'attribut utilisateur pour les serveurs LDAP :

serveur LDAP	Attribut utilisateur	Sensibles à
Serveur Microsoft Active Directory	sAMAccountName	Non
Novell eDirectory	ou	Oui
IBM Directory Server	uid	Oui
Lotus Domino	CN	Oui
Sun ONE directory (anciennement iPlanet)	uid ou cn	Oui

Ce tableau contient des exemples de nom unique de base :

serveur LDAP	DN de base
Serveur Microsoft Active Directory	DC =citrix, DC = local
Novell eDirectory	ou=users, ou=dev
IBM Directory Server	cn=utilisateurs
Lotus Domino	OU=ville, O=Citrix, C = États-Unis
Sun ONE directory (anciennement iPlanet)	OU=personnes, dc =citrix, dc = com

Le tableau suivant contient des exemples de nom unique de liaison :

serveur LDAP	DN de liaison
Serveur Microsoft Active Directory	CN = administrateur, CN = utilisateurs, DC =citrix, DC = local
Novell eDirectory	cn=admin, o=citrix
IBM Directory Server	LDAP_DN
Lotus Domino	CN=Notes Administrateur, O=Citrix, C=US
Sun ONE directory (anciennement iPlanet)	uid=admin,ou=Administrators, ou=TopologyManagement,o=NetscapeRoot

Remarque : Pour plus d'informations sur les paramètres du serveur LDAP, consultez la section Détermination des attributs dans votre annuaire LDAP.

Pour configurer l'authentification LDAP à l'aide de l'utilitaire de configuration

March 27, 2024

1. Accédez à **NetScaler Gateway** > **Policies** > **Authentification**.
2. Cliquez sur **LDAP**.
3. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
4. Dans **Nom**, tapez le nom de la politique.
5. À côté de **Serveur**, cliquez sur **Nouveau**.

6. Dans **Nom**, tapez le nom du serveur.
7. Sous **Serveur**, dans **Adresse IP et port**, tapez l'adresse IP et le numéro de port du serveur LDAP.
8. Dans **Type**, sélectionnez **AD** pour Active Directory ou **NDS** pour Novell Directory Services.
9. Sous **Paramètres de connexion**, effectuez les opérations suivantes :

   a) Dans **Nom unique de base (emplacement des utilisateurs)**, tapez le nom unique de base sous lequel se trouvent les utilisateurs. Le nom unique de base recherche les utilisateurs situés dans le répertoire sélectionné (AD ou NDS).

   Le nom unique de base est dérivé du nom unique de liaison en supprimant le nom d'utilisateur et en spécifiant le groupe dans lequel se trouvent les utilisateurs. Voici des exemples de syntaxe pour le nom unique de base :

   ```
   ou=users,dc=ace,dc=com
   cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   b) Dans **Administrator Bind DN**, tapez le nom unique de liaison de l'administrateur pour les requêtes adressées à l'annuaire LDAP. Voici des exemples de syntaxe du nom unique de liaison :

   ```
   domain/user name
   ou=administrator,dc=ace,dc=com
   user@domain.name (for Active Directory)
   cn=Administrator,cn=Users,dc=ace,dc=com
   <!--NeedCopy-->
   ```

   Pour Active Directory, le nom de groupe spécifié comme cn=groupname est requis. Le nom du groupe que vous définissez dans NetScaler Gateway et le nom du groupe sur le serveur LDAP doivent être identiques.

   Pour les autres répertoires LDAP, le nom du groupe n'est pas obligatoire ou, si nécessaire, est spécifié comme ou=groupname.

   NetScaler Gateway se lie au serveur LDAP à l'aide des informations d'identification de l'administrateur, puis recherche l'utilisateur. Après avoir localisé l'utilisateur, NetScaler Gateway dissocie les informations d'identification de l'administrateur et les associe de nouveau aux informations d'identification de l'utilisateur.

   c) Dans les **champs Mot de passe administrateur et Confirmer le mot de passe**administrateur, tapez le mot de passe administrateur du serveur LDAP.

10. Pour récupérer automatiquement d'autres paramètres LDAP, cliquez sur **Récupérer les attributs**.

    Lorsque vous cliquez sur **Récupérer les attributs**, les champs situés sous Autres paramètres

sont automatiquement renseignés. Si vous souhaitez ignorer cette étape, passez aux étapes 12 et 13. Sinon, passez directement à l'étape 14.

11. Sous **Autres paramètres**, dans Attribut du nom de connexion au serveur, tapez l'attribut sous lequel NetScaler Gateway doit rechercher les noms de connexion des utilisateurs pour le serveur LDAP que vous configurez. La valeur par défaut est `samAccountName`.
12. Dans **Filtre de recherche**, tapez la valeur pour rechercher les utilisateurs associés à un ou plusieurs groupes Active Directory.

    Par exemple, « MemberOf=CN=GatewayAccess, OU=Groups, DC=Users, DC=Lab ».

    > **Remarque**
    >
    > Vous pouvez utiliser l'exemple précédent pour restreindre l'accès à NetScaler Gateway uniquement aux membres d'un groupe AD spécifique.

13. Dans **Attribut de groupe**, conservez le membre par défaut d'Active Directory ou remplacez l'attribut par l'attribut du type de serveur LDAP que vous utilisez. Cet attribut permet à NetScaler Gateway d'obtenir les groupes associés à un utilisateur lors de l'autorisation.
14. Dans Type **de sécurité**, sélectionnez le type de sécurité, puis cliquez sur **Créer**.
15. Pour autoriser les utilisateurs à modifier leur mot de passe LDAP, sélectionnez **Autoriser la modification du mot de passe**.

    Remarque :

    - Si vous sélectionnez **PLAINTEXT** comme type de sécurité, l'autorisation des utilisateurs de modifier leurs mots de passe n'est pas prise en charge.
    - Si vous sélectionnez **PLAINTEXT** ou **TLS** pour la sécurité, utilisez le numéro de port 389. Si vous sélectionnez **SSL**, utilisez le numéro de port 636.

Déterminer les attributs de votre annuaire LDAP

March 27, 2024

Si vous avez besoin d'aide pour déterminer vos attributs d'annuaire LDAP afin de pouvoir configurer les paramètres d'authentification sur NetScaler Gateway, vous pouvez facilement les rechercher avec le navigateur LDAP gratuit de Softerra.

Vous pouvez télécharger le navigateur LDAP à partir du site Web de Softerra LDAP Administrator. Après avoir installé le navigateur, définissez les attributs suivants :

- Le nom d'hôte ou l'adresse IP de votre serveur LDAP.

- Le port de votre serveur LDAP. La valeur par défaut est 389.
- Le champ DN de base, que vous pouvez laisser vide. Les informations fournies par le navigateur LDAP peuvent vous aider à déterminer le DN de base sur lequel vous devez configurer ce paramètre sur NetScaler Gateway.
- La vérification de liaison anonyme détermine si le serveur LDAP a besoin des informations d'identification de l'utilisateur pour se connecter à celui-ci. Si le serveur LDAP nécessite des informations d'identification, laissez la case à cocher désactivée.

Après avoir terminé les paramètres, le navigateur LDAP affiche le nom du profil dans le volet gauche et se connecte au serveur LDAP.

Configuration de l'extraction de groupes LDAP

January 26, 2024

Si vous utilisez l'authentification à deux facteurs, les groupes extraits des sources d'authentification principale et secondaire sont concaténés. Les stratégies d'autorisation peuvent être appliquées au groupe extrait du serveur d'authentification principal ou secondaire.

Les noms de groupe obtenus à partir du serveur LDAP sont comparés aux noms de groupe créés localement sur NetScaler Gateway. Si les deux noms de groupe correspondent, les propriétés du groupe local s'appliquent au groupe obtenu à partir des serveurs LDAP.

Si les utilisateurs appartiennent à plusieurs groupes LDAP, NetScaler Gateway extrait les informations utilisateur de tous les groupes auxquels les utilisateurs appartiennent. Si un utilisateur est membre de deux groupes sur NetScaler Gateway et que chaque groupe possède une stratégie de session liée, l'utilisateur hérite des stratégies de session des deux groupes. Pour vous assurer que les utilisateurs reçoivent la stratégie de session correcte, définissez la priorité de la stratégie de session.

Pour plus d'informations sur les attributs d'appartenance à un groupe LDAP, consultez les sections suivantes :

- Fonctionnement direct de l'extraction de groupe LDAP à partir de l'objet utilisateur
- Fonctionnement indirectement de l'extraction de groupe LDAP à partir de l'objet de groupe

Fonctionnement direct de l'extraction de groupe LDAP à partir de l'objet utilisateur

January 26, 2024

Les serveurs LDAP qui évaluent les appartenances à des groupes à partir d'objets de groupe prennent en charge l'autorisation NetScaler Gateway.

Certains serveurs LDAP permettent aux objets utilisateur de contenir des informations sur les groupes auxquels les objets appartiennent, tels qu'Active Directory (à l'aide de l'attribut MemberOf) ou IBM eDirectory (à l'aide de l'attribut GroupMembership). L'appartenance au groupe d'un utilisateur peut être des attributs de l'objet utilisateur, tels qu'IBM Directory Server (à l'aide d'IBM-AllGroups) ou le serveur d'annuaire Sun ONE (à l'aide de NSRole). Ces deux types de serveurs LDAP prennent en charge l'extraction de groupes NetScaler Gateway.

Par exemple, dans IBM Directory Server, toutes les appartenances aux groupes, y compris les groupes statiques, dynamiques et imbriqués, peuvent être renvoyées à l'aide de l'attribut IBM-AllGroups. Dans Sun ONE, tous les rôles, y compris les rôles gérés, filtrés et imbriqués, sont calculés à l'aide de l'attribut NSRole.

Fonctionnement indirectement de l'extraction de groupe LDAP à partir de l'objet de groupe

January 26, 2024

Les serveurs LDAP qui évaluent indirectement les appartenances à des groupes à partir d'objets de groupe ne sont pas compatibles avec l'autorisation NetScaler Gateway.

Certains serveurs LDAP, tels que Lotus Domino, n'autorisent les objets de groupe qu'à contenir des informations sur les utilisateurs. Ces serveurs LDAP ne permettent pas à l'objet utilisateur de contenir des informations sur les groupes et ne sont donc pas compatibles avec l'extraction de groupes par NetScaler Gateway. Pour ce type de serveur LDAP, les recherches d'appartenance à un groupe sont effectuées en localisant l'utilisateur dans la liste des membres des groupes.

Champs d'attribut du groupe d'autorisations LDAP

January 26, 2024

Le tableau suivant contient des exemples de champs attributaires de groupe LDAP :

Serveurs LDAP	Attribut LDAP
Serveur Microsoft Active Directory	memberOf

Serveurs LDAP	Attribut LDAP
Novell eDirectory	groupMembership
IBM Directory Server	ibm-allGroups
Sun ONE directory (anciennement iPlanet)	nsRole

Pour configurer l'autorisation LDAP

March 27, 2024

Vous configurez l'autorisation LDAP dans la stratégie d'authentification en définissant le nom de l'attribut de groupe et le sous-attribut.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Sous Authentification, cliquez sur un type d'authentification.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans Nom, tapez le nom de la stratégie.
5. À côté de Serveur, cliquez sur Nouveau.
6. Dans Nom, tapez le nom du serveur.
7. Sous Serveur, tapez l'adresse IP et le port du serveur LDAP.
8. Dans Attribut de groupe, saisissez MemberOf.
9. Dans Nom du sous-attribut, tapez CN, puis cliquez sur Créer.
10. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez l'expression, cliquez sur Ajouter une expression, cliquez sur Créer, puis sur Fermer.

Configuration de l'extraction des groupes imbriqués LDAP

March 27, 2024

NetScaler Gateway peut interroger des groupes LDAP et extraire des informations sur les groupes et les utilisateurs à partir des groupes ancêtres que vous configurez sur le serveur d'authentification. Par exemple, vous avez créé group1 et au sein de ce groupe, vous avez créé group2 et group3. Si l'utilisateur appartient au groupe 3, NetScaler Gateway extrait les informations de tous les groupes d'ancêtres imbriqués (groupe2, groupe1) jusqu'au niveau spécifié.

Vous pouvez utiliser une stratégie d'authentification pour configurer l'extraction de groupes imbriqués LDAP. Lorsque la requête est exécutée, NetScaler Gateway recherche les groupes jusqu'à atteindre le niveau d'imbrication maximal ou jusqu'à ce qu'il recherche tous les groupes disponibles.

Pour configurer l'extraction de groupes imbriqués LDAP

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies > Authentification/Authorization > Authentication >** Authentification, puis cliquez sur **LDAP**.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Serveur, cliquez sur **Nouveau**.
5. Dans Nom, tapez le nom du serveur.
6. Configurez les paramètres du serveur LDAP.
7. Développez **Extraction de groupes imbriqués**, puis cliquez sur **Activer**.
8. Dans **Niveau d'imbrication maximal**, tapez le nombre de niveaux que NetScaler Gateway vérifie.
9. Dans **Group Name Identifier**, tapez le nom de l'attribut LDAP qui identifie de manière unique un nom de groupe sur le serveur LDAP, par exemple `sAMAccountName`.
10. Dans **Attribut de recherche de groupe**, tapez le nom de l'attribut LDAP à obtenir dans la réponse de recherche pour déterminer les groupes parents de n'importe quel groupe. Par exemple, `memberOf`.
11. Dans **Sous-attribut de recherche de groupe**, tapez le nom du sous-attribut LDAP à rechercher dans le cadre de l'attribut de recherche de groupe pour déterminer les groupes parents de n'importe quel groupe. Par exemple, saisissez CN.
12. Dans **Filtre de recherche de groupe**, tapez la chaîne de requête. Par exemple, le filtre peut être `&(samaccountname=test)(objectClass=\*)`.
13. Cliquez sur **Créer**, puis sur **Fermer**.
14. Dans la boîte de dialogue Créer une politique d'authentification, à côté de Expressions nommées, sélectionnez l'expression, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Configuration de l'extraction de groupes LDAP pour plusieurs domaines

January 26, 2024

Si vous disposez de plusieurs domaines pour l'authentification et que vous utilisez StoreFront ou l'interface Web, vous pouvez configurer NetScaler Gateway pour utiliser l'extraction de groupe afin d'envoyer le nom de domaine correct à l'interface Web.

Dans Active Directory, vous devez créer un groupe pour chaque domaine de votre réseau. Après avoir créé le groupe, vous ajoutez des utilisateurs qui appartiennent au groupe et au domaine spécifié. Une fois les groupes configurés dans Active Directory, vous configurez l'extraction de groupes LDAP pour plusieurs domaines sur NetScaler Gateway.

Pour configurer NetScaler Gateway pour l'extraction de groupes pour plusieurs domaines, vous devez créer le même nombre de stratégies de session et d'authentification que le nombre de domaines de votre réseau. Par exemple, vous disposez de deux domaines, nommé Sampa et Child. Chaque domaine reçoit une stratégie de session et une stratégie d'authentification.

Après avoir créé les stratégies, vous créez des groupes sur NetScaler Gateway et vous liez les stratégies de session au groupe. Ensuite, vous liez les stratégies d'authentification à un serveur virtuel.

Si vous déployez StoreFront dans plusieurs domaines, il doit exister une relation d'approbation entre les domaines.

Si vous déployez Citrix Endpoint Management ou l'interface Web dans plusieurs domaines, les domaines n'ont pas besoin de se faire confiance.

Création de stratégies de session pour l'extraction de groupes

March 27, 2024

La première étape de la création de stratégies de session pour l'extraction de groupes consiste à créer deux profils de session et à définir les paramètres suivants :

- Activez le proxy ICA.
- Ajoutez l'adresse Web de l'interface Web.
- Ajoutez le domaine Windows.
- Ajoutez le profil à une stratégie de session et définissez l'expression sur true.

Pour créer les profils de session pour l'extraction de groupes

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, cliquez sur l'onglet **Profils**, puis sur **Ajouter**.
3. Dans **Nom**, saisissez le nom du profil. Par exemple, tapez Sampa.
4. Dans l'onglet **Applications publiées**, procédez comme suit :

a) À côté de **ICA Proxy**, cliquez sur **Override Global**, puis sélectionnez **ON**.
b) À côté de **Adresse de l'interface Web**, cliquez sur **Remplacer l'adresse globale**, puis tapez l'adresse Web de l'interface Web.
c) En regard de **Single Sign-On Domain (Domaine**d'authentification unique), cliquez sur **Override Global**, tapez le nom du domaine Windows, puis cliquez sur **Create (Créer**).

5. Dans **Nom**, effacez le nom du premier domaine et saisissez le nom du second domaine, par exemple Child.
6. En regard de **Domaine d'authentification unique**, effacez le nom du premier domaine Windows et tapez le nom du deuxième domaine, cliquez sur **Créer,** puis sur **Fermer**.

Après avoir créé les profils de session, vous créez deux stratégies de session. Chaque stratégie de session utilise l'un des profils.

Pour créer une stratégie de session

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. Dans **Demande de profil**, sélectionnez le profil du premier domaine.
5. En regard de **Expressions nommées**, cliquez sur **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression,** puis cliquez sur **Créer**.
6. Dans **Nom**, remplacez le nom par le second domaine.
7. Dans **Demander un profil**, sélectionnez le profil du deuxième domaine, cliquez sur **Créer,** puis cliquez sur **Fermer**.

Création de stratégies d'authentification LDAP pour plusieurs domaines

March 27, 2024

Une fois que vous avez créé des stratégies de session sur NetScaler Gateway, vous créez des stratégies d'authentification LDAP quasiment identiques. Lors de la configuration de la stratégie d'authentification, le champ important est le filtre
de recherche. Dans ce champ, vous devez taper le nom du groupe que vous avez créé dans Active Directory.

Créez d'abord les profils d'authentification, puis créez la stratégie d'authentification.

Pour créer des profils d'authentification pour plusieurs extractions de groupes de domaines

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez Citrix **Gateway > Politiques > Authentification**.
2. Dans le panneau de navigation, cliquez sur **LDAP**.
3. Dans le volet d'informations, cliquez sur l'onglet **Serveurs**, puis sur **Ajouter**.
4. Dans **Nom**, tapez le nom du premier domaine, par exemple `Sampa`.
5. Configurez les paramètres du serveur LDAP, puis cliquez sur **Créer**.
6. Répétez les étapes 3, 4 et 5 pour configurer le profil d'authentification du deuxième domaine, puis cliquez sur **Fermer**.

Après avoir créé et enregistré les profils, créez les stratégies d'authentification.

Pour créer des stratégies d'authentification pour plusieurs extractions de groupes de domaines

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Dans le volet d'informations, cliquez sur l'onglet **Stratégies**, puis sur **Ajouter**.
3. Dans **Nom**, tapez le nom du premier domaine.
4. Dans **Type d'authentification**, sélectionnez **LDAP**.
5. Dans **Serveur**, sélectionnez le profil d'authentification pour le premier domaine.
6. En regard de **Expressions nommées**, cliquez sur **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression,** puis cliquez sur **Créer**.
7. Dans Nom, tapez le nom du deuxième domaine.
8. Dans **Serveur**, sélectionnez le profil d'authentification du deuxième domaine, cliquez sur **Créer,** puis sur **Fermer**.

Création de groupes et de stratégies de liaison pour l'extraction de groupes LDAP pour plusieurs domaines

March 27, 2024

Après avoir créé des stratégies d'authentification, vous créez des groupes sur NetScaler Gateway. Après avoir créé les groupes, vous liez la stratégie d'authentification à un serveur virtuel.

Pour créer des groupes sur NetScaler Gateway

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, ouvrez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **AAA Groups**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom du groupe**, tapez le nom du premier groupe Active Directory.
   Important : lors de la création de groupes sur NetScaler Gateway pour l'extraction de groupes à partir de plusieurs domaines, les noms des groupes doivent être identiques à ceux que vous avez définis dans Active Directory. Les noms de groupes sont également sensibles à la casse et la casse doit correspondre à la casse que vous avez entrée dans Active Directory.
4. Dans l'onglet **Stratégies**, cliquez sur **Session**, puis sur **Insérer une stratégie**.
5. Sous **Nom de la stratégie**, double-cliquez sur la stratégie, puis cliquez sur **Créer**.

Pour lier les stratégies d'authentification à un serveur virtuel

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Virtual Servers.**
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet Authentification, cliquez sur **Principal**, sous **Nom de la stratégie**, double-cliquez sur **Insérer une stratégie**, puis sélectionnez la première stratégie d'authentification.
4. Sous **Nom de la stratégie**, cliquez sur **Insérer une stratégie**, double-cliquez sur la deuxième stratégie d'authentification, puis cliquez sur **OK**.

Notification d'expiration de 14 jours pour l'authentification LDAP

January 26, 2024

L'appliance NetScaler Gateway prend en charge la notification d'expiration des mots de passe de 14 jours pour l'authentification basée sur LDAP. En utilisant cette fonctionnalité, les administrateurs peuvent informer les utilisateurs finaux du délai d'expiration du mot de passe en jours. Pour plus de détails, consultez Notification d'expiration du mot de passe de 14 jours pour l'authentification LDAP

Configuration de l'authentification du certificat client

January 26, 2024

Les utilisateurs qui se connectent à un serveur virtuel NetScaler Gateway peuvent également être authentifiés en fonction des attributs du certificat client présentés au serveur virtuel. L'authentification par certificat client peut également être utilisée avec d'autres types d'authentification, tels que LDAP ou RADIUS, pour fournir une authentification à deux facteurs.

Pour authentifier les utilisateurs en fonction des attributs de certificat côté client, l'authentification du client doit être activée sur le serveur virtuel et le certificat client doit être demandé. Vous devez lier un certificat racine au serveur virtuel sur NetScaler Gateway.

Lorsque les utilisateurs ouvrent une session sur le serveur virtuel NetScaler Gateway, après l'authentification, les informations sur le nom d'utilisateur sont extraites à partir du champ spécifié du certificat. Ce champ est généralement Subject:CN. Si le nom d'utilisateur est extrait avec succès, l'utilisateur est authentifié. L'authentification échoue dans les cas suivants.

- Si l'utilisateur ne fournit pas de certificat valide pendant la prise de liaison SSL (Secure Sockets Layer).
- L'extraction du nom d'utilisateur échoue, l'authentification échoue.

Vous pouvez authentifier les utilisateurs en fonction du certificat client en définissant le type d'authentification par défaut de manière à utiliser le certificat client. Vous pouvez également créer une action de certificat dont la tâche est de définir les opérations à réaliser durant l'authentification basée sur un certificat client SSL.

Pour configurer le certificat client en tant que type d'authentification par défaut à l'aide de l'interface graphique

1. Accédez à **Configuration > NetScaler Gateway,** puis cliquez sur Paramètres **généraux**.
2. Dans le volet d'informations, sous **Paramètres d'authentification**, cliquez sur **Modifier les paramètres du certificat d'authentification**.
3. Sélectionnez **ON** pour activer l'authentification à deux facteurs à l'aide du certificat, conformément à vos besoins.
4. Dans **Champ de nom d'utilisateur**, sélectionnez le type de champ de certificat qui contient les noms d'utilisateurs.
5. Dans **Champ de nom de groupe**, sélectionnez le type du champ de certificat qui contient le nom du groupe.
6. Dans **Groupe d'autorisations par défaut**, tapez le nom du groupe par défaut, puis cliquez sur **OK**.

Extraction du nom d'utilisateur du certificat client

Si l'authentification par certificat client est activée sur NetScaler Gateway, les utilisateurs sont authentifiés en fonction de certains attributs du certificat client. Une fois l'authentification réussie, le

nom d'utilisateur ou le nom d'utilisateur et de groupe de l'utilisateur sont extraits du certificat. Les stratégies spécifiées pour cet utilisateur sont également appliquées.

Configuration et liaison d'une stratégie d'authentification de certificat client

March 27, 2024

Vous pouvez créer une stratégie d'authentification de certificat client et la lier à un serveur virtuel. Vous pouvez utiliser la stratégie pour restreindre l'accès à des groupes ou utilisateurs spécifiques. Cette stratégie est prioritaire sur la stratégie globale.

Pour configurer une stratégie d'authentification de certificat client :

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Dans le volet de navigation, sous **Authentification**, cliquez sur **CERT**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans le champ **Nom**, saisissez le nom de la stratégie.
5. À côté de **Serveur**, cliquez sur **Nouveau**.
6. Dans **Nom**, saisissez le nom du profil.
7. En regard de **Deux facteurs**, sélectionnez **DÉSACTIVÉ**.
8. Dans les champs **Nom d'utilisateur** et **Nom de groupe**, sélectionnez les valeurs, puis cliquez sur**Créer**.
   Remarque : Si vous avez déjà configuré des certificats clients comme type d'authentification par défaut, utilisez les mêmes noms que ceux que vous avez utilisés pour la stratégie. Si vous avez renseigné les champs Nom
   d'utilisateur et Nom de
   groupe pour le type d'authentification par défaut, utilisez les mêmes valeurs pour le profil.
9. Dans la boîte de dialogue **Créer une stratégie d'authentification**, en regard de **Expressions nommées**, sélectionnez l'expression, cliquez sur **Ajouter une expression**, cliquez sur **Créer**, puis sur **Fermer**.

Pour lier une stratégie de certificat client à un serveur virtuel, procédez comme suit :

Après avoir configuré la stratégie d'authentification du certificat client, vous pouvez la lier à un serveur virtuel.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis sur **Ouvrir**.

3. **Dans la boîte de dialogue Configurer le**serveur virtuel NetScaler Gateway**, cliquez sur l'onglet Authentification.**
4. Cliquez sur **Primary** ou **Secondary**.
5. Sous **Détails**, cliquez sur **Insérer une stratégie**.
6. Dans **Nom de la stratégie**, sélectionnez la stratégie, puis cliquez sur **OK**.

Pour configurer un serveur virtuel afin qu'il demande le certificat client, procédez comme suit :

Lorsque vous souhaitez utiliser un certificat client pour l'authentification, vous devez configurer le serveur virtuel de manière à ce que les certificats clients soient demandés lors de l'établissement de liaison SSL.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un **serveur virtuel**, puis cliquez sur **Ouvrir**.
3. Dans l'onglet **Certificats**, cliquez sur **Paramètre SSL**.
4. Sous **Autres**, cliquez sur **Authentification du client**.
5. Dans **Certificat client**, sélectionnez **Facultatif** ou **Obligatoire**, puis cliquez deux fois sur OK. Sélectionnez **Facultatif** si vous souhaitez autoriser d'autres types d'authentification sur le même serveur virtuel sans nécessiter l'utilisation de certificats clients.

> **Remarque**
>
> - Pour plus d'informations sur l'URL de rappel, consultez Importer un NetScaler Gateway.
> - Pour plus d'informations sur les certificats, consultez Installer, lier et mettre à jour des certificats.

Configuration de l'authentification par certificat client à deux facteurs

January 26, 2024

Vous pouvez configurer un certificat client pour authentifier d'abord les utilisateurs, puis demander aux utilisateurs d'ouvrir une session avec un type d'authentification secondaire, tel que LDAP ou RADIUS. Dans ce scénario, le certificat client authentifie d'abord les utilisateurs. Ensuite, une page de connexion apparaît où ils peuvent entrer leur nom d'utilisateur et leur mot de passe. Lorsque la connexion SSL (Secure Sockets Layer) est terminée, la séquence d'ouverture de session peut prendre l'un des deux chemins suivants :

- Ni le nom d'utilisateur ni le groupe ne sont extraits du certificat. La page de connexion apparaît à l'utilisateur et invite l'utilisateur à entrer des informations d'identification de connexion valides. NetScaler Gateway authentifie les informations d'identification de l'utilisateur comme dans le cas d'une authentification par mot de passe normale.

- Le nom d'utilisateur et le nom du groupe sont extraits du certificat client. Si seul le nom d'utilisateur est extrait, une page de connexion apparaît à l'utilisateur dans laquelle le nom d'ouverture de session est présent et l'utilisateur ne peut pas modifier le nom. Seul le champ du mot de passe est vide.

Les informations de groupe que NetScaler Gateway extrait lors du deuxième cycle d'authentification sont ajoutées aux informations de groupe, le cas échéant, que NetScaler Gateway a extraites du certificat.

Configuration de l'authentification par carte à puce

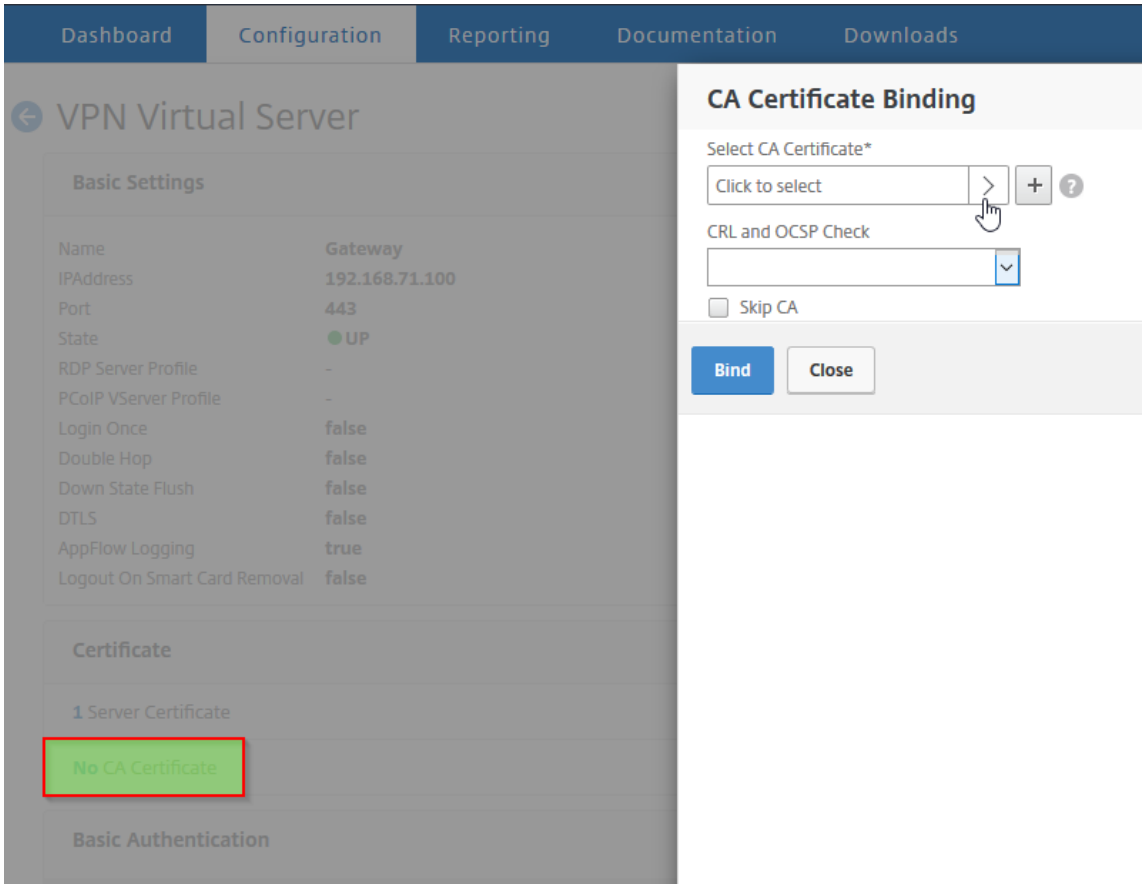
March 27, 2024

Vous pouvez configurer NetScaler Gateway pour qu'il utilise une carte à puce cryptographique pour authentifier les utilisateurs.

Pour configurer une carte à puce avec NetScaler Gateway, procédez comme suit :

- Créez une stratégie d'authentification de certificat. Pour plus d'informations, consultez la section Configuration de l'authentification du certificat client.
- Liez la stratégie d'authentification à un serveur virtuel.
- Ajoutez le certificat racine de l'autorité de certification (CA) qui émet les certificats clients à NetScaler Gateway. Pour de plus amples informations, consultez la section Pour installer un certificat racine sur NetScaler Gateway.

  Important : Lorsque vous ajoutez le certificat racine au serveur virtuel pour l'authentification par carte à puce, vous devez sélectionner le certificat dans la liste **Sélectionner un certificat d'autorité** de certification.



Après avoir créé le certificat client, vous pouvez écrire le certificat, appelé Flash, sur la carte à puce. Une fois cette étape terminée, vous pouvez tester la carte à puce.

Si vous configurez l'interface Web pour l'authentification relais par carte à puce, si l'une des conditions suivantes existe, l'authentification unique à l'interface Web échoue :

- Si vous définissez plutôt le domaine sous l'onglet **Applications publiées** sur `mydomain`.com `mydomain`.
- Si vous ne définissez pas le nom de domaine dans l'onglet **Applications publiées** et si vous exécutez la commande `wi-sso-split-upn` définissant la valeur sur 1. Dans ce cas, UserPrincipalName contient le nom de domaine «`mydomain`.com. »

Vous pouvez utiliser l'authentification par carte à puce pour simplifier le processus d'ouverture de session de vos utilisateurs tout en améliorant la sécurité de l'accès des utilisateurs à votre infrastructure. L'accès au réseau interne de l'entreprise est protégé par une authentification à deux facteurs basée sur un certificat à l'aide de l'infrastructure à clé publique. Les clés privées sont protégées par des contrôles matériels et ne quittent jamais la carte à puce. Vos utilisateurs bénéficient d'un accès à leurs bureaux et applications à partir d'une large gamme de périphériques d'entreprise à l'aide de leurs cartes à puce et codes PIN.

Vous pouvez utiliser des cartes à puce pour l'authentification utilisateur via StoreFront aux bureaux et

applications fournis par Citrix Virtual Apps and Desktops. Les utilisateurs de cartes à puce qui se connectent à StoreFront peuvent également accéder aux applications fournies par NetScaler Endpoint Management. Toutefois, les utilisateurs doivent s'authentifier à nouveau pour accéder aux applications Web Endpoint Management qui utilisent l'authentification par certificat client.

Pour plus d'informations, consultez Configurer l'authentification par carte à puce dans la documentation StoreFront.

Configuration de l'authentification par carte à puce avec des connexions ICA sécurisées

Les utilisateurs qui se connectent et établissent une connexion ICA sécurisée à l'aide d'une carte à puce avec authentification unique configurée sur NetScaler Gateway peuvent être invités à saisir leur numéro d'identification personnel (PIN) à deux reprises.

- Lorsque vous ouvrez une session et que vous essayez de démarrer une ressource publiée. Cette situation se produit si le navigateur Web et l'application Citrix Workspace utilisent le même serveur virtuel configuré pour utiliser les certificats client.
- L'application Citrix Workspace ne partage pas de processus ni de connexion SSL (Secure Sockets Layer) avec le navigateur Web. Par conséquent, lorsque la connexion ICA termine l'établissement de liaison SSL avec NetScaler Gateway, le certificat client est requis une seconde fois.

Pour empêcher les utilisateurs de recevoir la deuxième invite de code PIN, vous devez modifier deux paramètres :

- L'authentification du client sur le serveur virtuel VPN doit être désactivée.
- La renégociation SSL doit être activée.

Après avoir configuré le serveur virtuel, liez un ou plusieurs serveurs STA au serveur virtuel, comme décrit dans la section Configuration des paramètres de NetScaler Gateway dans l'interface Web 5.3.

Vous pouvez également tester l'authentification par carte à puce.

Pour désactiver l'authentification client :

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Sélectionnez le serveur virtuel approprié dans le volet de détails principal, puis cliquez sur Modifier.
3. Dans le volet Options avancées, cliquez sur Paramètres SSL.
4. Décochez la case Authentification du client.
5. Cliquez sur Terminé.

Pour activer la renégociation SSL :

1. À l'aide de l'utilitaire de configuration, dans l'onglet Configuration, accédez à Gestion du trafic, puis cliquez sur SSL.
2. Dans le panneau principal, cliquez sur Modifier les paramètres SSL avancés.
3. Dans le menu Refuser la renégociation SSL, sélectionnez NON.

Pour tester l'authentification par carte à puce :

1. Connectez la carte à puce à la machine utilisateur.
2. Ouvrez votre navigateur Web et connectez-vous à NetScaler Gateway.

Configuration de l'authentification RADIUS

January 26, 2024

Vous pouvez configurer NetScaler Gateway pour authentifier l'accès des utilisateurs à un ou plusieurs serveurs RADIUS. Si vous utilisez des produits RSA SecurID, SafeWord ou Gemalto Protiva, chacun de ces produits est configuré à l'aide d'un serveur RADIUS.

Votre configuration peut nécessiter l'utilisation d'une adresse IP du serveur d'accès réseau (IP NAS) ou d'un identifiant de serveur d'accès réseau (ID NAS). Lorsque vous configurez NetScaler Gateway pour utiliser un serveur d'authentification RADIUS, suivez les instructions suivantes :

- Si vous activez l'utilisation de l'adresse IP du NAS, l'appliance envoie son adresse IP configurée au serveur RADIUS, plutôt que l'adresse IP source utilisée pour établir la connexion RADIUS.
- Si vous configurez l'ID NAS, l'appliance envoie l'identificateur au serveur RADIUS. Si vous ne configurez pas l'ID NAS, l'appliance envoie son nom d'hôte au serveur RADIUS.
- Lorsque vous activez l'adresse IP du NAS, l'appliance ignore tout ID NAS configuré à l'aide de l'adresse IP du NAS pour communiquer avec le serveur RADIUS.

Configuration de Gemalto Protiva

Protiva est une plateforme d'authentification forte que Gemalto a développée pour exploiter les points forts de l'authentification par carte à puce de Gemalto. Avec Protiva, les utilisateurs ouvrent une session avec un nom d'utilisateur, un mot de passe et un mot de passe unique générés par l'appareil Protiva. Comme pour RSA SecurID, la demande d'authentification est envoyée au serveur d'authentification Protiva et le serveur valide ou rejette le mot de passe. Pour configurer Gemalto Protiva afin qu'il soit compatible avec NetScaler Gateway, suivez les instructions suivantes :

- Installez le serveur Protiva.

- Installez le logiciel Protiva SAS Agent, qui étend le serveur d'authentification Internet (IAS), sur un serveur RADIUS Microsoft IAS. N'oubliez pas de noter l'adresse IP et le numéro de port du serveur IAS.
- Configurez un profil d'authentification RADIUS sur NetScaler Gateway et entrez les paramètres du serveur Protiva.

Configuration de SafeWord

La gamme de produits SafeWord fournit une authentification sécurisée à l'aide d'un code secret basé sur des jetons. Une fois que l'utilisateur a saisi le code d'accès, SafeWord l'invalide immédiatement et il ne peut plus être utilisé. Lorsque vous configurez le serveur SafeWord, vous avez besoin des informations suivantes :

- Adresse IP de NetScaler Gateway. L'adresse IP doit être la même que celle que vous avez configurée dans la configuration du client du serveur RADIUS. NetScaler Gateway utilise l'adresse IP interne pour communiquer avec le serveur RADIUS. Lorsque vous configurez le secret partagé, utilisez l'adresse IP interne. Si vous configurez deux dispositifs pour la haute disponibilité, utilisez l'adresse IP interne virtuelle.
- Un secret commun.
- L'adresse IP et le port du serveur SafeWord. Le numéro de port par défaut est 1812.

Pour configurer l'authentification RADIUS

March 27, 2024

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Cliquez sur RADIUS, puis dans le volet d'informations, sous l'onglet Stratégies, cliquez sur Ajouter.
3. Dans la boîte de dialogue Créer une politique d'authentification, dans Nom, tapez le nom de la stratégie.
4. Dans Nom, tapez le nom de la stratégie.
5. À côté de Serveur, cliquez sur Nouveau.
6. Dans la boîte de dialogue Créer une stratégie d'authentification, dans Nom, tapez un nom pour le serveur.
7. Sous Serveur, dans Adresse IP, tapez l'adresse IP du serveur RADIUS.
8. Dans Port, tapez le port. La valeur par défaut est 1812.

9. Sous Détails, dans Clé secrète et Confirmation de la clé secrète, tapez le secret du serveur RADIUS.
10. Dans NAS ID, tapez le numéro d'identification, puis cliquez sur Créer.
11. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez l'expression, cliquez sur Ajouter une expression, cliquez sur Créer, puis sur Fermer.

Choix des protocoles d'authentification RADIUS

January 26, 2024

NetScaler Gateway prend en charge les implémentations de RADIUS configurées pour utiliser plusieurs protocoles d'authentification des utilisateurs, notamment :

- Protocole d'authentification par mot de passe (PAP)
- Protocole CHAP (Challenge-Handshake Authentication Protocol)
- Protocole d'authentification Microsoft Challenge-Handshake (MS-CHAP version 1 et version 2)

Si votre déploiement de NetScaler Gateway est configuré pour utiliser l'authentification RADIUS et que votre serveur RADIUS est configuré pour utiliser PAP, vous pouvez renforcer l'authentification des utilisateurs en attribuant un secret partagé renforcé au serveur RADIUS. Les secrets partagés Strong RADIUS sont constitués de séquences aléatoires de lettres majuscules et minuscules, de chiffres et de signes de ponctuation et comportent au moins 22 caractères. Si possible, utilisez un programme de génération de caractères aléatoires pour déterminer les secrets partagés RADIUS.

Pour mieux protéger le trafic RADIUS, attribuez un secret partagé différent à chaque appliance ou serveur virtuel NetScaler Gateway. Lorsque vous définissez des clients sur le serveur RADIUS, vous pouvez également attribuer un secret partagé distinct à chaque client. Dans ce cas, vous devez configurer séparément chaque stratégie NetScaler Gateway qui utilise l'authentification RADIUS.

Lorsque vous créez une stratégie RADIUS, vous configurez des secrets partagés sur NetScaler Gateway dans le cadre de la stratégie.

Configuration de l'extraction d'adresses IP

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour extraire l'adresse IP d'un serveur RADIUS. Lorsqu'un utilisateur s'authentifie auprès du serveur RADIUS, le serveur renvoie une adresse IP encadrée qui lui

est attribuée. L'adresse IP encadrée est également appelée adresse IP encadrée de l'attribut RADIUS 8 dans les demandes d'accès.

Les composants suivants sont destinés à l'extraction d'adresses IP :

- Permet à un serveur RADIUS distant de fournir une adresse IP depuis le réseau interne à un utilisateur connecté à NetScaler Gateway.
- Permet la configuration de n'importe quel attribut RADIUS à l'aide du type **adresse IP**, y compris les attributs codés par le fournisseur.

Lors de la configuration du serveur RADIUS pour l'extraction d'adresses IP, vous configurez l'identificateur fournisseur et le type d'attribut. L'ID et les attributs du fournisseur sont utilisés pour établir l'association entre le client RADIUS et le serveur RADIUS.

- L'identificateur de fournisseur (ID) permet au serveur RADIUS d'attribuer une adresse IP au client à partir d'un pool d'adresses IP configurées sur le serveur RADIUS. L'ID du fournisseur est l'attribut de la réponse RADIUS qui fournit l'adresse IP du réseau interne. La valeur zéro indique que l'attribut n'est pas codé par le fournisseur
- Le type d'attribut est l'attribut d'adresse IP distante dans une réponse RADIUS. La valeur minimale est 1 et la valeur maximale est 255.

Une configuration courante consiste à extraire l'**adresse IP encadrée**de l'attribut RADIUS. L'ID du fournisseur est défini sur 0 ou n'est pas spécifié. Le type d'attribut est défini sur 8.

Pour configurer l'extraction d'adresses IP à partir d'un serveur RADIUS à l'aide de l'interface graphique :

1. Accédez à **NetScaler Gateway > Policies > Authentification**, puis cliquez sur **RADIUS**.
2. Dans le volet d'**informations**, sous **l'onglet Stratégies**, sélectionnez une stratégie RADIUS, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer la politique d'authentification**, à côté de Serveur, cliquez sur **Modifier**.
4. Sous **Détails**, dans **Identifiant du fournisseur du groupe**, tapez la valeur.
5. Dans **Type d'attribut de groupe**, tapez la valeur, puis cliquez deux fois sur **OK**.

Configuration de l'extraction de groupes RADIUS

January 26, 2024

Vous pouvez configurer l'autorisation RADIUS à l'aide d'une méthode appelée extraction de groupe. La configuration de l'extraction de groupes vous permet d'administrer les utilisateurs sur votre serveur RADIUS au lieu de les ajouter à NetScaler Gateway.

Vous configurez l'autorisation RADIUS à l'aide d'une stratégie d'authentification et en configurant l'identificateur de fournisseur (ID) du groupe, le type d'attribut de groupe, le préfixe de groupe et un séparateur de groupe. Lorsque vous configurez la stratégie, vous ajoutez une expression, puis vous liez la stratégie globalement ou à un serveur virtuel.

Configuration de RADIUS sur Windows Server 2003

Si vous utilisez Microsoft Internet Authentication Service (IAS) pour l'autorisation RADIUS sous Windows Server 2003, lors de la configuration de NetScaler Gateway, vous devez fournir les informations suivantes :

- L'ID fournisseur est le code spécifique au fournisseur que vous avez saisi dans IAS.
- Type correspond au numéro d'attribut attribué par le fournisseur.
- Le nom d'attribut est le type de nom d'attribut que vous avez défini dans IAS. Le nom par défaut est CTXSUserGroups=

Si IAS n'est pas installé sur le serveur RADIUS, vous pouvez l'installer à partir de l'option Ajout/Suppression de programmes du Panneau de configuration. Pour plus d'informations, consultez l'aide en ligne de Windows.

Pour configurer IAS, utilisez la console de gestion Microsoft (MMC) et installez le composant logiciel enfichable pour IAS. Suivez l'assistant, en vous assurant de sélectionner les paramètres suivants :

- Sélectionnez l'ordinateur local.
- Sélectionnez Stratégies d'accès à distance et créez une stratégie personnalisée.
- Sélectionnez Groupes Windows pour la stratégie.
- Sélectionnez l'un des protocoles suivants :
  - Protocole d'authentification Microsoft Challenge-Handshake version 2 (MS-CHAP v2)
  - Protocole d'authentification Microsoft Challenge-Handshake (MS-CHAP)
  - Protocole CHAP (Challenge-Handshake Authentication Protocol)
  - Authentification non chiffrée (PAP, SPAP)
- Sélectionnez l'attribut spécifique au fournisseur.

  L'attribut spécifique au fournisseur doit correspondre aux utilisateurs que vous avez définis dans le groupe sur le serveur avec les utilisateurs de NetScaler Gateway. Pour répondre à cette exigence, vous envoyez les attributs spécifiques au fournisseur à NetScaler Gateway. Assurez-vous de sélectionner RADIUS=Standard.
- La valeur par défaut de RADIUS est 0. Utilisez ce numéro comme code fournisseur.

- Le numéro d'attribut attribué par le fournisseur est 0.

  Il s'agit du numéro attribué à l'attribut Groupe d'utilisateurs. L'attribut est au format chaîne.

- Sélectionnez String pour le format d'attribut.

  La valeur Attribute nécessite le nom de l'attribut et les groupes.

  Pour Access Gateway, la valeur de l'attribut est CTXSUserGroups=GroupName. Si deux groupes sont définis, tels que ventes et finances, la valeur de l'attribut est CTXSUserGroups=Sales ; finance. Séparez chaque groupe par un point-virgule.

- Supprimez toutes les autres entrées de la boîte de dialogue Modifier le profil d'accès à distance, en laissant celle qui indique Spécifique au fournisseur.

Après avoir configuré la stratégie d'accès à distance dans IAS, vous configurez l'authentification et l'autorisation RADIUS sur NetScaler Gateway.

Lorsque vous configurez l'authentification RADIUS, utilisez les paramètres que vous avez configurés sur le serveur IAS.

Configuration de RADIUS pour l'authentification sur Windows Server 2008

Sur Windows Server 2008, vous configurez l'authentification et l'autorisation RADIUS à l'aide du serveur de stratégie réseau (NPS), qui remplace le service d'authentification Internet (IAS). Vous pouvez utiliser le gestionnaire de serveurs et ajouter NPS en tant que rôle pour installer ce dernier.

Lorsque vous installez NPS, sélectionnez le service de stratégie réseau. Après l'installation, vous pouvez configurer les paramètres RADIUS pour votre réseau en démarrant le NPS à partir des services d'administration du menu Démarrer. Lorsque vous ouvrez le NPS, vous ajoutez NetScaler Gateway en tant que client RADIUS, puis vous configurez des groupes de serveurs.

Lorsque vous configurez le client RADIUS, veillez à sélectionner les paramètres suivants :

- Pour le nom du fournisseur, sélectionnez RADIUS Standard.
- Prenez note du secret partagé car vous devrez configurer le même secret partagé sur NetScaler Gateway.

Pour les groupes RADIUS, vous avez besoin de l'adresse IP ou du nom d'hôte du serveur RADIUS. Ne modifiez pas les paramètres par défaut.

Après avoir configuré le client et les groupes RADIUS, vous configurez les paramètres dans les deux stratégies suivantes :

- Stratégies de demande de connexion dans lesquelles vous configurez les paramètres de la connexion NetScaler Gateway, notamment le type de serveur réseau, les conditions de la stratégie réseau et les paramètres de la stratégie.

- Stratégies réseau dans lesquelles vous configurez l'authentification EAP (Extensible Authentication Protocol) et les attributs spécifiques au fournisseur.

Lorsque vous configurez la stratégie de demande de connexion, sélectionnez Non spécifié pour le type de serveur réseau. Vous configurez ensuite votre condition en sélectionnant Type de port NAS comme condition et Virtuel (VPN) comme valeur.

Lorsque vous configurez une stratégie réseau, vous devez configurer les paramètres suivants :

- Sélectionnez Remote Access Server (VPN Dial-up) comme type de serveur d'accès réseau.
- Sélectionnez Encrypted Authentication (CHAP) et Uncrypted Authentication (PAP et SPAP) pour l'EAP.
- Sélectionnez RADIUS Standard pour l'attribut spécifique au fournisseur.

  Le numéro d'attribut par défaut est 26. Cet attribut est utilisé pour l'autorisation RADIUS.

  NetScaler Gateway a besoin de l'attribut spécifique au fournisseur pour faire correspondre les utilisateurs définis dans le groupe sur le serveur à ceux de NetScaler Gateway. Cela se fait en envoyant les attributs spécifiques au fournisseur à NetScaler Gateway.
- Sélectionnez String (Chaîne) pour le format d'attribut.

  La valeur Attribute nécessite le nom de l'attribut et les groupes.

  Pour NetScaler Gateway, la valeur de l'attribut est CtxSUserGroups= groupname. Si deux groupes sont définis, tels que ventes et finances, la valeur de l'attribut est CTXSUserGroups=Sales ; finance. Séparez chaque groupe par un point-virgule.
- Le séparateur est celui que vous avez utilisé sur le NPS pour séparer des groupes, tels qu'un point-virgule, un deux-points, un espace ou un point.

Lorsque vous avez terminé de configurer la stratégie d'accès à distance dans IAS, vous pouvez configurer l'authentification et l'autorisation RADIUS sur NetScaler Gateway.

Pour configurer l'autorisation RADIUS

March 27, 2024

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.
2. Cliquez sur RADIUS.
3. Dans l'onglet Stratégies, cliquez sur Ajouter.
4. Dans Nom, tapez le nom de la stratégie.

5. Sous le serveur* cliquez sur +
6. Dans Nom, tapez le nom du serveur RADIUS.
7. Sous Serveur, tapez l'adresse IP et le port du serveur RADIUS.
8. Sous Détails, saisissez les valeurs de Group Vendor Identifier et Group Attribute Type.
9. Dans Encodage de mot de passe, sélectionnez le protocole d'authentification, puis cliquez sur Créer.
10. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez l'expression, cliquez sur Ajouter une expression, cliquez sur Créer, puis sur Fermer.

Configuration de la gestion des comptes utilisateur RADIUS

March 27, 2024

NetScaler Gateway peut envoyer des messages de démarrage et d'arrêt de session utilisateur à votre serveur de gestion RADIUS. Les messages, qui sont envoyés pour chaque session utilisateur, incluent un sous-ensemble des attributs définis dans la RFC2866. Le tableau 1 répertorie les attributs pris en charge et les types de messages de gestion des comptes RADIUS (RAD_START et RAD_STOP) dans lesquels ils sont envoyés. Le tableau 2 répertorie les valeurs prédéfinies qui peuvent être attribuées à l'attribut,`Acct-Terminate-Cause` ainsi que les événements NetScaler Gateway correspondants.

Tableau 1 Attributs RADIUS pris en charge

Attribut	Signification	RAD_START	RAD_STOP
Nom d'utilisateur	Nom de l'utilisateur associé à la session.	X	X
ID de session	ID de session NetScaler.	X	X
Acct-Session-Time	Durée de la session en secondes.		X
Acct-Terminate-Cause	Motif de la résiliation du compte.		X

Tableau 2. Causes de la terminaison RADIUS

Méthode de déconnexion NetScaler	Cause de terminaison RADIUS
LOGOUT_SESSN_TIMEDOUT	RAD_TERM_SESSION_TIMEOUT

Méthode de déconnexion NetScaler	Cause de terminaison RADIUS
LOGOUT_SESSN_INITIATEDBYUSER	RAD_TERM_USER_REQUEST
LOGOUT_SESSN_KILLEDBYADMIN	RAD_TERM_ADMIN_RESET
LOGOUT_SESSN_TLOGIN	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_MAXLICRCHD	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_CLISECCHK_FAILED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_PREAUTH_CHANGED	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_COOKIE_MISMATCH	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_DHT	RAD_TERM_NAS_REQUEST
LOGOUT_SESSS_2FACTOR_FAIL	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_ICALIC	RAD_TERM_NAS_REQUEST
LOGOUT_SESSN_INTERNALERR	RAD_TERM_NAS_ERROR
Autre	RAD_TERM_NAS_ERROR

La configuration de la gestion des comptes utilisateur RADIUS nécessite la création d'une paire de stratégies. La première stratégie est une stratégie d'authentification RADIUS qui désigne un serveur RADIUS auquel envoyer des messages de gestion des comptes. La seconde est une stratégie de session qui utilise la stratégie de comptabilité RADIUS comme action.

Pour configurer la gestion des comptes utilisateur RADIUS, vous devez :

1. Créez une stratégie RADIUS pour définir le serveur de gestion de comptes RADIUS. Le serveur de gestion des comptes peut être le même que celui que vous utilisez pour l'authentification RADIUS.
2. Créez une stratégie de session, en utilisant la stratégie RADIUS comme action spécifiant le serveur de gestion des comptes d'utilisateurs RADIUS.
3. Liez la stratégie de session soit globalement, afin qu'elle s'applique à l'ensemble du trafic, soit à un serveur virtuel NetScaler Gateway, afin qu'elle s'applique uniquement au trafic passant par ce serveur virtuel.

Pour créer une stratégie RADIUS

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez le nœud NetScaler Gateway, puis Policies.
2. Développez Authentification et sélectionnez RADIUS.

3. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
4. Entrez un nom pour la stratégie.
5. Sélectionnez un serveur dans le menu Serveur ou cliquez sur l'icône + et suivez les instructions pour ajouter un nouveau serveur RADIUS.
6. Dans le volet Expression, dans le menu Expressions de stratégie enregistrées, sélectionnez ns_true.
7. Cliquez sur Créer.

Pour créer une stratégie de session

Après avoir configuré une stratégie RADIUS spécifiant le serveur de gestion de comptes RADIUS, créez une stratégie de session qui applique ce serveur de gestion de comptes dans une action, comme suit :

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez le nœud NetScaler Gateway, puis Policies.
2. Sélectionnez Session.
3. Dans le volet de détails principal, sélectionnez Ajouter.
4. Entrez un nom pour la stratégie.
5. Dans le menu Action, cliquez sur l'icône + pour ajouter une nouvelle action de session.
6. Entrez le nom de l'action de session.
7. Cliquez sur l'onglet Expérience client .
8. Dans le menu Stratégie de gestion des comptes, sélectionnez la stratégie RADIUS que vous avez créée précédemment.
9. Cliquez sur Créer.
10. Dans le volet Expression, dans le menu Expressions de stratégie enregistrées, sélectionnez ns_true.
11. Cliquez sur Créer.

Pour lier la stratégie de session à l'échelle mondiale

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez le nœud NetScaler Gateway, puis Policies.
2. Sélectionnez Session.
3. Dans le menu Action du volet de détails principal, sélectionnez Liaisons globales.
4. Cliquez sur Bind.
5. Dans le volet Stratégies, sélectionnez la stratégie de session que vous avez créée précédemment, puis cliquez sur Insérer.
6. Dans la liste des stratégies, cliquez sur l'entrée Priorité de la stratégie de session et saisissez une valeur comprise entre 0 et 64000.

7. Cliquez sur OK.

Pour lier la stratégie de session à un serveur virtuel NetScaler Gateway

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez le nœud NetScaler Gateway, puis sélectionnez Virtual Servers.
2. Dans le volet de détails principal, sélectionnez un serveur virtuel, puis cliquez sur Modifier.
3. Dans le volet Stratégies, cliquez sur l'icône + pour sélectionner une stratégie.
4. Dans le menu Choisir une stratégie, sélectionnez Session et assurez-vous que la demande est sélectionnée dans le menu Choisir un type.
5. Cliquez sur Continuer.
6. Cliquez sur Bind.
7. Dans le volet Stratégies, sélectionnez la stratégie de session que vous avez créée précédemment, puis cliquez sur Insérer.
8. Cliquez sur OK.

Configuration de l'authentification SAML

March 27, 2024

Le langage SAML (Security Assertion Markup Language) est une norme XML pour l'échange d'authentification et d'autorisation entre les fournisseurs d'identité (IdP) et les fournisseurs de services. NetScaler Gateway prend en charge l'authentification SAML.

Lorsque vous configurez l'authentification SAML, vous créez les paramètres suivants :

- Nom du certificat IdP. Il s'agit de la clé publique qui correspond à la clé privée de l'IdP.
- URL de redirection. Il s'agit de l'URL de l'IdP d'authentification. Les utilisateurs qui ne sont pas authentifiés sont redirigés vers cette URL.
- Champ utilisateur. Vous pouvez utiliser ce champ pour extraire le nom d'utilisateur si l'IdP envoie le nom d'utilisateur dans un format différent de celui de la balise NameIdentifier de la balise Subject. Ce paramètre est facultatif.
- Nom du certificat de signature. Il s'agit de la clé privée du serveur NetScaler Gateway qui est utilisée pour signer la demande d'authentification auprès de l'IdP. Si vous ne configurez pas de nom de certificat, l'assertion est envoyée sans signature ou la demande d'authentification est rejetée.
- Nom de l'émetteur SAML. Cette valeur est utilisée lors de l'envoi de la demande d'authentification. Il doit y avoir un nom unique dans le champ émetteur pour indiquer l'autorité à partir de laquelle l'assertion est envoyée. Il s'agit d'un champ facultatif.

- Groupe d'authentification par défaut. Il s'agit du groupe sur le serveur d'authentification à partir duquel les utilisateurs sont authentifiés.
- Deux facteurs. Ce paramètre active ou désactive l'authentification à deux facteurs.
- Rejette l'assertion non signée. Si cette option est activée, NetScaler Gateway rejette l'authentification des utilisateurs si le nom du certificat de signature n'est pas configuré.

NetScaler Gateway prend en charge le protocole HTTP post-binding. Dans cette liaison, l'expéditeur répond à l'utilisateur avec un OK 200 contenant une publication automatique de formulaire avec les informations requises. Plus précisément, le formulaire par défaut doit contenir deux champs cachés appelés `SAMLRequest` et,`SAMLResponse` selon qu'il s'agit d'une demande ou d'une réponse. Le formulaire inclut également RelayState, qui est un état ou une information utilisés par la partie expéditrice pour envoyer des informations arbitraires qui ne sont pas traitées par une partie utilisatrice. La partie utilisatrice renvoie les informations de sorte que lorsque la partie expéditrice reçoit l'assertion avec RelayState, la partie expéditrice sache quoi faire ensuite. Il est recommandé de crypter ou de masquer le RelayState.

> **Remarque**
>
> - Lorsque NetScaler Gateway est utilisé comme IdP vers Citrix Cloud, vous n'avez pas besoin de configurer la règle **RelayState** sur NetScaler Gateway.
> - En cas de chaînage d'IdP, il suffit de configurer la règle **RelayState** uniquement sur la première stratégie SAML. Dans ce contexte, le chaînage d'IdP est un scénario dans lequel une action SAML configurée fait référence à un IdP de serveur virtuel d'authentification contenant une autre action SAML.

Configuration d'Active Directory Federation Services 2.0

Vous pouvez configurer Active Directory Federation Services (AD FS) 2.0 sur n'importe quel ordinateur Windows Server 2008 ou Windows Server 2012 que vous utilisez dans un rôle de serveur fédéré. Lorsque vous configurez le serveur ADFS pour qu'il soit compatible avec NetScaler Gateway, vous devez configurer les paramètres suivants à l'aide de l'assistant Reying Party Trust dans Windows Server 2008 ou Windows Server 2012.

Paramètres Windows Server 2008 :

- Fiducie de la partie de confiance. Vous indiquez l'emplacement du fichier de métadonnées NetScaler Gateway, par exemple,`https://vserver.fqdn.com/ns.metadata.xml` où vserver.fqdn.com est le nom de domaine complet (FQDN) du serveur virtuel NetScaler Gateway. Le nom de domaine complet se trouve sur le certificat de serveur lié au serveur virtuel.
- Règles d'autorisation. Vous pouvez autoriser ou refuser aux utilisateurs l'accès à la partie de confiance.

Paramètres Windows Server 2012 :

- Fiducie de la partie de confiance. Vous indiquez l'emplacement du fichier de métadonnées NetScaler Gateway, par exemple,`https://vserver.fqdn.com/ns.metadata.xml` où vserver.fqdn.com est le nom de domaine complet (FQDN) du serveur virtuel NetScaler Gateway. Le nom de domaine complet se trouve sur le certificat de serveur lié au serveur virtuel.
- Profil AD FS. Sélectionnez le profil AD FS.
- Certificat. NetScaler Gateway ne prend pas en charge le chiffrement. Il n'est pas nécessaire de sélectionner un certificat.
- Activez la prise en charge du protocole WebSSO SAML 2.0. Ceci active la prise en charge de l'SSO SAML 2.0. Vous fournissez l'URL du serveur virtuel NetScaler Gateway, par exemple. `https://netScaler.virtualServerName.com/cgi/samlauth`

  Cette URL est l'URL du service Assertion Consumer sur l'appliance NetScaler Gateway. Il s'agit d'un paramètre constant et NetScaler Gateway attend une réponse SAML sur cette URL.
- Identificateur de confiance de la partie de confiance. Entrez le nom NetScaler Gateway. Il s'agit d'une URL qui identifie les parties de confiance, telles que `https://netscalerGateway.virtualServerName.com/adfs/services/trust`.
- Règles d'autorisation. Vous pouvez autoriser ou refuser aux utilisateurs l'accès à la partie de confiance.
- Configurez les règles de réclamation. Vous pouvez configurer les valeurs des attributs LDAP en utilisant les règles de transformation des émissions et en utilisant le modèle Envoyer les attributs LDAP sous forme de réclamations. Vous configurez ensuite les paramètres LDAP qui incluent :
  - Adresses e-mail
  - sAMAccountName
  - User Principal Name (UPN)
  - Membre de
- Signature du certificat. Vous pouvez spécifier les certificats de vérification de signature en sélectionnant les propriétés d'une partie de relais, puis en ajoutant le certificat.

  Si le certificat de signature est inférieur à 2 048 bits, un message d'avertissement apparaît. Vous pouvez ignorer cet avertissement pour continuer. Si vous configurez un déploiement de test, désactivez la liste de révocation de certificats (CRL) sur la partie relais. Si vous ne désactivez pas la vérification, AD FS tente de valider le certificat par la CRL.

  Vous pouvez désactiver la liste de révocation de certificats en exécutant la commande suivante : Set-ADFWRelayingPartyTrust - SigningCertficateRevocatOnCheck NoneTargetName NetScaler

Après avoir configuré les paramètres, vérifiez les données de la partie de confiance avant de terminer l'Assistant d'approbation de la partie relais. Vous vérifiez le certificat du serveur virtuel NetScaler Gateway à l'aide de l'URL du point de terminaison, par exemple. `https://vserver.fqdn.com/cgi/samlauth`

Une fois que vous avez terminé de configurer les paramètres de l'Assistant d'approbation de partie relais, sélectionnez l'approbation configurée, puis modifiez les propriétés. Procédez comme suit :

- Définissez l'algorithme de hachage sécurisé sur SHA-1.

  Remarque : NetScaler prend uniquement en charge SHA-1.

- Supprimez le certificat de chiffrement. Les assertions chiffrées ne sont pas prises en charge.
- Modifiez les règles de réclamation, notamment les suivantes :

  - Sélectionnez la règle de transformation
  - Ajouter une règle de réclamation
  - Sélectionner un modèle de règle de réclamation : Envoyer les attributs LDAP en tant que revendications
  - Donnez un nom
  - Sélectionner le magasin d'attributs : Active Directory
  - Sélectionnez l'attribut LDAP : <Active Directory parameters>
  - Sélectionnez Règle de réclamation sortante comme « ID de nom »

  Remarque : Les balises XML de nom d'attribut ne sont pas prises en charge.

- Configurez l'URL de déconnexion pour l'authentification unique. La règle de réclamation est Envoyer l'URL de déconnexion. La règle personnalisée doit être la suivante :

  ```
  pre codeblock => issue(Type = "logoutURL", Value = "https://<adfs
  .fqdn.com>/adfs/ls/", Properties["http://schemas.xmlsoap.org/ws
  /2005/05/identity/claimproperties/attributename"] = "urn:oasis:
  names:tc:SAML:2.0:attrname-format:unspecified"); <!--NeedCopy-->
  ```

Après avoir configuré les paramètres AD FS, téléchargez le certificat de signature AD FS, puis créez une clé de certificat sur NetScaler Gateway. Vous pouvez ensuite configurer l'authentification SAML sur NetScaler Gateway à l'aide du certificat et de la clé.

Configuration de l'authentification à deux facteurs SAML

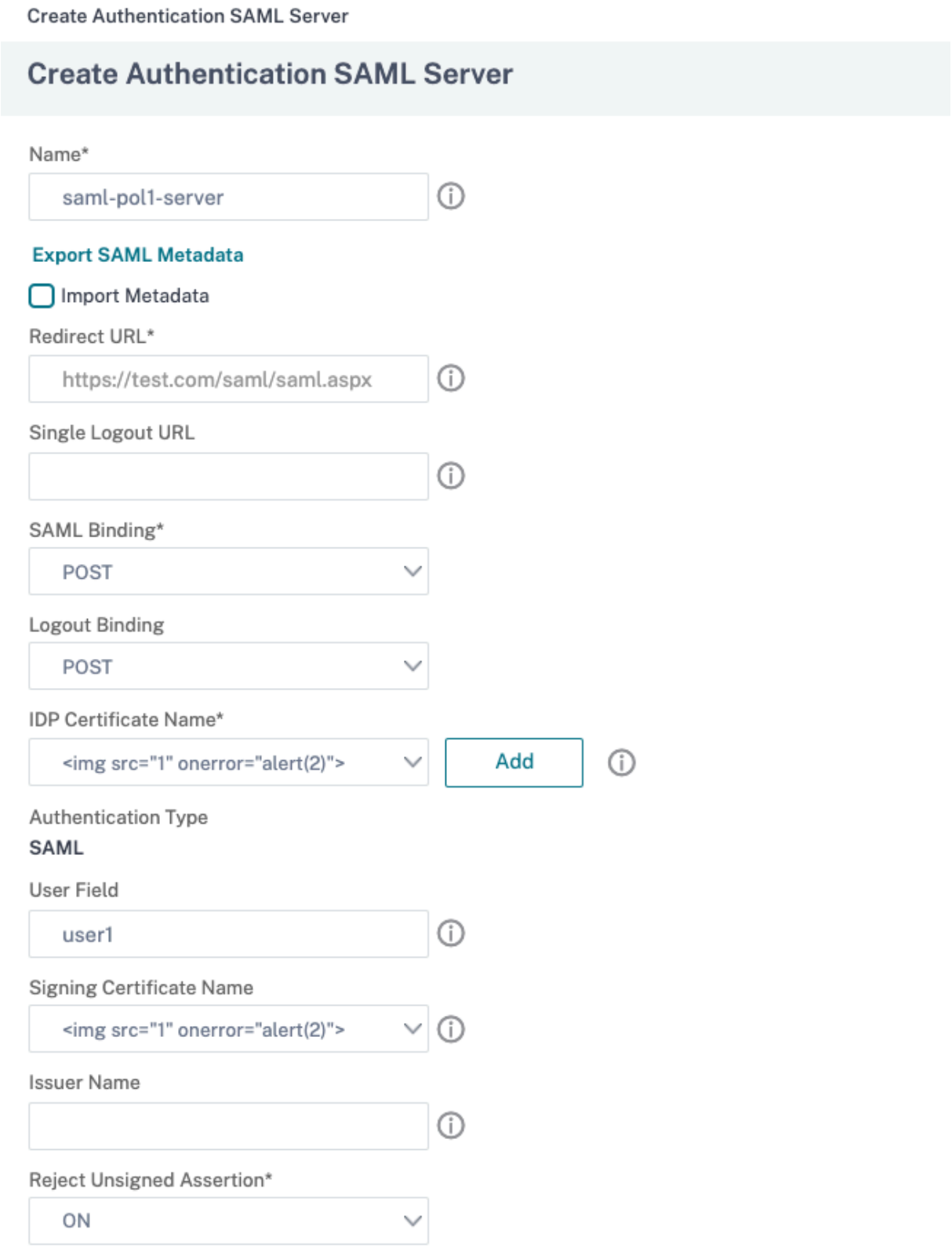
Vous pouvez configurer l'authentification à deux facteurs SAML. Lorsque vous configurez l'authentification SAML avec l'authentification LDAP, suivez les instructions suivantes :

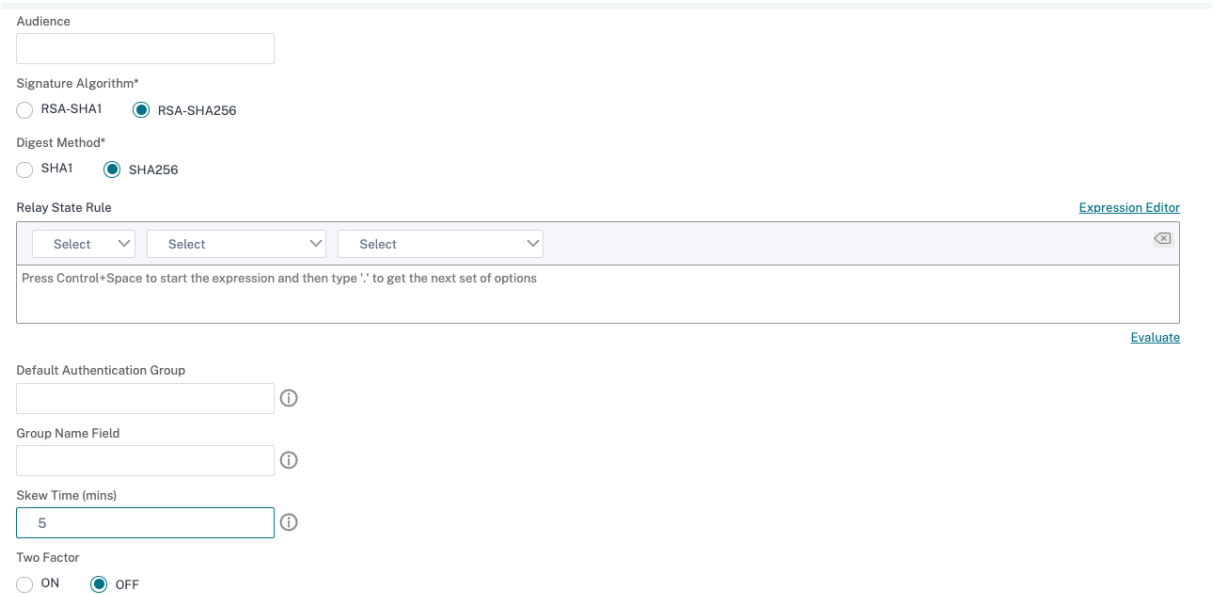
- Si SAML est le principal type d'authentification, désactivez l'authentification dans la stratégie LDAP et configurez l'extraction de groupe. Ensuite, liez la stratégie LDAP en tant que type d'authentification secondaire.
- L'authentification SAML n'utilise pas de mot de passe et utilise uniquement le nom d'utilisateur. De plus, l'authentification SAML n'informe les utilisateurs que lorsque l'authentification réussit. Si l'authentification SAML échoue, les utilisateurs ne sont pas avertis. Étant donné qu'aucune réponse d'échec n'est envoyée, SAML doit être la dernière stratégie de la cascade ou la seule stratégie.
- Il est recommandé de configurer des noms d'utilisateur réels plutôt que des chaînes opaques.
- SAML ne peut pas être lié en tant que type d'authentification secondaire.

Pour configurer l'authentification SAML

March 27, 2024

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Dans le volet de navigation, cliquez sur **SAML**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue Créer une politique d'authentification, dans **Nom**, tapez le nom de la stratégie.





1. À côté de Serveur, cliquez sur **Nouveau**.
2. Dans **Nom**, saisissez le nom du profil de serveur.
3. Dans Nom du certificat IdP, sélectionnez un certificat ou cliquez sur **Installer**. Il s'agit du certificat installé sur le serveur SAML ou IdP.

   Si vous cliquez sur Installer, ajoutez le certificat et la clé privée. Pour de plus amples informations, consultez la section Installation et gestion des certificats.
4. Dans la zone **URL de redirection**, saisissez l'URL du fournisseur d'identité d'authentification (IdP).

   Il s'agit de l'URL de l'ouverture de session de l'utilisateur sur le serveur SAML. Il s'agit du serveur vers lequel NetScaler Gateway redirige la demande initiale.
5. Dans **URL de déconnexion unique**, spécifiez l'URL afin que l'appliance puisse reconnaître quand renvoyer le client à l'IdP pour terminer le processus de déconnexion.
6. Dans la **liaison SAML**, sélectionnez la méthode à utiliser pour déplacer le client du fournisseur de services vers l'IdP. Il doit en être de même pour l'IdP afin qu'il comprenne comment le client s'y connecte. Lorsque l'appliance agit en tant que SP, elle prend en charge les liaisons POST, REDIRECT et ARTIFACT.
7. Dans **Liaison de déconnexion**, sélectionnez **REDIRIGER.**
8. Dans **Nom du certificat IDP**, sélectionnez le certificat IDPCert (Base64) présent sous le certificat de signature SAML.

> **Remarque :**
>
> Vous pouvez également cliquer sur **Importer les métadonnées** et sélectionner l'URL dans laquelle la configuration des métadonnées est stockée.

9. Dans le **champ Utilisateur**, entrez le nom d'utilisateur à extraire.
10. Dans **Nom du certificat de signature**, sélectionnez le certificat SP SAML (avec clé privée) que l'appliance utilise pour signer les demandes d'authentification à l'IdP. Le même certificat (sans clé privée) doit être importé sur l'IdP, de sorte que l'IdP puisse vérifier la signature de la demande d'authentification. Ce champ n'est pas nécessaire pour la plupart des IdP

    Il s'agit du certificat lié à l'adresse IP virtuelle de NetScaler Gateway. Le nom de l'émetteur SAML est le nom de domaine complet (FQDN) auquel les utilisateurs ouvrent une session, par exemple lb.example.com ou ng.example.com.
11. Dans **Nom de l'émetteur**, entrez le nom de domaine complet de l'équilibrage de charge ou de l'adresse IP virtuelle NetScaler Gateway à laquelle l'appliance envoie la demande d'authentification initiale (GET).
12. Dans **Refuser une assertion non signée**, spécifiez si vous souhaitez que les assertions de l'IdP soient signées. Vous pouvez vous assurer que seule l'assertion doit être signée (ON) ou que l'assertion et la réponse de l'IdP doivent être signées (STRICT).
13. Dans **Audience**, saisissez l'audience pour laquelle l'assertion envoyée par IdP est applicable. Il s'agit généralement d'un nom d'entité ou d'une URL qui représente le fournisseur de services.
14. Dans **Signature Algorithm**, sélectionnez RSA-SHA256
15. Dans **Méthode Digest**, sélectionnez SHA256
16. Dans **Groupe d'authentification**par défaut, entrez le groupe par défaut choisi lorsque l'authentification réussit en plus des groupes extraits.
17. Dans **Nom du groupe**, saisissez le nom de la balise dans l'assertion qui contient des groupes d'utilisateurs.
18. Dans **Skew Time (minutes)**, spécifiez le décalage d'horloge autorisé en minutes que le fournisseur de services autorise sur une assertion entrante.
19. Cliquez sur **Créer,** puis sur **Fermer**.
20. Dans la boîte de dialogue Créer une politique d'authentification, à côté de Expressions nommées, sélectionnez Général, sélectionnez Valeur vraie, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Références

- NetScaler en tant que SP SAML
- NetScaler en tant qu'IdP SAML
- Fonctionnalités supplémentaires prises en charge par SAML

Utilisation de l'authentification SAML pour se connecter à NetScaler Gateway

January 26, 2024

Vous pouvez utiliser l'authentification SAML pour vous connecter à NetScaler Gateway à l'aide des clients VPN et de l'application Workspace. Le plug-in prend en charge l'authentification SAML uniquement via des stratégies SAML avancées liées au serveur virtuel d'authentification, à savoir l'authentification nFactor.

Important : Le plug-in ne prend pas en charge l'authentification SAML lorsque les stratégies SAML sont directement liées au serveur virtuel VPN, c'est-à-dire l'authentification non NFactor.

Plateformes et applications prises en charge

Le tableau suivant répertorie les plateformes et applications qui prennent en charge l'authentification SAML pour la connexion à NetScaler Gateway.

Produit	Version
NetScaler Gateway	Version 12.0 build 41.16 et ultérieure
Client VPN	Version 12.1 build 49.37 et ultérieure. **Plates-formes prises en charge** : Windows 7, Windows 8, Windows 8.1, Windows 10
Versions de l'application Workspace	Windows : 1808 ; Mac : 1808

Configuration pour l'authentification SAML à l'aide de stratégies SAML avancées

Pour plus d'informations sur la configuration de l'authentification SAML à l'aide de stratégies SAML avancées, voir NetScaler en tant qu'IdP SAML.

Améliorations de l'authentification SAML

March 27, 2024

Cette fonctionnalité nécessite une connaissance SAML, une maîtrise fondamentale de l'authentification et une compréhension FIPS pour utiliser ces informations.

Vous pouvez utiliser les fonctionnalités NetScaler suivantes avec des applications et des serveurs tiers compatibles avec la spécification SAML 2.0 :

- Fournisseur de services SAML (SP)
- Fournisseur d'identité SAML (IdP)

Le SP et l'IdP permettent un SingleSignon (SSO) entre les services cloud. La fonctionnalité de fournisseur de services SAML fournit un moyen de répondre aux réclamations des utilisateurs d'un fournisseur d'identité. L'IdP peut être un service tiers ou une autre appliance NetScaler. La fonctionnalité IdP SAML est utilisée pour affirmer les connexions utilisateur et fournir des réclamations consommées par les SP.

Dans le cadre de la prise en charge SAML, les modules IdP et SP signent numériquement les données envoyées aux homologues. La signature numérique inclut une demande d'authentification du fournisseur de services, une assertion du fournisseur d'identité et des messages de déconnexion entre ces deux entités. La signature numérique valide l'authenticité du message.

Les implémentations actuelles du SP SAML et de l'IdP effectuent le calcul de signature dans un moteur de paquets. Ces modules utilisent des certificats SSL pour signer les données. Dans un NetScaler conforme à la norme FIPS, la clé privée du certificat SSL n'est pas disponible dans le moteur de paquets ou dans l'espace utilisateur. Le module SAML actuel n'est donc pas prêt pour le matériel FIPS.

Ce document décrit le mécanisme de déchargement des calculs de signature sur la carte FIPS. La vérification de la signature est effectuée dans le logiciel, car la clé publique est disponible.

Solution

Le jeu de fonctionnalités SAML est amélioré pour utiliser une API SSL pour le déchargement des signatures. Consultez la documentation du produit NetScaler pour plus de détails sur les sous-fonctionnalités SAML concernées :

1. Post Binding du SP SAML —Signature de la requête AuthnRequest
2. Post Binding de l'IdP SAML —Signature de l'assertion/Réponse/Les deux
3. Scénarios de déconnexion unique du SP SAML —Signature de LogoutRequest dans le modèle initié par le SP et Signature de LogoutResponse dans le modèle initié par l'IdP

4. Liaison d'artefact du SP SAML —Signature de la demande ArtifactResolve
5. Liaison de redirection du SP SAML —Signature de la requête AuthnRequest
6. Liaison de redirection IdP SAML —Signature de la réponse/assertion/les deux
7. Prise en charge du chiffrement SP SAML —Déchiffrement de l'assertion

Plateforme

L'API ne peut être déchargée que vers une plateforme FIPS.

Configuration

La configuration du déchargement est effectuée automatiquement sur la plateforme FIPS.

Toutefois, étant donné que les clés privées SSL ne sont pas disponibles pour l'espace utilisateur dans le matériel FIPS, il y a un léger changement de configuration lors de la création du certificat SSL sur le matériel FIPS.

Voici les informations de configuration :

- `add ssl fipsKey fips-key`

  Créez une demande de signature de certificat et utilisez-la sur le serveur de l'autorité de certification pour générer un certificat. Vous pouvez ensuite copier ce certificat dans `/nsconfig/ssl`. Supposons que le fichier soit fips3cert.cer.

- `add ssl certKey fips-cert -cert fips3cert.cer -fipsKey fips-key`

  Spécifiez ensuite ce certificat dans l'action SAML du module SP SAML.

- `set samlAction <name> -samlSigningCertName fips-cert`

  De même, vous l'utilisez dans le module `samlIdpProfile` pour le fournisseur d'identité SAML.

- `set samlidpprofile fipstest –samlIdpCertName fips-cert`

La clé FIPS n'est pas disponible la première fois. S'il n'y a pas de clé FIPS, créez-en une comme décrit sur Créer une clé FIPS.

```
create ssl fipskey <fipsKeyName> -modulus <positive_integer> [-exponent
    (3 | F4)]

create certreq <reqFileName> -fipskeyName <string>
<!--NeedCopy-->
```


Configuration de l'authentification TACACS+

March 27, 2024

Vous pouvez configurer un serveur TACACS+ pour l'authentification. Comme pour l'authentification RADIUS, TACACS+ utilise une clé secrète, une adresse IP et le numéro de port. Le numéro de port par défaut est 49.

Pour configurer NetScaler Gateway afin qu'il utilise un serveur TACACS+, fournissez l'adresse IP du serveur et le secret TACACS+. Vous devez spécifier le port uniquement lorsque le numéro de port du serveur utilisé est différent du numéro de port par défaut de 49.

Pour configurer l'authentification TACACS+ à l'aide de l'interface utilisateur, effectuez les opérations suivantes.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies Authentication**.
2. Cliquez sur **TACACS**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans le champ **Nom**, saisissez le nom de la stratégie.
5. En regard **du champ Serveur**, cliquez sur **Ajouter** pour créer un nouveau serveur TACACS ou cliquez sur **Modifier** pour apporter des modifications à un serveur TACACS existant.
6. Dans le champ **Nom**, saisissez le nom du serveur.
7. Sous **Adresse IP**, saisissez l'adresse IP.
8. Sous **Port**, utilisez le numéro de port par défaut 49.
9. Dans le champ **Clé TACACS**, tapez la clé. Dans le champ **Confirmer la clé TACACS**, tapez la même clé pour confirmer.
10. Cliquez sur **Plus**.
11. Dans **Autorisation**, sélectionnez **ACTIVÉ**, puis cliquez sur **Créer**.
12. Dans la boîte de dialogue **Créer une stratégie TACACS d'authentification**, sélectionnez l'expression, cliquez sur Créer, puis sur Fermer.

Pour configurer l'authentification TACACS+ à l'aide de l'interface de ligne de commande, tapez la commande suivante.

```
1 add authentication tacacsAction <name> [-serverIP <ip_addr|ipv6_addr
     |*>][-serverPort <port>] [-authTimeout <positive_integer>] {
2  -tacacsSecret  }
3
4 [-authorization ( ON | OFF )] [-accounting ( ON | OFF )][-
     auditFailedCmds ( ON | OFF )] [-groupAttrName <string>][-
     defaultAuthenticationGroup <string>] [-Attribute1 <string>] [-
     Attribute2 <string>] [-Attribute3 <string>] [-Attribute4 <string>]
5 [-Attribute5 <string>] [-Attribute6 <string>] [-Attribute7 <string>] [-
     Attribute8 <string>] [-Attribute9 <string>] [-Attribute10 <string>]
```



```
[-Attribute11 <string>] [-Attribute12 <string>] [-Attribute13 <string>]
    [-Attribute14 <string>] [-Attribute15 <string>] [-Attribute16 <
   string>]
<!--NeedCopy-->
```

Après avoir configuré les paramètres du serveur TACACS+ dans NetScaler Gateway, liez la stratégie pour la rendre active. Vous pouvez lier la stratégie au niveau global ou au niveau du serveur virtuel. Pour plus d'informations sur les stratégies d'authentification de liaison, consultez Stratégies d'authentification de liaison.

Clear Config Basic ne doit pas effacer la configuration TACACS

January 26, 2024

Cette rubrique se concentre sur le fait de ne pas effacer toutes les configurations liées à RBA (Role Based Access) lorsque la commande clear config est exécutée.

La commande clear config actuelle est exécutée à l'un des trois niveaux suivants :

- De base
- Extended
- Complet

En fonction du niveau, les configurations NetScaler sont effacées et réinitialisées aux paramètres d'usine par défaut.

La commande utilisée est :

```
clear ns config [-force] <level>
<!--NeedCopy-->
```

La nouvelle commande ajoute un bouton pour autoriser/refuser la suppression de toutes les configurations liées à RBA.

Nouvelle commande

Les fonctionnalités de configuration Clear RBA sont décrites :

1. Bouton OUI/NON avec valeur par défaut : OUI.

   L'administrateur décide de conserver ou non la configuration RBA.

2. Seul le niveau de base de la configuration claire est pris en charge.
3. Les configurations suivantes n'ont pas été effacées :

- Ajouter/lier un utilisateur/groupe système.
- Ajoutez une stratégie cmd.
- Commandes TACACS (ajoutez une action/stratégie TACACS).
- Système de liaison global

Remarque : la configuration liée à TACACS (action/stratégie) est préservée si la stratégie est liée au système global ou si elle est effacée

Configuration de la CLI

La commande utilisée est :

```
clear config [ – force] <level> [-RBAconfig]
<!--NeedCopy-->
```

Par défaut, il est défini sur OUI et efface les configurations en fonction du niveau.

Si —RBAconfig est défini sur NO, la configuration associée à RBA est conservée. Les éléments suivants sont inclus :

- Ajouter un utilisateur système /bind /group
- Système de liaison global
- Commandes liées à TACACS (ajout d'action/stratégie TACACS)
- Ajouter une stratégie cmd

Configuration de l'authentification multifacteur

January 26, 2024

Vous pouvez configurer deux types d'authentification multifactorielle dans NetScaler Gateway :

- Authentification en cascade qui définit le niveau de priorité d'authentification
- Authentification à deux facteurs qui exige que les utilisateurs se connectent à l'aide de deux types d'authentification

Si vous disposez de plusieurs serveurs d'authentification, vous pouvez définir la priorité de vos stratégies d'authentification. Les niveaux de priorité que vous définissez déterminent l'ordre dans lequel le serveur d'authentification valide les informations d'identification des utilisateurs. Une stratégie avec un numéro de priorité inférieur est prioritaire sur une stratégie avec un numéro supérieur.

Les utilisateurs peuvent s'authentifier sur deux serveurs d'authentification différents. Par exemple, vous pouvez configurer une stratégie d'authentification LDAP et une stratégie d'authentification RSA.

Lorsque les utilisateurs ouvrent une session, ils s'authentifient d'abord avec leur nom d'utilisateur et leur mot de passe. Ensuite, ils s'authentifient avec un numéro d'identification personnel (PIN) et le code du jeton RSA.

Configuration de l'authentification en cascade

March 27, 2024

L'authentification vous permet de créer une cascade de plusieurs serveurs d'authentification à l'aide de la hiérarchisation des stratégies. Lorsque vous configurez une cascade, le système parcourt chaque serveur d'authentification, tel que défini par les stratégies en cascade, pour valider les informations d'identification d'un utilisateur. Les stratégies d'authentification priorisées sont mises en cascade par ordre croissant et peuvent avoir des valeurs de priorité comprises entre 1 et 9999. Vous définissez ces priorités lorsque vous liez vos stratégies au niveau global ou au niveau du serveur virtuel.

Au cours de l'authentification, lorsqu'un utilisateur ouvre une session, le serveur virtuel est d'abord vérifié, puis les stratégies d'authentification globale sont vérifiées. Si un utilisateur appartient à une stratégie d'authentification sur le serveur virtuel et globalement, la stratégie du serveur virtuel est appliquée en premier lieu, puis la stratégie d'authentification globale. Si vous souhaitez que les utilisateurs reçoivent la stratégie d'authentification liée globalement, modifiez la priorité de la stratégie. Lorsqu'une stratégie d'authentification globale a un numéro de priorité et qu'une stratégie d'authentification liée à un serveur virtuel a une priorité numéro deux, la stratégie d'authentification globale est prioritaire. Par exemple, trois stratégies d'authentification peuvent être liées au serveur virtuel et vous pouvez définir la priorité de chaque stratégie.

Si un utilisateur ne parvient pas à s'authentifier par rapport à une stratégie de la cascade principale, ou s'il réussit à s'authentifier par rapport à une stratégie de la cascade principale, mais ne parvient pas à s'authentifier par rapport à une stratégie de la cascade secondaire, le processus d'authentification s'arrête et l'utilisateur est redirigé vers une page d'erreur.

Remarque : Citrix recommande que lorsque vous liez plusieurs stratégies à un serveur virtuel ou globalement, vous définissez des priorités uniques pour toutes les stratégies d'authentification.

Pour définir la priorité des stratégies d'authentification globale

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **NetScaler Gateway > Policies**Authentication.
2. Sélectionnez la politique qui est liée globalement, puis dans **Action**, cliquez sur **Liaisons globales**.

3. Dans la **boîte de dialogue Lind/Unbind Authentication Global Stratégies**, sous Priorité, tapez le numéro, puis cliquez sur **OK**.

Pour modifier la priorité d'une stratégie d'authentification liée à un serveur virtuel

Vous pouvez également modifier une stratégie d'authentification liée à un serveur virtuel.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Virtual**Servers.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Cliquez sur l'onglet **Authentification**, puis sur **Primaire** ou **Secondaire**.
4. En regard de la stratégie d'authentification, sous **Priorité**, tapez le numéro, puis cliquez sur **OK**.

Configuration de l'authentification à deux facteurs

March 27, 2024

NetScaler Gateway prend en charge l'authentification à deux facteurs. Normalement, lors de l'authentification des utilisateurs, NetScaler Gateway arrête le processus d'authentification dès qu'il authentifie avec succès un utilisateur via l'une des méthodes d'authentification configurées. Dans certains cas, vous devrez peut-être authentifier un utilisateur sur un serveur, mais extraire des groupes d'un autre serveur. Par exemple, si votre réseau authentifie les utilisateurs sur un serveur RADIUS, mais que vous utilisez également l'authentification par jeton RSA SecurID et que des groupes d'utilisateurs sont stockés sur ce serveur, vous devrez peut-être authentifier les utilisateurs sur ce serveur afin de pouvoir extraire les groupes.

Si les utilisateurs sont authentifiés à l'aide de deux types d'authentification, et si l'un de ces types est l'authentification par certificat client, vous pouvez configurer la stratégie d'authentification de certificat en tant que deuxième méthode d'authentification. Par exemple, vous utilisez LDAP comme type d'authentification principal et le certificat client comme authentification secondaire. Lorsque les utilisateurs ouvrent une session avec leur nom d'utilisateur et leur mot de passe, ils ont alors accès aux ressources réseau.

Lorsque vous configurez l'authentification à deux facteurs, vous sélectionnez si le type d'authentification est le type principal ou secondaire.

Pour configurer l'authentification à deux facteurs

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez NetScaler Gateway > Policies Authentication.

2. Dans l'onglet Stratégies, cliquez sur Liaisons globales.
3. Dans la boîte de dialogue Lier/délier les stratégies d'authentification à la stratégie globale, cliquez sur Primaire.
4. Cliquez sur Insérer une stratégie.
5. Sous Nom de la stratégie, sélectionnez la stratégie d'authentification.
6. Cliquez sur Secondaire, répétez les étapes 4 et 5, puis cliquez sur OK.

Sélection du type d'authentification pour l'authentification unique

March 27, 2024

Si vous avez configuré l'authentification unique et l'authentification à deux facteurs sur NetScaler Gateway, vous pouvez sélectionner le mot de passe à utiliser pour l'authentification unique. Par exemple, LDAP est configuré en tant que type d'authentification principal et RADIUS est configuré en tant que type d'authentification secondaire. Lorsque les utilisateurs accèdent à des ressources nécessitant une authentification unique, le nom d'utilisateur et le mot de passe principal sont envoyés par défaut. Vous définissez le mot de passe à utiliser pour l'authentification unique aux applications Web au sein d'un profil de session.

Pour configurer l'authentification pour l'authentification unique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**Session.
2. Dans le volet d'informations, cliquez sur l'onglet **Profils**, puis effectuez l'une des opérations suivantes :
    - Pour créer un nouveau profil, cliquez sur **Ajouter**.
    - Pour modifier un profil existant, cliquez sur **Ouvrir**.
3. Dans l'onglet Expérience client, à côté de Credential Index, cliquez sur **Override Global**, puis sélectionnez **Principal** ou **Secondaire** .
4. S'il s'agit d'un nouveau profil, cliquez sur **Créer**, puis sur **Fermer**.
5. Si vous modifiez un profil existant, cliquez sur **OK**.

Configuration des certificats clients et de l'authentification à deux facteurs LDAP

March 27, 2024

Vous pouvez utiliser un certificat client sécurisé avec authentification et autorisation LDAP, par exemple en utilisant l'authentification par carte à puce avec LDAP. L'utilisateur ouvre une session, puis le nom d'utilisateur est extrait du certificat client. Le certificat client est la principale forme d'authentification et LDAP est le formulaire secondaire. L'authentification du certificat client doit être prioritaire sur la stratégie d'authentification LDAP. Lorsque vous définissez la priorité des stratégies, attribuez à la stratégie d'authentification de certificat client un nombre inférieur à celui que vous attribuez à la stratégie d'authentification LDAP.

Pour utiliser un certificat client, vous devez disposer d'une autorité de certification (CA) d'entreprise, telle que les services de certificats dans Windows Server 2008, exécutée sur le même ordinateur qui exécute Active Directory. Vous pouvez utiliser l'autorité de certification pour créer un certificat client.

Pour utiliser un certificat client avec authentification et autorisation LDAP, il doit s'agir d'un certificat sécurisé qui utilise le protocole SSL (Secure Sockets Layer). Pour utiliser des certificats clients sécurisés pour LDAP, installez le certificat client sur la machine utilisateur et installez un certificat racine correspondant sur NetScaler Gateway.

Avant de configurer un certificat client, procédez comme suit :

- Créez un serveur virtuel.
- Créez une stratégie d'authentification LDAP pour le serveur LDAP.
- Définissez l'expression de la stratégie LDAP sur la valeur True.

Pour configurer l'authentification du certificat client avec LDAP

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Policies \ > Authentication**.
2. Dans le volet de navigation, sous Authentification, cliquez sur Cert.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans Nom, tapez le nom de la stratégie.
5. Dans Type d'authentification, sélectionnez Cert.
6. À côté de Serveur, cliquez sur Nouveau.
7. Dans Nom, tapez un nom pour le serveur, puis cliquez sur Créer.
8. Dans la boîte de dialogue Créer un serveur d'authentification, dans Nom, tapez le nom du serveur.

9. En regard de Deux facteurs, sélectionnez ACTIVÉ.
10. Dans le champ Nom d'utilisateur, sélectionnez Subject:CN, puis cliquez sur Créer.
11. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez Valeur vraie, cliquez sur Ajouter une expression, sur Créer, puis sur Fermer.

Après avoir créé la stratégie d'authentification des certificats, liez-la au serveur virtuel. Après avoir lié la stratégie d'authentification de certificat, liez la stratégie d'authentification LDAP au serveur virtuel.

Important : Vous devez lier la stratégie d'authentification de certificat au serveur virtuel avant de lier la stratégie d'authentification LDAP au serveur virtuel.

Pour installer un certificat racine sur NetScaler Gateway

Après avoir créé la stratégie d'authentification des certificats, vous téléchargez et installez un certificat racine à partir de votre autorité de certification au format Base64, puis vous l'enregistrez sur votre ordinateur. Vous pouvez ensuite télécharger le certificat racine sur NetScaler Gateway.

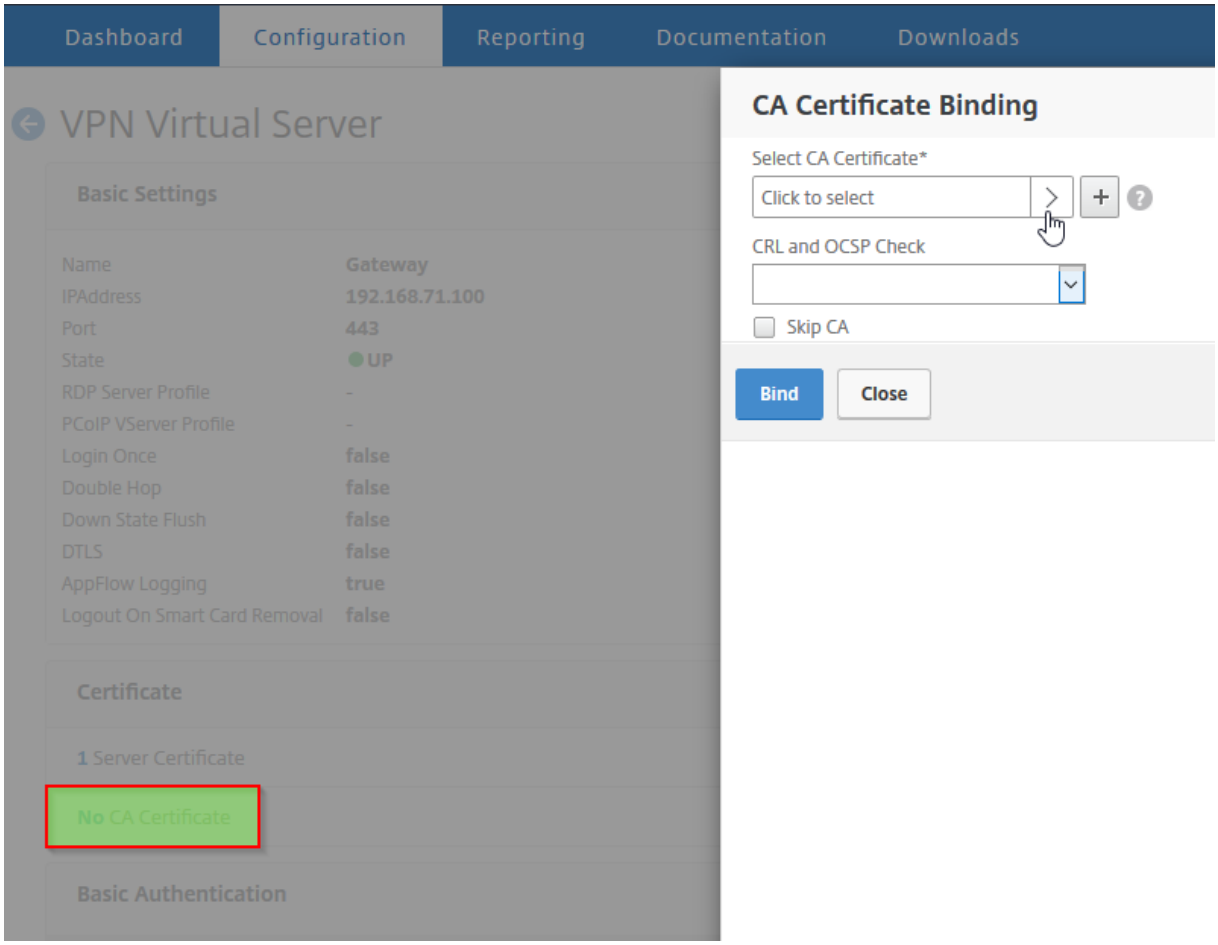
1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez SSL, puis cliquez sur Certificats.
2. Dans le volet d'informations, cliquez sur Installer.
3. Dans Certificat - Nom de la paire de clés, tapez un nom pour le certificat.
4. Dans Nom du fichier de certificat, cliquez sur Parcourir et dans la liste, sélectionnez Appliance ou Local.
5. Accédez au certificat racine, cliquez sur Ouvrir, puis sur Installer.

Pour ajouter un certificat racine à un serveur virtuel

Après avoir installé le certificat racine sur NetScaler Gateway, ajoutez-le au magasin de certificats du serveur virtuel.

Important : Lorsque vous ajoutez le certificat racine au serveur virtuel pour l'authentification par carte à puce, vous devez sélectionner le certificat dans la zone de liste
Sélectionner un certificat d'autorité de certification, comme illustré dans la figure suivante.

Figure 1. Ajout d'un certificat racine en tant qu'autorité de certification



1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur Ouvrir.
3. Dans l'onglet Certificats, sous Disponible, sélectionnez le certificat, en regard de Ajouter, dans la liste, cliquez sur CA, puis sur OK.
4. Répétez l'étape 2.
5. Dans l'onglet Certificats, cliquez sur Paramètres SSL.
6. Sous Autres, sélectionnez Authentification du client.
7. Sous Autres, en regard de Certificat client, sélectionnez Facultatif, puis cliquez deux fois sur OK.
8. Après avoir configuré le certificat client, testez l'authentification en vous connectant à NetScaler Gateway avec le client Citrix Secure Access. Si plusieurs certificats sont installés, un message vous invite à sélectionner le bon certificat. Une fois le certificat sélectionné, l'écran d'ouverture de session apparaît avec le nom d'utilisateur renseigné avec les informations obtenues à partir du certificat. Tapez le mot de passe, puis cliquez sur Connexion.

Si vous ne voyez pas le nom d'utilisateur correct dans le champ Nom d'utilisateur de l'écran d'ouverture de session, vérifiez les comptes d'utilisateurs et les groupes de votre annuaire LDAP. Les groupes définis sur NetScaler Gateway doivent être les mêmes que ceux de l'annuaire LDAP. Dans Active Directory, configurez les groupes au niveau de la racine du domaine. Si vous créez des groupes Active Directory qui ne se trouvent pas au niveau racine du domaine, une lecture incorrecte du certificat client peut en résulter.

Si les utilisateurs et les groupes ne se trouvent pas au niveau racine du domaine, la page d'ouverture de session de NetScaler Gateway affiche le nom d'utilisateur configuré dans Active Directory. Par exemple, dans Active Directory, vous avez un dossier appelé Utilisateurs et le certificat indique CN=Users. Dans la page d'ouverture de session, dans Nom d'utilisateur, le mot Utilisateurs apparaît.

Si vous ne souhaitez pas déplacer vos comptes de groupe et d'utilisateur vers le niveau du domaine racine, lors de la configuration du serveur d'authentification par certificat sur NetScaler Gateway, laissez les champs Nom d'utilisateur et Nom de groupe vides.

Configuration de l'authentification unique

January 26, 2024

Vous pouvez configurer NetScaler Gateway pour qu'il prenne en charge l'authentification unique avec Windows, les applications Web (telles que SharePoint), les partages de fichiers et l'interface Web. L'authentification unique s'applique également aux partages de fichiers auxquels les utilisateurs peuvent accéder via l'utilitaire de transfert de fichiers dans l'interface d'accès ou depuis le menu d'icônes NetScaler Gateway dans la zone de notification.

Si vous configurez l'authentification unique lorsque les utilisateurs ouvrent une session, ils sont automatiquement reconnectés sans avoir à entrer leurs informations d'identification une deuxième fois.

Configuration de l'authentification unique avec Windows

March 27, 2024

Les utilisateurs ouvrent une connexion en démarrant le client Citrix Secure Access depuis le bureau. Vous pouvez spécifier que le client Citrix Secure Access démarre automatiquement lorsque l'utilisateur ouvre une session Windows en activant l'authentification unique. Lorsque vous configurez l'authentification unique, les informations d'identification Windows des utilisateurs sont transmises

à NetScaler Gateway à des fins d'authentification. L'activation de l'authentification unique pour le client Citrix Secure Access facilite les opérations sur la machine utilisateur, telles que les scripts d'installation et le mappage automatique des lecteurs.

Activez l'authentification unique uniquement si les machines utilisateur se connectent au domaine de votre organisation. Si l'authentification unique est activée et qu'un utilisateur se connecte à partir d'un appareil qui n'est pas sur votre domaine, l'utilisateur est invité à ouvrir une session.

Vous configurez l'authentification unique avec Windows soit globalement, soit à l'aide d'un profil de session attaché à une stratégie de session.

Pour configurer l'authentification unique avec Windows dans le monde entier

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Expérience client**, cliquez sur **Single Sign-On with Windows**, puis cliquez sur **OK**.

Pour configurer l'authentification unique avec Windows à l'aide d'une stratégie de session

1. **Dans l'utilitaire de configuration, sous l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. **À côté de Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, en regard de **Single Sign-On with Windows**, cliquez sur **Override Global**, **sur Single Sign-On with Windows**, puis sur **OK**.
7. Dans la boîte de dialogue **Créer une politique de session**, à côté de **Expressions nommées**, sélectionnez **Général**, sélectionnez Valeur vraie, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Configuration de l'authentification unique sur les applications Web

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour fournir une authentification unique aux serveurs du réseau interne qui utilisent l'authentification Web. Avec l'authentification unique, vous pouvez rediriger l'utilisateur vers une page d'accueil personnalisée, telle qu'un site SharePoint ou vers l'interface Web. Vous pouvez également configurer l'authentification unique aux ressources via le client Citrix Secure Access à partir d'un favori configuré sur la page d'accueil ou d'une adresse Web que les utilisateurs saisissent dans le navigateur Web.

Si vous redirigez la page d'accueil vers un site SharePoint ou une interface Web, indiquez l'adresse Web du site. Lorsque les utilisateurs sont authentifiés, soit par NetScaler Gateway, soit par un serveur d'authentification externe, les utilisateurs sont redirigés vers la page d'accueil spécifiée. Les informations d'identification de l'utilisateur sont transmises de manière transparente au serveur Web. Si le serveur Web accepte les informations d'identification, les utilisateurs sont automatiquement connectés. Si le serveur Web refuse les informations d'identification, les utilisateurs reçoivent une invite d'authentification leur demandant leur nom d'utilisateur et leur mot de passe.

Vous pouvez configurer l'authentification unique pour les applications Web globalement ou à l'aide d'une stratégie de session.

Pour configurer l'authentification unique sur les applications Web à l'échelle mondiale

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Expérience client, cliquez sur Connexion unique aux applications Web, puis sur OK.

Pour configurer l'authentification unique sur les applications Web à l'aide d'une stratégie de session

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway > Policies, puis cliquez sur Session.
2. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez une stratégie de session, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer la stratégie de session, à côté de Profil de demande, cliquez sur Modifier.
4. Dans l'onglet Expérience client, en regard de Single Sign-On to Web Applications, cliquez sur Global Override, sur Single Sign-On to Web Applications, puis sur OK.

Pour définir le port HTTP pour l'authentification unique vers les applications Web

L'authentification unique est tentée uniquement pour le trafic réseau pour lequel le port de destination est considéré comme un port HTTP. Pour autoriser l'authentification unique aux applications qui utilisent un port autre que le port 80 pour le trafic HTTP, ajoutez un ou plusieurs numéros de port sur NetScaler Gateway. Vous pouvez activer plusieurs ports. Les ports sont configurés globalement.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Configuration réseau, cliquez sur Paramètres avancés.
4. Sous Ports HTTP, tapez le numéro de port, cliquez sur Ajouter, puis cliquez deux fois sur OK.

   Vous pouvez répéter l'étape 4 pour chaque port que vous souhaitez ajouter.

Remarque : Si les applications Web du réseau interne utilisent des adresses IP publiques, l'authentification unique ne fonctionne pas. Pour activer l'authentification unique, le split tunneling doit être activé dans le cadre du paramètre de stratégie globale, que l'accès sans client ou le client Citrix Secure Access soit utilisé pour les connexions aux machines des utilisateurs. S'il n'est pas possible d'activer le split tunneling au niveau global, créez un serveur virtuel qui utilise une plage d'adresses privée.

Configuration de l'authentification unique sur les applications Web à l'aide de LDAP

March 27, 2024

Lorsque vous configurez l'authentification unique et que les utilisateurs ouvrent une session à l'aide du nom d'utilisateur principal (UPN) au format username@domain.com, l'authentification unique échoue par défaut et les utilisateurs doivent s'authentifier deux fois. Si vous devez utiliser ce format pour l'ouverture de session utilisateur, modifiez la stratégie d'authentification LDAP pour accepter ce formulaire de nom d'utilisateur.

Pour configurer l'authentification unique sur les applications Web

1. Dans l'utilitaire de configuration, dans l'onglet **Configuration**, développez **NetScaler Gateway > Policies**Authentication.
2. Dans le volet d'informations, sous **l'onglet Stratégies**, sélectionnez une stratégie LDAP, puis cliquez sur **Ouvrir**.

3. Dans la boîte de dialogue **Configurer la politique d'authentification**, à côté de **Serveur**, cliquez sur **Modifier**.
4. Sous **Paramètres de connexion**, dans le DN de base (emplacement des utilisateurs), tapez DC=domainname, DC=com.
5. Dans **Administrator Bind DN**, tapez LDAPaccount@domainname.com, où domainname.com est le nom de votre domaine.
6. Dans **Mot de passe administrateur** et **Confirmer le mot de passe administrateur**, tapez le mot de
7. Sous **Autres paramètres**, dans **Attribut du nom d'ouverture de session du serveur**, saisissez UserPrincipalName.
8. Dans **Attribut de groupe**, saisissez MemberOf.
9. Dans **Nom du sous-attribut**, saisissez CN.
10. Dans **Attribut de nom SSO**, tapez le format selon lequel les utilisateurs ouvrent une session, puis cliquez deux fois sur **OK**. Cette valeur est soit, `SamAccountName` soit `UserPrincipalName`.

Configuration de l'authentification unique sur un domaine

March 27, 2024

Si les utilisateurs se connectent à des serveurs exécutant Citrix Virtual Apps et utilisent SmartAccess, vous pouvez configurer l'authentification unique pour les utilisateurs qui se connectent à la batterie de serveurs. Lorsque vous configurez l'accès aux applications publiées à l'aide d'une stratégie de session et d'un profil, utilisez le nom de domaine de la batterie de serveurs.

Vous pouvez également configurer l'authentification unique pour les partages de fichiers de votre réseau.

Pour configurer l'authentification unique sur un domaine

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway > Policies, puis cliquez sur Session.
2. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez une stratégie de session, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer la stratégie de session, à côté de Profil de demande, cliquez sur Modifier.
4. Dans la boîte de dialogue Configurer le profil de session, sous l'onglet Applications publiées, dans Domaine d'authentification unique, cliquez sur Remplacer global, tapez le nom de domaine, puis cliquez deux fois sur OK.

Pour plus d'informations sur la configuration de NetScaler Gateway avec Citrix Virtual Apps, voir Intégrer NetScaler Gateway à Citrix Virtual Apps andDesktops.

Configuration de l'authentification unique pour Microsoft Exchange 2010

January 26, 2024

La section suivante décrit la configuration de l'authentification unique (SSO) pour Microsoft Exchange 2010 sur NetScaler Gateway. L'accès SSO pour Outlook Web Access (OWA) 2010 ne fonctionne pas dans les conditions suivantes :

- Utilisation de l'authentification basée sur les formulaires sur Microsoft Exchange 2010.
- Serveur virtuel d'équilibrage de charge avec stratégie de gestion du trafic d'authentification, d'autorisation et d'audit.

> **Remarque :** Cette configuration fonctionne uniquement pour le serveur virtuel d'équilibrage de charge avec stratégie de gestion du trafic d'authentification, d'autorisation et d'audit. Il ne fonctionne pas pour l'SSO dans OWA 2010 avec un VPN sans client.

Les étapes suivantes sont des prérequis que vous devez prendre en compte avant de configurer le SSO pour Microsoft Exchange 2010 sur NetScaler Gateway.

- L'URL d'action pour le formulaire SSO est différente dans OWA 2010. Modifiez la stratégie de gestion du trafic en conséquence.
- Vous avez besoin d'une stratégie de réécriture pour définir le `PBack` cookie dans la demande logon.aspx. Dans des scénarios normaux, vous définissez le `PBack` cookie sur le client et cliquez sur Envoyer.
- Lorsque vous utilisez le SSO, la réponse à logon.aspx est consommée et NetScaler Gateway génère la demande de formulaire. Le cookie n'est pas joint à la demande de soumission du formulaire.
- Le serveur OWA attend le `PBack` cookie dans la demande de soumission du formulaire. La stratégie de réécriture est nécessaire pour joindre le `PBack` cookie à la demande de soumission du formulaire.

Effectuez les opérations suivantes à l'aide de l'interface de ligne de commande

1. Configuration de la gestion du trafic d'authentification, d'autorisation et d'audit


```
add tm formSSOAction OWA_Form_SSO_SSOPro -actionURL "/owa/auth.
owa"-userField username -passwdField password -ssoSuccessRule "
http.RES.SET_COOKIE.COOKIE(\"cadata\").VALUE(\"cadata\").LENGTH.
GT(70"-responsesize 15000 -submitMethod POST
```

2. Configurez la stratégie de gestion du trafic et liez la stratégie

   - `add tm trafficAction OWA_2010_Prof -appTimeout 1 -SSO ON -formSSO Action OWA_Form_SSO_SSOPro`
   - `add tm trafficPolicy owa2k10_pol "HTTP.REQ.URL.CONTAINS(\"owa/auth/logon.aspx\")"OWA_2010_Prof`
   - `bind tm global -policyName owa2k10_pol -priority 100`

Réécrire la configuration à l'aide de la CLI

À l'invite de commandes, tapez :

- `add rewrite action set_pback_cookie insert_after "http.REQ.COOKIE.VALUE(\"OutlookSession\")""\";PBack=0\""-bypassSafetyCheck YES`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Configuration de réécriture alternative

Dans de rares cas, Microsoft Outlook peut ne pas émettre de cookies de session OWA et les `Pback` cookies peuvent également ne pas être insérés. Le problème peut se produire après que vous ayez exécuté les commandes précédentes pour implémenter la configuration de réécriture.

Pour surmonter de tels scénarios et pour contourner ce problème, vous pouvez configurer les commandes suivantes au lieu de la configuration de réécriture.

À l'invite de commandes, tapez :

- `add rewrite action set_pback_cookie insert_http_header "Cookie"'" PBack=0"'`
- `add rewrite policy set_pback_cookie "http.REQ.URL.CONTAINS(\"logon.aspx\")"set_pback_cookie`
- `set rewrite policy set_pback_cookie -action set_pback_cookie`
- `bind rewrite global set_pback_cookie 100 END -type REQ_DEFAULT`

Configuration de l'utilisation unique d'un mot de passe

January 26, 2024

Vous pouvez configurer NetScaler Gateway pour qu'il utilise des mots de passe à usage unique, tels qu'un jeton, un code d'identification personnel (PIN) ou un code d'accès. Une fois qu'un utilisateur a entré le code secret ou le code PIN, le serveur d'authentification invalide immédiatement le mot de passe à usage unique et l'utilisateur ne peut pas entrer à nouveau le même code PIN ou mot de passe.

Les produits qui incluent l'utilisation d'un mot de passe à usage unique sont les suivants :

- RSA SecurID
- Imprivata OneSign
- SafeWord
- Gemalto Protiva
- Nordic SMS PASSCODE

Pour utiliser chacun de ces produits, configurez le serveur d'authentification du réseau interne pour qu'il utilise RADIUS. Pour plus d'informations, consultez Configuration de l'authentification RADIUS.

Si vous configurez l'authentification sur NetScaler Gateway pour utiliser un mot de passe à usage unique avec RADIUS, tel que fourni par un jeton RSA SecurID, par exemple, NetScaler Gateway tente de réauthentifier les utilisateurs à l'aide du mot de passe mis en cache. Cette réauthentification se produit lorsque vous apportez des modifications à NetScaler Gateway ou si la connexion entre le client Citrix Secure Access et NetScaler Gateway est interrompue puis rétablie.

Une tentative de réauthentification peut également se produire lorsque les connexions sont configurées pour utiliser l'application Citrix Workspace et que les utilisateurs se connectent à l'interface Web à l'aide de RADIUS ou de LDAP. Lorsqu'un utilisateur démarre une application et l'utilise, puis retourne dans Receiver pour démarrer une autre application, NetScaler Gateway utilise les informations mises en cache pour authentifier l'utilisateur.

Configuration de l'authentification RSA SecurID

January 26, 2024

Lorsque vous configurez le serveur RSA/ACE pour l'authentification RSA SecureID, vous devez effectuer les étapes suivantes :

Configurez le client RADIUS avec les informations suivantes :

- Indiquez le nom de l'appliance NetScaler Gateway.
- Fournissez une description (non obligatoire).
- Indiquez l'adresse IP du système.
- Fournissez le secret partagé entre NetScaler Gateway et le serveur RADIUS.
- Configurez la marque ou le modèle en tant que RADIUS standard.

Dans la configuration de l'hôte de l'agent, vous devez disposer des informations suivantes :

- Indiquez le nom de domaine complet (FQDN) de NetScaler Gateway (tel qu'il apparaît sur le certificat lié au serveur virtuel). Après avoir fourni le nom de domaine complet, cliquez sur la touche de tabulation et la fenêtre Adresse réseau s'affiche automatiquement.

  Une fois que vous avez entré le nom de domaine complet, l'adresse réseau apparaît automatiquement. Si ce n'est pas le cas, saisissez l'adresse IP du système.
- Indiquez le type d'agent à l'aide du Serveur de communication.
- Configurez pour importer tous les utilisateurs ou un ensemble d'utilisateurs autorisés à s'authentifier via NetScaler Gateway.

S'il n'est pas déjà configuré, créez une entrée d'hôte de l'agent pour le serveur RADIUS, y compris les informations suivantes :

- Indiquez le nom de domaine complet du serveur RSA.

  Une fois que vous avez entré le nom de domaine complet, l'adresse réseau apparaît automatiquement. Si ce n'est pas le cas, indiquez l'adresse IP du serveur RSA.
- Indiquez le type d'agent, qui est le serveur RADIUS.

Pour plus d'informations sur la configuration d'un serveur RADIUS RSA, consultez la documentation du fabricant.

Pour configurer RSA SecurID, créez un profil d'authentification et une stratégie, puis liez la stratégie globalement ou à un serveur virtuel. Pour créer une stratégie RADIUS pour utiliser RSA SecurID, consultez Configuration de l'authentification RADIUS.

Après avoir créé la stratégie d'authentification, liez-la à un serveur virtuel ou globalement. Pour plus d'informations, consultez la section Stratégies d'authentification de liaison.

Configuration du retour de mot de passe avec RADIUS

March 27, 2024

Vous pouvez remplacer les mots de passe de domaine par un mot de passe à usage unique généré par un jeton à partir d'un serveur RADIUS. Lorsque les utilisateurs se connectent à NetScaler Gateway, ils saisissent un numéro d'identification personnel (PIN) et le code d'accès du jeton. Une fois que NetScaler Gateway a validé ses informations d'identification, le serveur RADIUS renvoie le mot de passe Windows de l'utilisateur à NetScaler Gateway. NetScaler Gateway accepte la réponse du serveur, puis utilise le mot de passe renvoyé pour l'authentification unique au lieu d'utiliser le code d'accès saisi par les utilisateurs lors de la connexion. Ce retour de mot de passe avec la fonctionnalité RADIUS vous permet de configurer l'authentification unique sans que les utilisateurs n'aient besoin de rappeler leur mot de passe Windows.

Lorsque les utilisateurs ouvrent une session en utilisant la fonction de retour de mot de passe, ils peuvent accéder à toutes les ressources réseau autorisées sur le réseau interne, y compris Citrix Endpoint Management, StoreFront et l'interface Web.

Pour activer l'authentification unique à l'aide des mots de passe renvoyés, vous configurez une stratégie d'authentification RADIUS sur NetScaler Gateway à l'aide des paramètres Password Vendor Identifier et Password Attribute Type. Ces deux paramètres renvoient le mot de passe Windows de l'utilisateur à NetScaler Gateway.

NetScaler Gateway prend en charge Imprivata OneSign. La version minimale requise d'Imprivata OneSign est 4.0 avec le Service Pack 3. L'identifiant du fournisseur de mot de passe par défaut pour Imprivata OneSign est 398. Le code de type d'attribut de mot de passe par défaut pour Imprivata OneSign est 5.

Vous pouvez utiliser d'autres serveurs RADIUS pour renvoyer un mot de passe, tels que RSA, Cisco ou Microsoft. Configurez le serveur RADIUS pour qu'il renvoie le mot de passe d'authentification unique de l'utilisateur dans une paire de valeurs d'attribut spécifique au fournisseur. Dans une stratégie d'authentification NetScaler Gateway, vous devez ajouter les paramètres **Password Vendor Identifier et Password** Attribute Type pour ces serveurs.

Vous trouverez une liste complète des identificateurs de fournisseurs sur le site Web de l'IANA (Internet Assigned Numbers Authority). Par exemple, l'identificateur de fournisseur pour la sécurité RSA est 2197, pour Microsoft, il est 311 et pour Cisco Systems, il est 9. L'attribut spécifique au fournisseur pris en charge par un fournisseur doit être confirmé auprès du fournisseur. Par exemple, Microsoft a publié une liste d'attributs spécifiques au fournisseur sous Attributs RADIUS spécifiques au fournisseur Microsoft.

Vous pouvez sélectionner n'importe quel attribut spécifique au fournisseur pour stocker le mot de passe d'authentification unique des utilisateurs sur le serveur RADIUS du fournisseur. Si vous configurez NetScaler Gateway avec l'identifiant du fournisseur et l'attribut dans lesquels le mot de passe utilisateur est stocké sur le serveur RADIUS, NetScaler Gateway demande la valeur de l'attribut dans le paquet de demande d'accès envoyé au serveur RADIUS. Si le serveur RADIUS répond avec la paire attribut-valeur correspondante dans le paquet d'acceptation d'accès, le retour du mot de passe fonctionne quel que soit le serveur RADIUS que vous utilisez.

Pour configurer l'authentification unique à l'aide des mots de passe renvoyés :

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, développez **NetScaler Gateway > Policies \ > Authentication**.
2. Dans le volet de navigation, cliquez sur **RADIUS**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer une politique d'authentification**, dans Nom, tapez le nom de la stratégie.
5. À côté de **Serveur**, cliquez sur **Nouveau**.
6. Dans **Nom**, tapez le nom du serveur.
7. Configurez les paramètres du serveur RADIUS.
8. Dans **Identificateur de fournisseur de mot**de passe, tapez l'identificateur du fournisseur renvoyé par le serveur RADIUS. Cet identifiant doit avoir une valeur minimale de 1.
9. Dans **Type d'attribut de mot de passe**, tapez le type d'attribut renvoyé par le serveur RADIUS dans le code AVP spécifique au fournisseur. La valeur peut aller de 1 à 255.
10. Dans la boîte de dialogue **Créer une politique d'authentification**, à côté de **Expressions nommées**, sélectionnez l'expression, cliquez sur **Ajouter** une expression, sur **Créer**, puis sur **Fermer**.

Configuration de l'authentification SafeWord

January 26, 2024

La gamme de produits SafeWord permet de fournir une authentification sécurisée à l'aide d'un code secret basé sur des jetons. Une fois que les utilisateurs ont saisi un code secret, celui-ci est invalidé par SafeWord et ne peut plus être utilisé.

Si Access Gateway remplace Secure Gateway dans un déploiement Secure Gateway et Interface Web, vous pouvez choisir de ne pas configurer l'authentification sur Access Gateway et de continuer à autoriser l'interface Web à fournir une authentification SafeWord pour le trafic HTTP entrant.

Access Gateway prend en charge l'authentification SafeWord pour les produits suivants :

- SafeWord 2008
- SafeWord PremierAccess
- SafeWord pour Citrix
- SafeWord RemoteAccess

Vous pouvez configurer Access Gateway pour qu'il s'authentifie à l'aide des produits SafeWord de la manière suivante :

- Configurez l'authentification pour utiliser un serveur RADIUS PremierAccess installé dans le cadre de SafeWord PremierAccess et autorisez-le à gérer l'authentification.
- Configurez l'authentification pour utiliser l'agent SafeWord IAS, qui est un composant de SafeWord RemoteAccess, SafeWord pour Citrix et SafeWord PremierAccess 4.0.
- Installez l'agent d'interface Web SafeWord pour prendre en charge l'interface Web Citrix. Il n'est pas nécessaire de configurer l'authentification sur Access Gateway et l'interface Web Citrix peut gérer cela. Cette configuration n'utilise pas le serveur RADIUS PremierAccess ni l'agent SafeWord IAS.

Lorsque vous configurez le serveur RADIUS SafeWord, vous avez besoin des informations suivantes :

- L'adresse IP d'Access Gateway. Lorsque vous configurez les paramètres du client sur le serveur RADIUS, utilisez l'adresse IP Access Gateway.
- Un secret commun.
- L'adresse IP et le port du serveur SafeWord.

Configuration de l'authentification Gemalto Protiva

January 26, 2024

Protiva est une plateforme d'authentification forte qui a été développée pour exploiter les points forts de l'authentification par carte à puce de Gemalto. Avec Protiva, les utilisateurs ouvrent une session avec un nom d'utilisateur, un mot de passe et un mot de passe unique générés par l'appareil Protiva. Comme pour RSA SecurID, la demande d'authentification est envoyée au serveur d'authentification Protiva et le mot de passe est validé ou rejeté.

Pour configurer Gemalto Protiva afin qu'il prenne en charge NetScaler Gateway, suivez les instructions suivantes :

- Installez le serveur Protiva.
- Installez le plug-in de l'agent Protiva Internet Authentication Server (IAS) sur un serveur RADIUS Microsoft IAS. N'oubliez pas de noter l'adresse IP et le numéro de port du serveur IAS.

NFactor pour l'authentification par passerelle

March 27, 2024

L'authentification nFactor offre un tout nouvel ensemble de possibilités en matière d'authentification. Les administrateurs qui utilisent nFactor bénéficient d'une flexibilité d'authentification, d'

autorisation et d'audit lors de la configuration des facteurs d'authentification pour les serveurs virtuels.

Deux banques de polices ou deux facteurs ne limitent plus un administrateur. Le nombre de banques de polices peut être étendu pour répondre à différents besoins. En fonction des facteurs précédents, nFactor détermine une méthode d'authentification. Les formulaires de connexion dynamiques et les actions en cas d'échec sont possibles à l'aide de nFactor.

> **Important**
>
> - À partir de la version 13.0 build 67.x, l'authentification nFactor est prise en charge avec la licence Standard uniquement pour le serveur virtuel Gateway/VPN, et non pour le serveur virtuel d'authentification. Dans la licence Standard, l'interface graphique du visualiseur nFactor ne peut pas être utilisée pour créer l'EPA dans le flux nFactor. De plus, vous ne pouvez pas modifier le schéma de connexion, mais vous devez utiliser le schéma de connexion prêt à l'emploi tel quel.
> - Pour que NetScaler prenne en charge l'authentification nFactor, une licence Advanced ou Premium est requise. Pour plus d'informations sur l'authentification nFactor avec NetScaler, consultez la section Authentification nFactor.

Exigences relatives aux licences des fonctionnalités d'authentification, d'autorisation et d'audit

Le tableau suivant répertorie les exigences de licence pour les fonctionnalités d'authentification, d'autorisation et d'audit disponibles.

	Licence Standard	Licence avancée	Licence Premium
authentification LOCALE	Oui	Oui	Oui
Authentification LDAP	Oui	Oui	Oui
Authentification RADIUS	Oui	Oui	Oui
authentification TACACS	Oui	Oui	Oui
L'authentification Web	Oui	Oui	Oui

		Licence Standard	Licence avancée	Licence Premium
	Authentification du certificat client	Oui	Oui	Oui
	Négocier l'authentification	Oui	Oui	Oui
	Authentification SAML	Oui	Oui	Oui
	Authentification OAuth	Non	Oui	Oui
	OTP natif	Non	Oui	Oui
	Envoyer un e-mail à OTP	Non	Oui	Oui
	Notification Push pour OTP	Non	Non	Oui
	Question et réponse basées sur les connaissances (authentification KBA)	Non	Oui	Oui
	Réinitialisation du mot de passe en libre-service (SSPR)	Non	Oui	Oui
	Visualiseur nFactor	Oui	Oui	Oui

Remarque

- Pour savoir comment configurer nFactor pour la licence NetScaler Standard, consultez la section Créer un serveur virtuel Gateway pour l'authentification nFactor dansla licence NetScaler Standard.
- Seul un serveur virtuel d'authentification, d'autorisation et d'audit non adressable peut être lié à un serveur virtuel Gateway/VPN sous licence NetScaler Standard.

> • La personnalisation de LoginSchema n'est pas autorisée dans la licence NetScaler Standard. La prise en charge de nFactor est de base avec uniquement les schémas de connexion par défaut et déjà ajoutés fournis avec l'appliance. L'administrateur peut les utiliser dans sa configuration, mais il ne peut pas ajouter de schéma de connexion. Par conséquent, l'option GUI est désactivée.

Cas d'utilisation

L'authentification nFactor permet des flux d'authentification dynamiques basés sur le profil utilisateur. Parfois, les flux peuvent être simples et intuitifs pour l'utilisateur. Dans d'autres cas, ils peuvent être associés à la sécurisation d'Active Directory ou d'autres serveurs d'authentification. Voici quelques exigences spécifiques à Gateway :

1. **Sélection dynamique du nom d'utilisateur et du mot de passe.** Traditionnellement, les clients (y compris les navigateurs et les récepteurs) utilisent le mot de passe Active Directory (AD) comme premier champ de mot de passe. Le deuxième mot de passe est réservé pour le mot de passe à usage unique (OTP). Toutefois, pour sécuriser les serveurs AD, OTP doit d'abord être validé. nFactor peut le faire sans nécessiter de modifications du client.
2. **Point de terminaison d'authentification multi-locataires.** Certaines organisations utilisent des serveurs de passerelle différents pour les utilisateurs de certificats et de non-certificats. Les utilisateurs utilisant leurs propres appareils pour se connecter, les niveaux d'accès des utilisateurs varient selon l'appliance NetScaler en fonction de l'appareil utilisé. La passerelle peut répondre à différents besoins d'authentification.
3. **Authentification basée sur l'appartenance à un groupe.** Certaines organisations obtiennent des propriétés utilisateur à partir de serveurs AD pour déterminer les exigences d'authentification. Les exigences d'authentification peuvent varier en fonction des utilisateurs individuels.
4. **Cofacteurs d'authentification.** Parfois, différentes paires de stratégies d'authentification sont utilisées pour authentifier différents ensembles d'utilisateurs. La fourniture de stratégies de paire augmente l'efficacité de l'authentification. Les stratégies dépendantes peuvent être définies à partir d'un seul flux. De cette manière, des ensembles de stratégies indépendants deviennent des flux propres qui augmentent l'efficacité et réduisent la complexité.

Gestion des réponses d'authentification

Les registres de rappel de NetScaler Gateway gèrent les réponses d'authentification. Les réponses AAAD (démon d'authentification) et les codes de réussite/échec/erreur/dialogue sont transmises au gestionnaire de rappel. Les codes de succès/échec/erreur/dialogue amènent Gateway à prendre les mesures appropriées.

Soutien à la clientèle

Le tableau suivant détaille les détails de la configuration.

Client	Prise en charge NFactor	Point de liaison de la stratégie d'authentification	EPA
Navigateurs	Oui	Authentification	Oui
Application Citrix Workspace	Oui	VPN	Oui
Plug-in de passerelle	Oui	VPN	Oui

Remarque :

- L'application Citrix Workspace prend en charge l'authentification nFactor pour les systèmes d'exploitation pris en charge à partir des versions répertoriées suivantes.
  - Windows 4.12
  - Linux 13.10
  - Mac 1808
  - iOS 2007
  - Android 1808
  - HTML5 : pris en charge via Store Web
  - Chrome : pris en charge via Store Web

Configuration en ligne de commande

Le serveur virtuel Gateway a besoin d'un serveur virtuel d'authentification nommé en tant qu'attribut. Le nom du serveur virtuel en tant qu'attribut est la seule configuration requise pour ce modèle.

```
1 add authnProfile <name-of-profile> -authnVsName <name-of-auth-vserver>
2 <!--NeedCopy-->
```

Le nom AuthNvsName est le nom du serveur virtuel d'authentification. Le serveur virtuel AuthNvsName doit être configuré avec des stratégies d'authentification avancées et est utilisé pour l'authentification NFactor.

```
1 add vpn vserver <name> <serviceType> <IP> <PORT> -authnProfile <name-of
     -profile>
2 set vpn vserver <name> -authnProfile <name-of-profile>
3 <!--NeedCopy-->
```

Où AuthnProfile est le profil d'authentification créé précédemment.

Défis Interop

La plupart des clients Legacy Gateway, en plus des clients RFWeb, sont modélisés sur les réponses envoyées par Gateway. Par exemple, une réponse 302 à /vpn/index.html est attendue pour de nombreux clients. Ces clients dépendent également de divers cookies de passerelle tels que "pwcount ,"*"NSC_CERT."

Analyse des critères d'évaluation (EPA)

L'EPA dans nFactor n'est pas pris en charge pour le module d'authentification, d'autorisation et d'audit de NetScaler. Par conséquent, le serveur virtuel NetScaler Gateway exécute l'EPA. Après l'EPA, les informations d'identification de connexion sont envoyées au serveur virtuel d'authentification à l'aide de l'API mentionnée précédemment. Une fois l'authentification terminée, Gateway poursuit le processus de post-authentification et établit la session utilisateur.

Considérations relatives aux erreurs

Le client Gateway n'envoie les informations d'identification de l'utilisateur qu'une seule fois. La passerelle obtient une ou deux informations d'identification du client avec la demande de connexion. Dans le mode hérité, il y a deux facteurs au maximum. Les mots de passe obtenus sont utilisés pour ces facteurs. Cependant, avec nFactor, le nombre de facteurs pouvant être configurés est pratiquement illimité. Les mots de passe obtenus auprès du client Gateway sont réutilisés (conformément à la configuration) pour les facteurs configurés. Il faut veiller à ce que le mot de passe à usage unique (OTP) ne soit pas réutilisé plusieurs fois. De même, un administrateur doit s'assurer que le mot de passe réutilisé à un facteur est bien applicable à ce facteur.

Définition des clients

L'option de configuration est fournie pour aider NetScaler à différencier les clients du navigateur des clients volumineux tels que Receiver.

Un ensemble de modèles, ns_vpn_client_useragents, est fourni à l'administrateur pour configurer les modèles pour tous les clients.

De même, en liant la chaîne « Citrix Receiver » à la chaîne patset ci-dessus pour ignorer tous les clients dont l'agent utilisateur contient « Citrix Receiver ».

Restriction de NFactor pour Gateway

NFactor pour l'authentification de passerelle ne se produit pas si les conditions suivantes sont présentes.

1. Le AuthnProfile n'est pas défini sur NetScaler Gateway.
2. Les stratégies d'authentification avancées ne sont pas liées au serveur virtuel d'authentification et le même serveur virtuel d'authentification est mentionné dans `authnProfile`.
3. La chaîne User-Agent de la requête HTTP correspond aux User-Agents configurés dans `patset` ns_vpn_client_useragents.

Si ces conditions ne sont pas remplies, la stratégie d'authentification classique liée à Gateway est utilisée.

Si un User-Agent, ou une partie de celui-ci, est lié à ce qui est mentionné précédemment,`patset` les demandes provenant de ces agents utilisateurs ne participent pas au flux nFactor. Par exemple, la commande suivante limite la configuration pour tous les navigateurs (en supposant que tous les navigateurs contiennent « Mozilla » dans la chaîne de l'agent utilisateur) :

```
bind patset ns_vpn_client_useragents Mozilla
<!--NeedCopy-->
```

Schéma de connexion

LoginSchema est une représentation logique du formulaire d'ouverture de session. Le langage XML le définit. La syntaxe du LoginSchema est conforme à la spécification Common Forms Protocol de Citrix.

LoginSchema définit la « vue » du produit. Un administrateur peut fournir une description personnalisée, un texte d'assistance, etc. du formulaire. Le schéma de connexion inclut les étiquettes du formulaire lui-même. Un client peut fournir le message de réussite ou d'échec qui décrit le formulaire présenté à un moment donné.

Utilisez la commande suivante pour configurer un schéma de connexion.

```
add authentication loginSchema <name> -authenticationSchema <string> [-
    userExpression <string>] [-passwdExpression <string>] [-
    userCredentialIndex <positive_integer>]
[-passwordCredentialIndex <positive_integer>] [-authenticationStrength
    <positive_integer>] [-SSOCredentials ( YES | NO )]
<!--NeedCopy-->
```

Description des paramètres

- name : nom du nouveau schéma de connexion. Il s'agit d'un argument obligatoire. Longueur maximale : 127
- AuthenticationSchema : nom du fichier de lecture du schéma d'authentification à envoyer pour l'interface utilisateur de la page de connexion. Ce fichier contient la définition XML des éléments

conformément au protocole d'authentification Citrix Forms pour pouvoir afficher le formulaire de connexion. Si l'administrateur ne souhaite pas inviter les utilisateurs à entrer d'autres informations d'identification, mais qu'il continue avec les informations d'identification obtenues précédemment, `noschema` peut être donné en argument. Cela s'applique uniquement aux schémas de connexion utilisés avec les facteurs définis par l'utilisateur, et non au facteur de serveur virtuel.

Il s'agit d'un argument obligatoire. Longueur maximale : 255

- userExpression - Expression pour l'extraction du nom d'utilisateur lors de la connexion. Il peut s'agir de n'importe quelle expression de stratégie avancée pertinente. Longueur maximale : 127
- userExpression - Expression pour l'extraction du mot de passe lors de la connexion. Il peut s'agir de n'importe quelle expression de stratégie avancée pertinente. Longueur maximale : 127
- userCredentialIndex - L'index dans lequel l'utilisateur a saisi le nom d'utilisateur doit être stocké dans la session. Valeur minimale : 1, Valeur maximale : 16
- passwordCredentialIndex - L'index dans lequel l'utilisateur a entré le mot de passe doit être stocké dans la session. Valeur minimale : 1, Valeur maximale : 16
- authenticationStrength - Poids de l'authentification actuelle Valeur minimale : 0, Valeur maximale : 65535
- `SSOCredentials` - Cette option indique si les informations d'identification de facteur actuelles sont les informations d'identification SSO (SingleSignon) par défaut. Valeurs possibles : OUI, NON. Valeur par défaut : NON

Connaissances requises pour LoginSchema et NFactor

Les fichiers LoginSchema prédéfinis se trouvent à l'emplacement NetScaler suivant /nsconfig/LoginSchema/LoginSchema/. Ces fichiers LoginSchema prédéfinis répondent aux cas d'utilisation courants et peuvent être modifiés pour de légères variations si nécessaire.

De plus, la plupart des cas d'utilisation à facteur unique avec peu de personnalisations n'ont pas besoin de la configuration du schéma de connexion.

Il est conseillé à l'administrateur de consulter la documentation pour connaître les autres options de configuration permettant à NetScaler de découvrir les facteurs. Une fois que l'utilisateur a soumis les informations d'identification, l'administrateur peut configurer plusieurs facteurs pour choisir et traiter les facteurs d'authentification de manière flexible.

Configuration de l'authentification à deux facteurs sans utiliser LoginSchema

NetScaler détermine automatiquement les exigences à double facteur en fonction de la configuration. Une fois que l'utilisateur présente ces informations d'identification, l'administrateur peut configurer le premier ensemble de stratégies sur le serveur virtuel. Pour chaque stratégie, il peut y avoir un « NextFactor » configuré en tant que « passthrough ». Un « passthrough » implique que NetScaler doit traiter l'ouverture de session à l'aide du jeu d'informations d'identification existant sans passer par l'utilisateur. En utilisant des facteurs de « passthrough », un administrateur peut piloter le flux d'authentification par programme. Il est conseillé aux administrateurs de lire la spécification nFactor ou les guides de déploiement pour plus de détails. Consultez la section Authentification multi-facteurs (nFactor).

Expressions de nom d'utilisateur et mot

Pour traiter les informations d'identification de connexion, l'administrateur doit configurer le schéma de connexion. Les cas d'utilisation à un ou deux facteurs avec peu de personnalisations LoginSchema ne nécessitent pas de définition XML spécifiée. Le schéma LoginSchema possède d'autres propriétés telles que UserExpression et PasswdExpression qui peuvent être utilisées pour modifier le nom d'utilisateur ou le mot de passe présenté par l'utilisateur.

Les schémas de connexion sont des expressions de stratégie avancées et peuvent également être utilisés pour remplacer l'entrée utilisateur. Cela peut être réalisé en ajoutant une chaîne pour les paramètres dans **-AuthenticationSchema**, comme illustré dans l'exemple suivant.

Voici des exemples de modification des entrées utilisateur pour le nom d'utilisateur et le mot de passe, respectivement.

- Changez l'entrée utilisateur pour le nom d'utilisateur de `username@citrix.com` à `username@xyz.com`

```
1 add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -userExpression "AAA.LOGIN.USERNAME.
    BEFORE_STR("@").APPEND("@xyz.com")"
2 <!--NeedCopy-->
```

- Imaginez un scénario dans lequel l'utilisateur fournit un mot de passe et un code secret dans le premier facteur dans le cadre du schéma de connexion configuré. Pour utiliser le **code secret** fourni par l'utilisateur dans le premier facteur et le **mot de passe** dans le second facteur, vous pouvez modifier le schéma de connexion existant à l'aide des commandes suivantes.

```
1 add authentication loginSchema user_schema -authenticationSchema
    LoginSchema/DualAuth.xml -passwdExpression "AAA.LOGIN.
    PASSWORD2"
2 <!--NeedCopy-->
```



```
add authentication loginSchema user_schema_second -
    authenticationSchema noschema  -passwdExpression "AAA.LOGIN.
    PASSWORD"
<!--NeedCopy-->
```

Étapes de haut niveau de la configuration NFactor

Le diagramme suivant illustre les étapes de haut niveau impliquées dans la configuration de nFactor.

Configuration de l'interface graphique

Les rubriques suivantes sont décrites dans cette section :

- Créer un serveur virtuel
- Créer un serveur virtuel d'authentification
- Créer un profil CERT d'authentification
- Créer une stratégie d'authentification
- Ajouter un serveur d'authentification LDAP
- Ajouter une stratégie d'authentification LDAP

- Ajouter un serveur d'authentification RADIUS
- Ajouter une stratégie d'authentification RADIUS
- Créer un schéma de connexion d'authentification
- Créer un libellé de stratégie

Créer un serveur virtuel

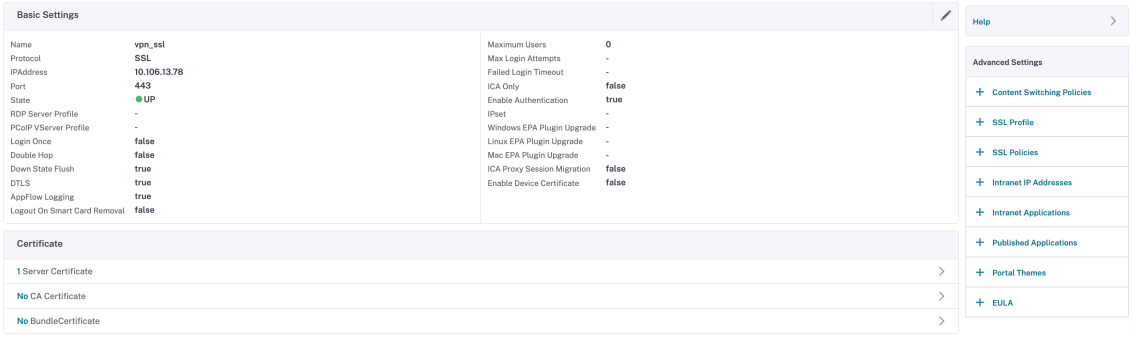
1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Cliquez sur le bouton **Ajouter** pour créer un serveur virtuel de passerelle.
3. Entrez les informations suivantes et cliquez sur **OK**.

Nom du paramètre	Description des paramètres
Entrez le nom du serveur virtuel.	Nom du serveur virtuel NetScaler Gateway. Doit commencer par un caractère alphabétique ASCII ou un trait de soulignement (_) et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), un espace, deux points (:), à (@), égal (=) et un trait d'union (-). Peut être modifié après la création du serveur virtuel. L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « mon serveur » ou « mon serveur »).
Entrez le type d'adresse IP du serveur virtuel	Sélectionnez une adresse IP ou une option non adressable dans le menu déroulant.
Entrez l'adresse IP du serveur virtuel.	Une adresse de protocole Internet (adresse IP) est une étiquette numérique attribuée à chaque périphérique participant au réseau informatique qui utilise le protocole Internet pour la communication.
Entrez le numéro de port du serveur virtuel.	Entrez le numéro de port.

Nom du paramètre	Description des paramètres
Entrez le profil d'authentification.	Entité de profil d'authentification sur le serveur virtuel. Cette entité peut être utilisée pour décharger l'authentification vers le serveur virtuel d'authentification, d'autorisation et d'audit pour l'authentification multifacteur (nFactor)
Entrez le profil du serveur RDP.	Nom du profil de serveur RDP associé au serveur virtuel.
Entrez le nombre maximal d'utilisateurs.	Nombre maximal de sessions utilisateur simultanées autorisées sur ce serveur virtuel. Le nombre réel d'utilisateurs autorisés à ouvrir une session sur ce serveur virtuel dépend du nombre total de licences utilisateur.
Entrez le nombre maximal de tentatives de connexion.	Nombre maximal de tentatives de connexion.
Entrez le délai d'expiration de la connexion en échec.	Nombre de minutes pendant lequel un compte est verrouillé si l'utilisateur dépasse le nombre maximal de tentatives autorisées.
Entrez la mise à niveau du plug-in Windows EPA.	Option permettant de définir le comportement de mise à niveau du plug-in pour Win.
Entrez la mise à niveau du plug-in Linux EPA.	Possibilité de définir le comportement de mise à niveau des plug-ins pour Linux.
Accédez à la mise à niveau du plug-in MAC EPA	Possibilité de définir le comportement de mise à niveau des plug-ins pour Mac.
Connexion une fois	Cette option active/désactive la connexion SSO transparente pour ce serveur virtuel.

Nom du paramètre	Description des paramètres
ICA uniquement	Lorsqu'il est défini sur ON, il implique le mode Basic dans lequel l'utilisateur peut ouvrir une session à l'aide de l'application Citrix Workspace ou d'un navigateur et accéder aux applications publiées configurées dans l'environnement Citrix Virtual Apps and Desktops indiqué par le paramètre `Wihome`. Les utilisateurs ne sont pas autorisés à se connecter à l'aide du client Citrix Secure Access et les scans des terminaux ne peuvent pas être configurés. Le nombre d'utilisateurs pouvant se connecter et accéder aux applications n'est pas limité par la licence dans ce mode. - Lorsqu'il est défini sur OFF, cela implique le mode SmartAccess dans lequel l'utilisateur peut se connecter à l'aide de l'application Citrix Workspace, d'un navigateur ou d'un client Citrix Secure Access. L'administrateur peut configurer les analyses des points de terminaison pour qu'elles soient exécutées sur les systèmes clients, puis utiliser les résultats pour contrôler l'accès aux applications publiées. Dans ce mode, le client peut se connecter à la passerelle dans d'autres modes client, à savoir VPN et VPN sans client. Le nombre d'utilisateurs pouvant se connecter et accéder aux ressources est limité par les licences CCU dans ce mode.
Activer l'authentification	Exigez l'authentification des utilisateurs qui se connectent à NetScaler Gateway.
Double Hop	Utilisez l'appliance NetScaler Gateway dans une configuration à double saut. Un déploiement à double saut fournit une couche de sécurité supplémentaire pour le réseau interne en utilisant trois pare-feu pour diviser la zone démilitarisée en deux étapes. Un tel déploiement peut comporter une appliance dans la zone démilitarisée et une appliance dans le réseau sécurisé.

Nom du paramètre	Description des paramètres
Flush de l'état bas	Fermez les connexions existantes lorsque le serveur virtuel est marqué en panne, ce qui signifie que le serveur a peut-être expiré. La déconnexion des connexions existantes libère des ressources et, dans certains cas, accélère la récupération des configurations d'équilibrage de charge surchargées. Activez ce paramètre sur les serveurs sur lesquels les connexions peuvent être fermées en toute sécurité lorsqu'elles sont marquées comme étant en panne. N'activez pas le vider de l'état DOWN sur les serveurs qui doivent terminer leurs transactions.
DTLS	Cette option démarre/arrête le service d'allumage sur le serveur virtuel
Journalisation AppFlow	Journaliser les enregistrements AppFlow qui contiennent des informations NetFlow ou IPFIX standard, telles que les horodatages pour le début et la fin d'un flux, le nombre de paquets et le nombre d'octets. Consignez également les enregistrements qui contiennent des informations au niveau de l'application, telles que les adresses Web HTTP, les méthodes de requête HTTP et les codes d'état de réponse, le temps de réponse du serveur et la latence.
Migration de session proxy ICA	Cette option détermine si une session de proxy ICA existante est transférée lorsque l'utilisateur ouvre une session à partir d'un autre appareil.
État	État actuel du serveur virtuel (UP, DOWN, BUSY, etc.).
Activer le certificat de périphérique	Indique si la vérification du certificat de l'appareil dans le cadre de l'EPA est activée ou désactivée.



4. Sélectionnez la section **Aucun certificat de serveur** de la page.
5. Cliquez sur ** sous **Sélectionner un certificat de serveur** pour sélectionner le certificat de serveur.
6. Sélectionnez le certificat SSL et cliquez sur le bouton **Sélectionner**.
7. Cliquez sur **Bind**.
8. Si vous voyez un avertissement indiquant qu'**aucun chiffrement utilisable s'affiche**, cliquez sur **OK**
9. Cliquez sur le bouton **Continuer**.
10. Dans la section Authentification, cliquez sur l'icône **+** en haut à droite.

Créer un serveur virtuel d'authentification

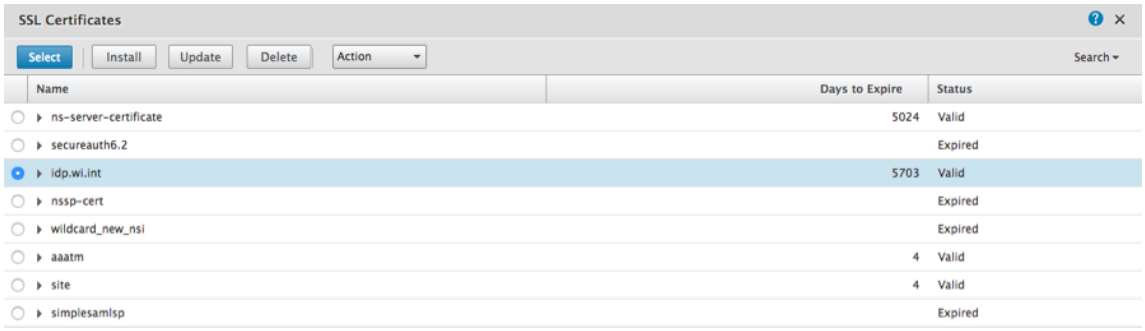
1. Accédez à **Sécurité > NetScaler AAA —Trafic des applications**> Serveurs virtuels.
2. Cliquez sur le bouton **Add**.
3. Renseignez les paramètres de base suivants pour créer le serveur virtuel d'authentification.

   Remarque : Le signe * à droite du nom du paramètre indique des champs obligatoires.

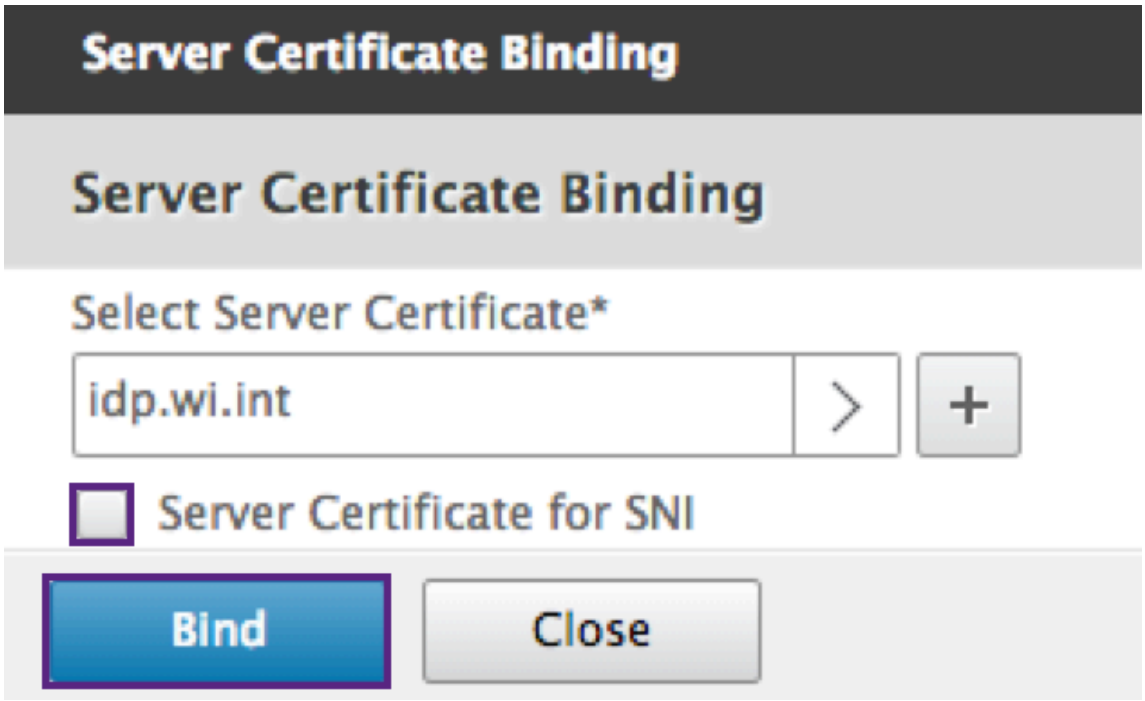
   - Entrez le **nom** du nouveau serveur virtuel d'authentification.
   - Entrez le **type d'adresse IP**. Le type d'adresse IP peut être configuré comme non adressable.
   - Entrez l'**adresse IP**. L'adresse IP peut être nulle.
   - Entrez le type de **protocole** du serveur virtuel d'authentification.
   - Entrez le **port TCP** sur lequel le serveur virtuel accepte les connexions.
   - Entrez le **domaine** du cookie d'authentification défini par le serveur virtuel d'authentification.
4. Cliquez sur **OK**.

5. Cliquez sur le **certificat No Server**.
6. Sélectionnez le certificat de serveur souhaité dans la liste.
7. Choisissez le certificat SSL souhaité et cliquez sur le bouton **Sélectionner**.

   Remarque : Le serveur virtuel d'authentification n'a pas besoin d'un certificat qui lui est lié.



8. Configurez la **liaison de certificat du serveur**.
   - Cochez la case **Certificat de serveur pour SNI** pour lier une ou plusieurs clés de certificat utilisées pour le traitement SNI.
   - Cliquez sur le bouton **Bind**.



Créer un profil CERT d'authentification

1. Accédez à **Sécurité -> NetScaler AAA —Trafic des applications -> Stratégies -> Authentification -> Stratégies de base -> CERT**.

2. Sélectionnez l'onglet Profils, puis **Ajouter**.
3. Remplissez les champs suivants pour créer le profil de CERT d'authentification. Le signe * à droite du nom du paramètre indique des champs obligatoires.
   - **Nom** : nom du profil du serveur d'authentification de certificat client (action).
   - **Deux facteurs** : dans ce cas, l'option d'authentification à deux facteurs est NOOP.
   - **Champ de nom d'utilisateur** : saisissez le champ client-cert à partir duquel le nom d'utilisateur est extrait. Doit être défini sur ""Subject""or ""Issuer""(inclure les deux jeux de guillemets doubles).
   - **Champ de nom de groupe** : saisissez le champ de certificat client à partir duquel le groupe est extrait. Doit être défini sur ""Subject""or ""Issuer""(inclure les deux jeux de guillemets doubles).
   - **Groupe d'authentification par** défaut : il s'agit du groupe par défaut qui est choisi lorsque l'authentification réussit en plus des groupes extraits.
4. Cliquez sur **Créer**.

Création d'une stratégie d'authentification

> **Remarque**
>
> Si vous configurez une stratégie de premier facteur avec une règle de stratégie à l'aide de AAA.Login, l'expression suivante doit être configurée avec la condition OR pour que l'application Citrix Workspace prenne en charge le déploiement nFactor.
>
> ```
> || HTTP.REQ.URL.CONTAINS("/cgi/authenticate")
> ```

1. Accédez à **Sécurité -> NetScaler AAA —Trafic des applications -> Stratégies -> Authentification -> Stratégies avancées -> Stratégie**.
2. Sélectionner le bouton **Ajouter**
3. Renseignez les informations suivantes pour créer une stratégie d'authentification. Le signe * à droite du nom du paramètre indique des champs obligatoires.

   a) **Nom** : saisissez le nom de la stratégie d'AUTHENTIFICATION avancée. Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne contenir que des lettres, des chiffres et des traits d'union (-), point (.) dièse (#), espace ( ), arobase (@), égal (=), deux-points (:) et trait de soulignement. Impossible de modifier une fois la stratégie d'authentification créée.

   L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « ma stratégie d'authentification » ou « ma stratégie d'authentification »).

b) **Type d'action :** entrez le type de l'action d'authentification.

c) **Action** : entrez le nom de l'action d'authentification à effectuer si la stratégie correspond.

d) **Action de consignation** : entrez le nom de l'action de journal des messages à utiliser lorsqu'une demande correspond à cette stratégie.

e) **Expression** : entrez le nom de la règle nommée NetScaler, ou d'une expression de syntaxe par défaut, que la stratégie utilise pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur AUTHENTICATION.

f) **Commentaires** : saisissez des commentaires pour conserver les informations relatives à cette stratégie.

4. Cliquez sur **Créer**.

Ajouter un serveur d'authentification LDAP

1. Accédez à **Sécurité -> NetScaler AAA —Trafic des applications -> Stratégies -> Authentification -> Stratégies de base -> LDAP**.
2. Ajoutez un serveur LDAP en sélectionnant l'onglet **Serveur** et en cliquant sur le bouton **Ajouter**.

Ajouter une stratégie d'authentification LDAP

1. Accédez à **Sécurité > NetScaler AAA —Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**.
2. Cliquez sur **Ajouter** pour ajouter une stratégie d'authentification.
3. Renseignez les informations suivantes pour créer une stratégie d'authentification. Le signe * à droite du nom du paramètre indique des champs obligatoires.

   a) **Nom : nom** de la stratégie d'AUTHENTIFICATION avancée.
   Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne contenir que des lettres, des chiffres et des traits d'union (-), point (.) dièse (#), espace ( ), arobase (@), égal (=), deux-points (:) et trait de soulignement. Impossible de modifier une fois la stratégie d'authentification créée.

   L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « ma stratégie d'authentification » ou « ma stratégie d'authentification »).

   b) **Type d'action** : type de l'action d'authentification.

   c) **Action** : nom de l'action d'authentification à effectuer si la stratégie correspond.

d) **Action de consignation** : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie.

e) **Expression** : nom de la règle nommée NetScaler, ou expression de syntaxe par défaut, que la stratégie utilise pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur AUTHENTICATION.

f) **Commentaires** - Tout commentaire visant à préserver les informations relatives à cette stratégie.

4. Cliquez sur **Créer**.

Ajouter un serveur d'authentification RADIUS

1. Accédez à **Sécurité > NetScaler AAA —Trafic des applications > Authentification des stratégies > Stratégies de base > RADIUS**.
2. Pour ajouter un serveur, sélectionnez l'onglet **Serveurs** et cliquez sur le bouton **Ajouter**.
3. Entrez les informations suivantes pour créer un serveur RADIUS d'authentification. Le signe * à droite du nom du paramètre indique des champs obligatoires.
   a) Entrez un **nom** pour l'action RADIUS.
   b) Entrez le **nom duserveur ou l'adresse IP du serveur** attribués au serveur RADIUS.
   c) Entrez le numéro de **port** sur lequel le serveur RADIUS écoute les connexions.
   d) Entrez la valeur du **délai** d'expiration en quelques secondes. L'appliance NetScaler attend une réponse du serveur RADIUS jusqu'à ce que la valeur de délai d'expiration configurée expire.
   e) Entrez la **clé secrète** qui est partagée entre le serveur RADIUS et l'appliance NetScaler. La clé secrète est requise pour permettre à l'appliance NetScaler de communiquer avec le serveur RADIUS.
   f) **Confirmez la clé secrète**.
4. Cliquez sur **Créer**.

Ajouter une stratégie d'authentification RADIUS

1. Accédez à **Sécurité > NetScaler AAA —Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégie**.
2. Cliquez sur **Ajouter** pour créer une stratégie d'authentification.

3. Renseignez les informations suivantes pour créer une stratégie d'authentification. Le signe * à droite du nom du paramètre indique des champs obligatoires.

   a) **Name** : nom de la stratégie d'AUTHENTIFICATION avancée.
   Doit commencer par une lettre, un chiffre ou le caractère de soulignement (_) et ne contenir que des lettres, des chiffres et des traits d'union (-), point (.) dièse (#), espace ( ), arobase (@), égal (=), deux-points (:) et trait de soulignement. Impossible de modifier une fois la stratégie d'AUTHENTIFICATION créée.

   L'exigence suivante s'applique uniquement à la CLI NetScaler : si le nom inclut un ou plusieurs espaces, placez le nom entre guillemets doubles ou simples (par exemple, « ma stratégie d'authentification » ou « ma stratégie d'authentification »).

   a) **Type d'action** : type de l'action d'authentification.

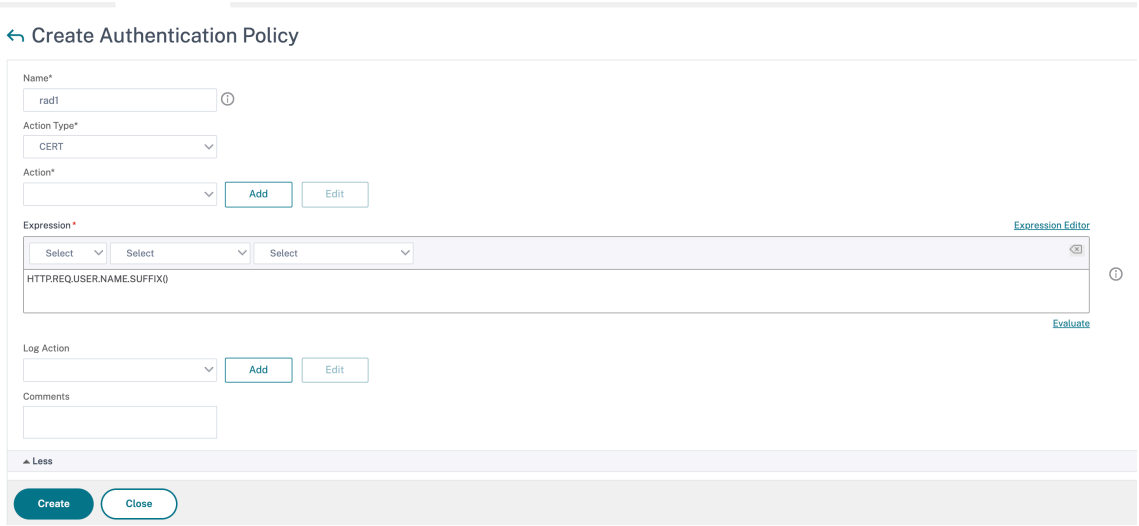
   b) **Action** : nom de l'action d'authentification à effectuer si la stratégie correspond.

   c) **Action de journalisation** : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie.

   d) **Expression** : nom de la règle nommée NetScaler, ou expression de syntaxe par défaut, que la stratégie utilise pour déterminer s'il faut tenter d'authentifier l'utilisateur auprès du serveur AUTHENTICATION.

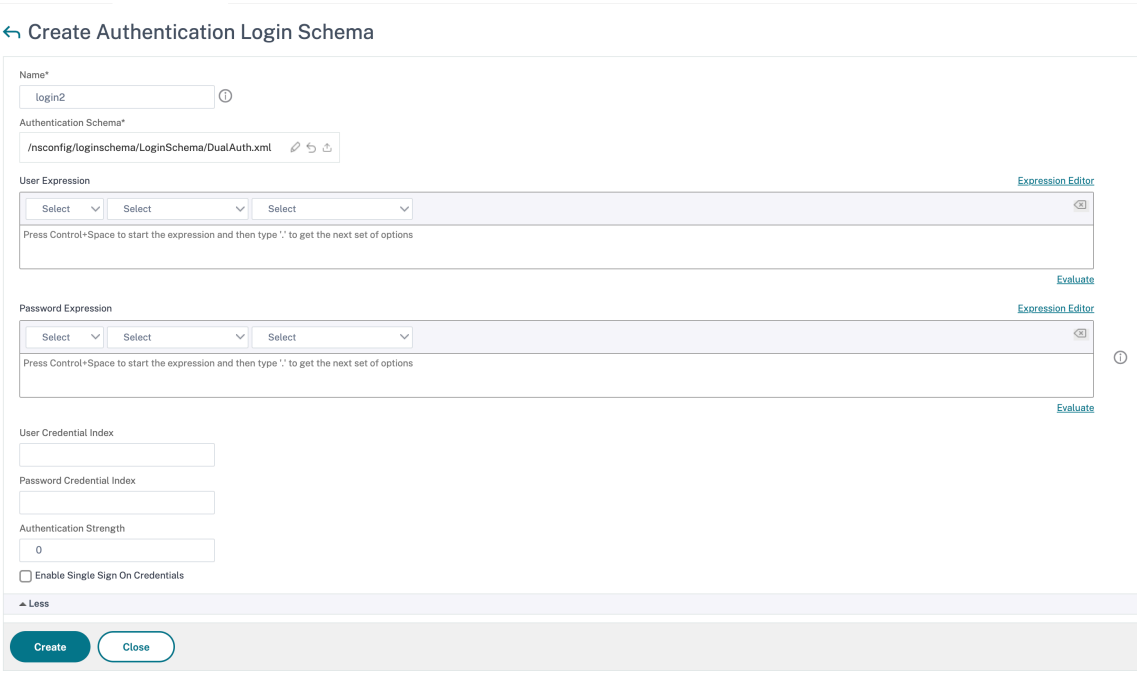
   e) **Commentaires** : tout commentaire destiné à préserver les informations relatives à cette stratégie.

4. Cliquez sur **OK.** La stratégie d'authentification que vous avez créée est répertoriée dans la liste des stratégies.



Créer un schéma de connexion d'authentification

1. Accédez à **Sécurité > NetScaler AAA —Trafic d'applications > Schéma de connexion**.
2. Sélectionnez l'onglet Profils et cliquez sur le bouton **Ajouter**.
3. Remplissez les champs suivants pour créer un schéma de connexion d'authentification :
   a) Saisir le **nom** : nom du nouveau schéma de connexion.
   b) Enter **Authentication Schema** : nom du fichier de lecture du schéma d'authentification à envoyer pour l'interface utilisateur de la page de connexion. Ce fichier doit contenir la définition XML des éléments conformément au protocole d'authentification Citrix Forms pour pouvoir afficher un formulaire de connexion. Si un administrateur ne souhaite pas inviter les utilisateurs à entrer d'autres informations d'identification, mais qu'ils continuent avec les informations d'identification précédemment obtenues, alors "noschema"peut être donné en tant qu'argument. Cela s'applique uniquement aux schémas de connexion utilisés avec des facteurs définis par l'utilisateur, et non au facteur de serveur virtuel.
   c) Enter **User Expression** : expression pour l'extraction du nom d'utilisateur lors de la connexion
   d) Enter **Password Expression** : expression pour l'extraction du mot de passe
   e) Enter **User Credential Index** : index dans lequel le nom d'utilisateur entré par l'utilisateur est stocké dans la session.
   f) Enter **Password Credential Index** : index dans lequel le mot de passe saisi par l'utilisateur doit être stocké dans la session.
   g) Enter **Authentication Strength** : poids de l'authentification actuelle.
4. Cliquez sur **Créer**. Le profil de schéma de connexion que vous avez créé doit apparaître dans la liste des profils de schéma de connexion.



Création d'une étiquette de stratégie

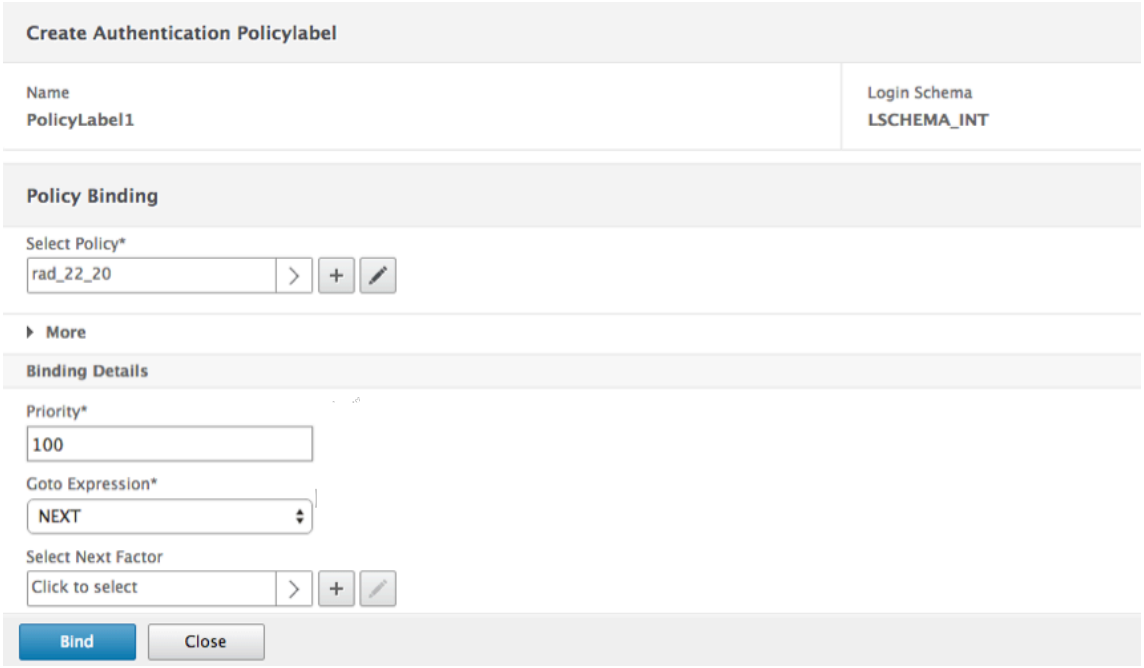
Une étiquette de stratégie spécifie les stratégies d'authentification pour un facteur particulier. Chaque étiquette de stratégie correspond à un seul facteur. L'étiquette de stratégie spécifie le formulaire de connexion qui doit être présenté à l'utilisateur. L'étiquette de stratégie doit être liée en tant que facteur suivant d'une stratégie d'authentification ou d'une autre étiquette de stratégie d'authentification. En règle générale, une étiquette de stratégie inclut des stratégies d'authentification pour un mécanisme d'authentification spécifique. Toutefois, vous pouvez également avoir une étiquette de stratégie qui comporte des stratégies d'authentification pour différents mécanismes d'authentification.

1. Accédez à **Sécurité > NetScaler AAA —Trafic des applications > Stratégies > Authentification > Stratégies avancées > Libellé de stratégie**.
2. Cliquez sur le bouton **Add**.
3. Remplissez les champs suivants pour créer une étiquette de stratégie d'authentification :
   a) Entrez le **nom** de la nouvelle étiquette de stratégie d'authentification.
   b) Entrez le **schéma de connexion** associé à l'étiquette de stratégie d'authentification.
   c) Cliquez sur **Continuer**.
4. **Sélectionnez une stratégie** dans le menu déroulant.
5. Choisissez la **stratégie d'authentification** souhaitée et cliquez sur le bouton **Sélectionner**.

6. Renseignez les champs suivants :

   a) Entrez la **priorité** de la liaison de stratégie.

   b) Entrez l'**expression Goto** : l'expression spécifie la priorité de la prochaine stratégie qui sera évaluée si la règle de stratégie actuelle est évaluée à TRUE.



7. Sélectionnez la stratégie d'authentification souhaitée, puis cliquez sur le bouton **Sélectionner**.
8. Cliquez sur le bouton **Bind**.
9. Cliquez sur **Terminé**.
10. Consultez l'étiquette de stratégie d'authentification.

Configuration Re-captcha pour l'authentification NFactor

À partir de la version 12.1 build 50.x de NetScaler, NetScaler Gateway prend en charge une nouvelle action de première classe, CaptchaAction, qui simplifie la configuration du Captcha. Captcha étant un premier recours collectif, il peut être un facteur à part entière. Vous pouvez injecter Captcha n'importe où dans le flux NFactor.

Auparavant, vous deviez également écrire des stratégies WebAuth personnalisées avec des modifications apportées à l'interface RFWebUI. Avec l'introduction de CaptchaAction, vous n'avez pas besoin de modifier le JavaScript.

> **Important**
>
> Si Captcha est utilisé avec des champs de nom d'utilisateur ou de mot de passe dans le schéma, le bouton Soumettre est désactivé jusqu'à ce que Captcha soit atteint.

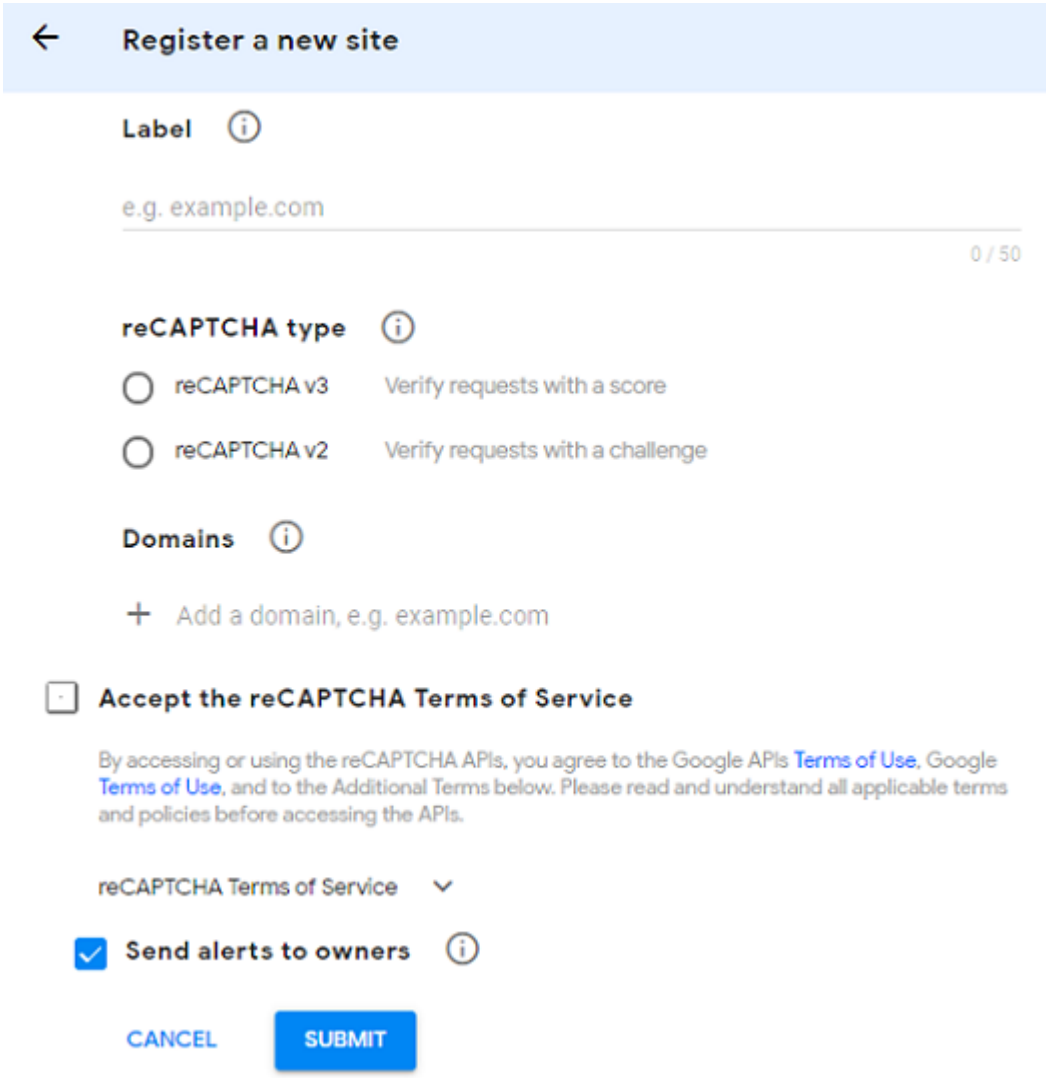
Configuration Captcha

La configuration Captcha comporte deux parties.

1. Configuration sur Google pour enregistrer Captcha.
2. Configuration sur l'appliance NetScaler pour utiliser le Captcha dans le cadre du flux de connexion.

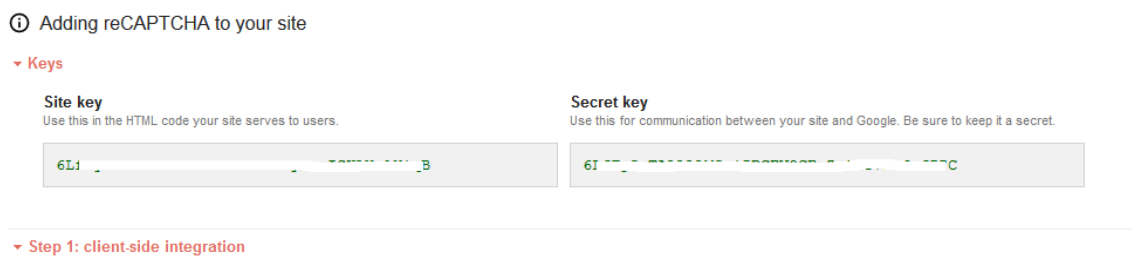
Configuration Captcha sur Google Enregistrez un domaine pour Captcha à l'adresse `https://www.google.com/recaptcha/admin#list`.

1. Lorsque vous accédez à cette page, l'écran suivant apparaît.



> **Remarque**
>
> Utilisez uniquement `reCAPTCHA` version v2. `reCAPTCHA` invisible est toujours en Tech Preview.

2. Après l'enregistrement d'un domaine, la « SiteKey » et la « SecretKey » s'affichent.



> **Remarque**
>
> Les paramètres « SiteKey » et « SecretKey » sont grisés pour des raisons de sécurité. « SecretKey » doit être gardé en sécurité.

Configuration du Captcha sur l'appliance NetScaler La configuration du Captcha sur l'appliance NetScaler peut être divisée en trois parties :

- Affichage de l'écran Captcha
- Publiez la réponse Captcha sur le serveur Google
- La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif)

Affichage de l'écran Captcha La personnalisation du formulaire de connexion s'effectue via le schéma de connexion SingleAuthCaptcha.xml. Cette personnalisation est spécifiée sur le serveur virtuel d'authentification et est envoyée à l'interface utilisateur pour afficher le formulaire de connexion. Le schéma de connexion intégré, SingleAuthCaptcha.xml, se trouve dans le /nsconfig/loginSchema/LoginSchema répertoire de l'appliance NetScaler.

> **Important**
>
> - En fonction de votre cas d'utilisation et de différents schémas, vous pouvez modifier le schéma existant. Par exemple, si vous n'avez besoin que du facteur Captcha (sans nom d'utilisateur ni mot de passe) ou d'une double authentification avec Captcha.
> - Si des modifications personnalisées sont effectuées ou si le fichier est renommé, Citrix recommande de copier tous les schémas de connexion du répertoire /nsconfig/loginschema/loginschema vers le répertoire parent, /nsconfig/loginschema.

Pour configurer l'affichage du Captcha à l'aide de l'interface de ligne de commande

```
1  -  add authentication loginSchema singleauthcaptcha -
       authenticationSchema /nsconfig/loginschema/SingleAuthCaptcha.xml
2
3  -  add authentication loginSchemaPolicy singleauthcaptcha -rule true -
       action singleauthcaptcha
4
5  -  add authentication vserver auth SSL <IP> <Port>
6
7  -  add ssl certkey vserver-cert -cert <path-to-cert-file> -key <path-to
       -key-file>
8  -  bind ssl vserver auth -certkey vserver-cert
9  -  bind authentication vserver auth -policy singleauthcaptcha -priority
        5 -gotoPriorityExpression END
10 <!--NeedCopy-->
```


Publiez la réponse Captcha sur le serveur Google Une fois que vous avez configuré le Captcha qui doit être affiché pour les utilisateurs, les administrateurs publient la configuration sur le serveur Google pour vérifier la réponse Captcha du navigateur.

Pour vérifier la réponse Captcha depuis le navigateur

```
1 - add authentication captchaAction myrecaptcha -sitekey <sitekey-
    copied-from-google> -secretkey <secretkey-from-google>
2
3 - add authentication policy myrecaptcha -rule true -action myrecaptcha
4 - bind authentication vserver auth -policy myrecaptcha -priority 1
5 <!--NeedCopy-->
```

Les commandes suivantes sont nécessaires pour configurer si l'authentification AD est souhaitée. Sinon, vous pouvez ignorer cette étape.

```
1 - add authentication ldapAction ldap-new -serverIP x.x.x.x -serverPort
     636 -ldapBase "cn=users,dc=aaatm,dc=com" -ldapBindDn
    adminuser@aaatm.com -ldapBindDnPassword <password> -encrypted -
    encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
     memberof -subAttributeName CN -secType SSL -passwdChange ENABLED -
    defaultAuthenticationGroup ldapGroup
2
3 - add authenticationpolicy ldap-new -rule true -action ldap-new
4 <!--NeedCopy-->
```

La configuration LDAP est le deuxième facteur d'ouverture de session utilisateur (facultatif) L'authentification LDAP se produit après Captcha, vous l'ajoutez au deuxième facteur.

```
1 - add authentication policylabel second-factor
2 - bind authentication policylabel second-factor -policy ldap-new -
    priority 10
3 - bind authentication vserver auth -policy myrecaptcha -priority 1 -
    nextFactor second-factor
4 <!--NeedCopy-->
```

L'administrateur doit ajouter des serveurs virtuels appropriés selon que le serveur virtuel d'équilibrage de charge ou l'appliance NetScaler Gateway est utilisé pour l'accès. L'administrateur doit configurer la commande suivante si un serveur virtuel d'équilibrage de charge est requis :

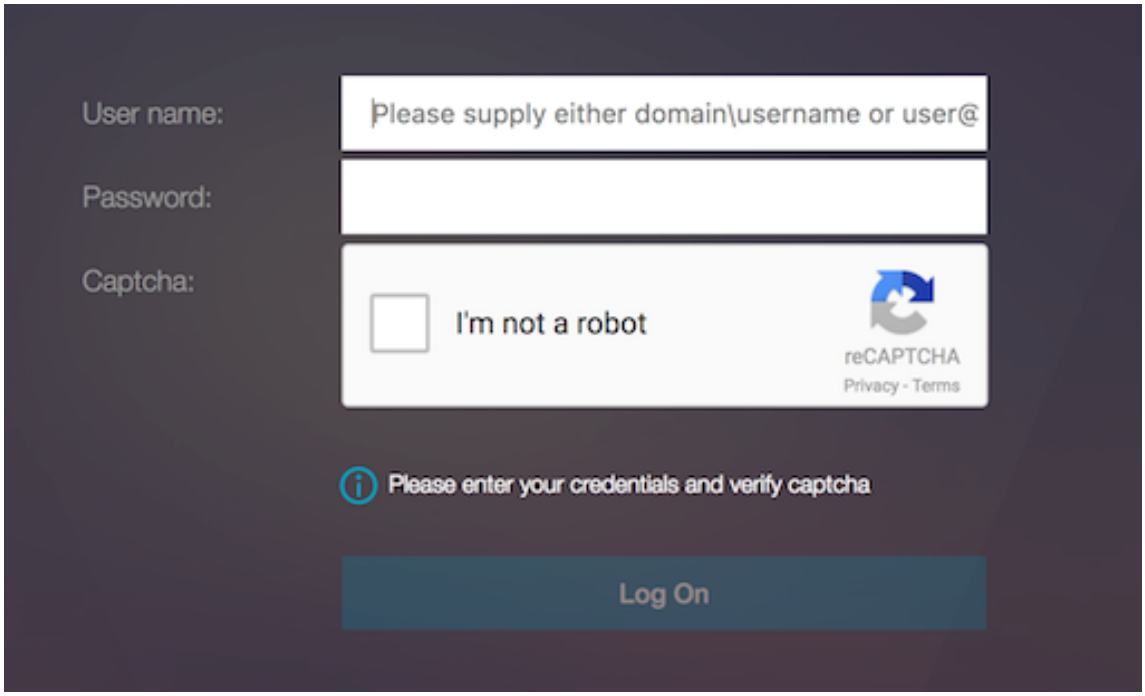
```
1 add lb vserver lbtest HTTP <IP> <Port> -authentication ON -
    authenticationHost nssp.aaatm.com`
2 <!--NeedCopy-->
```

nssp.aaatm.com —Résolution en serveur virtuel d'authentification.

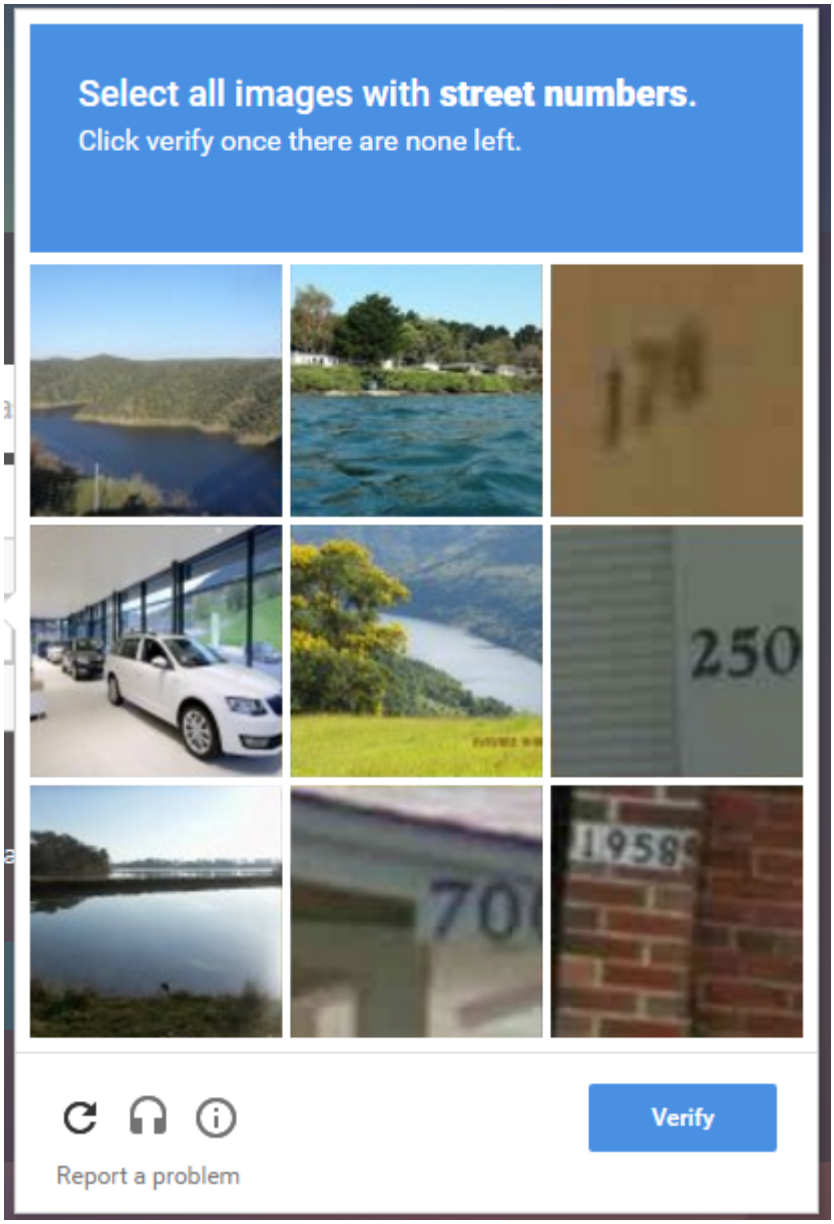
Validation du Captcha par l'utilisateur Une fois que vous avez configuré toutes les étapes mentionnées dans les sections précédentes, consultez les captures d'écran de l'interface utilisateur précé-

dentes.

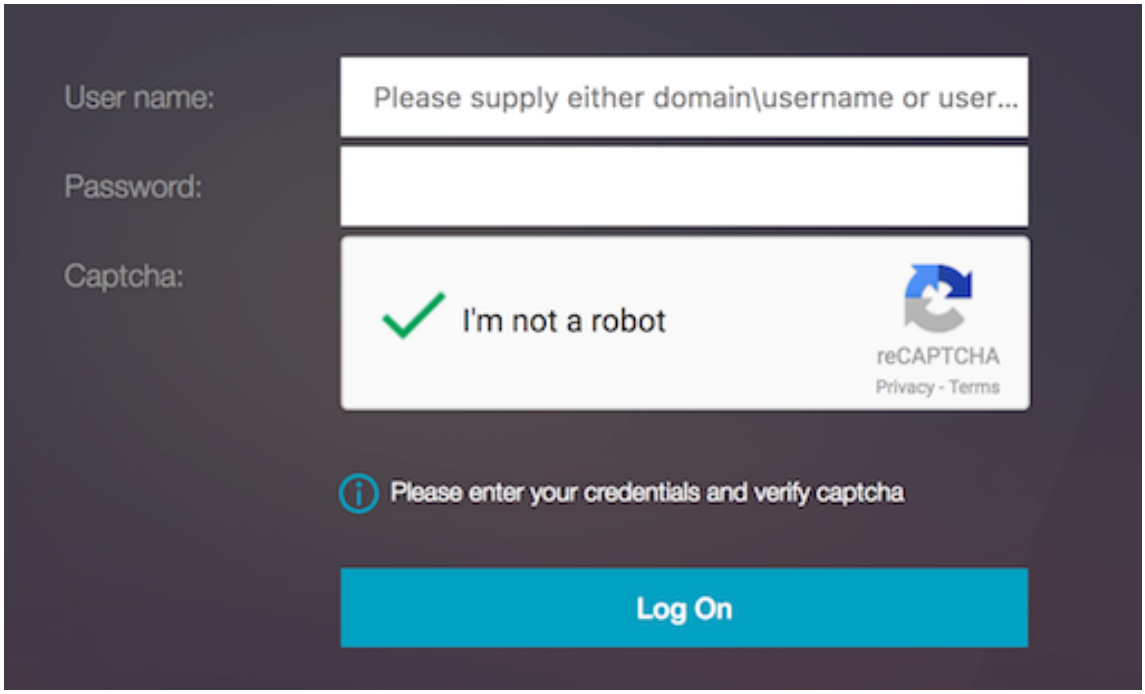
1. Une fois que le serveur virtuel d'authentification charge la page de connexion, l'écran de connexion s'affiche. La**connexion** est désactivée jusqu'à ce que Captcha soit terminé.



2. Sélectionnez l'option Je ne suis pas un robot. Le widget Captcha s'affiche.



3. Vous parcourez une série d'images Captcha avant que la page de fin ne s'affiche.
4. Entrez les informations d'identification AD, activez la case à cocher **Je ne suis pas un robot** et cliquez **sur Ouvrir une session**. Si l'authentification réussit, vous êtes redirigé vers la ressource souhaitée.

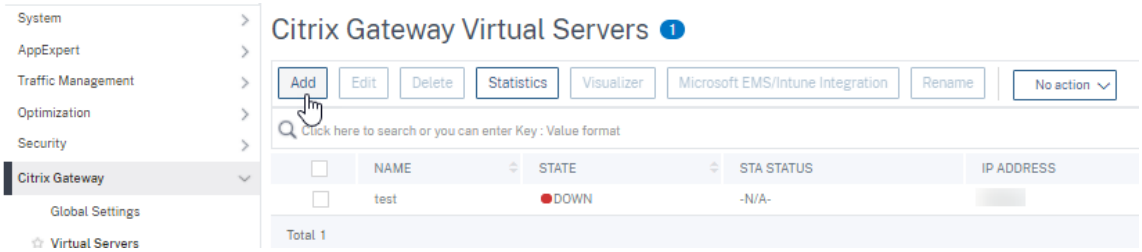


Remarque :

- Si Captcha est utilisé avec l'authentification AD, le bouton Soumettre pour les informations d'identification est désactivé jusqu'à ce que Captcha soit terminé.
- Le Captcha se produit dans un facteur qui lui est propre. Par conséquent, toute validation ultérieure telle que AD doit avoir lieu dans `nextfactor` le Captcha.

Créer un serveur virtuel Gateway pour l'authentification nFactor dans la licence NetScaler Standard

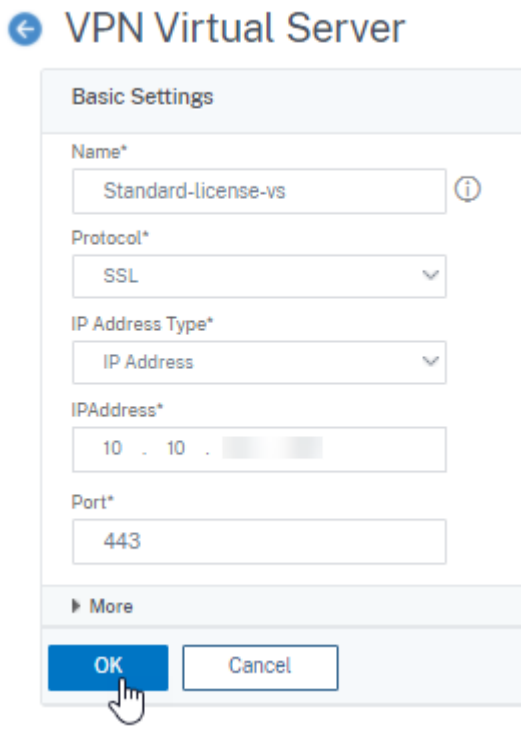
1. Accédez à **NetScaler Gateway>Serveurs**virtuels.
2. Sur la page **Serveurs virtuels NetScaler Gateway**, cliquez sur **Ajouter**.



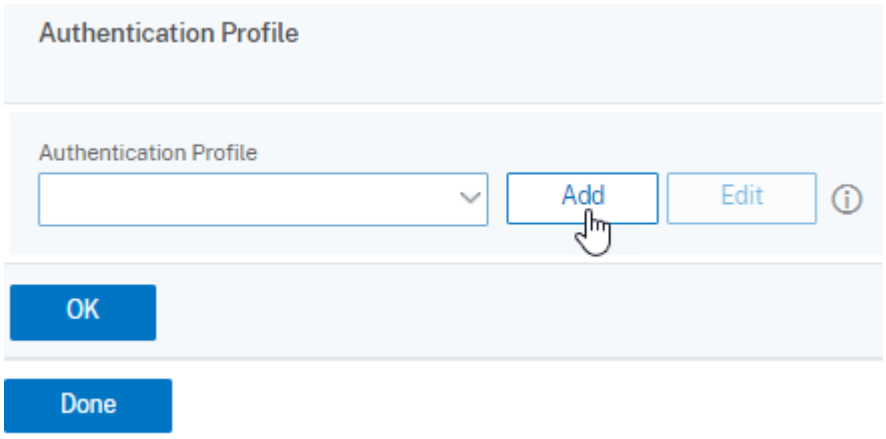
3. Entrez les informations suivantes sur la page **Serveur virtuel VPN**, cliquez sur **OK**, puis sur **Continuer**.

   - Nom : nom du serveur virtuel NetScaler Gateway
   - Protocole - Sélectionnez **SSL**

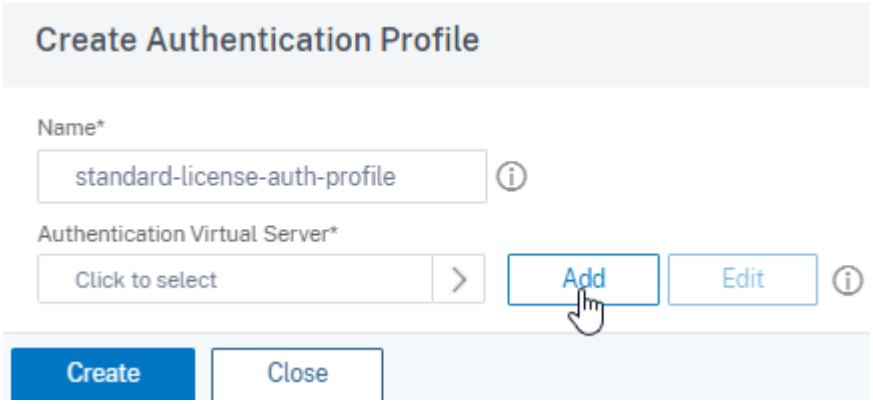
- Adresse IP : adresse IP du serveur virtuel NetScaler Gateway
- Port - Entrée 443



4. Sur la page **Serveur virtuel VPN**, cliquez sur l'icône Plus en regard de **Profil d'authentification**.
5. Cliquez sur **Ajouter** pour configurer le profil d'authentification.

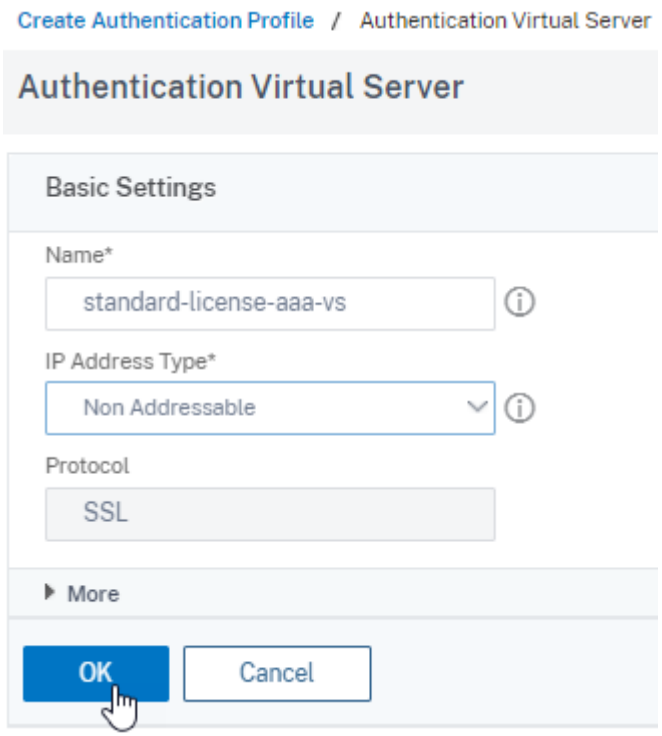


6. Saisissez un nom pour le profil d'authentification, puis cliquez sur **Ajouter**.



7. Entrez les informations suivantes sur la page **Serveur virtuel VPN**, cliquez sur **OK,** puis sur **Continuer**.

   - Nom : nom du serveur virtuel d'authentification, d'autorisation et d'audit
   - Protocole - Sélectionnez **Non adressable**. Seul un serveur virtuel d'authentification, d'autorisation et d'audit non adressable peut être lié à un serveur virtuel Gateway/VPN sous licence NetScaler Standard.



> **Remarque :**
>
> - Dans la licence NetScaler Standard, les étapes de création d'une stratégie sont les mêmes que dans la licence Premium pour les types de stratégies pris en charge.
> - La licence NetScaler Standard ne prend pas en charge l'ajout de nouveaux schémas

> de connexion dans la configuration de nFactor.

Références

Pour un exemple de configuration nFactor de bout en bout, consultez Configuration de l'authentification nFactor.

Visualiseur Unified Gateway

March 27, 2024

Le visualiseur Unified Gateway fournit une représentation visuelle des configurations à l'aide de l'assistant Unified Gateway. Le visualiseur Unified Gateway permet d'ajouter et de modifier la configuration, et de diagnostiquer un problème principal.

Le visualiseur Unified Gateway présente les éléments suivants :

Configuration	Configuration
Stratégies de pré-authentification	Authentication policies
Serveurs virtuels CS	Serveurs virtuels VPN
Serveurs virtuels LB	Applications XA/XD
Applications Web	Applications SaaS

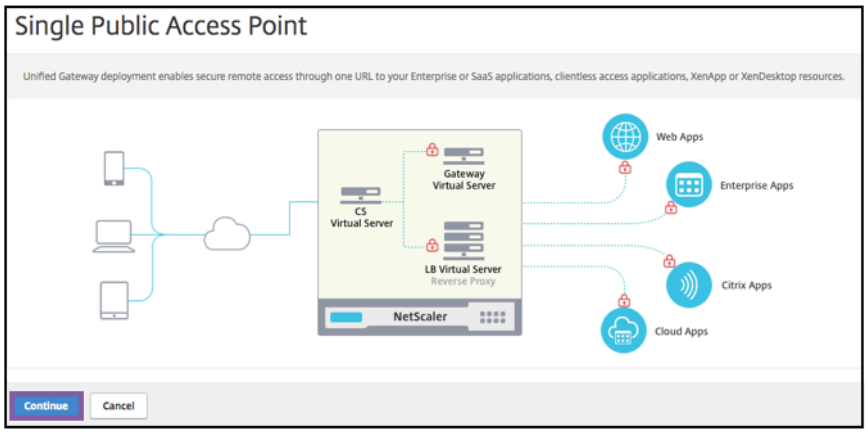
Le déploiement d'Unified Gateway permet un accès distant sécurisé via une URL vers vos applications Enterprise ou SaaS, vos applications d'accès sans client, vos ressources Citrix Virtual Apps et Desktops.

Configurer Unified Gateway

1. Sélectionnez Unified Gateway dans le menu.
2. Dans l'écran suivant, vérifiez que vous disposez des informations suivantes, puis cliquez sur **Commencer** :
   - Adresse IP publique pour Unified Gateway.
   - Chaîne de certificats de serveur (.PFX ou .PEM) avec certificat Root-CA en option.
   - Détails de l'authentification basée sur le certificat LDAP/RADIUS/client.

- Détails de l'application (URL des applications SaaS ou détails du serveur Citrix Virtual Apps and Desktops).

3. Cliquez sur le bouton **Continuer**.

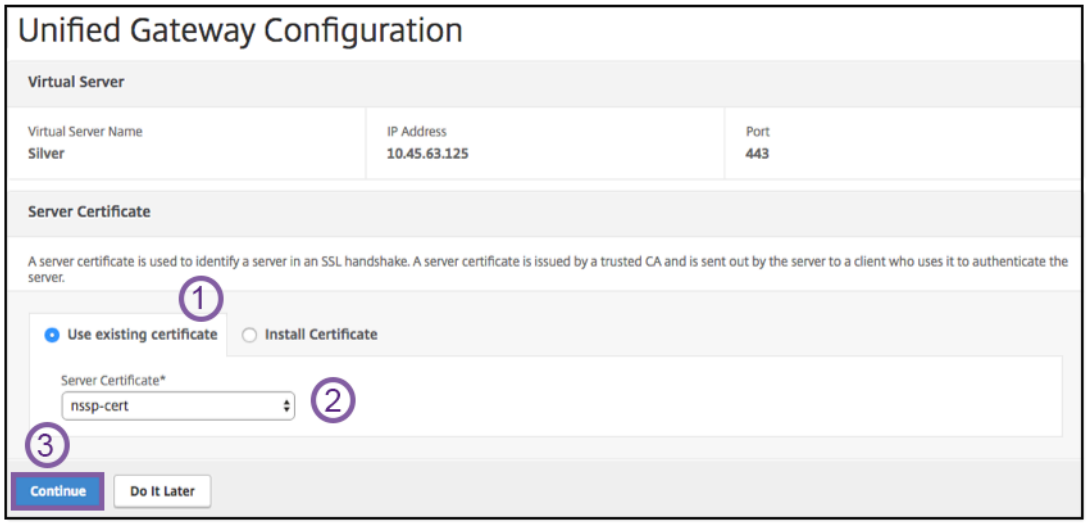


Créez un serveur virtuel de configuration Unified Gateway.

1. Entrez le **nom de** configuration du serveur virtuel.
2. Entrez l'**adresse IP Unified Gateway accessible** au public pour le déploiement d'Unified Gateway.
3. Entrez le numéro de **port**. La plage de numéros de port est comprise entre 1 et 65535.
4. Cliquez sur **Continuer**.

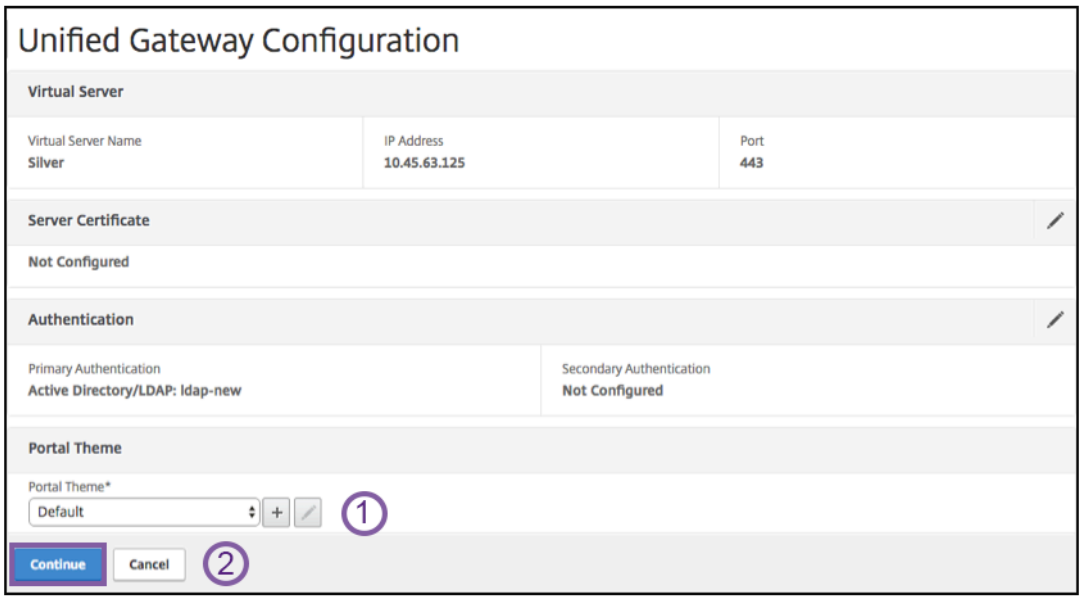
Renseignez les informations suivantes pour spécifier le certificat de serveur.

1. Sélectionnez les boutons radio **Utiliser un certificat existant** ou **Installer le certificat**.
2. Sélectionnez un **certificat de serveur** dans le menu.
3. Cliquez sur le bouton **Continuer**.



Renseignez les informations suivantes pour spécifier l'authentification.

1. Sélectionnez une **méthode d'authentification principale** dans le menu.
2. Sélectionnez les boutons radio **Utiliser un serveur existant** ou **Ajouter un nouveau serveur**.
3. Cliquez sur le bouton **Continuer**.
4. Sélectionnez le **thème du portail** dans le menu.
5. Cliquez sur **Continuer**.
6. Sélectionnez les boutons radio **Application Web** ou **Citrix Virtual Apps Desktops**.
7. Cliquez sur **Continuer**.



Sélectionnez une application

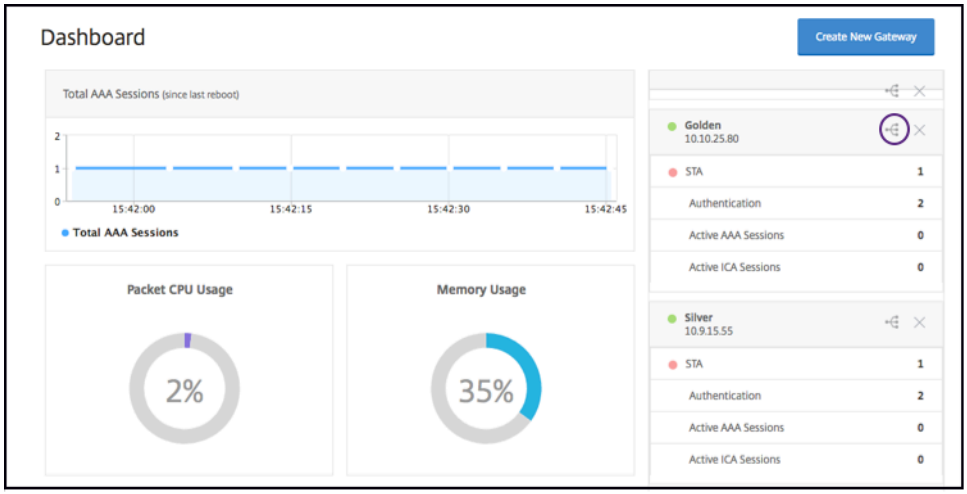
Renseignez les informations suivantes pour spécifier l'application Web.

1. Saisissez le nom du lien de signet.
2. Sélectionnez le type d'application que représente l'URL VPN. Les valeurs possibles sont les suivantes :
   - Application Intranet
   - Accès sans client
   - SaaS
   - Application préconfigurée sur ce NetScaler
3. Cochez cette case pour rendre cette application accessible via l'URL Unified Gateway.
4. Saisissez l'URL du lien de signet.
5. Dans l'URL de l'icône, choisissez un fichier pour récupérer un fichier d'icônes. Le MaxLength = 255
6. Cliquez sur le bouton **Continuer**.

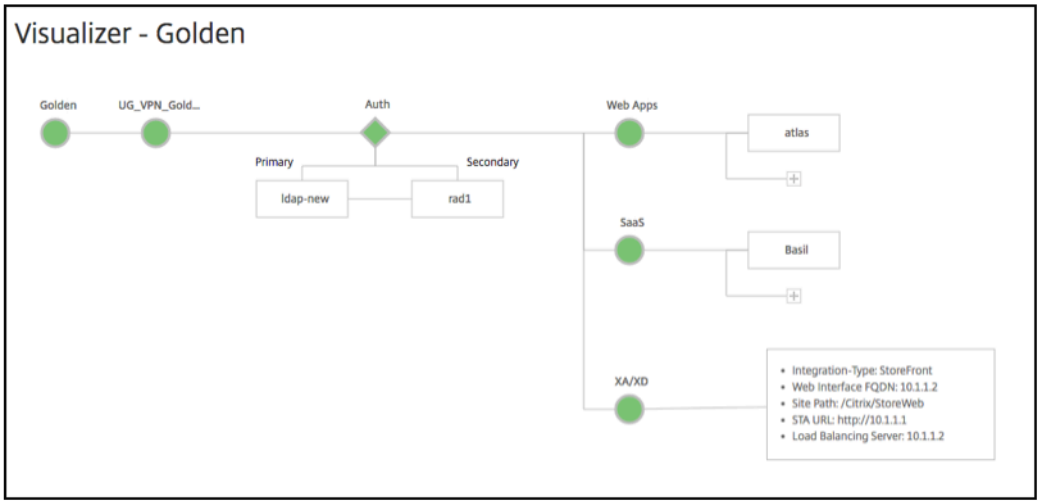
7. Cliquez sur **Terminé**.
8. Cliquez sur **Continuer**.
9. Cliquez sur **Terminé**.

Configuration de l'interface graphique

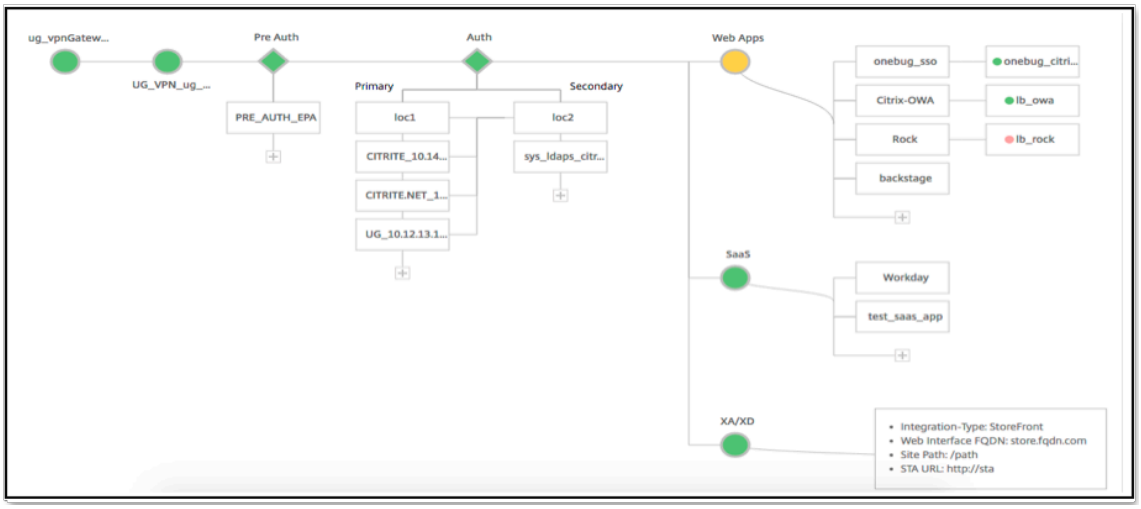
1. Sélectionnez Unified Gateway dans le menu.
2. Cliquez sur l'icône **Unified Gateway Visualizer** pour accéder aux instances de passerelle configurées.



Le visualiseur Unified Gateway ressemble à un diagramme de flux, comme le montre l'image suivante :



Le visualiseur Unified Gateway dispose de PreAuth et d'une section Apps. `Auth` Si le serveur virtuel VPN dispose d'une stratégie de pré-authentification, alors seulement le `pre-auth` est affiché dans le visualiseur Unified Gateway.



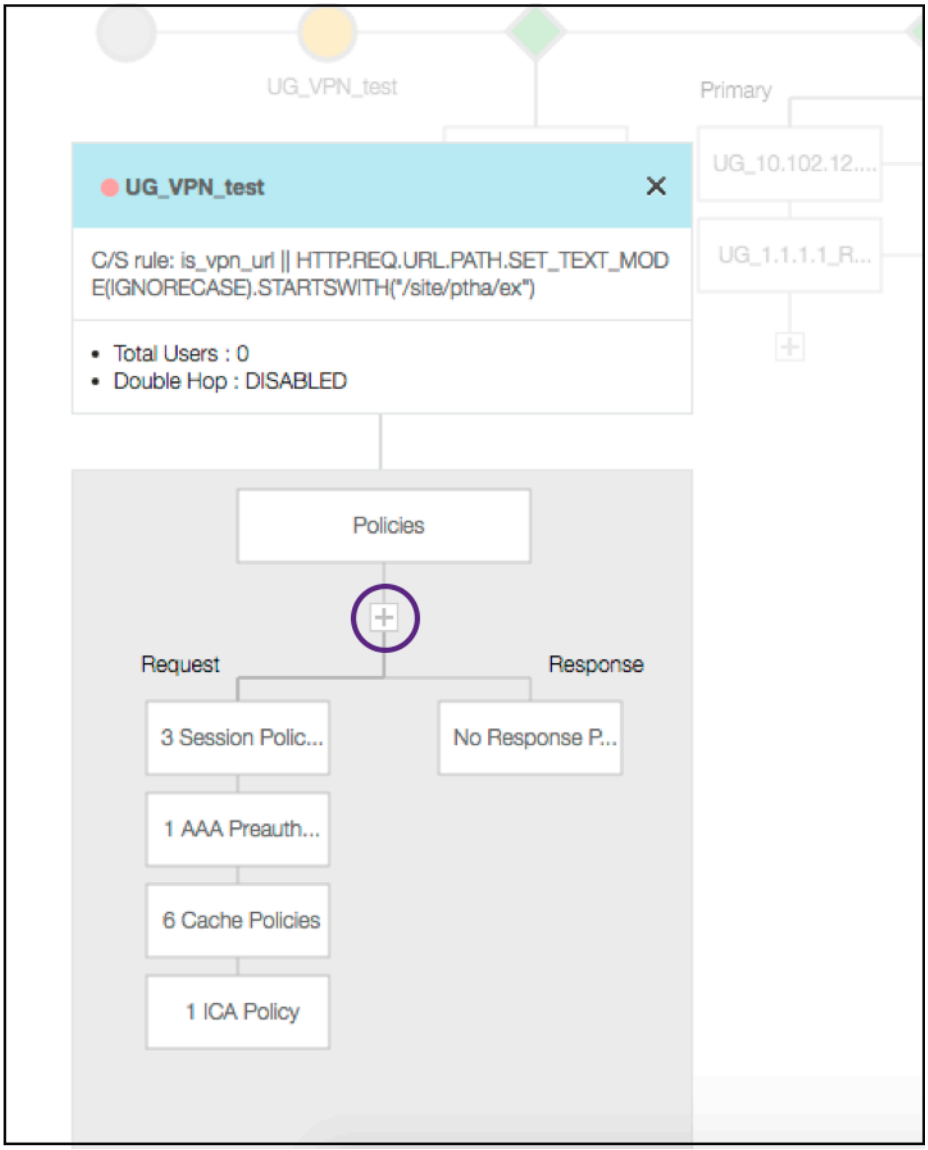
Le visualiseur Unified Gateway utilise un schéma de codage couleur pour l'équilibrage de charge et les serveurs virtuels VPN pour indiquer leur état.

Couleur	Description
Rouge	signifie que le serveur est en panne.
gris	signifie que WebApps/Citrix Virtual Apps n'ont pas été configurés.
Vert	signifie que tout va bien avec le serveur virtuel.
Orange	signifie que l'un des services de serveur virtuel d'équilibrage de charge est en panne, mais il fonctionne toujours correctement.

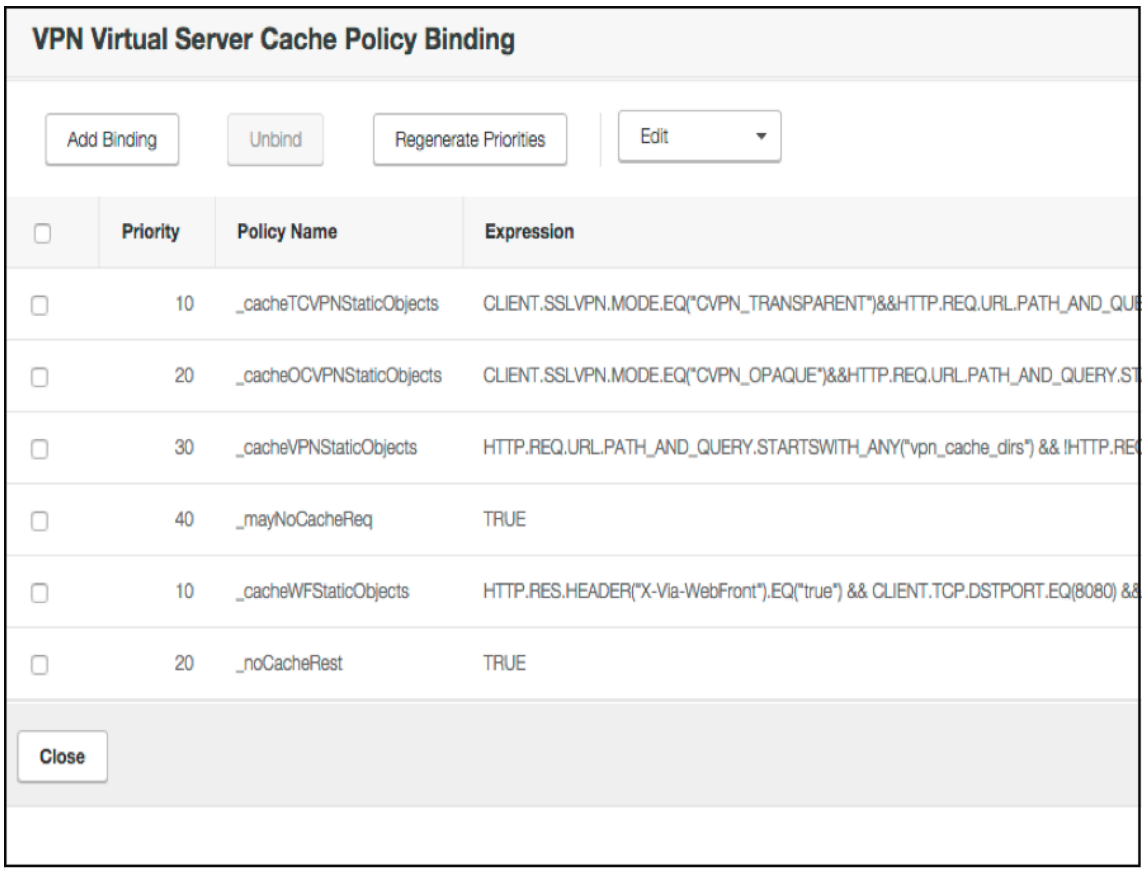
Détails des serveurs virtuels VPN

Pour obtenir les détails des serveurs virtuels VPN, cliquez sur le **nœud Serveurs virtuels VPN**. La fenêtre contextuelle affiche des détails tels que la règle C/S et toutes les stratégies.

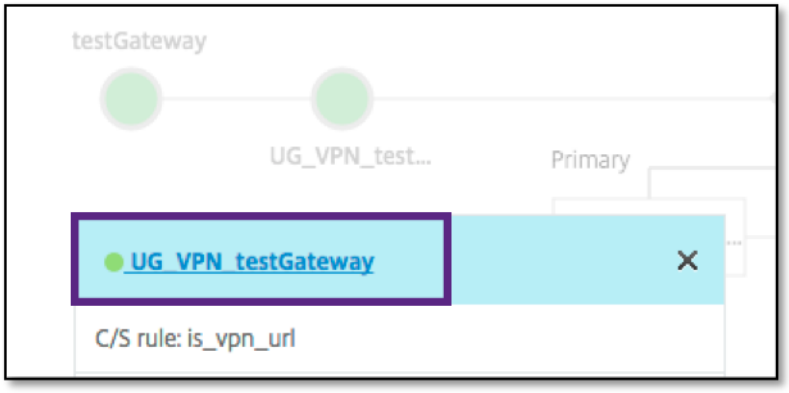
1. Ajoutez des stratégies à l'entité VPN en cliquant sur l'icône (+).



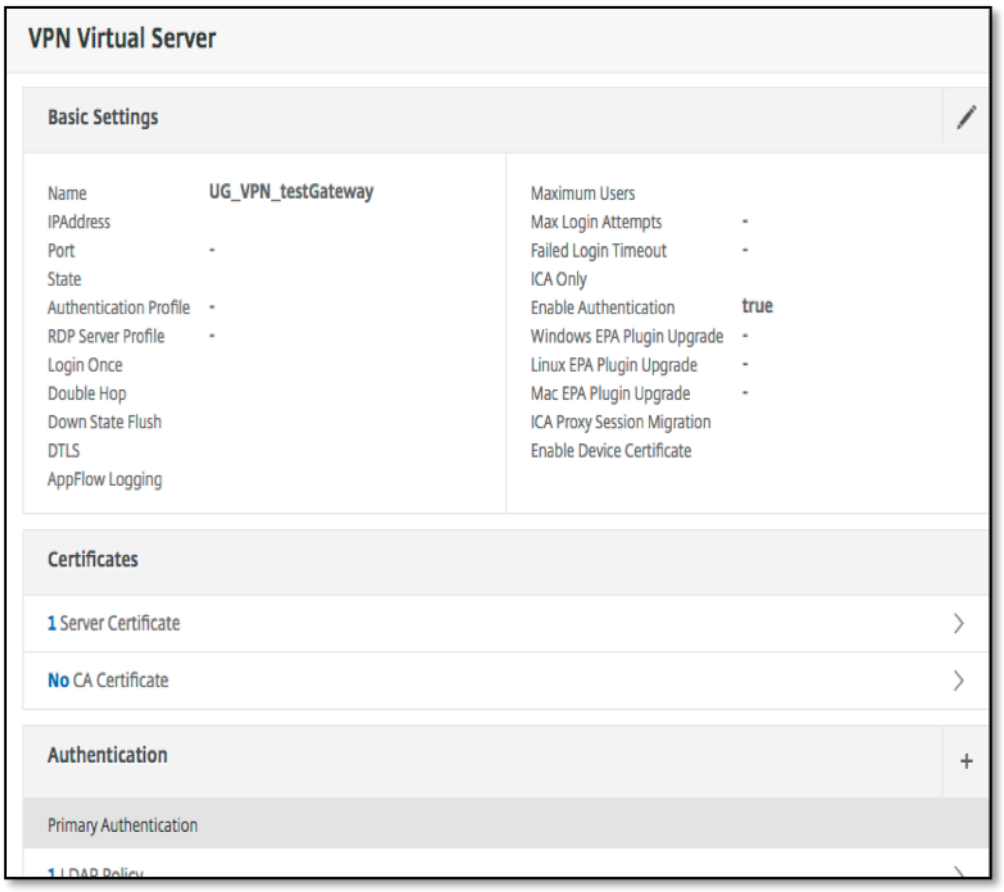
2. Cliquez sur le nœud souhaité pour obtenir des détails sur les stratégies déjà configurées.



Pour les informations sur le serveur virtuel VPN, le titre VPN dans la fenêtre contextuelle est une entité cliquable qui se dirige vers un curseur qui détaille le serveur virtuel VPN.



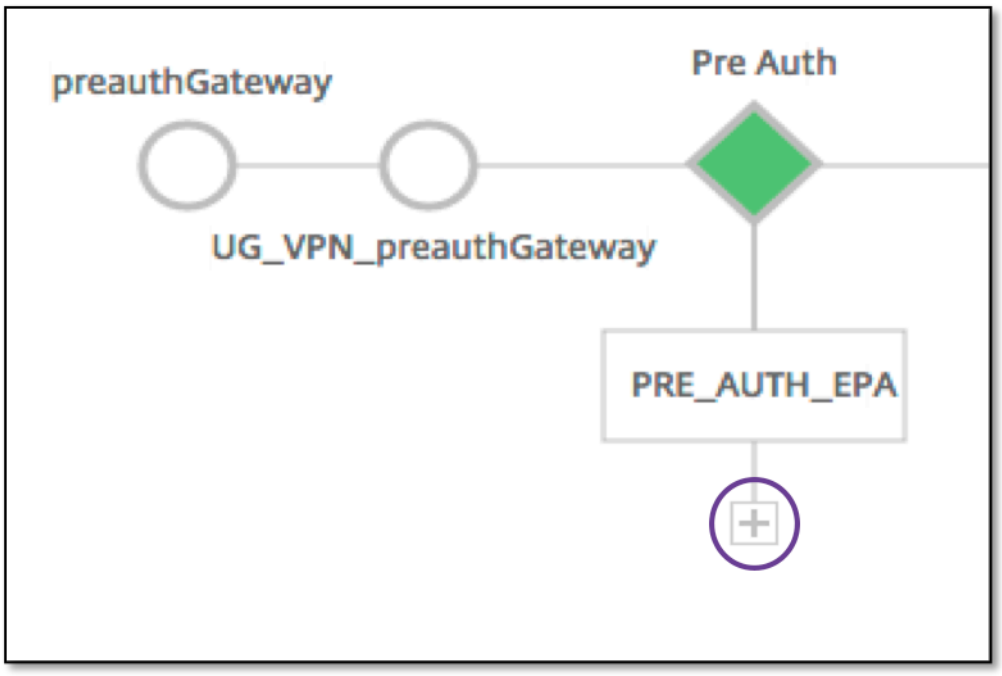
Les détails du serveur VPN sont affichés ici.



The Pre Auth Block

Si un serveur virtuel VPN est associé à des stratégies de pré-authentification, le visualiseur Unified Gateway affiche un `Pre Auth` blocage. Le `Pre Auth` bloc affiche les stratégies et offre une option permettant d'ajouter des stratégies de pré-authentification au VPN.

1. Cliquez sur le **signe +** pour ajouter une `preauth` stratégie.

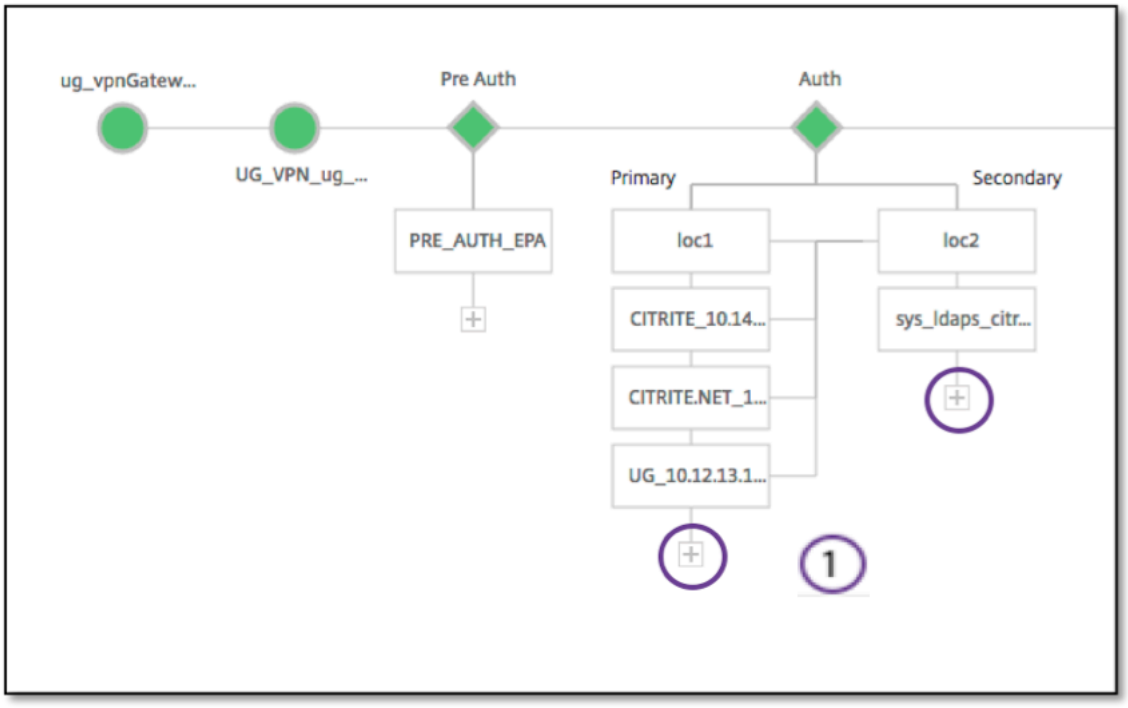


Dans le cas où aucune stratégie de pré-authentification n'est associée, ce bloc est masqué dans la vue.

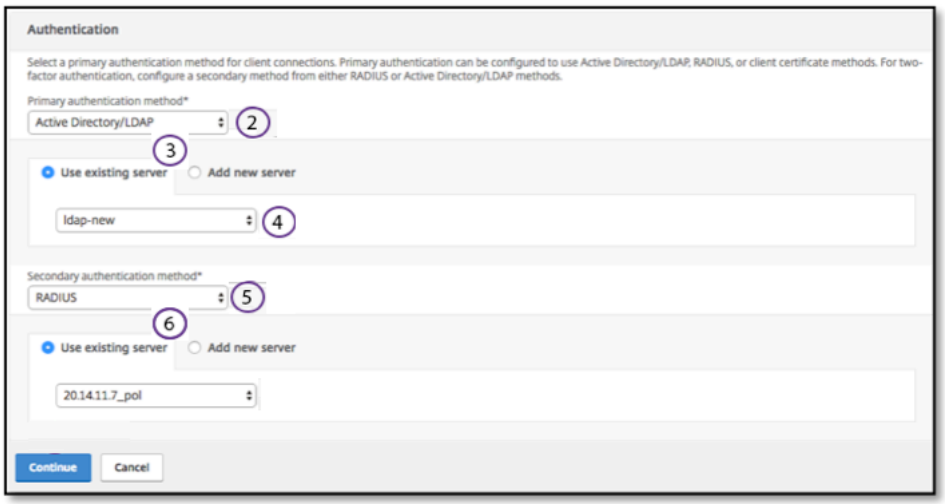
The Auth Block

Le `Auth` bloc répertorie les stratégies principale et secondaire. Le `Auth` bloc offre une option permettant d'ajouter des stratégies.

1. Cliquez sur **+** dans la liste principale pour ajouter une liaison d'authentification principale ou cliquez sur + dans la liste secondaire pour ajouter une liaison d'authentification secondaire.

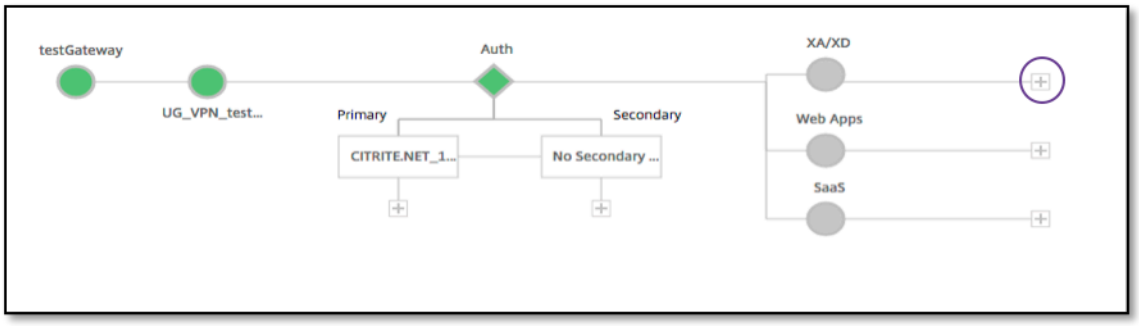


2. Sélectionnez une option dans le menu **Méthode d'authentification principale**.
3. Indiquez s'il s'agit d'un **serveur existant** ou **Ajouter un nouveau serveur** en sélectionnant le bouton radio.
4. Sélectionnez une option dans le menu **Nom de la stratégie LDAP**.
5. Sélectionnez **RADIUS** dans le menu **Méthode d'authentification secondaire**.
6. Spécifiez si vous souhaitez**utiliser un serveur existant** ou **Ajouter un nouveau serveur** en sélectionnant le bouton radio.
7. Cliquez sur **Continuer**.



Ajout de StoreFront

1. Cliquez sur **+** près du XA/XD pour ajouter des applications « XA/XD ».



Vous pouvez choisir votre point d'intégration. Les options sont StoreFront, WI ou WiOnNS. Cliquez sur **Continuer**.

1. Renseignez les champs suivants pour configurer StoreFront. Les champs qui nécessitent des informations obligatoires sont signalés par le astérisque *.

Champ	**Description**
—	—
FQDN StoreFront *	Entrez le nom de domaine complet du serveur StoreFront. Longueur maximale : 255 caractères. Exemple : //storefront.xendt.net
Chemin d'accès au site*	Entrez le chemin d'accès à Receiver pour le site Web déjà configuré sur StoreFront.
`Single Sign-on Domain`*	Entrez le domaine par défaut pour l'authentification des utilisateurs
Nom du magasin*	Entrez le nom des moniteurs StoreFront.
STORENAME est un argument définissant le nom du magasin de services StoreFront pour vérifier l'intégrité des serveurs StoreFront. Applicable aux moniteurs StoreFront. Longueur maximale : 31
Serveur Secure Ticket Authority *	Entrez l'URL Secure Ticket Authority, généralement présente sur le Delivery Controller.
Exemple :`http://sta`
StoreFront Server*	Entrez l'adresse IP du serveur StoreFront Server
Protocol	*Entrez le protocole utilisé par le serveur.*
Port	Entrez le port utilisé par le serveur.
Équilibrage de charge	Entrez la configuration d'équilibrage de charge pour les serveurs StoreFront.
Serveur virtuel*	Entrez l'adresse IP publique pour le déploiement d'Unified Gateway.

2. Cliquez sur **Continuer.**

Ajout de SaaS

1. Cliquez sur **+** pour ajouter des applications SaaS. Vous accédez à la page Ajouter SaaS. Renseignez les champs suivants pour configurer le SaaS. Les champs qui nécessitent des informations obligatoires sont signalés par un*.

Champ	Description
Nom*	Saisissez le nom du lien de signet.
Type d'application	Entrez le type d'application que représente cette URL VPN. Les valeurs possibles sont les suivantes : Application intranet/Accès sans client/SaaS/Application préconfigurée sur ce NetScaler
Entrez l'URL*	Entrez l'URL de l'application Intranet.
Choisir un **fichier**	Entrez l'URL pour récupérer le fichier d'icônes permettant d'afficher cette ressource. Longueur maximale = 255

Ajout de WebApps

1. Cliquez sur **+** pour ajouter des applications Web. Vous accédez à la page Ajouter des applications Web. Renseignez les champs suivants pour configurer une application Web. Les champs qui nécessitent des informations obligatoires sont signalés par un*.

Champ	Description
Nom*	Saisissez le nom du lien de signet.
Type d'application	Entrez le type d'application que représente cette URL VPN. Les valeurs possibles sont les suivantes : Application intranet/Accès sans client/SaaS/Application préconfigurée sur ce NetScaler
Entrez l'URL*	Entrez l'URL de l'application Intranet.
Choisir un **fichier**	Entrez l'URL pour récupérer le fichier d'icônes pour afficher cette ressource.MaxLength = 255

Si une application est accessible via l'URL Unified Gateway, les détails du serveur d'équilibrage de charge sont accessibles en cliquant sur l'application :

De nouvelles stratégies peuvent être ajoutées en cliquant sur (+) et toutes les stratégies liées peuvent être affichées en cliquant sur le nœud qui affiche les informations de stratégie.

Le nombre de services liés à l'équilibreur de charge est également affiché, ainsi que les informations d'état globales. Cliquez ensuite sur la liste de tous les services. De nouveaux services peuvent être ajoutés à l'équilibreur de charge.

Pour plus d'informations sur l'équilibreur de charge, il est possible de cliquer sur le titre de la fenêtre contextuelle et d'accéder à la page des détails du serveur virtuel d'équilibrage de charge.

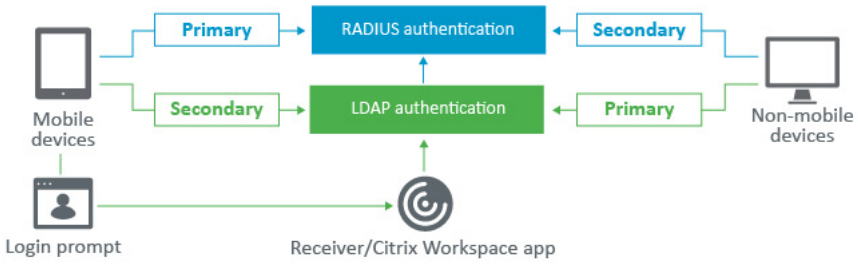
Configurer NetScaler Gateway pour utiliser l'authentification RADIUS et LDAP avec des appareils mobiles/tablettes

March 27, 2024

Cette section explique comment configurer l'appliance NetScaler Gateway pour utiliser l'authentification RADIUS comme principale et l'authentification LDAP comme secondaire avec les appareils mobiles/tablettes.

La configuration présentée dans la section permet toujours à toutes les autres connexions d'utiliser LDAP en premier et RADIUS en second lieu.

Lorsque vous configurez l'authentification à deux facteurs sur l'application Citrix Workspace pour une utilisation avec des appareils mobiles/tablettes, vous devez ajouter l'authentification RSA SecureID (authentification RADIUS) en tant qu'authentification principale. Mais lorsque les utilisateurs reçoivent l'invite pour le nom d'utilisateur et le mot de passe, le code secret sur Receiver, ils placent LDAP en premier et RADIUS comme deuxième informations d'identification. Du point de vue de l'administrateur, il s'agit d'une configuration différente de celle d'une configuration non mobile.



Suivez la procédure suivante pour configurer l'appliance NetScaler Gateway afin qu'elle utilise l'authentification RADIUS comme principale et l'authentification LDAP comme secondaire avec les appareils mobiles/tablettes.

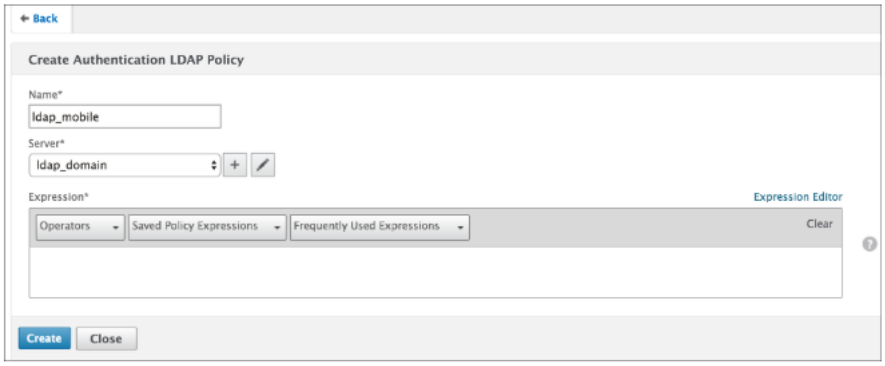
1. Dans l'utilitaire de configuration, sélectionnez **NetScaler Gateway > Stratégies > Authentification et créez une stratégie d'authentification** pour LDAP et RSA pour les appareils mobiles et non mobiles. Cela est nécessaire pour éviter une condition logique qui peut permettre aux utilisateurs de contourner l'authentification RADIUS.
2. Entrez les détails du serveur LDAP après avoir cliqué sur l'option **Ajouter** sous l'onglet **Serveurs** pour LDAP.
3. Créez une stratégie LDAP pour les appareils mobiles en choisissant le serveur LDAP requis.

   Pour lier cette stratégie uniquement aux appareils mobiles, utilisez l'expression suivante :

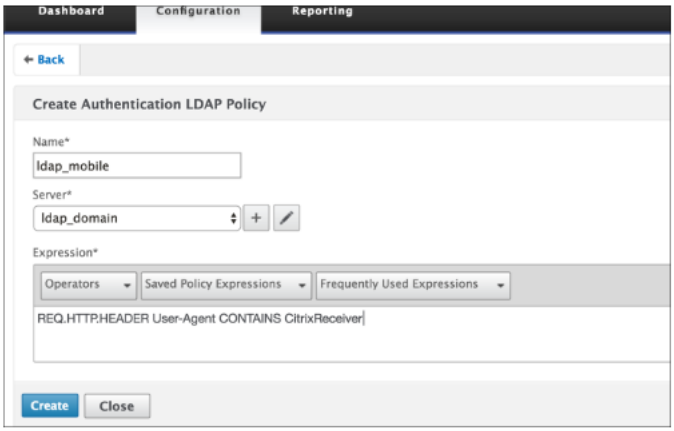
   ```
   1 REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```


L'expression avancée correspondante est la suivante :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")
```



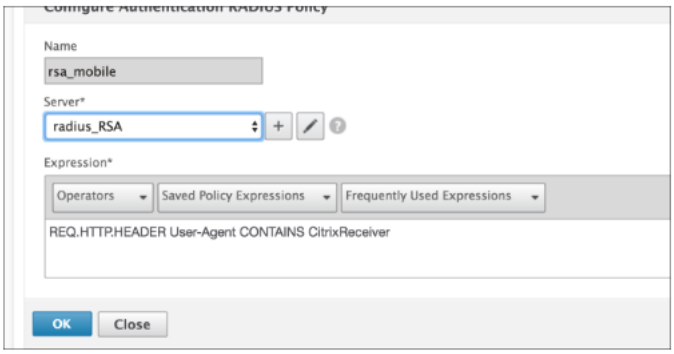
4. Cliquez sur **Expression Editor** pour créer une politique :



5. Créez une stratégie RADIUS et un serveur RADIUS pour les appareils mobiles.

- Accédez à l'option RADIUS depuis **NetScaler Gateway > Policies > Authentication**RADIUS. Cliquez sur **Ajouter** sous l'onglet Serveur.
- Ajoutez les informations requises. Le port par défaut de l'authentification RADIUS est 1812.

- Pour lier cette stratégie uniquement aux appareils mobiles, utilisez l'expression suivante :

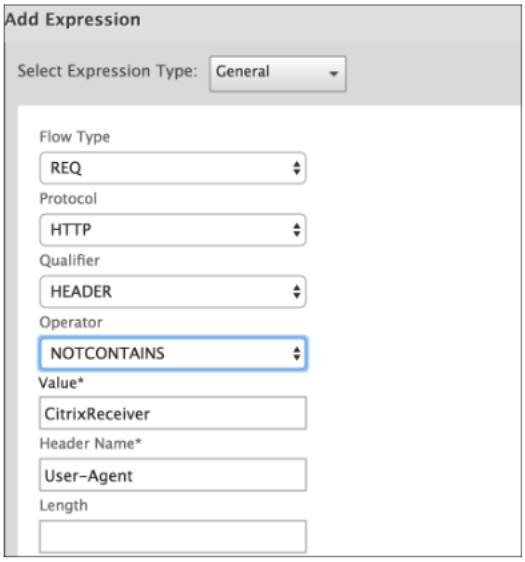


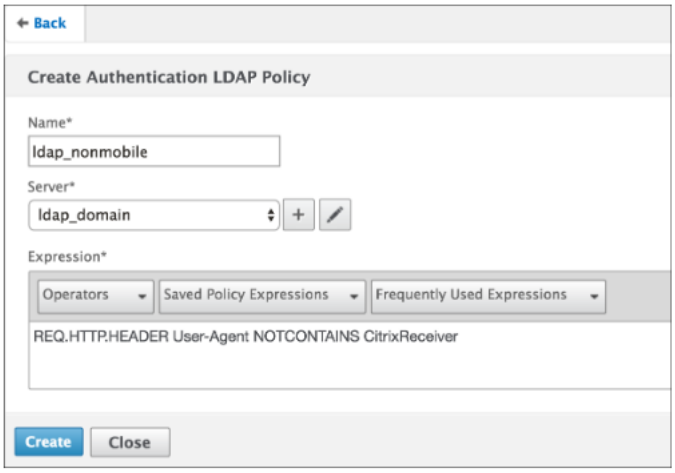
6. Suivez la même étape pour créer une stratégie LDAP pour les appareils non mobiles. Pour lier cette stratégie uniquement aux appareils non mobiles, utilisez l'expression suivante :

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

L'expression avancée correspondante est la suivante :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

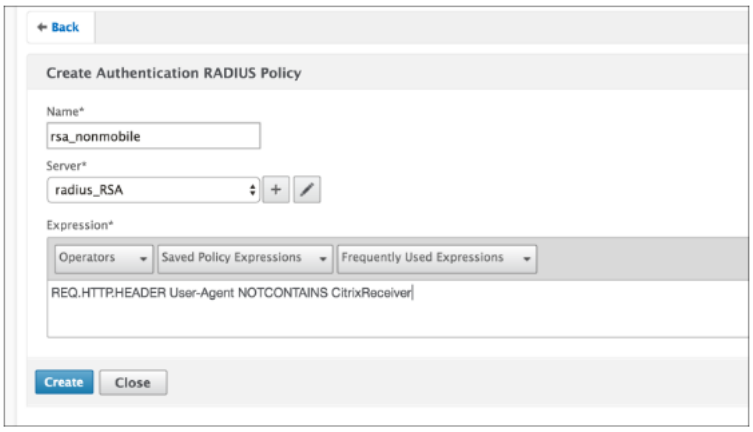


7. Créez une stratégie RADIUS pour les appareils non mobiles. Pour lier cette stratégie uniquement aux appareils non mobiles, utilisez l'expression suivante :

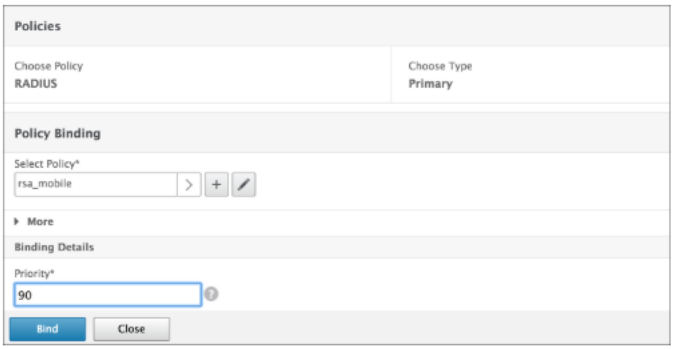
```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

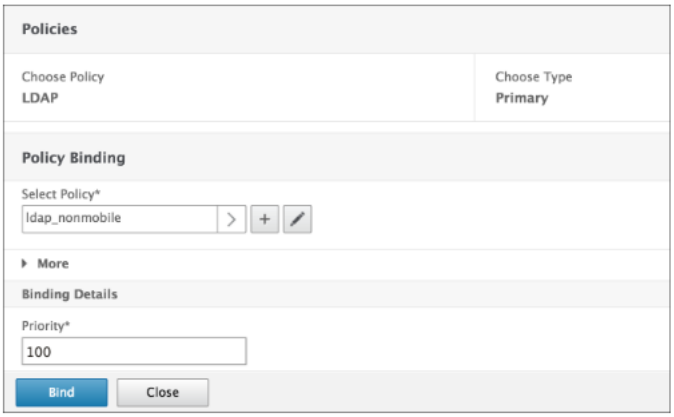
L'expression avancée correspondante est la suivante :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```

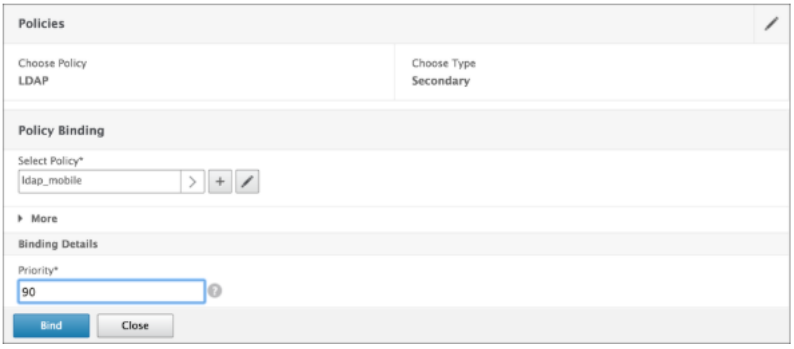



8. Accédez aux propriétés du serveur virtuel NetScaler Gateway et cliquez sur l'onglet **Authentification**. Dans les stratégies d'authentification principales, ajoutez la stratégie RSA_Mobile en priorité supérieure et la stratégie LDAP_NonMobile en tant que priorité secondaire :





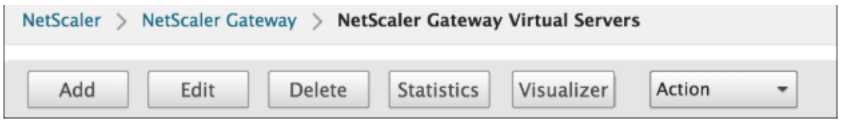
9. Dans les stratégies d'authentification secondaires, ajoutez la stratégie LDAP_Mobile en priorité supérieure, puis la stratégie RSA_NonMobile en tant que priorité secondaire :

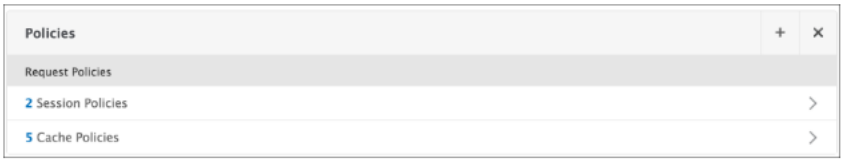


> La stratégie de session doit avoir l'index d'informations d'identification d'authentification unique correct, c'est-à-dire qu'il doit s'agir des informations d'identification LDAP. Pour les appareils mobiles, l'**index des informations d'identification** sous **Profil de session > Expérience client** doit être défini sur **Secondaire**, qui est LDAP.

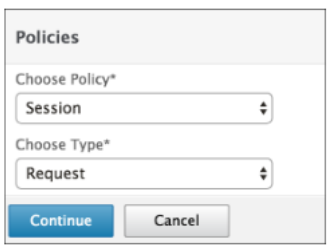
Par conséquent, vous avez besoin de deux stratégies de session, l'une pour les appareils mobiles et l'autre pour les appareils non mobiles.

- Pour les appareils mobiles, la stratégie de session et le profil de session s'affichent comme indiqué dans la capture d'écran suivante.
  Pour créer une stratégie de session, accédez au serveur virtuel requis et cliquez sur **Modifier**, accédez à la section Stratégie, puis cliquez sur le signe + :





- Sélectionnez l'option **Session** dans le menu.



- Entrez le nom de stratégie de session souhaité et cliquez sur + pour créer un profil. Pour les appareils mobiles, l'**index des informations d'identification** sous **Profil de session > Expérience client** doit être défini sur **Secondaire**, qui est LDAP.

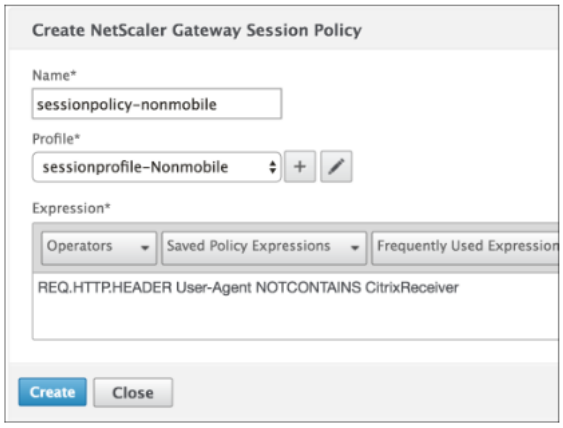
- Pour les appareils non mobiles, suivez les mêmes étapes. **L'index des informations d'identification** sous **Profil de session > Expérience client** doit être défini sur **Primary**, qui est LDAP.

L'expression doit être remplacée par :

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver
```

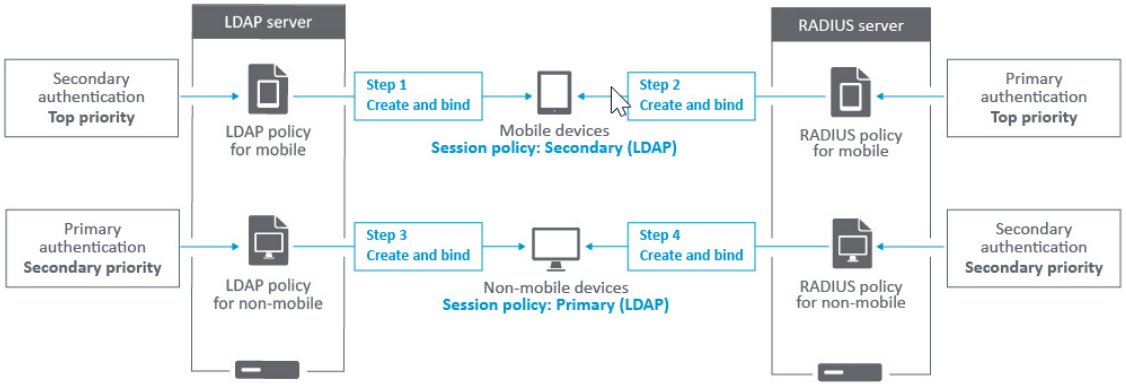
L'expression avancée correspondante est la suivante :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
```



- Pour créer un profil pour un utilisateur non mobile, cliquez sur le signe +.

10. La figure suivante affiche les stratégies et les profils sous le serveur virtuel requis.
11. Toujours sur StoreFront, dans la configuration de NetScaler Gateway, définie pour utiliser « Logon Type » = « Domaine et jeton de sécurité »



Restreindre l'accès à NetScaler Gateway pour les membres d'un groupe Active Directory

March 27, 2024

NetScaler Gateway prend en charge deux méthodes de restriction de l'accès à la connexion.

- Filtre de recherche LDAP : seuls les noms d'utilisateur correspondant au filtre de recherche LDAP (par exemple, appartenance à un groupe Active Directory) peuvent se connecter à NetScaler Gateway.
- Groupes autorisés à se connecter dans le cadre d'une stratégie ou d'un profil de session NetScaler Gateway : cette méthode prend en charge plusieurs groupes Active Directory. Pour plus d'informations, consultez la section https://support.citrix.com/article/CTX125797.

Cet article décrit la méthode de filtrage de recherche LDAP.

Vue d'ensemble

Lorsqu'un utilisateur saisit les informations d'identification sur la page de connexion du serveur virtuel NetScaler Gateway et appuie sur ENTER, l'appliance recherche d'abord le nom d'utilisateur dans Active Directory (LDAP). Si aucun filtre de recherche LDAP n'est défini dans la stratégie LDAP ou dans le serveur, l'appliance recherche une correspondance dans tous les noms d'utilisateurs Active Directory. Une fois qu'une correspondance est trouvée, l'appliance extrait le nom distinctif (DN) complet de l'utilisateur et utilise le nom unique et le mot de passe de l'utilisateur pour s'authentifier auprès d'Active Directory.

Si un filtre de recherche LDAP est défini, seuls les noms d'utilisateurs qui correspondent au filtre de recherche LDAP sont recherchés pour trouver une correspondance de nom d'utilisateur. Par exemple, si le filtre de recherche LDAP est conçu pour rechercher uniquement les membres d'un groupe Active Directory, le nom d'utilisateur saisi par l'utilisateur doit correspondre aux membres du groupe.

Pré-requis

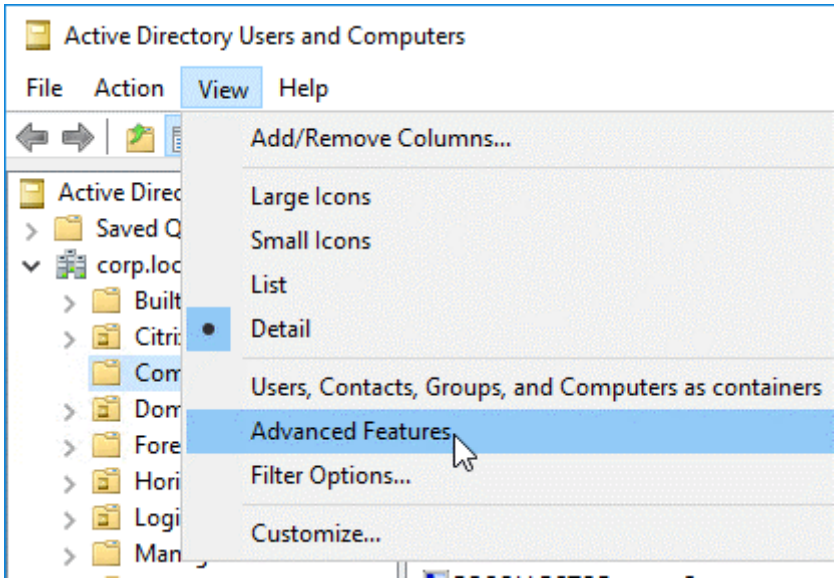
Le serveur virtuel NetScaler Gateway doit être configuré pour l'authentification LDAP.

Étapes à suivre pour configurer un filtre de recherche LDAP pour les membres d'un groupe Active Directory

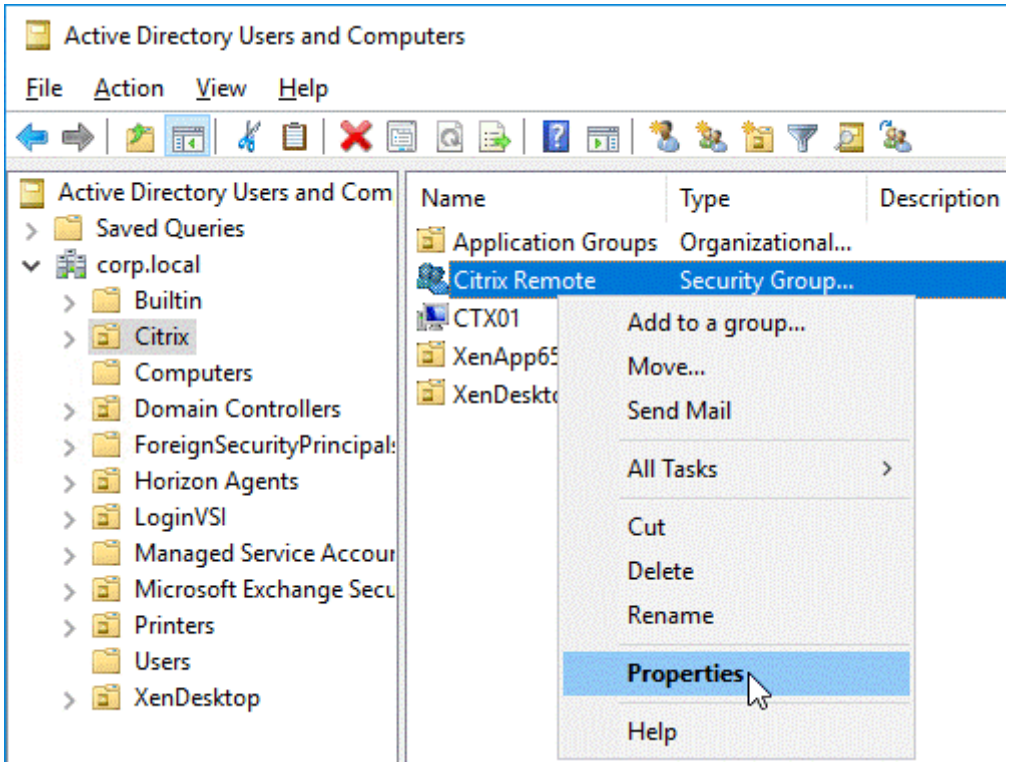
1. Déterminez le groupe Active Directory qui dispose d'une autorisation d'accès et obtenez son nom distinctif complet.

Un moyen simple d'obtenir le nom distinctif complet du groupe consiste à utiliser Utilisateurs et ordinateurs Active Directory.

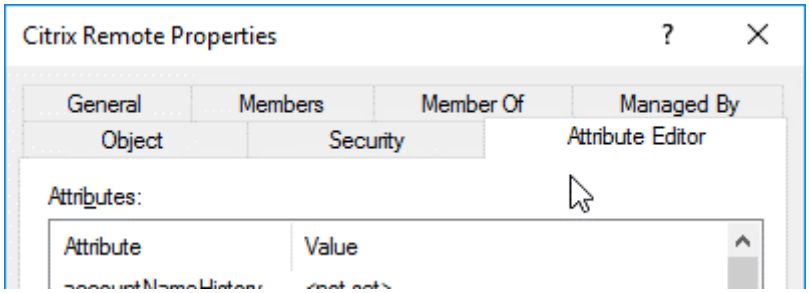
2. Dans Utilisateurs et ordinateurs Active Directory, dans le menu **Affichage**, activez les **fonctionnalités avancées**.



3. Parcourez l'arborescence jusqu'à l'objet de groupe, cliquez avec le bouton droit de la souris, puis cliquez sur **Propriétés**.
Remarque : Vous ne pouvez pas utiliser la **fonction Rechercher**. Au lieu de cela, vous devez parcourir l'arborescence pour trouver l'objet.

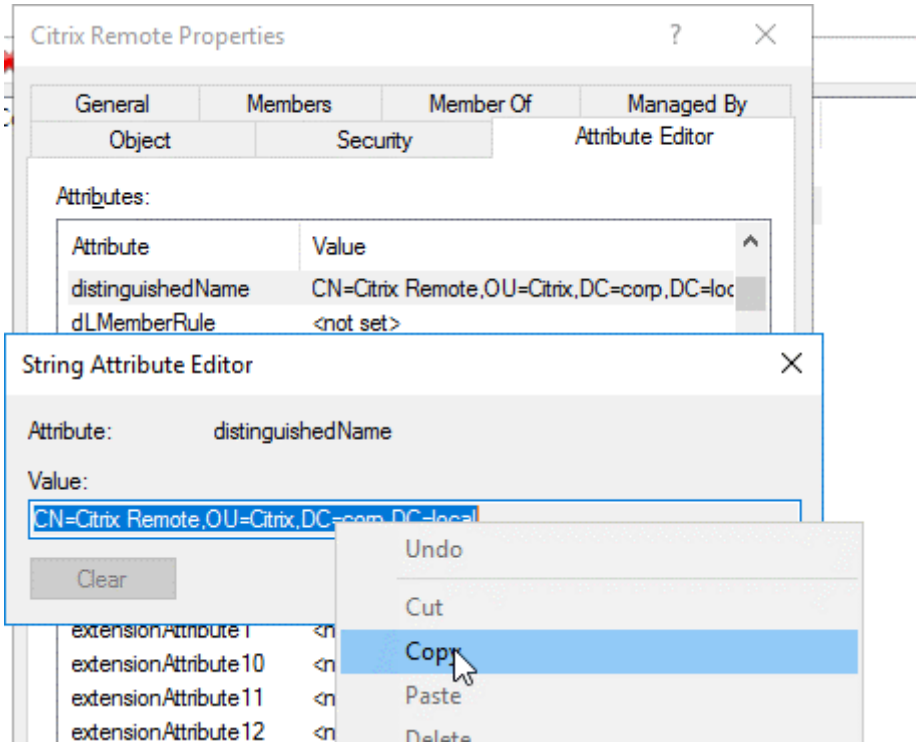


4. Sur la droite, accédez à l'onglet **Éditeur d'attributs**.

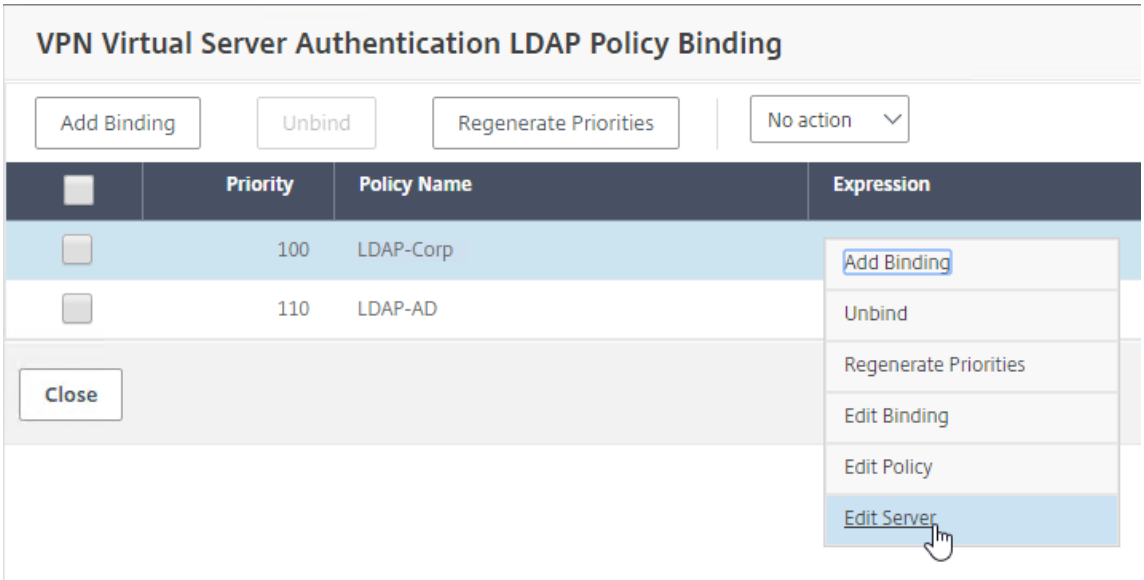


   Cet onglet n'est visible que si les **fonctionnalités avancées** sont activées et si vous n'avez pas utilisé la fonction **Rechercher**.

5. Faites défiler l'écran jusqu'à **DistinguishedName**, double-cliquez dessus, puis copiez-le dans le presse-papiers.

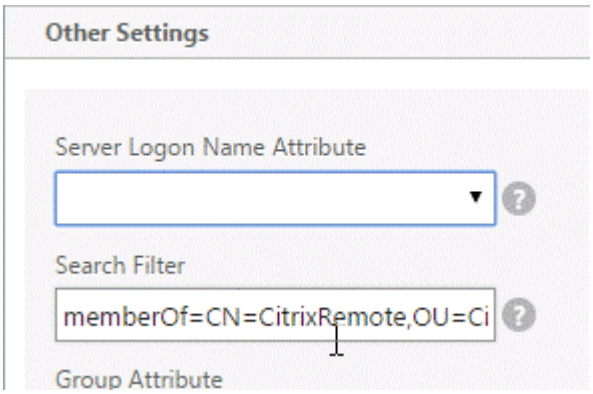


6. Dans l'interface graphique de NetScaler Gateway, accédez à **NetScaler Gateway**> Serveurs virtuels.
7. **Sélectionnez un serveur virtuel NetScaler Gateway existant et cliquez sur Modifier.**
8. Dans la section Authentification de base, cliquez sur **Stratégies LDAP**.
9. Cliquez avec le bouton droit de la souris sur une stratégie LDAP existante, puis cliquez sur **Modifier le serveur**.



10. Dans la section **Autres paramètres**, dans le champ **Filtre de recherche**, tapez **memberOf=**,

puis collez le nom unique du groupe Active Directory après le signe égal (=).



Un exemple de filtre de recherche est le suivant :
memberof=CN=Citrix Remote, OU=Citrix, DC=Corp, DC=Local
Remarque : Par défaut, NetScaler recherche uniquement les noms d'utilisateurs qui sont des membres directs du groupe Active Directory. Si vous souhaitez rechercher des groupes imbriqués, ajoutez le Microsoft OID au filtre de recherche LDAP. L'OID est inséré entre MemberOf et =.

Exemple : memberof:1.2.840.113556.1.4.1941 : =CN=Citrix Remote, OU=Citrix, DC=Corp, DC = local

11. Cliquez sur **OK**.

Utilisation de la haute disponibilité

January 26, 2024

Un déploiement à haute disponibilité de deux appliances NetScaler Gateway peut garantir un fonctionnement ininterrompu lors de n'importe quelle transaction. Lorsque vous configurez une appliance en tant que nœud principal et l'autre en tant que nœud secondaire, le nœud principal accepte les connexions et gère les serveurs tandis que le nœud secondaire surveille le nœud principal. Si, pour une raison quelconque, le nœud principal n'est pas en mesure d'accepter les connexions, le nœud secondaire prend le relais.

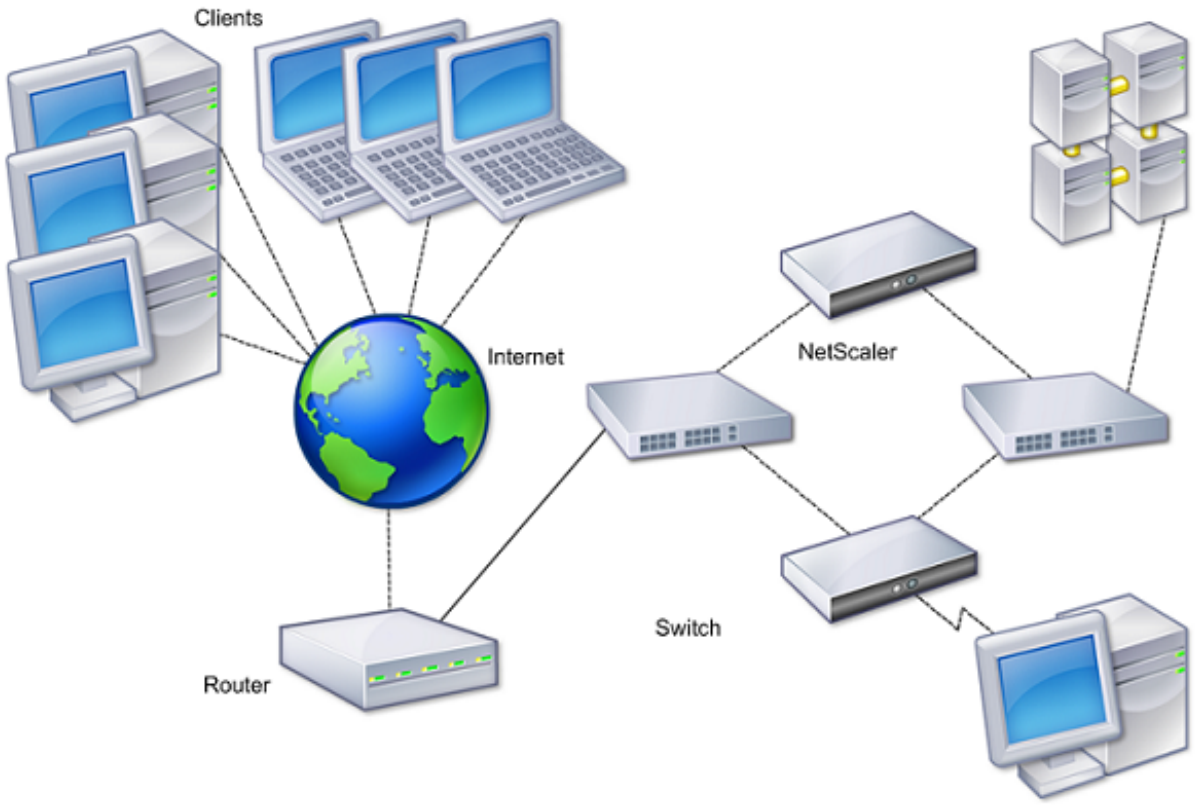
Le nœud secondaire surveille le nœud principal en envoyant des messages périodiques (souvent appelés messages de pulsation ou vérifications de l'état) pour déterminer si le nœud principal accepte les connexions. Si une vérification de l'état échoue, le nœud secondaire tente de nouveau la connexion pendant une période spécifiée, après quoi il détermine que le nœud principal ne fonctionne pas normalement. Le nœud secondaire prend ensuite le relais du nœud principal (processus appelé basculement).

Après un basculement, tous les clients doivent rétablir leurs connexions aux serveurs gérés, mais les règles de persistance de session sont conservées comme elles l'étaient avant le basculement.

Lorsque la persistance de la journalisation du serveur Web est activée, aucune donnée de journal n'est perdue en raison du basculement. Pour que la persistance de la journalisation soit activée, la configuration du serveur de journaux doit contenir des entrées pour les deux systèmes dans le fichier log.conf.

La figure suivante illustre une configuration réseau avec une paire haute disponibilité.

Figure 1. Appliances NetScaler Gateway dans une configuration haute disponibilité



Les étapes de base de la configuration de la haute disponibilité sont les suivantes :

1. Créez une configuration de base, avec les deux nœuds dans le même sous-réseau.
2. Personnalisez les intervalles auxquels les nœuds communiquent les informations de vérification de l'état.
3. Personnalisez le processus par lequel les nœuds maintiennent la synchronisation.
4. Personnalisez la propagation des commandes du principal vers le secondaire.
5. Le cas échéant, configurez le mode de sécurité intégrée pour éviter une situation dans laquelle aucun nœud n'est principal.
6. Configurez des adresses MAC virtuelles si votre environnement inclut des appareils qui n'acceptent pas les messages ARP gratuits de NetScaler Gateway.

Lorsque vous êtes prêt pour une configuration plus complexe, vous pouvez configurer des nœuds haute disponibilité dans différents sous-réseaux.

Pour améliorer la fiabilité de votre configuration haute disponibilité, vous pouvez configurer des moniteurs de routage et créer des liens redondants. Dans certaines situations, par exemple lors du dépannage ou de l'exécution de tâches de maintenance, vous pouvez forcer un nœud à basculer (attribuer le statut principal à l'autre nœud), ou forcer le nœud secondaire à rester secondaire ou le nœud principal à rester principal.

Fonctionnement de la haute disponibilité

January 26, 2024

Lorsque vous configurez NetScaler Gateway dans une paire haute disponibilité, le NetScaler Gateway secondaire surveille le premier dispositif en envoyant des messages périodiques, également appelés message cardiaque ou bilan de santé, afin de déterminer si le premier dispositif accepte les connexions. Si une vérification d'intégrité échoue, l'instance NetScaler Gateway secondaire tente à nouveau la connexion pendant une durée spécifiée jusqu'à ce qu'elle détermine que l'appliance principale ne fonctionne pas. Si l'appliance secondaire confirme l'échec de la vérification d'intégrité, l'instance NetScaler Gateway secondaire prend la relève de l'instance NetScaler Gateway principale. C'est ce qu'on appelle le basculement.

Les ports suivants sont utilisés pour échanger des informations relatives à la haute disponibilité entre les appliances NetScaler Gateway :

- Le port UDP 3003 est utilisé pour échanger des paquets Hello afin de communiquer l'état des intervalles.
- Le port TCP 3010 est utilisé pour la synchronisation de la configuration haute disponibilité.
- Le port TCP 3011 est utilisé pour synchroniser les paramètres de configuration.

Instructions relatives à la configuration de la haute disponibilité

Avant de configurer une paire haute disponibilité, vous devez passer en revue ces instructions :

- Chaque appliance NetScaler Gateway doit exécuter la même version du logiciel NetScaler Gateway. Vous trouverez le numéro de version en haut de la page dans l'utilitaire de configuration.
- NetScaler Gateway ne synchronise pas automatiquement les mots de passe entre deux appliances. Vous pouvez choisir de configurer chaque NetScaler Gateway avec le nom d'utilisateur et le mot de passe de l'autre appliance de la paire.
- Les entrées du fichier de configuration, ns.conf, sur le NetScaler Gateway principal et secondaire doivent correspondre, avec les exceptions suivantes :

  - Les appliances NetScaler Gateway principale et secondaire doivent chacune être configurées avec leur propre adresse IP système unique. Utilisez l'assistant de configuration pour configurer ou modifier l'adresse IP du système sur l'un ou l'autre de NetScaler Gateway.
  - Dans une paire haute disponibilité, l'ID NetScaler Gateway et l'adresse IP associée doivent pointer vers l'autre NetScaler Gateway.

    Par exemple, si vous possédez deux appliances, nommées AG1 et AG2, vous devez configurer AG1 avec l'ID NetScaler Gateway et l'adresse IP uniques d'AG2. Vous devez configurer AG2 avec l'ID NetScaler Gateway et l'adresse IP uniques d'AG1.

    Remarque : Chaque appliance NetScaler Gateway est toujours identifiée comme Node 0. Configurez chaque appliance avec un ID de nœud unique.

- Chaque appliance de la paire haute disponibilité doit posséder la même licence. Pour plus d'informations sur le système de licences, consultez la section Système de licences.
- Si vous créez un fichier de configuration sur l'un ou l'autre des nœuds à l'aide d'une méthode qui ne passe pas directement par l'utilitaire de configuration ou l'interface de ligne de commande (par exemple, importation de certificats SSL ou modification de scripts de démarrage), vous devez copier le fichier de configuration sur l'autre nœud ou créer un sur ce noeud.
- Lorsque vous configurez une paire haute disponibilité, assurez-vous que les adresses IP mappées et l'adresse de passerelle par défaut des dispositifs principal et secondaire sont identiques. Si nécessaire, vous pouvez modifier l'adresse IP mappée à tout moment en exécutant l'assistant d'installation.

Vous pouvez utiliser la liste de contrôle de pré-installation pour afficher la liste des paramètres spécifiques que vous devez configurer dans un déploiement haute disponibilité. Pour plus de détails, consultez la section Liste de contrôle de pré-installation.

Configuration des paramètres de haute disponibilité

March 27, 2024

Pour configurer une configuration de haute disponibilité, vous créez deux nœuds, chacun définissant l'adresse IP NetScaler Gateway de l'autre en tant que nœud distant. Vous pouvez commencer par vous connecter à l'une des deux appliances NetScaler que vous souhaitez configurer pour la haute disponibilité et ajouter un nœud. Spécifiez l'adresse IP NetScaler Gateway de l'autre appliance comme adresse du nouveau nœud. Ouvrez ensuite une session sur l'autre appliance et ajoutez un nœud qui possède l'adresse IP NetScaler Gateway de la première appliance. Un algorithme détermine quel nœud devient principal et lequel devient secondaire.

Avant de configurer les solutions matérielles-logicielles, ajoutez un nœud haute disponibilité. Ce nœud représente le premier ou le deuxième NetScaler Gateway de la paire haute disponibilité. Pour configurer la haute disponibilité, vous devez d'abord créer le nœud, puis configurer les paramètres de haute disponibilité.

Pour ajouter un nœud haute disponibilité

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système > Haute disponibilité**.
2. Dans le volet d'informations, dans l'onglet Nœuds, cliquez sur **Ajouter**.
3. Sur la page **Créer un nœud HA**, dans la zone de texte **Adresse IP du nœud distant**, tapez l'adresse NSIP du NetScaler à ajouter en tant que nœud distant. Si l'adresse IP de NetScaler Gateway est une adresse IPv6, cochez la case **IPv6** avant de saisir l'adresse.
4. Si vous souhaitez ajouter automatiquement le nœud local au nœud distant, sélectionnez Configurer le système distant pour participer à la configuration de la haute disponibilité. Si vous ne sélectionnez pas cette option, vous devez vous connecter à l'appliance représentée par le nœud distant et ajouter le nœud en cours de configuration.
5. Cliquez pour activer **Désactiver les interfaces/canaux du moniteur HA qui sont hors**tension.
6. Si l'appliance distante possède un nom d'utilisateur et un mot de passe différents, dans Informations d'identification de connexion au système distant, cliquez sur Les informations d'identification de connexion du système distant sont différentes de celles du nœud automatique.
7. Dans **Nom d'utilisateur**, tapez le nom d'utilisateur de l'appliance distante.
8. Dans **Mot de passe**, saisissez le mot de passe de l'appliance distante.
9. Cliquez sur **OK**.

Pour activer ou désactiver le nœud secondaire

Vous pouvez désactiver ou activer le nœud secondaire uniquement. Lorsque vous désactivez un nœud secondaire, il cesse d'envoyer des messages de pulsation au nœud principal et, par conséquent, le nœud principal ne peut plus vérifier l'état du nœud secondaire. Lorsque vous activez un nœud, ce dernier participe à la configuration de haute disponibilité.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez le nœud local, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue Configurer le nœud HA, dans État de la haute disponibilité, sélectionnez ACTIVÉ (Ne pas participer à HA).
4. Cliquez sur OK. Un message apparaît dans la barre d'état, indiquant que le nœud a été correctement configuré.

Pour configurer les paramètres de haute disponibilité

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système > Haute disponibilité**.
2. Dans le volet d'informations, dans l'onglet Nœuds, sélectionnez un nœud, puis cliquez sur **Modifier**.
3. Dans la boîte de dialogue **HA Configure Node**, dans ID, tapez le numéro de l'identifiant du nœud. ID spécifie le numéro de nœud unique de l'autre appliance.
4. Dans **Adresse IP**, tapez l'adresse IP du système, puis cliquez sur OK. L'adresse IP spécifie l'adresse IP de l'autre appliance.

Remarque : L'ID maximal pour les nœuds d'une paire haute disponibilité est de 64.

Modification du mot de passe d'un nœud RPC

March 27, 2024

Pour communiquer avec d'autres appliances NetScaler Gateway, chaque appliance doit connaître les autres appliances, notamment comment s'authentifier sur NetScaler Gateway. Les nœuds RPC sont des entités système internes utilisées pour la communication système à système des informations de configuration et de session. Un nœud RPC existe sur chaque NetScaler Gateway et stocke des informations, telles que les adresses IP de l'autre appliance NetScaler Gateway et les mots de passe utilisés pour l'authentification. Le NetScaler Gateway qui entre en contact avec un autre NetScaler Gateway vérifie le mot de passe dans le nœud RPC.

NetScaler Gateway nécessite des mots de passe de nœud RPC sur les deux appliances formant une paire haute disponibilité. Les mots de passe doivent être les mêmes sur les deux appliances. L'appliance principale doit connaître le mot de passe du nœud RPC secondaire et l'appliance secondaire doit connaître le mot de passe du nœud RPC principal. Au départ, chaque NetScaler Gateway est configuré avec le même mot de passe de nœud RPC. Pour améliorer la sécurité, vous devez modifier les mots de passe par défaut des nœuds RPC. Vous pouvez utiliser l'utilitaire de configuration pour configurer et modifier les nœuds RPC.

Les nœuds RPC sont implicitement créés lors de l'ajout d'un nœud ou d'un site Global Server Load Balancing (GSLB). Vous ne pouvez pas créer ou supprimer des nœuds RPC manuellement.

> **Important :**
>
> vous devez également sécuriser la connexion réseau entre les appliances. Vous pouvez configurer la sécurité lorsque vous configurez le mot de passe du nœud RPC en cochant la case **Sécurisé**.

Pour modifier le mot de passe d'un nœud RPC et activer une connexion sécurisée

1. Accédez à **Système > Réseau > RPC.**
2. Dans le volet d'informations, sélectionnez le nœud, puis cliquez sur **Modifier**.
3. Dans **Mot de passe** et **Confirmer le mot de passe**, tapez le nouveau mot
4. Dans **Adresse IP source, tapez l'adresse**IP système de l'autre appliance NetScaler Gateway.
5. Cliquez sur **Sécurisé**, puis cliquez sur **OK**.

> **Remarque :**
>
> lorsque vous activez l'option **Sécurisé**, l'appliance chiffre toutes les communications envoyées du nœud vers d'autres nœuds RPC, sécurisant ainsi la communication RPC.

Pour modifier le mot de passe d'un nœud RPC à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set ns rpcNode <IPAddress> {
 -password }
  [-secure ( YES | NO )]

show ns rpcNode
<!--NeedCopy-->
```

Exemple :

```
> set ns rpcNode 192.0.2.4 -password mypassword -secure YES
 Done
> show rpcNode
.
.
.
 IPAddress:  192.0.2.4 Password:  d336004164d4352ce39e
     SrcIP:  *           Secure:  ON
Done
>
<!--NeedCopy-->
```

Configuration des appliances principale et secondaire pour une haute disponibilité

January 26, 2024

Après avoir modifié le mot de passe du nœud RPC et activé la communication sécurisée, utilisez l'utilitaire de configuration pour configurer les nœuds NetScaler Gateway High Availability principal et secondaire.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Sous High Availability Status, cliquez sur Activé (Participer activement à HA), puis cliquez sur OK.

Configuration des intervalles de communication

January 26, 2024

Lorsque vous configurez NetScaler Gateway en tant que paire de haute disponibilité, vous pouvez configurer le NetScaler Gateway secondaire pour qu'il écoute à des intervalles spécifiques, mesurés en millisecondes (msec). Ces intervalles sont connus sous le nom d'intervalles Hello et d'intervalles morts.

L'intervalle Hello est l'intervalle auquel les messages de pulsation sont envoyés au nœud homologue. L'intervalle mort est l'intervalle de temps après lequel le nœud homologue est marqué en panne si les paquets de pulsation ne sont pas reçus. Les messages de pulsation sont des paquets UDP envoyés au port 3003 de l'autre nœud d'une paire haute disponibilité.

Lorsque vous configurez l'intervalle Hello, vous pouvez utiliser les valeurs 200 à 1000. La valeur par défaut est 200. Les valeurs de l'intervalle mort sont comprises entre 3 et 60. La valeur par défaut est 3.

> **Remarque**
>
> L'intervalle mort doit être défini comme un multiple de l'intervalle Hello.

Pour configurer les intervalles de communication pour le NetScaler Gateway secondaire

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Sous Intervalles, effectuez l'une des opérations suivantes ou les deux :

- Dans Intervalle Hello (msec), tapez la valeur, puis cliquez sur OK. La valeur par défaut est 200 millisecondes.
- Dans Intervalle mort (secondes), tapez la valeur, puis cliquez sur OK. La valeur par défaut est de trois secondes.

Synchronisation des appliances NetScaler Gateway

January 26, 2024

La synchronisation automatique des appliances NetScaler Gateway dans une paire haute disponibilité est activée par défaut. Avec la synchronisation automatique, vous pouvez apporter des modifications à une appliance et activer leur propagation automatique vers la seconde appliance. La synchronisation utilise le port 3010.

La synchronisation démarre lorsque les événements suivants se produisent :

- Le nœud secondaire redémarre.
- Le nœud principal devient secondaire après un basculement.

Vous pouvez désactiver la synchronisation, ce qui empêche le NetScaler Gateway secondaire de synchroniser sa configuration avec le NetScaler Gateway principal lorsqu'une modification intervient sur l'appliance principale. Vous pouvez également forcer la synchronisation.

Vous activez ou désactivez la synchronisation haute disponibilité sur le nœud secondaire de la paire.

Pour activer ou désactiver la synchronisation haute disponibilité

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Dans la boîte de dialogue Configurer le nœud, sous Synchronisation HA, effectuez l'une des opérations suivantes :
   - Pour désactiver la synchronisation, désactivez la case à cocher Le nœud secondaire récupérera la configuration à partir du serveur principal.
   - Pour activer la synchronisation, activez la case à cocher Le nœud secondaire récupérera la configuration à partir du serveur principal.
4. Cliquez sur OK. Un message apparaît dans la barre d'état indiquant que la configuration du nœud a réussi.

Pour forcer la synchronisation entre les appliances

Outre la synchronisation automatique, NetScaler Gateway prend en charge la synchronisation forcée entre les deux nœuds d'une paire haute disponibilité.

Vous pouvez forcer la synchronisation sur les appliances NetScaler Gateway principales et secondaires. Toutefois, si la synchronisation est déjà en cours, la commande échoue et NetScaler Gateway affiche un avertissement. La synchronisation forcée échoue également dans les cas suivants :

- Vous forcez la synchronisation sur un système autonome.
- Le nœud secondaire est désactivé.
- Vous désactivez la synchronisation haute disponibilité sur le nœud secondaire.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans l'onglet Noeuds, cliquez sur Forcer la synchronisation.

Synchronisation des fichiers de configuration dans une configuration haute disponibilité

March 27, 2024

Dans une configuration haute disponibilité, vous pouvez synchroniser divers fichiers de configuration du nœud principal vers le nœud secondaire.

Paramètres de synchronisation des fichiers dans une configuration haute disponibilité

- Mode

  Type de synchronisation à effectuer. Les descriptions suivantes incluent, entre parenthèses, l'argument de ligne de commande qui spécifie l'option.

  - **Tout sauf les licences et rc.conf** (tous). Synchronise les fichiers liés à la configuration du système, aux signets NetScaler Gateway, aux certificats SSL, aux listes CRL SSL, aux scripts d'injection HTML et aux objets XML d'Application Firewall.
  - **Signets** (signets). Synchronise tous les signets NetScaler Gateway.
  - **Certificats et clés SSL** (`ssl`). Synchronise tous les certificats, clés et CRL pour la fonctionnalité SSL.
  - **Licences et rc.conf** (divers). Synchronise tous les fichiers de licence et le fichier rc.conf.

- **Tout y compris les licences et rc.conf** (all_plus_misc). Synchronise les fichiers liés à la configuration du système, aux signets NetScaler Gateway, aux certificats SSL, aux listes CRL SSL, aux scripts d'injection HTML, aux objets XML d'Application Firewall, aux licences et au fichier rc.conf.

Remarque : d'autres options sont disponibles si vous installez une licence NetScaler sur l'appliance.

Pour synchroniser les fichiers dans une configuration haute disponibilité à l'aide de l'utilitaire de configuration

1. Dans le volet de navigation, développez **Système**, puis cliquez sur **Diagnostics**.
2. Dans le volet d'informations, sous **Utilitaires**, cliquez sur **Démarrer la synchronisation des fichiers HA**.
3. Dans la boîte de dialogue **Démarrer la synchronisation des fichiers**, dans le menu **Mode**, sélectionnez le type de synchronisation approprié (par exemple, Tout sauf les licences et rc.conf), puis cliquez sur **OK**.

Configuration de la propagation des commandes

March 27, 2024

Dans une configuration haute disponibilité, toute commande émise sur le nœud principal se propage automatiquement au nœud secondaire et s'exécute sur celui-ci avant l'exécution de la commande sur le nœud principal. Si la propagation des commandes échoue ou si l'exécution de la commande échoue sur le nœud secondaire, le nœud principal exécute la commande et consigne une erreur. La propagation des commandes utilise le port 3011.

Dans une configuration de paire haute disponibilité, la propagation des commandes est activée par défaut sur les nœuds principal et secondaire. Vous pouvez activer ou désactiver la propagation des commandes sur l'un des nœuds d'une paire haute disponibilité. Si vous désactivez la propagation des commandes sur le nœud principal, les commandes ne sont pas propagées vers le nœud secondaire. Si vous désactivez la propagation des commandes sur le nœud secondaire, les commandes propagées à partir du nœud principal ne sont pas exécutées sur le nœud secondaire.

Remarque : Après avoir réactivé la propagation, n'oubliez pas de forcer la synchronisation.

Remarque : Si la synchronisation a lieu pendant que vous désactivez la propagation, toutes les modifications liées à la configuration que vous apportez avant que la désactivation de la propagation ne prenne effet sont synchronisées avec le nœud secondaire. Cela vaut également pour les cas où la propagation est désactivée pendant la synchronisation.

Pour activer ou désactiver la propagation sur le nœud principal

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système**, puis cliquez sur **Haute disponibilité**.
2. Dans le volet d'informations, dans l'onglet **Nœuds**, sélectionnez un nœud, puis cliquez sur **Modifier**.
3. Dans la section **Propagation HA**, effectuez l'une des opérations suivantes :
   - Pour désactiver la propagation de la haute disponibilité, désactivez la case **à cocher Le nœud principal propage la configuration au secondaire**.
   - Pour activer la propagation haute disponibilité, activez la case à cocher Le **nœud principal propage la configuration au secondaire**.
4. Cliquez sur **OK**.

Dépannage de la propagation des commandes

January 26, 2024

La liste suivante décrit les raisons pour lesquelles la propagation des commandes peut échouer et les solutions permettant de restaurer le paramètre :

- La connectivité réseau n'est pas active. Si la propagation d'une commande échoue, vérifiez la connexion réseau entre les appliances NetScaler Gateway principales et secondaires.
- Ressources manquantes sur le NetScaler Gateway secondaire. Si l'exécution d'une commande réussit sur le NetScaler Gateway principal mais ne parvient pas à se propager vers le NetScaler Gateway secondaire, exécutez la commande directement sur le NetScaler Gateway secondaire pour voir le message d'erreur. L'erreur s'est peut-être produite parce que les ressources requises par la commande sont présentes sur le NetScaler Gateway principal et ne sont pas disponibles sur le NetScaler Gateway secondaire. Vérifiez également que les fichiers de licences de chaque appliance correspondent.

  Par exemple, vérifiez que tous vos certificats SSL (Secure Sockets Layer) sont présents sur chaque NetScaler Gateway. Vérifiez qu'une personnalisation du script d'initialisation existe sur les deux appliances NetScaler Gateway.
- Échec de l'authentification. Si vous recevez un message d'erreur d'échec de l'authentification, vérifiez les paramètres du nœud RPC sur chaque appliance.

Configurer le mode de sécurité intégrée

January 26, 2024

Dans une configuration haute disponibilité, le mode de sécurité intégrée garantit qu'un nœud est toujours principal lorsque les deux nœuds échouent à la vérification de l'état. Le mode de sécurité intégrée garantit que lorsqu'un nœud n'est que partiellement disponible, les méthodes de sauvegarde peuvent être activées et peuvent gérer le trafic.

Vous configurez le mode de sécurité intégrée haute disponibilité indépendamment sur chaque nœud.

Le tableau suivant présente certains des cas de sécurité intégrée. L'état NOT_UP signifie que le nœud a échoué à la vérification de l'état et que le nœud est partiellement disponible. L'état UP signifie que le nœud a réussi la vérification de santé.

Tableau 1 Boîtiers en mode de sécurité intégrée

État de santé du nœud A (principal)	État de santé du nœud B (secondaire)	Comportement de haute disponibilité par défaut	Comportement de haute disponibilité à sécurité intégrée	Description
NOT_UP (dernier échec)	NOT_UP (échec en premier)	A (secondaire), B (secondaire)	A (primaire), B (secondaire)	Si les deux nœuds tombent en panne, l'un après l'autre, le nœud qui était le dernier nœud principal reste principal.
NOT_UP (échec en premier)	NOT_UP (dernier échec)	A (secondaire), B (secondaire)	A (secondaire), B (primaire)	Si les deux nœuds tombent en panne, l'un après l'autre, le nœud qui était le dernier nœud principal reste principal.

État de santé du nœud A (principal)	État de santé du nœud B (secondaire)	Comportement de haute disponibilité par défaut	Comportement de haute disponibilité à sécurité intégrée	Description
UP	UP	A (primaire), B (secondaire)	A (primaire), B (secondaire)	Si les deux nœuds réussissent la vérification de l'état, aucun changement de comportement avec la sécurité intégrée activée.
UP	NOT_UP	A (primaire), B (secondaire)	A (primaire), B (secondaire)	Si seul le nœud secondaire tombe en panne, aucun changement de comportement lorsque la sécurité intégrée est activée.
NOT_UP	UP	A (secondaire), B (primaire)	A (secondaire), B (primaire)	Si seul le serveur principal échoue, aucun changement de comportement lorsque la sécurité intégrée est activée.
NOT_UP	UP (STAYSEC-ONDARY)	A (secondaire), B (secondaire)	A (primaire), B (secondaire)	Si le secondaire est configuré en tant que STAYSECONDARY, le principal reste principal même en cas de défaillance.

Pour configurer le mode de sécurité intégrée

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Dans la boîte de dialogue Configurer le nœud, sous Mode de sécurité intégrée, sélectionnez Conserver un nœud principal même lorsque les deux nœuds ne sont pas sains, puis cliquez sur OK.

Configuration de l'adresse MAC virtuelle

January 26, 2024

L'adresse MAC virtuelle est partagée par les appliances NetScaler Gateway principales et secondaires dans une configuration haute disponibilité.

Dans une configuration à haute disponibilité, le NetScaler Gateway principal possède toutes les adresses IP flottantes, telles que l'adresse IP mappée ou l'adresse IP virtuelle. Il répond aux demandes ARP (Address Resolution Protocol) de ces adresses IP avec sa propre adresse MAC. Par conséquent, la table ARP d'un périphérique externe (tel qu'un routeur) est mise à jour avec l'adresse IP flottante et l'adresse MAC principale de NetScaler Gateway. En cas de basculement, le NetScaler Gateway secondaire prend le relais en tant que nouveau NetScaler Gateway principal. Il utilise ensuite le protocole GARP (gratuitous address resolution protocol) pour annoncer les adresses IP flottantes qu'il a acquises auprès de l'appliance principale. L'adresse MAC, publiée par la nouvelle appliance principale, est celle de sa propre interface.

Certains appareils n'acceptent pas les messages GARP générés par NetScaler Gateway. Par conséquent, certains appareils externes conservent l'ancien mappage IP-Mac annoncé par l'ancien NetScaler Gateway principal. Cette situation peut entraîner l'indisponibilité d'un site. Pour résoudre le problème, vous devez configurer une adresse MAC virtuelle sur les deux appliances NetScaler Gateway d'une paire haute disponibilité. Cette configuration implique que les deux appliances NetScaler Gateway possèdent des adresses MAC identiques. Par conséquent, en cas de basculement, l'adresse MAC du NetScaler Gateway secondaire reste inchangée et les tables ARP des périphériques externes n'ont pas besoin d'être mises à jour.

Pour créer une adresse MAC virtuelle, créez un identificateur de routeur virtuel (ID) et liez-le à une interface. Dans une configuration haute disponibilité, l'utilisateur doit lier l'ID aux interfaces des deux solutions matérielles-logicielles.

Lorsque l'ID du routeur virtuel est lié à une interface, le système génère une adresse MAC virtuelle avec l'ID de routeur virtuel comme dernier octet. Un exemple d'adresse MAC virtuelle générique est 00:00:5e:00:01:<VRID>. Par exemple, si vous avez créé un ID de routeur virtuel de valeur 60 et que vous le liez à une interface, l'adresse MAC virtuelle résultante est 00:00:5 e : 00:01:3 c, où 3c est la représentation hexadécimale de l'ID de routeur virtuel. Vous pouvez créer 255 ID de routeur virtuel allant de 1 à 254.

Vous pouvez configurer des adresses MAC virtuelles pour IPv4 et IPv6.

Configuration des adresses MAC virtuelles IPv4

January 26, 2024

Lorsque vous créez une adresse MAC virtuelle IPv4 et que vous la liez à une interface, tout paquet IPv4 envoyé depuis l'interface utilise l'adresse MAC virtuelle liée à l'interface. Si aucune adresse MAC virtuelle IPv4 n'est liée à une interface, l'adresse MAC physique de l'interface est utilisée.

L'adresse MAC virtuelle générique est de la forme 00:00:5e:00:01:<VRID>. Par exemple, si vous créez un VRID avec une valeur de 60 et que vous le liez à une interface, l'adresse MAC virtuelle résultante est 00:00:5 e : 00:01:3 c, où 3c est la représentation hexadécimale du VRID. Vous pouvez créer 255 VRID avec des valeurs comprises entre 1 et 255.

Création ou modification d'une adresse MAC virtuelle IPv4

March 27, 2024

Vous créez une adresse MAC virtuelle IPv4 en lui attribuant un ID de routeur virtuel. Vous pouvez ensuite lier l'adresse MAC virtuelle à une interface. Vous ne pouvez pas lier plusieurs ID de routeur virtuel à la même interface. Pour vérifier la configuration de l'adresse MAC virtuelle, vous devez afficher et examiner l'adresse MAC virtuelle et les interfaces liées à l'adresse MAC virtuelle.

Paramètres de configuration d'une adresse MAC virtuelle

- vRID

  ID du routeur virtuel qui identifie l'adresse MAC virtuelle. Valeurs possibles : 1—255.

- `ifnum`

  Numéro d'interface (notation slot/port) à lier à l'adresse MAC virtuelle.

Pour configurer une adresse MAC virtuelle

1. Accédez à **Système > Réseau**, puis cliquez sur **VMAC**.
2. Dans le volet d'informations, sous l'onglet **VMAC**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un VMAC**, dans **Virtual Router ID**, tapez la valeur.
4. Sous **Interfaces associées**, dans **Interfaces disponibles**, sélectionnez une interface réseau, cliquez sur **Ajouter**, sur **Créer**, puis sur **Fermer**.

Une fois que vous avez créé l'adresse MAC virtuelle, elle apparaît dans l'utilitaire de configuration. Si vous avez sélectionné une interface réseau, l'ID du routeur virtuel est lié à cette interface.

Pour supprimer une adresse MAC virtuelle

Pour supprimer une adresse MAC virtuelle, vous devez supprimer l'ID de routeur virtuel correspondant.

1. Accédez à **Système > Réseau,** puis cliquez sur **VMAC**.
2. Dans le volet d'informations, sélectionnez un élément, puis cliquez sur **Supprimer**.

Pour lier et délier une adresse MAC virtuelle

Lorsque vous avez créé l'ID du routeur virtuel, vous avez sélectionné une interface réseau sur NetScaler Gateway, puis vous avez lié l'ID du routeur virtuel à l'interface réseau. Vous pouvez également dissocier une adresse MAC virtuelle de l'interface réseau, tout en conservant l'adresse MAC configurée sur NetScaler Gateway.

1. Accédez à **Système > Réseau**, puis cliquez sur **VMAC**.
2. Dans le volet d'informations, sélectionnez un élément, puis cliquez sur **Ouvrir**.
3. Sous **Interfaces configurées**, sélectionnez une interface réseau, cliquez sur **Supprimer**, sur **OK**, puis sur **Fermer**.

Configuration des adresses MAC virtuelles IPv6

January 26, 2024

NetScaler Gateway prend en charge les adresses MAC virtuelles pour les paquets IPv6. Vous pouvez lier n'importe quelle interface à une adresse MAC virtuelle pour IPv6, même si une adresse MAC virtuelle IPv4 est liée à l'interface. Tout paquet IPv6 envoyé depuis l'interface utilise l'adresse MAC virtuelle liée à cette interface. Si aucune adresse MAC virtuelle n'est liée à une interface, un paquet IPv6 utilise le MAC physique.

Création ou modification d'une adresse MAC virtuelle pour IPv6

March 27, 2024

Créez une adresse MAC virtuelle IPv6 en lui attribuant un ID de routeur virtuel IPv6. Liez ensuite l'adresse MAC virtuelle à une interface. Vous ne pouvez pas lier plusieurs ID de routeur virtuel IPv6 à une interface. Pour vérifier la configuration de l'adresse MAC virtuelle, affichez et examinez les adresses MAC virtuelles et les interfaces liées à l'adresse MAC virtuelle.

Paramètres de configuration d'une adresse MAC virtuelle pour IPv6

- `Virtual Router ID`

  ID du routeur virtuel qui identifie l'adresse MAC virtuelle. Valeurs possibles : 1—255.

- `ifnum`

  Numéro d'interface (notation slot/port) à lier à l'adresse MAC virtuelle.

Pour configurer une adresse MAC virtuelle pour IPv6

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **Système > Réseau**, puis cliquez sur VMAC.
2. Dans le volet d'informations, sous l'onglet VMAC6, effectuez l'une des opérations suivantes :
   - Pour créer une nouvelle adresse MAC virtuelle, cliquez sur Ajouter.
   - Pour modifier une adresse MAC virtuelle existante, cliquez sur Ouvrir.
3. Dans la boîte de dialogue Create VMAC6 ou Configure VMAC6, dans Virtual Router ID, entrez la valeur, telle que vRID6.
4. Dans Associate Interfaces, cliquez sur **Ajouter > Créer > Fermer**. Un message apparaît dans la barre d'état, indiquant que l'adresse MAC virtuelle est configurée.

Pour supprimer une adresse MAC virtuelle pour IPv6

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, développez **Système > Réseau**, puis cliquez sur VMAC.
2. Dans le volet d'informations, sous l'onglet VMAC6, sélectionnez l'ID du routeur virtuel que vous souhaitez supprimer, puis cliquez sur Supprimer. Un message apparaît dans la barre d'état, indiquant que l'adresse MAC virtuelle a été supprimée.

Configuration des paires haute disponibilité dans différents sous-réseaux

January 26, 2024

Un déploiement de haute disponibilité typique se produit lorsque les deux appliances d'une paire haute disponibilité résident sur le même sous-réseau. Un déploiement à haute disponibilité peut également consister en deux appliances NetScaler Gateway dans lesquelles chaque appliance se trouve dans un réseau différent. Cette rubrique décrit cette dernière configuration et inclut des exemples de configuration et une liste des différences entre les configurations haute disponibilité au sein d'un réseau et entre les réseaux.

Vous pouvez également configurer la redondance des liens et les moniteurs de routage. Ces fonctions de NetScaler Gateway sont utiles dans une configuration de haute disponibilité inter-réseaux. Les fonctions couvrent également le processus de vérification de l'état utilisé par chaque NetScaler Gateway pour s'assurer que l'appliance partenaire est active.

Fonctionnement de la configuration réseau indépendante

Les appliances NetScaler Gateway sont connectées à différents routeurs, appelés R3 et R4, sur deux réseaux différents. Les appliances échangent des paquets de pulsation via ces routeurs. Un paquet de pulsation est un signal qui se produit à intervalles réguliers et qui garantit que la connexion est toujours active. Vous pouvez développer cette configuration pour prendre en charge les déploiements impliquant un nombre illimité d'interfaces.

Remarque : Si vous utilisez le routage statique sur votre réseau, vous devez ajouter des routes statiques entre tous les systèmes pour garantir que les paquets de pulsation sont envoyés et reçus correctement. (Si vous utilisez le routage dynamique sur vos systèmes, les itinéraires statiques ne sont pas nécessaires.)

Lorsque les appliances d'une paire haute disponibilité résident sur deux réseaux différents, le NetScaler Gateway secondaire doit disposer d'une configuration réseau indépendante. Cela signifie que les appliances NetScaler Gateway sur différents réseaux ne peuvent pas partager d'adresses IP mappées, de réseaux locaux virtuels ou d'itinéraires réseau. Ce type de configuration, dans lequel les appliances NetScaler Gateway d'une paire haute disponibilité possèdent des paramètres configurables différents, est appelé configuration réseau indépendante ou configuration réseau symétrique.

Le tableau suivant récapitule les paramètres configurables pour une configuration réseau indépendante et montre comment vous devez les définir sur chaque NetScaler Gateway :

Paramètres configurables	Comportement
Adresses IP	Spécifique à NetScaler Gateway. Active uniquement sur cette appliance.
Adresse IP virtuelle	flottant.
LAN virtuel	Spécifique à NetScaler Gateway. Active uniquement sur cette appliance.
Itinéraires	Spécifique à NetScaler Gateway. Active uniquement sur cette appliance. Une route d'équilibrage de charge de liaison (LLB) est flottante.
listes de contrôle d'accès (ACL)	Flottant (commun). Actif sur les deux appareils.
Routage dynamique	Spécifique à NetScaler Gateway. Active uniquement sur cette appliance. Le NetScaler Gateway secondaire doit également exécuter les protocoles de routage et s'associer aux routeurs en amont.
Mode L2	Flottant (commun). Actif sur les deux appareils.
Mode L3	Flottant (commun). Actif sur les deux appareils.
Traduction inverse d'adresses réseau (NAT)	Spécifique à NetScaler Gateway. Inverser le NAT avec une adresse IP virtuelle car l'adresse IP NAT est flottante.

> **Remarque :**
>
> IPSET en mode INC est pris en charge avec les adresses IP publiques. Pour plus de détails, consultez NetScaler High Availability with Azure Load Balancer FrontEnd Validated IP Reference Design.

Ajout d'un nœud distant

March 27, 2024

Lorsque deux nœuds d'une paire haute disponibilité résident sur des sous-réseaux différents, chaque nœud doit avoir une configuration réseau différente. Par conséquent, pour configurer deux systèmes indépendants pour qu'ils fonctionnent comme une paire haute disponibilité, vous devez spécifier un mode de calcul réseau indépendant au cours du processus de configuration.

Lorsque vous ajoutez un nœud haute disponibilité, vous devez désactiver le moniteur de haute disponibilité pour chaque interface qui n'est pas connectée ou utilisée pour le trafic.

Pour ajouter un nœud distant pour un mode de calcul réseau indépendant

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système > Haute disponibilité**.
2. Dans le volet d'informations, cliquez sur l'onglet **Noeuds**, puis cliquez sur **Ajouter**.
3. Dans la boîte de dialogue High Availability Setup, dans la zone de texte **Remote Node IP Address**, tapez l'adresse IP NetScaler Gateway de l'appliance qui est le nœud distant.

   Pour utiliser une adresse IPv6, cochez la case **IPv6** avant de saisir l'adresse IP.
4. Si vous souhaitez ajouter automatiquement le nœud local au nœud distant, sélectionnez Configurer le système distant pour participer à la configuration de la haute disponibilité. Si vous ne sélectionnez pas cette option, vous devez ouvrir une session sur l'appliance représentée par le nœud distant et ajouter le nœud en cours de configuration.
5. Cliquez pour activer le moniteur HA clair sur les interfaces/canaux qui sont en panne.
6. Cliquez sur ce bouton pour activer le mode INC (Independent Network Configuration) en mode automatique.
7. Cliquez sur **OK**. La page **Noeuds** affiche les nœuds locaux et distants de votre configuration haute disponibilité.

Pour supprimer un nœud distant

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **Système > Haute disponibilité**.
2. Dans le volet d'informations, cliquez sur l'onglet **Noeuds**.
3. Sélectionnez le nœud que vous souhaitez supprimer, cliquez sur **Supprimer,** puis cliquez sur **Oui**.

Configuration des moniteurs de routage

March 27, 2024

Vous pouvez utiliser des moniteurs de routage pour faire en sorte que l'état de haute disponibilité dépend de la table de routage interne, que la table contienne des itinéraires statiques ou appris dynamiquement. Dans une configuration haute disponibilité, un moniteur de routage sur chaque nœud

vérifie la table de routage interne pour s'assurer qu'une entrée de route pour atteindre un réseau particulier est toujours présente. Si l'entrée de route n'est pas présente, l'état du moniteur de route passe à DOWN.

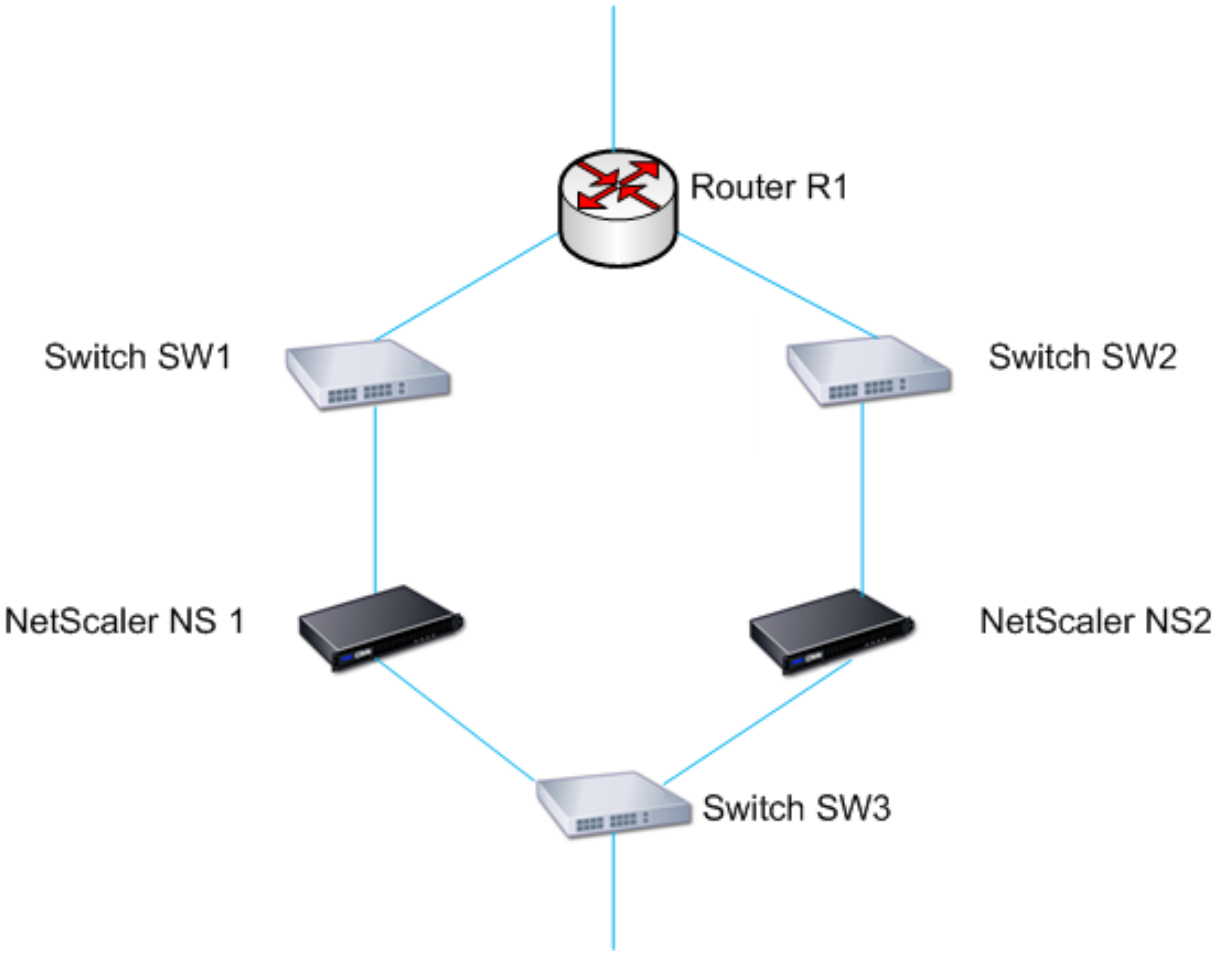
Lorsqu'une appliance NetScaler Gateway ne possède que des routes statiques pour atteindre un réseau et que vous souhaitez créer un moniteur de routage pour le réseau, vous devez activer les routes statiques surveillées pour les routes statiques. L'itinéraire statique surveillé supprime les routes statiques inaccessibles de la table de routage interne. Si vous désactivez les routes statiques surveillées sur des itinéraires statiques, une route statique inaccessible peut rester dans la table de routage interne, ce qui va à l'encontre de l'objectif du moniteur d'itinéraires.

Les moniteurs de routage sont pris en charge sur les paramètres de configuration réseau indépendante activés ou désactivés. Le tableau suivant montre ce qui se produit lorsque les moniteurs de routage sont configurés en haute disponibilité et lorsque la configuration réseau indépendante est activée ou désactivée.

Moniteurs de routage en haute disponibilité en mode Configuration réseau indépendante désactivé	Moniteurs de routage en haute disponibilité en mode Configuration réseau indépendante activé
Les moniteurs d'itinéraires sont propagés par les nœuds et échangés au cours de la synchronisation.	Les moniteurs d'itinéraires ne sont ni propagés par les nœuds ni échangés pendant la synchronisation.
Les moniteurs de routage ne sont actifs que dans le nœud principal actuel.	Les moniteurs de routage sont actifs sur le nœud principal et le nœud secondaire.
L'appliance NetScaler Gateway affiche toujours l'état d'un moniteur de routage comme étant ouvert, que l'entrée de route soit présente ou non dans la table de routage interne.	L'appliance NetScaler Gateway affiche l'état du moniteur de routage comme étant inactif si l'entrée de route correspondante n'est pas présente dans la table de routage interne.
Un moniteur d'itinéraires commence à surveiller son itinéraire dans les cas suivants, afin de permettre à NetScaler Gateway de connaître les itinéraires dynamiques, ce qui peut prendre jusqu'à 180 secondes : redémarrage, basculement, commande set route6 pour les routes v6, commande set route `msr` enable/disable pour routes v4, ajout d'un nouveau moniteur de route	Sans objet.

Les moniteurs de routage sont utiles lorsque vous désactivez le mode Configuration réseau indépendante et que vous souhaitez qu'une passerelle à partir d'un nœud principal soit aussi inaccessible que l'une des conditions du basculement haute disponibilité.

Par exemple, vous désactivez la configuration réseau indépendante dans une configuration haute disponibilité dans une topologie à deux bras comportant les appliances NetScaler Gateway NS1 et NS2 dans le même sous-réseau, avec le routeur R1 et les commutateurs SW1, SW2 et SW3, comme illustré dans la figure suivante. Étant donné que R1 est le seul routeur de cette configuration, vous souhaitez que la configuration haute disponibilité soit basculée chaque fois que R1 n'est pas accessible à partir du nœud principal actuel. Vous pouvez configurer un moniteur d'itinéraire (par exemple, RM1 et RM2, respectivement) sur chacun des nœuds pour surveiller l'accessibilité de R1 à partir de ce nœud.



Avec NS1 comme nœud principal actuel, le flux réseau est le suivant :

1. Le moniteur de routage RM1 sur NS1 surveille la table de routage interne de NS1 pour détecter la présence d'une entrée de route pour le routeur R1. NS1 et NS2 échangent des messages de pulsation via le commutateur SW1 ou SW3 à intervalles réguliers.
2. En cas de défaillance du commutateur SW1, le protocole de routage sur NS1 détecte que R1 n'est pas accessible et supprime donc l'entrée de route pour R1 de la table de routage interne. NS1 et NS2 échangent des messages de pulsation via le commutateur SW3 à intervalles réguliers.
3. En détectant que l'entrée de route pour R1 n'est pas présente dans la table de routage interne, RM1 lance un basculement. Si la route vers R1 est indisponible depuis NS1 et NS2, le bascule-

ment se produit toutes les 180 secondes jusqu'à ce que l'un des dispositifs parvienne à atteindre R1 et à restaurer la connexion.

Ajout ou suppression de moniteurs d'itinéraire

January 26, 2024

Lorsque les dispositifs d'une paire de dispositifs de haute disponibilité résident sur des réseaux différents, l'état de haute disponibilité de NetScaler Gateway dépend du fait que l'appliance est accessible ou non. Dans une configuration de haute disponibilité inter-réseaux, un moniteur de routage sur chaque NetScaler Gateway analyse la table de routage interne pour s'assurer qu'une entrée pour l'autre NetScaler Gateway est toujours présente.

Pour ajouter un moniteur de routage

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans la boîte de dialogue Lier/délier les moniteurs de routage, sous l'onglet Moniteurs de routage, cliquez sur Action, puis sur Configurer.
3. Sous Spécifier le moniteur d'itinéraire, dans Réseau, tapez l'adresse IP du réseau de l'autre appliance NetScaler Gateway.

   Pour configurer une adresse IPv6, cliquez sur IPv6, puis tapez l'adresse IP.
4. Dans Masque de réseau, tapez le masque de sous-réseau de l'autre réseau, cliquez sur Ajouter, puis sur OK.

Lorsque cette procédure est terminée, le moniteur de routage est lié à NetScaler Gateway.

Remarque : Lorsqu'un moniteur de routage n'est pas lié à NetScaler Gateway, l'état de haute disponibilité de l'une ou l'autre appliance est déterminé par l'état des interfaces.

Pour supprimer un moniteur de routage

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans l'onglet Moniteurs de routage, cliquez sur Action, puis sur Configurer.
3. Sous Moniteurs de routage configurés, sélectionnez le moniteur, cliquez sur Supprimer, puis sur OK.

Configuration de la redondance des liens

January 26, 2024

La redondance des liens regroupe les interfaces réseau afin d'empêcher le basculement en cas de défaillance d'une interface réseau d'un NetScaler Gateway qui possède d'autres interfaces fonctionnelles. La défaillance de la première interface sur le NetScaler Gateway principal déclenche le basculement, bien que la première interface puisse toujours utiliser son second lien pour répondre aux demandes des utilisateurs. Lorsque vous configurez la redondance des liens, vous pouvez regrouper les deux interfaces dans un ensemble d'interfaces de basculement, afin d'éviter que la défaillance d'un seul lien n'entraîne le basculement vers le NetScaler Gateway secondaire, sauf si toutes les interfaces du NetScaler Gateway principal ne fonctionnent pas.

Chaque interface d'un ensemble d'interfaces de basculement conserve des entrées de pont indépendantes. Les interfaces de surveillance activées et la haute disponibilité d'un NetScaler Gateway qui ne sont pas liées à un ensemble d'interfaces défaillant sont appelées interfaces critiques, car si l'une de ces interfaces échoue, le basculement est déclenché.

Pour configurer la redondance des liens

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans l'onglet Ensemble d'interfaces de basculement, cliquez sur Ajouter.
3. Dans la zone Nom, saisissez le nom du jeu.
4. Dans Interfaces, cliquez sur Ajouter.
5. Sous Interfaces disponibles, sélectionnez une interface, puis cliquez sur la flèche pour déplacer l'interface vers Configuré.
6. Répétez les étapes 4 et 5 pour la deuxième interface, puis cliquez sur Créer.

Vous pouvez ajouter autant d'interfaces que nécessaire pour le basculement entre les interfaces.

Pour supprimer des interfaces du jeu d'interfaces de basculement

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans l'onglet Ensemble d'interfaces de basculement, sélectionnez un ensemble, puis cliquez sur Supprimer.

Pour supprimer un ensemble d'interfaces de basculement

Si vous n'avez plus besoin d'un ensemble d'interfaces de basculement, vous pouvez le supprimer de NetScaler Gateway.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans l'onglet Ensemble d'interfaces de basculement, sélectionnez un ensemble, puis cliquez sur Supprimer.

Comprendre les causes du basculement

January 26, 2024

Les événements suivants peuvent entraîner un basculement dans une configuration haute disponibilité :

1. Si le nœud secondaire ne reçoit pas de paquet de pulsation du nœud principal pendant une période qui dépasse l'intervalle de temps mort défini sur le nœud secondaire. Pour plus d'informations sur la définition de l'intervalle mort, consultez Configuration des intervalles de communication. Les causes possibles pour un nœud ne recevant pas de paquets de pulsations d'un nœud homologue sont les suivantes :
    - Un problème de configuration réseau empêche les pulsations de traverser le réseau entre les nœuds de haute disponibilité.
    - Le nœud homologue rencontre une défaillance matérielle ou logicielle qui provoque le blocage (blocage), le redémarrage ou l'arrêt du traitement et du transfert des paquets de pulsation.
2. Le nœud principal rencontre une défaillance matérielle de sa carte SSL.
3. Le nœud principal ne reçoit aucun paquet de pulsation sur ses interfaces réseau pendant trois secondes.
4. Sur le nœud principal, une interface réseau qui ne fait pas partie d'un ensemble d'interfaces de basculement (FIS) ou d'un canal d'agrégation de liens (LA) et dont le moniteur de haute disponibilité (HAMON) est activé échoue. Les interfaces sont activées, mais passent à l'état DOWN.
5. Sur le nœud principal, toutes les interfaces d'un FIS échouent. Les interfaces sont activées, mais passent à l'état DOWN.
6. Sur le nœud principal, un canal LA avec HAMON activé échoue. Les interfaces sont activées, mais passent à l'état DOWN.
7. Sur le nœud principal, toutes les interfaces échouent. Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.

8. Sur le nœud principal, toutes les interfaces sont désactivées manuellement. Dans ce cas, le basculement se produit indépendamment de la configuration HAMON.
9. Vous forcez un basculement en exécutant la commande Forcer le basculement sur l'un des nœuds.
10. Un moniteur d'itinéraire lié au nœud principal est en panne.

Forcer le basculement à partir d'un nœud

January 26, 2024

Vous souhaiterez peut-être forcer un basculement si, par exemple, vous devez remplacer ou mettre à niveau le nœud principal. Vous pouvez forcer le basculement à partir du nœud principal ou du nœud secondaire. Un basculement forcé n'est ni propagé ni synchronisé. Pour afficher l'état de la synchronisation après un basculement forcé, vous pouvez afficher l'état du nœud.

Un basculement forcé échoue dans l'une des circonstances suivantes :

- Vous forcez le basculement sur un système autonome.
- Le nœud secondaire est désactivé.
- Le nœud secondaire est configuré pour rester secondaire.

L'appliance NetScaler Gateway affiche un message d'avertissement si elle détecte un problème potentiel lorsque vous exécutez la commande force failover. Le message inclut les informations qui ont déclenché l'avertissement et demande une confirmation avant de continuer.

Forcer le basculement sur le nœud principal ou secondaire

January 26, 2024

Si vous forcez le basculement sur le nœud principal, le nœud principal devient le nœud secondaire et le secondaire devient le nœud principal. Le basculement forcé n'est possible que lorsque le nœud principal peut déterminer que le nœud secondaire est actif.

Si le nœud secondaire est en panne, la commande Forcer le basculement renvoie le message d'erreur suivant : « Opération impossible en raison d'un état de pair non valide. Rectifier et réessayer."

Si le système secondaire est en état de réclamation ou inactif, la commande renvoie le message d'erreur suivant : `"Operation not possible now. Please wait for system to stabilize before retrying."`

Si vous exécutez la commande forcer le basculement à partir du nœud secondaire, le nœud secondaire devient principal et le nœud principal devient secondaire. Un basculement forcé ne peut se produire que si l'état du nœud secondaire est bon et que le nœud n'est pas configuré pour rester secondaire.

Si le nœud secondaire ne peut pas devenir le nœud principal, ou si le nœud secondaire a été configuré pour rester secondaire (à l'aide de l'option STAYSECONDARY), le nœud affiche le message d'erreur suivant : « Opération impossible car mon état n'est pas valide. Consultez le nœud pour plus d'informations. »

Pour forcer le basculement sur le nœud principal ou secondaire

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez le nœud principal, puis dans Actions, cliquez sur Forcer le basculement.
3. Dans la boîte de dialogue Avertissement, cliquez sur Oui.

Forcer le nœud principal à rester principal

January 26, 2024

Dans une configuration à haute disponibilité, vous pouvez forcer le NetScaler Gateway principal à rester principal même après le basculement de l'appliance. Vous ne pouvez configurer ce paramètre que sur des appliances NetScaler Gateway autonomes et sur NetScaler Gateway qui est l'appliance principale d'une paire haute disponibilité.

Pour forcer le nœud principal à rester principal

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Sous High Availability Status, cliquez sur Rester principal, puis cliquez sur OK.

Vous pouvez effacer cette configuration uniquement à l'aide de la commande suivante :

```
clear configuration full
```


Les commandes suivantes ne modifient pas la configuration de haute disponibilité de NetScaler Gateway :

```
clear configuration basic
clear configuration extended
```

Forcer le nœud secondaire à rester secondaire

March 27, 2024

Dans une configuration à haute disponibilité, vous pouvez forcer le NetScaler Gateway secondaire à rester secondaire, indépendamment de l'état du NetScaler Gateway principal. Lorsque vous configurez NetScaler Gateway pour qu'il reste secondaire, il reste secondaire même en cas de défaillance du NetScaler Gateway principal.

Par exemple, dans une configuration de haute disponibilité existante, supposons que vous deviez mettre à niveau le NetScaler Gateway principal et que ce processus prenne un certain temps. Pendant la mise à niveau, le NetScaler Gateway principal peut devenir indisponible, mais vous ne souhaitez pas que le NetScaler Gateway secondaire prenne le relais. Vous souhaitez qu'il reste le NetScaler Gateway secondaire, même s'il détecte une défaillance dans le NetScaler Gateway principal.

Si l'état d'un NetScaler Gateway appartenant à une paire haute disponibilité est configuré pour rester secondaire, il ne participe pas aux transitions d'état de haute disponibilité des machines. Vous pouvez vérifier l'état de NetScaler Gateway dans l'utilitaire de configuration de l'onglet **Nœuds**.

Ce paramètre fonctionne à la fois sur un NetScaler Gateway autonome et secondaire.

Lorsque vous définissez le nœud de haute disponibilité, il n'est ni propagé ni synchronisé et n'affecte que le NetScaler Gateway sur lequel le paramètre est configuré.

Pour forcer le nœud secondaire à rester secondaire

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, dans l'onglet Nœuds, sélectionnez un nœud, puis cliquez sur Modifier.
3. Sous État de haute disponibilité, cliquez sur Rester secondaire (rester en mode d'écoute), puis cliquez sur OK.

Pour remettre NetScaler Gateway en service en tant qu'appliance de haute disponibilité active

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez Système, puis cliquez sur Haute disponibilité.
2. Dans le volet d'informations, sous l'onglet Noeuds, sélectionnez l'appliance qui restera le nœud principal, puis cliquez sur Ouvrir.
3. Sous High Availability Status, cliquez sur Activé (Participer activement à HA), puis cliquez sur OK.

Utilisation du clustering

January 26, 2024

NetScaler Gateway peut être déployé dans des configurations de clusters afin de fournir un débit, une disponibilité et une évolutivité élevés pour le trafic client VPN. Dans un cluster, un groupe d'appliances ou de machines virtuelles NetScaler Gateway fonctionne comme une seule image système pour coordonner les sessions utilisateur et gérer le trafic vers les ressources réseau. Un cluster NetScaler Gateway peut être créé avec un minimum de deux et un maximum de 32 appliances ou machines virtuelles NetScaler Gateway configurées en tant que nœuds de cluster.

Lisez la documentation de
NetScaler Clustering avant de commencer à configurer votre cluster NetScaler Gateway. Portez une attention particulière aux rubriques suivantes de cette documentation.

- Consultez la section Configuration matérielle et logicielle requise pour vérifier que les systèmes que vous prévoyez d'utiliser répondent à la configuration requise.
- Consultez la section Fonctionnement du clustering pour obtenir une description des concepts de clustering.
- Consultez la section Configuration de la communication inter-nœuds pour planifier le déploiement et identifier les mises en garde pouvant être pertinentes pour votre environnement.

Un cluster NetScaler Gateway fonctionne comme un cluster NetScaler de type de configuration VIP repéré.

> **Important :**
>
> L'Assistant **XenApp et XenDesktop** n'est pas pris en charge pour la mise en cluster. Par conséquent, vous ne trouvez pas l'Assistant **XenApp et XenDesktop** dans la section **GUI > Volet de navigation > Intégrer avec les produits NetScaler**.

Configuration de la mise en cluster

March 27, 2024

Les principales tâches liées à la configuration du clustering NetScaler Gateway sont les suivantes :

1. Déterminez quel dispositif NetScaler Gateway ou quelle machine virtuelle est le coordinateur de configuration et créez une instance de cluster sur ce système (s'il n'en existe pas déjà une).
2. Joignez les systèmes NetScaler Gateway au cluster en tant que nœuds.
3. Créez un groupe de nœuds sur l'instance de cluster, avec l'option STICKY définie.
4. Liez un seul nœud de cluster au groupe de nœuds de cluster.
5. Configurez un serveur virtuel NetScaler Gateway sur le coordinateur de configuration et liez-le au groupe de nœuds du cluster.

Plusieurs méthodes sont disponibles pour configurer un cluster NetScaler. L'ensemble de tâches suivant utilise la méthode la plus directe disponible dans l'utilitaire de configuration.

Pour créer une instance de cluster NetScaler Gateway à l'aide de l'utilitaire de configuration

Une fois que les détails du déploiement sont en ordre, commencez la configuration sur NetScaler Gateway qui est le coordinateur de configuration.

Attention : La création de l'instance de cluster efface la configuration. Si vous devez enregistrer la configuration système existante pour référence, archivez une copie avant de poursuivre la configuration du cluster. Tous les paramètres existants à utiliser dans le cluster peuvent être réappliqués sur le coordinateur de configuration une fois le cluster établi.

1. Connectez-vous à l'utilitaire de configuration NetScaler à l'adresse NSIP.
2. Développez le nœud Système, puis le sous-nœud Cluster.
3. Dans le volet d'informations, cliquez sur Gérer le cluster.
4. Dans la boîte de dialogue Configuration du cluster, définissez les paramètres requis pour créer le cluster.

    a) Entrez un ID d'instance de cluster. L'ID d'instance de cluster est l'identificateur numérique de l'instance de cluster. La valeur par défaut est 1, mais vous pouvez la définir sur n'importe quel nombre compris entre 1 et 16.
    b) Entrez l'adresse IP du cluster. L'adresse IP du cluster est l'adresse IP du coordinateur de configuration du cluster, qui est l'adresse IP de gestion du cluster.
    c) Sélectionnez l'interface de fond de panier préférée. Il s'agit de cette interface NetScaler Gateway à utiliser pour la communication entre les nœuds du cluster.

5. Cliquez sur Créer.
6. À l'invite de confirmation du redémarrage du système, cliquez sur Oui.
7. Une fois que le nœud est activé et que la synchronisation a réussi, à partir de l'adresse IP du cluster, modifiez les informations d'identification RPC pour le nœud et l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.
8. Attendez que le système redémarre. Une fois disponible, connectez-vous à l'utilitaire de configuration à l'adresse IP du cluster configurée à l'étape 4 (2).

Remarque : Dans le volet de **détails Informations système**, le nœud local à l'adresse NSIP est signalé en tant que coordinateur de configuration. Cela confirme que l'instance de cluster de base fonctionne désormais.

Le nœud local du coordinateur de configuration est automatiquement ajouté au cluster. D'autres nœuds peuvent être ajoutés dans la tâche suivante.

Ajouter des nœuds à un cluster NetScaler Gateway

Une fois l'instance de cluster établie, vous pouvez commencer à ajouter d'autres nœuds NetScaler Gateway au cluster.

Pour ajouter d'autres systèmes NetScaler Gateway au cluster, vous pouvez utiliser l'utilitaire de configuration pour émettre à distance les paramètres de création de nœuds de cluster et de join-cluster.

Remarque : L'ajout de nœuds au cluster doit être terminé avant de configurer votre configuration NetScaler Gateway. Ainsi, vous n'avez pas à répéter la configuration de NetScaler Gateway en cas de problème avec la configuration de votre cluster et que vous souhaitez supprimer le cluster et recommencer.

1. Connectez-vous à l'utilitaire de configuration NetScaler à l'adresse IP du cluster.
2. Développez le nœud **Système**, puis le sous-nœud Cluster.
3. Dans le volet d'informations, cliquez sur **Gérer le cluster**.
4. Dans le volet de détails des nœuds de cluster, cliquez sur **Ajouter**.
5. Dans le volet **Create Cluster Node**, entrez un ID de nœud unique pour ce nœud.
6. Entrez l'adresse IP NetScaler du système à ajouter en tant que nœud de cluster.
7. Dans le volet des **informations d'identification du nœud de cluster**, entrez le nom d'utilisateur et le mot de passe NetScaler Gateway pour le système NetScaler Gateway distant.
8. Dans le volet Informations d'identification de Configuration Coordinator, saisissez le mot de passe de l'utilisateur autorisé local.
9. Cliquez sur **Créer**.
10. Lorsque vous y êtes invité, cliquez sur **OUI** pour autoriser l'enregistrement de la configuration du système et redémarrer à chaud le NetScaler Gateway distant.

11. Une fois que le nœud est activé et que la synchronisation a réussi, à partir de l'adresse IP du cluster, modifiez les informations d'identification RPC pour le nœud et l'adresse IP du cluster. Pour plus d'informations sur la modification du mot de passe d'un nœud RPC, voir Modifier le mot de passe d'un nœud RPC.

Répétez les étapes 4 à 11 pour chaque système NetScaler Gateway distant supplémentaire que vous souhaitez configurer en tant que nœud de cluster.

Vérifiez que les nœuds de cluster sont inclus dans la liste des nœuds actifs dans le volet de détails des nœuds de cluster. Si des nœuds sont manquants, répétez les étapes 4 à 10 jusqu'à ce que tous les nœuds nécessaires soient répertoriés.

Création d'un groupe de nœuds de cluster

Une fois les nœuds de cluster ajoutés, un groupe de nœuds de cluster peut être créé.

1. Connectez-vous à l'utilitaire de configuration NetScaler à l'adresse IP du cluster.
2. Développez le nœud **Système**, puis le sous-nœud Cluster.
3. Cliquez sur **Groupes de nœuds**.
4. Dans le volet d'informations, cliquez sur **Ajouter**.
5. Entrez le nom du groupe de nœuds de cluster.
6. Sélectionnez l'option **Sticky** pour prendre en charge le type de serveur virtuel NetScaler Gateway.
7. Cliquez sur **Continuer**.

Le groupe de nœuds de cluster est maintenant établi. Avant de quitter cette zone de l'utilitaire de configuration, vous pouvez lier le nœud NetScaler Gateway local au nouveau groupe de nœuds du cluster. Il s'agit du seul nœud lié au groupe de clusters.

Liez le nœud de cluster local au groupe de nœuds de cluster

Étant donné qu'une configuration de cluster NetScaler Gateway est de type repéré, un seul nœud peut être lié au groupe de nœuds. La procédure suivante lie le nœud local du coordinateur de configuration au groupe de nœuds, mais n'importe quel nœud du cluster peut être utilisé pour cette liaison.

1. Dans le volet Avancé, développez Noeuds de cluster.
2. Dans le volet Nœuds de cluster central, sélectionnez Aucun nœud de cluster.
3. Dans l'écran de configuration du nœud de cluster, cliquez sur Liaison.
4. Sélectionnez le nœud local représenté par l'adresse NSIP pour ce système NetScaler Gateway.
5. Cliquez sur Insérer.
6. Cliquez sur OK.
7. Cliquez sur Terminé.

Le cluster est maintenant rempli et prêt à partager un serveur virtuel NetScaler Gateway tel que configuré par la tâche suivante.

Liaison d'un serveur virtuel NetScaler Gateway au groupe de nœuds de cluster

Une fois le cluster établi, vous pouvez procéder à la création de la configuration NetScaler Gateway que le déploiement du cluster est destiné à servir. Pour lier la configuration au cluster, vous devez créer le serveur virtuel NetScaler Gateway et le lier à un groupe de nœuds de cluster configuré pour être de type Sticky. Une fois que le serveur virtuel est lié au groupe de nœuds du cluster, vous pouvez continuer à configurer NetScaler Gateway.

Si plusieurs serveurs virtuels NetScaler Gateway sont configurés, ils doivent également être liés au groupe de nœuds du cluster.

Remarque : Si les serveurs virtuels NetScaler Gateway n'ont pas encore été configurés, vous devrez peut-être d'abord activer NetScaler Gateway et les fonctionnalités d'authentification, d'autorisation et d'audit sous
Système > Paramètres Configurer les fonctionnalités de base.

1. Connectez-vous à l'utilitaire de configuration NetScaler à l'adresse IP du cluster.
2. Développez le nœud **Système**, puis le sous-nœud Cluster.
3. Cliquez sur **Groupes de nœuds**.
4. Dans le volet **Groupe de nœuds**, sélectionnez le nom du groupe de nœuds souhaité, puis cliquez sur **Modifier**.
5. Dans le volet **Avancé** sur la droite, développez l'option **Serveurs virtuels**, puis cliquez sur l'icône + pour ajouter un serveur virtuel.
6. Choisissez le type de serveur virtuel VPN, puis cliquez sur **Continuer**.
7. Cliquez sur **Bind**.
8. Si le serveur virtuel requis est répertorié, sélectionnez-le, puis cliquez sur **Insérer**, puis sur **OK**.
9. Si vous devez créer un nouveau serveur virtuel, cliquez sur **Ajouter**. Procédez à la configuration du serveur virtuel NetScaler. Au minimum, il suffit de créer le serveur virtuel afin qu'il puisse être lié au groupe de nœuds de cluster.
10. **Une fois que le serveur virtuel est disponible dans la liste des serveurs virtuels NetScaler Gateway, sélectionnez-le, puis cliquez sur Insérer.**
11. Cliquez sur **OK**.
12. Cliquez sur **Terminé**.

Remarque : Si plusieurs serveurs virtuels NetScaler Gateway sont configurés, ils doivent également être liés au groupe de nœuds du cluster en utilisant la même méthode.

Unified Gateway

March 27, 2024

NetScaler avec Unified Gateway : une seule URL

NetScaler avec Unified Gateway permet un accès sécurisé simplifié à n'importe quelle application via une URL unique pour les utilisateurs de bureau et mobiles. Derrière cette URL unique, les administrateurs disposent d'un point unique pour la configuration, la sécurité et le contrôle de l'accès à distance aux applications. De plus, les utilisateurs distants bénéficient d'une expérience améliorée avec une connexion unique transparente à toutes les applications dont ils ont besoin, ainsi qu'une connexion/déconnexion une fois qu'ils sont faciles à utiliser.

Pour ce faire, NetScaler with Gateway, associé aux capacités de commutation de contenu de NetScaler et à sa vaste infrastructure d'authentification, permet d'accéder aux sites et applications de l'organisation via cette URL unique. Les utilisateurs distants peuvent également utiliser des appareils mobiles iOS ou Android et des systèmes Linux, PC ou Mac avec le client Citrix Secure Access pour un accès uniforme à l'URL Unified Gateway, où qu'ils se trouvent.

Un déploiement Unified Gateway permet d'accéder à une seule URL aux catégories d'applications suivantes :

- Applications Intranet.
- Applications sans client
- Application de logiciel en tant que service
- Applications préconfigurées desservies par NetScaler
- Applications publiées Citrix Virtual Apps and Desktops

Les applications intranet peuvent être n'importe quelle application Web qui réside dans le réseau d'entreprise sécurisé. Il s'agit de ressources internes telles qu'un site intranet organisationnel, une application de suivi des bogues ou un wiki.

Habituellement résidant également dans le réseau d'entreprise sécurisé, les **applications sans client** Unified Gateway fournissent un accès URL unique à Outlook Web Access et SharePoint. Ces applications permettent d'accéder aux ressources de messagerie et d'équipe Exchange sans logiciel client dédié qui doit être disponible pour les utilisateurs distants.

Les applications SaaS, également connues sous le nom de Cloud Apps, sont des applications externes basées sur le cloud dont les entreprises dépendent, telles que ShareFile, Salesforce ou NetSuite. L'authentification unique basée sur SAML est prise en charge avec les applications SaaS qui l'offrent.

Certaines entreprises peuvent avoir**préconfiguré des applications desservies par NetScaler**déployées dans une configuration d'équilibrage de charge NetScaler. Souvent, cette application est également appelée « proxy inverse ». Unified Gateway prend en charge ces applications lorsqu'un serveur virtuel pour le déploiement réside sur la même instance ou le même dispositif NetScaler Unified Gateway. Ces applications peuvent avoir leur propre configuration d'authentification, qui est indépendante de la configuration d'Unified Gateway.

Toutes les **applications publiées Citrix Virtual Apps and Desktops publiées**peuvent être mises à disposition via une URL Unified Gateway. Les stratégies SmartAccess et SmartControl peuvent éventuellement être appliquées à une stratégie granulaire et à un contrôle d'accès à ces ressources.

Assistant de configuration d'Unified Gateway

La méthode recommandée pour configurer un déploiement de NetScaler avec Unified Gateway consiste à utiliser l'assistant de configuration d'Unified Gateway. L'assistant vous guide tout au long de la configuration et crée tous les serveurs virtuels, stratégies et expressions nécessaires, et applique les paramètres en fonction des détails fournis. Après la configuration initiale, l'assistant peut être utilisé pour gérer votre déploiement et surveiller son fonctionnement.

> **Remarque :**
>
> L'assistant de configuration d'Unified Gateway n'effectue pas de configuration initiale des systèmes. L'installation de base de votre appliance NetScaler Gateway ou de votre instance VPX doit être terminée avant de configurer Unified Gateway. Reportez-vous aux instructions d'installation pourconfigurer NetScaler Gateway à l'aide de l'assistant de première configurationpour terminer la configuration de base.

Les éléments d'Unified Gateway configurés par l'assistant sont les suivants :

- Le serveur virtuel principal Unified Gateway
- Un certificat de serveur SSL pour le serveur virtuel Unified Gateway
- Une configuration d'authentification principale et toute configuration d'authentification secondaire facultative
- Une sélection de thèmes de portail et une personnalisation facultative
- Les applications utilisateur accessibles via le portail Unified Gateway

Pour chacun de ces éléments, vous devez fournir des informations de configuration. Pour un déploiement de base d'Unified Gateway, les informations suivantes sont nécessaires.

- Pour le serveur virtuel Unified Gateway principal, l'adresse IP publique et le numéro de port IP du déploiement. Il s'agit de l'adresse IP qui se résout dans le DNS en nom d'hôte de l'URL Unified Gateway. Par exemple, si l'URL de votre déploiement Unified Gateway est,`https://mycompany.com/` l'adresse IP doit être résolue en monentreprise.com.

- Certificat de serveur SSL signé pour le déploiement. NetScaler Gateway prend en charge les certificats au format PEM ou PFX.
- Informations sur le serveur d'authentification principal. Les systèmes d'authentification pris en charge pour cette configuration d'authentification sont LDAP/Active Directory, RADIUS et basés sur un certificat. Une configuration d'authentification LDAP ou RADIUS secondaire peut également être créée. L'adresse IP du serveur d'authentification doit être fournie avec les informations d'identification de l'administrateur ou les attributs d'annuaire pertinents. Pour l'authentification par certificat, les attributs du certificat de l'appareil et un certificat d'autorité de certification doivent être fournis.
- Un thème de portail peut être sélectionné. Si une conception de portail personnalisée ou de marque est souhaitée, des graphiques personnalisés peuvent être téléchargés sur le système à l'aide de l'assistant.
- Pour les applications utilisateur Web, les URL des applications individuelles doivent être spécifiées. Pour les applications Web qui doivent utiliser l'authentification unique SAML, l'utilitaire collecte l'URL Assertion Consumer Service ainsi que d'autres paramètres SAML facultatifs. Rassemblez les détails de configuration à l'avance pour les applications qui utilisent un système d'authentification SAML.
- Pour que les ressources publiées par Citrix Virtual Apps and Desktops soient mises à disposition via le déploiement d'Unified Gateway, vous devez spécifier le point d'intégration (StoreFront, l'interface Web ou l'interface Web sur NetScaler). L'utilitaire nécessite le nom de domaine complet du point d'intégration, le chemin d'accès au site, le domaine d'authentification unique, l'URL du serveur STA (Secure Ticket Authority) et d'autres, selon le type de point d'intégration.

Gestion de la configuration supplémentaire

Pour les paramètres spécifiques au site qui ne sont pas disponibles dans l'utilitaire de configuration d'Unified Gateway, tels que les paramètres SSL alternatifs ou les stratégies de session, vous pouvez gérer les paramètres nécessaires dans l'utilitaire de configuration NetScaler Gateway. Vous pouvez modifier ces paramètres sur les serveurs virtuels de commutation de contenu ou VPN une fois qu'ils sont créés par l'utilitaire de configuration Unified Gateway.

Serveur virtuel de commutation de contenu

Il s'agit de l'entité de configuration NetScaler à l'origine de l'adresse IP et de l'URL principales du déploiement. Les certificats et paramètres du serveur SSL sont gérés sur ce serveur virtuel. Comme ce serveur virtuel est l'hôte réseau répondant au déploiement, la réponse du serveur ICMP et l'état RHI peuvent être modifiés sur ce serveur virtuel, si nécessaire. Le serveur virtuel de commutation de

contenu se trouve sous l'onglet **Configuration**, dans **Gestion du trafic** > **Commutation de contenu** > **Serveurs virtuels**.

> **Important :**
>
> Lorsque vous mettez à niveau votre environnement Unified Gateway vers la version 13.0 build 58.x ou ultérieure, le bouton DTLS est désactivé sur le serveur virtuel de commutation de contenu configuré avant la passerelle ou le serveur virtuel VPN. Activez manuellement le bouton DTLS sur le serveur virtuel de commutation de contenu après la mise à niveau. N'activez pas le potentiomètre DTLS si vous utilisez l'assistant pour la configuration.

Serveur virtuel VPN

Tous les autres paramètres, profils et liaisons de stratégie VPN pour la configuration d'Unified Gateway sont gérés sur ce serveur virtuel, y compris la configuration d'authentification principale. Cette entité est gérée sous l'onglet **Configuration** sous **NetScaler Gateway** > **Serveurs virtuels**. Le nom du serveur virtuel VPN concerné inclut le nom donné au serveur virtuel de commutation de contenu lors de la configuration initiale d'Unified Gateway.

> **Remarque :**
>
> Les serveurs virtuels VPN créés pour un déploiement Unified Gateway ne sont pas adressables et l'adresse IP 0.0.0.0 est attribuée.

FAQ sur Unified Gateway

March 27, 2024

Qu'est-ce qu'Unified Gateway ?

Unified Gateway est une nouvelle fonctionnalité de la version 11.0 de NetScaler qui permet de recevoir du trafic sur un seul serveur virtuel (appelé serveur virtuel Unified Gateway), puis de diriger ce trafic en interne, le cas échéant, vers des serveurs virtuels liés au serveur virtuel Unified Gateway.

La fonctionnalité Unified Gateway permet aux utilisateurs finaux d'accéder à plusieurs services à l'aide d'une adresse IP ou d'une URL unique (associée au serveur virtuel Unified Gateway). Les administrateurs peuvent libérer des adresses IP et simplifier la configuration du déploiement de NetScaler Gateway.

Chaque serveur virtuel Unified Gateway peut frontaliser un serveur virtuel NetScaler Gateway ainsi qu'un ou plusieurs serveurs virtuels d'équilibrage de charge dans le cadre d'une formation. Unified Gateway fonctionne à l'aide de la fonction de commutation de contenu de l'appliance NetScaler.

Voici quelques exemples de déploiements d'Unified Gateway :

- Serveur virtuel Unified Gateway -> [un serveur virtuel NetScaler Gateway]
- Serveur virtuel Unified Gateway -> [un serveur virtuel NetScaler Gateway, un serveur virtuel d'équilibrage de charge]
- Serveur virtuel Unified Gateway -> [un serveur virtuel NetScaler Gateway, deux serveurs virtuels d'équilibrage de charge]
- Serveur virtuel Unified Gateway -> [un serveur virtuel NetScaler Gateway, trois serveurs virtuels d'équilibrage de charge]

Chacun des serveurs virtuels d'équilibrage de charge peut être n'importe quel serveur d'équilibrage de charge standard hébergeant un service principal, tel que Microsoft Exchange ou Citrix ShareFile.

Pourquoi utiliser Unified Gateway ?

La fonctionnalité Unified Gateway permet aux utilisateurs finaux d'accéder à plusieurs services à l'aide d'une adresse IP ou d'une URL unique (associée au serveur virtuel Unified Gateway). Pour les administrateurs, l'avantage est de libérer des adresses IP et de simplifier la configuration du déploiement de NetScaler Gateway.

Est-ce qu'il y a plus d'un serveur virtuel Unified Gateway ?

Oui. Il peut y avoir autant de serveurs virtuels Unified Gateway que nécessaire.

Pourquoi la commutation de contenu est-elle nécessaire pour Unified Gateway ?

La fonctionnalité de commutation de contenu est nécessaire car le serveur virtuel de commutation de contenu est celui qui reçoit le trafic et le dirige en interne vers le serveur virtuel approprié. Le serveur virtuel de commutation de contenu est le principal composant de la fonctionnalité Unified Gateway.

Dans les versions antérieures à la version 11.0, la commutation de contenu peut être utilisée pour recevoir du trafic pour plusieurs serveurs virtuels. Cette utilisation est-elle également appelée Unified Gateway ?

L'utilisation d'un serveur virtuel de commutation de contenu pour recevoir du trafic pour plusieurs serveurs virtuels est prise en charge dans les versions antérieures à la version 11.0. Toutefois, la com-

mutation de contenu ne peut pas diriger le trafic vers un serveur virtuel NetScaler Gateway.

Les améliorations apportées à la version 11.0 permettent à un serveur virtuel de commutation de contenu de diriger le trafic vers n'importe quel serveur virtuel, y compris un serveur virtuel NetScaler Gateway.

Qu'est-ce qui a changé avec les stratégies de commutation de contenu dans Unified Gateway ?

1. Un nouveau paramètre de ligne de commande « -TargetvServer » est ajouté pour l'action de changement de contenu. Le nouveau paramètre est utilisé pour spécifier le serveur virtuel NetScaler Gateway cible. Exemple:

   ```
   add cs action UG_CSACT_MyUG -targetVserver UG_VPN_MyUG
   ```

   Dans l'utilitaire de configuration de NetScaler Gateway, l'action de commutation de contenu comporte une nouvelle option, Target Virtual Server, qui peut référencer un serveur virtuel NetScaler Gateway.
2. Une nouvelle expression de stratégie avancée, is_vpn_url, peut être utilisée pour faire correspondre NetScaler Gateway et les demandes spécifiques à l'authentification.

Quelles fonctionnalités de NetScaler Gateway ne sont actuellement pas prises en charge dans Unified Gateway ?

Toutes les fonctionnalités sont prises en charge dans Unified Gateway. Toutefois, un problème mineur (ID de problème 544325) a été signalé lors de l'ouverture de session native via le plug-in VPN. Dans ce cas, l'authentification unique (SSO) transparente ne fonctionne pas.

Avec Unified Gateway, quel est le comportement des analyses EPA ?

Avec Unified Gateway, l'analyse des points de terminaison est déclenchée uniquement pour les méthodes d'accès à NetScaler Gateway, et non pour l'accès à NetScaler AAA TM. Si un utilisateur essaie d'accéder à un serveur virtuel NetScaler AAA TM alors que l'authentification est effectuée sur le serveur virtuel NetScaler Gateway, le scan EPA n'est pas déclenché. Toutefois, si l'utilisateur tente d'obtenir un accès VPN sans client/VPN complet, l'analyse EPA configurée est déclenchée. Dans ce cas, l'authentification ou l'authentification unique transparente sont effectuées.

Quelles sont les conditions de licence requises pour Unified Gateway ?

Unified Gateway n'est pris en charge que pour les licences Advanced et Premium. Il n'est pas disponible uniquement pour NetScaler Gateway ou les éditions de licence Standard.

Le serveur virtuel NetScaler Gateway utilisé avec Unified Gateway nécessite-t-il une configuration IP/port/SSL ?

Pour un serveur virtuel NetScaler Gateway utilisé avec le serveur virtuel Unified Gateway, aucune configuration IP/port/SSL n'est requise sur le serveur virtuel NetScaler Gateway. Toutefois, pour la fonctionnalité de proxy RDP, vous pouvez lier le même certificat de serveur SSL/TLS au serveur virtuel NetScaler Gateway.

Dois-je reprovisionner les certificats SSL/TLS qui se trouvent sur le serveur virtuel NetScaler Gateway pour les utiliser avec un serveur virtuel Unified Gateway ?

Il n'est pas nécessaire de reprovisionner les certificats qui sont actuellement liés à votre serveur virtuel NetScaler Gateway. Vous êtes libre de réutiliser tous les certificats SSL existants et de les lier au serveur virtuel Unified Gateway.

Quelle est la différence entre une URL unique et un déploiement multi-hôtes ? De laquelle ai-je besoin ?

Une URL unique fait référence à la capacité du serveur virtuel Unified Gateway à gérer le trafic pour un nom de domaine complet (FQDN). Cette restriction existe lorsque Unified Gateway utilise un certificat de serveur SSL/TLS dont l'objet du certificat est renseigné avec le nom de domaine complet. Par exemple : ug.citrix.com

Si Unified Gateway utilise un certificat de serveur générique, il peut gérer le trafic pour plusieurs sous-domaines. Par exemple :*.citrix.com

Une autre option est la configuration SSL/TLS avec la fonctionnalité d'indicateur de nom de serveur (SNI) pour permettre la liaison de plusieurs certificats de serveur SSL/TLS. Exemples : auth.citrix.com, auth.citrix.de, auth.citrix.co.uk, auth.citrix.co.jp

Un seul hôte par rapport à plusieurs hôtes est analogue à la façon dont les sites Web sont généralement hébergés sur un serveur Web (par exemple, le serveur HTTP Apache ou Microsoft Internet Information Services (IIS)). S'il existe un seul hôte, vous pouvez utiliser un chemin d'accès au site pour basculer le trafic de la même manière que vous utilisez un alias ou un « répertoire virtuel » dans Apache. S'il y a plusieurs hôtes, vous utilisez un en-tête d'hôte pour basculer le trafic de la même manière que vous utilisez les hôtes virtuels dans Apache.

Quels mécanismes d'authentification peuvent être utilisés avec Unified Gateway ?

Tous les mécanismes d'authentification existants qui sont compatibles avec NetScaler Gateway le sont également avec Unified Gateway.

Il s'agit notamment de LDAP, RADIUS, SAML, Kerberos, l'authentification basée sur des certificats, etc.

Quel que soit le mécanisme d'authentification configuré sur le serveur virtuel NetScaler Gateway avant la mise à niveau, il est automatiquement utilisé lorsque le serveur virtuel NetScaler Gateway est placé derrière le serveur virtuel Unified Gateway. Aucune étape de configuration supplémentaire n'est requise, à part l'attribution d'une adresse IP non adressable (0.0.0.0) au serveur virtuel NetScaler Gateway.

Qu'est-ce que l'authentification « SelfAuth » ?

SelfAuth n'est pas un type d'authentification en soi. SelFauth décrit comment une URL est créée. Un nouveau paramètre de ligne de commande `ssotype` est disponible pour la configuration de l'URL VPN. Exemple:

```
> add vpn url RGB RGB "http://blue.citrix.lab/"-vServerName Blue -
ssotype selfauth
```

SelFauth est l'une des valeurs du paramètre `ssotype`. Ce type d'URL peut être utilisé pour accéder à des ressources qui ne se trouvent pas dans le même domaine que le serveur virtuel Unified Gateway. Le paramètre est visible dans l'utilitaire de configuration lors de la configuration d'un signet.

Qu'est-ce que « StepUp » Authentication ?

Lorsque des niveaux d'authentification supplémentaires et plus sécurisés sont requis pour accéder à une ressource NetScaler AAA TM, vous pouvez utiliser l'authentification StepUp. Sur la ligne de commande, utilisez une commande AuthnProfile pour définir le paramètre AuthnLevel. Exemple:

```
1 add authentication authnProfile AuthProfile -authnVsName AAATMVserver -
     AuthenticationHost auth.citrix.lab -AuthenticationDomain citrix.lab
     **-**AuthenticationLevel 100
2 <!--NeedCopy-->
```

Ce profil d'authentification est lié au serveur virtuel d'équilibrage de charge.

L'authentification StepUp est-elle prise en charge pour les serveurs virtuels NetScaler AAA TM ?

Oui, il est pris en charge.

Qu'est-ce que c'est `login once/logout once` ?

`Login Once`: les utilisateurs du VPN se connectent une seule fois à un serveur virtuel NetScaler AAA TM ou NetScaler Gateway. À partir de ce moment, les utilisateurs de VPN ont un accès transparent à toutes les applications d'entreprise/Cloud/Web. Il n'est pas nécessaire de réauthentifier l'utilisateur. Toutefois, la réauthentification est effectuée dans des cas particuliers, tels que NetScaler AAA TM StepUp.

`Logout Once`: une fois la première session NetScaler AAA TM ou NetScaler Gateway créée, elle est utilisée pour créer les sessions NetScaler AAA TM ou NetScaler Gateway suivantes pour cet utilisateur. Si l'une de ces sessions est déconnectée, l'appliance NetScaler déconnecte également les autres applications ou sessions de l'utilisateur.

Des stratégies d'authentification communes peuvent-elles être spécifiées au niveau de la Unified Gateway avec un serveur virtuel d'équilibrage de charge NetScaler AAA TM spécifique authentifié lié au niveau du serveur virtuel d'équilibrage de charge ? Quelles sont les étapes de configuration pour prendre en charge ce cas d'utilisation ?

Si vous devez spécifier des stratégies d'authentification distinctes pour le serveur virtuel NetScaler AAA TM situé derrière Unified Gateway, vous devez disposer d'un serveur virtuel d'authentification distinct et adressable indépendamment (similaire à une configuration NetScaler AAA TM ordinaire). Le paramètre d'hôte d'authentification sur le serveur virtuel d'équilibrage de charge doit pointer vers ce serveur virtuel d'authentification.

Comment configurer Unified Gateway pour que les serveurs virtuels NetScaler AAA TM liés disposent de leurs propres stratégies d'authentification ?

Dans ce scénario, le serveur d'équilibrage de charge doit avoir l'option FQDN d'authentification définie pour pointer vers le serveur virtuel NetScaler AAA TM. Le serveur virtuel NetScaler AAA TM doit disposer d'une adresse IP indépendante et être accessible depuis NetScaler et ses clients.

Un serveur virtuel d'authentification NetScaler AAA TM est-il requis pour authentifier les utilisateurs via un serveur virtuel Unified Gateway ?

Non. Le serveur virtuel NetScaler Gateway authentifie même les utilisateurs de NetScaler AAA TM.

Où définissez-vous les stratégies d'authentification de NetScaler Gateway : sur le serveur virtuel Unified Gateway ou sur le serveur virtuel NetScaler Gateway ?

Les stratégies d'authentification doivent être liées au serveur virtuel NetScaler Gateway.

Comment activer l'authentification sur les serveurs virtuels NetScaler AAA TM situés derrière un serveur virtuel de commutation de contenu Unified Gateway ?

Activez l'authentification sur NetScaler AAA TM et pointez l'hôte d'authentification vers le FQDN de commutation de contenu Unified Gateway.

Comment ajouter des serveurs TM Virtual à la commutation de contenu (URL unique ou multi-hôtes) ?

Il n'y a aucune différence entre l'ajout des serveurs virtuels NetScaler AAA TM pour une seule URL et l'ajouter pour plusieurs hôtes. Dans les deux cas, le serveur virtuel est ajouté en tant que cible dans une action de changement de contenu. La différence entre une URL unique et plusieurs hôtes est implémentée par des règles de stratégie de commutation de contenu.

Qu'arrive-t-il aux stratégies d'authentification liées à un serveur virtuel d'équilibrage de charge NetScaler AAA TM si ce serveur virtuel est déplacé derrière un serveur virtuel Unified Gateway ?

Les stratégies d'authentification sont liées au serveur virtuel d'authentification, et le serveur virtuel d'authentification est lié au serveur virtuel d'équilibrage de charge. Pour le serveur virtuel Unified Gateway, Citrix recommande d'utiliser le serveur virtuel NetScaler Gateway comme point d'authentification unique, ce qui évite de devoir effectuer une authentification sur un serveur virtuel d'authentification (ni même d'avoir besoin d'un serveur virtuel d'authentification spécifique). Le fait de pointer l'hôte d'authentification vers le nom de domaine complet du serveur virtuel Unified Gateway garantit que l'authentification est effectuée par le serveur virtuel NetScaler Gateway. Si vous pointez l'hôte d'authentification vers la commutation de contenu pour Unified Gateway et que vous disposez toujours d'un serveur virtuel d'authentification lié, les stratégies d'authentification liées au serveur virtuel d'authentification sont ignorées. Toutefois, si vous pointez un hôte d'authentification vers un serveur virtuel d'authentification adressable indépendant, les stratégies d'authentification liées prennent effet.

Comment configurer les stratégies de session pour les sessions NetScaler AAA TM ?

Si, dans Unified Gateway, aucun serveur virtuel d'authentification n'est spécifié pour le serveur virtuel NetScaler AAA TM, les sessions NetScaler AAA TM héritent des stratégies de session NetScaler Gateway. Si le serveur virtuel d'authentification est spécifié, les stratégies de session NetScaler AAA TM liées à ce serveur virtuel sont appliquées.

Quelles sont les modifications apportées au portail NetScaler Gateway dans NetScaler 11.0 ?

Dans les versions de NetScaler antérieures à la version 11.0, une personnalisation de portail unique peut être configurée au niveau mondial. Chaque serveur virtuel de passerelle d'une appliance NetScaler donnée utilise la personnalisation globale du portail.

Dans NetScaler 11.0, grâce à la fonctionnalité des thèmes de portail, vous pouvez configurer plusieurs thèmes de portail. Les thèmes peuvent être liés globalement ou à des serveurs virtuels spécifiques.

NetScaler 11.0 prend-il en charge la personnalisation du portail NetScaler Gateway ?

À l'aide de l'utilitaire de configuration, vous pouvez utiliser la nouvelle fonctionnalité de thèmes de portail pour personnaliser et créer complètement les thèmes de portail. Vous pouvez télécharger différentes images, définir des jeux de couleurs, modifier les étiquettes de texte, etc.

Les pages du portail qui peuvent être personnalisées sont les suivantes :

- Page de connexion
- Page Analyse des points de terminaison
- Page d'erreur Endpoint Analysis
- Page Post Endpoint Analysis
- Page de connexion VPN
- Page d'accueil du portail

Avec cette version, vous pouvez personnaliser les serveurs virtuels NetScaler Gateway avec des conceptions de portail uniques.

Les thèmes de portail sont-ils pris en charge dans les déploiements de haute disponibilité ou de clusters de NetScaler ?

Oui. Les thèmes de portail sont pris en charge dans les déploiements de haute disponibilité et de clusters de NetScaler.

Mes personnalisations doivent-elles être migrées dans le cadre du processus de mise à niveau de NetScaler 11.0 ?

Non. Les personnalisations existantes de la page du portail NetScaler Gateway qui sont invoquées via la modification du fichier rc.conf/rc.netscaler ou à l'aide de fonctionnalités de thème personnalisées dans les versions 10.1/10.5 ne sont pas migrées automatiquement lors de la mise à niveau vers NetScaler 11.0.

Y a-t-il des étapes à suivre avant la mise à niveau pour être prêt à utiliser les thèmes de portail dans NetScaler 11.0 ?

Toutes les personnalisations existantes doivent être supprimées des fichiers rc.conf ou rc.netscaler.

L'autre option est que si des thèmes personnalisés sont utilisés, ils doivent être affectés au paramètre Par défaut :

1. Accédez à **Configuration > NetScaler Gateway > Paramètres généraux**
2. Cliquez sur **Modifier les paramètres globaux**.
3. Cliquez sur **Expérience client** et sélectionnez **Par défaut** dans la liste **Thème de l'interface utilisateur**.

J'ai des personnalisations qui sont stockées sur l'instance NetScaler, invoquée par rc.conf ou rc.netscaler. Comment passer aux thèmes du portail ?

L'article CTX126206 du centre de connaissances Citrix détaille une telle configuration pour les versions 9.3 et 10.0 de NetScaler jusqu'à la version 10.0 build 73.5001.e. Depuis la version 10.0 de NetScaler 10.0 73.5002.e (y compris 10.1 et 10.5), le paramètre UITHEME CUSTOM est disponible pour aider les clients à conserver leurs personnalisations après les redémarrages. Si les personnalisations sont stockées sur le disque dur de NetScaler et que vous souhaitez continuer à les utiliser, sauvegardez les fichiers de l'interface graphique 11.0 et insérez-les dans le fichier de thème personnalisé existant. Si vous souhaitez passer aux thèmes du portail, vous devez d'abord désactiver le paramètre UITHEME dans les paramètres généraux ou dans le profil de session, sous **Expérience client**. Vous pouvez également le définir sur DEFAULT ou GREENBUBBLE. Ensuite, vous pouvez commencer à créer et à lier un thème de portail.

Comment puis-je exporter mes personnalisations actuelles et les enregistrer avant de passer à NetScaler 11.0 ? Puis-je déplacer les fichiers exportés vers une autre appliance NetScaler ?

Les fichiers personnalisés qui ont été téléchargés dans le dossier **ns_gui_custom** se trouvent sur le disque et sont conservés pendant les mises à niveau. Toutefois, ces fichiers peuvent ne pas être entièrement compatibles avec le nouveau noyau NetScaler 11.0 et les autres fichiers d'interface graphique qui font partie du noyau. Par conséquent, Citrix recommande de sauvegarder les fichiers de l'interface graphique 11.0 et de personnaliser les sauvegardes.

De plus, l'utilitaire de configuration ne contient aucun utilitaire permettant d'exporter le dossier **ns_custom_gui** vers une autre appliance NetScaler. Utilisez SSH ou un utilitaire de transfert de fichiers tel que WinSCP pour retirer les fichiers de l'instance NetScaler.

Les thèmes de portail sont-ils pris en charge pour les serveurs virtuels NetScaler AAA TM ?

Oui. Les thèmes de portail sont pris en charge pour les serveurs virtuels NetScaler AAA TM.

Qu'est-ce qui a changé dans la fonctionnalité de proxy RDP pour NetScaler Gateway 11.0 ?

De nombreuses améliorations ont été apportées au proxy RDP depuis la version améliorée de NetScaler 10.5.e. Dans NetScaler 11.0, cette fonctionnalité est disponible dès la première version publiée.

Changements de licence

La fonctionnalité RDP Proxy de NetScaler 11.0 ne peut être utilisée qu'avec les éditions Premium et Advanced. Les licences Citrix Concurrent User (CCU) doivent être obtenues pour chaque utilisateur.

Commande Enable

Dans NetScaler 10.5.e, aucune commande ne permettait d'activer le proxy RDP. Dans NetScaler 11.0, la commande enable a été ajoutée :

```
enable feature rdpproxy
<!--NeedCopy-->
```

La fonctionnalité doit être sous licence pour exécuter cette commande.

Autres modifications apportées au proxy RDP

Un attribut de clé pré-partagée (PSK) sur le profil de serveur a été rendu obligatoire.

Pour migrer les configurations NetScaler 10.5.e existantes pour le proxy RDP vers NetScaler 11.0, les détails suivants doivent être compris et traités.

Si un administrateur souhaite ajouter une configuration de proxy RDP existante à un déploiement Unified Gateway choisi :

- L'adresse IP du serveur virtuel NetScaler Gateway doit être modifiée et définie sur une adresse IP non adressable (0.0.0.0).
- Tous les certificats de serveur SSL/TLS et les stratégies d'authentification doivent être liés au serveur virtuel NetScaler Gateway qui fait partie de la formation Unified Gateway choisie.

Comment migrer une configuration de proxy RDP (Remote Desktop Protocol) basée sur NetScaler 10.5.e vers NetScaler 11.0 ?

Option 1 : conserver le serveur virtuel NetScaler Gateway existant avec la configuration du proxy RDP tel quel, avec une licence Premium ou Advanced.

Option 2 : déplacez le serveur virtuel NetScaler Gateway existant avec la configuration du proxy RDP, en le plaçant derrière un serveur virtuel Unified Gateway.

Option 3 : ajouter un serveur virtuel NetScaler Gateway autonome avec une configuration de proxy RDP à une appliance Standard Edition existante.

Comment configurer NetScaler Gateway pour la configuration du proxy RDP à l'aide de la version 11.0 de NetScaler ?

Il existe deux options pour déployer un proxy RDP à l'aide de la version NS 11.0 :

1. Utilisation d'un serveur virtuel NetScaler Gateway orienté vers l'extérieur. Cela nécessite une adresse IP/FQDN visible de l'extérieur pour le serveur virtuel NetScaler Gateway. Cette option est disponible dans NetScaler 10.5.e.
2. Utilisation d'un serveur virtuel Unified Gateway frontal au serveur virtuel NetScaler Gateway.

Avec l'option 2, le serveur virtuel NetScaler Gateway n'a pas besoin de sa propre adresse IP/FQDN, car il utilise une adresse IP non adressable (0.0.0.0).

HDX Insight est-il compatible avec Unified Gateway ?

Lorsque NetScaler Gateway est déployé avec Unified Gateway, les conditions suivantes doivent être remplies :

- Le serveur virtuel NetScaler Gateway doit être associé à un certificat SSL valide.
- Le serveur virtuel NetScaler Gateway doit être activé pour générer des enregistrements AppFlow sur NetScaler ADM, pour les rapports HDX Insight.

Comment migrer ma configuration HDX Insight existante ?

Aucune migration n'est nécessaire. Les stratégies AppFlow liées à un serveur virtuel NetScaler Gateway sont reportées si ce serveur virtuel NetScaler Gateway est placé derrière un serveur virtuel Unified Gateway.

Pour les données existantes sur NetScaler ADM pour le serveur virtuel NetScaler Gateway, il existe deux possibilités :

- Si l'adresse IP du serveur virtuel NetScaler Gateway est attribuée à un serveur virtuel Unified Gateway dans le cadre de la migration vers Unified Gateway, les données restent liées au serveur virtuel NetScaler Gateway
- Si une adresse IP distincte est attribuée au serveur virtuel Unified Gateway, les données AppFlow du serveur virtuel NetScaler Gateway sont liées à cette nouvelle adresse IP. Par conséquent, les données existantes ne font pas partie des nouvelles données.

Configuration VPN sur une appliance NetScaler Gateway

March 27, 2024

> **Important :**
>
> Les captures d'écran de cette section sont conservées en niveaux de gris pour les raisons suivantes :
>
> - Aidez les lecteurs malvoyants, en particulier ceux qui souffrent de daltonisme ou de carence en couleur.
> - L'utilisation d'une image en niveaux de gris représente l'image sous une forme générique qui ne montre aucun impact de la personnalisation du codage couleur qui aurait pu être effectuée dans le navigateur de l'utilisateur ou le système d'exploitation.

Les utilisateurs peuvent utiliser les méthodes suivantes pour se connecter aux ressources réseau de votre organisation via NetScaler Gateway :

- Application Citrix Workspace qui contient tous les plug-ins Citrix installés sur la machine utilisateur.
- Application Citrix Workspace pour le Web qui permet aux utilisateurs de se connecter aux applications, aux bureaux et à ShareFile à l'aide d'un navigateur Web.
- Secure Hub pour permettre aux utilisateurs d'accéder à Secure Mail, WorxWeb et aux applications mobiles depuis leurs appareils iOS et Android.
- Client Citrix Secure Access pour Windows, macOS X ou Linux.
- Application NetScaler Gateway pour iOS et Android.
- Accès sans client qui fournit aux utilisateurs l'accès dont ils ont besoin sans installer de logiciel utilisateur.
- Interopérabilité avec le plug-in Citrix SD-WAN.

Si les utilisateurs installent le client Citrix Secure Access puis installent l'application Citrix Workspace depuis Citrix Virtual Apps 6.5 pour Windows Server 2008 (y compris le Feature Pack et le Feature Pack

2), Citrix Virtual Desktops 7.0 ou version ultérieure, l'application Citrix Workspace ajoute automatiquement le client Citrix Secure Access. Les utilisateurs peuvent se connecter au client Citrix Secure Access depuis un navigateur Web ou depuis l'application Citrix Workspace.

SmartAccess détermine automatiquement les méthodes d'accès autorisées pour une machine utilisateur en fonction des résultats d'une analyse d'analyse des terminaux. Pour plus d'informations sur SmartAccess, consultez la section Configuration de SmartAccess.

NetScaler Gateway prend en charge les applications de productivité mobiles Citrix Endpoint Management pour les appareils mobiles iOS et Android. NetScaler Gateway contient Secure Browse qui permet de se connecter à NetScaler Gateway à partir d'appareils mobiles iOS qui établissent le tunnel micro VPN. Les appareils Android qui se connectent au Secure Hub établissent également automatiquement un tunnel micro VPN qui fournit un accès sécurisé au niveau des applications Web et mobiles aux ressources de votre réseau interne. Si les utilisateurs se connectent depuis un appareil Android via des applications de productivité mobiles, vous devez configurer les paramètres DNS sur NetScaler Gateway. Pour plus d'informations, consultez Prise en charge des requêtes DNS à l'aide de suffixes DNS pour les appareils Android.

Comment les utilisateurs se connectent au client Citrix Secure Access

March 27, 2024

NetScaler Gateway fonctionne comme suit :

- Lorsque les utilisateurs tentent d'accéder aux ressources réseau via le tunnel VPN, le client Citrix Secure Access chiffre tout le trafic réseau destiné au réseau interne de l'organisation et transmet les paquets à NetScaler Gateway.
- NetScaler Gateway met fin au tunnel SSL, accepte tout trafic entrant destiné au réseau privé et transfère le trafic vers le réseau privé. NetScaler Gateway renvoie le trafic vers l'ordinateur distant via un tunnel sécurisé.

Lorsque les utilisateurs saisissent l'adresse Web, ils reçoivent une page d'ouverture de session dans laquelle ils entrent leurs informations d'identification et ouvrent une session. Si les informations d'identification sont correctes, NetScaler Gateway termine la liaison avec la machine utilisateur.

Si l'utilisateur se situe derrière un serveur proxy, il peut spécifier des informations d'identification pour le serveur proxy et l'authentification. Pour plus d'informations, consultez Activation de la prise en charge du proxy pour les connexions utilisateur.

Le client Citrix Secure Access est installé sur la machine utilisateur. Après la première connexion, si les utilisateurs ouvrent une session à l'aide d'un ordinateur Windows, ils peuvent utiliser l'icône de la zone de notification pour établir la connexion.

Établir le tunnel sécurisé

Lorsque les utilisateurs se connectent au client Citrix Secure Access, à Secure Hub ou à l'application Citrix Workspace, le logiciel client établit un tunnel sécurisé sur le port 443 (ou tout port configuré sur NetScaler Gateway) et envoie des informations d'authentification. Lorsque le tunnel est établi, NetScaler Gateway envoie des informations de configuration au client Citrix Secure Access, à Secure Hub ou à l'application Citrix Workspace décrivant les réseaux à sécuriser et contenant une adresse IP si vous activez les pools d'adresses.

Tunnel du trafic réseau privé sur des connexions sécurisées

Lorsque le client Citrix Secure Access démarre et que l'utilisateur est authentifié, tout le trafic réseau destiné à des réseaux privés spécifiés est capturé et redirigé via le tunnel sécurisé vers NetScaler Gateway. L'application Citrix Workspace doit prendre en charge le client Citrix Secure Access pour établir la connexion via le tunnel sécurisé lorsque les utilisateurs ouvrent une session.

Secure Hub, Secure Mail et WorxWeb utilisent Micro VPN pour établir le tunnel sécurisé pour les appareils mobiles iOS et Android.

NetScaler Gateway intercepte toutes les connexions réseau établies par la machine utilisateur et les multiplexe via SSL (Secure Sockets Layer) vers NetScaler Gateway, où le trafic est démultiplexé et les connexions sont transférées vers la combinaison hôte et port appropriée.

Les connexions sont soumises à des stratégies de sécurité administratives qui s'appliquent à une seule application, à un sous-ensemble d'applications ou à un intranet complet. Vous spécifiez les ressources (plages de paires d'adresses IP/sous-réseaux) auxquelles les utilisateurs distants peuvent accéder via la connexion VPN.

Le client Citrix Secure Access intercepte et tunnelise les protocoles suivants pour les applications intranet définies :

- TCP (tous les ports)
- UDP (tous les ports)
- ICMP (types 8 et 0 - demande/réponse d'écho)

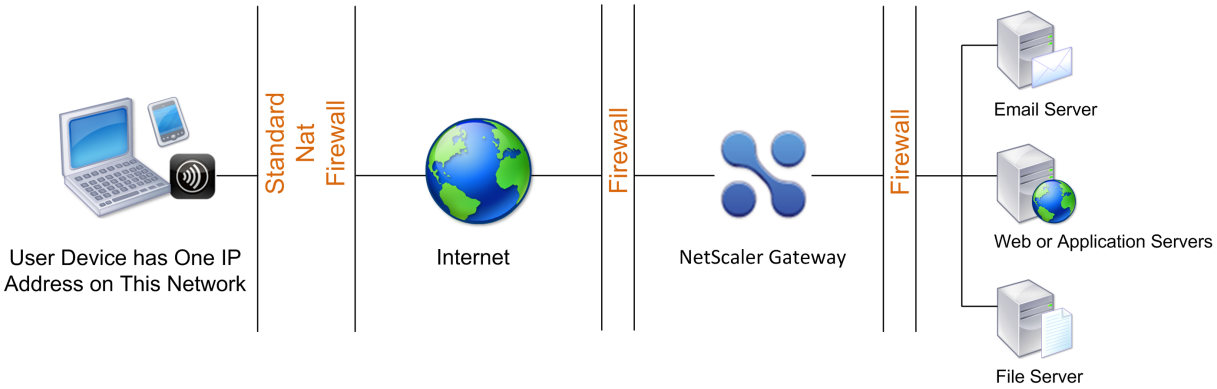
Les connexions provenant d'applications locales sur la machine utilisateur sont transférées de manière sécurisée vers NetScaler Gateway, qui rétablit les connexions avec le serveur cible. Les serveurs cibles considèrent les connexions comme provenant du NetScaler Gateway local sur le réseau privé, masquant ainsi la machine utilisateur. C'est ce qu'on appelle également la traduction d'adresses réseau inversée (NAT). Le masquage des adresses IP renforce la sécurité des emplacements sources.

Localement, sur la machine utilisateur, tout le trafic lié à la connexion, tel que les paquets SYN-ACK, PUSH, ACK et FIN, est recréé par le client Citrix Secure Access pour apparaître depuis le serveur

privé.

Connectez-vous via des pare-feu et des proxys

Les utilisateurs du client Citrix Secure Access se trouvent parfois à l'intérieur du pare-feu d'une autre organisation, comme le montre la figure suivante :



Les pare-feux NAT tiennent à jour une table qui leur permet d'acheminer des paquets sécurisés depuis NetScaler Gateway vers la machine utilisateur. Pour les connexions orientées circuit, NetScaler Gateway gère une table de traduction NAT inversée mappée aux ports. La table de traduction NAT inverse permet à NetScaler Gateway de faire correspondre les connexions et de renvoyer les paquets via le tunnel à la machine utilisateur avec les numéros de port corrects afin que les paquets soient renvoyés vers la bonne application.

Contrôlez la mise à niveau des clients Citrix Secure Access

Les administrateurs système contrôlent les performances du plug-in NetScaler lorsque sa version ne correspond pas à la révision de NetScaler Gateway. Les nouvelles options contrôlent le comportement de mise à niveau du plug-in pour Mac, Windows ou les systèmes d'exploitation.

Pour les plug-ins VPN, l'option de mise à niveau peut être définie à deux endroits dans l'interface utilisateur de l'appliance NetScaler :

- Dans les paramètres globaux
- Au niveau du profil de session

Exigences

- La version du plug-in Windows EPA et VPN doit être supérieure à 11.0.0.0
- La version du plug-in Mac EPA doit être supérieure à 3.0.0.31
- La version du plug-in VPN Mac doit être supérieure à 3.1.4 (357)

> **Remarque :**
>
> Si l'appliance NetScaler est mise à niveau vers la version 11.0, tous les plug-ins VPN (et EPA) précédents sont mis à niveau vers la dernière version, quelle que soit la configuration du contrôle de mise à niveau. Pour les mises à niveau suivantes, elles respectent la configuration précédente du contrôle de mise à niveau.

Comportements des plug-ins

Pour chaque type de client, NetScaler Gateway propose les trois options suivantes pour contrôler le comportement de mise à niveau des plug-ins :

- **Always**

Le plug-in est toujours mis à niveau chaque fois que la version du plug-in de l'utilisateur final ne correspond pas au plug-in fourni avec l'appliance NetScaler. Il s'agit du comportement par défaut. Sélectionnez cette option si vous ne souhaitez pas que plusieurs versions de plug-in soient exécutées dans votre entreprise.

- **Essentiel** (et sécurité)

Le plug-in n'a été mis à niveau que lorsque cela est jugé nécessaire. Les mises à niveau sont jugées nécessaires dans les deux cas suivants :

- Le plug-in installé n'est pas compatible avec la version actuelle de l'appliance NetScaler.
- Le plug-in installé doit être mis à jour pour obtenir le correctif de sécurité nécessaire.

Sélectionnez cette option si vous souhaitez réduire le nombre de mises à niveau de plug-in, mais ne souhaitez pas manquer de mises à jour de sécurité de plug-in

- **Jamais**

Le plug-in n'est pas mis à niveau.

Paramètres CLI pour contrôler la mise à niveau du plug-in VPN

NetScaler Gateway prend en charge deux types de plug-ins (EPA et VPN) pour les systèmes d'exploitation Windows et Mac. Pour permettre le contrôle de la mise à niveau des plug-ins VPN au niveau de la session, NetScaler Gateway prend en charge deux paramètres de profil de session nommés WindowsInPluginUpgrade et MacPluginUpgrade.

Ces paramètres sont disponibles au niveau global, au niveau du serveur virtuel, du groupe et de l'utilisateur. Chaque paramètre peut avoir la valeur Toujours, Essentiel ou Jamais. Pour obtenir une description de ces paramètres, reportez-vous à la section Comportements des plug-ins.

Paramètres CLI pour contrôler la mise à niveau du plug-in EPA

NetScaler Gateway prend en charge les plug-ins EPA pour les systèmes d'exploitation Windows et Mac. Pour prendre en charge le contrôle de la mise à niveau des plug-ins EPA au niveau du serveur virtuel, NetScaler Gateway prend en charge deux paramètres de serveur virtuel nommés WindowsePAPlugin-Upgrade et MacEPAPluginUpgrade.

Les paramètres sont disponibles au niveau du serveur virtuel. Chaque paramètre peut avoir la valeur Toujours, Essentiel ou Jamais. Pour obtenir une description de ces paramètres, voir Comportements des plug-ins.

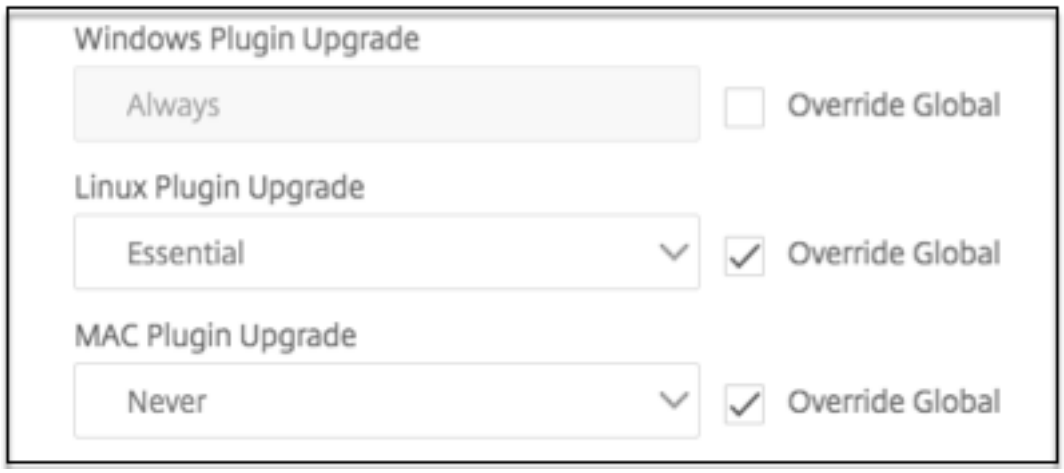
Configuration VPN

Suivez ces étapes pour **configurer le VPN des** plug-ins Windows, Linux et Mac.

1. Accédez à **NetScaler > Stratégies**Session.
2. Sélectionnez la stratégie de session souhaitée, puis cliquez sur **Modifier**.
3. Sélectionnez l'onglet **Expérience client**.
4. Ces options de boîte de dialogue affectent le comportement de mise à niveau.

   - Always
   - Essentiel
   - Jamais

   La valeur par défaut est Toujours.
5. Cochez la case située à droite de chaque option. Sélectionnez la fréquence à laquelle appliquer le comportement de mise à niveau.



Configuration EPA

Suivez ces étapes pour la configuration EPA des plug-ins Windows, Linux et Apple.

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez un serveur et cliquez sur le bouton **Modifier**.
3. Cliquez sur l'icône représentant **un crayon**.

4. Cliquez sur **Plus**
5. Les boîtes de dialogue qui s'affichent affectent le comportement de mise à niveau. Les options disponibles sont :
    - Always
    - Essentiel
    - Jamais

Configuration complète du VPN sur NetScaler Gateway

March 27, 2024

Cette section explique comment configurer la configuration complète du VPN sur une appliance NetScaler Gateway. Il contient des considérations de mise en réseau et l'approche idéale pour résoudre les problèmes du point de vue de la mise en réseau.

Pré-requis

- Installez un certificat SSL et liez-le au serveur virtuel VPN.

  - CTX109260 - Comment générer et installer un certificat SSL public sur un dispositif NetScaler
  - CTX122521 - Comment remplacer le certificat par défaut d'un dispositif NetScaler par un certificat d'autorité de certification approuvé qui correspond au nom d'hôte de l'appliance
  - Documentation NetScaler - Liaison de la paire de clés de certificat au serveur virtuel basé surSSL

- Créez un profil d'authentification pour NetScaler Gateway.
  - Pour plus d'informations, consultez la documentation NetScaler - Configuration de l'authentification utilisateur externe
  - Pour plus d'informations, reportez-vous à la section Liste de contrôle : Utiliser AD FS pour implémenter et gérer l'authentification unique
- Téléchargez le client VPN.
- Créez une stratégie de session autorisant les connexions VPN complètes.

Lorsque les utilisateurs se connectent au client Citrix Secure Access, à Secure Hub ou à l'application Citrix Workspace, le logiciel client établit un tunnel sécurisé sur le port 443 (ou tout port configuré sur NetScaler Gateway) et envoie des informations d'authentification. Une fois le tunnel établi, NetScaler Gateway envoie des informations de configuration au client Citrix Secure Access, à Citrix Secure Hub ou à l'application Citrix Workspace décrivant les réseaux à sécuriser. Ces informations contiennent également une adresse IP si vous activez les adresses IP intranet.

Vous configurez les connexions de machine utilisateur en définissant les ressources auxquelles les utilisateurs peuvent accéder sur le réseau interne. La configuration des connexions de machine utilisateur comprend les éléments suivants :

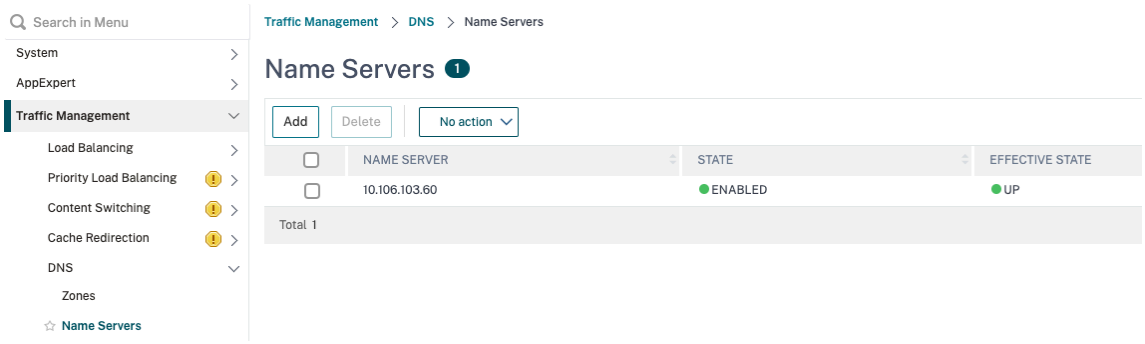
- Split tunneling
- Adresses IP des utilisateurs, y compris les pools d'adresses (IP intranet)
- Connexions via un serveur proxy
- Définition des domaines auxquels les utilisateurs sont autorisés à accéder
- Paramètres de délai d'expiration
- Single Sign-On
- Logiciel utilisateur qui se connecte via NetScaler Gateway
- Accès pour appareils mobiles

Vous configurez la plupart des connexions utilisateur et machine à l'aide d'un profil qui fait partie d'une stratégie de session. Vous pouvez également définir les paramètres de connexion de l'appareil utilisateur en utilisant des stratégies d'authentification, de trafic et d'autorisation par authentification. Ils peuvent également être configurés à l'aide d'applications intranet.

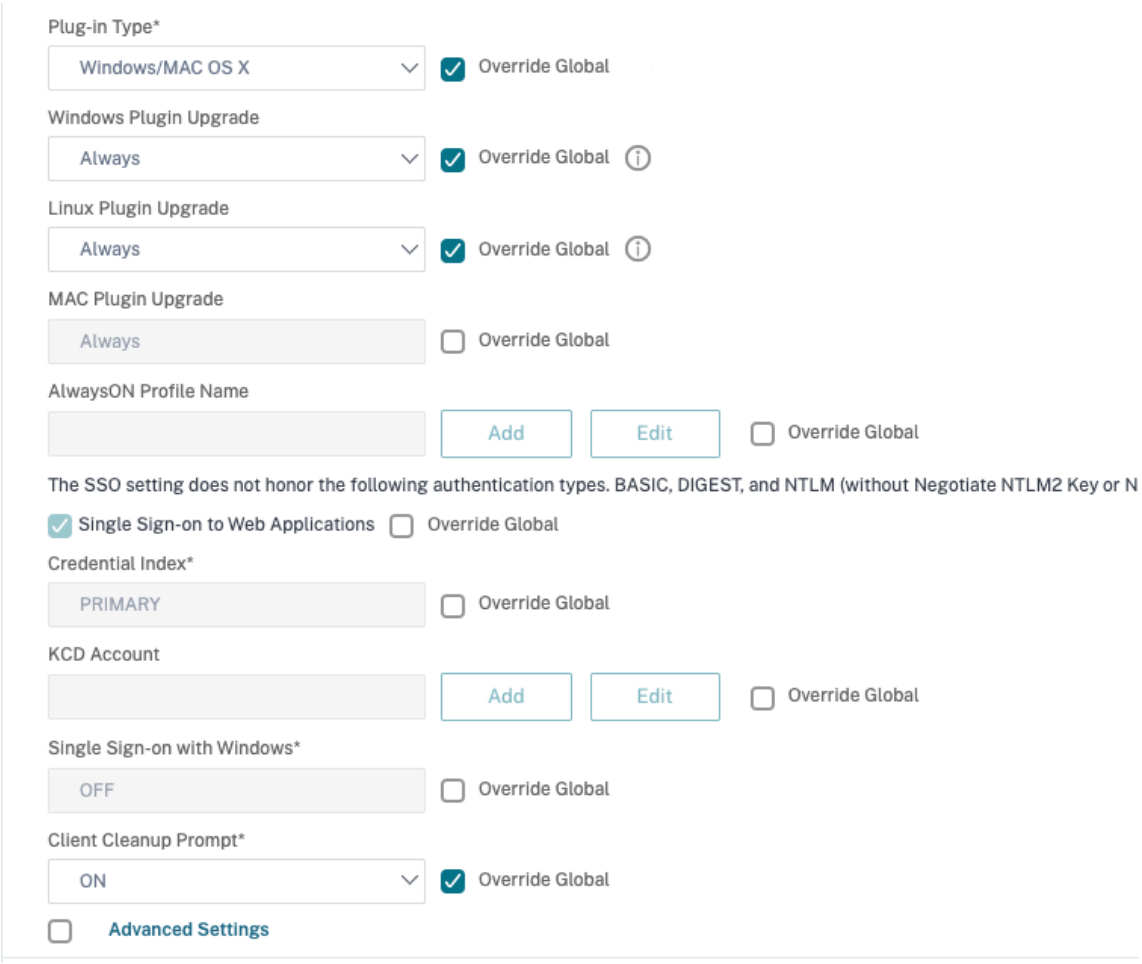
Configurer une configuration VPN complète sur une appliance NetScaler Gateway

Pour configurer une configuration VPN sur l'appliance NetScaler Gateway, procédez comme suit :

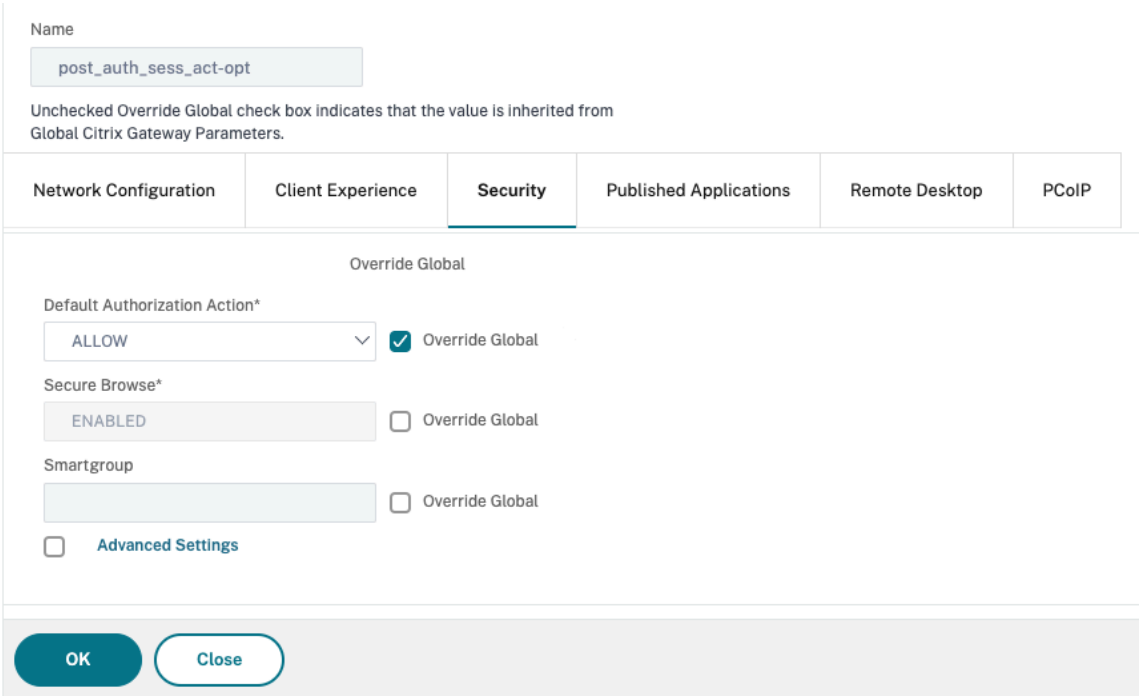
1. Accédez à **Gestion du trafic > DNS**.
2. Sélectionnez le nœud Serveurs de noms, comme illustré dans la capture d'écran suivante. Assurez-vous que le serveur de noms DNS est répertorié. S'il n'est pas disponible, ajoutez un serveur de noms DNS.



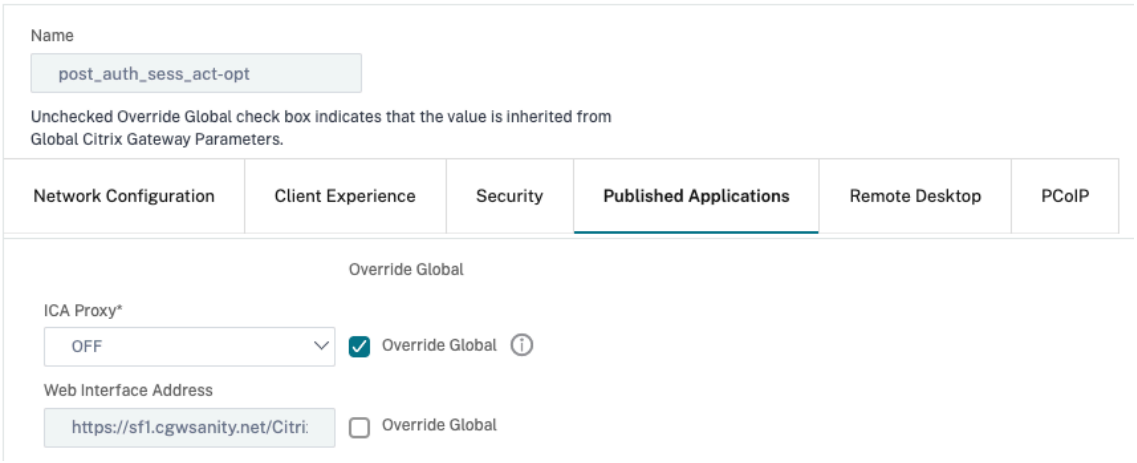
3. Développez **NetScaler Gateway > Stratégies**.
4. Sélectionnez le nœud **Session**.
5. Sur la page Stratégies et profils de session NetScaler Gateway, cliquez sur l'onglet **Profils**, puis sur **Ajouter**.
   Pour chaque composant que vous configurez dans la boîte de dialogue Configurer le profil de session NetScaler Gateway, assurez-vous de sélectionner l'option **Override Global** pour le composant correspondant.
6. Cliquez sur l'onglet **Expérience client** .
7. Tapez l'URL du portail intranet dans le champ Page d'accueil si vous souhaitez présenter une URL lorsque l'utilisateur se connecte au VPN. Si le paramètre de la page d'accueil est défini sur « nohomepage.html », la page d'accueil n'est pas affichée. Lorsque le plug-in démarre, une instance de navigateur démarre et est automatiquement supprimée.
8. Assurez-vous de sélectionner le paramètre souhaité dans la liste Split Tunnel.
9. Sélectionnez **DÉSACTIVÉ** dans la liste **Accès sans client** si vous souhaitez utiliser FullVPN.
10. Assurez-vous que **Windows/Mac OS X** est sélectionné dans la liste **Type de plug-in**.
11. Sélectionnez l'option **Single Sign-On to Web Applications** si vous le souhaitez.
12. Assurez-vous que l'option **Invite de nettoyage du client** est sélectionnée si nécessaire, comme illustré dans la capture d'écran suivante :



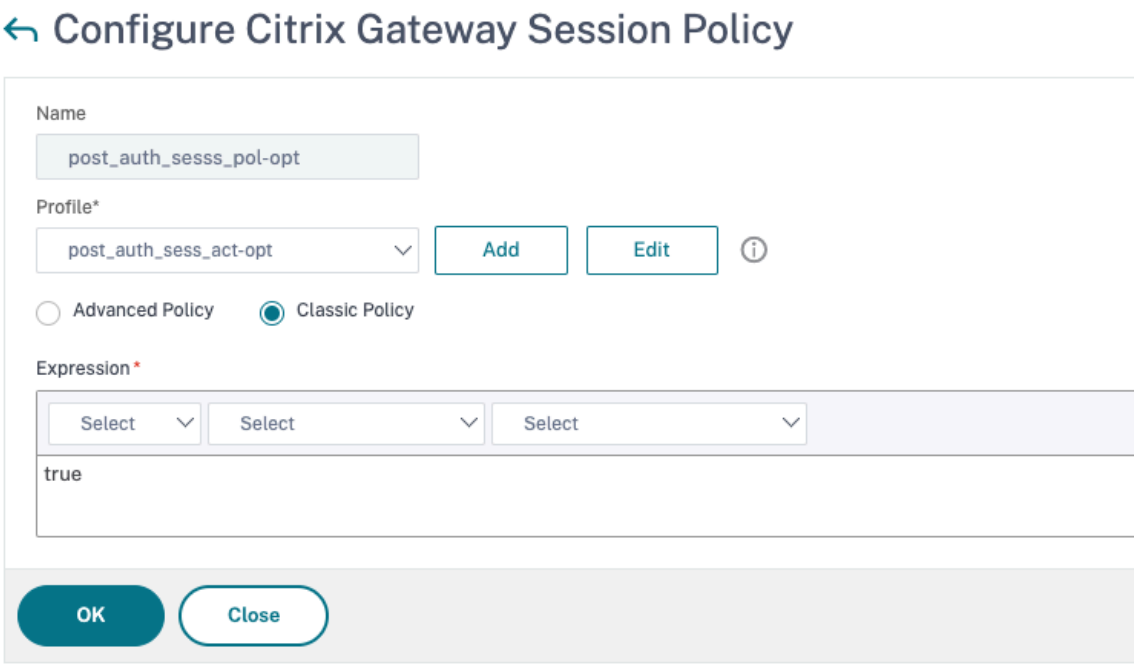
13. Cliquez sur l'onglet **Sécurité**.
14. Assurez-vous que l'option **AUTORISER** est sélectionnée dans la liste des **actions d'autorisation par défaut**.



15. Cliquez sur l'onglet **Published Applications**.
16. Assurez-vous que **OFF** est sélectionné dans la liste **Proxy ICA** sous l'option **Applications publiées**.



17. Cliquez sur **Créer**.
18. Cliquez sur **Fermer**.
19. Cliquez sur l'onglet **Policies** de la page NetScaler Gateway Session Policies and Profiles sur le serveur virtuel ou activez les stratégies de session au niveau GROUPE/UTILISATEUR selon les besoins.
20. Créez une stratégie de session avec une expression requise ou true, comme illustré dans la capture d'écran suivante :

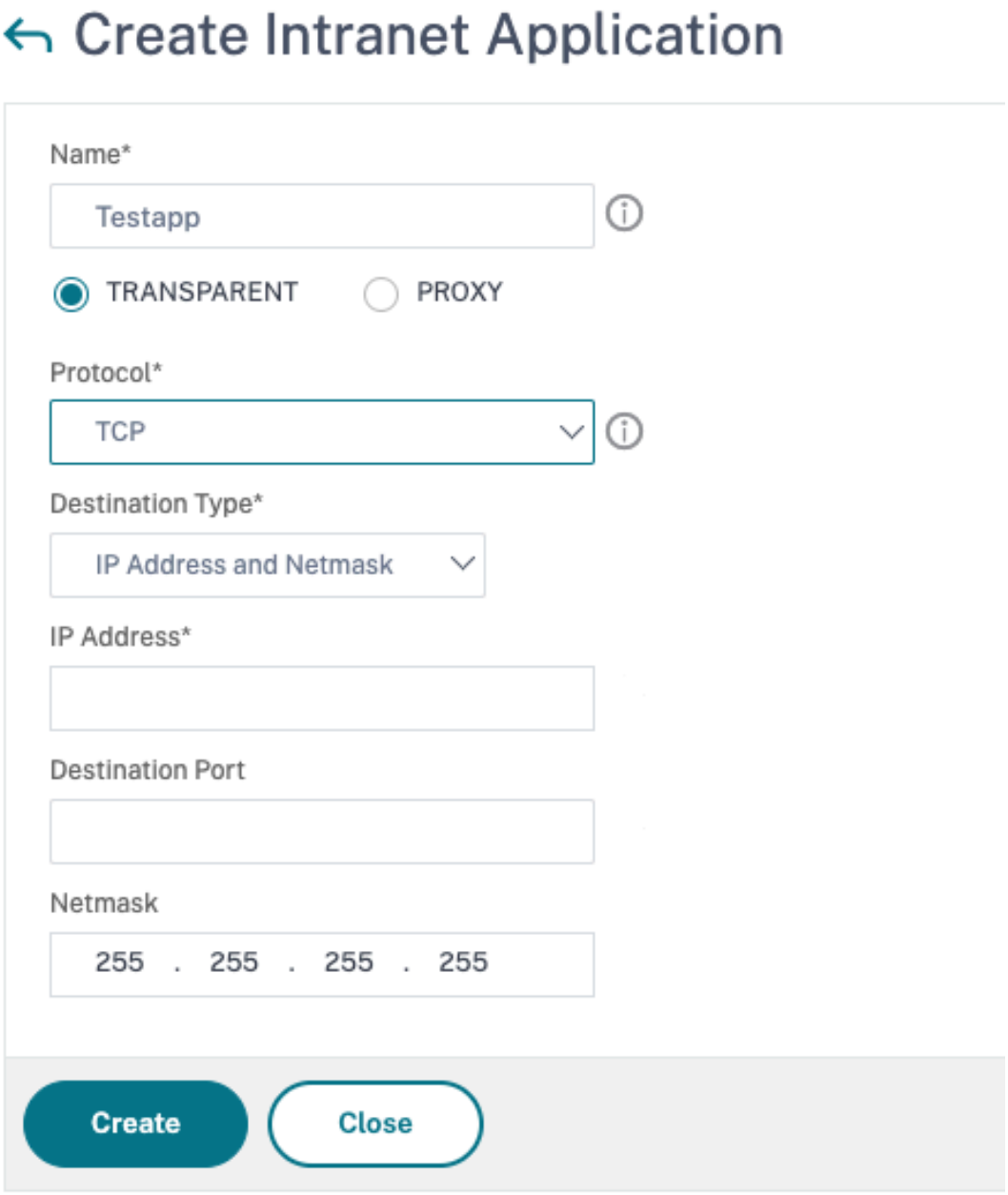


21. Liez la stratégie de session au serveur virtuel VPN. Pour plus de détails, consultez la section Politiques de session Bind.

    Si Split Tunnel a été configuré sur ON, vous devez configurer les applications intranet auxquelles vous souhaitez que les utilisateurs accèdent lorsqu'ils sont connectés au VPN. Pour plus d'informations sur les applications intranet, voir Configuration des applications intranet pour le client Citrix Secure Access.

    a) Accédez à **NetScaler Gateway > Ressources > Applications intranet**.

    b) Créez une application Intranet. Sélectionnez Transparent pour FullVPN avec client Windows. Sélectionnez le protocole que vous souhaitez autoriser (TCP, UDP ou ANY), le type de destination (adresse IP et masque, plage d'adresses IP ou nom d'hôte).



c) Si nécessaire, définissez une nouvelle politique pour le VPN sur iOS et Android à l'aide de l'expression suivante :

```
HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixVPN")&&HTTP.
REQ.HEADER("User-Agent").CONTAINS("NSGiOSplugin")&&HTTP.REQ.
HEADER("User-Agent").CONTAINS("Android")
```

d) Liez les applications intranet créées au niveau USER/GROUPE/VSERVER selon les besoins.

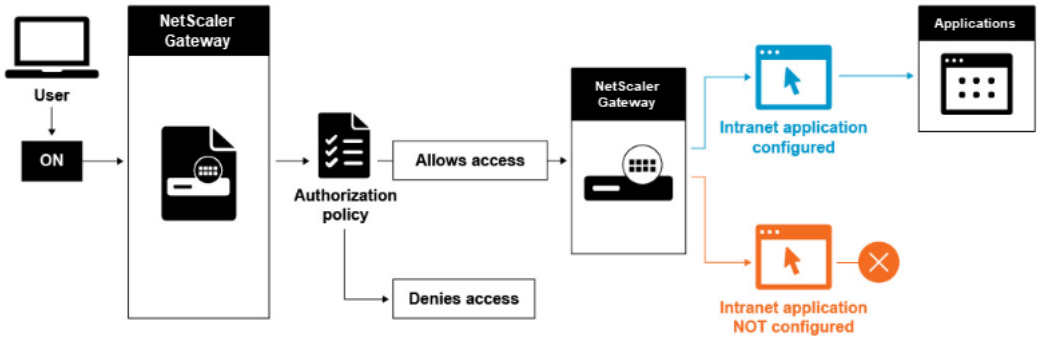
Configurer le split tunneling

1. Accédez à **Configuration** > **NetScaler Gateway > Politiques Session**.
2. Dans le volet d'informations, sous l'onglet Profils, sélectionnez un profil, puis cliquez sur **Modifier**.
3. Dans l'onglet **Expérience client**, en regard de **Split Tunnel**, sélectionnez **Global Override**, sélectionnez une option, puis cliquez sur **OK**.

   Configuration du split tunneling et de l'autorisation

   Lors de la planification de votre déploiement de NetScaler Gateway, il est important de prendre en compte le split tunneling ainsi que l'action d'autorisation par défaut et les stratégies d'autorisation.

   Par exemple, vous disposez d'une stratégie d'autorisation qui autorise l'accès à une ressource réseau. Le split tunneling est activé et vous ne configurez pas les applications intranet pour envoyer du trafic réseau via NetScaler Gateway. Lorsque NetScaler Gateway dispose de ce type de configuration, l'accès à la ressource est autorisé, mais les utilisateurs ne peuvent pas y accéder.



Si la stratégie d'autorisation refuse l'accès à une ressource réseau, le client Citrix Secure Access envoie du trafic à NetScaler Gateway, mais l'accès à la ressource est refusé dans les conditions suivantes.

- Vous avez défini le split tunneling sur ON.
- Les applications intranet sont configurées pour acheminer le trafic réseau via NetScaler Gateway

Pour plus d'informations sur les stratégies d'autorisation, consultez les points suivants :

- Configuration de l'autorisation
- Configuration des stratégies d'autorisation
- Définition de l'autorisation globale par défaut

Pour configurer l'accès réseau aux ressources réseau internes

1. Accédez à **Configuration** > **NetScaler Gateway > Ressources > Applications intranet**.

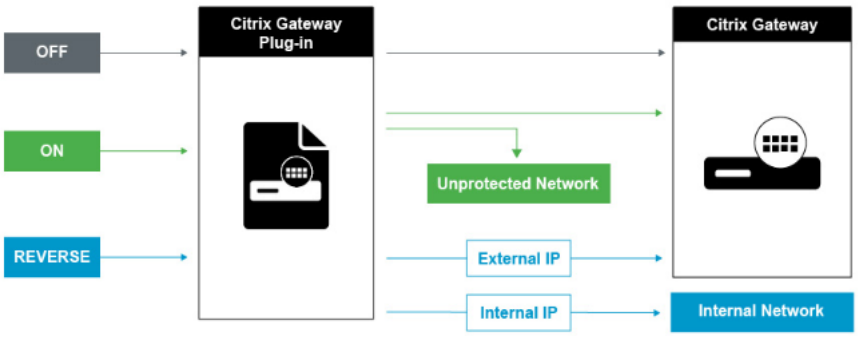
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Renseignez les paramètres d'autorisation d'accès au réseau, cliquez sur **Créer**, puis sur **Fermer**.

Lorsque nous ne configurons pas les adresses IP intranet pour les utilisateurs du VPN, l'utilisateur envoie le trafic au NetScaler Gateway VIP, puis à partir de là, l'appliance NetScaler crée un nouveau paquet vers la ressource de l'application intranet sur le réseau local interne. Ce nouveau paquet provient du SNIP vers l'application intranet. À partir de là, l'application intranet récupère le paquet, le traite, puis tente de répondre à la source de ce paquet (le SNIP dans ce cas). Le SNIP récupère le paquet et envoie la réponse au client qui a effectué la demande.

Lorsqu'une adresse IP intranet est utilisée, l'utilisateur envoie le trafic au NetScaler Gateway VIP, puis l'appliance NetScaler mappe l'adresse IP du client sur l'une des adresses IP INTRANET configurées à partir du pool. Sachez que l'appliance NetScaler sera propriétaire du pool d'adresses IP de l'intranet et que, pour cette raison, ces plages ne doivent pas être utilisées sur le réseau interne. L'appliance NetScaler attribue une adresse IP intranet aux connexions VPN entrantes comme le ferait un serveur DHCP. L'appliance NetScaler crée un nouveau paquet pour l'application intranet sur le réseau local auquel l'utilisateur aurait accès. Ce nouveau paquet provient de l'une des adresses IP intranet vers l'application intranet. À partir de là, les applications intranet obtiennent le paquet, le traitent, puis tentent de répondre à la source de ce paquet (l'adresse IP INTRANET). Dans ce cas, le paquet de réponse doit être redirigé vers l'appliance NetScaler, où se trouvent les adresses IP INTRANET (n'oubliez pas que l'appliance NetScaler possède les sous-réseaux IP de l'intranet). Pour accomplir cette tâche, l'administrateur réseau doit disposer d'une route vers l'adresse IP INTRANET, pointant vers l'un des SNIP. Il est recommandé de rediriger le trafic vers le SNIP qui contient l'itinéraire à partir duquel le paquet quitte l'appliance NetScaler pour la première fois afin d'éviter tout trafic asymétrique.

Options de split tunneling

Voici les différentes options de split tunneling.



Tunnel divisé OFF

Lorsque le split tunnel est désactivé, le client Citrix Secure Access capture tout le trafic réseau provenant d'une machine utilisateur et envoie le trafic via le tunnel VPN à NetScaler Gateway. En d'autres termes, le client VPN établit un itinéraire par défaut à partir du PC client pointant vers le NetScaler Gateway VIP, ce qui signifie que tout le trafic doit être envoyé via le tunnel pour atteindre la destination. Étant donné que tout le trafic va être envoyé via le tunnel, les stratégies d'autorisation doivent déterminer si le trafic est autorisé à passer aux ressources réseau internes ou s'il est refusé.

Lorsqu'il est défini sur « Désactivé », tout le trafic passe par le tunnel, y compris le trafic Web standard vers les sites Web. Si l'objectif est de surveiller et de contrôler ce trafic Web, vous devez transmettre ces demandes à un proxy externe à l'aide de l'appliance NetScaler. Les machines utilisateur peuvent également se connecter via un serveur proxy pour accéder aux réseaux internes.
NetScaler Gateway prend en charge les protocoles HTTP, SSL, FTP et SOCKS. Pour activer la prise en charge du proxy pour les connexions utilisateur, vous devez spécifier ces paramètres sur NetScaler Gateway. Vous pouvez spécifier l'adresse IP et le port utilisés par le serveur proxy sur NetScaler Gateway. Le serveur proxy est utilisé comme proxy de transfert pour toutes les connexions ultérieures au réseau interne.

Pour plus d'informations, consultez les liens suivants :

- Activation de la prise en charge des serveurs proxy pour

Tunnel Split ON

Vous pouvez activer le split tunneling pour empêcher le client Citrix Secure Access d'envoyer du trafic réseau inutile à NetScaler Gateway. Si le split tunnel est activé, le client Citrix Secure Access envoie uniquement le trafic destiné aux réseaux protégés (applications intranet) par NetScaler Gateway via le tunnel VPN. Le client Citrix Secure Access n'envoie pas le trafic réseau destiné aux réseaux non protégés à NetScaler Gateway. Lorsque le client Citrix Secure Access démarre, il obtient la liste des applications intranet auprès de NetScaler Gateway et établit un itinéraire pour chaque sous-réseau défini dans l'onglet de l'application intranet du PC client. Le client Citrix Secure Access examine tous les paquets transmis depuis la machine utilisateur et compare les adresses contenues dans les paquets à la liste des applications intranet (table de routage créée lors du démarrage de la connexion VPN). Si l'adresse de destination du paquet se trouve dans l'une des applications intranet, le client Citrix Secure Access envoie le paquet via le tunnel VPN à NetScaler Gateway. Si l'adresse de destination ne se trouve pas dans une application intranet définie, le paquet n'est pas chiffré et la machine utilisateur achemine ensuite le paquet de manière appropriée en utilisant le routage par défaut initialement défini sur le PC client. « Lorsque vous activez le split tunneling, les applications intranet définissent le trafic réseau qui est intercepté et envoyé via le tunnel ».

Tunnel divisé inversé

NetScaler Gateway prend également en charge le tunneling fractionné inversé, qui définit le trafic réseau que NetScaler Gateway n'intercepte pas. Si vous configurez le split tunneling sur l'inverse, les applications intranet définissent le trafic réseau que NetScaler Gateway n'intercepte pas. Lorsque vous activez le split tunneling inversé, tout le trafic réseau dirigé vers des adresses IP internes contourne le tunnel VPN, tandis que le reste du trafic passe par NetScaler Gateway. Le split tunneling inverse peut être utilisé pour enregistrer tout le trafic LAN non local. Par exemple, si les utilisateurs disposent d'un réseau domestique sans fil et sont connectés via le client Citrix Secure Access, NetScaler Gateway n'intercepte pas le trafic réseau destiné à une imprimante ou à un autre appareil du réseau sans fil.

> **Remarque :**
>
> Le client Citrix Secure Access pour Windows prend également en charge le tunnel de fractionnement inversé basé sur un FQDN à partir de Citrix Secure Access version 22.6.1.5 et versions ultérieures.

Points à noter Tunneling inversé basé sur IP :

- Le nombre de règles basées sur les adresses IP est limité à 1024.
- Pris en charge avec les pilotes DNE et WFP.

Tunneling inversé basé sur le nom d'hôte :

- Le nombre de noms d'hôtes accessibles au cours d'une session VPN est limité par le nombre d'adresses IP utilisables spécifiées dans la plage d'usurpation du nom de domaine complet (FQDN spoofing). En effet, chaque nom d'hôte utilise une adresse IP de la plage d'usurpation du FQDN. Une fois la plage d'adresses IP épuisée, la dernière adresse IP attribuée est réutilisée pour le nouveau nom d'hôte suivant.
- Les suffixes DNS doivent être configurés.

  > **Remarque :**
  >
  > Pour les clients Windows, le split tunneling inversé basé sur le nom d'hôte n'est pris en charge qu'avec le pilote WFP. Activez le mode pilote WFP en définissant la valeur de registre « EnableWFP » sur 1. Pour plus d'informations, consultez la section Client Windows Citrix Secure Access à l'aide de Windows Filtering Platform.

Tunneling inversé basé sur l'adresse IP et le nom d'hôte :

- Pris en charge uniquement avec le pilote WFP. Toutes les autres directives mentionnées dans le split-tunneling inversé basé sur IP et le split-tunneling inversé basé sur le nom d'hôte sont applicables.

Configuration de la résolution du service de noms

Lors de l'installation de NetScaler Gateway, vous pouvez utiliser l'assistant NetScaler Gateway pour configurer d'autres paramètres, notamment les fournisseurs de services de noms. Les fournisseurs de services de noms traduisent le nom de domaine complet (FQDN) en adresse IP. Dans l'assistant NetScaler Gateway, vous pouvez également effectuer les opérations suivantes :

- Configuration d'un serveur DNS ou WINS
- Définir la priorité de la recherche DNS
- Définissez le nombre de tentations de connexion au serveur.

Lorsque vous exécutez l'assistant NetScaler Gateway, vous pouvez alors ajouter un serveur DNS. Vous pouvez ajouter d'autres serveurs DNS et un serveur WINS à NetScaler Gateway à l'aide d'un profil de session. Vous pouvez ensuite diriger les utilisateurs et les groupes pour qu'ils se connectent à un serveur de résolution de noms différent de celui que vous avez initialement utilisé pour configurer l'assistant.

Avant de configurer un autre serveur DNS sur NetScaler Gateway, créez un serveur virtuel qui fait office de serveur DNS pour la résolution des noms.

Pour ajouter un serveur DNS ou WINS dans un profil de session

1. Dans l'utilitaire de configuration, onglet Configuration > **NetScaler Gateway > Policies Session**.
2. Dans le volet d'informations, sous l'onglet Profils, sélectionnez un profil, puis cliquez sur Ouvrir.
3. Dans l'onglet Configuration réseau, effectuez l'une des opérations suivantes :
    - Pour configurer un serveur DNS, à côté de **Serveur virtuel DNS**, cliquez sur **Override Global**, sélectionnez le serveur, puis cliquez sur **OK.**
    - Pour configurer un serveur WINS, à côté de l'**adresse IP du serveur WINS**, cliquez sur **Override Global**, tapez l'adresse IP, puis cliquez sur **OK.**

Références

- Split tunneling
- Comment les utilisateurs se connectent au client Citrix Secure Access
- À propos de NetScaler Gateway
- Sélectionner la méthode d'accès utilisateur

Sélectionner la méthode d'accès utilisateur

January 26, 2024

Vous pouvez configurer NetScaler Gateway pour fournir des connexions utilisateur via les scénarios suivants :

- Connexions utilisateur à l'aide de l'application Citrix Workspace. L'application Citrix Workspace est compatible avec StoreFront ou l'interface Web pour fournir aux utilisateurs un accès aux applications publiées ou aux bureaux virtuels d'une batterie de serveurs. L'application Citrix Workspace est un logiciel qui utilise le protocole réseau ICA pour établir des connexions utilisateur. Les utilisateurs installent l'application Citrix Workspace sur la machine utilisateur. Lorsque les utilisateurs installent l'application Citrix Workspace sur leur ordinateur Windows ou Mac, l'application Citrix Workspace intègre tous les plug-ins, y compris le client Citrix Secure Access pour les connexions utilisateur. NetScaler Gateway prend également en charge les connexions depuis les applications Citrix Workspace pour Android et Citrix Workspace pour iOS. Les utilisateurs peuvent se connecter à leurs bureaux virtuels et à leurs applications Windows, Web, mobiles et SaaS via Citrix Endpoint Management, StoreFront ou l'interface Web.
- Connexions utilisateur avec Secure Hub. Les utilisateurs peuvent se connecter aux applications mobiles, Web et SaaS configurées dans Endpoint Management. Les utilisateurs installent Secure Hub sur leur appareil mobile (Android ou iOS). Lorsque les utilisateurs ouvrent une session sur Secure Hub, ils peuvent installer WorxMail et WorxWeb, ainsi que toute autre application mobile installée dans Endpoint Management. Secure Hub, Secure Mail et WorxWeb utilisent la technologie Micro VPN pour établir des connexions via NetScaler Gateway.
- Connexions utilisateur à l'aide du client Citrix Secure Access en tant qu'application autonome. Le client Citrix Secure Access est un logiciel que les utilisateurs peuvent télécharger et installer sur une machine utilisateur. Lorsque les utilisateurs ouvrent une session avec le plug-in, ils peuvent accéder aux ressources du réseau sécurisé comme s'ils se trouvaient au bureau. Les ressources incluent les serveurs de messagerie, les partages de fichiers et les sites Web intranet.
- Connexions utilisateur à l'aide d'un accès sans client. L'accès sans client fournit aux utilisateurs l'accès dont ils ont besoin sans avoir à installer de logiciel, tel que le client Citrix Secure Access ou l'application Citrix Workspace, sur la machine utilisateur. L'accès sans client permet de se connecter à un ensemble limité de ressources Web, telles qu'Outlook Web Access ou SharePoint, aux applications publiées sur Citrix Virtual Apps, aux bureaux virtuels de Citrix Virtual Apps and Desktops et aux partages de fichiers dans le réseau sécurisé via l'interface d'accès. Les utilisateurs se connectent en saisissant l'adresse Web de NetScaler Gateway dans un navigateur Web, puis en sélectionnant l'accès sans client sur la page de choix.
- Connexions utilisateur en cas d'échec d'une analyse de pré-authentification ou de post-

authentification. Ce scénario s'appelle le scénario de secours du scénario d'accès. Le scénario de secours d'accès permet à une machine utilisateur de revenir du client Citrix Secure Access à StoreFront ou à l'interface Web, à l'aide de l'application Citrix Workspace, si la machine utilisateur ne passe pas avec succès l'analyse initiale des terminaux.

Si les utilisateurs se connectent à NetScaler Gateway via l'application Citrix Workspace, le scan de pré-authentification ne fonctionne pas. Les scans post-authentification fonctionnent lorsque NetScaler Gateway établit le tunnel VPN.

Les utilisateurs peuvent télécharger et installer le client Citrix Secure Access en utilisant les méthodes suivantes :

- Connexion à NetScaler Gateway à l'aide d'un navigateur Web.
- Connexion à StoreFront configuré pour accepter les connexions NetScaler Gateway.
- Installation du plug-in à l'aide d'un objet de stratégie de groupe (GPO).
- Chargement du plug-in NetScaler sur le Merchandising Server.

Déployer le client Citrix Secure Access pour l'accès des utilisateurs

March 27, 2024

NetScaler Gateway est fourni avec les plug-ins suivants pour l'accès des utilisateurs :

- Client Citrix Secure Access pour Windows
- Client Citrix Secure Access pour Mac

Lorsque les utilisateurs se connectent à NetScaler Gateway pour la première fois, ils téléchargent et installent le client Citrix Secure Access à partir d'une page Web. Les utilisateurs ouvrent une session en cliquant sur l'icône NetScaler Gateway dans la zone de notification d'un ordinateur Windows. Sur un ordinateur macOS X, les utilisateurs peuvent ouvrir une session à partir du **Dock ou du menu Applications**. Si vous effectuez la mise à niveau de NetScaler Gateway vers une nouvelle version logicielle, le client Citrix Secure Access est automatiquement mis à jour sur la machine utilisateur.

Déployez le client Citrix Secure Access à l'aide du package d'installation MSI

Vous pouvez déployer le client Citrix Secure Access à l'aide d'une infrastructure Microsoft Active Directory ou d'un outil de déploiement MSI tiers standard, tel que Windows Server Update Services. Si vous utilisez un outil qui prend en charge les packages Windows Installer, vous pouvez les déployer avec n'importe quel outil prenant en charge les fichiers MSI. Ensuite, vous utilisez votre outil de déploiement pour déployer et installer le logiciel sur les machines utilisateur appropriées.

Avantages de l'utilisation d'un outil de déploiement centralisé

- Possibilité de respecter les consignes de sécurité. Par exemple, vous pouvez installer un logiciel utilisateur sans activer les privilèges d'installation de logiciels pour les utilisateurs non administratifs.
- Contrôle des versions logicielles. Vous pouvez déployer une version mise à jour du logiciel pour tous les utilisateurs simultanément.
- Évolutivité. Une stratégie de déploiement centralisée évolue facilement pour prendre en charge un plus grand nombre d'utilisateurs.
- Aucun impact sur les utilisateurs. Vous pouvez déployer, tester et résoudre les problèmes liés à l'installation sans impliquer les utilisateurs dans ce processus.

Citrix recommande cette option lorsque le contrôle administratif de l'installation du logiciel utilisateur est préféré et que l'accès aux machines utilisateur est facilement disponible.

Pour plus d'informations, consultez la section Déploiement du client Citrix Secure Access depuis Active Directory.

Déterminez le plug-in logiciel à déployer

Si votre déploiement NetScaler Gateway ne nécessite aucun plug-in logiciel sur les machines des utilisateurs, votre déploiement est considéré comme fournissant un accès sans client. Dans ce scénario, les utilisateurs n'ont besoin que d'un navigateur Web pour accéder aux ressources réseau. Toutefois, certaines fonctionnalités nécessitent le plug-in sur l'appareil de l'utilisateur.

Sélectionner le client Citrix Secure Access pour les utilisateurs

March 27, 2024

Lorsque vous configurez NetScaler Gateway, vous pouvez choisir la manière dont les utilisateurs se connectent. Les utilisateurs peuvent ouvrir une session à l'aide de l'un des plug-ins suivants :

- Client Citrix Secure Access pour Windows
- Client Citrix Secure Access pour macOS

Vous terminez la configuration en créant une stratégie de session, puis en la liant aux utilisateurs, groupes ou serveurs virtuels. Vous pouvez également activer les plug-ins en configurant les paramètres globaux. Dans le profil global ou de session, vous sélectionnez Windows ou macOS X comme type de module externe. Lorsque les utilisateurs ouvrent une session, ils reçoivent le plug-in tel que défini globalement ou dans le profil de session et la stratégie. Créez des profils distincts pour le type de plug-in.

Configurez le plug-in globalement

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Expérience client, en regard de Type de plug-in, sélectionnez Windows/macOS X, puis cliquez sur OK.

Configurer le type de plug-in pour Windows ou macOS dans un profil de session

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Procédez comme suit :
    - Si vous créez une stratégie de session, dans le volet d'informations, cliquez sur **Ajouter**.
    - Si vous modifiez une stratégie existante, sélectionnez-en une, puis cliquez sur **Ouvrir**.
3. Créez un profil ou modifiez un profil existant. Pour ce faire, effectuez l'une des opérations suivantes :
    - À côté de **Demander un profil**, cliquez sur **Nouveau**.
    - À côté de **Demander un profil**, cliquez sur **Modifier**.
4. Dans l'onglet **Expérience client**, en regard de **Type de plug-in**, cliquez sur **Override Global**, puis sélectionnez **Windows/macOS X.**
5. Procédez comme suit :
    - Si vous créez un profil, cliquez sur **Créer**, définissez l'expression dans la boîte de dialogue de stratégie, cliquez sur **Créer,** puis sur **Fermer**.
    - Si vous modifiez un profil existant, après avoir effectué la sélection, cliquez deux fois sur OK .

Client Citrix Secure Access pour Windows

Lorsque les utilisateurs se connectent à NetScaler Gateway, ils téléchargent et installent le client Citrix Secure Access sur la machine utilisateur.

Pour installer le plug-in, les utilisateurs doivent être un administrateur local ou un membre du groupe Administrateurs. Cette restriction s'applique uniquement à la première installation. Les mises à niveau de plug-in ne nécessitent pas d'accès de niveau administrateur.

Pour permettre aux utilisateurs de se connecter à NetScaler Gateway et de l'utiliser, vous devez leur fournir les informations suivantes :

- Adresse Web NetScaler Gateway, telle que https://NetScalerGatewayFQDN/
- Toute configuration système requise pour exécuter le client Citrix Secure Access si vous avez configuré des ressources et des stratégies de point de terminaison

Selon la configuration de la machine utilisateur, vous devrez peut-être également fournir les informations suivantes :

- Si les utilisateurs exécutent un pare-feu sur leur ordinateur, ils doivent modifier les paramètres du pare-feu afin que celui-ci ne bloque pas le trafic à destination ou en provenance des adresses IP correspondant aux ressources auxquelles vous avez accordé l'accès. Le client Citrix Secure Access gère automatiquement le pare-feu de connexion Internet dans Windows XP et le pare-feu Windows dans Windows XP Service Pack 2, Windows Vista, Windows 7, Windows 8 ou Windows 8.1.
- Les utilisateurs qui souhaitent envoyer du trafic vers FTP via une connexion NetScaler Gateway doivent configurer leur application FTP pour effectuer des transferts passifs. Un transfert passif signifie que l'ordinateur distant établit la connexion de données à votre serveur FTP, plutôt que l'établissement de la connexion de données par le serveur FTP à l'ordinateur distant.
- Les utilisateurs qui souhaitent exécuter des applications clientes X sur la connexion doivent exécuter un serveur X, par exemple,`XManager` sur leurs ordinateurs.
- Les utilisateurs qui installent Receiver pour Windows ou Receiver pour Mac peuvent démarrer le client Citrix Secure Access depuis Receiver ou à l'aide d'un navigateur Web. Fournissez des instructions aux utilisateurs sur la façon de se connecter avec le client Citrix Secure Access via Receiver ou un navigateur Web.

Étant donné que les utilisateurs travaillent sur des fichiers et des applications comme s'ils étaient locaux sur le réseau de l'organisation, il n'est pas nécessaire de recycler les utilisateurs ou de configurer des applications.

Pour établir une connexion sécurisée pour la première fois, connectez-vous à NetScaler Gateway à l'aide de la page de connexion Web. Le format typique d'une adresse Web est https://companyname.com. Lorsque les utilisateurs ouvrent une session, ils peuvent télécharger et installer le client Citrix Secure Access sur leur ordinateur.

Installation du client Citrix Secure Access pour Windows

1. Dans un navigateur Web, saisissez l'adresse Web de NetScaler Gateway.
2. Tapez le nom d'utilisateur et le mot de passe, puis cliquez sur Ouverture de session.
3. Sélectionnez Accès réseau, puis cliquez sur Télécharger.
4. Suivez les instructions pour installer le plug-in.

Une fois le téléchargement terminé, le client Citrix Secure Access se connecte et affiche un message dans la zone de notification d'un ordinateur Windows.

Si vous souhaitez que les utilisateurs se connectent au client Citrix Secure Access sans utiliser de navigateur Web, vous pouvez configurer le plug-in pour qu'il affiche la boîte de dialogue d'ouverture de session lorsque les utilisateurs cliquent avec le bouton droit sur l'icône **NetScaler Gateway** dans la zone de notification d'un ordinateur Windows ou démarrent le plug-in depuis le menu Démarrer.

Configurer la boîte de dialogue d'ouverture de session pour le client Citrix Secure Access pour Windows

Pour configurer le client Citrix Secure Access afin qu'il utilise la boîte de dialogue d'ouverture de session, les utilisateurs doivent être connectés pour terminer cette procédure.

1. Sur un ordinateur Windows, dans la zone de notification, cliquez avec le bouton droit sur l'icône NetScaler Gateway, puis cliquez sur Configurer NetScaler Gateway.
2. Cliquez sur l'onglet Profil, puis sur Modifier le profil.
3. Dans l'onglet Options, cliquez sur Utiliser le client Citrix Secure Access pour l'ouverture de session.
   Remarque : Si les utilisateurs ouvrent la boîte de dialogue Configurer NetScaler Gateway depuis Receiver, l'onglet Options n'est pas disponible.

Définissez le mode d'interception pour le client Citrix Secure Access pour Windows

Si vous configurez le client Citrix Secure Access pour Windows, vous devez également configurer le mode d'interception et le définir sur transparent.

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, ouvrez **NetScaler Gateway > Ressources,** puis cliquez sur Applications **intranet**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. Cliquez sur **Transparent**.
5. Dans **Protocole**, sélectionnez **N'IMPORTE** LEQUEL.
6. Dans **Type de destination**, sélectionnez **Adresse IP et masque réseau**.
7. Dans la **zone Adresse IP**, tapez l'adresse IP.
8. Dans **Masque de réseau**, tapez le masque de sous-réseau, cliquez sur **Créer,** puis sur **Fermer**.

Appliquer l'accès au réseau local aux utilisateurs finaux en fonction de la configuration ADC

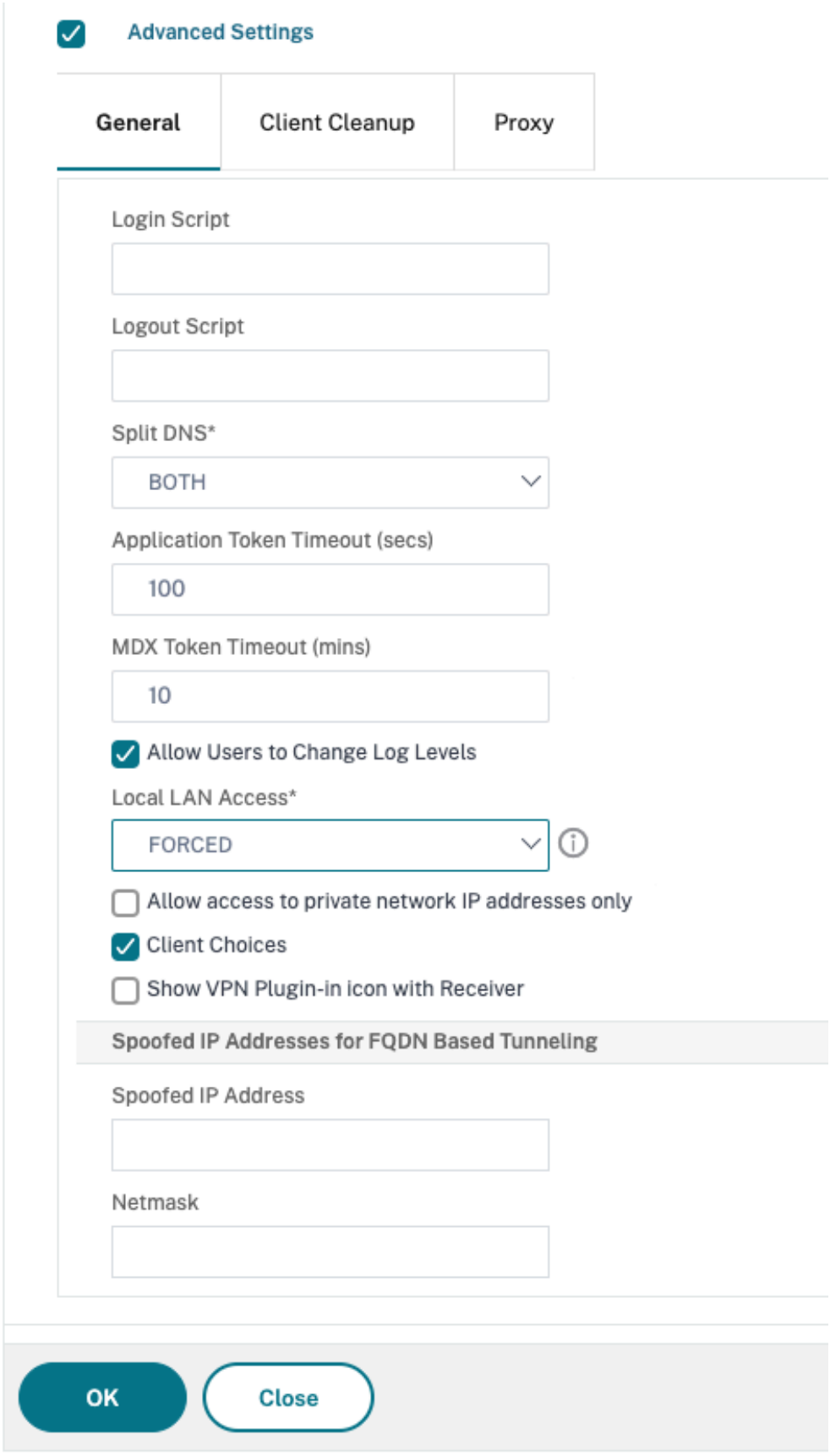
Les administrateurs peuvent empêcher les utilisateurs finaux de désactiver l'option d'accès au réseau local sur leurs machines clientes. Une nouvelle option, FORCED, est ajoutée aux valeurs des paramètres d'accès au réseau local existants. Lorsque la valeur Accès au réseau local est définie

sur FORCED, l'accès au réseau local est toujours activé pour les utilisateurs finaux sur les machines clientes. Les utilisateurs finaux ne peuvent pas désactiver les paramètres du réseau local à l'aide de l'interface utilisateur du client Citrix Secure Access.

Les administrateurs peuvent permettre aux utilisateurs finaux d'accéder aux ressources du réseau local sur leur machine cliente en réglant le paramètre d'accès au réseau local sur ON. Pour empêcher les utilisateurs finaux d'accéder aux ressources du réseau local sur leur machine cliente, les administrateurs peuvent définir le paramètre d'accès au réseau local sur OFF. Pour plus de détails sur les configurations de l'utilisateur final, voir Accès au réseau local pour macOS et Accès au réseau local pour iOS.

Pour activer l'option Forced à l'aide de l'interface graphique :

1. Accédez à **NetScaler Gateway > Paramètres globaux > Modifier les paramètres globaux**.
2. Cliquez sur l'onglet **Expérience client**, puis sur **Paramètres avancés**.
3. Dans **Accès au réseau local**, sélectionnez **FORCÉ**.



Pour activer l'option Forced à l'aide de l'interface de ligne de commande, exécutez la commande suivante :

```
set vpn parameter -localLanAccess FORCED
<!--NeedCopy-->
```

Remarques :

- Le client Citrix Secure Access pour macOS/iOS et les versions ultérieures prennent en charge la fonctionnalité d'accès au réseau local de NetScaler Gateway.
- À partir du client Citrix Secure Access pour Windows 23.10.1.7, l'accès au réseau local est pris en charge sur un tunnel au niveau de la machine si le paramètre Accès au réseau local est défini sur **Forced** on NetScaler Gateway.

Support de Microsoft Edge WebView pour Windows Citrix Secure Access —Version préliminaire

La prise en charge de Microsoft Edge WebView pour Windows Citrix Secure Access améliore l'expérience de l'utilisateur final. Pour plus de détails, consultez la section Support de Microsoft Edge WebView pour Windows Citrix Secure Access

Client Windows Citrix Secure Access utilisant la plateforme de filtrage Windows

La plate-forme de filtrage Windows (WFP) est un ensemble d'API et de services système qui fournit une plate-forme pour créer une application de filtrage réseau. WFP est conçu pour remplacer les technologies de filtrage de paquets précédentes, le filtre NDIS (Network Driver Interface Specification) qui était utilisé avec le pilote DNE. Le mode WFP est pris en charge avec la version 22.6.1.5 du client Windows Citrix Secure Access.

Installez la version WFP

Vous pouvez installer la version WFP en utilisant l'une des méthodes suivantes.

- Installez le plug-in VPN avec les pilotes DNE et WFP (méthode par défaut)

  Lorsque le plug-in est installé avec les pilotes DNE et WFP, les administrateurs peuvent utiliser le pilote WFP ou DNE pour créer un tunnel via un bouton de registre. Par défaut, le pilote DNE est utilisé pour le tunneling.

- Installez le plug-in VPN avec uniquement le pilote WFP (Ignorer l'installation du pilote DNE)

Les pilotes DNE ne sont pas pris en charge par certaines applications tierces, même lorsqu'ils ne sont pas utilisés. Pour ces déploiements, les administrateurs peuvent utiliser ce type d'installation. Comme le pilote DNE n'est pas installé, seul le pilote WFP est utilisé pour le tunneling.

Sélectionnez un pilote WFP au lieu d'un pilote DNE

Effectuez les étapes suivantes pour sélectionner le pilote WFP au lieu du pilote DNE.

> **Remarque :**
>
> Cela fonctionne uniquement avec la méthode d'installation par défaut.

1. Téléchargez la version du plug-in VPN pris en charge par WFP et installez le nouveau plug-in VPN.
2. Par défaut, le pilote DNE est utilisé pour tunneler le trafic. Pour utiliser le pilote WFP pour le tunneling, les administrateurs doivent créer l'entrée de registre suivante :
   - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
     - REG_TYPE - REG_DWORD
     - REG_NAME - EnableWFP
     - REG_VALUE —Définissez la valeur sur 1 pour utiliser WFP et 0 pour utiliser DNE (par défaut, DNE est activé si cette valeur de registre n'est pas présente ou est définie sur 0)

> **Remarque :**
>
> Après avoir basculé le mode tunneling de DNE à WFP ou inversement, le système doit être redémarré pour que les modifications soient prises en compte correctement.

Ignorez complètement l'installation DNE

Effectuez les étapes suivantes pour ignorer l'installation du DNE.

1. Effectuez une désinstallation propre du plug-in VPN.
   a) Désinstallez le plug-in VPN actuel présent sur la machine et redémarrez la machine.
   b) Vérifiez si le pilote DNE est désinstallé à l'aide de l'une des options suivantes.
      - Ouvrez une invite de commandes avec privilèges élevés (ou PowerShell). Exécutez les commandes suivantes (l'exemple de sortie montre que le pilote basé sur DNE est installé sur le système)

```
PS C:\Users\Administrator> sc qc cag
[SC] QueryServiceConfig SUCCESS
```



```
SERVICE_NAME: cag
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 2   AUTO_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : ??\C:\Program Files\Common Files\
   Deterministic Networks\Common Files\cag.sys
LOAD_ORDER_GROUP   :
TAG                : 0
DISPLAY_NAME       : Citrix cag plugin for Access Gateway
DEPENDENCIES       :
SERVICE_START_NAME :
PS C:\Users\Administrator> sc qc dne
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: dne
TYPE               : 1  KERNEL_DRIVER
START_TYPE         : 1   SYSTEM_START
ERROR_CONTROL      : 1   NORMAL
BINARY_PATH_NAME   : \SystemRoot\system32\DRIVERS\dnelwf64.sys
LOAD_ORDER_GROUP   : NDIS
TAG                : 38
DISPLAY_NAME       : DNE LightWeight Filter
DEPENDENCIES       :
SERVICE_START_NAME :
<!--NeedCopy-->
```

Si le pilote n'est pas installé, la sortie suivante s'affiche :

```
The specified service does not exist as an installed service.
```

Le pilote DNE (dnelwf64.sys) étant également utilisé par d'autres fournisseurs, il peut être présent même lorsque le client Citrix Secure Access n'est pas installé sur le système. En revanche, le plug-in CAG est uniquement utilisé par le client Citrix Secure Access.

- La présence d'un DNE peut également être vérifiée en essayant de démarrer les pilotes CAG et DNE. Ouvrez l'invite de commandes à l'aide des droits d'administrateur et exécutez les commandes suivantes :

```
net start cag
net start dne
<!--NeedCopy-->
```

  - Si le message de sortie indique que les services ne peuvent pas être localisés (le nom du service n'est pas valide.), les composants du plug-in et du pilote sont désinstallés avec succès. Dans ce cas, passez à l'étape 2.
  - Si les composants du plug-in et du pilote ne sont pas désinstallés correctement, exécutez l'utilitaire de nettoyage sur la machine cliente en suivant les instructions fournies à la section https://citrix.sharefile.com/d-s829800c3821a4a8f869ad324de6f0332.

    * Décompressez l'utilitaire Cleanup et copiez-le dans un dossier.
    * Exécutez nsRmSAC.exe à partir de l'invite de commandes.
    * Redémarrez la machine cliente.

2. Créez les entrées de registre suivantes.

    - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
        - REG_TYPE - REG_DWORD
        - REG_NAME - SkipDNE
        - REG_VALUE - Définissez sur 1 pour vous assurer que DNE n'est pas installé sur la machine
    - REG_PATH - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
        - REG_TYPE - REG_DWORD
        - REG_NAME - EnableWFP
        - REG_VALUE - Définissez sur 1 pour activer WFP (cette entrée doit être créée si l'installation DNE est ignorée)

    > **Remarque :**
    >
    > - Si les entrées de registre ne sont pas créées avant l'installation, DNE est installé par défaut. Vous pouvez également consulter les fichiers journaux VPN pour vérifier si WFP ou DNE est utilisé.
    > - Si l'installation DNE est ignorée, EnableWFP doit être défini sur 1. Dans ce cas, vous ne pouvez pas passer au plug-in basé sur DNE sans réinstaller le client Citrix Secure Access.

3. Installez le nouveau plug-in VPN.
4. Vérifiez si le pilote WFP est installé sur le système. Ouvrez une invite de commandes avec privilèges élevés et exécutez la commande suivante. L'exemple de sortie montre que le pilote WFP est installé sur le système.

```
PS C:\Users\Administrator> sc qc ctxsgwcallout
[SC] QueryServiceConfig SUCCESS

SERVICE_NAME: ctxsgwcallout
    TYPE               : 1  KERNEL_DRIVER
    START_TYPE         : 1   SYSTEM_START
    ERROR_CONTROL      : 0   IGNORE
    BINARY_PATH_NAME   : ??\C:\Program Files\Citrix\Secure Access
       Client\ctxsgwcallout.sys
    LOAD_ORDER_GROUP   :
    TAG                : 0
    DISPLAY_NAME       : Citrix Secure Access Callout Driver
    DEPENDENCIES       :
    SERVICE_START_NAME :
<!--NeedCopy-->
```


Si le pilote n'est pas installé, la sortie suivante s'affiche :

```
The specified service does not exist as an installed service.
```

1. Redémarrez la machine cliente.

Avantages de WFP

Voici quelques-uns des avantages de WFP si l'installation du pilote WFP autonome est effectuée sur le client.

- **Prise en charge du split tunneling inversé basé sur le nom de domaine complet :** le pilote WFP permet la prise en charge du split tunneling REVERSE basé sur Il n'est pas pris en charge par le pilote DNE. Pour plus de détails, consultez la section Options de split tunneling.
- **Prise en charge de Wireshark :** DNE ne permet pas de capturer le trafic bidirectionnel sur une machine cliente en raison de sa liaison avec la carte Ethernet/Wi-Fi. Ce n'est pas un problème avec le nouveau pilote WFP. Toute capture de trafic (unidirectionnelle ou bidirectionnelle) est cryptée et nécessite des clés SSL pour le déchiffrer.
- **Support NMAP :** le nouveau pilote WFP prend en charge l'analyse NMAP alors que le plug-in VPN est utilisé pour tunneliser le trafic, tandis que le DNE n'autorise pas l'analyse NMAP, tandis que le plug-in VPN est utilisé pour tunneliser le trafic.
- **Vitesse du réseau :** dans certains scénarios, si DNE est installé sur une machine cliente, la vitesse de téléchargement et de téléversement est affectée, ce qui n'est pas le cas avec WFP.
- **Amélioration des performances de nslookup :** Parfois, avec DNE, `nslookup` ne répond pas avec un nombre moindre d'essais, et la même chose n'est pas observée avec WFP.
- **Amélioration des performances iperf par rapport à UDP :** avec DNE, une certaine perte de paquets a été observée lors des tests d'évolutivité utilisant iperf sur UDP. La perte de paquets n'est pas observée avec le WFP.

Déployer le client Citrix Secure Access depuis Active Directory

January 26, 2024

Si les utilisateurs ne disposent pas des privilèges administratifs nécessaires pour installer le client Citrix Secure Access sur la machine utilisateur, vous pouvez déployer le plug-in pour les utilisateurs depuis Active Directory. Lorsque vous utilisez cette méthode pour déployer le client Citrix Secure Access, vous pouvez extraire le programme d'installation, puis utiliser une stratégie de groupe pour déployer le programme. Les étapes générales de ce type de déploiement sont les suivantes :

- Extraction du package MSI.
- Distribution du plug-in à l'aide d'une stratégie de groupe.
- Création d'un point de distribution.
- Attribution du package client Citrix Secure Access à l'aide d'un objet de stratégie de groupe.

  Remarque : La distribution du client Citrix Secure Access depuis Active Directory est uniquement prise en charge sous Windows 7, Windows 8 et Windows 10.

Vous pouvez télécharger le package MSI à partir de l'utilitaire de configuration ou du site Web Citrix.

Pour télécharger le package MSI du client Citrix Secure Access à partir de l'utilitaire de configuration

1. Dans l'utilitaire de configuration, cliquez sur **Téléchargements**.
2. Sous le client Citrix Secure Access, cliquez sur **Télécharger le plug-in NetScaler Gateway pour Windows**, puis enregistrez le fichier **nsvpnc_setup.exe** sur votre serveur Windows.

   Remarque :

   - Pour les machines 64 bits, vous devez enregistrer le fichier Agee_setup.exe sur votre serveur Windows.
   - Si la boîte de dialogue de **téléchargement de fichiers** ne s'affiche pas, appuyez sur la touche CTRL lorsque vous cliquez sur le lien **Télécharger le client Citrix Secure Access pour Windows**.

3. À l'invite de commandes, accédez au dossier dans lequel vous avez enregistré **nsvpnc_setup.exe**, puis tapez :

   ```
   1 nsvpnc_setup /c
   2 <!--NeedCopy-->
   ```

   Ceci extrait le fichier agee.msi.

   Remarque : Pour les ordinateurs 64 bits, accédez au dossier dans lequel vous avez enregistré **Agee_setup.exe**, puis tapez :

   ```
   1 Agee_setup.exe /c
   2 <!--NeedCopy-->
   ```

   Ceci extrait le fichier agee64.msi.

4. Enregistrez le fichier extrait dans un dossier sur le serveur Windows.

Après avoir extrait le fichier, utilisez une stratégie de groupe sur Windows Server pour distribuer le fichier.

Avant de commencer la distribution, installez la console de gestion des stratégies de groupe sur Windows Server 2003, Windows Server 2008 ou Windows Server 2012. Pour plus d'informations, consultez l'aide en ligne de Windows.

Remarque : Lorsque vous utilisez une stratégie de groupe pour publier le client Citrix Secure Access, Citrix recommande d'attribuer le package à la machine utilisateur. Le package MSI est installé par appareil.

Avant de pouvoir distribuer le logiciel, créez un point de distribution sur un partage réseau sur un serveur de publication, tel que Microsoft Internet Security and Acceleration (ISA) Server.

Pour créer un point de distribution

1. Ouvrez une session sur le serveur de publication en tant qu'administrateur.
2. Créez un dossier et partagez-le sur le réseau avec une autorisation de lecture pour tous les comptes qui ont besoin d'accéder au package de distribution.
3. À l'invite de commandes, accédez au dossier dans lequel vous enregistrez le fichier extrait, puis tapez : msiexec -a agee.msi
4. Sur l'écran **Emplacement réseau**, cliquez sur **Modifier**, puis accédez au dossier partagé dans lequel vous souhaitez créer l'installation administrative du client Citrix Secure Access.
5. Cliquez sur **OK**, puis sur **Installer**.

Après avoir placé le package extrait sur le partage réseau, affectez-le à un objet de stratégie de groupe dans Windows.

Une fois que vous avez correctement configuré le client Citrix Secure Access en tant que package logiciel géré, le plug-in est installé automatiquement au prochain démarrage de la machine utilisateur.

> **Remarque :** Lorsque le package d'installation est attribué à un ordinateur, l'utilisateur doit redémarrer l'ordinateur.

Lorsque l'installation démarre, les utilisateurs reçoivent un message indiquant que le client Citrix Secure Access est en cours d'installation.

Gérer le client Citrix Secure Access à l'aide d'Active Directory

January 26, 2024

Chaque version du client Citrix Secure Access est fournie sous forme d'installation complète du produit, et non sous forme de correctif. Lorsque les utilisateurs ouvrent une session et que le client Citrix Secure Access détecte une nouvelle version du plug-in, celui-ci est automatiquement mis à niveau. Vous pouvez également déployer le client Citrix Secure Access pour effectuer une mise à niveau à l'aide d'Active Directory.

Pour ce faire, créez un point de distribution pour le client Citrix Secure Access. Créez un objet de stratégie de groupe et attribuez-lui la nouvelle version du plug-in. Ensuite, créez un lien entre le nouveau package et le package existant. Une fois le lien créé, le client Citrix Secure Access est mis à jour.

Supprimer le client Citrix Secure Access des appareils utilisateur

Pour supprimer le client Citrix Secure Access des machines utilisateur, supprimez le package attribué dans l'éditeur d'objets de stratégie de groupe.

Lorsque le plug-in est supprimé de la machine utilisateur, les utilisateurs reçoivent un message indiquant qu'il est en cours de désinstallation.

Résoudre les problèmes d'installation du client Citrix Secure Access à l'aide d'Active Directory

Si l'installation du package attribué échoue au démarrage de la machine utilisateur, l'avertissement suivant peut s'afficher dans le journal des événements de l'application :

Impossible d'appliquer les modifications apportées aux paramètres d'installation du logiciel. L'application de la stratégie d'installation du logiciel a été retardée jusqu'à la prochaine ouverture de session, car un administrateur a activé l'optimisation de la connexion pour la stratégie de groupe. L'erreur était la suivante : La structure de stratégie de groupe doit appeler l'extension lors de l'actualisation synchrone de la stratégie de premier plan.

Cette erreur est due à l'optimisation de l'ouverture de session rapide dans Windows XP, dans laquelle les utilisateurs sont autorisés à ouvrir une session avant que le système d'exploitation n'initialise tous les composants réseau, y compris le traitement des objets de stratégie de groupe. Certaines stratégies peuvent nécessiter plusieurs redémarrages pour être prises en compte. Pour résoudre ce problème, désactivez l'optimisation de la connexion rapide dans Active Directory.

Pour résoudre d'autres problèmes d'installation de logiciels gérés, Citrix recommande d'utiliser une stratégie de groupe pour activer la journalisation de Windows Installer.

Intégrer le client Citrix Secure Access à l'application Citrix Workspace

January 26, 2024

NetScaler Gateway prend en charge l'application Citrix Workspace. Le système orchestré comprend les composants suivants :

- Application Citrix Workspace pour Windows 3.4 ou version ultérieure
- Application Citrix Workspace pour Mac
- Application Citrix Workspace pour Android
- Application Citrix Workspace pour iOS
- StoreFront 2.1 ou version ultérieure
- Endpoint Management 2.8 et versions ultérieures ou Citrix Endpoint Management 10
- Service de mise à jour Citrix hébergé sur le site Web Citrix

Pour plus d'informations sur la compatibilité de NetScaler Gateway avec les produits NetScaler, consultez la section Compatibilitéavec les produits NetScaler.

Vous pouvez configurer NetScaler Gateway de telle sorte que lorsque les utilisateurs ouvrent une session sur l'appliance, le client Citrix Secure Access ouvre un navigateur Web qui permet l'authentification unique sur la page d'accueil de l'application Citrix Workspace. Les utilisateurs peuvent télécharger l'application Citrix Workspace depuis la page d'accueil.

Lorsque les utilisateurs ouvrent une session avec l'application Citrix Workspace, les connexions utilisateur peuvent être acheminées via NetScaler Gateway de la manière suivante :

- Directement vers Endpoint Management
- Directement vers StoreFront
- Dans StoreFront puis Endpoint Management si vous ne configurez pas les applications mobiles MDX dans Endpoint Management
- Vers Endpoint Management, puis StoreFront si vous configurez des applications mobiles MDX dans Endpoint Management

> **Remarque :**
>
> Les connexions qui sont acheminées directement vers Endpoint Management sont prises en charge dans Endpoint Management 2.0, Endpoint Management 2.5, Endpoint Management 2.6, Endpoint Management 2.8 et Endpoint Management 2.9 uniquement. Si Endpoint Management 1.1 est déployé sur votre réseau, les connexions utilisateur doivent être acheminées via StoreFront.

Comment les utilisateurs se connectent à l'application Citrix Workspace

January 26, 2024

Les utilisateurs peuvent se connecter aux applications, bureaux et données suivants à partir de l'application Citrix Workspace :

- Applications Windows et bureaux virtuels publiés dans StoreFront et l'interface Web
- Données ShareFile accessibles via Citrix Endpoint Management

Les utilisateurs peuvent ouvrir une session à l'aide de l'une des applications Citrix Workspace suivantes :

- Application Citrix Workspace pour le Web
- Application Citrix Workspace pour Windows
- Application Citrix Workspace pour Mac
- Application Citrix Workspace pour iOS
- Application Citrix Workspace pour Android

Les utilisateurs peuvent ouvrir une session avec l'application Citrix Workspace pour le Web à l'aide d'un navigateur Web ou à partir de l'icône de l'application Citrix Workspace sur la machine utilisateur.

Lorsque les utilisateurs ouvrent une session avec n'importe quelle version de l'application Citrix Workspace, les applications, les données ShareFile et les bureaux apparaissent dans la fenêtre du navigateur ou de l'application Citrix Workspace.

Découpler l'icône de l'application Citrix Workspace

March 27, 2024

Lorsqu'un déploiement Citrix Virtual Apps and Desktops est configuré avec le client Citrix Secure Access intégré à l'application Citrix Workspace, l'icône du plug-in n'est pas visible pour les utilisateurs connectés au VPN. L'icône **Citrix Secure Access** se trouve normalement dans la barre d'état système Windows ou dans la barre de menus de macOS X Finder. Cette icône est l'interface des paramètres et des commandes du plug-in. Pour les utilisateurs de Windows, lorsque l'application Citrix Workspace et le client Citrix Secure Access sont intégrés, la boîte de dialogue **À propos** de l'application Citrix Workspace affiche les commandes du client Citrix Secure Access. Pour les utilisateurs de macOS X, aucun contrôle n'est disponible pour le client Citrix Secure Access après l'intégration.

Certains déploiements intégrés peuvent nécessiter d'exposer les contrôles du plug-in tout en conservant l'intégration de la fonctionnalité sous-jacente. Pour ce faire, utilisez la commande CLI suivante

ou la tâche de l'utilitaire de configuration NetScaler pour activer l'intégration des icônes pour les clients VPN.

Définir l'intégration des icônes à l'aide de la CLI

À l'invite de commande, tapez ;

```
set vpn parameter [-iconWithReceiver (ON/OFF)]

<!--NeedCopy-->
```

Définir l'intégration des icônes à l'aide de l'interface graphique

1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Paramètres généraux**.
2. Cliquez sur **Modifier les paramètres globaux**, puis sélectionnez l'onglet **Expérience client**.
3. Cliquez sur **Paramètres avancés.**
4. Sélectionnez **Afficher l'icône du plug-in VPN** dans l'application Citrix Workspace.

Configurer IPv6 pour les connexions ICA

March 27, 2024

NetScaler Gateway prend en charge les adresses IPv6 pour les connexions ICA. Les connexions IPv6 à l'interface Web ou à StoreFront fonctionnent de la même manière que les connexions IPv4. Lorsque les utilisateurs se connectent à l'aide de l'adresse Web de NetScaler Gateway, NetScaler Gateway transmet la connexion par proxy à l'interface Web ou à StoreFront.

Vous pouvez configurer IPv6 pour NetScaler Gateway déployé dans une zone démilitarisée ou déployé dans une zone démilitarisée à double saut.

Vous activez IPv6 sur NetScaler Gateway à l'aide de la ligne de commande. Vous pouvez suivre les instructions suivantes :

- Activez IPv6 sur l'appliance.
- Configurez les adresses IP du sous-réseau.
- Définissez l'ordre de résolution DNS.
- Définissez l'interface Web ou l'adresse Web StoreFront.
- Liez la Secure Ticket Authority (STA) à NetScaler Gateway.

Par défaut, l'adresse IP mappée ne prend pas en charge les adresses IPv6. Pour acheminer les communications des utilisateurs vers le réseau interne, vous devez créer des adresses IP de sous-réseau, puis configurer NetScaler Gateway pour utiliser les adresses IP de sous-réseau.

Si vous déployez plusieurs sous-réseaux IPv6 sur votre réseau, créez plusieurs adresses IP de sous-réseaux IPv6 sur NetScaler Gateway, une pour chaque sous-réseau de votre réseau. Le routage réseau envoie les paquets IPv6 aux sous-réseaux respectifs en utilisant les adresses IP du sous-réseau.

Pour configurer IPv6 pour le proxy ICA à l'aide de l'interface de ligne de commande

1. Connectez-vous à NetScaler Gateway à l'aide d'une connexion Secure Shell (SSH), par exemple depuis PuTTY. À l'invite de commande, tapez ;

```
enable ns feature IPv6PT. This enables IPv6.

enable ns mode USNIP.

set dns parameter  – resolutionOrder AAAAThenAQuery AThenAAAAQuery
   OnlyAAAAQuery OnlyAQuery

set vpn parameter -wihome `http://XD_domain/Citrix/StoreWeb`

<!--NeedCopy-->
```

où est le nom de domaine ou l'adresse IP de StoreFront.

Exemple :

```
set vpn parameter -wihome `http://storefront.domain.com/Citrix/StoreWeb
   `.
<!--NeedCopy-->
```

Ou

```
set vpn parameter -wihome `http://[1000:2000::3000]/Citrix/StoreWeb`
<!--NeedCopy-->
```

> **Remarque :**
>
> Si vous utilisez l'adresse IPv6 pour configurer ce paramètre, l'adresse IP doit être placée entre crochets.

Configurer la page d'accueil de l'application Citrix Workspace sur NetScaler Gateway

March 27, 2024

Vous pouvez configurer la page d'accueil de l'application Citrix Workspace globalement ou dans le cadre d'un profil de session. Si vous souhaitez configurer l'application Citrix Workspace pour le Web et les versions antérieures de l'application Citrix Workspace qui ne reconnaissent pas StoreFront via NetScaler Gateway, vous devez créer deux profils de session distincts. Le champ Page d'accueil de l'application Citrix Workspace doit comporter l'adresse Web correcte pour chaque profil afin que les utilisateurs puissent se connecter correctement.

Pour les applications Citrix Workspace qui reconnaissent StoreFront via NetScaler Gateway, vous pouvez demander à l'application Citrix Workspace pour Web et à l'application Citrix Workspace de partager un profil. Toutefois, Citrix vous recommande de configurer un profil de session pour l'application Citrix Workspace pour Web et un profil de session distinct pour toutes les autres applications Citrix Workspace.

Pour configurer la page d'accueil de l'application Citrix Workspace globalement

Pour configurer la page d'accueil de l'application Citrix Workspace globalement, procédez comme suit :

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans la boîte de dialogue Paramètres globaux de NetScaler Gateway, cliquez sur l'onglet Applications publiées.
4. Dans la page d'accueil de l'application Citrix Workspace, tapez l'adresse Web de l'application Citrix Workspace ou de la page d'accueil de l'application Citrix Workspace pour le Web, puis cliquez sur OK.

Pour configurer la page d'accueil de l'application Citrix Workspace dans un profil de session

Pour configurer la page d'accueil de l'application Citrix Workspace dans un profil de session, procédez comme suit :

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, dans l'onglet **Profils**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer un profil de session NetScaler Gateway**, sous l'onglet **Application publiée**, en regard de la page d'**accueil de Citrix Receiver**, cliquez sur **Remplacer le profil global**.
4. Dans la page d'accueil de l'application Citrix Workspace, tapez l'adresse Web de la page d'accueil de l'application Citrix Workspace ou de l'application Citrix Workspace pour le Web, puis cliquez sur **Créer**.

Appliquer le thème de l'application Citrix Workspace à la page de connexion de NetScaler Gateway

March 27, 2024

Vous pouvez utiliser l'interface utilisateur de NetScaler Gateway pour appliquer le thème de l'application Citrix Workspace à la page de connexion de NetScaler Gateway. Vous pouvez basculer entre le thème de l'application Citrix Workspace et le thème personnalisé que vous créez. Une fois le thème personnalisé créé, effacez le cache du navigateur pour empêcher l'affichage des pages mises en cache.

Par défaut, la page de connexion de NetScaler Gateway utilise le thème visuel RFWebUI qui correspond au style de l'interface utilisateur unifiée utilisée par StoreFront. Si vous utilisez la plateforme Citrix Workspace ou StoreFront sur site avec l'[interface utilisateur New Workspace](https://docs.citrix.com/fr-fr/citrix-workspace/get-started/user-experience), suivez les instructions fournies dans cet article de support. Vous pouvez également créer votre propre thème personnalisé. Pour plus de détails, voir Création d'un thème personnalisé pour la page de connexion à NetScaler Gateway.

Assurez-vous que le thème du portail NetScaler Gateway est lié à un serveur virtuel VPN. Pour plus de détails, voir Associer un thème de portail à un serveur virtuel VPN.

Création d'un thème personnalisé pour la page de connexion de NetScaler Gateway

January 26, 2024

Vous pouvez utiliser l'interface graphique pour créer un thème personnalisé pour la page de connexion de NetScaler Gateway. Vous pouvez également quitter le thème par défaut ou utiliser le thème de l'application Citrix Workspace. Lorsque vous choisissez d'appliquer un thème personnalisé à la page de connexion, vous utilisez la ligne de commande NetScaler Gateway pour créer et déployer le thème. Vous utilisez ensuite l'interface graphique pour définir la page de thème personnalisée.

Vous configurez la page de thème personnalisée à l'aide des paramètres globaux de NetScaler Gateway.

Vous pouvez utiliser cette fonctionnalité avec les versions suivantes de NetScaler Gateway :

- NetScaler Gateway 10.1
- Access Gateway 10, Build 73.5002.e (vous devez installer cette version après la version 71.6104.e pour utiliser cette fonctionnalité avec Endpoint Management versions 2.5, 2.6 ou 2.8)
- Passerelle d'accès 10, version 71.6104.e

Créez et déployez le thème personnalisé à l'aide de l'interface de ligne de commande

Pour créer et déployer le thème personnalisé à l'aide de la ligne de commande :

1. Connectez-vous à la ligne de commande NetScaler Gateway.
2. À l'invite de commandes, tapez shell.
3. À l'invite de commandes, tapez `mkdir /var/ns_gui_custom; cd /netscaler; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*`.
4. Utilisez l'utilitaire de configuration pour basculer vers le thème personnalisé, puis effectuez des modifications de personnalisation sous /var/ns_gui_custom/ns_gui/vpn. Vous pouvez :
    - Apportez des modifications au fichier css/ctx.authentication.css.
    - Copiez un logo personnalisé dans le dossier /var/ns_gui_custom/ns_gui/vpn/media. **Remarque :** Vous pouvez utiliser WinSCP pour transférer les fichiers.
5. Si vous possédez plusieurs appliances NetScaler Gateway, répétez les étapes 3 et 4 pour toutes les appliances.

Clés de registre du client VPN NetScaler Gateway pour Windows

March 27, 2024

Les clés de registre du client VPN sont disponibles sous **HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client**. Le tableau suivant répertorie les clés de registre et les valeurs du client VPN NetScaler Gateway, ainsi qu'une brève description de chaque valeur.

Clé de registre	Type de registre	Valeurs et description
AlwaysOnService	REG_DWORD	1 => Établir un tunnel au niveau machine mais pas un tunnel au niveau utilisateur. 2 => Établir un tunnel au niveau machine et un tunnel au niveau utilisateur.
AlwaysOnURL	REG_SZ	URL du serveur virtuel NetScaler Gateway auquel l'utilisateur souhaite se connecter. Exemple : *https://xyz.companyDomain.com*
AlwaysOn	REG_DWORD	1 => Autoriser l'accès réseau en cas de défaillance du VPN. 2=> Bloquer l'accès réseau en cas de panne du VPN.
locationDetection	REG_DWORD	1 => Pour activer la détection de position. 0 => Pour désactiver la détection de position.
suffixList	REG_SZ	Liste des domaines intranet sous forme de points-virgules. Utilisé lorsque la détection de position est activée.
AlwaysOnAllowlist	REG_SZ	Liste séparée par des points-virgules des adresses IP ou des noms de domaine complets autorisés par le pilote en mode strict Always On.
ProductVersion	REG_SZ	Version actuelle du client Citrix Secure Access installée.
InstallDir	REG_SZ	Emplacement où le client Citrix Secure Access est installé.

Clé de registre	Type de registre	Valeurs et description
userCertCAList	REG_SZ	Utilisé dans le contexte du service Always On où un client peut spécifier la liste des autorités de certification dans lesquelles choisir le certificat client.
addedRoutes/modifiedRoutes	REG_SZ	Créé pour la communication interne du plug-in. Les utilisateurs ne doivent pas modifier cette clé.
ProductCode	REG_SZ	Cette clé est utilisée en interne. Les utilisateurs ne doivent pas modifier cette clé
EnableAutoUpdate	REG_DWORD	Permet de contrôler la fonctionnalité de mise à jour du plug-in du côté client. Définissez cette valeur sur 0 pour désactiver la fonctionnalité de mise à jour automatique. Définissez sur 1 pour respecter la configuration ADC.
Connecté	REG_DWORD	En cas de connexion réussie, cette clé est définie sur 1 et sinon sur 0. Cette clé est utilisée en interne. Les utilisateurs ne doivent pas modifier cette clé.
EnableVA	REG_DWORD	Si l'adaptateur Citrix Virtual doit être activé lorsque IIP est présent. Cette clé est utilisée en interne. Les utilisateurs ne doivent pas modifier cette clé.
DisableGA	REG_DWORD	Définissez cette option sur 1 pour désactiver Google Analytics.

Clé de registre	Type de registre	Valeurs et description
DisableCredProv	REG_DWORD	Lorsque Always On before user logon est activé, le plug-in VPN Windows ajoute le fournisseur d'informations d'identification pour afficher l'état du tunnel sur l'écran d'ouverture de session. Si vous n'avez pas besoin de cette fonctionnalité supplémentaire, créez et définissez ce registre sur 1.
ClientControl	REG_DWORD	1 => Permet aux utilisateurs de se déconnecter ou de se connecter à d'autres passerelles. 0 => Bloque les utilisateurs de se déconnecter ou de se connecter à d'autres passerelles.
ForcedLogging	REG_DWORD	Définissez cette clé sur 1 pour activer la journalisation du débogage.
NoDHCPRoute	REG_DWORD	Si la valeur 1 est définie, la route du serveur DHCP n'est pas ajoutée.
DisableIntuneDeviceEnrollment	REG_DWORD	Si cette valeur est définie sur 1, l'inscription des appareils Intune n'est pas effectuée.
HttpTimeout	REG_DWORD	Le délai d'expiration HTTP est configuré en quelques secondes. Si le délai d'expiration n'est pas configuré, le délai d'expiration par défaut est utilisé. La valeur du délai d'expiration par défaut est de 100 secondes, selon les normes Windows.

Clé de registre	Type de registre	Valeurs et description
secureDNSUpdate	REG_DWORD	0 => Le plug-in VPN essaie uniquement la mise à jour DNS non sécurisée. 1 => Le plug-in VPN essaie d'abord la mise à jour DNS non sécurisée. Si la mise à jour DNS non sécurisée échoue, le plug-in VPN essaie ensuite la mise à jour DNS sécurisée. Il s'agit du comportement par défaut à partir de la version 21.3.1.2 du plug-in Windows. 2 => Le plug-in VPN essaie uniquement la mise à jour DNS sécurisée.
DisableIconHide	REG_DWORD	1 => L'application Citrix Workspace et le plug-in de passerelle sont affichés dans la barre des tâches. 0 => L'icône du plug-in de passerelle est intégrée à l'application Citrix Workspace pour Windows. Le plug-in de passerelle n'est pas visible dans la barre des tâches lors de l'exécution d'une session VPN complète.

Clé de registre	Type de registre	Valeurs et description
SecureChannelResetTimeoutSeconds	REG_DWORD	Par défaut, cette valeur de registre n'est ni définie ni ajoutée. Lorsque la valeur de « SecureChannelResetTimeout-Seconds » est 0xFFFFFFFF ou qu'elle n'est pas présente dans le registre, le plug-in VPN attend la fin de l'appel d'API SecureChannelReset () avant de commencer à tunneliser le trafic de données. Il s'agit du comportement par défaut. L'administrateur doit configurer ce registre sur le client pour que le plug-in VPN commence à tunnéliser le trafic de données après avoir attendu l'heure spécifiée pour la fin de l'appel d'API.
DisableDNSRoutes	REG_DWORD	Valeur par défaut 0 => Le plug-in VPN ajoute des routes pour les serveurs DNS s'ils sont différents de la passerelle par défaut pour une interface physique. Toutefois, en fonction de la topologie de la machine cliente Windows, les routes du serveur DNS peuvent ne pas toujours être requises. S'il est défini sur 1, le plug-in VPN n'ajoute pas de routes explicites pour les serveurs DNS.
overrideIPV6DnsDrop	REG_DWORD	1 => Autoriser le trafic DNS IPv6 à passer par le VPN. 0 => Restreindre le flux de trafic DNS IPv6.

Clé de registre	Type de registre	Valeurs et description
DisallowCaptivePortals	REG_DWORD	1 => Le plug-in VPN vérifie la présence de portails captifs en essayant de se connecter à la page de test de Microsoft Connect avant de démarrer une session VPN. 0 => Le plug-in VPN ignore la vérification des portails captifs.
EnableWFP	REG_DWORD	Valeur par défaut 0 => Par défaut, DNE est activé. 1 => Le plug-in VPN utilise WFP. 0 => Le plug-in VPN utilise DNE.
ConfigSize	REG_DWORD	Le client Windows prend en charge la taille du fichier de configuration de 64 Ko, par défaut. Utilisez ce registre pour augmenter la taille du fichier de configuration. Si la taille du fichier de configuration est supérieure à la valeur par défaut (64 Ko), la valeur de registre ConfigSize doit être définie sur 5 x 64 Ko (après conversion en octets) pour chaque ajout de 64 Ko. Par exemple, si vous ajoutez 64 Ko supplémentaires, vous devez définir la valeur du registre sur 64 x 1024 x 5 = 327680. De même, si vous ajoutez 128 Ko, vous devez définir la valeur de registre sur 64 x 1024 x (5+5) = 655360.

Clé de registre	Type de registre	Valeurs et description
SecureAccessLogInScript	REG_SZ	Le service Citrix Secure Access accède à la configuration du script de connexion à l'aide de cette clé de registre lorsqu'il se connecte au service Citrix Secure Private Access. Pour plus de détails, consultez la section Registres de configuration des scripts de connexion et de déconnexion.
SecureAccessLogOutScript	REG_SZ	Le service Citrix Secure Access accède à la configuration du script de déconnexion à l'aide de cette clé de registre lorsqu'il se connecte au service Citrix Secure Private Access. Pour plus de détails, consultez la section Registres de configuration des scripts de connexion et de déconnexion.
EnableKerberosAuth	REG_DWORD	0 => Valeur par défaut.1 => Le client VPN utilise la méthode d'authentification Kerberos pour la connexion automatique.

Clé de registre	Type de registre	Valeurs et description
SicBeginPort	REG_DWORD	Évite les conflits qui peuvent survenir lorsque vous utilisez des ports pour créer des sockets entre le client Citrix Secure Access et des applications tierces sur les machines clientes. La plage autorisée est comprise entre 49152 et 64535 (C000 à FC17 au format hexadécimal). Le client VPN utilise jusqu'à 1 000 ports à partir de `SicBeginPort`uniquement s'il `EnableWFP`est également configuré sur.1

Important :

- Vous pouvez appliquer des clés de registre en fonction de vos déploiements. Par exemple, la clé de registre AlwaysOnService s'applique uniquement au service Always On alors que la clé de registre ClientControl ne s'applique pas au service Always On. Consultez la documentation de déploiement individuel pour plus de détails.
- `secureDNSUpdate` s'applique uniquement aux appareils clients joints à un domaine.
- Pour le client Citrix Secure Access pour Windows 23.1.1.8 et versions ultérieures, le nom de la clé de registre est. `overrideIPV6DnsDrop` Pour le client Citrix Secure Access pour Windows 22.10.1.9 et versions antérieures, le nom de la clé de registre est. `overrideIP6DnsDrop`

Appliquer le drapeau HttpOnly aux cookies d'authentification

March 27, 2024

À partir des versions 13.1-37.x et ultérieures de NetScaler Gateway, l'indicateur HttpOnly est disponible sur les cookies d'authentification des scénarios VPN, à savoir les cookies NSC_AAAC et NSC_TMAS. Le cookie d'authentification NSC_TMAS est utilisé lors de l'authentification nFactor et le

cookie NSC_AAAC est utilisé pour la session authentifiée. Le drapeau HttpOnly sur un cookie limite l'accès aux cookies à l'aide de l'option de cookie de document JavaScript. Cela permet de prévenir le vol de cookie dû à des scripts intersites.

Scénario pris en charge

L'indicateur HttpOnly est pris en charge pour l'authentification nFactor.

Comportement lorsque le bouton HttpOnlyCookie du paramètre NetScaler AAA est utilisé conjointement avec le bouton HttpOnlyCookie de tmsession :

- Lorsque le bouton HttpOnlyCookie du paramètre d'authentification, d'autorisation et d'audit est activé et que l'authentification nFactor est utilisée, le bouton HttpOnlyCookie du paramètre d'authentification, d'autorisation et d'audit remplace le bouton HttpOnlyCookie de la session TM. De plus, NSC_TMAS et NSC_AAAC sont marqués HttpOnly quel que soit le type de session, qu'il s'agisse d'une session VPN, d'une session TM ou lors de l'authentification nFactor.
- Si le bouton HttpOnlyCookie est désactivé, l'indicateur HttpOnly n'est pas défini pour une session VPN. Pour le scénario d'authentification, d'autorisation et d'audit, l'indicateur HttpOnly est défini en fonction de la valeur du bouton de session TM.

Configurez la fonctionnalité HttpOnly à l'aide de l'interface de ligne de commande

- Activer le drapeau HttpOnly

```
set aaa parameter -httpOnlyCookie ENABLED
<!--NeedCopy-->
```

- Vérifiez l'état de la fonctionnalité HttpOnly

```
show aaa parameter
<!--NeedCopy-->
```

Limitations

- Lorsque la fonctionnalité HttpOnly est activée, le bouton de la page d'accueil du client Citrix Secure Access ne fonctionne pas.
- L'indicateur HttpOnly n'est défini dans aucune authentification classique.

Personnalisation du portail utilisateur pour les utilisateurs VPN

March 27, 2024

Les installations NetScaler Gateway qui fournissent le portail aux utilisateurs VPN incluent une option permettant de sélectionner un thème de portail afin de personnaliser l'apparence des pages du portail. Vous pouvez choisir parmi un ensemble de thèmes fourni ou utiliser un thème comme modèle pour créer un portail personnalisé ou de marque. À l'aide de l'utilitaire de configuration, vous pouvez modifier un thème en ajoutant de nouveaux logos, images d'arrière-plan, étiquettes de zone de saisie personnalisées et divers autres attributs de la conception du portail basé sur CSS. Les thèmes du portail intégrés incluent du contenu en cinq langues : anglais, français, espagnol, allemand et japonais. Les différents utilisateurs sont servis dans différentes langues, en fonction des paramètres régionaux signalés par leur navigateur Web.

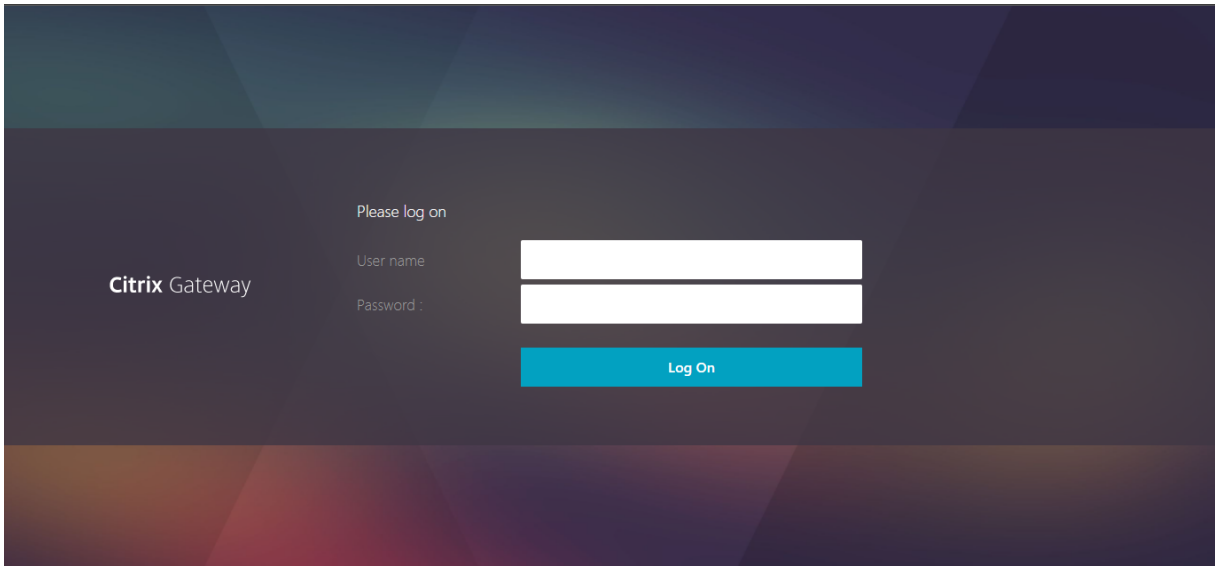
Vous pouvez créer un CLUF personnalisé qui sera présenté aux utilisateurs du VPN avant qu'ils ne soient autorisés à se connecter. La fonctionnalité CLUF prend en charge les versions locales d'un CLUF, qui sont présentées aux utilisateurs en fonction des paramètres régionaux signalés par leur navigateur Web.

Les thèmes du portail et les configurations de CLUF peuvent être liés indépendamment au niveau du serveur virtuel VPN et du VPN global.

> **Important :**
>
> NetScaler ne prend pas en charge la personnalisation nécessitant des modifications de code et ne propose pas d'assistance pour résoudre des problèmes autres que le retour à un thème par défaut.

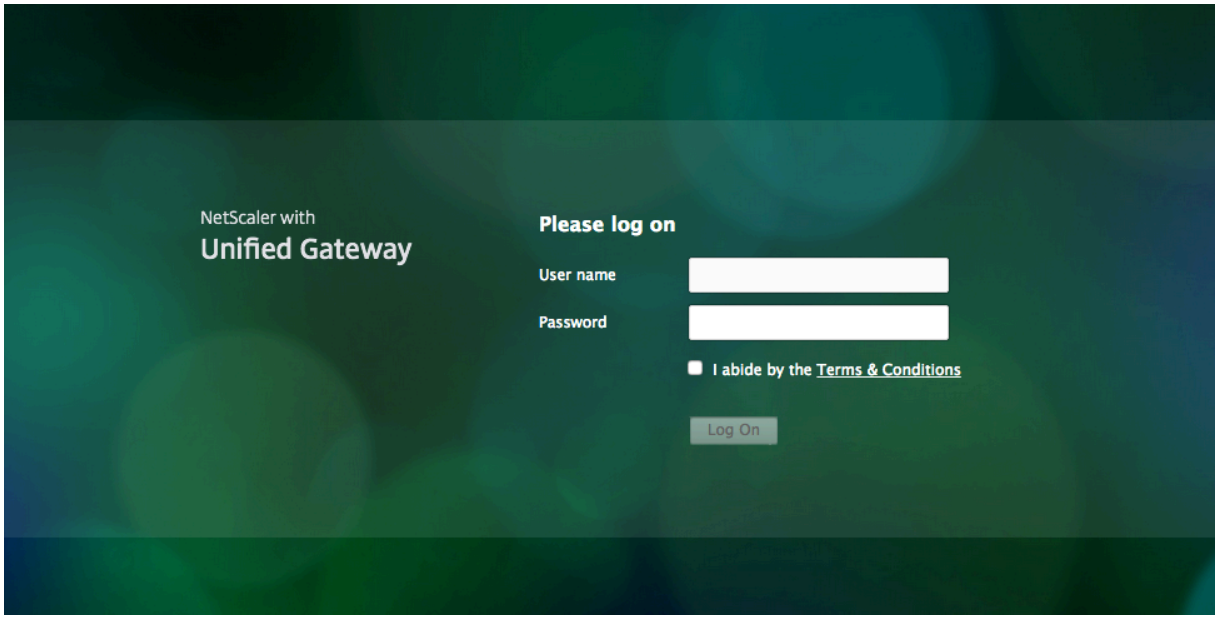
Appliquer un thème de portail

À partir de la version 13.0 build 67.43, le portail VPN est configuré pour utiliser le thème RFWebUI, par défaut. Auparavant, `Caxton theme` c'était le thème par défaut. Vous pouvez également appliquer les thèmes Green Bubble et X1.

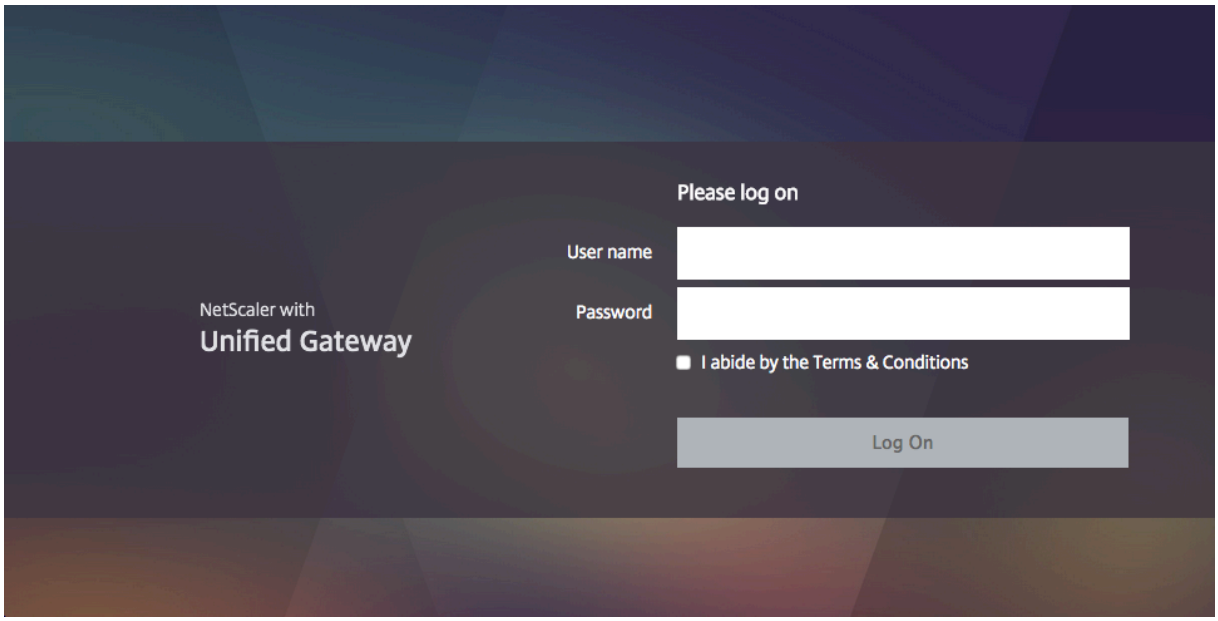


Thème Caxton

Thème Green Bubble



Thème X1



Vous pouvez appliquer n'importe lequel des thèmes fournis directement à un serveur virtuel VPN ou en tant que liaison VPN globale.

Liaison d'un thème de portail à un serveur virtuel VPN

Vous pouvez lier un thème de portail sur un serveur virtuel existant ou lors de la création d'un nouveau serveur virtuel.

Liez un thème de portail à un serveur virtuel VPN à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
bind vpn vserver <name> - portaltheme <name>
<!--NeedCopy-->
```

Liez un thème de portail à un serveur virtuel VPN à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway** et cliquez sur **Virtual Servers.**
2. Sélectionnez un serveur virtuel, puis cliquez sur **Modifier**.
3. Si un thème de portail n'a pas encore été lié au serveur virtuel, cliquez sur **Thème du portail** sous **Paramètres avancés** dans le volet d'informations. Sinon, l'option **Thème du portail**est déjà développée dans le volet d'informations.
4. Dans le volet d'informations, sous **Thèmes du portail**, cliquez sur **Aucun thème de portail**pour développer la fenêtre de liaison du thème du portail.
5. `Click` **Cliquez pour sélectionner**.
6. Dans la fenêtre **Thèmes du portail**, cliquez sur le nom d'un thème, puis sur **Sélectionner**.
7. Cliquez sur **Bind**.
8. Cliquez sur **Terminé**.

Si vous créez un serveur virtuel VPN, vous pouvez suivre les étapes de la procédure précédente en commençant par l'étape 3 dans le volet d'**édition du serveur virtuel VPN** pour lier un thème de portail.

Liez un thème de portail à VPN global

Liez un thème de portail à VPN global à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
bind vpn global portaltheme <name>
<!--NeedCopy-->
```


Liez un thème de portail à VPN global à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway**.
2. Dans le volet de détails principal, cliquez sur **NetScaler Gateway Policy Manager**.
3. Cliquez sur l'icône « **+** ».
4. Dans la liste **des points de liaison**, sélectionnez **Ressources**.
5. Dans la liste**Type de connexion**, sélectionnez**Thème du portail.**
6. Cliquez sur **Continuer**.
7. Dans l'écran **Point de liaison**, cliquez sur **Ajouter une liaison**.
8. Cliquez **sur Cliquez pour sélectionner**.
9. Dans la fenêtre **Thèmes du portail**, cliquez sur le nom d'un thème, puis sur **Sélectionner**.
10. Cliquez sur **Bind**.
11. Cliquez sur **Fermer**.
12. Cliquez sur **Terminé.**

> **Conseil :**
>
> Après avoir apporté les modifications, utilisez la commande « save ns config » sur la ligne de commande ou cliquez sur l'icône Enregistrer dans l'utilitaire de configuration pour vous assurer que vos modifications sont enregistrées dans le fichier de configuration NetScaler.

Créer un thème de portail

Pour créer une conception de portail personnalisée, vous utilisez l'un des thèmes de portail fournis comme modèle. Le système crée une copie du thème de modèle sélectionné avec un nom que vous spécifiez.

Utiliser un thème de portail boursier comme modèle pour un thème de portail personnalisé

Pour créer un thème de portail, vous pouvez utiliser l'utilitaire de configuration ou la ligne de commande pour créer l'entité de thème. Toutefois, les contrôles de personnalisation détaillés ne sont disponibles que dans l'utilitaire de configuration.

Créer un thème de portail à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
add portaltheme <name> basetheme <name>
<!--NeedCopy-->
```


Créer un thème de portail à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway** et cliquez sur **Portal Themes**.
2. Dans le volet de détails principal, cliquez sur **Ajouter**.
3. Entrez le nom du thème et sélectionnez un modèle dans la liste des modèles, puis cliquez sur **OK**.
4. À ce stade, la première vue de la fenêtre d'édition du thème du portail s'affiche. Cliquez sur **OK** pour quitter.

Vous pouvez procéder à la personnalisation du nouveau thème du portail avec la première vue.

Une fois qu'un nouveau thème est créé, vous pouvez le lier à un serveur virtuel VPN ou à un VPN global. Vous pouvez lier un nouveau thème immédiatement après sa création ou après avoir terminé vos personnalisations.

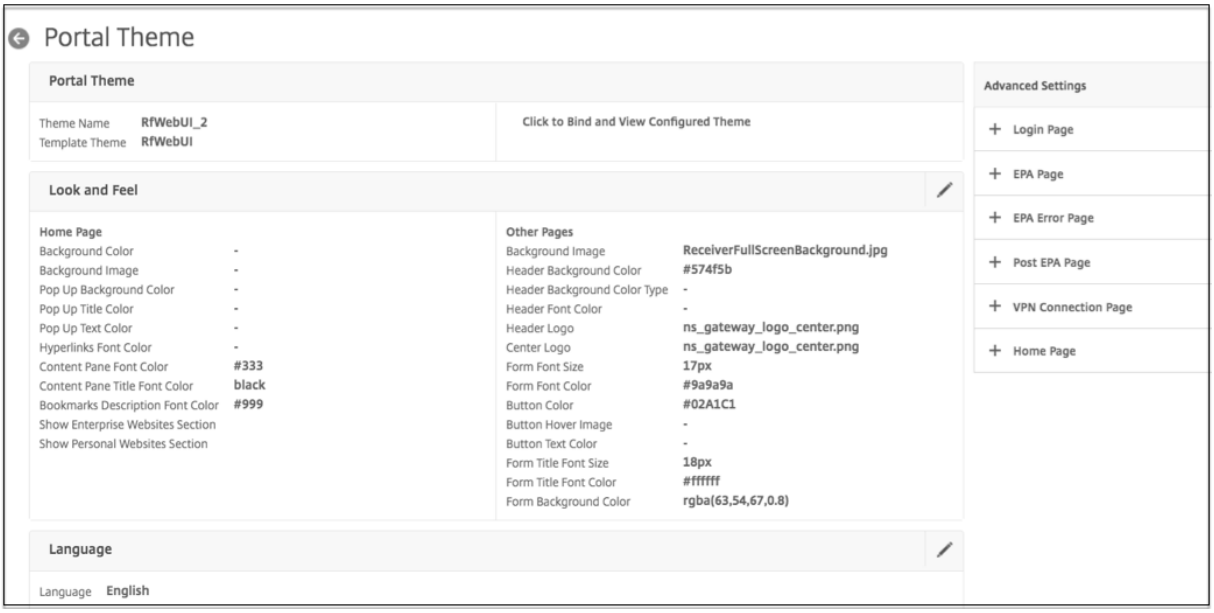
Personnalisation du thème du portail

Pour personnaliser un thème de portail, utilisez l'interface du thème du portail dans l'utilitaire de configuration. Pour obtenir les meilleurs résultats, vous devez comprendre les différents éléments de cette interface avant de l'utiliser.

À propos de l'interface du thème du portail

Pour ouvrir l'**interface du thème du portail** dans l'utilitaire de configuration NetScaler Gateway, sous l'onglet **Configuration**, accédez à **NetScaler Gateway** et cliquez sur **Thèmes du portail**. Vous pouvez créer un thème comme décrit dans la section *Création d'un thème de portail* ou sélectionner un thème existant dans le volet de détails principal et cliquer sur **Modifier**.

La page de personnalisation du thème du portail comporte quatre volets principaux permettant de modifier la conception d'un portail : le volet **Thème du portail**, le volet Look & Feel, le volet **Paramètres avancés** et le volet **Langue**.



Le volet **Thème du portail** en haut de la page indique le thème chargé en vue de la modification et le thème de modèle sur lesquels il est basé. L'option d'affichage ici vous permet de visualiser vos personnalisations sans accéder au VPN avec une connexion utilisateur. L'utilisation de l'option de visualisation nécessite de lier le thème à un serveur virtuel VPN et la liaison reste en vigueur après la fermeture de la fenêtre de visualisation.

Avec le volet **Look & Feel** au centre de la page, vous configurez les propriétés générales d'un thème, telles que les en-têtes, les couleurs et images d'arrière-plan, les propriétés de police et les logos. Lorsque ce volet est en mode de modification, les légendes d'attributs sont disponibles pour vous aider à savoir où les attributs Look & Feel sont utilisés sur les pages du portail.

Le volet **Paramètres avancés** contient les contrôles de contenu à l'écran pour les pages individuelles du portail. Pour charger le contenu d'une page à modifier, cliquez sur l'une des pages répertoriées. Les contrôles de page s'ouvrent ensuite sous les autres volets centraux. Une page reste réduite dans le volet **Paramètres avancés** lors des modifications du thème du portail tant qu'elle n'a pas été modifiée.

Dans le volet **Langue**, vous pouvez sélectionner la langue qui sera chargée lorsqu'une page est sélectionnée pour modification dans le volet **Paramètres avancés**. Les pages de langue anglaise sont chargées par défaut.

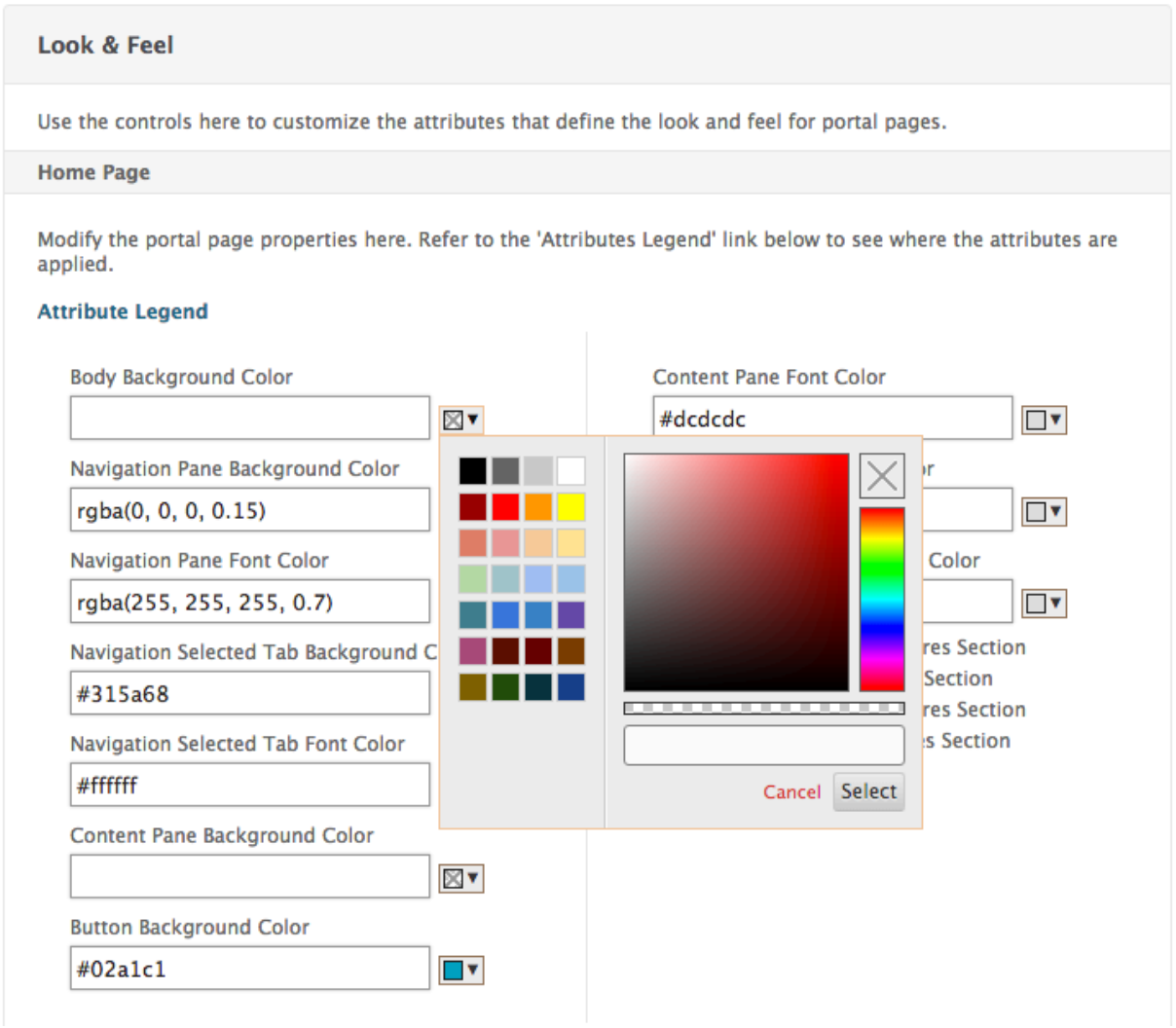
Types d'attributs de page personnalisables

Lorsque vous personnalisez un thème de portail, vous pouvez modifier une série d'attributs dans l'interface du thème du portail. Outre le texte et les langues prises en charge qui peuvent être modifiés, les éléments graphiques de la mise en page du portail peuvent être adaptés à vos besoins. Chaque

type d'élément de page comporte des paramètres ou des recommandations à prendre en compte avant de les modifier.

Couleurs

La conception du portail spécifie les couleurs des attributs tels que les arrière-plans de page, les surlignements, le texte des titres et du contenu du corps, les contrôles des boutons et les réponses au survol. Pour personnaliser un attribut de couleur, vous pouvez entrer une valeur de couleur directement pour un élément sélectionné, ou vous pouvez utiliser le sélecteur de couleurs fourni pour générer une valeur de couleur. L'interface prend en charge la saisie de valeurs de couleur HTML valides au format RGBA, au format triolet hexadécimal HTML et aux noms de couleurs X11. Le sélecteur de couleurs est accessible pour n'importe quel attribut de couleur applicable en cliquant sur la zone de couleur en regard du champ de saisie de l'attribut.



Polices

En plus des couleurs de police, vous pouvez modifier les tailles de police de certains attributs de page.

Pour chacun de ces attributs, un menu propose les tailles disponibles pour chaque attribut, telles que déterminées par la conception du portail.

Images

Pour les images, une description contextuelle disponible pour chaque contrôle fournit des recommandations de taille et d'autres exigences. Les descriptions varient en fonction de l'emplacement d'un attribut sur la page et de sa fonction. Vous pouvez utiliser les formats de fichier image PNG ou JPEG. Vous pouvez sélectionner une image à télécharger en cochant la case située sous le nom de fichier d'un élément, puis en accédant à l'emplacement de l'image sur le lecteur de votre ordinateur local.

Étiquettes

Dans la section **Paramètres avancés**, vous pouvez sélectionner le texte d'une page de portail spécifique à modifier. Si vous modifiez le texte anglais par défaut d'une page, le texte des autres langues n'est pas retraduit. Le contenu de la page dans une autre langue est fourni à titre de commodité, mais nécessite des mises à jour manuelles pour toute personnalisation. Pour modifier une autre version linguistique d'une page, commencez par réduire la fenêtre, si elle est ouverte, en cliquant sur l'icône **X** de la page de portail ouverte. Sélectionnez ensuite la langue dans le volet **Langue**, puis cliquez sur **OK**. Toutes les pages du portail ouvertes à partir du volet **Paramètres avancés** sont dans cette langue jusqu'à ce que vous en sélectionniez une autre.

> **Important**
>
> Dans les déploiements à haute disponibilité ou en cluster, les thèmes du portail sont distribués dans la configuration partagée uniquement lorsque les paramètres du thème du portail sont définis sur les entités NetScaler principales ou coordinatrices de configuration, respectivement.

Personnalisations de portail plus anciennes

Pour les installations dont la conception de portail personnalisé a été modifiée manuellement et créée dans les versions de NetScaler Gateway ou Access Gateway antérieures à la version 11.0, NetScaler recommande vivement de commencer par un nouveau thème de portail dans l'interface de personnalisation. Si vous ne pouvez pas le faire, vous pouvez appliquer une personnalisation manuellement, mais aucune prise en charge directe n'est fournie.

Lorsque vous utilisez un portail personnalisé manuellement, vous devez définir le portail personnalisé en tant que configuration globale du portail. Cela signifie cependant qu'une configuration de portail global appliquée *ne peut pas* être remplacée par des liaisons de thème de portail au niveau du serveur virtuel VPN. La tentative de création d'une liaison de serveur virtuel VPN dans ce cas avec l'utilitaire de configuration ou la ligne de commande renvoie une erreur.

De plus, dans le cas de configurations de haute disponibilité et de clusters, toute personnalisation manuelle doit être effectuée sur chaque nœud du déploiement car les fichiers sous-jacents du système de fichiers NetScaler ne sont pas distribués dans la configuration partagée automatiquement.

Création manuelle d'une configuration de portail personnalisée

Pour appliquer manuellement une ancienne configuration de portail personnalisé après la mise à niveau vers NetScaler Gateway 11.0, vous devez modifier une copie d'une page de portail existante, placer les fichiers de portail personnalisés dans le système de fichiers NetScaler et sélectionner **CUSTOM** comme paramètre **UITHEME**.

Vous pouvez utiliser WinSCP ou tout autre programme de copie sécurisée pour transférer des fichiers vers le système de fichiers NetScaler.

1. Connectez-vous à la ligne de commande NetScaler Gateway.
2. À l'invite de commandes, tapez**shell**
3. À l'invite de commandes, tapez **mkdir /var/ns_gui_custom ; cd /netscaler ; tar -cvzf /var/ns_gui_custom/customtheme.tar.gz ns_gui/*.**
4. À l'invite de commandes, tapez **cd /var/netscaler/logon/themes/**

    - Si vous souhaitez personnaliser le thème de la bulle verte, entrez**cp -r** `Greenbubble` **Custom** pour créer une copie du thème Green Bubble.
    - Si vous souhaitez personnaliser le thème par défaut (`Caxton`), tapez **cp -r Default Custom.**
    - Pour personnaliser le thème X1, tapez**cp -r X1 Custom.**

5. Apportez les modifications nécessaires aux fichiers copiés sous**/var/netscaler/logon/themes/custom** pour personnaliser le thème manuellement.

    - Apportez les modifications nécessaires au **fichier css/base.css**.
    - Copiez les images personnalisées dans le répertoire **/var/ns_gui_custom/ns_gui/vpn/media**.
    - Apportez des modifications aux étiquettes des fichiers présents dans le répertoire **resources/**. Ces fichiers correspondent aux paramètres régionaux pris en charge par le portail.
    - Si des modifications de pages HTML ou de fichiers javascript sont également nécessaires, vous pouvez rendre les fichiers pertinents dans **/var/ns_gui_custom/ns_gui/**.

6. Une fois toutes les modifications de personnalisation terminées, à l'invite, entrez : **tar —cvzf /var/ns_gui_custom/customtheme.tar.gz /var/ns_gui_custom/ns_gui/***

> **Important**
>
> Lorsque vous copiez un répertoire de thème au cours des étapes précédentes, le nom du dossier copié doit être saisi exactement sous la forme « Personnalisé » car les noms de répertoires font la distinction entre majuscules et minuscules dans l'interface shell NetScaler. Si le nom du répertoire n'est pas entré avec précision, le dossier n'est pas reconnu lorsque le paramètre **UITHEME** est configuré **sur CUSTOM**.

Sélectionnez le thème personnalisé en tant que paramètre global VPN

Une fois que la configuration du portail personnalisée manuellement est terminée et copiée dans le système de fichiers NetScaler, elle doit être appliquée à la configuration de NetScaler Gateway. Cela se fait en définissant le paramètre UITHEME sur CUSTOM et peut être complété à l'aide de la ligne de commande ou de l'utilitaire de configuration.

Pour utiliser la ligne de commande, entrez la commande suivante pour définir le paramètre **UITHEME**.

```
set vpn parameter UITHEME CUSTOM
<!--NeedCopy-->
```

Pour définir le paramètre UITHEME à l'aide de l'utilitaire de configuration, procédez comme suit.

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway**> Paramètres généraux.
2. Cliquez sur **Modifier les paramètres globaux**.
3. Cliquez sur l'onglet **Expérience client** .
4. Faites défiler l'écran jusqu'au bas de l'écran, puis sélectionnez **PERSONNALISÉ** dans le menu de la liste **Thème de l'interface utilisateur**.
5. Cliquez sur **OK**.

Votre portail personnalisé manuellement est désormais la conception du portail présentée aux utilisateurs de VPN.

Créer un CLUF

Le système de portail VPN offre la possibilité d'appliquer un CLUF à une configuration de portail. Une fois qu'un CLUF est lié à la configuration de NetScaler Gateway, soit au niveau mondial du VPN, soit à un serveur virtuel VPN approprié, les utilisateurs du VPN doivent accepter le CLUF en tant que termes et conditions avant d'être autorisés à s'authentifier auprès du VPN.

Comme pour les thèmes du portail, les utilisateurs bénéficient d'un CLUF spécifique à la langue en fonction des paramètres régionaux signalés par leur navigateur Web. Dans le cas d'un paramètre régional qui ne correspond à aucune des langues prises en charge, la langue utilisée par défaut est l'anglais. Pour chaque CLUF, vous pouvez entrer un message personnalisé dans chacune des langues prises en charge. Le contenu pré-traduit n'est pas fourni pour les configurations de CLUF, comme c'est le cas pour les thèmes du portail. Si les paramètres régionaux signalés par un utilisateur correspondent à une langue dans laquelle aucun contenu CLUF n'est entré, une page vide est renvoyée à l'utilisateur lorsqu'il clique sur le lien « Conditions générales » sur la page de connexion VPN.

Pour créer un CLUF, vous pouvez utiliser l'une des commandes de l'utilitaire de configuration sous l'onglet **Configuration** de **NetScaler Gateway > Paramètres globaux > CLUF ou**NetScaler**Gateway > Ressources > CLUF**. Les contrôles du volet **Paramètres globaux** sont utilisés pour gérer les liaisons

de CLUF globales VPN tandis que le contrôle du nœud **Ressources > CLUF** est destiné aux opérations générales sur les configurations de CLUF. Vous pouvez gérer les liaisons EULA d'un serveur virtuel VPN en modifiant un serveur virtuel VPN dans **NetScaler Gateway** > Serveurs virtuels. Certaines commandes sont également disponibles avec la ligne de commande pour gérer les entités CLUF. Toutefois, les contrôles complets de gestion du CLUF sont disponibles uniquement dans l'utilitaire de configuration.

Créer une entité CLUF à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
add vpn eula <name>
<!--NeedCopy-->
```

Créer une entité CLUF à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Ressources > CLUF**.
2. Cliquez sur **Ajouter** pour créer une entité.
3. Entrez le nom de l'entité.
4. Pour chacune des langues, collez le contenu sous les onglets correspondants. Vous pouvez utiliser du texte brut ou des balises HTML pour mettre en forme le contenu, y compris une < br> balise pour ajouter des sauts de ligne.
5. Cliquez sur **Créer**.

Une fois qu'une entité CLUF a été créée, elle peut être globalement liée à la configuration VPN ou à un serveur virtuel VPN.

Liez un CLUF à VPN global à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
bind vpn global eula <name>
<!--NeedCopy-->
```

Liez un CLUF à VPN global à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway**> Paramètres généraux.
2. Dans le volet de détails principal, cliquez sur **Configurer un contrat de licence d'utilisateur final**.
3. Cliquez sur **Add Binding**.

4. Cliquez **sur Cliquez pour sélectionner**.
5. Sélectionnez une entité CLUF, puis cliquez sur **Sélectionner**.
6. Cliquez sur **Bind**.
7. Cliquez sur **Fermer**.

Liez un CLUF à un serveur virtuel VPN à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez ;

```
bind vpn vserver <name> eula <name>
<!--NeedCopy-->
```

Liez un CLUF à un serveur virtuel VPN à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway**> Virtual Servers.
2. Dans le volet de détails principal, sélectionnez un serveur virtuel VPN et cliquez sur **Modifier**.
3. Dans le volet **Paramètres avancés** sur le côté droit de la page, cliquez sur **CLUF**.
4. Dans le volet CLUF récemment ajouté, cliquez sur **Aucun CLUF**.
5. `Click` **Cliquez pour sélectionner**.
6. Sélectionnez une entité CLUF, puis cliquez sur **Sélectionner**.
7. Cliquez sur **Bind**.
8. Cliquez sur **Terminé**.

Inviter les utilisateurs à mettre à niveau des navigateurs plus anciens ou non pris en charge en créant une page personnalisée

January 26, 2024

Si un client se connecte à une adresse VIP NetScaler à l'aide d'un chiffrement non sécurisé tel que SSLv3, il peut être redirigé vers une page personnalisée l'invitant à effectuer une mise à niveau vers la dernière version d'Internet Explorer, Firefox, Chrome ou Safari.

Remarque : Selon la RFC6176 de l'Internet Engineering Task Force (ITEF), les serveurs TLS ne doivent pas prendre en charge SSLv2. Par conséquent, le dispositif NetScaler ne prend pas en charge SSLv2 à partir de la version 12.1 et ultérieure.

Comment créer une page personnalisée pour inviter les utilisateurs à mettre à niveau les anciens navigateurs non pris en charge en fonction du protocole SSL

- Créez une stratégie de répondeur NetScaler avec la règle `client.ssl.version.eq()`. La version renvoie la version du protocole SSL.
  - Renvoie 0 si la transaction n'est pas basée sur SSL.
  - Renvoie 0x002 si la transaction est SSLv2.
  - Renvoie 0x300 si la transaction est SSLv3.
  - Renvoie 0x301 si la transaction est TLSv1.
- Vous devez activer SSLv3 (ou une autre version antérieure) pour déclencher la stratégie de répondeur.

  Par exemple, si SSLv3 est désactivé sur le dispositif NetScaler et qu'un client avec un navigateur plus ancien utilisant SSLv3 tente de se connecter, l'accès est refusé.
- Si votre déploiement nécessite SSLv3 ou une version antérieure pendant une période spécifiée (un mois ou deux), configurez les éléments suivants :
  - Activez le protocole SSLv3.
  - Mettez à jour la page personnalisée pour inclure des informations indiquant qu'après la période spécifiée, le navigateur ne peut pas se connecter à l'appliance.

Configurer l'accès VPN sans client avec NetScaler Gateway

March 27, 2024

L'accès sans client fournit aux utilisateurs l'accès dont ils ont besoin sans qu'ils aient à installer de logiciel utilisateur, tel que le client Citrix Secure Access ou Receiver. Les utilisateurs peuvent utiliser leur navigateur Web pour se connecter à des applications Web, telles qu'Outlook Web Access.

Pour configurer l'accès sans client, procédez comme suit :

- Activation de l'accès sans client soit globalement, soit à l'aide d'une stratégie de session liée à un utilisateur, un groupe ou un serveur virtuel.
- Sélection de la méthode de codage des adresses Web.

Pour activer l'accès sans client uniquement pour un serveur virtuel spécifique, désactivez l'accès sans client globalement, puis créez une stratégie de session pour l'activer.

Si vous utilisez l'assistant NetScaler Gateway pour configurer l'appliance, vous avez le choix de configurer l'accès sans client dans l'assistant. Les paramètres de l'assistant sont appliqués globalement.

Dans l'assistant NetScaler Gateway, vous pouvez configurer les méthodes de connexion client suivantes :

- Client Citrix Secure Access. Les utilisateurs sont autorisés à se connecter à l'aide du client Citrix Secure Access uniquement.
- Utilisez le client Citrix Secure Access et autorisez le scénario d'accès de secours. Les utilisateurs se connectent à NetScaler Gateway avec le client Citrix Secure Access. Si la machine utilisateur échoue à une analyse d'analyse des points de terminaison, les utilisateurs sont autorisés à ouvrir une session à l'aide d'un accès sans client. Dans ce cas, les utilisateurs ont un accès limité aux ressources réseau.
- Autorisez les utilisateurs à ouvrir une session à l'aide d'un navigateur Web et d'un accès sans client. Les utilisateurs peuvent ouvrir une session uniquement en utilisant un accès sans client et bénéficier d'un accès limité aux ressources réseau.

Fonctionnement des stratégies d'accès VPN sans client

Vous configurez l'accès sans client aux applications Web en créant des stratégies. Vous pouvez configurer les paramètres d'une stratégie d'accès sans client dans l'utilitaire de configuration. Une stratégie d'accès sans client est composée d'une règle et d'un profil. Vous pouvez utiliser les stratégies d'accès sans client préconfigurées fournies avec NetScaler Gateway. Vous pouvez également créer vos propres stratégies d'accès sans client personnalisées.

NetScaler Gateway fournit des stratégies préconfigurées pour les éléments suivants :

- Outlook Web Access et Outlook Web App
- SharePoint 2007
- Toutes les autres applications Web

> **Remarque :**
>
> OWA 2016 et SharePoint 2016 sont pris en charge uniquement à l'aide d'un accès sans client avancé.

Gardez à l'esprit les caractéristiques suivantes des stratégies d'accès sans client préconfigurées :

- Ils sont configurés automatiquement et ne peuvent pas être modifiés.
- Chaque stratégie est liée au niveau mondial.
- Chaque stratégie n'est pas appliquée, sauf si vous activez l'accès sans client soit globalement, soit en créant une stratégie de session.
- Vous ne pouvez pas supprimer ou modifier les liaisons globales, même si vous n'activez pas l'accès sans client.

La prise en charge des autres applications Web dépend des stratégies de réécriture que vous configurez sur NetScaler Gateway. Citrix recommande de tester toutes les stratégies personnalisées que vous créez pour garantir que tous les composants de l'application se réécrivent correctement.

Si vous autorisez les connexions depuis Receiver pour Android, Receiver pour iOS ou Citrix Secure Hub, vous devez activer l'accès sans client. Pour Citrix Secure Hub qui s'exécute sur un appareil iOS, vous devez également activer la Secure Browse dans le profil de session. La Secure Browse et l'accès sans client fonctionnent ensemble pour permettre les connexions à partir d'appareils iOS. Il n'est pas nécessaire d'activer la Secure Browse si les utilisateurs ne se connectent pas à des appareils iOS.

L'assistant de configuration rapide configure les stratégies et paramètres d'accès sans client corrects pour les appareils mobiles. Citrix recommande d'exécuter l'assistant de configuration rapide pour configurer les stratégies appropriées pour les connexions à StoreFront et Citrix Endpoint Management.

Vous pouvez lier des stratégies d'accès sans client personnalisées globalement ou à un serveur virtuel. Si vous souhaitez lier des stratégies d'accès sans client à un serveur virtuel, vous devez créer une stratégie personnalisée, puis la lier. Pour appliquer différentes stratégies d'accès sans client globalement ou pour un serveur virtuel, modifiez le numéro de priorité de la stratégie personnalisée afin qu'elle ait un nombre inférieur à celui des stratégies préconfigurées, ce qui donne à la stratégie personnalisée une priorité plus élevée. Si aucune autre stratégie d'accès sans client n'est liée au serveur virtuel, les stratégies globales préconfigurées sont prioritaires.

> **Remarque :**
>
> Vous ne pouvez pas modifier les numéros de priorité des stratégies d'accès sans client préconfigurées.

Activer l'accès VPN sans client

Lorsque vous activez l'accès sans client au niveau global, tous les utilisateurs reçoivent les paramètres de l'accès sans client. Vous pouvez utiliser l'assistant NetScaler Gateway, une stratégie globale ou une stratégie de session pour activer l'accès sans client.

Dans un paramètre global ou un profil de session, l'accès sans client comporte les paramètres suivants :

- **Sur**. Permet un accès sans client. Si vous désactivez les choix des clients et que vous ne configurez pas ou ne désactivez pas StoreFront, les utilisateurs ouvrent une session en utilisant un accès sans client.
- **Désactivé**. L'accès sans client n'est pas activé par défaut. L'accès sans client est activé une fois que les utilisateurs se connectent avec le client Citrix Secure Access. Si vous désactivez les choix du client et que vous ne configurez ni ne désactivez StoreFront, les utilisateurs ouvrent une session avec le client Citrix Secure Access. Si l'analyse des points de terminaison échoue

lorsque les utilisateurs ouvrent une session, les utilisateurs reçoivent la page de choix avec un accès sans client disponible.

- **Désactivé**. L'accès sans client est désactivé. Lorsque vous sélectionnez **Désactivé**, les utilisateurs ne peuvent pas ouvrir de session à l'aide de l'accès sans client et l'icône d'accès sans client n'apparaît pas sur la page de choix.

Si vous n'activez pas l'accès sans client à l'aide de l'assistant NetScaler Gateway, vous pouvez l'activer globalement ou dans une stratégie de session à l'aide de l'utilitaire de configuration.

Pour activer l'accès sans client à l'échelle mondiale

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Expérience client**, en regard de **Accès sans client**, sélectionnez ACTIVÉ,**** puis cliquez sur **OK**.

Pour activer l'accès sans client à l'aide d'une stratégie de session

Si vous souhaitez qu'un groupe restreint d'utilisateurs, de groupes ou de serveurs virtuels utilise l'accès sans client, désactivez ou effacez l'accès sans client à l'échelle mondiale. Ensuite, à l'aide d'une stratégie de session, activez l'accès sans client et liez-le à des utilisateurs, des groupes ou des serveurs virtuels.

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**Session.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, à côté de Clientless Access, cliquez **sur**Override Global**, sélectionnez Activé,** puis cliquez sur **Créer**.
7. Dans la boîte de dialogue **Créer une politique de session**, à côté de **Expressions nommées**, sélectionnez Général, sélectionnez Valeur vraie, cliquez sur Ajouter une expression, sur **Créer,** puis sur **Fermer**.
8. Cliquez sur **Créer,** puis sur **Fermer**.

Après avoir créé la stratégie de session qui autorise l'accès sans client, vous la liez à un utilisateur, un groupe ou un serveur virtuel.

Encodez l'adresse Web

Lorsque vous activez l'accès sans client, vous pouvez choisir d'encoder les adresses des applications Web internes ou de laisser l'adresse en texte clair. Les paramètres sont les suivants :

- Obscure. Cela utilise des mécanismes de codage standard pour masquer la partie domaine et protocole de la ressource.
- Transparent. L'adresse Web n'est pas codée et est visible par les utilisateurs.
- Crypter. Le domaine et le protocole sont chiffrés à l'aide d'une clé de session. Lorsque l'adresse Web est chiffrée, l'URL est différente pour chaque session utilisateur de la même ressource Web. Si les utilisateurs mettent l'adresse Web codée dans un signet, l'enregistrent dans le navigateur Web, puis se déconnectent. Lorsque les utilisateurs ouvrent une session et tentent de se connecter à nouveau à l'adresse Web à l'aide du signet, ils ne peuvent pas se connecter à l'adresse Web.
  Remarque : Si les utilisateurs enregistrent le signet chiffré dans l'interface d'accès au cours de leur session, le signet fonctionne chaque fois que l'utilisateur ouvre une session.

Vous pouvez configurer ce paramètre globalement ou dans le cadre d'une stratégie de session. Si vous configurez le codage dans le cadre de la stratégie de session, vous pouvez le lier aux utilisateurs, aux groupes ou à un serveur virtuel.

Configurer l'encodage des adresses Web globalement

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Expérience client, en regard de Codage d'URL d'accès sans client, sélectionnez le niveau de codage, puis cliquez sur OK.

Configurez le codage des adresses Web en créant une stratégie de session

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Session.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Demander un profil, cliquez sur Nouveau.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet Expérience client, à côté de Codage de l'URL d'accès sans client, cliquez sur Override Global, sélectionnez le niveau de codage, puis cliquez sur OK.

7. Dans la boîte de dialogue Créer une politique de session, à côté de Expressions nommées, sélectionnez Général, sélectionnez Valeur vraie, cliquez sur Ajouter une expression, sur Créer, puis sur Fermer.

Créer des stratégies d'accès sans client

Si vous souhaitez utiliser les mêmes paramètres que pour les stratégies d'accès sans client par défaut, mais que vous souhaitez lier la stratégie à un serveur virtuel, vous pouvez copier les stratégies par défaut en fournissant un nouveau nom pour la stratégie. Vous pouvez utiliser l'utilitaire de configuration pour copier les stratégies par défaut.

Après avoir lié la nouvelle stratégie au serveur virtuel, vous pouvez définir la priorité de la stratégie de sorte qu'elle s'exécute en premier lorsqu'un utilisateur ouvre une session.

Créer une stratégie d'accès sans client à l'aide des paramètres par défaut

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Clientless Access.
2. Dans le volet d'informations, sous l'onglet Stratégies, cliquez sur une stratégie par défaut, puis sur Ajouter.
3. Dans Nom, tapez un nouveau nom pour la stratégie, cliquez sur Créer, puis cliquez sur Fermer.

Liaison d'une stratégie d'accès sans client à un serveur virtuel

Après avoir créé la stratégie, liez-la au serveur virtuel.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue de configuration du serveur virtuel NetScaler Gateway, cliquez sur l'onglet Stratégies, puis sur Clientless.
4. Cliquez sur Insérer une stratégie, sélectionnez une stratégie dans la liste, puis cliquez sur OK.

Créer et évaluer des expressions de stratégie d'accès sans client

Lorsque vous créez une stratégie d'accès sans client, vous pouvez créer votre propre expression pour la stratégie. Lorsque vous avez fini de créer l'expression, vous pouvez ensuite évaluer la précision de l'expression.

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Clientless Access.
2. Dans le volet d'informations, sous l'onglet Stratégies, cliquez sur une stratégie par défaut, puis sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Profil, cliquez sur Nouveau.
5. Dans Nom, saisissez le nom du profil.
6. Configurez les paramètres de réécriture, puis cliquez sur Créer.
7. Dans la boîte de dialogue Créer une stratégie d'accès sans client, sous Expression, cliquez sur Ajouter.
8. Dans la boîte de dialogue Ajouter une expression, créez l'expression, puis cliquez sur OK.
9. Dans la boîte de dialogue Créer une stratégie d'accès sans client, cliquez sur Evaluer, et si l'expression est correcte, cliquez sur Créer.

Accès VPN sans client avancé avec NetScaler Gateway

March 27, 2024

Le VPN sans client permet de fournir un accès à distance aux ressources intranet de l'entreprise via NetScaler Gateway sans application cliente VPN sur la machine cliente. Le VPN sans client fournit un accès à distance aux applications Web d'entreprise, aux portails et à d'autres ressources à l'aide d'un navigateur Web du côté du client.
La solution VPN sans client avancée élimine les limitations suivantes relatives au VPN sans client :

- Les URL relatives ne peuvent pas être identifiées à certains moments.
- Les URL relatives générées dynamiquement ne peuvent pas être identifiées.

Le VPN sans client avancé identifie l'URL absolue et les noms d'hôte et les réécrit d'une manière nouvelle et unique au lieu d'essayer de réécrire les URL relatives présentes dans les réponses HTTP/pages Web. SharePoint n'a plus besoin d'utiliser le dossier par défaut pour réécrire les URL et un accès SharePoint personnalisé est pris en charge.

Pré-requis

Voici les conditions préalables à la configuration du VPN sans client avancé.

- **Certificat de serveur Wildcard** - Le VPN avancé sans client réécrit les URL d'une manière unique. Ce caractère unique est maintenu pour chaque URL par utilisateur. Par exemple, si l'application Web est hébergée sur `https://webapp.customer.com`et que le serveur

virtuel VPN est hébergé sur,`https://vpn.customer.com` le VPN sans client avancé la réécrit en tant que `https://cvpneqwerty.vpn.customer.com`. Cela signifie que chaque URL est réécrite en tant que sous-domaine du serveur virtuel VPN. Dans cette nouvelle URL, `cvpneqwerty` peut être déchiffré vers `https://webapp.customer.com`. La chaîne `cvpneqwerty` est dynamique et, par conséquent, pour SSL, vous devez lier le serveur virtuel VPN avec un certificat générique.

Si le serveur est hébergé avec,`https://vpn.customer.com` le certificat de serveur doit maintenant comporter des entrées pour (vpn.customer.com et .vpn.customer.com) dans le cadre des certificats CN ou SAN (où CN=nom commun, SAN = Subject Alternative Name). Le processus de liaison de ce certificat reste le même sur NetScaler Gateway.
Remarque : les certificats génériques ne prennent en charge qu'un seul niveau (c'est-à-dire ..customer.com n'est pas autorisé). Si vous utilisez déjà un certificat Wildcard (pour *.customer.com) et un hébergement,`https://vpn.customer.com` cela ne fonctionne pas pour le VPN sans client avancé. Vous devez obtenir un nouveau certificat avec `*.vpn.customer.com`.

- **Entrée DNS WildCard** - Les clients (navigateurs Web) doivent résoudre le nom de domaine complet de l'application VPN sans client avancée. Lors de la configuration du serveur NetScaler Gateway, vous devez avoir configuré une entrée DNS pour résoudre vpn.customer.com. Cela permet au navigateur de résoudre vpn.customer.com en l'adresse IP de votre serveur virtuel VPN. Pour résoudre des URL similaires `https://cvpnqwerty.vpn.customer.com` à la même adresse IP (adresse IP du serveur virtuel VPN), vous devez ajouter un nouvel enregistrement pour le domaine de `vpn.customer.com`. Recherchez le paramètre de domaine sur votre serveur DNS et ajoutez un nouvel enregistrement d'hôte pour « * » avec la même adresse IP qu'auparavant. Après avoir ajouté l'enregistrement d'hôte, vous devez voir les réponses ping réussies pour `https://cpvnanything.vpn.customer.com`.

Configuration de l'accès VPN sans client avancé

Pour configurer l'accès VPN sans client avancé à l'aide de l'interface de ligne de commande, à l'invite de commande, tapez :

```
set vpn parameter -clientlessVpnMode ON
set vpn parameter -advancedClientlessVpnMode ENABLED
<!--NeedCopy-->
```

Si une action de session est liée au serveur virtuel, vous devez également activer l'option Mode VPN sans client avancé pour cette action de session.

Exemple :

```
set vpn sessionaction SessionActionName -advancedclientlessvpn ENABLED
<!--NeedCopy-->
```


Pour configurer un accès VPN sans client avancé à l'aide de l'interface graphique NetScaler :

1. Dans l'interface graphique de NetScaler, accédez à **Configuration > NetScaler**Paramètres généraux.
2. Sur la **page Paramètres** généraux, cliquez sur **Modifier les paramètres** généraux, puis sélectionnez l'onglet **Expérience client** .
3. Dans l'onglet **Expérience client**, dans la liste **Accès sans client**, cliquez **sur On**.
4. Dans l'onglet **Expérience client**, dans la liste **Mode VPN sans client avancé**, cliquez sur **Activé**.
   Si vous sélectionnez **STRICT** dans la liste du **mode VPN sans client avancé**, l'appliance NetScaler répond uniquement aux URL StoreFront sous forme de VPN sans client classique et bloque toutes les autres demandes VPN sans client classiques. Cette option fournit une configuration plus sécurisée sur l'appliance pour la mise à disposition de ressources Web internes.

> **Remarque :**
>
> - Si une action de session est liée au serveur virtuel, vous devez également activer l'option **Mode VPN sans client avancé** pour cette action de session depuis l'onglet **Expérience client** de la page **Configurer le profil de session NetScaler Gateway**.
> - Vous pouvez sélectionner l'option **Remplacer le paramètre global** pour remplacer les paramètres globaux.
> - Vous pouvez également configurer la fonctionnalité VPN sans client avancée au niveau de la session.

mises en garde

Le VPN sans client avancé vise à fournir un accès aux applications Web d'entreprise. Ces applications n'ont qu'un seul nom de domaine complet pour chaque type de ressource dont elles ont besoin (JavaScript, css, images, etc.). Comme nous encodons le nom de domaine complet des applications internes dans un seul octet (VPN sans client), nous perdons la relation de sous-domaine. Par conséquent, chaque fois qu'une application Web d'entreprise est configurée avec CORS, vous remarquerez parfois des problèmes lors de l'accès via le VPN sans client avancé.

Configuration de l'accès au domaine pour les utilisateurs

January 26, 2024

Si les utilisateurs se connectent en utilisant un accès sans client, vous pouvez restreindre les ressources réseau, les domaines et les sites Web auxquels les utilisateurs sont autorisés à accéder. Vous pouvez utiliser l'assistant NetScaler Gateway ou les paramètres globaux pour créer des listes permettant d'inclure ou d'exclure l'accès à des domaines.

Vous pouvez autoriser l'accès à toutes les ressources réseau, domaines et sites Web, puis créer une liste d'exclusion. La liste d'exclusion cite un ensemble spécifique de ressources auxquelles les utilisateurs ne sont pas autorisés à accéder. Les utilisateurs ne peuvent pas accéder aux domaines figurant dans la liste d'exclusion.

Vous pouvez également refuser l'accès à toutes les ressources réseau, domaines et sites Web, puis créer une liste d'inclusion spécifique. La liste d'inclusion cite les ressources auxquelles les utilisateurs peuvent accéder. Les utilisateurs ne peuvent accéder à aucun domaine qui n'apparaît pas dans la liste.

Remarque : Si vous configurez des stratégies d'accès sans client pour Citrix Endpoint Management ou StoreFront et que les utilisateurs se connectent à Receiver pour Web, vous devez autoriser les domaines auxquels Receiver pour Web peut accéder. Cela est nécessaire pour que NetScaler Gateway puisse réécrire le trafic réseau pour StoreFront et Endpoint Management.

Pour configurer l'accès au domaine à l'aide de l'assistant NetScaler Gateway

1. Dans l'utilitaire de configuration, cliquez sur l'onglet Configuration, puis dans le volet de navigation, cliquez sur NetScaler Gateway.
2. Dans le volet d'informations, sous Getting Started, cliquez sur l'assistant NetScaler Gateway.
3. Cliquez sur Suivant, puis suivez les instructions de l'assistant jusqu'à ce que vous atteigniez la page Configurer l'accès sans client.
4. Cliquez sur Configurer les domaines pour l'accès sans client et effectuez l'une des opérations suivantes :
    - Pour créer une liste des domaines exclus, cliquez sur Exclure les domaines.
    - Pour créer une liste des domaines inclus, cliquez sur Autoriser les domaines.
5. Sous Noms de domaine, tapez le nom de domaine, puis cliquez sur Ajouter.
6. Répétez l'étape 5 pour chaque domaine que vous souhaitez ajouter à la liste, puis cliquez sur OK lorsque vous avez terminé.
7. Continuez à configurer l'appliance à l'aide de l'assistant NetScaler Gateway.

Pour configurer les paramètres de domaine à l'aide de l'utilitaire de configuration

Vous pouvez également créer ou modifier la liste des domaines en utilisant les paramètres globaux de l'utilitaire de configuration.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet de détails, sous Accès sans client, cliquez sur Configurer les domaines pour l'accès sans client.
3. Procédez comme suit :
    - Pour créer une liste des domaines exclus, cliquez sur Exclure les domaines.
    - Pour créer une liste des domaines inclus, cliquez sur Autoriser les domaines.
4. Sous Noms de domaine, tapez le nom de domaine, puis cliquez sur Ajouter.
5. Répétez l'étape 4 pour chaque domaine que vous souhaitez ajouter à la liste, puis cliquez sur OK lorsque vous avez terminé.

Accès VPN sans client pour SharePoint 2003, SharePoint 2007 et SharePoint 2013

March 27, 2024

NetScaler Gateway peut réécrire le contenu d'un ou de plusieurs sites SharePoint 2003, SharePoint 2007 ou SharePoint 2013 afin que le contenu soit disponible pour les utilisateurs sans avoir besoin du client Citrix Secure Access. Pour que le processus de réécriture aboutisse, vous devez configurer NetScaler Gateway avec le nom d'hôte de chaque serveur SharePoint de votre réseau.

Vous pouvez utiliser l'assistant NetScaler Gateway ou l'utilitaire de configuration pour configurer le nom d'hôte des sites SharePoint.

Dans l'assistant NetScaler Gateway, parcourez l'assistant pour configurer vos paramètres. Lorsque vous accédez à la page Configurer l'accès sans client, tapez l'adresse Web du site SharePoint, puis cliquez sur **Ajouter**.

Pour ajouter d'autres sites Web ou pour configurer SharePoint pour la première fois après avoir exécuté l'assistant NetScaler Gateway, vous utilisez l'utilitaire de configuration.

> **Important :**
>
> Classic Clientless Access prend en charge les versions allant jusqu'à SharePoint 2013 et OWA 2013. Advanced Clientless Access prend en charge SharePoint 2016 et OWA 2016, ainsi que les versions ultérieures.

Configurer l'accès sans client pour SharePoint à l'aide de l'interface graphique NetScaler

1. Accédez à **NetScaler Gateway** > **Paramètres généraux**.
2. Dans le volet d'informations, sous Accès sans client, cliquez sur **Configurer l'accès sans client pour SharePoint**.
3. Sous Accès sans client pour SharePoint, dans Nom d'hôte du serveur SharePoint, tapez le nom d'hôte du site SharePoint, puis cliquez sur **Ajouter**.
4. Répétez l'étape 3 pour chaque site SharePoint que vous souhaitez ajouter à la liste, puis cliquez sur **OK** lorsque vous avez terminé.

Définir un site SharePoint en tant que page d'accueil

Si vous souhaitez définir un site SharePoint comme page d'accueil des utilisateurs, configurez un profil de session et entrez le nom d'hôte du site SharePoint.

Pour configurer un site SharePoint en tant que page d'accueil

1. Accédez à **NetScaler Gateway > Policies**, puis cliquez sur **Session**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet Expérience client, en regard de Page d'accueil, cliquez sur **Remplacer la valeur globale,** puis tapez le nom du site SharePoint.
7. En regard de Accès sans client, cliquez sur **Override Global**, sélectionnez **On,** puis cliquez sur **Create**.
8. Dans la boîte de dialogue Créer une politique de session, à côté de Expressions nommées, sélectionnez **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Une fois la stratégie de session terminée, liez-la aux utilisateurs, aux groupes, aux serveurs virtuels ou globalement. Lorsque les utilisateurs ouvrent une session, ils voient le site Web SharePoint comme page d'accueil.

Activer la résolution des noms pour les serveurs SharePoint 2007

Les serveurs SharePoint 2007 envoient le nom du serveur configuré en tant que nom d'hôte dans diverses URL dans le cadre de la réponse. Si le nom d'un serveur SharePoint configuré n'est pas le nom

de domaine complet (FQDN), NetScaler Gateway ne peut pas résoudre l'adresse IP à l'aide du nom du serveur SharePoint et certaines fonctions utilisateur expirent avec le message d'erreur « HTTP/1.1 Gateway Time-out ». Ces fonctions peuvent inclure l'archivage et la sortie de fichiers, l'affichage de l'espace de travail et le téléchargement de plusieurs fichiers lorsque les utilisateurs sont connectés à l'aide d'un accès sans client.

Pour résoudre ce problème, vous pouvez essayer l'une des solutions suivantes :

- Configurez un suffixe DNS sur NetScaler Gateway afin que le nom d'hôte SharePoint soit converti en FQDN avant la résolution du nom.
- Configurez une entrée DNS locale sur NetScaler Gateway pour chaque nom de serveur SharePoint.
- Modifiez tous les noms de serveurs SharePoint pour utiliser le nom de domaine complet, tel que SharePoint.IntranetDomain au lieu de SharePoint,

Configurer un suffixe DNS

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **DNS**, puis cliquez sur **Suffixe DNS**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Suffixe DNS**, tapez le nom de domaine intranet comme suffixe, cliquez sur **Créer**, puis cliquez sur **Fermer**.

Vous pouvez répéter l'étape 3 pour chaque domaine que vous souhaitez ajouter.

Pour configurer un enregistrement DNS local pour chaque nom de serveur SharePoint sur NetScaler Gateway

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **DNS > Enregistrements**, puis cliquez sur **Enregistrements d'adresses**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom d'hôte**, tapez le nom d'hôte SharePoint pour l'enregistrement d'adresse DNS.
4. Dans **Adresse IP**, tapez l'adresse IP du serveur SharePoint, cliquez sur **Ajouter**, sur **Créer**, puis sur **Fermer**.

Le nom d'hôte pour lequel un enregistrement A est ajouté ne doit pas comporter d'enregistrement CNAME. De plus, il ne peut pas y avoir d'enregistrements A en double sur l'appliance.

Activer les cookies persistants d'accès VPN sans client

March 27, 2024

Les cookies persistants sont nécessaires pour accéder à certaines fonctionnalités de SharePoint, telles que l'ouverture et la modification de documents Microsoft Word, Excel et PowerPoint hébergés sur le serveur SharePoint.

Un cookie persistant reste sur la machine utilisateur et est envoyé avec chaque demande HTTP. NetScaler Gateway chiffre le cookie persistant avant de l'envoyer au plug-in sur la machine utilisateur et actualise le cookie régulièrement tant que la session existe. Le cookie devient obsolète à la fin de la session.

Dans l'assistant NetScaler Gateway, les administrateurs peuvent activer les cookies persistants à l'échelle mondiale. Vous pouvez également créer une stratégie de session pour activer les cookies persistants par utilisateur, groupe ou serveur virtuel.

Les options suivantes sont disponibles pour les cookies persistants :

- Autoriser active les cookies persistants et les utilisateurs peuvent ouvrir et modifier les documents Microsoft stockés dans SharePoint.
- Refuser désactive les cookies persistants et les utilisateurs ne peuvent pas ouvrir ni modifier les documents Microsoft stockés dans SharePoint.
- L'invite invite les utilisateurs à autoriser ou à refuser les cookies persistants pendant la session.

Les cookies persistants ne sont pas nécessaires pour un accès sans client si les utilisateurs ne se connectent pas à SharePoint.

Configuration des cookies persistants pour l'accès VPN sans client pour SharePoint

Vous pouvez configurer des cookies persistants pour un accès sans client à SharePoint, soit globalement, soit dans le cadre d'une stratégie de session.

Pour configurer les cookies persistants globalement

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Expérience client, en regard de Cookies persistants d'accès sans client, sélectionnez une option, puis cliquez sur OK.

Pour configurer les cookies persistants dans le cadre d'une stratégie de session

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Session.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Demander un profil, cliquez sur Nouveau.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet Expérience client, en regard de Cookies persistants d'accès sans client, cliquez sur Remplacer Global, sélectionnez une option, puis cliquez sur Créer.
7. Dans la boîte de dialogue Créer une stratégie d'authentification, en regard de Expressions nommées, sélectionnez Général, sélectionnez Valeur vraie, cliquez sur Ajouter une expression, cliquez sur Créer, puis sur Fermer.

Client VPN Citrix SSO pour appareils mobiles

January 26, 2024

Citrix SSO est le client VPN pour les appareils mobiles (macOS, iOS et iOS). Citrix SSO fournit une prise en charge complète de la gestion des appareils mobiles (MDM) sur macOS, iOS et Android. Avec un serveur MDM, un administrateur peut configurer et gérer à distance des profils VPN au niveau de l'appareil et des profils VPN par application.
Citrix SSO prend également en charge la plupart des fonctionnalités couramment utilisées.

Références

- Client Citrix Secure Access
- Clients VPN NetScaler Gateway et fonctionnalités prises en charge

Configurer la page Choix du client

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour fournir aux utilisateurs plusieurs options d'ouverture de session. En configurant la page des choix du client, les utilisateurs ont la possibilité de se connecter à partir d'un emplacement unique avec les options suivantes :

- Client Citrix Secure Access pour Windows
- Client Citrix Secure Access pour macOS X
- StoreFront
- Interface Web
- Accès sans client

Les utilisateurs se connectent à NetScaler Gateway à l'aide de l'adresse Web figurant dans le certificat lié à NetScaler Gateway ou au serveur virtuel. En créant une stratégie de session et un profil, vous pouvez déterminer les choix d'ouverture de session reçus par les utilisateurs. Selon la façon dont vous configurez NetScaler Gateway, la page des choix du client affiche jusqu'à trois icônes représentant les choix d'ouverture de session suivants :

- Accès réseau. Lorsque les utilisateurs se connectent à NetScaler Gateway pour la première fois à l'aide d'un navigateur Web, puis qu'ils sélectionnent Accès réseau, la page de téléchargement s'affiche. Lorsque les utilisateurs cliquent sur Télécharger, le plug-in est téléchargé et installé sur la machine utilisateur. Lorsque le téléchargement et l'installation sont terminés, l'interface d'accès apparaît. Si vous installez une version plus récente ou si vous revenez à une ancienne version de NetScaler Gateway, le client Citrix Secure Access pour Windows passe en mode silencieux à la version de l'appliance. Si les utilisateurs se connectent à l'aide du client Citrix Secure Access pour Mac, le plug-in est mis à niveau silencieusement si une nouvelle version de l'appliance est détectée lorsque les utilisateurs ouvrent une session. Cette version du plug-in n'est pas rétrogradée en mode silencieux.
- Interface Web ou StoreFront. Si les utilisateurs sélectionnent l'interface Web pour ouvrir une session, la page Interface Web apparaît. Les utilisateurs peuvent ensuite accéder à leurs applications publiées ou à leurs bureaux virtuels. Si les utilisateurs sélectionnent StoreFront pour ouvrir une session, Receiver s'ouvre et les utilisateurs peuvent accéder aux applications et aux bureaux.
  Remarque : Si vous configurez StoreFront en tant que choix de client, les applications et bureaux n'apparaissent pas dans le volet gauche de l'interface d'accès.
- Accès sans client. Si les utilisateurs choisissent un accès sans client pour ouvrir une session, l'interface d'accès ou votre page d'accueil personnalisée apparaît. Dans l'interface d'accès, les utilisateurs peuvent accéder aux partages de fichiers, aux sites Web et utiliser Outlook Web Access.

Secure Browse permet aux utilisateurs de se connecter via NetScaler Gateway à partir d'un appareil iOS. Si vous activez la navigation sécurisée, lorsque les utilisateurs ouvrent une session à l'aide de Secure Hub, Secure Browse désactive la page des choix du client.

Afficher la page Choix du client lors de l'ouverture de session

Lorsque vous activez l'option de choix du client, les utilisateurs peuvent se connecter à l'aide du client Citrix Secure Access, de l'interface Web, de Receiver ou d'un accès sans client à partir d'une page Web après une authentification réussie auprès de NetScaler Gateway. Lorsque l'ouverture de session est réussie, des icônes apparaissent sur la page Web à partir desquelles les utilisateurs peuvent choisir la méthode d'établissement d'une connexion.

Vous pouvez activer les choix des clients sans utiliser l'analyse des points de terminaison ou la mise en œuvre d'un scénario de secours d'accès. Si vous ne définissez pas d'expression de sécurité client, les utilisateurs reçoivent des options de connexion pour les paramètres configurés sur NetScaler Gateway. Si une expression de sécurité client existe pour la session utilisateur et que l'analyse de l'analyse des points de terminaison échoue sur la machine utilisateur, la page de choix offre uniquement la possibilité d'utiliser l'interface Web si elle est configurée. Sinon, les utilisateurs peuvent utiliser un accès sans client pour ouvrir une session.

Vous configurez les choix des clients globalement ou à l'aide d'un profil de session et d'une stratégie.

> **Important :**
>
> Lorsque vous configurez les choix du client, ne configurez pas les groupes de quarantaine. Les machines utilisateur qui échouent à l'analyse des points de terminaison et sont mises en quarantaine et traitées de la même manière que les machines utilisateur qui réussissent l'analyse des points de terminaison.

Activer les options de choix client globalement

1. Dans l'interface graphique, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway,** puis cliquez sur Paramètres **généraux**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur **Modifier les paramètres** généraux.
3. Dans l'onglet Expérience client, cliquez sur **Paramètres avancés**.
4. Dans l'onglet Général, cliquez sur **Choix du client,** puis cliquez sur **OK**.

Activer les choix du client dans le cadre d'une stratégie de session

Vous pouvez également configurer les choix des clients dans le cadre d'une stratégie de session, puis les lier aux utilisateurs, aux groupes et aux serveurs virtuels.

1. Dans l'interface graphique, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Stratégies,** puis cliquez sur **Session**.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.

3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Demander un profil, cliquez sur **Nouveau**.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet Expérience client, cliquez sur **Avancé**.
7. Dans l'onglet Général, en regard de Choix du client, cliquez sur **Remplacer les options globales**, sur **Choix du client, sur OK**, puis sur**Créer**.
8. Dans la boîte de dialogue Créer une politique de session, à côté de Expressions nommées, sélectionnez **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Options de configuration des choix du client

En plus d'activer les choix des clients à l'aide d'un profil et d'une stratégie de session, vous devez configurer les paramètres du logiciel utilisateur. Par exemple, vous souhaitez que les utilisateurs se connectent via le client Citrix Secure Access, StoreFront ou l'interface Web, ou via un accès sans client. Vous créez un profil de session qui active les trois options et les choix du client. Ensuite, vous créez une stratégie de session avec l'expression définie sur la valeur True avec le profil associé. Ensuite, vous liez la stratégie de session à un serveur virtuel.

Avant de créer la stratégie et le profil de session, vous devez créer un groupe d'autorisation pour les utilisateurs.

Créer un groupe d'autorisations

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, sélectionnez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **AAA**Groups.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom du groupe**, tapez le nom du groupe.
4. Dans l'onglet **Utilisateurs**, sélectionnez les utilisateurs, cliquez sur **Ajouter** pour chacun d'eux, sur **Créer**, puis sur **Fermer**.

La procédure suivante est un exemple de profil de session pour les choix des clients avec le client Citrix Secure Access, StoreFront et l'accès sans client.

Créer un profil de session pour les choix des clients

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**Session.
2. Dans le volet d'informations, cliquez sur l'onglet **Profils**, puis sur **Ajouter**.
3. Dans **Nom**, saisissez le nom du profil.

4. Dans l'onglet **Expérience client**, procédez comme suit :
    a) À côté de la page d'accueil, cliquez sur **Remplacer le contenu global**, puis désactivez **Afficher la page d'accueil**. Cette opération désactive l'interface d'accès.
    b) En regard de **Accès sans client**, cliquez sur **Override Global**, puis sélectionnez **OFF**.
    c) En regard de **Type de plug-in**, cliquez sur **Remplacer le module global**, puis sélectionnez Windows/Mac OS X.
    d) Cliquez sur **Paramètres avancés**, puis en regard de **Choix du client**, cliquez sur **Remplacer les paramètres globaux**, puis sur **Choix du client**.
5. Dans l'onglet **Sécurité**, à côté de l'**action d'autorisation par défaut**, cliquez sur **Annuler la valeur globale**, puis sélectionnez **AUTORISER**.
6. Dans l'onglet **Sécurité**, cliquez sur **Paramètres avancés**.
7. Sous **Groupes d'autorisations**, cliquez sur **Remplacer l'**ensemble, puis sur **Ajouter**, puis sélectionnez le groupe.
8. Dans l'onglet **Applications publiées**, procédez comme suit :
    a) En regard de **Proxy ICA**, cliquez sur **Override Global**, puis sélectionnez **OFF**.
    b) À côté de **Adresse de l'interface Web**, cliquez sur **Override Global**, puis tapez l'adresse Web de StoreFront, telle que. http://ipAddress/Citrix/
    c) En regard de **Web Interface Portal Mode**, cliquez sur **Ignorer Global**, puis sélectionnez **COMPACT**.
    d) À côté de **Domaine d'authentification unique**, cliquez sur **Override Global**, puis tapez le nom du domaine.
9. Cliquez sur **Créer**, puis sur **Fermer**.

Si vous souhaitez utiliser le client Citrix Secure Access pour Java comme client de choix, dans l'onglet **Expérience client**, dans Type de plug-in, sélectionnez **Java**. Si vous sélectionnez cette option, vous devez configurer une application intranet et définir le mode d'interception sur Proxy.

Après avoir créé le profil de session, créez une stratégie de session. Dans la stratégie, sélectionnez le profil et définissez l'expression sur la valeur True.

Pour utiliser StoreFront comme choix client, vous devez également configurer la Secure Ticket Authority (STA) sur NetScaler Gateway. La STA est liée au serveur virtuel.

> **Remarque :**
>
> Si le serveur exécutant StoreFront n'est pas disponible, le choix Citrix Virtual Apps n'apparaît pas sur la page des choix.

Configurez le serveur STA globalement

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur Paramètres **généraux**.
2. Dans le volet d'informations, sous Serveurs, cliquez sur **Lind/Unbind STA Servers** à utiliser par la Secure Ticket Authority.
3. **Dans la boîte de dialogue**Lier/dissocier les serveurs STA**, cliquez sur Ajouter.**
4. Dans la boîte de dialogue **Configurer le serveur STA**, dans URL, tapez l'adresse Web du serveur STA, puis cliquez sur **Créer**.
5. Répétez les étapes 3 et 4 pour ajouter d'autres serveurs STA, puis cliquez sur **OK**.

Liez la STA à un serveur virtuel

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Virtual Servers**.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet **Applications publiées**, sous **Secure Ticket Authority**, sous **Active**, sélectionnez les serveurs STA, puis cliquez sur **OK**.

Vous pouvez également ajouter des serveurs STA dans l'onglet **Applications publiées**.

Configurer le scénario de secours d'accès

March 27, 2024

SmartAccess permet à NetScaler Gateway de déterminer automatiquement les méthodes d'accès autorisées pour une machine utilisateur en fonction des résultats d'une analyse des terminaux. Le scénario Access Fallback étend encore cette fonctionnalité en permettant à une machine utilisateur de passer du client Citrix Secure Access à l'interface Web ou à StoreFront à l'aide de l'application Citrix Workspace si la machine utilisateur ne passe pas avec succès l'analyse initiale des terminaux.

Pour activer le scénario d'accès alternatif, vous configurez une stratégie de post-authentification qui détermine si les utilisateurs reçoivent une autre méthode d'accès lorsqu'ils se connectent à NetScaler Gateway. Cette stratégie de post-authentification est définie comme une expression de sécurité client que vous configurez globalement ou dans le cadre d'un profil de session. Si vous configurez un profil de session, le profil est associé à une stratégie de session que vous liez ensuite aux utilisateurs, groupes ou serveurs virtuels. Lorsque vous activez le scénario d'accès de secours, NetScaler Gateway lance une analyse des terminaux après authentification de l'utilisateur. Les résultats pour les machines utilisateur qui ne répondent pas aux exigences d'une analyse post-authentification de secours sont les suivants :

- Si les choix du client sont activés, les utilisateurs peuvent ouvrir une session sur l'interface Web ou StoreFront à l'aide de l'application Citrix Workspace uniquement.
- Si l'accès sans client et les choix de client sont désactivés, les utilisateurs peuvent être mis en quarantaine dans un groupe qui fournit un accès uniquement à l'interface Web ou à StoreFront.
- Si l'accès sans client et l'interface Web ou StoreFront sont activés sur NetScaler Gateway et que le proxy ICA est désactivé, les utilisateurs reviennent à l'accès sans client.
- Si l'interface Web ou StoreFront n'est pas configuré et que l'accès sans client est configuré pour autoriser, les utilisateurs reviennent à l'accès sans client.

Lorsque l'accès sans client est désactivé, la combinaison de paramètres suivante doit être configurée pour le scénario de secours d'accès :

- Définissez les paramètres de sécurité du client pour l'analyse de secours après authentification.
- Définissez la page d'accueil de l'interface Web.
- Désactivez les choix du client.
- Si les machines utilisateur échouent au contrôle de sécurité du client, les utilisateurs sont placés dans un groupe de quarantaine qui autorise l'accès uniquement à l'interface Web ou à StoreFront et aux applications publiées.

Créer des stratégies pour le scénario de secours Access Scenario

Pour configurer NetScaler Gateway pour le scénario de secours d'accès, vous devez créer des stratégies et des groupes de la manière suivante :

- Créez un groupe de quarantaine dans lequel les utilisateurs sont placés en cas d'échec de l'analyse de l'analyse des points de terminaison.
- Créez une interface Web globale ou un paramètre StoreFront qui sera utilisé en cas d'échec de l'analyse d'analyse des points de terminaison.
- Créez une stratégie de session qui remplace le paramètre global, puis liez la stratégie de session à un groupe.
- Créez une stratégie de sécurité client globale qui sera appliquée en cas d'échec de l'analyse des points de terminaison.

Lorsque vous configurez le scénario de secours d'accès, suivez les instructions suivantes :

- L'utilisation des choix du client ou du scénario de secours d'accès nécessite le plug-in Endpoint Analysis pour tous les utilisateurs. Si l'analyse des points de terminaison ne peut pas être exécutée ou si les utilisateurs sélectionnent Ignorer l'analyse pendant l'analyse, l'accès est refusé aux utilisateurs.
  Remarque : L'option permettant d'ignorer l'analyse est supprimée dans NetScaler Gateway 10.1, build 120.1316.e

- Lorsque vous activez les choix du client, si la machine utilisateur échoue à l'analyse d'analyse des points de terminaison, les utilisateurs sont placés dans le groupe de quarantaine. Les utilisateurs peuvent continuer à se connecter à l'interface Web ou à StoreFront à l'aide du client Citrix Secure Access ou de l'application Citrix Workspace.
  Remarque : Citrix recommande de ne pas créer de groupe de quarantaine si vous activez les choix des clients. Les machines utilisateur qui échouent à l'analyse des points de terminaison sont mises en quarantaine sont traitées de la même manière que les machines utilisateur qui réussissent l'analyse des terminaux.
- Si l'analyse de l'analyse des points de terminaison échoue et que l'utilisateur est placé dans le groupe de quarantaine, les stratégies liées au groupe de quarantaine ne sont effectives que si aucune stratégie liée directement à l'utilisateur n'a un numéro de priorité égal ou inférieur à celui des stratégies liées au groupe de quarantaine.
- Vous pouvez utiliser différentes adresses Web pour l'interface d'accès et l'interface Web ou StoreFront. Lorsque vous configurez les pages d'accueil, la page d'accueil de l'interface d'accès est prioritaire pour le client Citrix Secure Access et la page d'accueil de l'interface Web est prioritaire pour les utilisateurs de l'interface Web. La page d'accueil de l'application Citrix Workspace est prioritaire pour StoreFront.

Créer un groupe de quarantaine

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, ouvrez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **AAA**Groups.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom du groupe**, tapez le nom du groupe, cliquez sur **Créer,** puis sur **Fermer**.
   Important: Le nom du groupe de quarantaine ne doit pas correspondre au nom d'un groupe de domaines auquel les utilisateurs pourraient appartenir. Si le groupe de quarantaine correspond à un nom de groupe Active Directory, les utilisateurs sont mis en quarantaine même si la machine utilisateur réussit l'analyse de sécurité de l'analyse des points de terminaison.

Après avoir créé le groupe, configurez NetScaler Gateway pour revenir à l'interface Web si la machine utilisateur échoue à l'analyse des terminaux.

Configuration des paramètres de mise en quarantaine des connexions utilisateur

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans la boîte de dialogue **Paramètres globaux de NetScaler Gateway**, sous l'onglet **Applications publiées**, en regard de **Proxy ICA**, sélectionnez **Désactivé**.

4. À côté de **Adresse de l'interface Web**, saisissez l'adresse Web de StoreFront ou de l'interface Web.
5. En regard de **Domaine d'authentification unique**, tapez le nom de votre domaine Active Directory, puis cliquez sur **OK**.

Après avoir configuré les paramètres globaux, créez une stratégie de session qui remplace le paramètre proxy ICA global, puis liez la stratégie de session au groupe de quarantaine.

Créer une stratégie de session pour le scénario de secours Access Scenario

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans l'onglet **Applications publiées**, en regard de **Proxy ICA**, cliquez sur **Override Global**, sélectionnez **On,** puis cliquez sur **Create**.
6. Dans la boîte de dialogue **Créer une politique de session**, à côté de **Expressions nommées**, sélectionnez **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression**, sur **Créer,** puis sur **Fermer**.

Après avoir créé la stratégie de session, liez la stratégie à un groupe de quarantaine.

Liez la stratégie de session au groupe de quarantaine

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, ouvrez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **AAA**Groups.
2. Dans le volet d'informations, sélectionnez un groupe, puis cliquez sur **Ouvrir**.
3. Cliquez sur Session.
4. Dans **l'onglet Stratégies**, sélectionnez **Session**, puis cliquez sur **Insérer une stratégie**.
5. Sous **Nom de la stratégie**, sélectionnez la stratégie, puis cliquez sur **OK**.

Après avoir créé la stratégie de session et le profil activant l'interface Web ou StoreFront sur NetScaler Gateway, créez une stratégie de sécurité client globale.

Créer une stratégie de sécurité client globale

1. **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.

3. Dans l'onglet **Sécurité**, cliquez sur **Paramètres avancés**.
4. Dans **Client Security**, saisissez l'expression. Pour plus d'informations sur la configuration des expressions système, consultez Configuration des expressions système et Configuration des expressions de sécurité du client composé
5. Dans **Groupe de quarantaine**, sélectionnez le groupe que vous avez configuré dans la procédure de groupe, puis cliquez sur **OK**.

Configurer les connexions pour le client Citrix Secure Access

January 26, 2024

Vous configurez les connexions de machine utilisateur en définissant les ressources auxquelles les utilisateurs peuvent accéder sur le réseau interne. La configuration des connexions de machine utilisateur comprend les éléments suivants :

- Définir les domaines auxquels les utilisateurs sont autorisés à accéder.
- Configuration des adresses IP des utilisateurs, y compris des pools d'adresses (IP intranet).
- Configuration des paramètres de délai d'expiration.
- Configuration de l'authentification unique.
- Configuration de l'interception des clients.
- Configuration du split tunneling.
- Configuration des connexions via un serveur proxy.
- Configuration du logiciel utilisateur pour qu'il se connecte via NetScaler Gateway.
- Configuration de l'accès pour les appareils mobiles.

Vous configurez la plupart des connexions utilisateur et machine à l'aide d'un profil qui fait partie d'une stratégie de session. Vous pouvez également définir les paramètres de connexion de la machine utilisateur à l'aide d'applications intranet, de préauthentification et de stratégies de trafic.

> **Remarque :**
>
> le plug-in VPN Windows et les plug-ins EPA collectent des données de télémétrie pour ses différentes opérations. Pour désactiver cette fonctionnalité, procédez comme suit sur la machine cliente.
>
> Définissez le registre « HKLM \ Software \ Citrix \ Secure Access Client \ DisableGA » de type REG_DWORD sur 1.

Configurer le nombre de sessions utilisateur

March 27, 2024

Vous pouvez configurer le nombre maximum d'utilisateurs autorisés à se connecter à NetScaler Gateway à un moment donné, au niveau global ou au niveau de chaque serveur virtuel. Les sessions ne sont pas créées sur NetScaler Gateway lorsque le nombre d'utilisateurs se connectant à l'appliance dépasse la valeur que vous configurez. Si le nombre d'utilisateurs dépasse le nombre autorisé, les utilisateurs reçoivent un message d'erreur.

Pour définir la limite globale d'utilisateurs

Lorsque vous configurez la limite d'utilisateurs globalement, la restriction s'applique à tous les utilisateurs qui établissent des sessions sur différents serveurs virtuels du système. Lorsque le nombre de sessions utilisateur atteint la valeur que vous avez définie, aucune nouvelle session ne peut être établie sur aucun serveur virtuel présent sur NetScaler Gateway.

Vous définissez le nombre maximum d'utilisateurs au niveau global lorsque vous définissez le type d'authentification par défaut pour NetScaler Gateway.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Paramètres globaux.
2. Dans le volet d'informations, sous Paramètres, cliquez sur Modifier les paramètres d'authentification.
3. Dans la boîte de dialogue Paramètres d'authentification globale, dans Nombre maximal d'utilisateurs, tapez le nombre d'utilisateurs, puis cliquez sur OK.

Pour définir la limite d'utilisateurs par serveur virtuel

Vous pouvez également appliquer la limite d'utilisateurs à chaque serveur virtuel du système. Lorsque vous configurez la limite d'utilisateurs par serveur virtuel, la restriction s'applique uniquement aux utilisateurs qui établissent des sessions avec le serveur virtuel particulier. Les utilisateurs qui établissent des sessions avec d'autres serveurs virtuels ne sont pas concernés par cette limite.

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur Virtual Servers.
2. Dans le volet d'informations, cliquez sur un serveur virtuel, puis sur Ouvrir.
3. Dans Max Users, tapez le nombre d'utilisateurs, puis cliquez sur OK.

Configuration des paramètres de délai d'expiration

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour forcer la déconnexion s'il n'y a aucune activité sur la connexion pendant un certain nombre de minutes. Une minute avant la fin d'une session (déconnexion), l'utilisateur reçoit une alerte indiquant la fermeture de la session. Si la session se ferme, l'utilisateur doit ouvrir une nouvelle session.

Les options de délai d'expiration suivantes sont disponibles.

- **Délai d'arrêt forcé.** Si vous activez ce paramètre, NetScaler Gateway déconnecte la session une fois le délai écoulé, indépendamment de ce que fait l'utilisateur. L'utilisateur ne peut prendre aucune mesure pour empêcher la déconnexion de se produire lorsque le délai d'expiration est écoulé. Ce paramètre est appliqué aux utilisateurs qui se connectent au client Citrix Secure Access, à l'application Citrix Workspace, à Secure Hub ou via un navigateur Web. La valeur minimale est 1 et la valeur maximale est 65535.
- **Délai d'expiration de session.** Si vous activez ce paramètre, NetScaler Gateway déconnecte la session si aucune activité réseau n'est détectée pendant l'intervalle spécifié. Ce paramètre est appliqué aux utilisateurs qui se connectent au client Citrix Secure Access, à l'application Citrix Workspace, à Citrix Secure Hub ou via un navigateur Web. Le délai d'expiration par défaut est de 30 minutes. La valeur minimale est 1 et la valeur maximale est 65535.
- **Délai d'inactivité de la session.** Durée après laquelle le client Citrix Secure Access met fin à une session inactive s'il n'y a aucune activité utilisateur, par exemple à l'aide de la souris, du clavier ou du toucher pendant l'intervalle spécifié. Ce paramètre est appliqué uniquement aux utilisateurs qui se connectent au client Citrix Secure Access. La valeur minimale est 1 et la valeur maximale est 9999.

Vous pouvez activer n'importe quel paramètre de délai d'expiration en entrant une valeur comprise entre 1 et 65 536 pour spécifier les minutes de l'intervalle de temporisation. Si vous activez plusieurs de ces paramètres, le premier délai d'expiration écoulé ferme la connexion de la machine utilisateur.

Vous configurez les paramètres de délai d'expiration en configurant des paramètres globaux ou en utilisant un profil de session. Lorsque vous ajoutez le profil à une stratégie de session, celle-ci est ensuite liée à un utilisateur, un groupe ou un serveur virtuel. Lorsque vous configurez les paramètres de délai d'expiration globalement, ces paramètres sont appliqués à toutes les sessions utilisateur.

> **Remarque :**
>
> - En mode Always On (mode service ou mode utilisateur), le client VPN ignore tous les délais d'attente. Les décisions relatives au délai d'expiration forcé et au délai d'expiration de

session sont prises sur l'appliance NetScaler et, par conséquent, ces délais d'expiration fonctionnent comme prévu. Si ce délai se produit, le plug-in VPN tente d'effectuer une authentification automatique.

Dans Always On, étant donné que la machine utilisateur doit être connectée en permanence via le tunnel VPN, ne configurez pas le délai d'attente forcé ou le délai d'inactivité du client. Toutefois, le délai d'expiration de session peut être configuré pour éliminer les sessions obsolètes.

- Certaines applications, telles que Microsoft Outlook, envoient automatiquement des sondes de trafic réseau aux serveurs de messagerie sans aucune intervention de l'utilisateur. Citrix vous recommande de configurer le délai d'expiration de la session inactive avec le délai d'expiration de session pour garantir qu'une session laissée sans surveillance sur une machine utilisateur arrive à expiration dans un délai raisonnable.

Configuration des délais d'expiration forcés

Un délai d'expiration forcé déconnecte automatiquement le client Citrix Secure Access après un laps de temps spécifié. Vous pouvez configurer un délai d'expiration forcé globalement ou dans le cadre d'une stratégie de session.

Configurer un délai d'expiration forcé global

1. Dans l'utilitaire de configuration, dans l'onglet **Configuration**, dans le volet de navigation, développez NetScaler Gateway, puis cliquez sur **Paramètres globaux**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Configuration réseau**, cliquez sur **Paramètres avancés**.
4. Dans la zone Délai d'expiration forcé (minutes), tapez le nombre de minutes que les utilisateurs peuvent rester connectés.
5. Dans Avertissement de délai d'expiration forcé (minutes), tapez le nombre de minutes avant que les utilisateurs soient avertis que la connexion est sur le point d'être déconnectée, puis cliquez sur **OK**.

Configurer un délai d'expiration forcé dans une stratégie de session

Si vous souhaitez contrôler davantage les personnes qui reçoivent le délai d'expiration forcé, créez une stratégie de session, puis appliquez la stratégie à un utilisateur ou à un groupe.

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**>**Policies**, puis cliquez sur Session.**

2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Demander un profil, cliquez sur **Nouveau**.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet **Configuration réseau**, cliquez sur **Avancé**.
7. Dans Timeouts, cliquez sur **Override Global** et dans Forced Timeout (minutes), tapez le nombre de minutes pendant lesquelles les utilisateurs peuvent rester connectés.
8. À côté de **Avertissement de temporisation forcée (minutes)**, cliquez sur **Override Global** et saisissez le nombre de minutes pendant lesquelles les utilisateurs sont avertis que la connexion va être déconnectée. Cliquez sur **OK** deux fois.
9. Dans la boîte de dialogue **Créer une politique de session**, à côté de **Expressions nommées**, sélectionnez Général, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression**, sur **Créer,** puis sur **Fermer**.

Configurer les délais d'attente de session ou d'inactivité

Vous pouvez utiliser l'interface graphique NetScaler pour configurer les paramètres de délai d'expiration des sessions et des clients de manière globale ou pour créer une stratégie de session. Lorsque vous créez une stratégie et un profil de session, définissez l'expression sur True.

> **Remarque :**
>
> si vous ne remplacez pas explicitement le paramètre global et ne définissez pas le délai d'expiration de la session dans **Expérience client > Délai d'expiration de la session (minutes)**, cela peut entraîner des boucles d'authentification nécessitant une reconnexion. Cela se produit même avec le délai d'expiration de session par défaut de 30 minutes.

Pour configurer globalement le délai d'inactivité d'une session ou d'un client à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Paramètres globaux**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Expérience client**, effectuez l'une des opérations suivantes ou les deux :
    - Dans la **zone Délai d'expiration de la session (minutes)**, tapez le nombre de minutes.
    - Dans **Délai d'inactivité du client (minutes)**, tapez le nombre de minutes, puis cliquez sur **OK**.

Pour configurer les paramètres de délai d'inactivité de session ou de client à l'aide d'une stratégie de session à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway** > **Policies**, puis cliquez sur **Session**
2. Dans la page **Stratégies et profils de session NetScaler Gateway**, cliquez sur **Profils de session**, puis sur **Ajouter**.
3. Dans Nom, saisissez le nom du profil.
4. Dans l'onglet **Expérience client**, effectuez l'une des opérations suivantes ou les deux :
    - En regard de **Délai d'expiration de la session (minutes)**, cliquez sur **Remplacer la valeur globale**, puis tapez le nombre de minutes, puis cliquez sur **Créer**.
    - En regard de **Délai d'inactivité du client (minutes)**, cliquez sur **Remplacer la valeur globale**, tapez le nombre de minutes, puis cliquez sur **Créer**.
5. a) Dans la page **Stratégies et profils de session NetScaler Gateway**, cliquez sur **Stratégies de session**, puis sur **Ajouter**.
6. Dans la stratégie de **session Create NetScaler Gateway,**
    - Dans la zone **Nom**, saisissez le nom de la stratégie.
    - Dans **Profil**, sélectionnez le profil qui spécifie l'action à appliquer par la nouvelle stratégie de session si les critères de la règle sont remplis.
    - sélectionnez **Stratégie avancée**.
    - Dans le champ **Expression**, ajoutez votre expression ou le nom d'une expression nommée, en spécifiant le trafic correspondant à la stratégie.
    - Cliquez sur **Créer**, puis sur **Fermer**.

Connexion aux ressources réseau internes

March 27, 2024

Vous pouvez configurer NetScaler Gateway pour permettre aux utilisateurs d'accéder aux ressources du réseau interne. Si vous désactivez le split tunneling, tout le trafic réseau provenant de la machine utilisateur est envoyé à NetScaler Gateway et les stratégies d'autorisation déterminent si le trafic est autorisé à transiter vers les ressources réseau internes. Lorsque vous activez le split tunneling, seul le trafic destiné au réseau interne est intercepté par la machine utilisateur et envoyé à NetScaler Gateway. Vous configurez les adresses IP interceptées par NetScaler Gateway à l'aide d'applications intranet.

Si vous utilisez le client Citrix Secure Access pour Windows, définissez le mode d'interception sur transparent. Si vous utilisez le client Citrix Secure Access pour Java, définissez le mode d'interception

sur proxy. Lorsque vous définissez le mode d'interception sur Transparent, vous pouvez autoriser l'accès aux ressources réseau à l'aide des éléments suivants :

- Une adresse IP et un masque de sous-réseau uniques
- Une gamme d'adresses IP

Si vous définissez le mode d'interception sur proxy, vous pouvez configurer les adresses IP et les numéros de port de destination et de source.

Configuration de l'accès réseau aux ressources réseau internes

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez NetScaler Gateway, développez Resources, puis cliquez sur **Intranet Applications.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**
3. Renseignez les paramètres d'autorisation d'accès au réseau, cliquez sur **Créer**, puis sur **Fermer.**

Configurer le split tunneling

March 27, 2024

Vous pouvez activer le split tunneling pour empêcher le client Citrix Secure Access d'envoyer du trafic réseau inutile à NetScaler Gateway.

Lorsque vous n'activez pas le split tunneling, le client Citrix Secure Access capture tout le trafic réseau provenant d'une machine utilisateur et envoie le trafic via le tunnel VPN à NetScaler Gateway.

Si vous activez le split tunneling, le client Citrix Secure Access envoie uniquement le trafic destiné aux réseaux protégés par NetScaler Gateway via le tunnel VPN. Le client Citrix Secure Access n'envoie pas le trafic réseau destiné aux réseaux non protégés à NetScaler Gateway.

Lorsque le client Citrix Secure Access démarre, il obtient la liste des applications intranet auprès de NetScaler Gateway. Le client Citrix Secure Access examine tous les paquets transmis sur le réseau depuis la machine utilisateur et compare les adresses contenues dans les paquets à la liste des applications intranet. Si l'adresse de destination du paquet se trouve dans l'une des applications intranet, le client Citrix Secure Access envoie le paquet via le tunnel VPN à NetScaler Gateway. Si l'adresse de destination ne se trouve pas dans une application intranet définie, le paquet n'est pas chiffré et la machine utilisateur achemine le paquet de manière appropriée. Lorsque vous activez le split tunneling, les applications intranet définissent le trafic réseau intercepté.

> **Remarque :**
>
> Si les utilisateurs se connectent à des applications publiées dans une batterie de serveurs à l'aide de l'application Citrix Workspace, il n'est pas nécessaire de configurer le split tunneling.

NetScaler Gateway prend également en charge le tunneling fractionné inversé, qui définit le trafic réseau que NetScaler Gateway n'intercepte pas. Si vous configurez le split tunneling sur l'inverse, les applications intranet définissent le trafic réseau que NetScaler Gateway n'intercepte pas. Lorsque vous activez le split tunneling inversé, tout le trafic réseau dirigé vers des adresses IP internes contourne le tunnel VPN, tandis que le reste du trafic passe par NetScaler Gateway. Le split tunneling inverse peut être utilisé pour enregistrer tout le trafic LAN non local. Par exemple, si les utilisateurs disposent d'un réseau domestique sans fil et sont connectés via le client Citrix Secure Access, NetScaler Gateway n'intercepte pas le trafic réseau destiné à une imprimante ou à un autre appareil du réseau sans fil.

Pour plus d'informations sur les applications intranet, consultez Configuration de l'interception des clients.

Vous configurez le split tunneling dans le cadre de la stratégie de session.

Pour configurer le split tunneling

1. **Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, sous l'onglet **Profils**, sélectionnez un profil, puis cliquez sur **Ouvrir.**
3. Dans l'onglet **Expérience client**, en regard de **Split Tunnel**, sélectionnez **Global Override**, sélectionnez une option, puis cliquez deux fois sur **OK**.

Configuration du split tunneling et de l'autorisation

Lors de la planification de votre déploiement de NetScaler Gateway, il est important de prendre en compte le split tunneling ainsi que l'action d'autorisation par défaut et les stratégies d'autorisation.

Par exemple, vous disposez d'une stratégie d'autorisation qui autorise l'accès à une ressource réseau. Le split tunneling est activé et vous ne configurez pas les applications intranet pour envoyer du trafic réseau via NetScaler Gateway. Lorsque NetScaler Gateway dispose de ce type de configuration, l'accès à la ressource est autorisé, mais les utilisateurs ne peuvent pas y accéder.

Si la stratégie d'autorisation refuse l'accès à une ressource réseau, si le split tunneling est activé et si les applications intranet sont configurées pour acheminer le trafic réseau via NetScaler Gateway,

le client Citrix Secure Access envoie le trafic vers NetScaler Gateway, mais l'accès à la ressource est refusé.

Pour plus d'informations sur les options de split tunneling, consultez la section Options de split tunneling.

Configurer l'interception des clients

March 27, 2024

Vous configurez les règles d'interception pour les connexions utilisateur sur NetScaler Gateway à l'aide des applications Intranet. Par défaut, lorsque vous configurez l'adresse IP du système, une adresse IP mappée ou une adresse IP de sous-réseau sur l'appliance, les routes de sous-réseau sont créées en fonction de ces adresses IP. Les applications intranet sont créées automatiquement en fonction de ces itinéraires et peuvent être liées à un serveur virtuel. Si vous activez le split tunneling, vous devez définir des applications intranet pour que l'interception des clients se produise.

Vous pouvez configurer des applications intranet à l'aide de l'interface graphique. Vous pouvez lier des applications intranet à des utilisateurs, des groupes ou des serveurs virtuels.

Si vous activez le split tunneling et que les utilisateurs se connectent à l'aide de WorxWeb ou WorxMail, lorsque vous configurez l'interception des clients, vous devez ajouter les adresses IP de Citrix Endpoint Management et de votre serveur Exchange. Si vous n'activez pas le split tunneling, il n'est pas nécessaire de configurer les adresses IP Endpoint Management et Exchange dans les applications Intranet.

Pour plus d'informations sur la configuration du split tunneling, voir Configurer le split tunneling.

Configuration des applications intranet pour le client Citrix Secure Access

Vous créez des applications intranet permettant aux utilisateurs d'accéder aux ressources en définissant les éléments suivants :

- Une adresse IP
- Une gamme d'adresses IP
- Un nom d'hôte

Lorsque vous définissez une application intranet sur NetScaler Gateway, le client Citrix Secure Access pour Windows intercepte le trafic utilisateur destiné à la ressource et envoie le trafic via NetScaler Gateway.

Lorsque vous configurez des applications intranet, prenez en compte les points suivants :

- Lorsque Split Tunnel est activé,
  - Configurez les applications intranet.
  - Attribuez des applications intranet à chaque groupe d'authentification, d'autorisation et d'audit.
- Lorsque Split Tunnel est OFF,
  - Tout le trafic est intercepté via le tunnel VPN.
  - Il n'est pas nécessaire de configurer les applications intranet.
- Lorsque Split Tunnel est REVERSE,
  - Configurez les applications intranet. Le trafic qui n'est pas spécifié par les applications intranet passe par le tunnel VPN.
  - Attribuez les applications intranet à exclure du VPN à chaque groupe d'authentification, d'autorisation et d'audit.

> **Important :**
>
> L'interception doit être réglée sur **TRANSPARENT** quelle que soit la configuration du tunnel divisé.

Remarque :

- Lors de la configuration d'une application intranet, vous devez sélectionner un mode d'interception correspondant au type de plug-in utilisé pour établir des connexions.
- Vous ne pouvez pas configurer une application intranet pour une interception par proxy et une interception transparente.

Pour créer une application intranet pour une adresse IP

1. **Dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway Resources**, puis cliquez sur Applications intranet.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**
3. Dans Nom, saisissez le nom du profil.
4. Dans la boîte de dialogue **Créer une application intranet**, sélectionnez **TRANSPARENT.**
5. Dans **Type de destination**, sélectionnez **Adresse IP**et **masque de réseau.**
6. Dans Protocole, sélectionnez le protocole qui s'applique à la ressource réseau.
7. Dans **Adresse IP**, saisissez l'adresse IP.
8. Dans **Masque de réseau**, tapez masque de sous-réseau, cliquez sur **Créer**, puis sur **Fermer.**

Pour configurer une plage d'adresses IP

Si votre réseau comporte plusieurs serveurs, tels que des partages Web, de messagerie et de fichiers, vous pouvez configurer une ressource réseau qui inclut la plage d'adresses IP des ressources réseau. Ce paramètre permet aux utilisateurs d'accéder aux ressources réseau contenues dans la plage d'adresses IP.

1. Dans l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway Resources**, puis cliquez sur **Applications intranet.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**
3. Dans **Nom**, saisissez le nom du profil.
4. Dans Protocole, sélectionnez le protocole qui s'applique à la ressource réseau.
5. Dans la boîte de dialogue **Créer une application intranet**, sélectionnez **TRANSPARENT**.
6. Dans **Type de destination**, sélectionnez **Plage d'adresses IP.**
7. Dans **IP Start**, tapez l'adresse IP de début et dans IP End, tapez l'adresse IP de fin, cliquez sur **Créer**, puis cliquez sur **Fermer.**

Pour créer une application intranet pour un nom d'hôte

1. **Dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway Resources**, puis cliquez sur Applications intranet.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**
3. Dans **Nom**, saisissez le nom du profil.
4. Dans la boîte de dialogue **Créer une application intranet**, sélectionnez **TRANSPARENT.**
5. Dans **Type de destination**, sélectionnez le **nom d'hôte**.
6. Dans Protocole, sélectionnez **ANY**, cliquez sur **Create (Créer),** puis sur **Close (Fermer).**

> **Important :**
>
> - À partir de la version 13.0, version 36.27 et ultérieure, le plug-in VPN Windows prend en charge les règles basées sur le nom d'hôte (FQDN) pour le split tunneling. Vous devez mettre à niveau l'appliance NetScaler et le plug-in VPN Windows vers la version 13.0 build 36.27 ou ultérieure.
> - Les noms d'hôtes génériques sont également pris en charge. Par exemple, si une application intranet portant le nom d'hôte « *.example.com » est configurée,„`a1.example.com` `b2.example.com` et ainsi de suite, passe par un tunnel.
> - L'application intranet basée sur le nom d'hôte ne fonctionne que lorsque le split tunneling est réglé sur ON ou REVERSE.

Configuration de la résolution du service de noms

March 27, 2024

Lors de l'installation de NetScaler Gateway, vous pouvez utiliser l'assistant NetScaler Gateway pour configurer d'autres paramètres, notamment les fournisseurs de services de noms. Les fournisseurs de services de noms traduisent le nom de domaine complet (FQDN) en adresse IP. Dans l'assistant NetScaler Gateway, vous pouvez configurer un serveur DNS ou WINS, définir la priorité de la recherche DNS et le nombre de tentatives de connexion au serveur.

Lorsque vous exécutez l'assistant NetScaler Gateway, vous pouvez alors ajouter un serveur DNS. Vous pouvez ajouter d'autres serveurs DNS et un serveur WINS à NetScaler Gateway à l'aide d'un profil de session. Vous pouvez ensuite diriger les utilisateurs et les groupes pour qu'ils se connectent à un serveur de résolution de noms différent de celui que vous avez initialement utilisé pour configurer l'assistant.

Avant de configurer un serveur DNS supplémentaire sur NetScaler Gateway, créez un serveur virtuel qui fait office de serveur DNS pour la résolution des noms.

Ajouter un serveur DNS ou WINS dans un profil de session

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway Policies**, puis cliquez sur **Session.**
2. Dans le volet d'informations, sous l'onglet Profils, sélectionnez un profil, puis cliquez sur Ouvrir.
3. Dans l'onglet Configuration réseau, effectuez l'une des opérations suivantes :
    - Pour configurer un serveur DNS, à côté de Serveur virtuel DNS, cliquez sur **Override Global**, sélectionnez le serveur, puis cliquez sur **OK.**
    - Pour configurer un serveur WINS, en regard de l'adresse IP du serveur WINS, cliquez sur **Remplacer global**, tapez l'adresse IP, puis cliquez sur **OK**.

> **Important :**
>
> Les stratégies de répondeur ne sont pas évaluées pour les serveurs virtuels DNS non adressables rattachés au profil de session VPN.

Activer la prise en charge du proxy pour les connexions

March 27, 2024

Les machines utilisateur peuvent se connecter via un serveur proxy pour accéder aux réseaux internes. NetScaler Gateway prend en charge les protocoles HTTP, SSL, FTP et SOCKS. Pour activer la prise en charge du proxy pour les connexions utilisateur, vous devez spécifier les paramètres sur NetScaler Gateway. Vous pouvez spécifier l'adresse IP et le port utilisés par le serveur proxy sur NetScaler Gateway. Le serveur proxy est utilisé comme proxy de transfert pour toutes les connexions ultérieures au réseau interne.

Paramètres du proxy

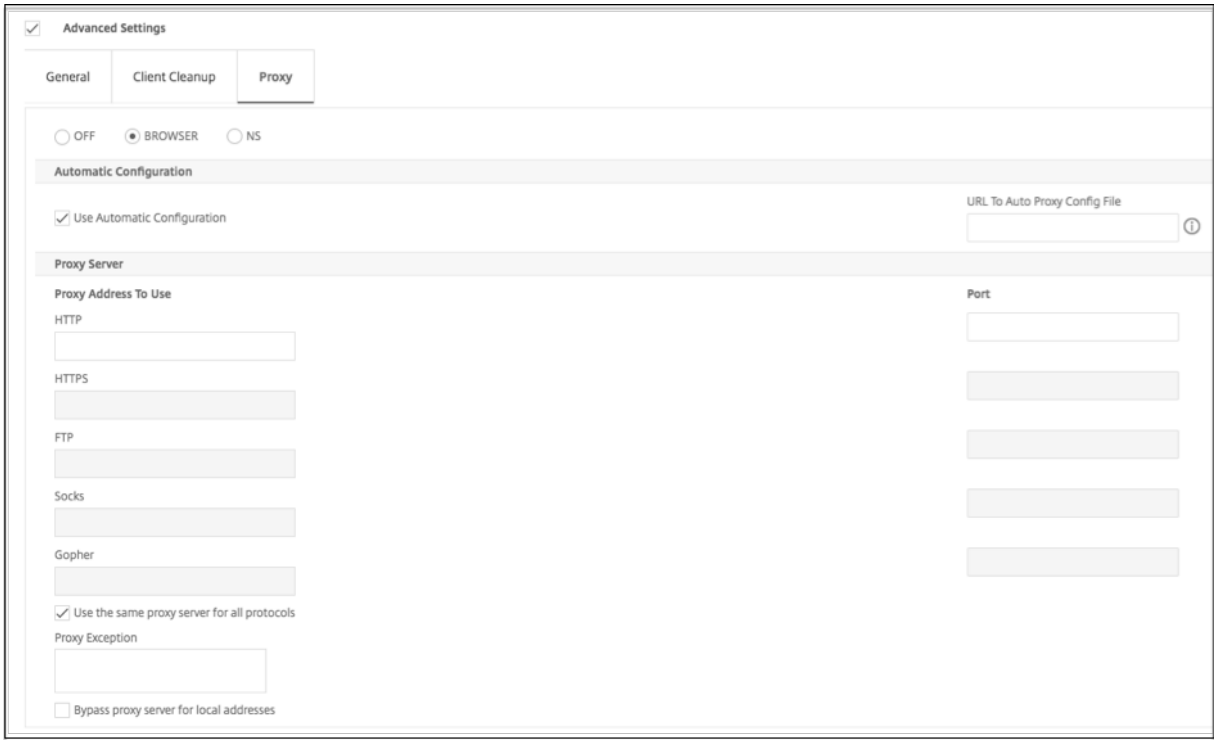
Vous pouvez configurer les paramètres du proxy sur le navigateur ou sur l'appliance NetScaler. Pour configurer les paramètres du proxy sur le navigateur ou l'appliance, accédez à **Paramètres globaux de NetScaler Gateway > onglet Expérience client > Paramètres avancés > Proxy**, puis sélectionnez **Navigateur** ou **NS selon le cas**.

- **Navigateur** : lorsque vous choisissez de configurer les paramètres du proxy sur le navigateur, vous pouvez utiliser l'option de configuration automatique en fournissant un lien vers le fichier de configuration du proxy automatique. La configuration automatique peut écraser les paramètres manuels.

  De plus, lorsque vous sélectionnez **Navigateur**, vous pouvez contourner les proxys précédemment configurés en sélectionnant l'option d'exception de proxy.

  Remarque : Différents types de clients ont des capacités différentes en ce qui concerne la configuration **du proxy du navigateur**. Pour en savoir plus, consultez la section Clients VPN NetScaler Gateway et fonctionnalités prises en charge.

- **NS** : Vous ne pouvez pas utiliser l'option de configuration automatique si vous configurez les paramètres du proxy sur l'appliance NetScaler. Vous ne pouvez pas contourner les proxys précédemment configurés lorsque vous configurez les paramètres du proxy sur l'appliance.



Pour configurer la prise en charge du proxy pour les connexions utilisateur

1. **Dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet Expérience client, cliquez sur **Paramètres avancés**.
4. Dans l'**onglet Proxy**, sous **Paramètres du proxy**, sélectionnez **Navigateur.**
5. Pour les protocoles, tapez l'adresse IP et le numéro de port, puis cliquez sur **OK.**

> **Remarque :**
>
> - Si vous sélectionnez **NS**, vous pouvez configurer des serveurs proxy qui prennent uniquement en charge les connexions HTTP sécurisées et non sécurisées.
> - Après avoir activé la prise en charge du proxy sur NetScaler Gateway, vous spécifiez les détails de configuration sur la machine utilisateur pour le serveur proxy qui correspond au protocole.
>
> Une fois que vous avez activé la prise en charge du proxy, NetScaler Gateway envoie les détails du serveur proxy au navigateur Web du client et modifie la configuration du proxy sur le navigateur.
>
> – When the user device connects to NetScaler Gateway, the user device can communi-

> cate with the proxy server directly for connection to the user's network.
> – When the user device disconnects from NetScaler Gateway, the proxy settings are restored to the previous default settings, that was present before connecting to the VPN plug-in.

Pour configurer un serveur proxy afin qu'il utilise tous les protocoles de NetScaler Gateway

Vous pouvez configurer un serveur proxy pour qu'il prenne en charge tous les protocoles utilisés par NetScaler Gateway. Ce paramètre fournit une combinaison d'adresse IP et de port pour tous les protocoles.

1. Dans le volet de navigation, développez **NetScaler Gateway**, puis cliquez sur **Paramètres globaux**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet **Expérience client**, cliquez sur **Paramètres avancés.**
4. Dans l'onglet **Proxy**, sous **Paramètres** du proxy, sélectionnez **Navigateur.**
5. Pour les protocoles, saisissez l'adresse IP et le numéro de port.
6. Cliquez sur Utiliser le même serveur proxy pour tous les protocoles, puis cliquez sur **OK.**

Lorsque vous désactivez le split tunneling et que vous définissez tous les paramètres de proxy sur Activé, les paramètres du proxy sont propagés aux machines utilisateur. Si les paramètres du proxy sont définis sur Appliance, les paramètres ne sont pas propagés aux machines utilisateur.

NetScaler Gateway établit des connexions au serveur proxy pour le compte de la machine utilisateur. Les paramètres du proxy ne sont pas propagés vers le navigateur de l'utilisateur, de sorte qu'aucune communication directe entre la machine utilisateur et le serveur proxy n'est possible.

Pour configurer NetScaler Gateway en tant que serveur proxy

Lorsque vous configurez NetScaler Gateway en tant que serveur proxy, le protocole HTTP non sécurisé et sécurisé est le seul protocole pris en charge.

1. **Dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet **Expérience client**, cliquez sur **Paramètres avancés.**
4. Dans l'onglet **Proxy**, sous **Paramètres du proxy**, sélectionnez **NS**.
5. Pour les protocoles, tapez l'adresse IP et le numéro de port, puis cliquez sur **OK.**

Configuration des pools d'adresses

March 27, 2024

Dans certains cas, les utilisateurs qui se connectent au client Citrix Secure Access ont besoin d'une adresse IP unique pour NetScaler Gateway. Par exemple, dans un environnement Samba, chaque utilisateur qui se connecte à un lecteur réseau mappé doit apparaître comme provenant d'une adresse IP différente. Lorsque vous activez des pools d'adresses (également appelés pool d'adresses IP) pour un groupe, NetScaler Gateway peut attribuer un alias d'adresse IP unique à chaque utilisateur.

Vous configurez des pools d'adresses à l'aide d'adresses IP intranet. Les types d'applications suivants peuvent avoir besoin d'utiliser une adresse IP unique extraite du pool d'adresses IP :

- Voix sur IP
- FTP actif
- Messagerie instantanée
- Shell sécurisé (SSH)
- Virtual Network Computing (VNC) pour se connecter au bureau d'un ordinateur
- Bureau à distance (RDP) pour se connecter à un poste de travail client

Vous pouvez configurer NetScaler Gateway pour attribuer une adresse IP interne aux utilisateurs qui se connectent à NetScaler Gateway. Les adresses IP statiques peuvent être attribuées aux utilisateurs ou une plage d'adresses IP peut être attribuée à un groupe, à un serveur virtuel ou au système globalement.

NetScaler Gateway vous permet d'attribuer des adresses IP de votre réseau interne à vos utilisateurs distants. Une adresse IP sur le réseau interne peut s'adresser à un utilisateur distant. Si vous choisissez d'utiliser une plage d'adresses IP, le système attribue dynamiquement une adresse IP de cette plage à un utilisateur distant à la demande.

Lorsque vous configurez des pools d'adresses, tenez compte des points suivants :

- Les adresses IP attribuées doivent être routées correctement. Pour garantir le bon routage, prenez en compte les points suivants :
  - Si vous n'activez pas le split tunneling, assurez-vous que les adresses IP peuvent être routées via des périphériques NAT (Network Address Translation).
  - Tous les serveurs auxquels des connexions utilisateur accèdent avec des adresses IP intranet doivent disposer des passerelles appropriées configurées pour atteindre ces réseaux.
  - Configurez des passerelles ou un itinéraire statique sur NetScaler Gateway afin que le trafic réseau provenant du logiciel utilisateur soit acheminé vers le réseau interne.

- Seuls les masques de sous-réseau contigus peuvent être utilisés lors de l'attribution de plages d'adresses IP. Un sous-ensemble d'une plage peut être affecté à une entité de niveau inférieur. Par exemple, si une plage d'adresses IP est liée à un serveur virtuel, liez un sous-ensemble de la plage à un groupe.
- Les plages d'adresses IP ne peuvent pas être liées à plusieurs entités au sein d'un niveau de liaison. Par exemple, un sous-ensemble d'une plage d'adresses lié à un groupe ne peut pas être lié à un deuxième groupe.
- NetScaler Gateway ne vous permet pas de supprimer ou de dissocier des adresses IP lorsqu'elles sont activement utilisées par une session utilisateur.
- Les adresses IP réseau internes sont attribuées aux utilisateurs à l'aide de la hiérarchie suivante :
  - Liaison directe de l'utilisateur
  - Pool d'adresses assigné au groupe
  - Pool d'adresses attribué au serveur virtuel
  - Gamme mondiale d'adresses
- Seuls les masques de sous-réseau contigus peuvent être utilisés pour attribuer des plages d'adresses. Toutefois, un sous-ensemble d'une plage attribuée peut être affecté à une entité de niveau inférieur.
  Une plage d'adresses globale liée peut comporter une plage liée aux éléments suivants :
  - Serveur virtuel
  - Groupe
  - Utilisateur
- Une plage d'adresses de serveur virtuel liée peut comporter un sous-ensemble lié aux éléments suivants :
  - Groupe
  - Utilisateur

Une plage d'adresses de groupe lié peut comporter un sous-ensemble lié à un utilisateur.

Lorsqu'une adresse IP est attribuée à un utilisateur, elle est réservée pour la prochaine connexion de l'utilisateur jusqu'à ce que la plage du pool d'adresses soit épuisée. Lorsque les adresses sont épuisées, NetScaler Gateway récupère l'adresse IP de l'utilisateur qui est déconnecté de NetScaler Gateway le plus longtemps.

Si une adresse ne peut pas être récupérée et que toutes les adresses sont activement utilisées, NetScaler Gateway n'autorise pas l'utilisateur à se connecter. Vous pouvez éviter cette situation en autorisant NetScaler Gateway à utiliser l'adresse IP mappée comme adresse IP intranet lorsque toutes les autres adresses IP ne sont pas disponibles.

Enregistrement DNS IP Intranet

Si une adresse IP intranet est attribuée à une machine cliente et après l'établissement du tunnel VIP, le plug-in VPN vérifie si cette machine cliente est jointe au domaine. Si la machine cliente appartient à un domaine, le plug-in VPN lance le processus d'enregistrement DNS pour lier l'intranet du nom d'hôte de la machine à l'adresse IP intranet attribuée. Cette inscription est annulée avant la désinstallation du tunnel.

Pour que l'enregistrement DNS soit réussi, assurez-vous que les `nsapimgr` boutons suivants sont définis. Assurez-vous également que le serveur DNS faisant autorité est configuré pour autoriser les mises à jour DNS « non sécurisées ».

- **`nsapimgr` -ys enable_vpn_dns_override=1** : Cet indicateur est envoyé au client VPN NetScaler Gateway avec les autres paramètres de configuration. Si cet indicateur n'est pas défini et que le client VPN intercepte une demande DNS/WINS, il envoie une requête HTTP « GET /DNS » correspondante au serveur virtuel NetScaler Gateway via le tunnel pour obtenir l'adresse IP résolue. Toutefois, si l'indicateur « enable_vpn_dnstruncate_fix » est défini, le client VPN transmet les demandes DNS/WINS de manière transparente au serveur virtuel NetScaler Gateway. Dans ce cas, le paquet DNS est envoyé tel qu'il est au serveur virtuel NetScaler Gateway via le tunnel VPN. Cela est utile dans les cas où les enregistrements DNS provenant des serveurs de noms configurés dans NetScaler Gateway sont volumineux et ne rentrent pas dans le paquet de réponse UPD. Dans ce cas, lorsque le client reprend l'utilisation de TCP-DNS, ce paquet TCP-DNS atteint le serveur NetScaler Gateway tel quel, et par conséquent le serveur NetScaler Gateway envoie une requête TCP-DNS à un serveur DNS.
- **nsapimgr -ys enable_vpn_dnstruncate_fix=1** : Cet indicateur est utilisé par le serveur NetScaler Gateway lui-même. Si cet indicateur est défini, NetScaler Gateway remplace la destination des « connexions TCP sur le port DNS » vers les serveurs DNS configurés sur NetScaler Gateway (au lieu d'essayer de les envoyer à l'adresse IP du serveur DNS initialement présente dans le paquet TCP-DNS entrant). Pour les demandes DNS UDP, la valeur par défaut consiste à utiliser les serveurs DNS configurés pour la résolution DNS. Le plug-in NetScaler Gateway pour Windows prend en charge les mises à jour DNS sécurisées et non sécurisées. La prise en charge de la mise à jour DNS sécurisée existe par défaut dans les versions 21.7.1.1 ou supérieures.

  La mise à jour DNS sécurisée sur le plug-in Windows est désactivée par défaut. Pour l'activer, créez une valeur de type REG_DWORD dans `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access` et définissez-la sur 1.

  - Lorsque vous définissez la valeur sur 1, le plug-in VPN essaie d'abord la mise à jour non sécurisée du DNS. Si la mise à jour DNS non sécurisée échoue, le plug-in VPN essaie la mise à jour DNS sécurisée.

- Pour essayer uniquement la mise à jour sécurisée du DNS, vous pouvez définir la valeur sur 2.

Pour plus d'informations sur la configuration de ces boutons, reportez-vous à la section https://support.citrix.com/article/CTX200243.

Configuration des pools d'adresses pour un utilisateur, un groupe ou un serveur virtuel

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **NetScaler Gateway**, effectuez l'une des opérations suivantes :
   - **Développez NetScaler Gateway User Administration, puis cliquez sur AAA Users.**
   - **Développez**NetScaler Gateway**>**Administration des utilisateurs**, puis cliquez sur Groupes AAA.**
   - **Développez**NetScaler Gateway**, puis cliquez sur Serveurs virtuels.**
2. Dans le volet d'informations, cliquez sur un utilisateur, un groupe ou un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Sous l'onglet IP **Intranet**, dans Adresse IP et masque de réseau, tapez l'adresse IP et le masque de sous-réseau, puis cliquez sur **Ajouter**.
4. Répétez l'étape 3 pour chaque adresse IP que vous souhaitez ajouter au pool, puis cliquez sur **OK**.

Configuration des pools d'adresses à l'échelle

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet de détails, sous **IP de l'intranet**, cliquez sur Pour attribuer une adresse IP statique unique ou un pool d'adresses IP à utiliser par toutes les sessions client NetScaler Gateway, configurez les adresses IP de l'intranet.
3. Dans la boîte **de dialogue Liaison des adresses IP intranet**, cliquez sur **Action,** puis sur **Insérer**.
4. Dans Adresse IP et masque de réseau, tapez l'adresse IP et le masque de sous-réseau, puis cliquez sur **Ajouter**.
5. Répétez les étapes 3 et 4 pour chaque adresse IP que vous souhaitez ajouter au pool, puis cliquez sur **OK**.

Définir les options du pool d'adresses

Vous pouvez utiliser une stratégie de session ou les paramètres globaux de NetScaler Gateway pour contrôler si des adresses IP intranet sont attribuées au cours d'une session utilisateur. La définition des options du pool d'adresses vous permet d'attribuer des adresses IP intranet à NetScaler Gateway, tout en désactivant l'utilisation des adresses IP intranet pour un groupe d'utilisateurs particulier.

Vous pouvez configurer des pools d'adresses à l'aide d'une stratégie de session de l'une des trois manières suivantes :

- `Nospillover` - Lorsque vous configurez des pools d'adresses pour l'adresse IP intranet, vous obtenez une session avec une adresse IP disponible à partir du pool. Pour les utilisateurs qui ont utilisé toutes les adresses IP intranet disponibles, la page Transfer Logon apparaît.
- **Spillover** - Lorsque vous configurez des pools d'adresses et que l'adresse IP mappée est utilisée comme adresse IP intranet, l'adresse IP mappée est utilisée pour les utilisateurs qui ont utilisé toutes les adresses IP intranet disponibles.
- **Désactivé : les pools**d'adresses ne sont pas configurés.

> **Remarque :**
>
> Si l'adresse IP mappée n'est pas configurée, SNIP est utilisé.

Pour définir des pools d'adresses

1. **Dans l'utilitaire de configuration, sous l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies,**puis cliquez sur Session.**
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans Nom, saisissez le nom du profil.
6. Dans l'onglet **Configuration réseau**, cliquez sur **Avancé**.
7. En regard de l'adresse IP intranet, cliquez sur **Remplacer l'adresse globale**, puis sélectionnez une option.
8. Si vous sélectionnez **DÉBORDEMENT** à l'étape 9, en regard de IP mappée, cliquez sur **Override Global**, sélectionnez le nom d'hôte de l'appliance, cliquez sur **OK,** puis cliquez sur **Créer**.
9. Dans la boîte de dialogue **Créer une stratégie de session**, créez une expression. Cliquez sur **Créer,** puis sur **Fermer**.

Configurer la page Transfer Logon

Si un utilisateur ne dispose pas d'adresse IP intranet et essaie ensuite d'établir une autre session avec NetScaler Gateway, la page Transfer Logon apparaît. La page Transfer Logon permet aux utilisateurs

de remplacer leur session NetScaler Gateway existante par une nouvelle session.

La page Transfer Logon peut également être utilisée si la demande de fermeture de session est perdue ou si l'utilisateur n'effectue pas une fermeture de session complète. Par exemple :

- Une adresse IP intranet statique est attribuée à un utilisateur et possède déjà une session NetScaler Gateway. Si l'utilisateur essaie d'établir une deuxième session à partir d'un autre appareil, la page Transfer Logon apparaît et l'utilisateur peut transférer la session vers le nouvel appareil.
- Un utilisateur se voit attribuer cinq adresses IP intranet et dispose de cinq sessions via NetScaler Gateway. Si l'utilisateur essaie d'établir une sixième session, la page Transfer Logon apparaît et l'utilisateur peut choisir de remplacer une session existante par une nouvelle session.

> **Remarques :**
>
> - Si aucune adresse IP attribuée à l'utilisateur n'est disponible et qu'une nouvelle session ne peut donc pas être établie, un message d'erreur s'affiche.
> - Citrix Secure Access pour Android 23.12.1 et versions ultérieures prennent en charge la fonctionnalité de connexion par transfert de NetScaler Gateway en mode VPN Always On.

La page Transfer Logon apparaît uniquement si vous configurez des pools d'adresses et désactivez le spillover.

Configurer un suffixe DNS

Lorsqu'un utilisateur se connecte à NetScaler Gateway et se voit attribuer une adresse IP, un enregistrement DNS pour la combinaison nom d'utilisateur et adresse IP est ajouté au cache DNS de NetScaler Gateway. Vous pouvez configurer un suffixe DNS à ajouter au nom d'utilisateur lorsque l'enregistrement DNS est ajouté au cache. Cela permet aux utilisateurs d'être référencés par le nom DNS, ce qui peut être plus facile à mémoriser qu'une adresse IP. Lorsque l'utilisateur se déconnecte de NetScaler Gateway, l'enregistrement est supprimé du cache DNS.

Pour configurer un suffixe DNS

1. **Dans l'utilitaire de configuration, sous l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies,**puis cliquez sur Session.**
2. Dans le volet d'informations, sous **l'onglet Stratégies**, sélectionnez une stratégie de session, puis cliquez sur **Ouvrir**.
3. À côté de Demander un profil, cliquez sur **Modifier**.
4. Dans l'onglet **Configuration réseau**, cliquez sur **Avancé**.

5. À côté de Suffixe DNS IP de l'intranet, cliquez sur **Override Global**, saisissez le suffixe DNS, puis cliquez trois fois sur **OK.**

Prise en charge des téléphones VoIP

January 26, 2024

Lorsque vous installez NetScaler Gateway en tant qu'appliance autonome et que les utilisateurs se connectent au client Citrix Secure Access, NetScaler Gateway prend en charge la communication bidirectionnelle avec les softphones VoIP (VoIP).

NetScaler Gateway prend en charge les softphones VoIP suivants.

- Téléphone logiciel Cisco
- Téléphone logiciel Avaya IP

Le tunneling sécurisé est pris en charge entre le PBX IP et le logiciel du téléphone logiciel exécuté sur la machine utilisateur. Pour permettre au trafic VoIP de traverser le tunnel sécurisé, vous devez installer le client Citrix Secure Access et l'un des softphones compatibles sur la même machine utilisateur. Lorsque le trafic VoIP est envoyé via le tunnel sécurisé, les fonctionnalités suivantes du téléphone logiciel sont prises en charge :

- Appels sortants passés depuis le téléphone logiciel IP
- Appels entrants placés sur le téléphone logiciel IP
- Trafic vocal bidirectionnel

La prise en charge des softphones VoIP est configurée à l'aide d'adresses IP intranet. Vous devez configurer une adresse IP intranet pour chaque utilisateur. Si vous utilisez Cisco Softphone Communication, après avoir configuré l'adresse IP intranet et liée à un utilisateur, aucune configuration supplémentaire n'est requise. Pour plus d'informations sur la configuration d'une adresse IP intranet, consultez Configuration des pools d'adresses.

Si vous activez le split tunneling, créez une application intranet et spécifiez l'application Avaya Softphone. En outre, vous devez activer l'interception transparente.

Configuration de l'interface d'accès

March 27, 2024

NetScaler Gateway inclut une page d'accueil par défaut qui s'affiche lorsque les utilisateurs se connectent. La page d'accueil par défaut s'appelle l'interface d'accès. Vous utilisez l'interface d'accès comme page d'accueil ou configurez l'interface Web en tant que page d'accueil ou page d'accueil personnalisée.

L'interface d'accès comporte trois panneaux. Si votre déploiement est doté de l'interface Web, les utilisateurs peuvent ouvrir une session sur Receiver dans le volet gauche de l'interface d'accès. Si StoreFront est présent dans votre déploiement, les utilisateurs ne peuvent pas se connecter à Receiver à partir du panneau de gauche.

L'interface d'accès est utilisée pour fournir des liens vers des sites Web, internes et externes, ainsi que des liens vers des partages de fichiers sur le réseau interne. Vous pouvez personnaliser l'interface d'accès de l'une des manières suivantes :

- Modification de l'interface d'accès.
- Création de liens d'interface d'accès.

Les utilisateurs peuvent également personnaliser l'interface d'accès en ajoutant leurs propres liens vers des sites Web et des partages de fichiers. Les utilisateurs peuvent également utiliser la page d'accueil pour transférer des fichiers du réseau interne vers leur appareil.

> **Remarque :**
>
> Lorsque les utilisateurs ouvrent une session et tentent d'ouvrir des partages de fichiers à partir de l'interface d'accès, le partage de fichiers ne s'ouvre pas et les utilisateurs reçoivent le message d'erreur « Échec de la connexion TCP au serveur ». Pour résoudre ce problème, configurez votre pare-feu de manière à autoriser le trafic depuis l'adresse IP du système NetScaler Gateway vers l'adresse IP du serveur de fichiers sur les ports TCP 445 et 139.

Modifier l'interface d'accès

Vous souhaiterez peut-être diriger les utilisateurs vers une page d'accueil personnalisée, plutôt que de vous fier à l'interface d'accès. Pour ce faire, installez la page d'accueil sur NetScaler Gateway, puis configurez la stratégie de session pour utiliser la nouvelle page d'accueil.

Pour installer une page d'accueil personnalisée

1. Dans l'utilitaire de configuration, cliquez sur l'onglet **Configuration**, puis dans le volet de navigation, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous **Personnaliser l'interface d'accès**, cliquez sur **Charger** l'**interface d'accès.**
3. Pour installer la page d'accueil à partir d'un fichier sur un ordinateur de votre réseau, dans Fichier local, cliquez sur **Parcourir**, accédez au fichier, puis cliquez sur **Sélectionner.**

4. Pour utiliser une page d'accueil installée sur NetScaler Gateway, dans Chemin distant, cliquez sur **Parcourir**, sélectionnez le fichier, puis cliquez sur **Sélectionner.**
5. Cliquez sur **Charger**, puis cliquez sur **Fermer.**

Remplacez l'interface d'accès par une page d'accueil personnalisée

Vous pouvez utiliser des paramètres globaux ou une stratégie de session et un profil pour configurer une page d'accueil personnalisée afin de remplacer la page d'accueil par défaut, l'interface d'accès. Après avoir configuré la stratégie, vous pouvez la lier à un utilisateur, un groupe, un serveur virtuel ou globalement. Lorsque vous configurez une page d'accueil personnalisée, l'interface d'accès n'apparaît pas lorsque les utilisateurs ouvrent une session.

Configuration globale de la page d'accueil personnalisée

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur Modifier les paramètres généraux.
3. Dans l'onglet **Expérience client**, dans la **page d'accueil**, cliquez sur **Afficher la page d'accueil,** puis entrez l'adresse Web de votre page d'accueil personnalisée.
4. Cliquez sur **OK**, puis sur **Fermer.**

Configuration d'une page d'accueil personnalisée dans un profil de session

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway Policies**, puis cliquez sur **Session.**
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter.**
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de **Demander un profil**, cliquez sur **Nouveau.**
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, en regard de **Page d'accueil**, cliquez sur **Remplacer la page globale**, cliquez sur **Afficher la page d'accueil,** puis tapez l'adresse Web de la page d'accueil.
7. Dans la boîte de dialogue **Créer une politique de session**, à côté de **Expressions nommées**, sélectionnez **Général**, sélectionnez Valeur vraie, cliquez sur **Ajouter une expression**, sur **Créer,** puis sur **Fermer.**

Créer et appliquer des liens Web

March 27, 2024

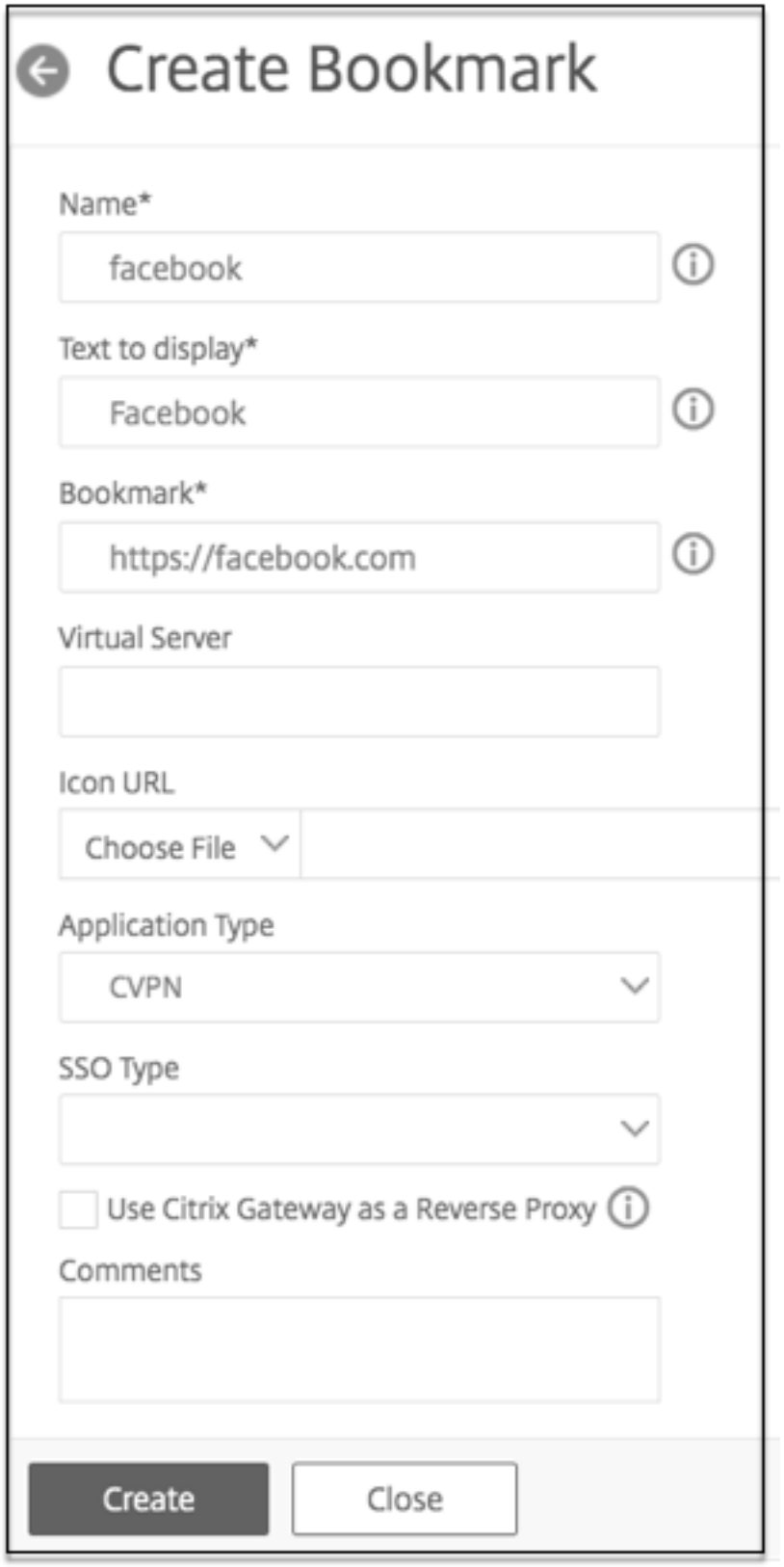
Vous pouvez configurer l'interface d'accès pour afficher un ensemble de liens vers des ressources internes disponibles pour les utilisateurs. Pour créer ces liens, vous devez d'abord définir les liens en tant que ressources. Ensuite, vous les liez à un utilisateur, un groupe, un serveur virtuel ou globalement pour les rendre actifs dans l'interface d'accès. Les liens que vous créez apparaissent dans les volets **Sites Web** sous **Sites Web d'entreprise**.

> **Important :**
>
> à partir de la version 13.0 build 64.xx de NetScaler, les partages de fichiers via NetScaler Gateway ne sont pas pris en charge.

Création de signets Enterprise

Pour créer un lien Access Interface dans une stratégie de session

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, dans le volet de navigation, développez **NetScaler Gateway > Resources**, puis cliquez sur **Portal Bookmarks.**
2. Dans le volet d'informations, cliquez sur **Ajouter.**



3. Dans **Nom**, saisissez le nom du signet.

4. Dans **Texte à afficher**, saisissez la description du lien. La description apparaît dans l'**interface d'accès.**
5. Dans **Signet**, saisissez l'adresse Web de l'application.
6. Dans **Virtual Server**, tapez le nom du serveur virtuel d'équilibrage de charge/de commutation de contenu associé. Ce champ est facultatif.
7. Dans **Icone URL**, les icônes téléchargées sont prises en charge pour tous les thèmes à l'exception du thème par défaut. La taille maximale recommandée est de 70 x 70 pixels. Nous vous recommandons d'utiliser des images transparentes. Ce champ est facultatif.
8. Dans **Type d'application**, sélectionnez le type d'application (VPN, VPN sans client ou SaaS) représenté par l'URL. Ce champ est facultatif.
9. Dans **Type SSO**, sélectionnez le type SSO que vous souhaitez configurer pour le signet. Lorsque l'authentification unique est configurée, les utilisateurs peuvent accéder aux applications sans avoir à saisir leurs informations d'identification lors des connexions suivantes. Les types de SSO suivants sont pris en charge :

   - Unified Gateway : cette configuration SSO permet un accès distant sécurisé à plusieurs ressources d'une application via une seule URL.
   - Auto-authentification : dans cette configuration SSO, les utilisateurs de NetScaler Gateway sont invités à fournir les informations de connexion pour accéder à l'application.
   - Authentification basée sur SAML : dans cette configuration SSO, NetScaler Gateway utilise un IdP pour valider les détails de l'utilisateur, génère une assertion SAML et l'envoie au SP. Si la validation est réussie, le SSO est réussi.

   > **Remarque :**
   >
   > Si vous activez l'accès sans client, vous pouvez vous assurer que les requêtes adressées aux sites Web passent par NetScaler Gateway. Par exemple, vous avez ajouté un signet pour Google. Cochez la case **Utiliser NetScaler Gateway comme proxy inverse**. Lorsque vous cochez cette case, les demandes de site Web sont transmises de la machine utilisateur à NetScaler Gateway, puis au site Web. Lorsque vous désactivez cette case à cocher, les demandes sont envoyées de la machine utilisateur vers le site Web. Cette case à cocher n'est disponible que si vous activez l'accès sans client.

10. Cliquez sur **Créer**, puis sur **Fermer.**

Pour lier un lien Access Interface

Vous pouvez lier les liens de l'interface d'accès aux emplacements suivants :

- Utilisateurs

- Groups
- Serveurs virtuels

Après avoir enregistré la configuration, les liens sont disponibles pour les utilisateurs dans l'interface d'accès de l'onglet **Accueil**, qui est la première page que les utilisateurs voient une fois qu'ils se sont connectés avec succès.

1. Dans l'utilitaire de configuration, dans le volet de navigation, effectuez l'une des opérations suivantes :
    - Développez **NetScaler Gateway User Administration**, puis cliquez sur **AAA Users.**
    - Développez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **Groupes AAA.**
    - Développez **NetScaler Gateway**, puis cliquez sur **Serveurs virtuels.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
    - Sélectionnez un utilisateur, puis cliquez sur Ouvrir.
    - Sélectionnez un groupe, puis cliquez sur Ouvrir.
    - Sélectionnez un serveur virtuel, puis cliquez sur Ouvrir.
3. Dans la boîte de dialogue, cliquez sur l'onglet **Signets**.
4. Sous **Signets disponibles**, sélectionnez un ou plusieurs signets, cliquez sur la flèche droite pour déplacer les signets sous Signets configurés, puis **sur OK.**

Pour lier des signets globalement à l'aide de l'interface graphique

1. **Dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Favoris**, cliquez sur **Créer des liens vers les applications HTTP et Windows File Share que vous souhaitez rendre accessibles sur la page du portail NetScaler Gateway**.

3. Dans la boîte de dialogue **Configurer la liaison globale VPN***, cliquez sur **Ajouter.**
4. Sous **Disponible**, sélectionnez un ou plusieurs signets, cliquez sur la flèche droite pour déplacer les signets sous **Configuré, puis sur OK**.

Pour ajouter un signet d'entreprise à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vpn url <urlName> <linkName> <actualURL>  [-ssotype <ssotype>]
<!--NeedCopy-->
```

Exemple :

Signet Web

```
add vpn url google google "https://www.google.com"
<!--NeedCopy-->
```

Pour lier un signet Enterprise à l'aide de l'interface de ligne de commande

Vous pouvez lier des signets d'entreprise aux utilisateurs, groupes, serveurs virtuels et globaux.

```
bind aaa user <userName> -urlName <string>
bind aaa group <groupName> -urlName <string>
bind vpn vserver <vserverName> -urlName <string>
bind vpn global  – urlName <string>
<!--NeedCopy-->
```

Exemple :

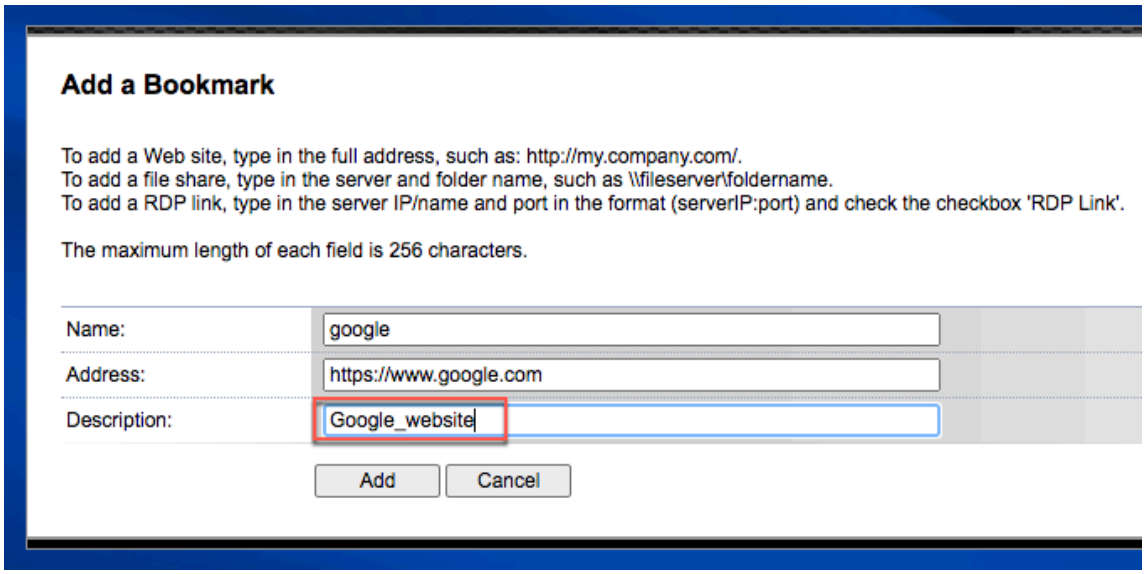

```
bind vpn global -urlName google
<!--NeedCopy-->
```

Création de signets personnels

Vous pouvez créer des sites Web personnels à partir du serveur virtuel VPN uniquement. Il n'existe aucune interface graphique d'administration NetScaler Gateway permettant d'ajouter des favoris personnels.

1. Ouvrez une session sur un serveur virtuel VPN.
2. Cliquez sur **Accès réseau** ou **Accès sans client** pour ajouter un signet.
3. Cliquez sur **Ajouter**.

4. Saisissez les détails du signet, tels que le nom, l'adresse et la description du site Web.



5. Cliquez sur **Ajouter**.

Les sites Web que vous avez ajoutés apparaissent sous les onglets respectifs.

Configurer les jetons de nom d'utilisateur dans les signets

Vous pouvez configurer des URL de signet et de partage de fichiers à l'aide d'un jeton spécial, %username %. Lorsque les utilisateurs ouvrent une session, le jeton est remplacé par le nom de connexion de chaque utilisateur. Par exemple, vous créez un signet pour un employé nommé Jack pour un dossier en tant que \ \ EmployeeServer \ %username % \. Lorsque Jack ouvre une session, l'URL du partage de fichiers est mappée à \ \ EmployeeServer \ Jack \. Lorsque vous configurez des jetons de nom d'utilisateur dans des signets, gardez à l'esprit les situations suivantes :

- Si vous utilisez un seul type d'authentification, le nom d'utilisateur remplace le jeton %username %.
- Si vous utilisez l'authentification à deux facteurs, le nom d'utilisateur du type d'authentification principal est utilisé pour remplacer le jetonusername % %.
- Si vous utilisez l'authentification par certificat client, le champ de nom d'utilisateur du profil d'authentification du certificat client est utilisé pour remplacer le jetonusername % %.

Stratégies de trafic

March 27, 2024

Les stratégies de trafic vous permettent de configurer les paramètres suivants pour les connexions utilisateur :

- Mise en œuvre de délais d'expiration plus courts pour les applications sensibles accessibles à partir de réseaux non fiables.
- Basculement du trafic réseau pour utiliser le protocole TCP pour certaines applications. Si vous sélectionnez TCP, vous devez activer ou désactiver l'authentification unique pour certaines applications.
- Identifier les situations dans lesquelles vous souhaitez utiliser d'autres fonctionnalités HTTP pour le trafic client Citrix Secure Access.
- Définir les extensions de noms de fichiers utilisées avec l'association de types de fichiers.

Créer une stratégie de trafic

Pour configurer une stratégie de trafic, vous devez créer un profil et configurer les paramètres suivants :

- Protocole (HTTP ou TCP)
- Délai d'expiration de
- Connexion unique aux applications Web
- Formulaire d'authentification unique
- Association de type de fichier
- Plug-in de répéteur
- Comptes Kerberos Constrained Delegated (KCD)

Après avoir créé la stratégie de trafic, vous pouvez la lier aux serveurs virtuels, aux utilisateurs, aux groupes ou globalement.

Par exemple, l'application Web PeopleSoft Human Resources est installée sur un serveur du réseau interne. Vous pouvez créer une stratégie de trafic pour cette application qui définit l'adresse IP de destination, le port de destination, et vous pouvez définir la durée pendant laquelle un utilisateur peut rester connecté à l'application, par exemple 15 minutes.

Si vous souhaitez configurer d'autres fonctionnalités, telles que la compression HTTP vers une application, vous pouvez utiliser une stratégie de trafic pour configurer les paramètres. Lorsque vous créez la stratégie, utilisez le paramètre HTTP pour l'action. Dans l'expression, créez l'adresse de destination du serveur exécutant l'application.

Exemples d'expressions de stratégie de trafic

Voici les exemples d'expressions de stratégies de trafic :

- `add vpn trafficPolicy trafPol1 "HTTP.REQ.URL.CONTAINS(\"/Citrix/\")|| HTTP.REQ.URL.CONTAINS(\"10.102.\")")"trafAct1`
- `add vpn trafficPolicy trafPol2 "HTTP.REQ.HOSTNAME.CONTAINS(\"portal-srv\")|| HTTP.REQ.URL.CONTAINS(\"homePage\"))"trafAct2`
- `add vpn trafficPolicy trafPol3 true trafAct3`

Configurer une stratégie de trafic à l'aide de l'interface graphique

1. Développez **NetScaler Gateway > Stratégies**, puis cliquez sur **Trafic**.
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue **Créer une stratégie de trafic**, dans **Nom**, tapez un nom pour la stratégie.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans **Protocole**, sélectionnez **HTTP** ou **TCP**.

   Remarque : Si vous sélectionnez TCP comme protocole, vous ne pouvez pas configurer l'authentification unique et le paramètre est désactivé dans la boîte de dialogue du profil.
7. Dans **AppTimeout (minutes)**, tapez le nombre de minutes. Ce paramètre limite la durée pendant laquelle les utilisateurs peuvent rester connectés à l'application Web.
8. Pour activer l'authentification unique sur l'application Web, dans **Single Sign-On**, sélectionnez **Activé**.

Remarque : Si vous souhaitez utiliser l'authentification unique basée sur des formulaires, vous pouvez configurer les paramètres dans le profil de trafic. Pour plus d'informations, consultez Configuration de l'authentification unique basée sur les formulaires.

9. Pour spécifier une association de type de fichier, dans **Association de types de fichiers**, sélectionnez **ON**.
10. Pour utiliser le plug-in du répéteur afin d'optimiser le trafic réseau, dans Citrix SD-WAN, sélectionnez **ON**, cliquez sur **Créer**, puis sur **Fermer**.
11. Si vous configurez KCD sur l'appliance, dans Compte KCD, sélectionnez le compte.

    Pour plus d'informations sur la configuration de KCD sur le dispositif, consultez Configuration de la délégation contrainte Kerberos sur un dispositif NetScaler.
12. Dans la boîte de dialogue Créer une politique de trafic, créez ou ajoutez une expression, cliquez sur **Créer,** puis sur **Fermer**.

Configuration de l'authentification unique basée sur les formulaires

L'authentification unique basée sur les formulaires permet aux utilisateurs de se connecter une fois à toutes les applications protégées de votre réseau. Lorsque vous configurez l'authentification unique basée sur un formulaire dans NetScaler Gateway, les utilisateurs peuvent accéder aux applications Web qui nécessitent une connexion basée sur un formulaire HTML sans avoir à saisir à nouveau leur mot de passe. Sans authentification unique, les utilisateurs doivent ouvrir une session séparément pour accéder à chaque application.

Après avoir créé le profil d'authentification unique du formulaire, vous créez un profil de trafic et une stratégie qui inclut le profil d'authentification unique du formulaire. Pour plus d'informations, consultez la section Création d'une stratégie de trafic.

Configuration de l'authentification unique basée sur les formulaires

1. Développez **NetScaler Gateway > Politiques,** puis cliquez sur **Trafic**.
2. Dans le volet d'informations, cliquez sur l'onglet **Form SSO Profiles**, puis sur **Ajouter**.
3. Dans **Nom**, saisissez le nom du profil.
4. Dans **URL de l'action**, saisissez l'URL à laquelle le formulaire rempli est envoyé.

   Remarque : L'URL est l'URL relative racine.
5. Dans **Nom d'utilisateur**, tapez le nom de l'attribut du champ de nom d'utilisateur.
6. Dans **Mot de passe**, tapez le nom de l'attribut du champ de mot de passe.

7. Dans **SSO Success Rule**, créez une expression qui décrit l'action que ce profil entreprend lorsqu'il est invoqué par une politique. Vous pouvez également créer l'expression à l'aide des boutons Préfixe, Ajouter et Opérateur situés sous ce champ.

   Cette règle vérifie si l'authentification unique est réussie ou non.

8. Dans **Paire de valeurs de nom**, tapez la valeur du champ du nom d'utilisateur, suivie d'une esperluette (&), puis de la valeur du champ de mot de passe.

   Les noms des valeurs sont séparés par une esperluette (&), telle que name1=value1&name2=value2.

9. Dans **la zone Taille de réponse**, tapez le nombre d'octets pour permettre la taille complète de la réponse. Tapez le nombre d'octets de la réponse à analyser pour extraire les formulaires.
10. Dans **Extraction**, sélectionnez si la paire nom/valeur est statique ou dynamique. Le paramètre par défaut est Dynamique.
11. Dans **Méthode d'envoi**, sélectionnez la méthode HTTP utilisée par le formulaire d'authentification unique pour envoyer les informations d'identification de connexion au serveur d'ouverture de session. La valeur par défaut est Obtenir.
12. Cliquez sur **Créer,** puis sur **Fermer**.

Configuration de l'authentification unique SAML

Vous pouvez créer un profil SAML 1.1 ou SAML 2.0 pour l'authentification unique (SSO). Les utilisateurs peuvent se connecter à des applications Web prenant en charge le protocole SAML pour l'authentification unique. NetScaler Gateway prend en charge l'authentification unique par fournisseur d'identité (IdP) pour les applications Web SAML.

Configuration de l'authentification unique SAML

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway \ > Policies**, puis cliquez sur Traffic.
2. Dans le volet d'informations, cliquez sur l'onglet Profil SSO SAML.
3. Dans le volet d'informations, cliquez sur Ajouter.
4. Dans Nom, saisissez le nom du profil.
5. Dans Nom du certificat de signature, saisissez le nom du certificat X.509.
6. Dans ACS URL, entrez le service ACS (consommateur d'assertion) du fournisseur de services ou d'identités. L'URL AssertionConsumerServiceUrl (ACS URL) fournit une fonctionnalité SSO aux utilisateurs.
7. Dans Relay State Rule, créez l'expression de la stratégie à partir des expressions de stratégie enregistrées et des expressions fréquemment utilisées. Sélectionnez dans la liste Opérateur pour définir le mode d'évaluation de l'expression. Pour tester l'expression, cliquez sur Evaluer.

8. Dans Envoyer le mot de passe, sélectionnez ON ou OFF.
9. Dans Nom de l'émetteur, saisissez l'identité de l'application SAML.
10. Cliquez sur Créer, puis sur Fermer.

Liaison d'une stratégie de trafic

Vous pouvez lier des stratégies de trafic à des serveurs virtuels, à des groupes, à des utilisateurs et à NetScaler Gateway Global. Vous pouvez utiliser l'utilitaire de configuration pour lier une stratégie de trafic.

Liez une stratégie de trafic globalement à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Traffic.
2. Dans le volet d'informations, sélectionnez une politique, puis dans Action, cliquez sur Liaisons globales.
3. Dans la boîte de dialogue Bind/Unbind Traffic Policies, sous Détails, cliquez sur Insérer une stratégie.
4. Sous Nom de la stratégie, sélectionnez la stratégie, puis cliquez sur OK.

Supprimer les stratégies de trafic

Vous pouvez utiliser l'utilitaire de configuration pour supprimer les stratégies de trafic de NetScaler Gateway. Si vous utilisez l'utilitaire de configuration pour supprimer une stratégie de trafic et que la stratégie est liée au niveau de l'utilisateur, du groupe ou du serveur virtuel, vous devez d'abord dissocier la stratégie. Vous pouvez ensuite supprimer la stratégie.

Délier une stratégie de trafic à l'aide de l'interface graphique

1. Développez **NetScaler Gateway,** puis cliquez sur Serveurs **virtuels**.
    - **Développez NetScaler Gateway > Administration**des utilisateurs, puis cliquez sur **Groupes AAA**.
    - Développez **NetScaler Gateway > Administration des utilisateurs**, puis cliquez sur **Utilisateurs AAA**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, un groupe ou un utilisateur, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue **Configurer le serveur virtuel NetScaler Gateway, Configurer le groupe AAA**ou **Configurer l'utilisateur AAA**, cliquez sur l'onglet **Stratégies**.

4. Cliquez sur **Trafic**, sélectionnez la stratégie, puis cliquez sur **Unbind Policy**.
5. Cliquez sur **OK,** puis sur **Fermer**.

Une fois la stratégie de trafic non liée, vous pouvez la supprimer.

Supprimer une stratégie de trafic à l'aide de l'interface graphique

1. **Développez**NetScaler Gateway > Politiques**, puis cliquez sur Trafic.**
2. Dans le volet d'informations, sous l'onglet Stratégies, sélectionnez la stratégie de trafic, puis cliquez sur **Supprimer**.

Stratégies de session

March 27, 2024

Une stratégie de session est un ensemble d'expressions et de paramètres appliqués aux utilisateurs, aux groupes, aux serveurs virtuels et globalement.

Vous utilisez une stratégie de session pour configurer les paramètres des connexions utilisateur. Vous pouvez définir des paramètres pour configurer les logiciels avec lesquels les utilisateurs se connectent, tels que le client Citrix Secure Access pour Windows ou le client Citrix Secure Access pour Mac. Vous pouvez également configurer des paramètres pour obliger les utilisateurs à ouvrir une session avec l'application Citrix Workspace ou Secure Hub. Les stratégies de session sont évaluées et appliquées après l'authentification de l'utilisateur.

Les stratégies de session sont appliquées conformément aux règles suivantes :

- Les stratégies de session remplacent toujours les paramètres globaux de la configuration.
- Tous les attributs ou paramètres qui ne sont pas définis à l'aide d'une stratégie de session sont définis sur les stratégies établies pour le serveur virtuel.
- Tous les autres attributs qui ne sont pas définis par une stratégie de session ou par le serveur virtuel sont définis par la configuration globale.

> **Important :**
>
> Les instructions suivantes sont des instructions générales pour la création de stratégies de session. Il existe des instructions spécifiques pour configurer les stratégies de session pour différentes configurations, telles que l'accès sans client ou l'accès aux applications publiées. Les instructions peuvent contenir des instructions pour configurer un paramètre spécifique. Toutefois, ce paramètre peut être l'un des nombreux paramètres contenus dans un profil de session et une stratégie. Les instructions vous indiquent de créer un paramètre dans un profil de session,

> puis d'appliquer le profil à une stratégie de session. Vous pouvez modifier les paramètres d'un profil et d'une stratégie sans créer de stratégie de session. En outre, vous pouvez créer tous vos paramètres au niveau global, puis créer une stratégie de session pour remplacer les paramètres globaux.

Si vous déployez Citrix Endpoint Management ou StoreFront sur votre réseau, Citrix vous recommande d'utiliser l'assistant de configuration rapide pour configurer les stratégies et les profils de session. Lorsque vous exécutez l'assistant, vous définissez les paramètres de votre déploiement. NetScaler Gateway crée ensuite les stratégies d'authentification, de session et d'accès sans client requises.

Créer une stratégie de session

1. Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez NetScaler Gateway > Policies, puis cliquez sur Session.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. À côté de Demander un profil, cliquez sur Nouveau.
5. Dans Nom, saisissez le nom du profil.
6. Renseignez les paramètres du profil de session, puis cliquez sur Créer.
7. Dans la boîte de dialogue Créer un profil de session, ajoutez une expression pour la stratégie, cliquez sur Créer, puis sur Fermer.
   Remarque : Dans l'expression, sélectionnez Valeur
   vraie pour que la stratégie soit toujours appliquée au niveau auquel elle est liée.

Exemples d'expressions de stratégie de session

Voici des exemples d'expressions de stratégies de session :

- `add vpn sessionPolicy sessPol1 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")|| HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixWorkspace\")"sessAct1`
- `add vpn sessionPolicy sessPol2 "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT"sessAct2`
- `add vpn sessionPolicy sessPol3 true sessAct3`

Stratégies de session de liaison

Après avoir créé une stratégie de session, liez-la à un utilisateur, à un groupe, à un serveur virtuel ou globalement. Les stratégies de session sont appliquées en tant que hiérarchie dans l'ordre suivant :

- Utilisateurs
- Groups
- Serveurs virtuels
- Globalement

Liez une stratégie de session à un serveur virtuel à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**. Vous pouvez également créer un nouveau serveur virtuel.
3. Faites défiler la page jusqu'à la section **Stratégies**, puis cliquez sur l'icône **+**.
4. Dans **Choisir une stratégie**, sélectionnez **Session**.
5. Dans **Choisir le type**, sélectionnez **Demande**, puis cliquez sur **Continuer**.
6. Dans **Sélectionner une stratégie**, sélectionnez la stratégie que vous souhaitez lier à ce serveur virtuel.
7. Dans **Priorité**, saisissez le numéro de priorité de la stratégie.
8. Cliquez sur **Bind**.

Lier une stratégie de session à un groupe d'authentification, d'autorisation et d'audit à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Administration des utilisateurs > Groupes AAA**.
2. Sélectionnez un groupe d'authentification, d'autorisation et d'audit existant, puis cliquez sur **Modifier**. Vous pouvez également créer un groupe d'authentification, d'autorisation et d'audit.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies,** puis sur l'icône **+**.
4. Dans **Choisir une stratégie**, sélectionnez **Session**, puis cliquez sur **Continuer**.
5. Dans **Sélectionner une stratégie**, sélectionnez la stratégie que vous souhaitez lier à ce groupe d'authentification, d'autorisation et d'audit.
6. Dans **Priorité**, saisissez le numéro de priorité de la stratégie.
7. Cliquez sur **Bind**.

Lier une stratégie de session à un utilisateur d'authentification, d'autorisation et d'audit à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Administration des utilisateurs > Utilisateurs AAA**.

2. **Sélectionnez un utilisateur NetScaler existant, puis cliquez sur Modifier.** Vous pouvez également créer un utilisateur d'authentification, d'autorisation et d'audit.
3. Dans **Paramètres avancés**, cliquez sur **Stratégies,** puis sur l'icône **+**.
4. Dans **Choisir une stratégie**, sélectionnez **Session**, puis cliquez sur **Continuer**.
5. Dans **Sélectionner une stratégie**, sélectionnez la stratégie que vous souhaitez lier à cet utilisateur d'authentification, d'autorisation et d'audit.
6. Dans **Priorité**, saisissez le numéro de priorité de la stratégie.
7. Cliquez sur **Bind**.

Remarque : Pour plus d'informations sur la priorité, reportez-vous à la section https://support.citrix.com/article/CTX214588.

Créer un profil de session

Un profil de session contient les paramètres des connexions utilisateur.

Les profils de session spécifient les actions qui sont appliquées à une session utilisateur si la machine utilisateur répond aux conditions d'expression de stratégie. Les profils sont utilisés avec les stratégies de session. Vous pouvez utiliser l'utilitaire de configuration pour créer des profils de session séparément d'une stratégie de session, puis utiliser le profil pour plusieurs stratégies. Vous ne pouvez utiliser qu'un seul profil avec une stratégie.

Configuration des paramètres réseau pour les connexions utilisateur dans un profil de session

Vous pouvez utiliser l'onglet **Configuration réseau** du profil de session pour configurer les paramètres réseau suivants pour les connexions utilisateur :

- Serveur DNS
- Adresse IP du serveur WINS
- Adresse IP mappée que vous pouvez utiliser comme adresse IP intranet
- Paramètres de débordement pour les pools d'adresses (adresses IP intranet)
- Suffixe DNS IP Intranet
- Ports HTTP
- Paramètres de délai d'expiration forcée

Configurer les paramètres de connexion dans un profil de session

Vous pouvez utiliser l'onglet **Expérience client** du profil de session pour configurer les paramètres de connexion suivants :

- Interface d'accès ou page d'accueil personnalisée

- Adresse Web pour la messagerie Web, telle qu'Outlook Web Access
- type de plug-in (client Citrix Secure Access pour Windows ou client Citrix Secure Access pour macOS X)
- Split tunneling
- Paramètres de temporisation de session et d'inactivité
- Accès sans client
- Encodage d'URL d'accès sans client
- type de plug-in (Windows ou Mac)
- Connexion unique aux applications Web
- Index des informations d'identification pour l'authentification
- Connexion unique avec Windows
- Comportement de nettoyage du client
- Scripts d'ouverture de session
- Paramètres de débogage du client
- Split DNS
- Accès aux adresses IP du réseau privé et à l'accès LAN local
- Choix du client
- Paramètres du proxy

Pour plus d'informations sur la configuration des paramètres des connexions utilisateur, consultez la section Configuration des connexions pour le client Citrix Secure Access.

Configuration des paramètres de sécurité dans un profil de session

Vous pouvez utiliser l'onglet **Sécurité** dans un profil de session pour configurer les paramètres de sécurité suivants :

- Action d'autorisation par défaut (autoriser ou refuser)
- Secure Browse pour les connexions à partir d'appareils iOS
- Groupes de quarantaine
- Groupes d'autorisation

Pour plus d'informations sur la configuration de l'autorisation sur NetScaler Gateway, consultez la section Configurationde l'autorisation.

Configuration des paramètres Citrix Virtual Apps and Desktops dans un profil de session

Vous pouvez utiliser l'onglet **Applications publiées** dans un profil de session pour configurer les paramètres suivants pour les connexions aux serveurs exécutant Citrix Virtual Apps and Desktops :

- Proxy ICA, qui correspond aux connexions client à l'aide de l'application Citrix Workspace

- Adresse de l'interface Web
- Mode portail de l'interface Web
- Connexion unique au domaine de la batterie de serveurs
- Page d'accueil de l'application Citrix Workspace
- Adresse des services de compte

Pour plus d'informations sur la configuration des paramètres de connexion aux applications publiées dans une batterie de serveurs, consultez Fourniture d'un accès aux applications publiées et aux bureaux virtuels via l'interface Web.

Vous pouvez créer des profils de session indépendamment d'une stratégie de session. Lorsque vous créez la stratégie, vous pouvez sélectionner le profil à attacher à la stratégie.

Pour créer un profil de session à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies,** puis cliquez sur **Session**.
2. Dans le volet d'informations, cliquez sur l'onglet **Profils**, puis cliquez sur **Ajouter**.
3. Configurez les paramètres du profil, cliquez sur **Créer,** puis sur **Fermer**.

Après avoir créé un profil, vous pouvez l'inclure dans une stratégie de session.

Pour ajouter un profil à une stratégie de session à l'aide de l'interface graphique

1. Dans l'utilitaire de configuration, dans le volet de navigation, développez **Access Gateway > Policies**, puis cliquez sur **Session**.
2. Dans l'onglet **Politiques**, effectuez l'une des opérations suivantes :
   - Cliquez sur **Ajouter** pour créer une stratégie de session.
   - Sélectionnez une stratégie, puis cliquez sur **Ouvrir**.
3. Dans **Demander un profil**, sélectionnez un profil dans la liste.
4. Terminez la configuration de la stratégie de session, puis effectuez l'une des opérations suivantes :
   a) Cliquez sur **Créer,** puis cliquez sur **Fermer** pour créer la stratégie.
   b) Cliquez sur **OK,** puis cliquez sur **Fermer** pour modifier la stratégie.

Support stratégique avancé pour les signets d'entreprise

March 27, 2024

Les signets d'entreprise (URL VPN) peuvent être configurés sous forme de stratégies avancées.

> **Remarques :**
>
> - NetScaler Gateway prend en charge les protocoles HTTP, HTTPS et RDP pour les signets d'entreprise.
> - NetScaler Gateway prend uniquement en charge les URL absolues pour les signets d'entreprise.

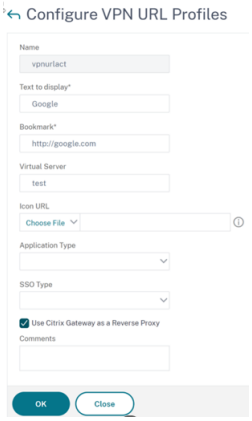
Configurer l'URL VPN en tant que stratégie avancée

Sur l'interface graphique

1. Créez un profil d'URL VPN.
    - Accédez à **Configuration > NetScaler Gateway > Stratégies > URL VPN**.
    - Sur la page **Stratégies et profils d'URL VPN**, sélectionnez l'onglet **Profils d'URL VPN** et cliquez sur **Ajouter**.
    - Mettez à jour les champs obligatoires et cliquez sur **Créer**.
        - Nom : nom du profil URL du VPN.
        - Texte à afficher : brève description du lien. La description apparaît sur l'interface d'accès.
        - Signet : adresse Web de l'application.
        - Serveur virtuel : nom du serveur virtuel d'équilibrage de charge ou de commutation de contenu associé qui est configuré. Ce champ est facultatif.
        - URL de l'icône : les icônes téléchargées dans ce champ sont prises en charge pour tous les thèmes à l'exception du thème par défaut. La taille maximale recommandée est de 70 x 70 pixels. Nous vous recommandons d'utiliser des images transparentes. Ce champ est facultatif.
        - Type d'application : sélectionnez le type d'application (VPN, VPN sans client ou SaaS) que l'URL représente. Ce champ est facultatif.
        - Type SSO : type SSO que vous souhaitez configurer pour le favori. Lorsque l'authentification unique est configurée, les utilisateurs peuvent accéder aux applications sans avoir à saisir leurs informations d'identification lors des connexions suivantes. Les types de SSO suivants sont pris en charge :
            * Unified Gateway : cette configuration SSO permet un accès distant sécurisé à plusieurs ressources d'une application via une seule URL.
            * Auto-authentification : dans cette configuration SSO, les utilisateurs de NetScaler Gateway sont invités à fournir les informations de connexion pour accéder à l'application.

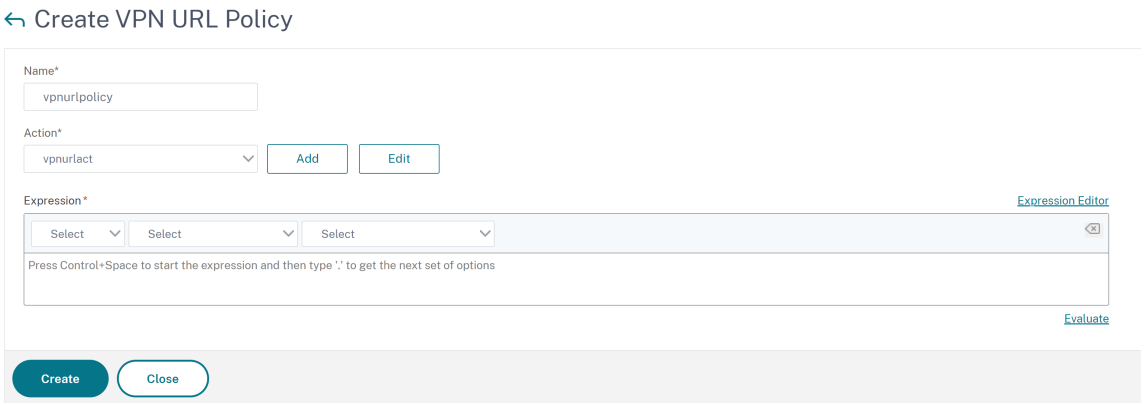
* Authentification basée sur SAML : dans cette configuration SSO, NetScaler Gateway utilise un IdP pour valider les détails de l'utilisateur, génère une assertion SAML et l'envoie au SP. Si la validation est réussie, le SSO est réussi.

> **Note:**
>
> If you enable clientless access, you can make sure that requests to websites go through NetScaler Gateway. For example, you added a bookmark for Google. Select the Use NetScaler Gateway as a reverse proxy check box. When you select this check box, website requests go from the user device to NetScaler Gateway and then to the website. When you clear the check box, requests go from the user device to the website. This check box is only available if you enable clientless access.



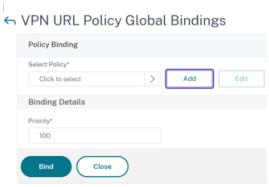
2. Créez une stratégie d'URL VPN.

   - Accédez à **Configuration > NetScaler Gateway > Stratégies > URL VPN**.
   - Sur la page **Stratégies et profils d'URL VPN**, sélectionnez l'onglet **Stratégie d'URL VPN** et cliquez sur **Ajouter**.
   - Mettez à jour les champs obligatoires et cliquez sur **Créer**.
     - Nom : nom de la stratégie d'URL du VPN.
     - Action : Sélectionnez le profil d'URL VPN configuré. Si aucun profil ne figure dans la liste déroulante, cliquez sur Ajouter et répétez l'étape 1.
     - Expression : reportez-vous à la section Stratégies et expressions pour plus d'informations sur les expressions de stratégie avancées.



3. Liez la stratégie d'URL VPN à un point de liaison.

   - Accédez à **Configuration > NetScaler Gateway > Stratégies > URL VPN**.
   - Sur la page **Stratégies et profils d'URL VPN**, sélectionnez l'onglet **Stratégie d'URL VPN**.
   - Sélectionnez **Global Bindings** dans la liste déroulante **Sélectionner une action**.
   - Sélectionnez la stratégie d'URL du VPN. Si aucune stratégie n'est répertoriée, cliquez sur **Ajouter** et répétez l'étape 2.
   - Dans la section **Détails de liaison**, attribuez une priorité à la stratégie d'URL du VPN.



Sur la CLI

Créez une action d'URL VPN :

À l'invite de commandes, tapez ce qui suit :

```
add vpn urlAction <name> -linkName <string> -actualURL <string> \[-
    vServerName <string>] \[-clientlessAccess \( ON | OFF )] \[-comment
    <string>] \[-iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype
     <applicationtype>] \[-samlSSOProfile <string>]
```

NetScaler Gateway prend en charge les opérations suivantes pour les actions sur les URL VPN :

- **ajouter**

```
add vpn urlAction <name> -linkName <string> -actualURL <string>
    \[-vServerName <string>] \[-clientlessAccess \( ON | OFF )]
    \[-comment <string>] \[-iconURL <URL>] \[-ssotype <ssotype>]
```



```
        \[-applicationtype <applicationtype>] \[-samlSSOProfile <
        string>]
```

- **lot**

```
1   set vpn urlAction <name> \[-vServerName <string>] \[-
       clientlessAccess \( ON | OFF )] \[-comment <string>] \[-
       iconURL <URL>] \[-ssotype <ssotype>] \[-applicationtype <
       applicationtype>] \[-samlSSOProfile <string>]
```

- **désinstaller**

```
1   unset vpn urlAction <name> [-vServerName] [-clientlessAccess] [-
       comment] [-iconURL] [-ssotype] [-applicationtype] [-
       samlSSOProfile]
```

> **Remarque :**
>
> Si vous définissez l'accès sans client sur Activé, vous pouvez vous assurer que les demandes adressées aux sites Web passent de la machine utilisateur à NetScaler Gateway, puis au site Web.

- **show**

```
1    show vpn urlAction [<name>]
```

- **supprimer**

```
1   remove vpn urlAction <name>
```

- **renommer**

```
1   rename vpn urlAction <name>@ <newName>@
```

Créez une stratégie d'URL VPN :

NetScaler Gateway prend en charge les opérations suivantes pour la stratégie d'URL VPN :

- **ajouter**

```
1   add vpn urlPolicy <name> -rule <expression> -action <string> [-
       comment <string>] [-logAction <string>]
```

- **lot**

```
1   set vpn urlPolicy <name> [-rule <expression>] [-action <string>]
       [-comment <string>] [-logAction <string>]
```

- **désinstaller**

```
1   unset vpn urlPolicy <name> [-comment] [-logAction]
```


- **show**

```
show vpn urlPolicy [<name>]
```

- **supprimer**

```
remove vpn urlPolicy <name>
```

- **renommer**

```
rename vpn urlpolicy <name>@ <newName>@
```

- **stat**

```
stat vpn urlpolicy \[<name>] \[-detail] \[-fullValues] \[-ntimes
   <positive\_integer>] \[-logFile <input\_filename>] \[-
   clearstats \( basic | full )]
```

Liez la stratégie à un point de liaison :

NetScaler Gateway prend en charge les opérations suivantes pour la liaison aux règles d'URL VPN :

- **lier**

```
bind vpn vserver <vserver name> -policy <string> -priority <
   positive_integer> [-gotoPriorityExpression <expression>]
bind vpn global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>]
bind aaa user <userName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
bind aaa group <groupName> -policy <string> [-priority <
   positive_integer>] [-type <type>] [-gotoPriorityExpression <
   expression>]
```

- **délier**

```
unbind vpn vserver <name> -policy <string>
unbind vpn global -policyName <string>
unbind aaa user <name> -policy <string>
unbind aaa group <name> -policy <string>
```

> **Remarque :**
>
> Les points de liaison sont,`aaauseraaagroup`,`vpnvserver` et `vpnglobal`.

Stratégies Endpoint

March 27, 2024

Endpoint Analysis (EPA) est un processus qui analyse l'appareil d'un utilisateur et détecte des informations, telles que la présence et le niveau de version des mises à jour du système d'exploitation, de l'antivirus, du pare-feu et du logiciel de navigation Web. Endpoint Analysis vous permet de déterminer si l'appareil d'un utilisateur répond à vos besoins avant qu'il ne se connecte à votre réseau. Il peut également être configuré pour vérifier périodiquement les modifications tout en maintenant la connexion de l'utilisateur. Vous pouvez vérifier les fichiers, les processus et les entrées de registre sur la machine utilisateur pendant la session utilisateur pour vous assurer que l'appareil continue de répondre aux exigences.

> **Important :**
>
> - Endpoint Analysis est destiné à analyser l'appareil de l'utilisateur par rapport à des critères de conformité prédéterminés et n'impose ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d'utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.
> - Le client EPA est disponible en tant que client autonome et est également intégré au client Citrix Secure Access. Le client Citrix EPA et le client Citrix Secure Access sont indépendants l'un de l'autre.

Fonctionnent des stratégies Endpoint

Vous pouvez configurer NetScaler Gateway pour vérifier si une machine utilisateur répond à certaines exigences avant qu'un utilisateur ne se connecte. C'est ce que l'on appelle une stratégie de pré-authentification. Vous pouvez configurer NetScaler Gateway pour vérifier la présence d'un antivirus, d'un pare-feu, d'un antispam, de processus, de fichiers, d'entrées de registre, de sécurité Internet ou de systèmes d'exploitation que vous spécifiez dans la stratégie. Si l'analyse de pré-authentification échoue sur la machine utilisateur, les utilisateurs ne sont pas autorisés à se connecter.

Pour vérifier d'autres exigences qui ne sont pas utilisées dans une stratégie de pré-authentification, vous pouvez configurer une stratégie de session et la lier à un utilisateur ou à un groupe. Ce type de stratégie est appelé stratégie de post-authentification, qui s'exécute pendant la session utilisateur afin de garantir la conformité des critères requis, tels qu'un logiciel antivirus ou un processus.

Lorsque vous configurez une stratégie de pré-authentification ou de post-authentification, NetScaler Gateway télécharge le plug-in Endpoint Analysis, puis exécute le scan sur l'appareil de l'utilisateur. Chaque fois qu'un utilisateur ouvre une session, le plug-in Endpoint Analysis s'exécute automatiquement.

Vous pouvez utiliser les trois types de stratégies suivants pour configurer les stratégies relatives aux terminaux :

- Stratégie de préauthentification qui utilise un paramètre Oui ou Non. L'analyse détermine si la machine utilisateur répond aux exigences spécifiées. Si l'analyse échoue, l'utilisateur ne peut

pas entrer d'informations d'identification sur la page d'ouverture de session.
- Stratégie de session conditionnelle pouvant être utilisée pour SmartAccess.
- Expression de vérification de l'appareil client dans le cadre d'une stratégie de session. Si la machine utilisateur ne répond pas aux exigences de l'expression de vérification de l'appareil client, vous pouvez configurer les utilisateurs pour qu'ils soient placés dans un groupe de quarantaine. Si la machine utilisateur réussit l'analyse, les utilisateurs peuvent être placés dans un autre groupe qui peut nécessiter d'autres vérifications.

Vous pouvez intégrer les informations détectées dans des stratégies, ce qui vous permet d'accorder différents niveaux d'accès en fonction de l'appareil utilisateur. Par exemple, vous pouvez fournir un accès complet avec une autorisation de téléchargement aux utilisateurs qui se connectent à distance à partir de machines utilisateur qui ont des exigences actuelles en matière de logiciels antivirus et de pare-feu. Pour les utilisateurs qui se connectent à partir d'appareils non conformes, vous pouvez fournir un niveau d'accès plus restreint qui permet aux utilisateurs de modifier des documents sur des serveurs distants sans les télécharger. Tous les appareils exécutant l'EPA sont considérés comme des appareils non conformes.

Endpoint Analysis effectue les étapes de base suivantes :

- Examine un premier ensemble d'informations concernant la machine utilisateur afin de déterminer les analyses à appliquer.
- Exécute toutes les analyses applicables. Lorsque les utilisateurs essaient de se connecter, le plug-in Endpoint Analysis vérifie que l'appareil utilisateur répond aux exigences spécifiées dans la stratégie de pré-authentification ou de session. Si la machine utilisateur réussit l'analyse, les utilisateurs sont autorisés à ouvrir une session. Si la machine utilisateur échoue à l'analyse, les utilisateurs ne sont pas autorisés à ouvrir une session.

  Remarque : Les analyses d'Endpoint Analysis sont terminées avant que la session utilisateur utilise une licence.
- Compare les valeurs de propriété détectées sur la machine utilisateur avec les valeurs de propriété souhaitées répertoriées dans vos scans configurés.
- Produit une sortie vérifiant si les valeurs de propriété souhaitées sont trouvées.

> **Attention :**
>
> Les instructions relatives à la création de stratégies Endpoint Analysis sont des instructions générales. Vous pouvez avoir plusieurs paramètres au sein d'une même stratégie de session. Les instructions spécifiques de configuration des stratégies de session peuvent contenir des instructions pour configurer un paramètre spécifique. Toutefois, ce paramètre peut être l'un des nombreux paramètres contenus dans un profil de session et une stratégie.

Exemples d'expressions EPA

Vous trouverez ci-dessous des exemples d'expression de certains composants de l'EPA tels que le processus de suppression, la suppression de fichiers et le certificat de périphérique :

- Windows :
  - Kill process: `sys.client_expr(\"proc_0_perl\")-killProcess processToKill.exe`
  - Device certificate :`sys.client_expr("device-cert_0_0")`
  - Delete files :`sys.client_expr(\"proc_0_perl\")-deletefiles "C:/removefile.txt"`
- MAC
  - Kill process: `sys.client_expr(\"proc_0_perl\")-killProcess processToKill.exe`
  - Device cert:`sys.client_expr("device-cert_0_0")`
  - Delete files:`sys.client_expr(\"proc_0_perl\")-deletefiles "C:/removefile.txt"`

Évaluer les options de connexion des utilisateurs

Lorsque les utilisateurs ouvrent une session, ils peuvent choisir d'ignorer l'analyse Endpoint Analysis. Si les utilisateurs ignorent l'analyse, NetScaler Gateway considère cette action comme un échec d'Endpoint Analysis. Lorsque les utilisateurs échouent au scan, ils n'ont accès qu'à l'interface Web ou via un accès sans client.

Par exemple, vous souhaitez fournir un accès aux utilisateurs à l'aide du client Citrix Secure Access. Pour se connecter à NetScaler Gateway à l'aide du plug-in, les utilisateurs doivent exécuter une application antivirus, telle que Norton Antivirus. Si la machine utilisateur n'exécute pas l'application, les utilisateurs peuvent ouvrir une session avec Receiver uniquement et utiliser les applications publiées. Vous pouvez également configurer l'accès sans client, ce qui limite l'accès à des applications spécifiées, telles qu'Outlook Web Access.

Pour configurer NetScaler Gateway afin de réaliser ce scénario d'ouverture de session, vous attribuez une stratégie de session restrictive comme stratégie par défaut. Vous configurez ensuite les paramètres pour mettre à niveau les utilisateurs vers une stratégie de session privilégiée lorsque la machine utilisateur réussit l'analyse Endpoint Analysis. À ce stade, les utilisateurs ont accès à la couche réseau et peuvent se connecter avec le client Citrix Secure Access.

Pour configurer NetScaler Gateway afin d'appliquer d'abord la stratégie de session restrictive, effectuez les étapes suivantes :

- Configurez les paramètres globaux avec le proxy ICA activé et tous les autres paramètres nécessaires si l'application spécifiée n'est pas exécutée sur la machine utilisateur.
- Créez une stratégie de session et un profil qui activent le client Citrix Secure Access.
- Créez une expression dans la partie règle de la stratégie de session pour spécifier l'application, telle que `(client.application.process(symantec.exe)exists)`

  Lorsque les utilisateurs ouvrent une session, la stratégie de session est appliquée en premier. Si Endpoint Analysis échoue ou si l'utilisateur ignore l'analyse, NetScaler Gateway ignore les paramètres de la stratégie de session (l'expression de la stratégie de session est considérée comme fausse). Par conséquent, les utilisateurs ont un accès restreint à l'aide de l'interface Web ou d'un accès sans client. Si Endpoint Analysis réussit, NetScaler Gateway applique la stratégie de session et les utilisateurs bénéficient d'un accès complet avec le client Citrix Secure Access.

Ignorer l'analyse EPA

Vous pouvez ignorer l'analyse EPA pour la post-authentification et l'authentification avancée uniquement. Skip EPA est disponible sur les navigateurs de tous les systèmes d'exploitation pris en charge. Les utilisateurs doivent cliquer sur le bouton **Ignorer l'EPA** qui apparaît lorsqu'ils accèdent à la passerelle. Si les utilisateurs ignorent l'analyse, NetScaler Gateway considère cette action comme un échec d'Endpoint Analysis. Lorsque les utilisateurs échouent au scan, ils n'ont accès qu'à l'interface Web ou via un accès sans client.

Voir aussi https://support.citrix.com/article/CTX200748.

Analyses Endpoint Analysis prises en charge pour Ubuntu

Les analyses EPA (Endpoint Analysis) suivantes sont prises en charge pour le plug-in EPA installé pour le système d'exploitation Ubuntu. Un exemple d'expression permettant de configurer chacun des scans est répertorié avec les scans EPA. Vous pouvez configurer ces expressions dans les stratégies d'authentification.

- **Fichier**
  - **Existence** : sys.client_expr("file_0_/home/user/test.txt")
  - **Somme de contrôle MD5** : sys.client_expr("file_0*/home/user/test.txt_md5* ce780e271debcc29f551546e
)
  - **Texte contenu dans un fichier (prise en charge des expressions régulières)** : sys.client_expr("file_0_/home/user/test.txt_search_cloud")
- **Processus**

  - **Existence** : sys.client_expr(“proc_0_perl”)
  - **Somme de contrôle MD5** : sys.client_expr(“proc_0*perl_md5* c060d3a5f97e27066cef8c116785567a”)
  - **Chemin** : sys.client_expr(“proc_0*perl_path*/usr/bin/perl”)

- **Nom du périphérique du système de fichiers ou du point de montage** : sys.client_expr(“mountpoint_0_/sys”)

Si vous utilisez des stratégies avancées, les expressions de chaque analyse peuvent être générées à partir de l’interface graphique (**Sécurité > AAA > Stratégies > Authentification > Stratégies avancées > EPA**).

Remarque : Dans la page Éditeur d’expressions, pour le client Linux, vous pouvez sélectionner **Commun,** puis **Processus, Fichier** ou **Point de montage**.

Stratégies et profils de pré-authentification

March 27, 2024

> **Important :**
>
> Endpoint Analysis vise à analyser l’appareil de l’utilisateur par rapport à des critères de conformité prédéterminés et n’applique ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d’utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.

Vous pouvez configurer NetScaler Gateway pour vérifier les appareils d’un utilisateur avant qu’il ne soit authentifié auprès de NetScaler Gateway. Cela peut être utilisé pour restreindre l’accès si l’appareil de l’utilisateur ne répond pas aux exigences de votre organisation. Les vérifications des appareils peuvent être mises en œuvre à l’aide de stratégies individuelles spécifiques à un serveur virtuel ou globalement, comme décrit dans les deux procédures suivantes.

Les stratégies de pré-authentification se composent d’un profil et d’une expression. Vous configurez le profil pour utiliser une expression permettant d’autoriser ou de refuser l’exécution d’un processus sur la machine utilisateur. Par exemple, le fichier texte, clienttext.txt, s’exécute sur l’appareil de l’utilisateur. Lorsque l’utilisateur se connecte à NetScaler Gateway, vous pouvez autoriser ou refuser l’accès selon que le fichier texte est en cours d’exécution. Si vous ne souhaitez pas autoriser les utilisateurs à se connecter lorsque le processus est en cours d’exécution, vous pouvez configurer un profil de pré-authentification pour arrêter le processus avant que les utilisateurs ne se connectent.

Vous pouvez configurer les paramètres suivants pour les stratégies de pré-authentification :

- Expression. Inclut les paramètres suivants pour vous aider à créer des expressions :

- Expression. Affiche toutes les expressions.
- Correspond à n'importe quelle expression. Configure la stratégie pour qu'elle corresponde à toutes les expressions présentes dans la liste des expressions sélectionnées.
- Correspond à toutes les expressions. Configure la stratégie pour qu'elle corresponde à toutes les expressions présentes dans la liste des expressions sélectionnées.
- Expressions tabulaires. Crée une expression composée avec les expressions existantes à l'aide des `OR (||)or AND (&&)` opérateurs.
- Forme libre avancée. Crée des expressions composées personnalisées à l'aide des noms d'expression et des `OR (||)and AND (&&)` opérateurs. Choisissez uniquement les expressions dont vous avez besoin et omettez les autres expressions de la liste des expressions sélectionnées.
- Add. Crée une expression.
- Modifier. Modifie une expression existante.
- Remove. Supprime l'expression sélectionnée de la liste des expressions composées.
- Expressions nommées. Sélectionnez une expression nommée configurée. Vous pouvez sélectionner des expressions nommées dans le menu des expressions déjà présentes sur NetScaler Gateway.
- Ajoutez une expression. Ajoute l'expression nommée sélectionnée à la stratégie.
- Remplacer l'expression. Remplace l'expression nommée sélectionnée par la stratégie.
- Expression d'aperçu. Affiche la chaîne détaillée qui est configurée sur NetScaler Gateway lorsque vous sélectionnez une expression nommée.

Configuration du profil de pré-authentification

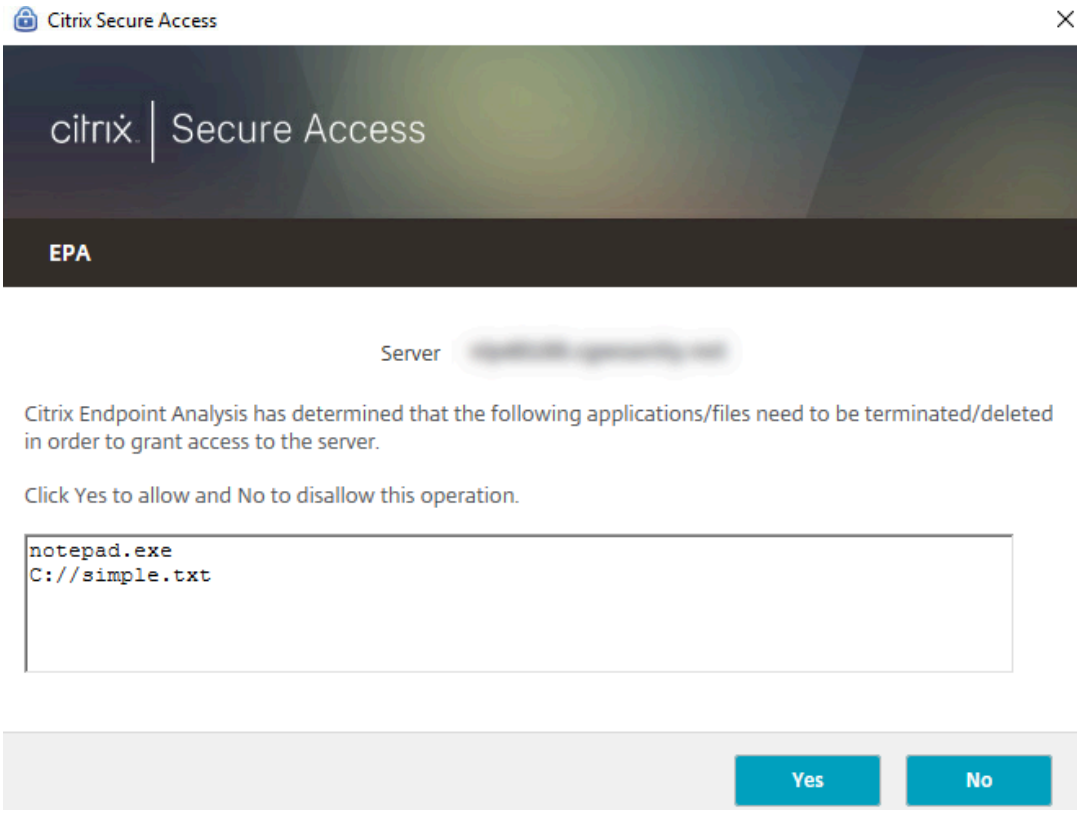
Pour configurer globalement un profil de pré-authentification à l'aide de l'interface graphique

1. Dans l'onglet Configuration, cliquez sur **NetScaler Gateway,** puis sur **Paramètres généraux**.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres de pré-authentification**.
3. Dans la boîte de dialogue **Paramètres de pré-authentification globale**, configurez les paramètres :

   a) Dans **Action**, sélectionnez **Autoriser ou Refuser**.
   Refend ou autorise les utilisateurs à ouvrir une session après l'analyse des points de terminaison.

   b) Dans **Processus à annuler**, entrez le processus.
   Ceci spécifie les processus que le plug-in Endpoint Analysis doit arrêter.

   c) Dans **Fichiers à supprimer**, entrez le nom du fichier.
   Ceci spécifie les fichiers que le plug-in Endpoint Analysis doit supprimer. Lorsque vous supprimez ou annulez un processus, une notification s'affiche pour les utilisateurs finaux.

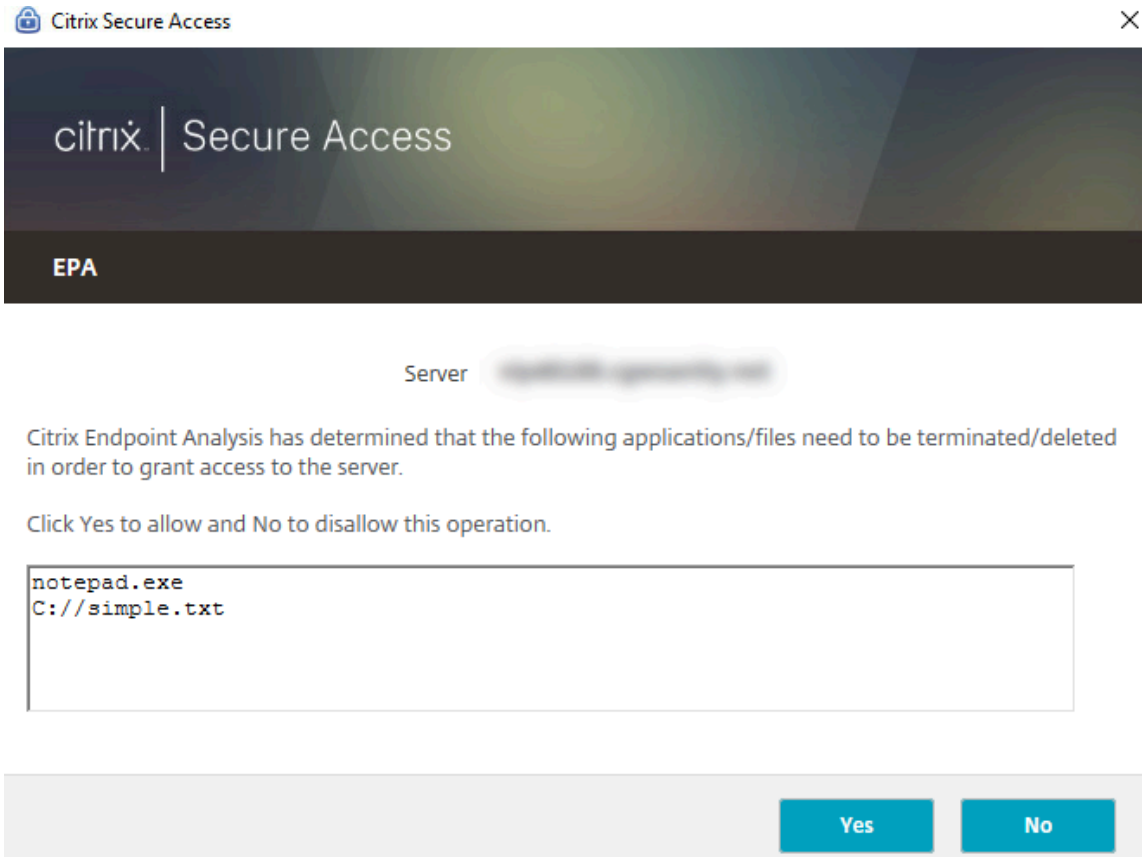


4. Dans Expression, vous pouvez laisser l'expression ns_true ou créer une expression pour une application spécifique, telle qu'un antivirus ou un logiciel de sécurité, puis cliquer sur **OK**.

Pour configurer un profil de pré-authentification à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Politiques > Authentification/Autorisation**, puis cliquez sur **Pre-Authentication EPA**.
2. Dans le volet d'informations, dans l'onglet **Profils**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de l'application à vérifier.
4. Dans **Action**, sélectionnez **AUTORISER** ou **REFUSER**.
5. Dans **Processus à annuler**, saisissez le nom du processus à arrêter.
6. Dans **Fichiers à supprimer**, tapez le nom du fichier à supprimer, par exemple c:\clientext.txt, cliquez sur **Créer,** puis cliquez sur **Fermer**.

   Ceci spécifie les fichiers que le plug-in Endpoint Analysis doit supprimer. Lorsque vous supprimez ou annulez un processus, une notification s'affiche pour les utilisateurs finaux.



Si vous utilisez l'interface graphique pour configurer un profil de préauthentification, vous créez ensuite la stratégie de préauthentification en cliquant sur **Ajouter** dans l'onglet **Stratégies**. Dans la boîte de dialogue **Créer une stratégie de pré-authentification**, sélectionnez le profil dans le menu **Demander un profil**.

Ajouter une expression préconfigurée à une stratégie de pré-authentification

NetScaler Gateway est fourni avec des expressions préconfigurées, appelées expressions nommées. Lorsque vous configurez une stratégie, vous pouvez utiliser une expression nommée pour la stratégie. Par exemple, vous souhaitez que la stratégie de pré-authentification vérifie la présence de Symantec antivirus 10 avec des définitions de virus mises à jour. Créez une stratégie de pré-authentification et ajoutez l'expression comme décrit dans la procédure suivante.

Lorsque vous créez une stratégie de pré-authentification ou de session, vous pouvez créer l'expression lorsque vous créez la stratégie. Vous pouvez ensuite appliquer la stratégie, avec l'expression, aux serveurs virtuels ou globalement.

La procédure suivante explique comment ajouter une expression antivirus préconfigurée à une stratégie à l'aide de l'utilitaire de configuration.

Ajouter une expression nommée à une stratégie de pré-authentification

1. Accédez à **NetScaler Gateway > Politiques > Authentification/Autorisation**, puis cliquez sur **Pre-Authentication EPA**.
2. Dans le volet d'informations, sélectionnez une politique, puis cliquez sur **Ouvrir**.
3. En regard de **Expressions nommées**, sélectionnez **Antivirus**, puis sélectionnez le produit antivirus dans la liste.
4. Cliquez sur **Ajouter une expression**, cliquez sur **Créer,** puis cliquez sur **Fermer**.

Configurer les expressions personnalisées

Une expression personnalisée est une expression que vous créez dans la stratégie. Lorsque vous créez une expression, vous configurez les paramètres de l'expression.

Vous pouvez également créer des expressions personnalisées pour faire référence à des chaînes couramment utilisées. Cela facilite le processus de configuration des stratégies de pré-authentification et de maintenance des expressions configurées.

Par exemple, vous souhaitez créer une expression personnalisée pour Symantec antivirus 10 et vous assurer que les définitions de virus ne datent pas de plus de trois jours. Créez une stratégie, puis configurez l'expression pour spécifier les définitions de virus.

La procédure suivante montre comment créer une expression dans une stratégie de préauthentification. Vous pouvez suivre les mêmes étapes dans une stratégie de session.

Création d'une stratégie de préauthentification et d'une expression personnalisée

1. **Accédez à**NetScaler Gateway > Politiques > Authentification/Autorisation, puis cliquez sur Pre-Authentication**EPA.**
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans la boîte de dialogue Créer un profil d'authentification, dans **Nom**, tapez un nom pour le profil et dans **Action**, sélectionnez **Autoriser**, puis cliquez sur **Créer**.
6. Dans la boîte de dialogue Créer une politique de pré-authentification, à **côté de Faire correspondre n'importe quelle expression**, cliquez sur **Ajouter**.
7. Dans **Type d'expression**, sélectionnez **Client Security**.
8. Configurez ce qui suit :

    a) Dans **Composant**, sélectionnez **Antivirus**.
    b) Dans **Nom**, saisissez le nom de l'application.
    c) Dans **Qualifier**, sélectionnez **Version**.

d) Dans **Opérateur**, sélectionnez **==**.
e) Dans **Valeur**, saisissez la valeur.
f) Dans **Fraîcheur**, tapez 3, puis cliquez sur **OK**.

9. Dans la boîte de dialogue Créer une stratégie de pré-authentification, cliquez sur **Créer**, puis sur **Fermer**.

Lorsque vous configurez une expression personnalisée, elle est ajoutée à la zone **Expression** de la boîte de dialogue de stratégie.

Configuration des expressions composées

Une stratégie de pré-authentification peut comporter un profil et plusieurs expressions. Si vous configurez des expressions composées, vous utilisez des opérateurs pour spécifier les conditions de l'expression. Par exemple, vous pouvez configurer des expressions composées pour que la machine utilisateur exécute l'une des applications antivirus suivantes :

- Symantec Antivirus 10
- McAfee Antivirus 11
- Sophos Antivirus 4

Vous configurez l'expression avec l'opérateur OR pour rechercher les trois applications précédentes. Si NetScaler Gateway détecte la version correcte de l'une des applications sur la machine utilisateur, les utilisateurs sont autorisés à se connecter. L'expression de la boîte de dialogue de stratégie apparaît comme suit :

```
av_5_Symantec_10 || av_5_McAfeevirusscan_11 || av_5_sophos_4
```

Pour plus d'informations sur les expressions composées, consultez la section Configuration des expressions composées.

Lier les stratégies de pré-authentification

Après avoir créé la stratégie de préauthentification, liez-la au niveau auquel elle s'applique. Vous pouvez lier les stratégies de pré-authentification aux serveurs virtuels ou globalement.

Créer et lier une stratégie de pré-authentification à l'échelle mondiale

1. Dans l'onglet Configuration, cliquez sur **NetScaler Gateway,** puis sur **Paramètres généraux**.
2. Dans le volet d'informations, cliquez sur **Modifier les paramètres de pré-authentification**.
3. Dans la boîte de dialogue Paramètres globaux de pré-authentification, dans **Action**, sélectionnez **Autoriser** ou **Refuser**.

4. Dans **Nom**, tapez le nom de la politique.
5. Dans la boîte de dialogue **Paramètres de pré-authentification globale**, en regard de **Expressions nommées**, sélectionnez **Général**, sélectionnez Valeur **réelle**, cliquez sur **Ajouter une expression**, cliquez sur **Créer**, puis sur **Fermer**.

Liaison d'une stratégie de pré-authentification à un serveur virtuel

1. Dans l'onglet Configuration, cliquez sur **NetScaler Gateway,** puis sur Serveurs **virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans la boîte de dialogue Configurer NetScaler Gateway Virtual Server, cliquez sur l'onglet **Stratégies**, puis sur **Pré-authentification**.
4. Sous Détails, cliquez sur **Insérer une stratégie**, puis sous Nom de la stratégie, sélectionnez la stratégie de pré-authentification.
5. Cliquez sur **OK**.

Délier et supprimer les stratégies de pré-authentification

Vous pouvez supprimer une stratégie de préauthentification de NetScaler Gateway si nécessaire. Avant de supprimer une stratégie de pré-authentification, déconnectez-la du serveur virtuel ou globalement.

Délier une stratégie de pré-authentification globale

1. Accédez à **NetScaler Gateway > Politiques > Authentification/Autorisation**, puis cliquez sur **Pre-Authentication EPA**.
2. Dans le volet d'informations, sélectionnez une politique, puis dans **Action**, cliquez sur **Liaisons globales**.
3. Dans la **boîte de dialogue Lier/délier les stratégies de pré-authentification à la stratégie globale**, sélectionnez une stratégie, cliquez sur **Délier la stratégie**, puis cliquez sur **OK**.

Délier une stratégie de pré-authentification à un serveur virtuel

1. Dans l'onglet Configuration, cliquez sur **NetScaler Gateway,** puis sur Serveurs **virtuels**.
2. Dans la boîte de dialogue **Configurer le serveur virtuel NetScaler Gateway**, cliquez sur l'onglet **Stratégies**, puis sur **Préauthentification**.
3. Sélectionnez la politique, puis cliquez sur **Dissocier la politique**.

Lorsque la stratégie de préauthentification n'est pas liée, vous pouvez la supprimer de NetScaler Gateway.

Supprimer une stratégie de pré-authentification

1. **Accédez à**NetScaler Gateway > Politiques > Authentification/Autorisation, puis cliquez sur Pre-Authentication**EPA.**
2. dans le volet d'informations, sélectionnez une politique, puis cliquez sur **Supprimer**.

Définir la priorité des stratégies de pré-authentification

Vous pouvez avoir plusieurs stratégies de pré-authentification liées à différents niveaux. Par exemple, vous avez une stratégie qui vérifie la présence d'une application antivirus spécifique liée au niveau mondial et une stratégie de pare-feu liée au serveur virtuel. Lorsque les utilisateurs ouvrent une session, la stratégie liée au serveur virtuel est appliquée en premier. La stratégie qui s'applique à l'échelle mondiale est appliquée en second lieu.

Vous pouvez modifier l'ordre dans lequel se déroulent les analyses de pré-authentification. Pour que NetScaler Gateway applique d'abord la stratégie globale, modifiez le numéro de priorité de la stratégie liée au serveur virtuel, en lui attribuant un numéro de priorité supérieur à celui de la stratégie liée globalement. Par exemple, définissez le numéro de priorité de la stratégie globale sur un et la stratégie de serveur virtuel sur deux. Lorsque les utilisateurs ouvrent une session, NetScaler Gateway exécute d'abord l'analyse des stratégies globales, puis l'analyse des stratégies du serveur virtuel.

Modifier la priorité d'une stratégie de pré-authentification

1. Dans l'onglet Configuration, cliquez sur **NetScaler Gateway,** puis sur Serveurs **virtuels**.
2. Dans le volet d'informations, sélectionnez un serveur virtuel, puis cliquez sur **Ouvrir**.
3. Dans l'onglet Politiques, cliquez sur **Pré-authentification**.
4. Sous Priorité, tapez le numéro de priorité de la stratégie, puis cliquez sur **OK**.

Stratégies de post-authentification

March 27, 2024

> **Important :**
>
> Endpoint Analysis vise à analyser l'appareil de l'utilisateur par rapport à des critères de conformité prédéterminés et n'applique ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d'utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.

Une stratégie de post-authentification est un ensemble de règles génériques que la machine utilisateur doit respecter pour maintenir la session active. Si la stratégie échoue, la connexion à NetScaler Gateway prend fin. Lorsque vous configurez la stratégie de post-authentification, vous pouvez configurer n'importe quel paramètre pour les connexions utilisateur pouvant être rendu conditionnel.

Vous utilisez des stratégies de session pour configurer les stratégies de post-authentification. Tout d'abord, vous créez les utilisateurs auxquels la stratégie s'applique. Vous ajoutez ensuite les utilisateurs à un groupe. Ensuite, vous liez la session, les stratégies de trafic et les applications intranet au groupe.

Vous pouvez également spécifier que les groupes soient des groupes d'autorisation. Ce type de groupe vous permet d'attribuer des utilisateurs à des groupes en fonction d'une expression de contrôle de l'appareil client dans la stratégie de session.

Vous pouvez également configurer une stratégie de post-authentification pour placer les utilisateurs dans un groupe de quarantaine si la machine utilisateur ne répond pas aux exigences de la stratégie. Une stratégie simple comprend une expression de contrôle de l'appareil client et un message. Lorsque les utilisateurs se trouvent dans le groupe de quarantaine, ils peuvent se connecter à NetScaler Gateway ; toutefois, ils bénéficient d'un accès limité aux ressources réseau.

Vous ne pouvez pas créer de groupe d'autorisation et de groupe de quarantaine en utilisant le même profil de session et la même stratégie. Les étapes de création de la stratégie de post-authentification sont les mêmes. Lorsque vous créez la stratégie de session, vous sélectionnez un groupe d'autorisation ou un groupe de quarantaine. Vous pouvez créer deux stratégies de session et lier chaque stratégie au groupe.

Les stratégies de post-authentification sont également utilisées avec SmartAccess. Pour de plus amples informations sur SmartAccess, consultez la section Configuration de SmartAccess sur NetScaler Gateway.

> **Remarque :**
>
> Cette fonctionnalité fonctionne uniquement avec le client Citrix Secure Access. Si les utilisateurs ouvrent une session avec l'application Citrix Workspace, l'analyse Endpoint Analysis s'exécute uniquement à l'ouverture de session.

Configurer une stratégie de post-authentification

Vous utilisez une stratégie de session pour configurer une stratégie de post-authentification. Une stratégie simple comprend une expression de contrôle de l'appareil client et un message.

Pour configurer une stratégie de post-authentification à l'aide de l'interface graphique

1. Développez **NetScaler Gateway > Policies**, puis cliquez sur **Session**.

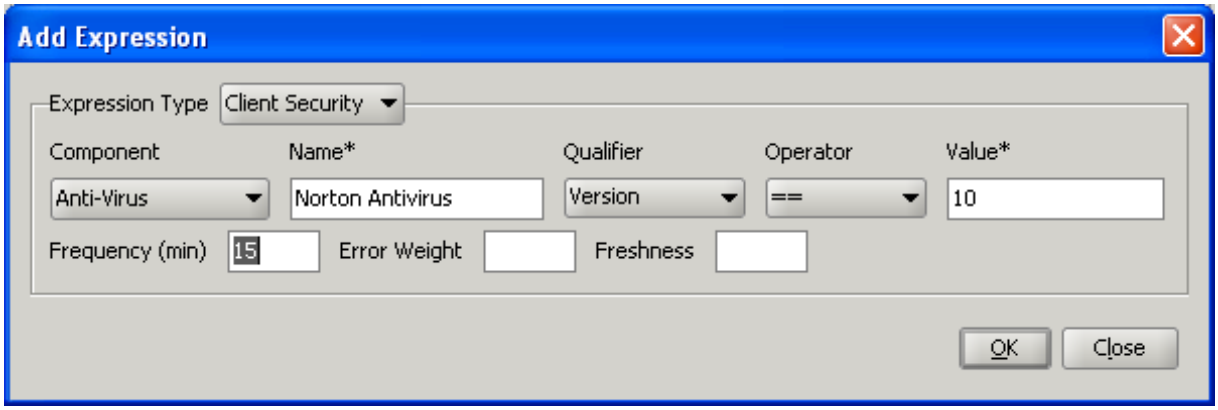
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet Sécurité, cliquez sur **Paramètres avancés**.
7. Sous **Client Security**, cliquez sur **Override Global,** puis cliquez sur **New**.
8. Configurez l'expression de contrôle de l'appareil client, puis cliquez sur **Créer**.
9. Sous **Client Security**, dans Groupe de quarantaine, sélectionnez un groupe.
10. Dans **Message d'erreur**, tapez le message que vous souhaitez que les utilisateurs reçoivent en cas d'échec de l'analyse post-authentification.
11. Sous Groupes d'autorisation, cliquez sur **Remplacer le groupe global**, sélectionnez un groupe, cliquez sur **Ajouter**, cliquez sur **OK**, puis cliquez sur **Créer**.
12. Dans la boîte de dialogue **Créer une politique de session**, à côté de Expressions nommées, sélectionnez **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression**, sur **Créer**, puis sur **Fermer**.

Configuration de la fréquence des analyses post-authentification

Vous pouvez configurer NetScaler Gateway pour exécuter la stratégie de post-authentification à des intervalles spécifiés. Par exemple, vous avez configuré une stratégie de vérification de l'appareil client et souhaitez qu'elle soit exécutée sur la machine utilisateur toutes les 10 minutes. Vous pouvez configurer cette fréquence en créant une expression personnalisée dans la stratégie.

> **Remarque :**
>
> La fonctionnalité de vérification de fréquence pour les stratégies de post-authentification fonctionne uniquement avec le client Citrix Secure Access. Si les utilisateurs ouvrent une session avec l'application Citrix Workspace, l'analyse Endpoint Analysis s'exécute uniquement à l'ouverture de session.

Vous pouvez définir la fréquence (en minutes) lorsque vous configurez la stratégie de contrôle de l'appareil client en suivant la procédure Configuration d'une stratégie post-authentification. La figure suivante montre où vous pouvez entrer une valeur de fréquence dans la boîte de dialogue **Ajouter une expression** .



Groupes de quarantaine et d'autorisation

Lorsque les utilisateurs se connectent à NetScaler Gateway, vous les attribuez à un groupe que vous configurez soit sur NetScaler Gateway, soit sur un serveur d'authentification du réseau sécurisé. Si un utilisateur échoue lors d'une analyse post-authentification, vous pouvez l'affecter à un groupe restreint, appelé groupe de quarantaine, qui limite l'accès aux ressources réseau.

Vous pouvez également utiliser des groupes d'autorisation pour restreindre l'accès des utilisateurs aux ressources réseau. Par exemple, il se peut qu'un groupe de contractuels n'ait accès qu'à votre serveur de messagerie et à un partage de fichiers. Lorsque les machines des utilisateurs répondent aux exigences de vérification des appareils que vous avez définies sur NetScaler Gateway, les utilisateurs peuvent devenir membres de groupes de manière dynamique.

Vous utilisez des paramètres globaux ou des stratégies de session pour configurer des groupes de quarantaine et d'autorisation liés à un utilisateur, un groupe ou un serveur virtuel. Vous pouvez affecter des utilisateurs à des groupes en fonction d'une expression de contrôle de l'appareil client dans la stratégie de session. Lorsque l'utilisateur est membre d'un groupe, NetScaler Gateway applique la stratégie de session en fonction de l'appartenance au groupe.

Configuration des groupes d'autorisation

Lorsque vous configurez une analyse Endpoint Analysis, vous pouvez ajouter dynamiquement des utilisateurs à un groupe d'autorisations lorsque la machine utilisateur réussit l'analyse. Par exemple, vous créez une analyse Endpoint Analysis qui vérifie l'appartenance au domaine de la machine utilisateur. Sur NetScaler Gateway, créez un groupe local appelé Domain-Joined Computers et ajoutez-le en tant que groupe d'autorisation pour tous ceux qui réussissent l'analyse. Lorsque des utilisateurs rejoignent le groupe, ils héritent des stratégies associées au groupe.

Vous ne pouvez pas lier des stratégies d'autorisation globalement ou à un serveur virtuel. Vous pouvez utiliser des groupes d'autorisation pour fournir un ensemble de stratégies d'autorisation par défaut

lorsque les utilisateurs ne sont pas configurés pour être membres d'un autre groupe sur NetScaler Gateway.

Pour configurer un groupe d'autorisations à l'aide d'une stratégie de session

1. Accédez à **NetScaler Gateway > Policies**, puis cliquez sur **Session**.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet Sécurité, cliquez sur **Paramètres avancés**.
7. Sous Groupes d'autorisation, cliquez sur **Remplacer le groupe global** et sélectionnez un groupe dans la liste déroulante.
8. Cliquez sur **Ajouter**, sur **OK**, puis sur **Créer**.
9. Dans la boîte de dialogue **Créer une politique de session**, à côté de Expressions nommées, sélectionnez **Général**, sélectionnez **Valeur vraie**, cliquez sur **Ajouter une expression, sur Créer**, puis sur**Fermer**.

Après avoir créé la stratégie de session, vous pouvez la lier à un utilisateur, un groupe ou un serveur virtuel.

Pour configurer un groupe d'autorisations global

1. Développez **NetScaler Gateway**, puis cliquez sur **Paramètres généraux**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur **Modifier les paramètres** généraux.
3. Dans l'onglet Sécurité, cliquez sur **Paramètres avancés**.
4. Sous Groupe d'autorisation, sélectionnez un groupe dans la liste déroulante.
5. Cliquez sur **Ajouter,** puis sur **OK**.

Si vous souhaitez supprimer un groupe d'autorisations globalement ou de la politique de session, dans la boîte de dialogue Paramètres de sécurité - Paramètres avancés, sélectionnez le groupe d'autorisations dans la liste, puis cliquez sur **Supprimer**.

Configuration des groupes de quarantaine

Lorsque vous configurez un groupe de quarantaine, vous configurez l'expression de contrôle de l'appareil client à l'aide de la boîte de dialogue Paramètres de sécurité - Paramètres avancés au sein d'un profil de session.

Pour configurer l'expression de contrôle de l'appareil client pour un groupe de quarantaine

1. Accédez à **NetScaler Gateway > Policies**, puis cliquez sur **Session**.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet Sécurité, cliquez sur **Paramètres avancés**.
7. Sous **Client Security**, cliquez sur **Override Global,** puis cliquez sur **New**.
8. Dans la boîte de dialogue **Expression client**, configurez l'expression de contrôle de l'appareil client, puis cliquez sur **Créer**.
9. Dans **Groupe de quarantaine**, sélectionnez le groupe.
10. Dans Message d'erreur, tapez un message décrivant le problème pour les utilisateurs, puis cliquez sur **Créer**.
11. Dans la boîte de dialogue **Créer une stratégie de session**, à côté de Expressions nommées, sélectionnez **Général**, sélectionnez **Valeur vraie**, puis cliquez sur **Ajouter une expression**.
12. Cliquez sur **Créer,** puis sur **Fermer**.

Après avoir créé la stratégie de session, liez-la à un utilisateur, un groupe ou un serveur virtuel.

> **Remarque :**
>
> Si l'analyse Endpoint Analysis échoue et que l'utilisateur est placé dans le groupe de quarantaine, les stratégies liées au groupe de quarantaine ne sont effectives que si aucune stratégie liée directement à l'utilisateur n'a un numéro de priorité égal ou inférieur à celui des stratégies liées au groupe de quarantaine.

Pour configurer un groupe de quarantaine global

1. Développez **NetScaler Gateway**, puis cliquez sur **Paramètres généraux**.
2. Dans le volet d'informations, sous Paramètres, cliquez sur **Modifier les paramètres** généraux.
3. Dans l'onglet **Sécurité**, cliquez sur **Paramètres avancés**.
4. Dans **Client Security**, configurez l'expression de contrôle de l'appareil client.
5. Dans **Groupe de quarantaine**, sélectionnez le groupe.
6. Dans **Message d'erreur**, tapez un message décrivant le problème aux utilisateurs, puis cliquez sur **OK**.

Expressions de contrôle des appareils de préauthentification pour les appareils utilisateurs

March 27, 2024

> **Important :**
>
> Endpoint Analysis vise à analyser l'appareil de l'utilisateur par rapport à des critères de conformité prédéterminés et n'applique ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d'utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.

NetScaler Gateway fournit divers contrôles de conformité des terminaux lors de l'ouverture de session de l'utilisateur ou à d'autres moments configurés au cours d'une session afin de valider les machines utilisateur. Seules les machines utilisateur qui réussissent ces vérifications sont autorisées à établir une session NetScaler Gateway.

Les types de contrôles sur les machines utilisateur que vous pouvez configurer sur NetScaler Gateway sont les suivants :

- Antispam
- Antivirus
- Stratégies de fichiers
- Sécurité sur Internet
- Système d'exploitation
- Pare-feu personnel
- Stratégies de processus
- Stratégies de registre
- Stratégies de service

Si une vérification de l'appareil échoue sur la machine utilisateur, aucune nouvelle connexion n'est établie avant la réussite d'une vérification ultérieure (dans le cas de contrôles effectués à intervalles réguliers) ; toutefois, le trafic passant par les connexions existantes continue d'emprunter un tunnel via NetScaler Gateway.

Vous pouvez utiliser l'utilitaire de configuration pour configurer des stratégies de préauthentification ou des expressions de contrôle des appareils dans le cadre de stratégies de session conçues pour effectuer des contrôles sur les machines des utilisateurs.

Configuration des expressions antivirus, pare-feu, sécurité Internet ou antispam

Vous configurez les paramètres de l'antivirus, du pare-feu, de la sécurité Internet et des politiques antispam dans la boîte de dialogue **Ajouter une expression** . Les paramètres de chaque stratégie sont les mêmes : les différences correspondent aux valeurs sélectionnées. Par exemple, si vous souhaitez vérifier la présence de Norton antivirus version 10 et de ZoneAlarm Pro sur la machine utilisateur, vous créez deux expressions dans la stratégie de session ou de pré-authentification qui spécifient le nom et le numéro de version de chaque application.

Lorsque vous sélectionnez Client Security comme type d'expression, vous pouvez configurer les éléments suivants :

- Composant : type de sécurité client, tel qu'un antivirus, un pare-feu ou une entrée de registre.
- Nom : nom de l'application, du processus, du fichier, de l'entrée de registre ou du système d'exploitation.
- Qualificatif : version ou valeur du composant pour lequel l'expression vérifie.
- Opérateur : vérifie si la valeur existe ou est égale à la valeur.
- Valeur : version de l'application pour les logiciels antivirus, pare-feu, sécurité Internet ou antispam sur la machine utilisateur.
- Fréquence : fréquence à laquelle une analyse post-authentification est exécutée, en minutes.
- Poids de l'erreur : pondération attribuée à chaque message d'erreur contenu dans une expression imbriquée lorsque plusieurs expressions ont des chaînes d'erreur différentes. Le poids détermine le message d'erreur qui s'affiche.
- Fraîcheur : définit l'âge d'une définition de virus. Par exemple, vous pouvez configurer l'expression de sorte que les définitions de virus ne datent pas de plus de trois jours.

Pour ajouter une stratégie de vérification des appareils clients à une stratégie de pré-authentification ou de session

1. Dans l'utilitaire de configuration, dans le volet de navigation, effectuez l'une des opérations suivantes :
    a) **Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
    b) **Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez**NetScaler Gateway > Policies > Authentication/Authorization, puis cliquez sur Pre-Authentication**EPA.**
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur **Ajouter**.
3. Dans Nom, tapez le nom de la stratégie.
4. En regard de Correspondance avec n'importe quelle expression, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une expression, dans Type d'expression, sélectionnez **Sécurité du client**.
6. Configurez les paramètres des éléments suivants :
    a) Dans Composant, sélectionnez l'élément à analyser.
    b) Dans Nom, tapez le nom de l'application.
    c) Dans Qualifier, sélectionnez **Version**.
    d) Dans Opérateur, sélectionnez la valeur.
    e) Dans Valeur, tapez la chaîne de contrôle de l'appareil client, cliquez sur **OK**, sur **Créer**, puis sur **Fermer**.

Configuration des stratégies de service

Un service est un programme qui s'exécute en mode silencieux sur la machine utilisateur. Lorsque vous créez une stratégie de session ou de pré-authentification, vous pouvez créer une expression qui garantit que les machines utilisateur exécutent un service particulier lorsque la session est établie.

Pour configurer une stratégie de service

1. Dans l'utilitaire de configuration, dans le volet de navigation, effectuez l'une des opérations suivantes :
    a) Dans l'utilitaire de configuration, dans l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies**, puis cliquez sur Session.
    b) Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway > Policies > Authentication/Authorization**, puis cliquez sur Pre-Authentication EPA.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. En regard de Correspondance avec n'importe quelle expression, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une expression, dans Type d'expression, sélectionnez Sécurité du client.
6. Configurez les paramètres des éléments suivants :
    a) Dans Composant, sélectionnez Service.
    b) Dans Nom, tapez le nom du service.
    c) Dans Qualificatif, laissez le champ vide ou sélectionnez Version.
    d) En fonction de votre sélection dans le Qualifier, effectuez l'une des opérations suivantes :
        - Si ce champ n'est pas renseigné, dans Opérateur, sélectionnez == ou ! =
        - Si vous avez sélectionné Version, dans Opérateur, dans Valeur, tapez la valeur, cliquez sur OK, puis cliquez sur Fermer.

Vous pouvez consulter la liste de tous les services disponibles et l'état de chacun d'eux sur un ordinateur Windows à l'emplacement suivant :

Panneau de configuration >Outils d'administration **> Services**

> **Remarque :**
>
> Le nom de service de chaque service varie de son nom répertorié. Vérifiez le nom du service en consultant la boîte de dialogue
> Propriétés.

Configuration des stratégies de processus

Lorsque vous créez une stratégie de session ou de pré-authentification, vous pouvez définir une règle qui exige que toutes les machines utilisateur disposent d'un processus particulier en cours d'exécution lorsque les utilisateurs ouvrent une session. Le processus peut être n'importe quelle application et peut inclure des applications personnalisées.

Remarque : La liste de tous les processus exécutés sur un ordinateur Windows apparaît dans l'onglet **Processus** du Gestionnaire des tâches de Windows.

Pour configurer une stratégie de processus

1. Dans l'utilitaire de configuration, dans le volet de navigation, effectuez l'une des opérations suivantes :
    a) Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway \ > Policies**, puis cliquez sur Session.
    b) Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, ouvrez **NetScaler Gateway > Policies \ > Authentication/Authorization, puis cliquez sur Pre-Authentication**EPA.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. En regard de Correspondance avec n'importe quelle expression, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une expression, dans Type d'expression, sélectionnez Sécurité du client.
6. Configurez les paramètres des éléments suivants :
    a) Dans Composant, sélectionnez Processus.
    b) Dans Nom, tapez le nom de l'application.
    c) Dans Opérateur, sélectionnez EXISTS ou NOTEXISTS, cliquez sur OK, puis sur Fermer.

Lorsque vous configurez une stratégie Endpoint Analysis (pré-authentification ou post-authentification) pour vérifier la présence d'un processus, vous pouvez configurer une somme de contrôle MD5.

Lorsque vous créez l'expression de la stratégie, vous pouvez ajouter la somme de contrôle MD5 au processus que vous vérifiez. Par exemple, si vous vérifiez si notepad.exe est en cours d'exécution sur la machine utilisateur, l'expression est :
CLIENT.APPLICATION.PROCESS (notepad.exe_md5_388b8fbc36a8558587afc90fb23a3b00) EXISTS

Configuration des stratégies du système d'exploitation

Lorsque vous créez une session ou une stratégie de préauthentification, vous pouvez configurer des chaînes de contrôle de l'appareil client afin de déterminer si l'appareil utilisateur exécute un système d'exploitation particulier lorsque les utilisateurs se connectent. Vous pouvez également configurer l'expression pour rechercher un service pack ou un correctif logiciel particulier.

Les valeurs pour Windows et Macintosh sont les suivantes :

Système d'exploitation	Valeur
macOS X	macOS
Windows 8.1	win8.1
Windows 8	win8
Windows 7	win7
Windows Vista	vista
Windows XP	`winxp`
Windows Server 2008	win2008
Windows Server 2003	win2003
Serveur Windows 2000	win2000
Plateforme Windows 64 bits	win64

Pour configurer une stratégie de système d'exploitation à l'aide de l'interface graphique

1. Dans le volet de navigation, effectuez l'une des opérations suivantes :
    a) Accédez à **NetScaler Gateway > Policies**, puis cliquez sur **Session**.
    b) Accédez à **NetScaler Gateway > Stratégies > Préauthentification**.
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. Dans **Demander une action**, sélectionnez une action existante ou créez-en une.
5. Cliquez sur **Expression Editor**.
6. Dans **Sélectionner le type d'expression**, sélectionnez **Client Security**.
7. Configurez les paramètres des éléments suivants :
    a) Dans **Composant**, sélectionnez **Système d'exploitation**.
    b) Dans **Nom**, tapez le nom du système d'exploitation.
    c) Dans Qualifier, effectuez l'une des opérations suivantes :

- Laissez ce champ vide
- Sélectionnez le **Service Pack**
- Sélectionnez **Hotfix**
- Sélectionnez la **version** (pour macOS uniquement)

d) En fonction de votre sélection à l'étape 7, dans Opérateur, effectuez l'une des opérations suivantes :

- Si le qualificatif est vide, dans Opérateur, sélectionnez EQUAL (= =), NOTEQUAL (! =), EXISTS ou NOTEXISTS.
- Si vous avez sélectionné Service Pack ou Hotfix, sélectionnez l'opérateur et, dans Valeur, saisissez la valeur.

8. Cliquez sur **Terminé**, puis cliquez sur **Fermer**.

Si vous configurez un service pack, tel que client.os, (`winxp`) `.sp` si aucun nombre ne figure dans le champ **Valeur**, NetScaler Gateway renvoie un message d'erreur car l'expression n'est pas valide.

Si le système d'exploitation comporte des Service Packs, tels que Service Pack 3 et Service Pack 4, vous pouvez configurer une vérification uniquement pour le Service Pack 4, car la présence du Service Pack 4 indique automatiquement la présence de Service Packs précédents.

Configuration des stratégies de registre

Lorsque vous créez une stratégie de session ou de pré-authentification, vous pouvez vérifier l'existence et la valeur des entrées de registre sur la machine utilisateur. La session n'est établie que si l'entrée particulière existe ou a la valeur configurée ou supérieure.

Lorsque vous configurez une expression de Registre, suivez les instructions suivantes :

- Quatre barres obliques inverses sont utilisées pour séparer les clés et les sous-clés, telles que

  HKEY_LOCAL_MACHINE\\\\SOFTWARE

- Les traits de soulignement sont utilisés pour séparer la sous-clé et le nom de la valeur associée, par exemple

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\VirusSoftware_Version

- Une barre oblique inverse (\) est utilisée pour indiquer un espace, comme dans les deux exemples suivants :

  HKEY_LOCAL_MACHINE\\\\SOFTWARE\\Citrix\\\\Secure\ Access\ Client_ProductVersion

  CLIENT.REG(HKEY_LOCAL_MACHINE\\\\Software\\\\Symantec\\Norton\ AntiVirus_Version).VALUE == 12.8.0.4 -frequency 5

Voici une expression de registre qui recherche la clé de registre du client Citrix Secure Access lorsque les utilisateurs ouvrent une session :

CLIENT.REG(secureaccess).VALUE==HKEY_LOCAL_MACHINE\\\\SOFTWARE\\\\CITRIX\\\\Secure\Access\Client

> **Remarque :**
>
> Si vous recherchez des clés et des valeurs de registre et que vous sélectionnez Advanced Free-Form dans la boîte de dialogue Expression, l'expression doit commencer par CLIENT.REG.

Les vérifications de registre sont prises en charge sous les cinq types les plus courants suivants :

- HKEY_CLASSES_ROOT
- HKEY_CURRENT_USER
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG

Les valeurs de Registre à vérifier utilisent les types suivants :

- Chaîne

  Pour le type de valeur de chaîne, la sensibilité à la casse est vérifiée.

- DWORD

  Pour le type DWORD, la valeur est comparée et doit être égale.

- String étendu

  Les autres types, tels que Binary et Multi-String, ne sont pas pris en charge.

- Seul l'opérateur de comparaison « == » est pris en charge.
- Les autres opérateurs de comparaison, tels que <, > et les comparaisons sensibles à la casse ne sont pas pris en charge.
- La longueur totale de la chaîne de Registre doit être inférieure à 256 octets.

Vous pouvez ajouter une valeur à l'expression. La valeur peut être une version du logiciel, une version du Service Pack ou toute autre valeur apparaissant dans le Registre. Si la valeur des données dans le Registre ne correspond pas à la valeur que vous effectuez le test, les utilisateurs se voient refuser l'ouverture de session.

> **Remarque :**
>
> Vous ne pouvez pas rechercher une valeur dans une sous-clé. L'analyse doit correspondre à la valeur nommée et à la valeur de données associée.

Pour configurer une stratégie de registre

1. Dans l'utilitaire de configuration, dans le volet de navigation, effectuez l'une des opérations suivantes :
    a) Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, développez **NetScaler Gateway \ > Policies**, puis cliquez sur Session.
    b) Dans l'utilitaire de configuration, sous l'onglet Configuration, dans le volet de navigation, ouvrez **NetScaler Gateway > Policies \ > Authentication/Authorization, puis cliquez sur Pre-Authentication**EPA.
2. Dans le volet d'informations, dans l'onglet Stratégies, cliquez sur Ajouter.
3. Dans Nom, tapez le nom de la stratégie.
4. En regard de Correspondance avec n'importe quelle expression, cliquez sur Ajouter.
5. Dans la boîte de dialogue Ajouter une expression, dans Type d'expression, sélectionnez Sécurité du client.
6. Configurez les paramètres des éléments suivants :
    a) Dans Composant, sélectionnez Registre.
    b) Dans Nom, tapez le nom de la clé de Registre.
    c) Dans Qualificatif, laissez le champ vide ou sélectionnez Valeur.
    d) Dans Opérateur, effectuez l'une des opérations suivantes :
        - Si le qualificatif n'est pas renseigné, sélectionnez EXISTS ou NOTEXISTS
        - Si vous avez sélectionné Valeur dans le qualificatif, sélectionnez == ou ! ==
    e) Dans Valeur, tapez la valeur telle qu'elle apparaît dans l'éditeur de registre, cliquez sur OK, puis sur Fermer.

Configurer des expressions de contrôle composées pour les appareils clients

Vous pouvez combiner des chaînes de contrôle de l'appareil client pour former des expressions de contrôle composées de l'appareil client.

Les opérateurs booléens pris en charge dans NetScaler Gateway sont les suivants :

- Et (&&)

Ou (

-

- Non (!)

Pour plus de précision, vous pouvez regrouper les chaînes entre parenthèses.

> **Remarque :**
>
> Si vous utilisez la ligne de commande pour configurer des expressions, utilisez des parenthèses pour regrouper les expressions de contrôle de l'appareil lorsque vous créez une expression composée. L'utilisation de parenthèses améliore la compréhension et le débogage de l'expression client.

Configurez les stratégies avec l'opérateur AND (&&)

L'opérateur AND (&&) fonctionne en combinant deux chaînes de contrôle de l'appareil client afin que le contrôle composé soit réussi uniquement lorsque les deux vérifications sont vraies. L'expression est évaluée de gauche à droite et si la première vérification échoue, la deuxième vérification n'est pas effectuée.

Vous pouvez configurer l'opérateur AND (&&) à l'aide du mot-clé « AND » ou des symboles « &&».

Exemple:

Ce qui suit est une vérification de l'appareil client qui détermine si la version 7.0 de l'antivirus Sophos est installée et en cours d'exécution sur l'appareil utilisateur. Il vérifie également si le service Net Logon est en cours d'exécution sur le même ordinateur.

```
CLIENT.APPLICATION.AV(sophos).version==7.0 AND CLIENT.SVC(netlogon)
EXISTS
```

Cette chaîne peut également être configurée comme suit :

```
CLIENT.APPLICATION.AV(sophos).version==7.0 && CLIENT.SVC(netlogon)
EXISTS
```

Configurer les stratégies avec l'opérateur OR (||)

L'opérateur OR (| |) fonctionne en combinant deux chaînes de contrôle de l'appareil. La vérification composée réussit lorsque l'une des vérifications est vraie. L'expression est évaluée de gauche à droite et si la première vérification réussit, la deuxième vérification n'est pas effectuée. Si le premier contrôle n'est pas réussi, le deuxième contrôle est effectué.

Vous pouvez configurer l'opérateur OR (| |) à l'aide du mot-clé `OR` ou du symbole | |.

Exemple:

Ce qui suit est une vérification de l'appareil client qui détermine si le fichier `c:\\file.txt` ou le processus `putty.exe` est en cours d'exécution sur la machine utilisateur.

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)OR (client.proc(putty.exe)
EXISTS
```


Cette chaîne peut également être configurée comme

```
client.file(c:\\\\\\\\\\file.txt)EXISTS)|| (client.proc(putty.exe)
EXISTS
```

Configurez les stratégies à l'aide de NOT (!) opérateur

L'opérateur NOT (!) ou l'opérateur de négation annule la chaîne de contrôle de l'appareil client.

Exemple:

La vérification suivante de l'appareil client est réussie si le fichier c:\sophos_virus_defs.dat file ne date pas de plus de deux jours :

```
\!(client.file(c:\\\\\\\\\\sophos\\_virus\\_defs.dat).timestamp==2dy)
```

L'analyse EPA en tant que facteur d'authentification nFactor

March 27, 2024

> **Important :**
>
> Endpoint Analysis vise à analyser l'appareil de l'utilisateur par rapport à des critères de conformité prédéterminés et n'applique ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d'utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.

Voici quelques-unes des entités de base de nFactor EPA.

Action EPA : EPA Action est un type d'action introduit pour nFactor EPA. Il contient les éléments suivants :

- Expression de vérification de l'appareil client : cette expression est envoyée au plug-in EPA de la passerelle pour évaluation.
- Groupe de réussite : ce groupe, s'il est configuré, est hérité de la session de passerelle si le résultat de l'EPA est vrai.
- Groupe de quarantaine : ce groupe, s'il est configuré, est hérité de la session de passerelle si le résultat de l'EPA est faux.
- KillProcess : Il s'agit du nom du processus auquel le processus EPA doit mettre fin.
- DeleteFiles : spécifie les chemins séparés par des virgules vers les fichiers que le processus EPA doit supprimer.

Les groupes peuvent être utilisés pendant la durée de la session pour déterminer si le client répond à certaines conditions EPA.
Si, à un facteur donné, l'EPA échoue et que la dernière action ne contient pas de « groupe de quarantaine », l'authentification est terminée pour cet utilisateur.
Si le « groupe de quarantaine » existe, l'authentification se poursuit et l'administrateur peut vérifier que le groupe accorde un accès limité. Pour plus de détails, consultez la section Exécution EPA.

Stratégie EPA : Dans nFactor, toutes les stratégies sont ajoutées avec la même syntaxe « ajouter une stratégie d'authentification ». Toutefois, le type d'action qualifie la stratégie de stratégie de l'EPA.

Facteur EPA : Le facteur EPA est un label de stratégie ordinaire. Il n'y a pas d'entité appelée facteur EPA. Une fois que la stratégie de l'EPA est liée à un facteur, elle hérite de certaines propriétés qui en font un facteur EPA.

> **Remarque :**
>
> Le terme « facteur EPA » est couramment utilisé dans ce document pour désigner un facteur soumis à des stratégies de l'EPA.

EPA —Quarantaine : si, à un facteur donné, toutes les expressions de vérification de l'appareil client issues de toutes les actions échouent, et si la dernière action contient un « groupe de quarantaine », ce groupe est ajouté à la session et le NextFactor est examiné. En d'autres termes, malgré l'échec, la présence du « groupe de quarantaine » qualifie la session à l'étape suivante. Toutefois, en raison de l'héritage d'un groupe spécial, l'administrateur peut reléguer la session à un accès restreint ou à des stratégies d'authentification supplémentaires telles que OTP ou SAML.

S'il n'y a pas de groupe de quarantaine lors de la dernière action, l'authentification se termine en cas d'échec.

L'EPA dans NFactor utilise également les entités suivantes :

- **LoginSchema :** représentation XML du formulaire de connexion. Il définit la « vue » du formulaire de connexion et possède également les propriétés d'un « facteur ».
- **Étiquette ou facteur de stratégie :** il s'agit d'un ensemble de stratégies qui sont essayées à un stade donné de l'authentification.
- **Étiquette de serveur virtuel :** le serveur virtuel est également une étiquette de stratégie, c'est-à-dire que l'on peut lier des stratégies à un serveur virtuel. Toutefois, le serveur virtuel est l'ensemble des différentes étiquettes de stratégie, car il constitue le point d'entrée de l'accès des utilisateurs.
- **facteur suivant :** il est utilisé pour spécifier l'étiquette/le facteur de stratégie à utiliser une fois que la stratégie d'authentification donnée est réussie.
- **Stratégie NO_AUTHN :** stratégie spéciale dont l'action aboutit toujours.
- **Facteur de transmission :** Il s'agit d'une étiquette ou d'un facteur de stratégie dont le schéma de connexion ne contient pas de vue. Cela indique à l'appliance NetScaler de poursuivre l'authentification au facteur donné sans intervention de l'utilisateur.

Pour plus d'informations, consultez la section Concepts, entités et terminologie nFactor.

Exclusivité mutuelle EPA Factor

EPA Factor contient une ou plusieurs stratégies de l'EPA. Une fois que les stratégies EPA sont liées à un facteur, les stratégies d'authentification standard ne sont pas autorisées sur ce facteur. Cette restriction vise à offrir la meilleure expérience utilisateur et une séparation nette de l'analyse des points de terminaison. La seule exception à cette règle est la stratégie NO_AUTHN. La stratégie NO_AUTHN étant une stratégie spéciale utilisée pour simuler un « saut en cas d'échec », elle est autorisée dans le facteur EPA.

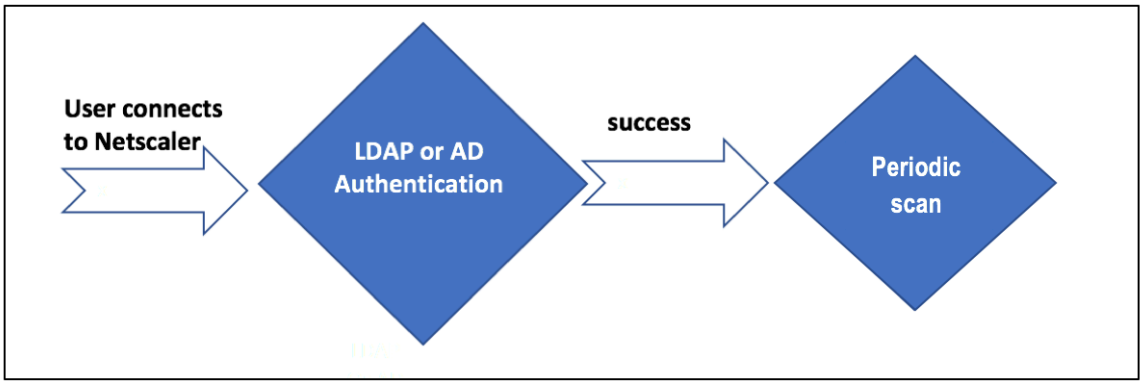
Exécution de l'EPA

Quel que soit le facteur (y compris le facteur serveur virtuel), avant de fournir le formulaire d'ouverture de session, l'appliance NetScaler vérifie si le facteur est configuré pour l'EPA. Si c'est le cas, il envoie une réponse spécifique au client (UI) de sorte que la séquence EPA soit déclenchée. Dans cette séquence, le client demande des expressions de contrôle de l'appareil client et envoie les résultats.
Les expressions de contrôle de l'appareil client pour toutes les stratégies d'un facteur sont envoyées en une seule fois au client. Une fois les résultats obtenus au niveau de l'appliance NetScaler, chacune des expressions de toutes les actions est évaluée dans un ordre. La première action qui aboutit à la réussite de l'EPA met fin à ce facteur, et DefaultGroup, s'il est configuré, est hérité dans la session. Si la stratégie NO_AUTHN est rencontrée, elle est considérée comme une réussite automatique. Si le facteur NextFactor est spécifié, l'appliance continue avec ce facteur. Sinon, l'authentification prend fin.
Cette condition s'applique également au premier facteur. S'il n'y a pas de facteur de stratégie d'authentification après l'EPA sur le serveur virtuel, l'authentification est interrompue. Ce comportement diffère du comportement de stratégie classique, où l'utilisateur affiche toujours la page de connexion après l'EPA.
Toutefois, en cas d'échec de la stratégie EPA, NetScaler Gateway examine le groupe de quarantaine configuré pour la dernière stratégie EPA dans ce facteur ou cette cascade. Si la dernière stratégie est configurée avec le groupe de quarantaine, ce groupe est ajouté à la session et le NextFactor est inspecté. S'il existe un facteur NextFactor, l'authentification passe à ce facteur. Sinon, l'authentification est terminée.

Configurer le scan EPA pour qu'il s'exécute après l'authentification

Vous pouvez configurer le scan EPA pour qu'il s'exécute après l'authentification. Dans l'exemple suivant, le scan EPA est utilisé comme vérification finale dans le cadre d'une authentification nFactor ou

multifactorielle. Dans cette configuration, si le scan EPA échoue lors d'une telle vérification, la session est terminée.



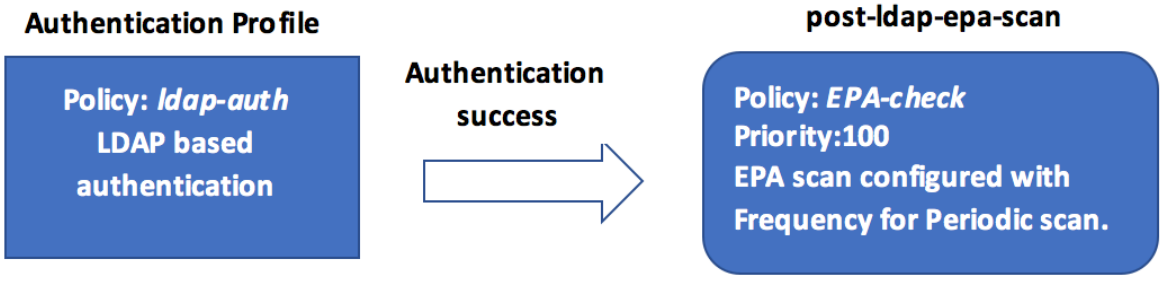
- L'utilisateur tente de se connecter à NetScaler Gateway Virtual IP.
- Une page de connexion avec un champ de nom d'utilisateur et de mot de passe est rendue à l'utilisateur pour fournir ses informations d'identification de connexion. Avec ces informations d'identification, l'authentification LDAP ou AD est effectuée au niveau du serveur principal. En cas de succès, une fenêtre contextuelle s'affiche pour autoriser l'analyse EPA.
- Une fois l'utilisateur autorisé, l'analyse EPA est effectuée et, en fonction de la réussite ou de l'échec des paramètres du client utilisateur, l'accès est fourni.
- Si l'analyse est réussie, l'analyse EPA est effectuée périodiquement pour savoir si les exigences de vérification de l'appareil configurées sont toujours satisfaites.
- Si l'analyse EPA échoue au cours d'une telle vérification, la session est interrompue.

Conditions préalables

Il est supposé que la configuration suivante est en place :

- Configuration du serveur virtuel VPN, de la passerelle et du serveur virtuel d'authentification
- Configurations du serveur LDAP et stratégies associées.

La section suivante capture les stratégies et les configurations d'étiquettes de stratégie requises, ainsi que le mappage des stratégies et des étiquettes de stratégie à un profil d'authentification.



Sur la CLI

1. Créez une action pour effectuer une analyse EPA avant l'authentification LDAP et associez-la à une stratégie d'analyse EPA.

```
add authentication epaAction pre-ldap-epa-action -csecexpr "sys.client_expr ("proc_2_firefox")"

add authentication Policy pre-ldap-epa-pol -rule true -action pre-ldap-epa-action
<!--NeedCopy-->
```

   L'expression précédente analyse si le processus « Firefox » est en cours d'exécution. Le client de l'EPA vérifie l'existence du processus toutes les 2 minutes, ce qui est indiqué par le chiffre « 2 » dans l'expression scannée.

2. Configurez l'étiquette de stratégie,`pre-ldap-epa-label` qui héberge la stratégie pour l'analyse EPA.

```
add authentication policylabel pre-ldap-epa-label -loginSchema LSCHEMA_INT
<!--NeedCopy-->
```

   > **Remarque :**
   >
   > LSCHEMA_INT est un schéma intégré sans schéma (noschema), ce qui signifie qu'aucune page Web supplémentaire n'est présentée à l'utilisateur à cette étape.

3. Associez la stratégie configurée à l'étape 1 à l'étiquette de stratégie configurée à l'étape 2. Le mécanisme d'authentification est terminé.

```
bind authentication policylabel pre-ldap-epa-label -policyName pre-ldap-epa-pol -priority 100 -gotoPriorityExpression END
<!--NeedCopy-->
```

4. Configurez une action et une stratégie LDAP.

```
add authentication ldapAction ldap-act -serverIP 10.106.103.60 -ldapBase "dc=cgwsanity,dc=net" -ldapBindDn user1@example.net -ldapBindDnPassword 1.cloud -ldapLoginName samAccountName -groupAttrName memberOf -subAttributeName CN -passwdChange ENABLED

add authentication Policy ldap-pol -rule true -action ldap-act
<!--NeedCopy-->
```

5. Créez un schéma de connexion avec le SSO activé.

```
add authentication loginSchema ldap-schema -authenticationSchema "/nsconfig/loginschema/LoginSchema/SingleAuth.xml" -SSOCredentials Yes
```



```
2 <!--NeedCopy-->
```

6. Configurez l'étiquette de stratégie, `ldap-pol-label` qui héberge la stratégie pour l'authentification LDAP.

```
1 add authentication policylabel ldap-pol-label -loginSchema ldap-
    schema
2 <!--NeedCopy-->
```

7. Liez le schéma de connexion configuré à l'étape 5 à l'étiquette de stratégie configurée à l'étape 6.

```
1 bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT
2 <!--NeedCopy-->
```

8. Créez une action pour effectuer un scan EPA après l'authentification LDAP et associez-le à une stratégie de scan EPA.

```
1 add authentication epaAction post-ldap-epa-action -csecexpr "sys.
    client_expr ("proc_2_chrome")"
2
3 add authentication Policy post-ldap-epa-pol -rule true -action
    post-ldap-epa-action
4
5 add authentication policylabel post-ldap-epa-label -loginSchema
    LSCHEMA_INT
6
7 bind authentication policylabel post-ldap-epa-label -policyName
    post-ldap-epa-pol -priority 100 -gotoPriorityExpression
8 <!--NeedCopy-->
```

9. En réunissant le tout, associez la stratégie `pre-ldap-epa-pol` au serveur virtuel d'authentification, l'étape suivante pointant vers l'étiquette de la stratégie `ldap-pol-label` pour effectuer une analyse EPA.

```
1 bind authentication vserver user.auth.test -policy pre-ldap-epa-
    pol -priority 100 -nextFactor ldap-pol-label -
    gotoPriorityExpression NEXT
2
3 bind authentication policylabel ldap-pol-label -policyName ldap-
    pol -priority 100 -gotoPriorityExpression NEXT -nextFactor post
    -ldap-epa-label
4 <!--NeedCopy-->
```

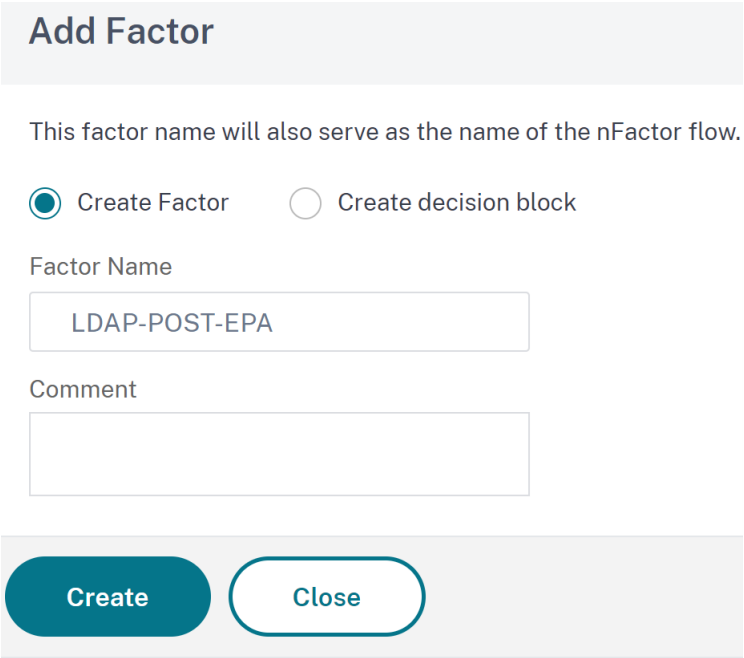
> **Remarque :**
>
> - Dans l'EPA périodique configuré en plusieurs facteurs, le dernier facteur avec une configuration EPA périodique est pris en compte.

- Les analyses périodiques ne peuvent être effectuées qu'à l'aide du plug-in EPA et non sur le navigateur.
- Dans le premier exemple, l'EPA est le premier facteur par lequel le scan recherche le processus « Firefox ».
- Si l'analyse EPA est réussie, elle entraîne une authentification LDAP, suivie du scan EPA suivant, qui recherche le processus « Chrome ».
- Lorsque plusieurs analyses périodiques sont configurées en tant que facteurs différents, la dernière analyse est prioritaire. Dans ce cas, le plug-in EPA recherche le processus « Chrome » toutes les 2 minutes après la réussite de la connexion.

Sur l'interface graphique (à l'aide de nFactor Visualizer)

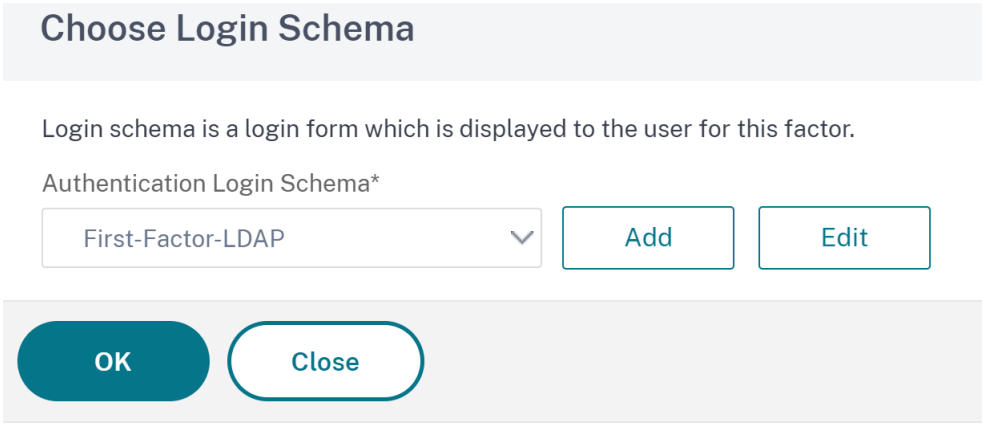
Vous pouvez configurer le scan EPA avancé en tant que facteur à l'aide du visualiseur nFactor sur l'interface graphique. Dans l'exemple suivant, nous avons utilisé le LDAP comme premier facteur et l'EPA comme facteur suivant.

1. Créez un premier facteur pour le flux nFactor.
   - Accédez à **Sécurité > Trafic des applications AAA > nFactor Visualizer > Flux nFactor**, puis cliquez sur **Ajouter**.
   - Cliquez sur **+** pour ajouter le flux nFactor.
   - Ajoutez un facteur et cliquez sur **Créer**.



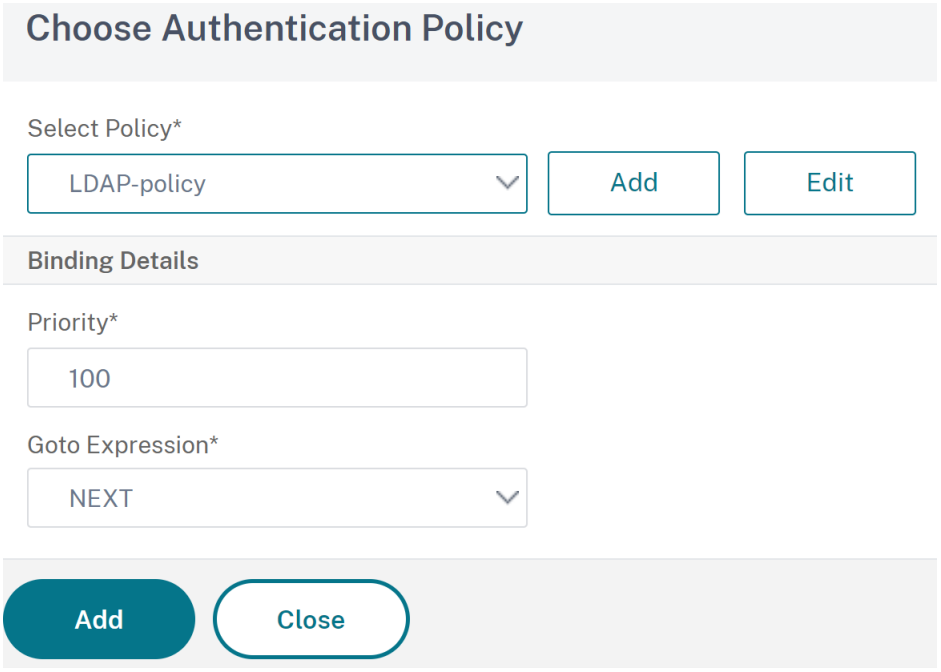
2. Créez un schéma de connexion et une stratégie pour le premier facteur.

- Sur la première vignette de facteurs, cliquez sur **Ajouter un schéma** pour ajouter un schéma de connexion. Vous pouvez sélectionner un schéma de connexion d'authentification existant dans la liste déroulante ou créer un schéma de connexion.
- Pour créer un schéma de connexion d'authentification, cliquez sur **Ajouter**. Pour des informations détaillées sur le schéma de connexion à l'authentification, consultez la section Configuration de l'authentification nFactor.



- Cliquez sur **Ajouter une stratégie** pour ajouter la stratégie LDAP. Si la stratégie LDAP est déjà créée, vous pouvez la sélectionner. Cliquez sur **Ajouter**.

> **Remarque :**
>
> Si aucune stratégie LDAP n'est créée, vous pouvez en créer une. Cliquez sur le bouton **Ajouter** à côté de la liste déroulante **Sélectionner une stratégie**. Dans le champ **Action**, sélectionnez LDAP. Pour plus d'informations sur l'ajout d'un serveur LDAP d'authentification, consultez `https://support.citrix.com/article/CTX123782`.

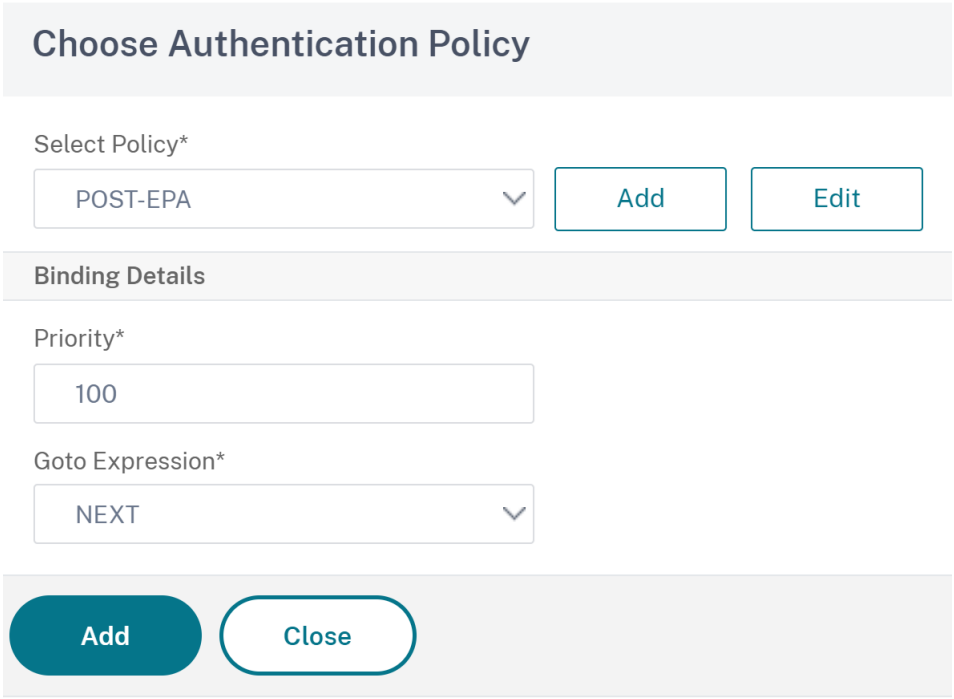


3. Créez un facteur suivant et connectez-le au premier facteur.

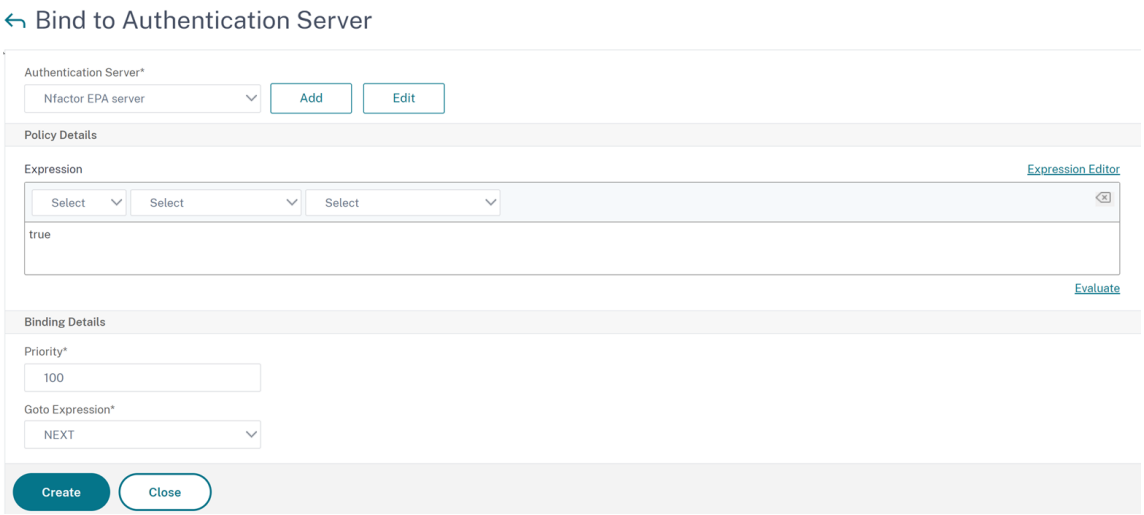
   - Cliquez sur l'icône **+** verte ou rouge pour ajouter l'EPA comme facteur suivant.
   - Créez le facteur suivant sur la page **Next Factor to Connect**.
   - Laissez la section **Ajouter un schéma** vide, afin qu'aucun schéma par défaut ne soit appliqué à ce facteur.

4. Ajoutez une stratégie pour le facteur suivant.

   - Cliquez sur **Ajouter une stratégie** pour ajouter la stratégie et l'action de l'EPA après authentification.
   - Vous pouvez choisir parmi une liste de stratégies existante ou créer une stratégie. Pour choisir parmi les stratégies existantes, sélectionnez-en une dans la liste déroulante **Sélectionner une stratégie**, fournissez les informations contraignantes, puis cliquez sur **Ajouter**.
   - Pour créer une stratégie, cliquez sur le bouton **Ajouter** à côté de la liste déroulante **Sélectionner une stratégie**.



5. Une fois le flux nFactor terminé, cliquez sur **Terminé**.
6. Liez le flux nFactor à un serveur d'authentification.
   - Accédez à **Security AAA - Trafic d'applications > nFactor Visualizer > nFactor Flows**.
   - Sélectionnez le nFactor et cliquez sur **Lier au serveur d'authentification**.



Références

- Concepts, entités et terminologie de nFactor
- Comment configurer l'authentification LDAP sur NetScaler Gateway

- Authentification LDAP
- Analyses avancées des points de terminaison

Types de classification de scan EPA sur le client Windows

March 27, 2024

> **Important :**
>
> Endpoint Analysis vise à analyser l'appareil de l'utilisateur par rapport à des critères de conformité prédéterminés et n'applique ni ne valide la sécurité des appareils des utilisateurs finaux. Il est recommandé d'utiliser des systèmes de sécurité des terminaux pour protéger les appareils contre les attaques des administrateurs locaux.

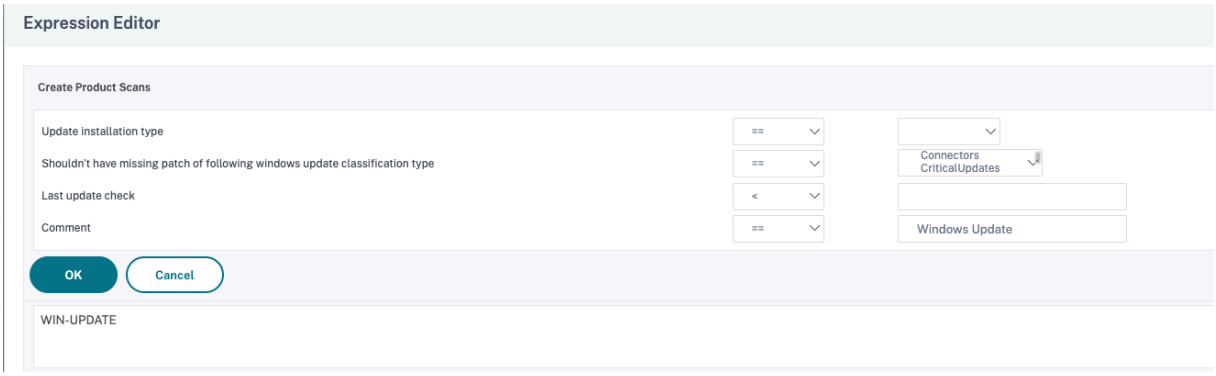
Les nouveaux types de classification suivants sont ajoutés à l'analyse EPA pour les correctifs manquants. L'analyse EPA échoue si le client possède l'un des correctifs manquants suivants.

- Application
- Connecteurs
- CriticalUpdates
- DefinitionUpdates
- DeveloperKits
- FeaturePacks
- Conseils
- SecurityUpdates
- ServicePacks
- Outils
- UpdateRollups
- Mises à jour

> **Remarques :**
>
> - Auparavant, les analyses de l'EPA pour détecter les correctifs manquants étaient effectuées selon les niveaux de gravité : critique, important, modéré et faible sur le client Windows.
> - Si vous utilisez Citrix Secure Access pour Windows 23.8.1.1 et versions ultérieures, l'analyse `CLIENT.SYSTEM('WIN-UPDATE_SCAN-TIME')` est limitée aux machines clientes sur lesquelles les mises à jour automatiques sont activées. Si les mises à jour automatiques sont désactivées, cette analyse renvoie un résultat différent.

Configurer les types de classification de scan EPA à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Stratégies > Préauthentification**.
2. Créez une nouvelle stratégie de préauthentification ou modifiez une stratégie existante.
3. Cliquez sur le lien **OPSWAT EPA Editor**.
4. Dans Expression Editor, sélectionnez **Windows > Windows Update**.
5. Dans **Should't have missing patch of the following security level**, sélectionnez le type de classification des correctifs manquants.
6. Cliquez sur **OK**.



Les clients peuvent effectuer une mise à niveau vers la version 4.3.2744.0s d'OPSWAT pour utiliser ces options.

Références

- Pour plus d'informations sur les GUID de classification des services de mise à jour Windows Server, consultez https://docs.microsoft.com/en-us/previous-versions/windows/desktop/ff357803(v=vs.85).
- Pour la description de la terminologie des mises à jour logicielles Microsoft, reportez-vous à la section https://docs.microsoft.com/en-us/troubleshoot/windows-client/deployment/standard-terminology-software-updates.

Analyses avancées des points de terminaison

March 27, 2024

L'analyse avancée des terminaux (EPA) est utilisée pour analyser les appareils des utilisateurs afin de vérifier les exigences de sécurité des terminaux configurées sur NetScaler Gateway. Si une machine utilisateur essaie d'accéder à NetScaler Gateway, elle est analysée pour détecter les informations de

sécurité, telles que le système d'exploitation, l'antivirus, les versions des navigateurs Web, etc., avant qu'un administrateur ne puisse autoriser l'accès à NetScaler Gateway. Pour plus d'informations sur la configuration système requise pour le client Citrix EPA, consultez la section Exigences relatives à Endpoint Analysis.

L'analyse EPA avancée est une analyse basée sur des règles que vous pouvez configurer sur NetScaler Gateway pour les sessions d'authentification. La stratégie effectue une vérification du registre sur une machine utilisateur et, sur la base d'une évaluation, elle autorise ou refuse l'accès au réseau NetScaler.

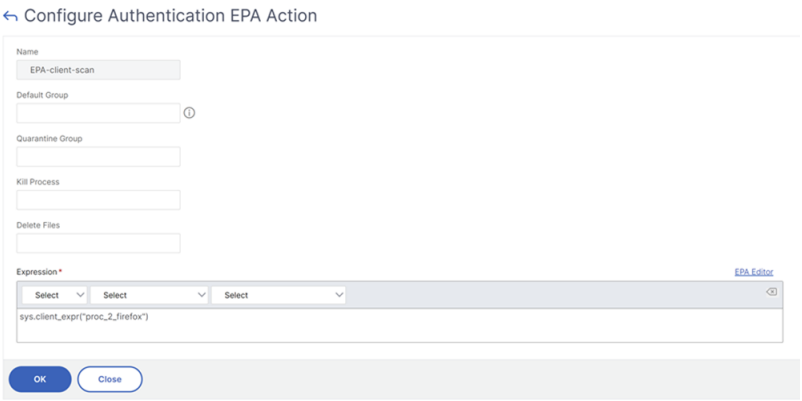
Vous pouvez configurer le scan EPA avancé à l'aide de l'interface graphique ou de l'interface de ligne de commande.

Sur l'interface graphique

1. Créez une action EPA.

   Accédez à **Sécurité > AAA - Trafic d'applications > Stratégies > Authentification > Stratégies avancées > Actions > EPA**, puis cliquez sur **Ajouter**. Sur la page **Créer une action EPA d'authentification**, mettez à jour les informations suivantes et cliquez sur **Créer**.

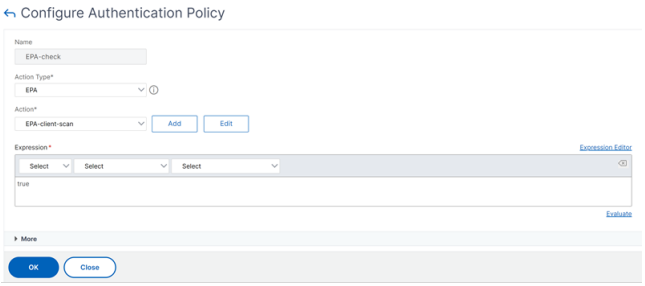
   - Nom : nom de l'action de l'EPA.
   - Groupe par défaut : groupe par défaut qui est choisi lorsque le contrôle EPA réussit.
   - Groupe de quarantaine : groupe de quarantaine choisi lorsque le contrôle de l'EPA échoue.
   - Kill Process : chaîne spécifiant le nom d'un processus à terminer par le plug-in EPA. Les processus multiples doivent être séparés par des virgules.
   - Supprimer les fichiers : chaîne spécifiant les chemins et les noms des fichiers à supprimer par le plug-in EPA. Les fichiers multiples doivent être séparés par des virgules.
   - Expression : Reportez-vous à la référence d'expression de stratégie Advanced Endpoint Analysis pour le format d'expression EPA.



2. Créez une stratégie EPA correspondante.

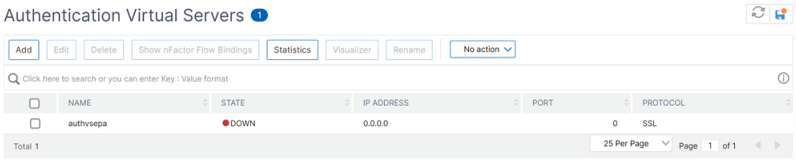
Accédez à **Sécurité > AAA - Trafic des applications > Stratégies > Authentification > Stratégies avancées > Stratégies**, puis cliquez sur **Ajouter**. Sur la page **Créer une stratégie d'authentification**, mettez à jour les informations suivantes et cliquez sur **Créer**.

- Nom : nom de la stratégie avancée de l'EPA.
- Type d'action : type de l'action d'authentification.
- Action : nom de l'action d'authentification à effectuer si la stratégie correspond.
- Expression : Reportez-vous à la référence d'expression de stratégie Advanced Endpoint Analysis pour le format d'expression EPA.
- Action de journalisation : nom de l'action du journal des messages à utiliser lorsqu'une demande correspond à cette stratégie. La longueur maximale autorisée est de 127 caractères.

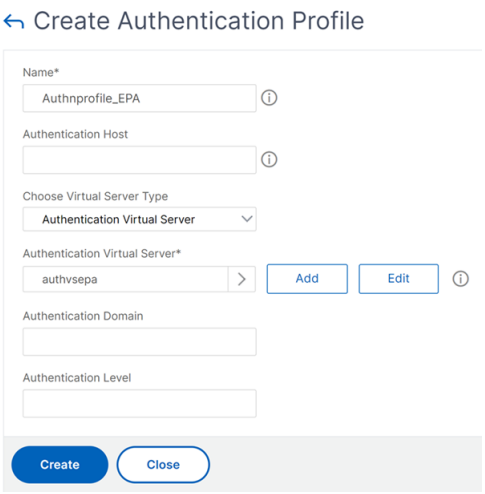


3. Configurez un serveur virtuel d'authentification et un profil d'authentification.

   - Accédez à **Sécurité > AAA - Trafic des applications > Authentification > Serveurs virtuels** et cliquez sur **Ajouter**.

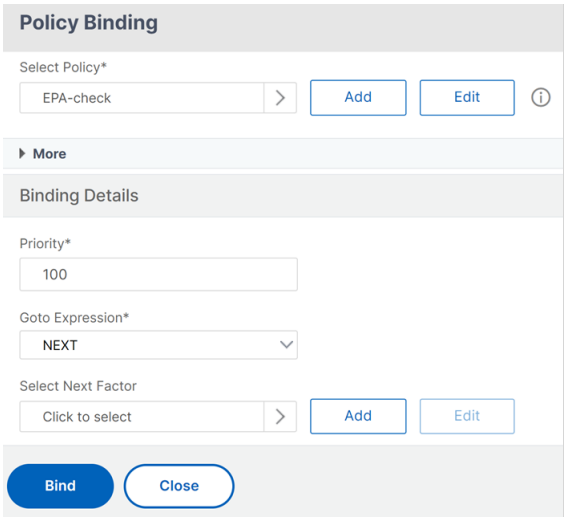


   - Accédez à **Sécurité > AAA - Trafic des applications > Profil d'authentification** et cliquez sur **Créer**.



4. Liez la stratégie EPA avancée au serveur virtuel d'authentification.

   - Accédez à **Sécurité > AAA —Trafic des applications > Serveurs virtuels d'authentification** et sélectionnez le serveur virtuel d'authentification.
   - Sélectionnez la stratégie dans la section **Stratégies d'authentification avancées**.
   - Cliquez sur **Lier** dans la section **Liaison des stratégies**.



5. Liez la stratégie de l'EPA au flux nFactor.

   Pour plus de détails sur la manière d'ajouter une stratégie EPA avancée en tant que facteur au flux nFactor, consultez le scan EPA en tant que facteur d'authentification nFactor.

Sur la CLI

1. Créez une action pour effectuer le scan EPA.

```
1 add authentication epaAction EPA-client-scan -csecexpr "sys.
    client_expr ("proc_2_firefox")"
```



```
<!--NeedCopy-->
```

L'expression précédente analyse si le processus « Firefox » est en cours d'exécution. Le plug-in EPA vérifie l'existence du processus toutes les 2 minutes, ce qui est indiqué par le chiffre « 2 » dans l'expression d'analyse.

2. Associez l'action de l'EPA à une stratégie avancée de l'EPA.

```
add authentication Policy EPA-check -rule true -action EPA-client-scan
<!--NeedCopy-->
```

3. Configurez un serveur virtuel d'authentification et un profil d'authentification.

```
add authentication vserver authnvsepa ssl -ip address 10.104.130.129 -port 443
<!--NeedCopy-->
```

```
add Authnprofile_EPA -authnVsName authnvsepa
<!--NeedCopy-->
```

4. Liez la stratégie EPA avancée au serveur virtuel d'authentification.

```
bind authentication vs authnvsepa -policy EPA-check -pr 1
<!--NeedCopy-->
```

Mise à niveau des bibliothèques EPA

Pour utiliser l'interface graphique NetScaler afin de mettre à niveau les bibliothèques EPA :

1. Accédez à**Configuration > NetScaler Gateway > Mettre à jour les composants du client**.
2. Sous **Mettre à jour les composants client,** cliquez sur le lien**Mettre à niveau les bibliothèques EPA**.
3. Sélectionnez le fichier requis et cliquez sur **Mettre à niveau**.

> **Important :**
>
> - Dans le cadre d'une haute disponibilité de NetScaler Gateway, les bibliothèques EPA doivent être mises à niveau à la fois sur les nœuds principal et secondaire.
> - Dans une configuration de clustering NetScaler Gateway, les bibliothèques EPA doivent être mises à niveau sur tous les nœuds du cluster.

Pour obtenir la liste des applications Windows et MAC prises en charge par OPSWAT pour les scans NetScaler, consultez. https://support.citrix.com/article/CTX234466

Dépannage des analyses avancées d'Endpoint Analysis

Pour faciliter le dépannage des analyses Advanced Endpoint Analysis, les plug-ins clients écrivent des informations de journalisation dans un fichier sur les systèmes de terminaux clients. Ces fichiers journaux se trouvent dans les répertoires suivants, en fonction du système d'exploitation de l'utilisateur.

Windows Vista, Windows 7, Windows 8, Windows 8.1 et Windows 10 :

C:\Users\<username>\AppData\Local\Citrix\AGEE\nsepa.txt

Windows XP :

C:\Documents and Settings\All Users\Application Data\Citrix\AGEE\nsepa.txt

Systèmes Mac OS X :

~/Bibliothèque/Application Support/Citrix/EPAPlugin/epaplugin.log

(Où le symbole ~ indique le chemin du répertoire personnel de l'utilisateur macOS concerné.)
(Où le symbole ~ indique le chemin du répertoire personnel de l'utilisateur macOS concerné.)

Ubuntu :

- ~/.citrix/nsepa.txt
- ~/.citrix/nsgcepa.txt

Référence des expressions de stratégie Advanced Endpoint Analysis

March 27, 2024

Cette rubrique décrit le format et la construction des expressions Advanced Endpoint Analysis. L'utilitaire de configuration de NetScaler Gateway crée automatiquement les éléments d'expression contenus ici et ne nécessite aucune configuration manuelle.

Format d'expression

Une expression Advanced Endpoint Analysis présente le format suivant :

```
CLIENT.APPLICATION (SCAN-type_ Product-id_ Method-name _ Method-comparator_ Method-param _...)
```

Où :

Le type de numérisation est le type d'application analysée.

Product-ID est l'identification du produit pour l'application analysée.

Le nom de la méthode est l'attribut produit ou système analysé.

Le comparateur de méthode est le comparateur choisi pour l'analyse.

Method-param est la ou les valeurs d'attribut analysées.

Exemple:

client.application(ANTIVIR_2600*RTP*==_TRUE)

> **Remarque :**
>
> Pour les types d'analyse autres que les applications, le préfixe d'expression est CLIENT.SYSTEM au lieu de CLIENT.APPLICATION.

chaînes d'expression

Chacun des types d'analyse pris en charge dans Advanced Endpoint Analysis utilise un identificateur unique dans les expressions. Le tableau suivant énumère les chaînes de chaque type d'analyse.

Type d'analyse	Chaîne d'expression de type d'analyse
Anti-hameçonnage	ANTIPHI
Antispyware	ANTISPY
Antivirus	ANTIVIR
Client de sauvegarde	BACKUP
Contrôle d'accès aux appareils	DEV-CONT
Protection contre la perte de données	DATA-PREV
Partage de bureau	DESK-SHARE
Pare-feu	FIREWALL
Agent de santé	HEALTH
Cryptage du disque dur	HD-ENC
Messagerie instantanée	IM
Navigateur Web	BROWSER
P2P	P2P
Gestion des correctifs	PATCH
filtrage d'URL	URL-FILT

Type d'analyse	Chaîne d'expression de type d'analyse
Adresse MAC	MAC
Vérification du domaine	DOMAIN
Analyse numérique du registre	REG-NUM

> **Remarque :**
>
> Pour les analyses spécifiques à macOS X, les expressions incluent le préfixe MAC- avant le type de méthode. Par conséquent, pour les analyses antivirus et anti-hameçonnage, les méthodes sont respectivement MAC-ANTIVIR et MAC-ANTIPHI.
>
> Par exemple :
>
> client.application (MAC-ANTIVIR_2600*RTP*==_TRUE)

Méthodes d'analyse des applications

Lors de la configuration des expressions Advanced Endpoint Analysis, des méthodes sont utilisées pour définir les paramètres des analyses des points de terminaison. Ces méthodes incluent un nom de méthode, un comparateur et une valeur. Les tableaux suivants énumèrent les méthodes disponibles pour une utilisation dans les expressions.

Méthodes d'analyse courantes :

Les méthodes suivantes sont utilisées pour plusieurs types d'analyses d'applications.

Méthode	Description	Comparateur	Valeurs possibles
VERSION*	Spécifie la version de l'application.	<, <=, >, >=, !=, ==	Chaîne de version
AUTHENTIQUE**	Vérifiez si l'application est authentique ou non.	==	TRUE
ACTIVÉ	Vérifiez si l'application est activée.	==	TRUE
COURSE	Vérifiez si l'application est en cours d'exécution.	==	TRUE

Méthode	Description	Comparateur	Valeurs possibles
COMMENTAIRE	Champ de commentaire (ignoré par l'analyse). Délimité par [] dans les expressions.	==	N'importe quel texte

* La chaîne VERSION peut spécifier une chaîne décimale de quatre valeurs maximum, par exemple 1.2.3.4.

** Une vérification AUTHENTIC permet de vérifier l'authenticité des fichiers binaires de l'application.

> **Remarque :**
>
> Vous pouvez sélectionner une version générique pour les types d'analyse des applications. Lorsque des analyses génériques sont sélectionnées, l'ID du produit est 0.

Gateway offre une option permettant de configurer des analyses génériques pour chaque type de logiciel. À l'aide de l'analyse générique, un administrateur peut analyser la machine cliente sans restreindre la vérification de l'analyse à un produit particulier.

Pour les analyses génériques, les méthodes d'analyse ne fonctionnent que si le produit installé sur le système de l'utilisateur prend en charge cette méthode d'analyse. Pour savoir quels produits prennent en charge une méthode d'analyse particulière, contactez le support NetScaler.

Méthodes d'analyse uniques :

Les méthodes suivantes sont uniques aux types d'analyses spécifiés.

Méthode	Description	Comparateur	Valeurs possibles
ENABLED-FOR	Vérifiez si le logiciel anti-hameçonnage est activé pour l'application sélectionnée.	`allof`, `anyof`, `noneof`	**Pour Windows** : Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Safari. **Pour Mac :** Safari, Mozilla Firefox, Google, Chrome, Opera

Tableau 2. Antispyware et antivirus

Méthode	Description	Comparateur	Valeurs possibles
RTP	Vérifiez si la protection en temps réel est allumée ou non.	==	TRUE
SCAN-TIME	Nombre de **minutes** écoulées depuis qu'une analyse complète du système a été effectuée.	<, <=, >, >=, !=, ==	Tout nombre positif
VIRDEF-FILE-TIME	Nombre de **minutes** écoulées depuis la mise à jour du fichier de définition de virus (c'est-à-dire le nombre de minutes entre l'estampille du fichier de définition de virus et l'horodatage actuel).	<, <=, >, >=, !=, ==	Tout nombre positif
VIRDEF-FILE-VERSION	Version du fichier de définition.	<, <=, >, >=, !=, ==	Chaîne de version
ENGINE-VERSION	Version du moteur.	<, <=, >, >=, !=, ==	Chaîne de version

Tableau 3. Client de sauvegarde

Méthode	Description	Comparateur	Valeurs possibles
LAST-BK-ACTIVITY	Nombre de **minutes** écoulées depuis la fin de la dernière activité de sauvegarde.	<, <=, >, >=, !=, ==	Tout nombre positif

Tableau 4. Prévention de la perte de données

Méthode	Description	Comparateur	Valeurs possibles
ACTIVÉ	Vérifiez si l'application est activée ou non et si la protection du temps est activée ou non.	==	TRUE

Tableau 5. Agent de vérification de l'état

Méthode	Description	Comparateur	Valeurs possibles
SYSTEM-COMPL	Vérifiez si le système est en conformité.	==	TRUE

Tableau 6. Cryptage du disque dur

Méthode	Description	Comparateur	Valeurs possibles
ENC-PATH	PATH pour vérifier l'état du chiffrement.	NO OPERATOR	N'importe quel texte
ENC-TYPE	Vérifiez si le type de chiffrement du chemin d'accès spécifié.	`allof`, `anyof`, `noneof`	**Liste avec les options suivantes** : UNENCRYPTED, PARTIAL, ENCRYPTED, VIRTUAL, SUSPENDED, PENDING

Tableau 7. Navigateur Web

Méthode	Description	Comparateur	Valeurs possibles
DEFAULT	Vérifiez s'il est défini comme navigateur par défaut.	==	TRUE

Tableau 8. Gestion des correctifs </caption>

|Méthode|Description|Comparateur|Valeurs possibles|
|—|—|—|—|
|SCAN-TIME|Combien de minutes se sont écoulées depuis la dernière analyse des correctifs.|<, <=, >,

>=, !=, ==|Tout nombre positif|
|MISSED-PATCH|Il ne manque pas de correctifs de ce type sur le système client.|anyof, noneof
|ANY Pré-sélectionné (correctifs présélectionnés sur le serveur Patch Manager)
NON|

Tableau 9. Adresse MAC

Méthode	Description	Comparateur	Valeurs possibles
ADDR	Vérifiez si les adresses MAC de la machine cliente figurent ou non dans la liste donnée.	anyof, noneof	Liste modifiable

Tableau 10. Adhésion au domaine

Méthode	Description	Comparateur	Valeurs possibles
SUFFIX	Vérifiez si la machine cliente existe ou n' existe pas dans la liste donnée.	anyof, noneof	Liste modifiable

Tableau 11. Entrée de registre numérique

Méthode	Description	Comparateur	Valeurs possibles
PATH	Chemin d'accès pour la vérification du registre. Au format : HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client\EnableAutoUpdate. Il n'est pas nécessaire d'échapper les caractères spéciaux. Toutes les clés racine du registre : HKEY_LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_USERS, HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG	NO OPERATOR	N'importe quel texte

Méthode	Description	Comparateur	Valeurs possibles
REDIR-64	Suivez la redirection 64 bits. Si elle est définie sur TRUE, la redirection WOW est suivie (c'est-à-dire que le chemin d'accès au Registre est vérifié sur les systèmes 32 bits, mais le chemin redirigé WOW est vérifié pour les systèmes 64 bits). Si elle n'est pas définie, la redirection WOW n'est pas suivie (c'est-à-dire que le même chemin d'accès au Registre est vérifié pour les systèmes 32 bits et 64 bits). Pour les entrées de Registre qui ne sont pas redirigées, ce paramètre n'a aucun effet. Consultez l'article suivant pour obtenir la liste des clés de Registre qui sont redirigées sur les systèmes 64 bits : http://msdn.microsoft.com/en-us/library/aa384253%28v=vs.85%29.aspx	==	TRUE

Méthode	Description	Comparateur	Valeurs possibles
VALEUR	Valeur attendue pour le chemin ci-dessus. Cette analyse ne fonctionne que pour les types de registre REG_DWORD et REG_QWORD.	<, <=, >, >=, !=, ==	N'importe quel numéro

Scan EPA pour les adresses MAC

March 27, 2024

À partir de la version 13.0-88.x de NetScaler, vous pouvez configurer les configurations de scan EPA pour les adresses MAC autorisées ou spécifiques. NetScaler utilise des expressions de stratégie et des ensembles de modèles pour spécifier la liste des adresses MAC.

Avant la version 13.0-88.x de NetScaler, la liste de toutes les adresses MAC autorisées devait être spécifiée dans le cadre d'une expression EPA. Si les clients disposaient d'une longue liste d'adresses MAC autorisées, il était fastidieux d'ajouter toutes les adresses MAC en une seule expression. En outre, le nombre d'adresses MAC à ajouter dans une seule expression était limité.

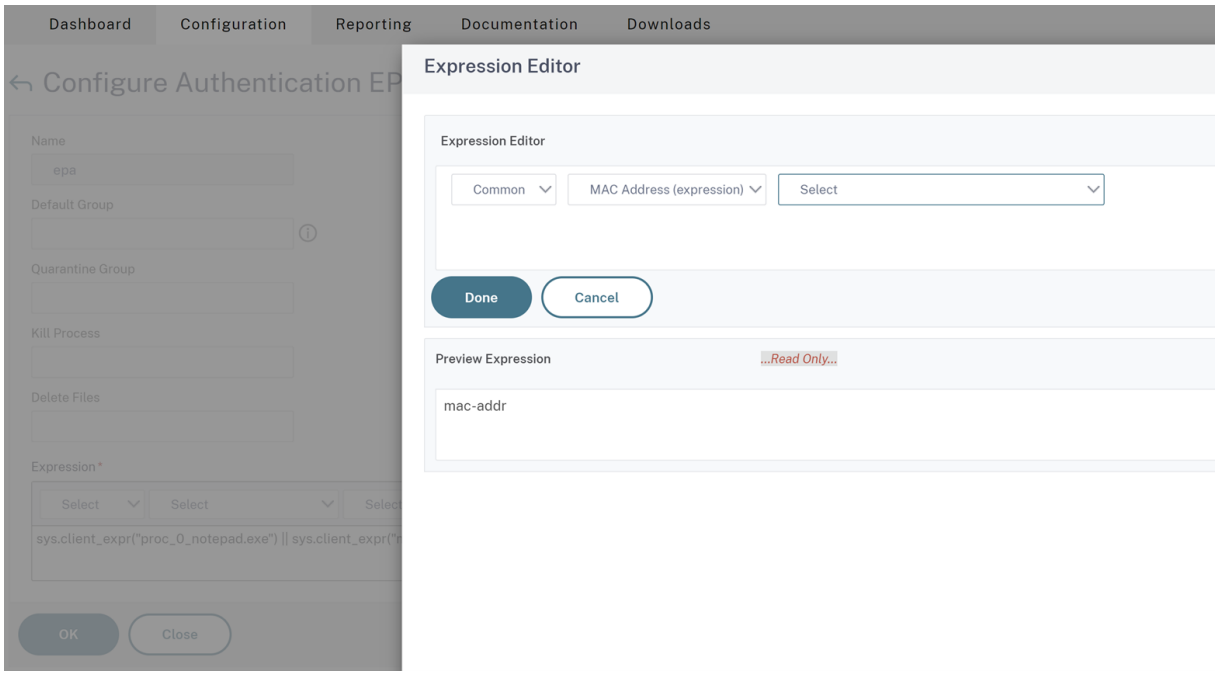
Par exemple,

```
1 add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome") || sys.
    client_expr("proc_0_firefox") && sys.client_expr("
    sys_0_MAC_ADDR_anyof_1AC89C83BOF7,0250F20A777C[COMMENT: MAC Address]
    ")/
2 <!--NeedCopy-->
```

Configurez le scan EPA pour les adresses MAC à l'aide de l'interface graphique

L'option **Adresses MAC (expression)** qui était auparavant disponible dans la catégorie de numérisation **Windows** est désormais disponible dans la catégorie de numérisation **commune** de l'interface graphique de NetScaler. Cette option permet aux utilisateurs de configurer un scan EPA pour une liste d'adresses MAC autorisées ou spécifiques.

> **Remarque :**
>
> Le client Citrix Secure Access 22.10.1 et les versions ultérieures prennent en charge cette méthode de gestion par NetScaler des configurations de scan EPA sur l'interface graphique.



1. Configurez un jeu de motifs. Pour plus de détails, voir Configuration d'un jeu de modèles.
2. Créez une expression de stratégie correspondante pour chaque jeu de modèles.

   Lors de la configuration de l'expression, dans l'éditeur d'expression, sélectionnez **AAA > LOGIN > CLIENT_MAC_ADDR > EQUAL_ANY (chaîne) > Jeu de motifs**.

   Pour plus d'informations sur la configuration d'une expression avancée, consultez la section Configurer des expressions de stratégie avancées dans une stratégie.
3. Créez une analyse EPA pour l'expression configurée dans les étapes précédentes. Pour plus de détails, voir Analyses avancées des points de terminaison.

Configurez le scan EPA pour les adresses MAC à l'aide de l'interface de ligne de commande

1. Stockez les adresses MAC dans des ensembles de modèles.

   À l'invite de commande, tapez ;

```
add policy patset <name> [-comment <string>]
<!--NeedCopy-->
```


Example:

‘‘‘

add policy patset patset1
bind policy patset patset1 1A-C8-9C-83-BO-F7
bind policy patset patset1 02-50-F2-0A-77-7C …and so on up to 3K entries.
add policy patset patset2
bind policy patset patset2 1A-2B-3C-4D-5E-6A
bind policy patset patset2 1A-2B-3C-4D-5E-6B …and so on up to 3K entries.
‘‘‘

2. Créez une expression de stratégie correspondante pour chaque jeu de modèles en utilisant AAA.Login.Client_Mac_Addr.equals_any ()

   À l’invite de commande, tapez ;

```
Add policy expression <name> <value> [-comment <string>] [-
    clientSecurityMessage <string>]
```

   Exemple:

```
add policy expression exp1 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
    patset1")
add policy expression exp2 AAA.LOGIN.CLIENT_MAC_ADDR.equals_any("
    patset2")
```

3. Créer des scans EPA à l’aide des expressions de stratégie configurées

   À l’invite de commande, tapez ;

```
add authentication epaAction <name>  -csecexpr <expression>
```

   Exemple:

```
add authentication epaAction epa -csecexpr q/sys.client_expr("
    proc_0_notepad.exe") || sys.client_expr("proc_0_chrome")  ||
    sys.client_expr("mac-addr_0_exp1") || sys.client_expr("mac-
    addr_0_exp2") || sys.client_expr("proc_0_firefox")/
```

   Configurez une stratégie de pré-authentification,

```
add authentication Policy epapol -rule true -action epa
```

   Liez la stratégie de préauthentification,

```
bind authentication vserver <name> -policy epapol -priority 10 -
    gotoPriorityExpression NEXT
```


Points à noter

- La configuration d'une analyse EPA pour une liste autorisée d'adresses MAC ne s'applique qu'aux flux d'authentification nFactor.
- Il est recommandé de ne pas stocker plus de 3 000 entrées dans un ensemble de modèles.
- Les adresses MAC doivent être configurées au format 1A-2B-3C-4D-5E-6F.
- Le format de l'analyse EPA est `mac-addr_0_<policy-expression-name>`. Dans ce format, `mac-addr_0_` est une valeur statique et vous devez entrer le nom de l'expression de stratégie après `mac-addr_0_`.
- Les scans de l'EPA peuvent être séparés de manière appropriée à l'aide des symboles (`||`, `&&`).
- Pour ajouter de nombreuses adresses MAC à un jeu de modèles, vous pouvez utiliser l'importation de jeux de modèles basés sur des fichiers. Il est recommandé de stocker un maximum de 3000 entrées/jeu de motifs pour des performances optimales.
- Si des adresses MAC sont présentes dans un fichier, vous pouvez créer un jeu de modèles en utilisant l'importation de jeux de modèles basés sur des fichiers et en spécifiant le délimiteur approprié lors de l'importation.

Références

- Configurez un jeu de motifs.
- Créez un ensemble de modèles à l'aide de l'importation basée sur des fichiers.
  “‘

Gérer les sessions utilisateur

March 27, 2024

Vous pouvez gérer les sessions utilisateur dans l'interface utilisateur graphique de NetScaler à partir de la boîte de dialogue **Active Users Sessions**. Cette boîte de dialogue affiche la liste des sessions utilisateur actives sur NetScaler Gateway. Vous pouvez afficher les sessions d'utilisateur final ou de groupe à l'aide du nom d'utilisateur, du nom du groupe ou de l'adresse IP. Vous pouvez également afficher les sessions actives dans cette boîte de dialogue. Les informations relatives à la session incluent :

- Nom d'utilisateur
- Adresse IP de la machine utilisateur
- Numéro de port de la machine utilisateur

- Adresse IP du serveur virtuel
- Numéro de port du serveur virtuel
- Adresse IP intranet attribuée à l'utilisateur

Gérer les sessions utilisateur à l'aide de l'interface graphique

Pour afficher les sessions utilisateur

1. Dans le volet de navigation de l'interface graphique de NetScaler, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Surveiller les connexions, cliquez sur **Sessions utilisateur actives**.
3. Dans **Active User Sessions**, sélectionnez l'un des types suivants.
    - **Utilisateurs actifs**
    - **Groupes actifs**
    - **IP intranet**- Lorsque vous sélectionnez IP intranet, vous devez entrer l'adresse IP intranet et le masque de sous-réseau.
4. Cliquez sur **Continuer**.

Pour actualiser la liste des sessions

Vous pouvez récupérer des informations mises à jour sur les sessions de NetScaler Gateway.

1. Dans le volet de navigation de l'interface graphique de NetScaler, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Surveiller les connexions, cliquez sur **Sessions utilisateur actives**.
3. Cliquez sur **Actualiser**.

Pour des sessions d'utilisateurs finaux ou de groupe ou pour une session dotée d'une adresse IP Intranet spécifique

Vous pouvez mettre fin aux sessions utilisateur et groupe. Vous pouvez également mettre fin à une session qui possède une adresse IP intranet et un masque de sous-réseau spécifiques.

1. Dans le volet de navigation de l'interface graphique de NetScaler, cliquez sur **NetScaler Gateway**.
2. Dans le volet d'informations, sous Surveiller les connexions, cliquez sur **Sessions utilisateur actives**.

3. Sous Sessions, sélectionnez un utilisateur, un groupe ou une session qui possède une adresse IP intranet spécifique, puis cliquez sur **Terminer**.

Gestion des sessions utilisateur à l'aide de l'interface de ligne de commande

Vous pouvez utiliser les commandes CLI suivantes pour afficher les sessions utilisateur, les sessions utilisateur final ou les sessions de groupe.

- `show aaa session`- Affiche toutes les connexions NetScaler d'authentification, d'autorisation et d'audit ou VPN liées à l'utilisateur, au groupe, à l'adresse IP ou à la plage d'adresses IP spécifiés.
- `show vpn icaConnection` - Affiche toutes les connexions actives qui utilisent le proxy ICA.
- `show system session` - Affiche des informations sur toutes les sessions système en cours ou sur la session spécifiée.

Always On

March 27, 2024

La fonctionnalité Always On de NetScaler Gateway garantit que les utilisateurs sont toujours connectés au réseau de l'entreprise. Cette connectivité VPN persistante est obtenue par l'établissement automatique d'un tunnel VPN.

> **Remarque**
>
> La fonctionnalité Always On prend en charge les portails captifs pour NetScaler 12.0 Build 51.24 et versions ultérieures.

Quand utiliser Always On

Utilisez Always On lorsque vous devez fournir une connectivité VPN transparente en fonction de l'emplacement de l'utilisateur et que vous devez empêcher l'accès au réseau d'un utilisateur qui n'est pas connecté à un VPN.

Les scénarios suivants illustrent l'utilisation de Always On.

- Un employé démarre l'ordinateur portable en dehors du réseau de l'entreprise et a besoin d'aide pour établir la connectivité VPN.
  Solution : Lorsque l'ordinateur portable est démarré en dehors du réseau de l'entreprise, Always On établit un tunnel de manière transparente et fournit une connectivité VPN.

- Un employé utilisant la connectivité VPN se déplace vers le réseau de l'entreprise. L'employé passe à un réseau d'entreprise mais reste connecté au tunnel VPN, ce qui n'est pas un état souhaitable.
  Solution : Lorsque l'employé se connecte au réseau de l'entreprise, Always On supprime le tunnel VPN et le transfère facilement vers le réseau de l'entreprise.
- Un employé quitte le réseau de l'entreprise et ferme l'ordinateur portable (sans l'éteindre). L'employé a besoin d'aide pour établir la connectivité VPN lors de la reprise du travail sur l'ordinateur portable.
  Solution : Lorsque l'employé quitte le réseau de l'entreprise, Always On établit facilement un tunnel et fournit une connectivité VPN.
- Une entreprise souhaite réglementer l'accès réseau fourni à ses utilisateurs lorsqu'ils ne sont pas connectés à un tunnel VPN.
  Solution : Selon la configuration, Always On limite l'accès, ce qui permet aux utilisateurs d'accéder uniquement au réseau de passerelle.

Comprendre le framework Always On

Always On connecte automatiquement un utilisateur à un tunnel VPN que le client a précédemment établi. La première fois que l'utilisateur a besoin d'un tunnel VPN, il doit se connecter à l'URL de NetScaler Gateway et établir le tunnel. Une fois la configuration Always On téléchargée sur le client, cette configuration entraîne l'établissement ultérieur du tunnel.

L'exécutable du client Citrix Secure Access est toujours en cours d'exécution sur l'ordinateur client. Lorsque l'utilisateur ouvre une session ou que le réseau change, le client Citrix Secure Access détermine si l'ordinateur portable de l'utilisateur se trouve sur le réseau de l'entreprise. Selon l'emplacement et la configuration, le client Citrix Secure Access établit un tunnel ou détruit un tunnel existant.

L'établissement du tunnel n'est lancé qu'une fois que l'utilisateur ouvre une session sur l'ordinateur. Le client Citrix Secure Access utilise les informations d'identification de l'ordinateur client pour s'authentifier auprès du serveur de passerelle et tente d'établir un tunnel.

Rétablissement automatique d'un tunnel

Le rétablissement automatique d'un tunnel est déclenché lorsqu'un tunnel VPN est détruit par NetScaler Gateway.

> **Remarque**
>
> Lorsque l'analyse des points de terminaison échoue, le client NetScaler Gateway ne tente pas à nouveau d'établir un tunnel, mais affiche un message d'erreur. En cas d'échec de l'authentification, le client NetScaler Gateway invite l'utilisateur à entrer ses informations d'identification.

Méthodes d'authentification utilisateur prises en charge pour un établissement de tunnel transparent

Les méthodes d'authentification utilisateur prises en charge sont les suivantes :

- Nom d'utilisateur et mot de passe AD : si le nom d'utilisateur et le mot de passe Windows sont utilisés pour l'authentification, le client Citrix Secure Access établit facilement le tunnel à l'aide de ces informations d'identification.
- Certificat utilisateur : si un certificat utilisateur est utilisé pour l'authentification et qu'il n'existe qu'un seul certificat sur la machine cliente, le client Citrix Secure Access établit un tunnel en toute transparence à l'aide de ce certificat. Si plusieurs certificats clients sont installés, le tunnel est établi une fois que l'utilisateur a sélectionné le certificat préféré. Le client Citrix Secure Access utilise ce certificat préféré pour les tunnels ultérieurs.

  Si les cartes à puce partagent un certificat utilisateur, l'auto-connexion ne peut pas être réalisée si les certificats sont installés dynamiquement dans le magasin par rapport aux certificats présents dans le magasin.
- Certificat utilisateur et nom d'utilisateur/mot de passe AD : Cette méthode d'authentification est la combinaison des méthodes d'authentification décrites précédemment.

> **Remarque**
>
> Tous les autres mécanismes d'authentification sont pris en charge, mais l'établissement du tunnel n'est pas transparent pour les autres méthodes d'authentification.

Configuration requise pour Always On

L'administrateur de l'entreprise doit appliquer les éléments suivants pour les appareils gérés :

- L'utilisateur ne doit pas être en mesure de mettre fin au processus/service pour une configuration spécifique
- L'utilisateur ne doit pas pouvoir désinstaller le package pour une configuration spécifique
- L'utilisateur ne doit pas pouvoir modifier des entrées de registre spécifiques

> **Remarque**
>
> La fonctionnalité peut ne pas fonctionner comme prévu si l'utilisateur dispose de privilèges d'administration, comme dans le cas des appareils non gérés.

Considérations relatives à l'activation de la fonction Toujours

Consultez la section suivante avant d'activer la fonction Always On.

Accès réseau principal : Lorsque le tunnel est établi, le trafic vers le réseau d'entreprise est décidé en fonction de la configuration du tunnel partagé. D'autres configurations ne sont pas fournies pour remplacer ce comportement.

Paramètres proxy de la machine cliente : Les paramètres proxy de la machine cliente sont ignorés pour la connexion au serveur de passerelle.

> **Remarque**
>
> La configuration du proxy de l'appliance NetScaler n'est pas ignorée. Seuls les paramètres proxy de la machine cliente sont ignorés. Les utilisateurs qui ont un proxy configuré sur leurs systèmes sont informés que le plug-in VPN a ignoré leurs paramètres de proxy.

Configuration d'Always On

Pour configurer Always On, créez un profil Always On sur l'appliance NetScaler Gateway et appliquez le profil.

Pour créer un profil Always On :

1. Dans l'interface graphique de NetScaler, accédez **à Configuration > NetScaler Gateway > Policies**> AlwaysOn.
2. Sur la page **Profils AlwaysOn**, cliquez sur **Ajouter**.
3. Sur la page **Créer un profil AlwaysOn**, entrez les informations suivantes :

    - **Nom** : nom de votre profil.
    - **VPN basé sur la localisation (nom de registre côté client : LocationDetection) : sélectionnez l'un des paramètres suivants :
        - **À distance** pour permettre à un client de détecter s'il se trouve dans le réseau d'entreprise et d'établir le tunnel s'il n'est pas dans le réseau d'entreprise. Remote est le paramètre par défaut.
        - **Partout** pour permettre à un client d'ignorer la détection de localisation et d'établir le tunnel, quel que soit l'emplacement du client
    - **Contrôle du client** : sélectionnez l'un des paramètres suivants :
        - **Refuser**pour empêcher l'utilisateur de se déconnecter et de se connecter à une autre passerelle. Refuser est le paramètre par défaut.
        - **Permet** à l'utilisateur de se déconnecter et de se connecter à une autre passerelle.
    - **Accès réseau en cas d'échec VPN (nom de registre côté client : AlwaysOn)** —Sélectionnez l'un des paramètres suivants :
        - **Accès complet** pour permettre au trafic réseau de circuler vers et depuis le client lorsque le tunnel n'est pas établi. L'accès intégral est le paramètre par défaut.

- **Seulement vers passerelle** pour empêcher le trafic réseau de circuler vers ou depuis le client lorsque le tunnel n'est pas établi. Toutefois, le trafic à destination ou en provenance de l'adresse IP de la passerelle est autorisé.
  Remarque : En mode **Uniquement vers passerelle**, seul le serveur virtuel, le trafic DNS et DHCP sont débloqués. Pour débloquer d'autres sites Web, des plages d'adresses IP ou des adresses IP, vous devez définir le registre **AlwaysOnAllowList avec une liste** de noms de domaine complets, de plages d'adresses IP ou d'adresses IP séparés par des points-virgules.
  Par exemple, mycompany.com,mycdn.com,10.120.67.0-10.120.67.255,67.67.67.67

4. Cliquez sur **Créer** pour terminer la création de votre profil.

Pour appliquer le profil Always On :

1. Dans l'interface NetScaler, sélectionnez **Configuration > NetScaler Gateway**Paramètres généraux.
2. Sur la page Paramètres globaux, cliquez sur le lien **Modifier les paramètres globaux**, puis sélectionnez l'onglet **Expérience client**.
3. Dans le menu déroulant **Nom du profil AlwaysOn**, sélectionnez le profil que vous venez de créer, puis cliquez sur **OK**.

Remarque : Une configuration similaire peut être effectuée dans le profil de session pour appliquer les stratégies au niveau du groupe, au niveau du serveur ou au niveau de l'utilisateur.

Note sur les IIP

Le tunnel au niveau de la machine utilise l'authentification basée sur les certificats et la session créée porte le nom commun du certificat en tant que nom d'utilisateur. Ainsi, si les certificats de périphériques ont des noms communs uniques, les sessions des machines différentes ont un nom d'utilisateur différent et donc des adresses IP différentes. Assurez-vous de générer un certificat d'appareil avec des noms uniques. Idéalement, vous devez utiliser des noms de machines comme nom commun du certificat de périphérique.

Résumé du comportement des différentes configurations pour les utilisateurs administrateurs et les utilisateurs non administrateurs

Le tableau suivant récapitule le comportement des différentes configurations. Il détaille également la possibilité que certaines actions de l'utilisateur puissent affecter la fonctionnalité Always On.

networkAccessONVPNFailure	Contrôle des clients	Utilisateur non administrateur	Utilisateur administrateur
fullaccess	Allow	Le tunnel est automatiquement établi. L'utilisateur peut fermer sa session et rester hors du réseau. L'utilisateur peut également pointer vers un autre NetScaler Gateway.	Le tunnel est automatiquement établi. L'utilisateur peut fermer sa session et rester hors du réseau d'entreprise. L'utilisateur peut également pointer vers un autre NetScaler Gateway.
fullaccess	Deny	Le tunnel est automatiquement établi. L'utilisateur ne peut pas se déconnecter ou pointer vers un autre NetScaler Gateway.	Le tunnel est automatiquement établi. L'utilisateur peut désinstaller le client Citrix Secure Access ou passer à un autre NetScaler Gateway.
onlyToGateway	Allow	Le tunnel est automatiquement établi. L'utilisateur peut fermer sa session (pas d'accès réseau). L'utilisateur peut également pointer vers un autre NetScaler Gateway, auquel cas l'accès est accordé uniquement au NetScaler Gateway nouvellement pointé.	Le tunnel est automatiquement établi. L'utilisateur peut désinstaller le client Citrix Secure Access ou passer à un autre NetScaler Gateway.

networkAccessONVPNFailure	Contrôle des clients	Utilisateur non administrateur	Utilisateur administrateur
onlyToGateway	Deny	Le tunnel est automatiquement établi. L'utilisateur ne peut pas se déconnecter ou pointer vers un autre NetScaler Gateway.	Le tunnel est automatiquement établi. L'utilisateur peut désinstaller le client Citrix Secure Access ou passer à un autre NetScaler Gateway.

Autorisation des URL sélectionnées lorsque l'option Always On est en panne

Les utilisateurs peuvent accéder à quelques sites Web même lorsque Always On est en panne et que le réseau est verrouillé. Les administrateurs peuvent utiliser le registre **AlwaysOnAllowList** pour ajouter les sites Web auxquels vous souhaitez activer l'accès lorsque l'option AlwaysOnAllowList est inactive.

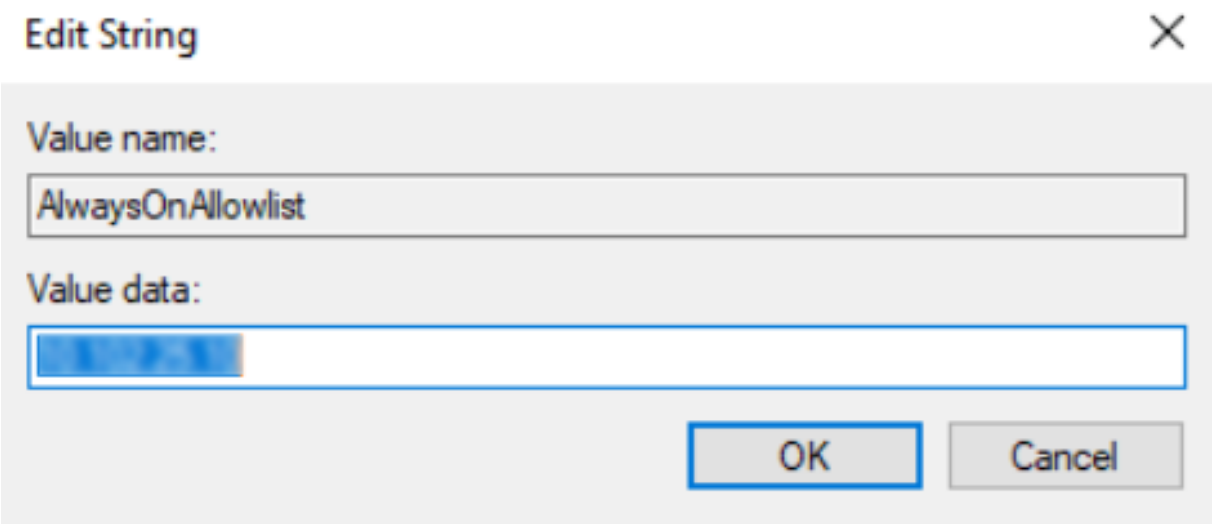
> **Remarque :**
>
> - Le registre**AlwaysOnAllowList** est pris en charge à partir des versions 13.0 build 47.x et ultérieures.
> - L'emplacement du Registre**AlwaysOnAllowList** est Computer \ HKEY_LOCAL_MACHINE \ SOFTWARE \ Citrix \ Secure Access Client.
> - Les URL/FQDN génériques ne sont pas pris en charge dans le registre **AlwaysOnAllowList**.

Pour définir le registre AlwaysOnAllowList

Définissez le registre **AlwaysOnAllowList** avec une liste de noms de domaine complets, de plages d'adresses IP ou d'adresses IP séparés par des points-virgules auxquels vous souhaitez autoriser l'accès.

Exemple : example.citrix.com ; 10.103.184.156 ; 10.102.0.0-10.102.255.100

La figure suivante présente un exemple de registre **AlwaysOnAllowList**.



VPN Always On avant l'ouverture de session Windows (anciennement service Always On)

March 27, 2024

La fonctionnalité **VPN AlwaysOn avant l'ouverture de session Windows** (anciennement service AlwaysOn) permet à un utilisateur d'établir un tunnel VPN au niveau de la machine avant même qu'un utilisateur ne se connecte à un système Windows. Le tunnel reste actif jusqu'à l'arrêt de la machine. Une fois que l'utilisateur s'est connecté, le tunnel VPN au niveau de la machine est pris en charge par un tunnel VPN au niveau de l'utilisateur. Une fois que l'utilisateur se déconnecte, le tunnel de niveau utilisateur est déchiré et un tunnel au niveau de la machine est établi. **Le VPN Always On avant l'ouverture de session Windows** peut être configuré à l'aide de stratégies d'authentification avancées uniquement. Pour plus d'informations, consultez Configurer le VPN Always On avant l'ouverture de session Windows.

Capacités d'ouverture de session Always On VPN avant Windows

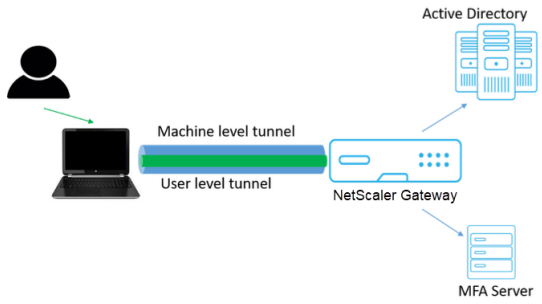
- L'administrateur peut fournir un mot de passe à usage unique aux utilisateurs qui travaillent pour la première fois à distance, à l'aide duquel les utilisateurs peuvent se connecter au contrôleur de domaine pour modifier leur mot de passe.
- L'administrateur peut gérer/appliquer à distance les stratégies AD sur l'appareil avant même que l'utilisateur ne se connecte.
- L'administrateur peut fournir un niveau de contrôle granulaire aux utilisateurs en fonction du groupe d'utilisateurs après la connexion de l'utilisateur. Par exemple, à l'aide d'un tunnel de

niveau utilisateur, vous pouvez restreindre ou accorder l'accès à une ressource à un groupe d'utilisateurs particulier.

- Le tunnel utilisateur peut être configuré pour MFA en fonction des besoins de l'utilisateur.
- Plusieurs utilisateurs peuvent utiliser la même machine. L'accès à des ressources sélectives est fourni en fonction du profil utilisateur. Par exemple, plusieurs utilisateurs peuvent utiliser une machine dans un kiosque sans problème.
- Les utilisateurs travaillant à distance se connectent au contrôleur de domaine pour modifier leur mot de passe.
- L'ordinateur Windows peut vérifier les informations d'identification de connexion de l'utilisateur à l'aide de l'annuaire Active Directory d'entreprise (AD) et les informations d'identification Windows sur la machine ne sont pas mises en cache. De plus, les nouveaux utilisateurs AD d'entreprise peuvent se connecter facilement à la machine.
- La machine Windows fait partie de l'intranet de l'entreprise avant même que les utilisateurs ne se connectent, ce qui permet aux administrateurs informatiques d'accéder à la machine cliente à partir du réseau de l'entreprise à des fins de débogage.
- Le tunnel VPN d'une machine Windows reste connecté même lorsque différents utilisateurs se connectent ou se déconnectent de la machine.

Présentation du VPN Always On avant l'ouverture de session Windows

Voici le flux d'événements pour la fonctionnalité **Always On VPN avant l'ouverture de session Windows**.



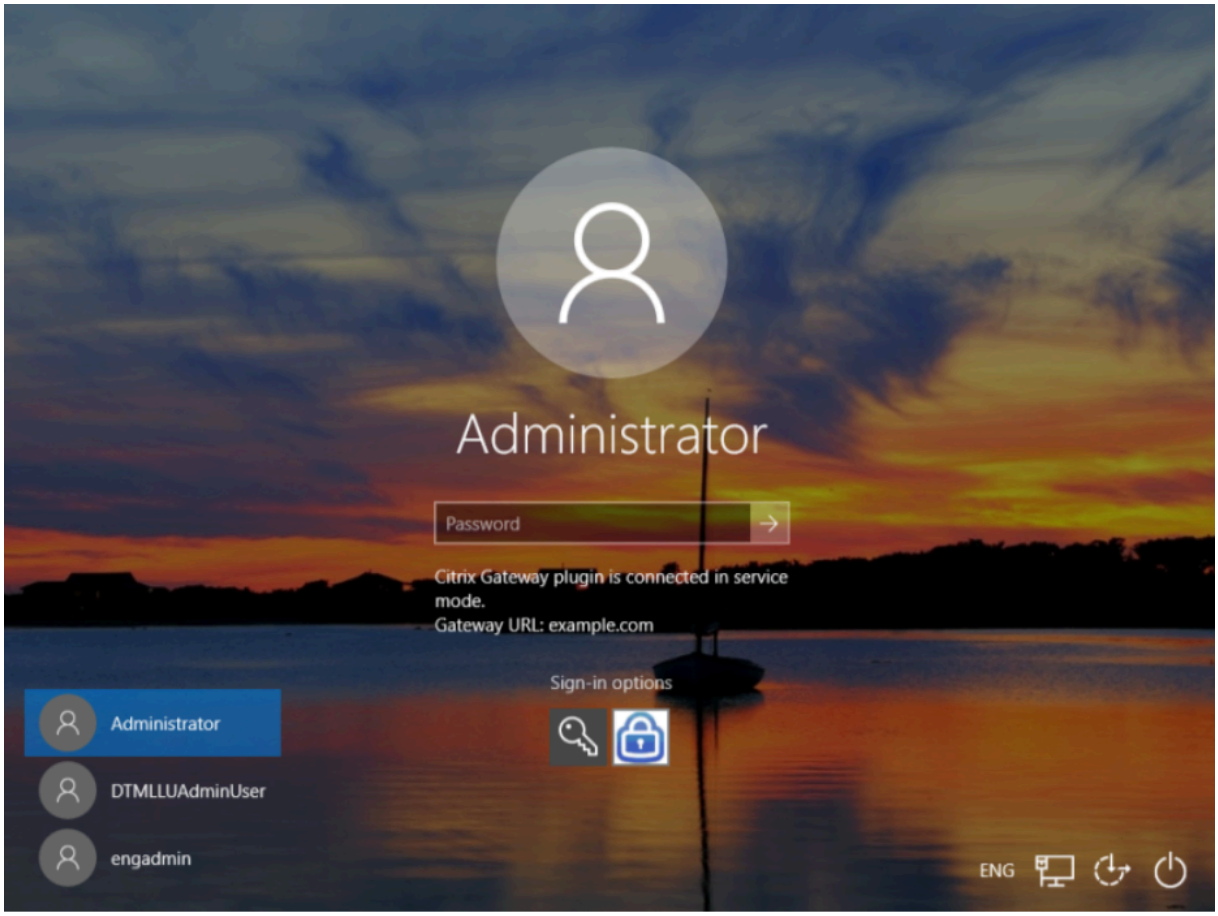
- L'utilisateur allume l'ordinateur portable. Le tunnel au niveau de la machine est établi vers NetScaler Gateway en utilisant le certificat de l'appareil comme identité.
- L'utilisateur se connecte à l'ordinateur portable à l'aide des informations d'identification AD.
- Après la connexion, l'utilisateur est confronté à un défi avec MFA.
- Une fois l'authentification réussie, le tunnel de niveau machine est remplacé par le tunnel de niveau utilisateur.
- Une fois que l'utilisateur se déconnecte, le tunnel de niveau utilisateur est remplacé par le tunnel au niveau de la machine.

Points à noter :

- NetScaler Gateway et le plug-in VPN doivent être de version 13.0.41.20 ou ultérieure.
- Si un ordinateur client n'a pas de connectivité Internet, **Always On VPN avant l'ouverture de session Windows** attend que la connectivité Internet soit disponible avant d'établir le tunnel VPN.
- Si un ordinateur client est connecté à un réseau de portail captif, **Always On VPN avant l'ouverture de session Windows** attend que l'utilisateur s'authentifie auprès du portail captif. Une fois que l'utilisateur s'est connecté et que l'accès Internet est activé, **Always On VPN avant l'ouverture de session Windows** établit le tunnel VPN.
- La fonctionnalité Always On VPN before Windows Logon prend en charge les portails captifs pour NetScaler.
- Si l'option des informations d'identification de connexion mises en cache n'est pas activée pour Windows, les utilisateurs ne peuvent pas ouvrir de session dans les scénarios suivants :
  - La machine n'a pas de connectivité Internet
  - La machine est connectée à un réseau de portails captifs
- Les administrateurs doivent vérifier l'état de révocation du certificat de l'appareil avant de présenter la page de connexion aux utilisateurs finaux.

Écran du gestionnaire d'informations d'identification Windows après le VPN Always On avant la configuration de l'ouverture de session Windows

Une fois que la fonctionnalité **VPN toujours actif avant ouverture de session Windows** est configurée, l'écran du **gestionnaire d'informations d'identification Windows** est modifié comme suit.



Lorsque vous cliquez sur **Options de connexion** sur l'écran d'ouverture de session, les informations suivantes s'affichent :

- L'icône NetScaler Gateway indique si la machine est connectée à NetScaler Gateway ou non.
- Selon le mode de configuration utilisateur, l'une des instructions suivantes s'affiche sur l'écran d'ouverture de session.
  - NetScaler Gateway est connecté en mode service
  - NetScaler Gateway est connecté en mode utilisateur

Configurer le VPN Always On avant l'ouverture de session Windows

March 27, 2024

Cette section contient les détails nécessaires pour configurer **le VPN permanent avant l'ouverture de session Windows** à l'aide d'une stratégie avancée.

Pré-requis

- NetScaler Gateway et le plug-in VPN doivent être de version 13.0.41.20 ou ultérieure.
- NetScaler Advanced Edition ou version ultérieure est requis pour que la solution fonctionne.
- Vous pouvez configurer la fonctionnalité uniquement à l'aide de stratégies avancées.
- Le serveur virtuel VPN doit être opérationnel.

Étapes de configuration de

La configuration **Always On VPN avant l'ouverture de session Windows** implique les étapes de haut niveau suivantes :

1. Configurer un tunnel au niveau de la machine
2. Configurer un tunnel au niveau utilisateur (facultatif)
3. Activer l'authentification des utilisateurs

    a) Configurez le serveur virtuel VPN, installez un certificat CA et liez la clé du certificat au serveur virtuel.
    b) Créer un profil d'authentification
    c) Créer un serveur virtuel d'authentification
    d) Créer des stratégies d'authentification
    e) Liez les stratégies au profil d'authentification

Tunnel de niveau machine

Un tunnel au niveau de la machine est établi vers NetScaler Gateway en utilisant le certificat de l'appareil comme identité. Le certificat d'appareil doit être installé sur la machine cliente sous le magasin de machines. Cela s'applique uniquement au service Always On before Windows Logon.

Pour plus de détails sur le certificat d'appareil, voir Utiliser des certificats d'appareil pour l'authentification.

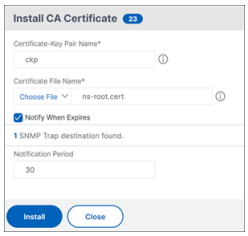
> **Important :**
>
> si le serveur virtuel VPN de l'appliance NetScaler Gateway est configuré sur un port non standard (autre que 443), le tunnel au niveau de la machine ne fonctionne pas comme prévu.

Configurer le tunnel au niveau de la machine à l'aide du certificat de l'appareil

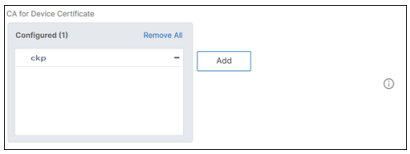
Configuration de l'authentification basée sur le certificat d'appareil à l'aide de

1. Dans l'onglet **Configuration**, accédez à **NetScaler Gateway**> Virtual Servers.

2. **Sur la page Serveurs virtuels NetScaler Gateway, sélectionnez un serveur virtuel existant et cliquez sur Modifier.**
3. Sous **Certificat**, cliquez sur Certificat **CA**.
4. Sur la page de liaison des **certificats CA**, cliquez sur **Ajouter** à côté du champ **Sélectionner un certificat CA**, mettez à jour les informations requises, puis cliquez sur **Installer**.



5. Sur la page du **serveur virtuel VPN**, cliquez sur l'icône de modification.
6. Dans la section **Paramètres de base**, cliquez sur **Plus**.
7. Cliquez sur **Ajouter** à côté de la section **CA for Device Certificate**, puis cliquez sur **OK**.



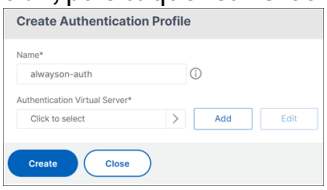
Remarque :ne cochez pas la case **Activer le certificat de l'appareil**.

8. Pour lier un certificat d'autorité de certification au serveur virtuel, cliquez sur Certificat d'autorité de **certification** sous la section **Certificat**. Cliquez sur **Ajouter une liaison** sous la page Liaison de **certificat de l'autorité de certification du serveur virtuel SSL**.

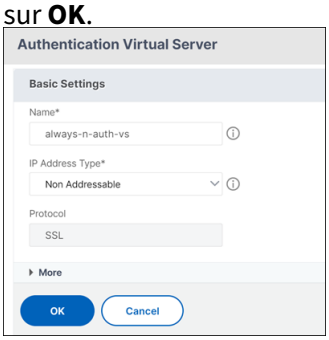
> **Remarque :**
>
> - Le champ Nom commun de l'objet (CN) du certificat de périphérique ne doit pas être vide. Si un appareil tente de se connecter avec des certificats d'appareil CN vides, sa session VPN est créée avec le nom d'utilisateur « anonyme ». Dans IIP, si plusieurs sessions ont le même nom d'utilisateur, les sessions précédentes sont déconnectées. Ainsi, lorsque l'IIP est activé, vous remarquez l'impact de la fonctionnalité en raison d'un nom commun vide.
> - Tous les certificats d'autorité de certification (racine et intermédiaire) susceptibles de signer le certificat de périphérique émis aux clients doivent être liés sous la section **CA for Device Certificate** et également dans la section **Liaison de certificat d'autorité** de certification pour le serveur virtuel aux étapes 4 et 5. Pour plus d'informations sur la liaison d'un certificat d'autorité de certification avec des certificats intermédiaires/-subordonnés, consultez Installer, lier et mettre à jour des certificats.
> - Si plusieurs certificats d'appareil sont configurés, le certificat dont la date d'expira-

> tion est la plus longue est essayé pour la connexion VPN. Si ce certificat autorise l'analyse EPA avec succès, la connexion VPN est établie. Si ce certificat échoue au cours du processus d'analyse, le certificat suivant est utilisé. Ce processus se poursuit jusqu'à ce que tous les certificats soient essayés.

9. Sur la page **CA Certificate Binding**, sélectionnez le certificat.
10. Cliquez sur **Bind**.
11. Créez un serveur virtuel d'authentification.
    a) Sur la page **Serveurs virtuels VPN**, accédez à **Paramètres avancés > Profil d'authentification** et cliquez sur **Ajouter**.
    b) Sur la page **Créer un profil d'authentification**, attribuez un nom au profil d'authentification, puis cliquez sur **Créer**.



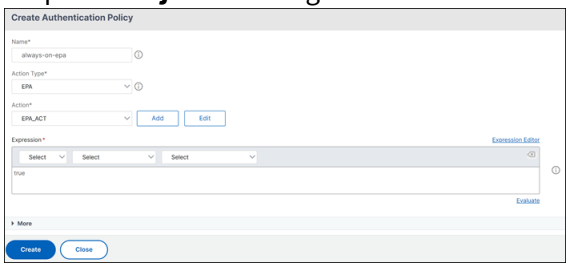
    c) Sur la page **Serveur virtuel d'authentification**, attribuez un nom au serveur virtuel d'authentification. Sélectionnez le type d'adresse IP comme **non adressable,** puis cliquez sur **OK**.



> **Remarque :**
>
> Le serveur virtuel d'authentification reste toujours à l'état DOWN.

12. Créez une stratégie d'authentification.
    a) Dans la section **Stratégies d'authentification avancées** de la page **Sécurité > Trafic des applications AAA > Serveurs virtuels d'authentification**, sélectionnez la stratégie d'authentification et cliquez sur **Ajouter** une liaison.
    b) Sur la page **Policy Binding**, cliquez sur **Ajouter** à côté du champ **Select Policy**.
    c) Sur la page Créer une stratégie d'authentification ;
        i. Attribuez un nom à la stratégie d'authentification avancée.
        ii. Sélectionnez **EPA** dans la liste **Type d'action**.

iii. Cliquez sur **Ajouter** en regard de **Action**.

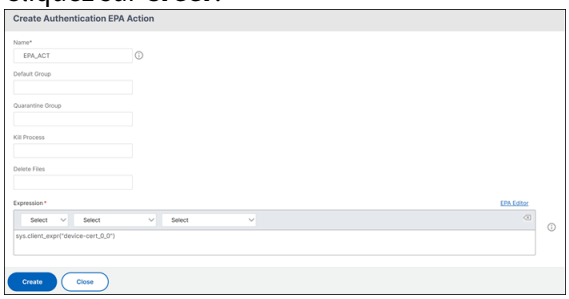


d) Sur la page Créer une action EPA d'authentification ;

i. Attribuez un nom à l'action EPA.

ii. Entrez `sys.client_expr("device-cert_0_0")` dans le champ **Expression**.

iii. Cliquez sur **Créer**.

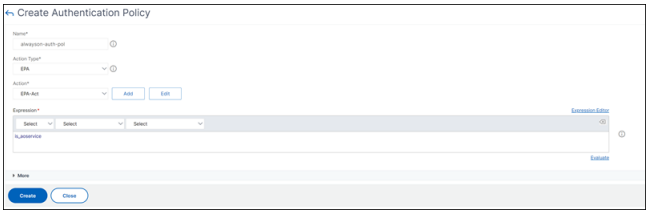


13. Sur la page **Créer une politique d'authentification** ;

a) Attribuez un nom à la stratégie d'authentification.

b) Entrez **is_aoservice** dans le champ **Expression**.

c) Cliquez sur **Créer**.



14. Sur la page Liaison de stratégie, saisissez **100** dans **Priorité**, puis cliquez sur **Liaison**.

Configuration de l'authentification basée sur le certificat d'appareil à l'aide de

1. Installez un certificat CA sur un serveur virtuel VPN.

```
1 add ssl certkey ckp -cert t_CA.cer
2 <!--NeedCopy-->
```

2. Liez le certificat CA au serveur virtuel VPN .


```
bind ssl vserver <vServerName> -certkeyName <string> -ocspCheck (
    Mandatory | Optional )
<!--NeedCopy-->
```

Exemple

```
bind ssl vserver TestClient -CertkeyName ag51.xm.nsi.test.com -CA
    -ocspCheck Mandatory
<!--NeedCopy-->
```

3. Ajoutez un serveur virtuel d'authentification.

```
add authentication authnProfile <name>  {
 -authnVsName <string> }

<!--NeedCopy-->
```

Exemple

```
add authentication authnProfile always_on -authnVsName
    always_on_auth_server
<!--NeedCopy-->
```

4. Créez une action d'authentification EPA.

```
add authentication epaAction <name> -csecexpr <expression>
<!--NeedCopy-->
```

Example

“‘

add authentication epaAction epa-act -csecexpr `sys.client_expr("device-cert_0_0")` -defaultgroup epa_pass

“‘

5. Création d'une stratégie d'authentification

```
add authentication Policy <name> -rule <expression> -action <
    string>
```

Exemple:

```
add authentication Policy always_on_epa_auth -rule is_aoservice -
    action epa_auth
```

> **Important :**
>
> - La configuration du tunnel au niveau de la machine est maintenant terminée. Pour configurer le tunnel au niveau utilisateur après l'ouverture de session Windows, reportez-vous à la section **Tunnel de niveau utilisateur**.

- Sur l'ordinateur client, le certificat de périphérique est au format .pfx. Le certificat .pfx est installé sur l'ordinateur Windows car Windows comprend le format .pfx. Ce fichier contient les fichiers de certificat et de clé. Ce certificat doit appartenir au même domaine qui est lié au serveur virtuel. Les certificats et clés .pfx et serveur peuvent être générés à l'aide de l'assistant de certificat client. Ces certificats peuvent être utilisés avec l'autorité de certification pour générer le .pfx respectif avec le certificat du serveur et le domaine. Le certificat .pfx est installé dans le compte d'ordinateur dans le dossier personnel. La `show aaa session` commande affiche le tunnel de l'appareil sur l'appliance NetScaler.

Tunnel au niveau utilisateur

Remplacer un tunnel au niveau de la machine par un tunnel au niveau utilisateur à l'aide de l'interface graphique

Remarque : L'expression `is_aoservice.not` est applicable à partir des versions 13.0.41.20 et ultérieures de NetScaler Gateway.

1. Configurez une stratégie pour l'authentification des utilisateurs.

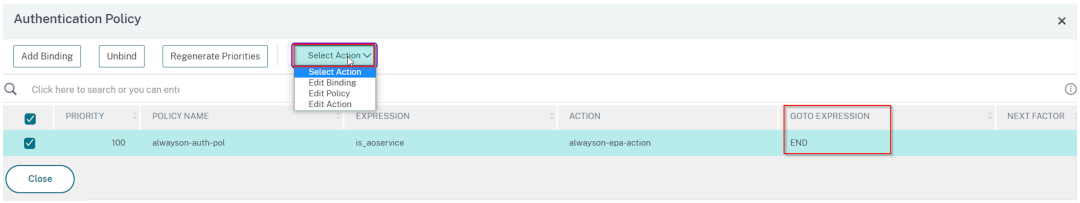
   a) Accédez à **NetScaler Gateway > Serveurs** virtuels et sélectionnez un serveur virtuel.

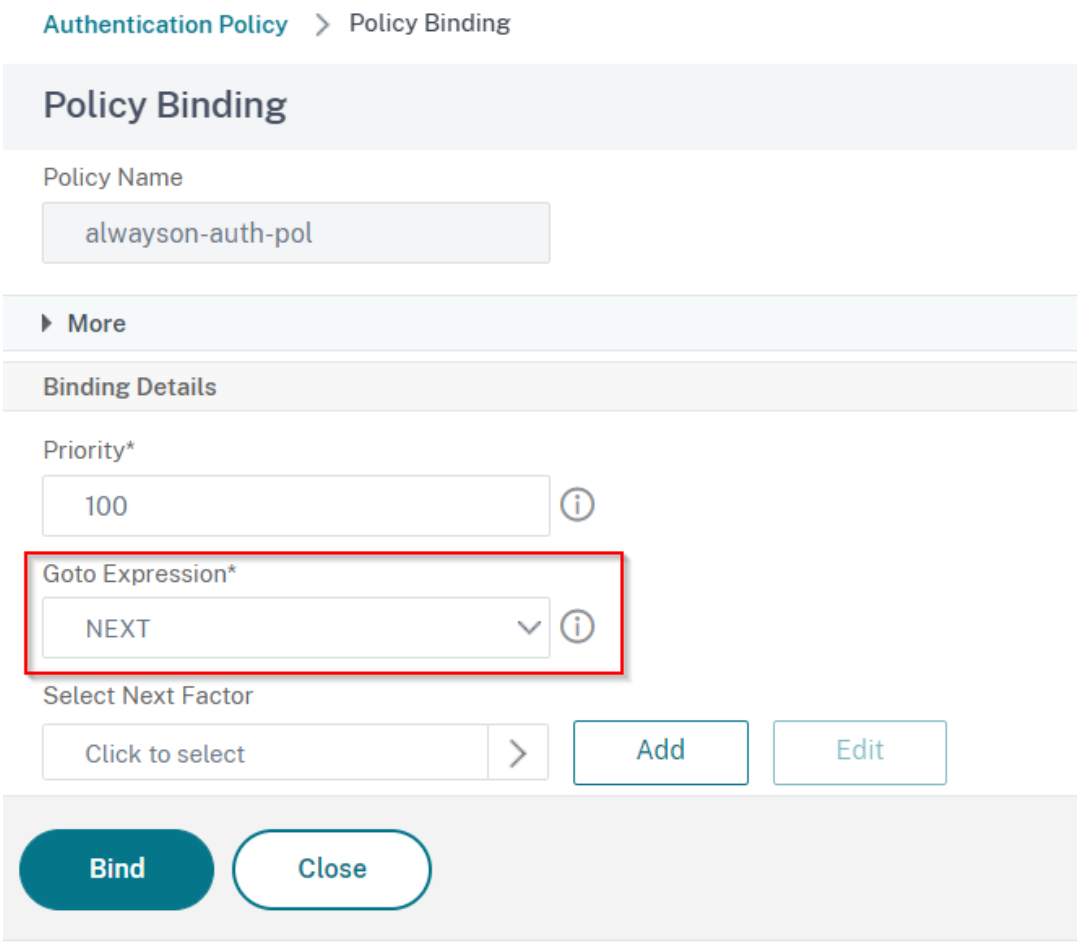
   b) Dans **les paramètres avancés**, cliquez sur **Profil d'authentification**.

   c) Configurez le profil d'authentification.

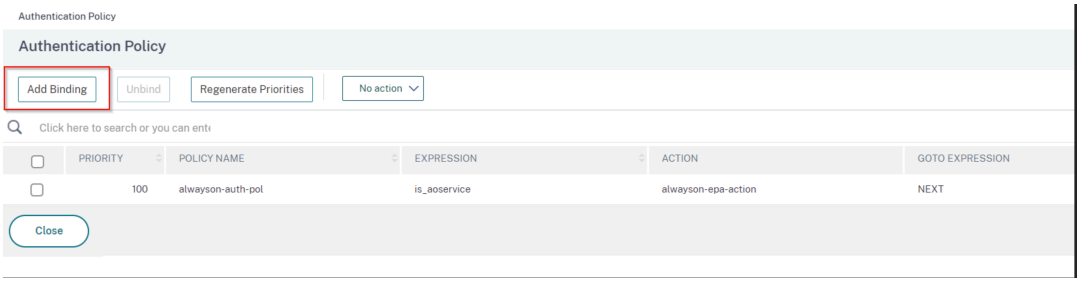
   d) Sur la page **Configuration > Sécurité > Trafic des applications AAA > Serveurs virtuels d'authentification**, sélectionnez la stratégie d'authentification.

   e) Dans **Sélectionner une action**, cliquez sur **Modifier la liaison** et **remplacez Expression GoTo** par **NEXT** au lieu de **END** pour la liaison de stratégie.





f) Cliquez sur **Lier**, puis sur la page **Politique d'authentification**, sélectionnez la stratégie d'authentification et cliquez sur **Ajouter une liaison**.

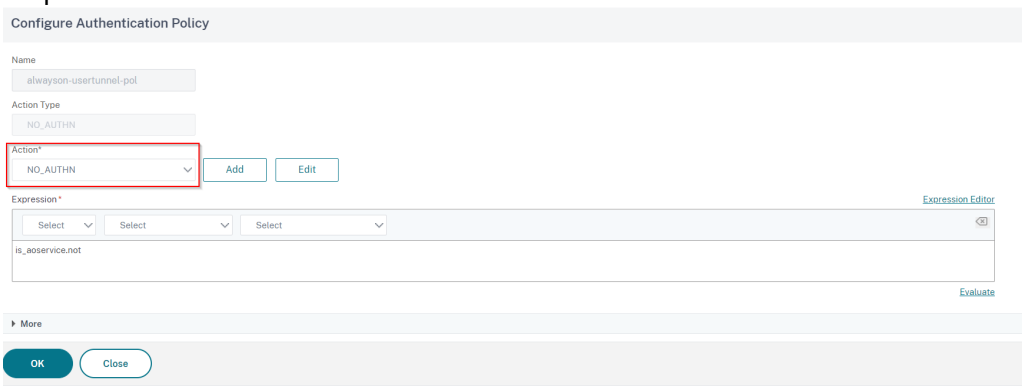


g) Sur la page Liaison de stratégie, cliquez sur **Ajouter** en regard de **Sélectionner une stratégie**.

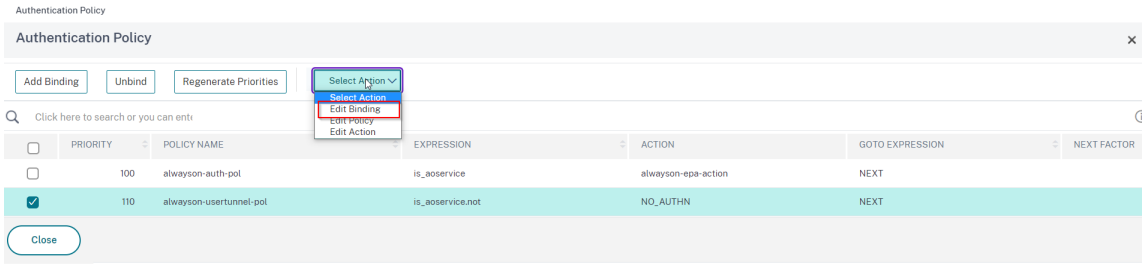
Sur la page Créer une stratégie d'authentification ;

i. Entrez le nom de la stratégie « aucune authentification » à créer.
ii. Sélectionnez le type d'action **No_Authn**.
iii. Entrez **is_aoservice.not** dans le champ **Expression**.

iv. Cliquez sur **Créer**.



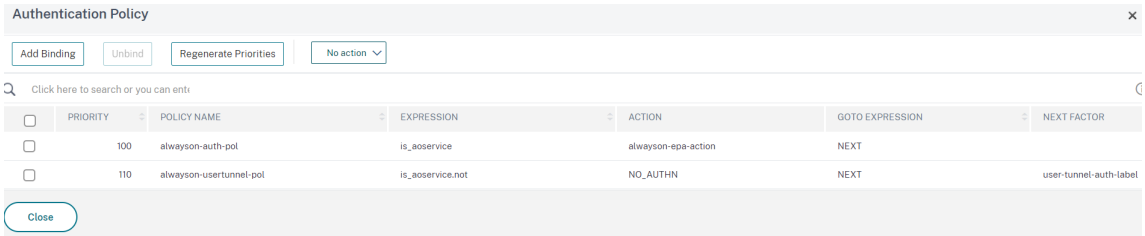
2. Dans **Sélectionner une action**, cliquez sur **Modifier la liaison**.



3. Sur la page Liaison de stratégie, saisissez **110** dans **Priorité**. Cliquez sur **Ajouter** en regard de **Sélectionner le facteur suivant**.

   a) Sur la page Étiquette de stratégie d'authentification, saisissez un nom descriptif pour l'étiquette de stratégie, sélectionnez le schéma de connexion, puis cliquez sur **Continuer**.
   b) Dans **Sélectionner une stratégie**, cliquez sur **Ajouter** et créez une stratégie d'authentification LDAP.
   c) Cliquez sur **Créer,** puis cliquez sur **Liaison.**
   d) Cliquez sur **Terminé,** puis sur **Liaison**.

   Dans la page Stratégie d'authentification, la colonne **Facteur suivant** affiche la stratégie de facteur suivant configurée.



4. Vous pouvez configurer la stratégie LDAP en tant que facteur suivant de la stratégie d'authentification.

   a) Sur la page Créer une stratégie d'authentification, entrez un nom pour la stratégie LDAP.

b) Sélectionnez **Type d'action** en tant que **LDAP**.
c) Entrez **Action en tant qu'action** LDAP configurée.

> **Remarque :**
>
> - Pour créer un fichier XML de schéma de connexion, consultez la section Fichier XML de schéma de connexion.
> - Pour créer des étiquettes de stratégie, voir Authentifier l'étiquette de stratégie.
> - Pour créer une stratégie d'authentification LDAP, consultez Pour configurer l'authentification LDAP à l'aide de l'utilitaire de configuration.

Remplacer un tunnel au niveau de la machine par un tunnel au niveau utilisateur en utilisant l'interface de ligne de commande

1. Lier une stratégie au serveur virtuel d'authentification

```
bind authentication vserver <name> -policy <name> -priority  <
    positive_integer> -gotoPriorityExpression <expression>
```

Exemple

```
bind authentication vserver alwayson-auth-vserver -policy alwayson
    -auth-pol -priority 100 -gotoPriorityExpression NEXT
```

2. Ajoutez une stratégie d'authentification avec l'action en tant que `NO_AUTH` et l'expression `is_aoservice.not`, et liez-la à la stratégie.

```
add authentication Policy <name> -rule <expression> -action <
    string>

bind authentication vserver <name> -policy <name> -priority <
    positive_integer> -gotoPriorityExpression <expression>
```

Exemple

```
add authentication Policy alwayson-usertunnel-pol -rule
    is_aoservice.not -action NO_AUTHN

bind authentication vserver alwayson-auth-vserver -policy alwayson
    -usertunnel-pol -priority 110
```

3. Ajoutez un facteur suivant et liez l'étiquette de stratégie au facteur suivant.

```
add authentication policylabel <labelName> -loginSchema <string>

bind authentication  policylabel <string>  -policyName <string>  -
    priority <positive_integer> -gotoPriorityExpression <expression
    > -nextFactor <string>
```


Exemple

```
add authentication policylabel user-tunnel-auth-label -loginSchema
    singleauth_alwayson

bind authentication policylabel user -policyName alwayson-
   usertunnel-pol -priority 100
```

4. Configurez une stratégie LDAP et liez-la à l'étiquette de stratégie de tunnel utilisateur.

```
add authentication policy <name>  -rule <expression>  -action <
   string>

bind authentication vserver <vserver_name> -policy <string>  -
   priorit < positive integer>  gotoPriorityExpression <string>
```

Exemple

```
add authentication Policy LDAP_new -rule true -action LDAP_new

bind authentication policylabel user-tunnel-auth-label -policyName
    LDAP_new -priority 100 -gotoPriorityExpression NEXT
```

Configuration côté client

Ils `AlwaysOn, locationDetection, and suffixList registries` sont facultatifs et ne sont nécessaires que si la fonctionnalité de détection d'emplacement est requise.

Pour accéder aux entrées de clé de registre, accédez au chemin suivant : **Ordinateur> HKEY_LOCAL_MACHINE>So Access Client**

Clé de registre	Type de registre	Valeurs et description
AlwaysOnService	REG_DWORD	1 => Établir un tunnel au niveau machine mais pas un tunnel au niveau utilisateur ; 2 => Établir un tunnel au niveau machine et un tunnel au niveau utilisateur

Clé de registre	Type de registre	Valeurs et description
AlwaysOnURL	REG SZ	URL du serveur virtuel NetScaler Gateway auquel l'utilisateur souhaite se connecter. **Exemple :** `https://xyz.companyDomain.com` **Important :** Une seule URL est responsable du tunnel au niveau de la machine et du tunnel au niveau utilisateur. Le registre AlwaysOnURL aide le composant de niveau service et utilisateur à travailler et à connecter un tunnel distinct, c'est-à-dire un tunnel au niveau machine et un tunnel au niveau utilisateur en fonction de la conception
AlwaysOn	REG_DWORD	1 => Autoriser l'accès au réseau en cas de défaillance du VPN ; 2=> Bloquer l'accès réseau en cas de panne VPN
AlwaysOnAllowlist	REG_SZ	Liste d'adresses IP ou de noms de domaine FQDN séparés par des points-virgules qui doivent être mis sur liste blanche lorsque la machine fonctionne en mode strict. **Exemple :** `8.8.8.8;linkedin.com`

Clé de registre	Type de registre	Valeurs et description
UserCertCAList	REG_SZ	Liste de noms d'autorité de certification racine séparés par des virgules ou des points-virgules, c'est-à-dire le nom de l'émetteur du certificat. Utilisé dans le contexte d'un service Always On dans lequel un client peut spécifier la liste des autorités de certification dans lesquelles choisir le certificat client. **Exemple**: `cgwsanity.net;xyz.gov.in`
locationDetection	REG_DWORD	1 => Pour activer la détection de position ; 0 => Pour désactiver la détection de position
suffixList	REG SZ	Liste de domaines séparés par des points-virgules et chargée de vérifier si la machine se trouve sur l'intranet ou non à un moment donné lorsque la détection de localisation est activée. **Example:** `citrite.net,cgwsanity.net`

Pour plus d'informations sur ces entrées de Registre, consultez Toujours allumé.

> **Remarque :**
>
> Lorsque le service Always On est configuré, le profil Always On configuré sur le serveur virtuel NetScaler Gateway ou sur NetScaler est ignoré côté client. Assurez-vous donc d'activer également les `locationDetection`registres et `AlwaysOn`VPN lors de la configuration du service Always On.
> ‘‘‘

Utilisation de la stratégie avancée pour créer des stratégies VPN

March 27, 2024

Classic Policy Engine (PE) et Advance Policy Infrastructure (PI) sont deux frameworks différents de configuration et d'évaluation des stratégies actuellement pris en charge par NetScaler.

Advance Policy Infrastructure est un langage d'expression puissant. Le langage d'expression peut être utilisé pour définir des règles dans la stratégie, définir diverses parties de l'action et d'autres entités prises en charge. Le langage d'expression peut analyser n'importe quelle partie de la requête ou de la réponse et vous permet également d'examiner en profondeur les en-têtes et la charge utile. Le même langage d'expression s'étend et fonctionne dans tous les modules logiques pris en charge par NetScaler.

> **Remarque :**
> Nous vous encourageons à utiliser des stratégies avancées pour créer des stratégies.

Pourquoi migrer de la stratégie classique vers la stratégie avancée ?

Advanced Policy dispose d'un jeu d'expressions riche et offre une plus grande flexibilité que la stratégie classique. NetScaler évolue et répond aux besoins d'une grande variété de clients. Il est donc impératif de prendre en charge des expressions qui dépassent largement les stratégies avancées. Pour plus d'informations, voir Stratégies et expressions.

Voici les fonctionnalités ajoutées pour Advance Policy.

- Possibilité d'accéder au corps des messages.
- Prend en charge de nombreux autres protocoles.
- Permet d'accéder à de nombreuses autres fonctionnalités du système.
- Il dispose d'un plus grand nombre de fonctions, d'opérateurs et de types de données de base.
- S'adresse à l'analyse des fichiers HTML, JSON et XML.
- Facilite la mise en correspondance rapide de plusieurs chaînes parallèles (`patsets`et ainsi de suite).

Les stratégies VPN suivantes peuvent désormais être configurées à l'aide de la stratégie avancée.

- Stratégie de session
- Stratégie d'autorisation
- Stratégie de trafic
- Stratégie de tunnel
- Stratégie d'audit

En outre, l'analyse des points de terminaison (EPA) peut être configurée en tant que fonction nFactor pour l'authentification. L'EPA est utilisé comme contrôleur d'accès pour les terminaux qui tentent de se connecter à l'appliance Gateway. Avant que la page d'ouverture de session de la passerelle ne s'affiche sur un périphérique de point de terminaison, la configuration matérielle et logicielle minimale requise est vérifiée sur le périphérique, en fonction des critères d'éligibilité configurés par l'administrateur de la passerelle. L'accès à la passerelle est accordé en fonction du résultat des vérifications effectuées. Auparavant, l'EPA était configuré dans le cadre de la stratégie de session. Désormais, il peut être lié à nFactor pour plus de flexibilité quant au moment où il peut être exécuté. Pour plus d'informations sur EPA, consultez la rubrique Fonctionnement des stratégies de point de terminaison. Pour en savoir plus sur NFactor, consultez la rubrique Authentification NFactor.

Cas d'utilisation :

EPA de pré-authentification à l'aide de l'EPA avancée

L'analyse EPA de pré-authentification a lieu avant qu'un utilisateur ne fournisse les informations d'identification d'ouverture de session. Pour plus d'informations sur la configuration de NetScaler Gateway pour l'authentification nFactor avec le scan EPA de pré-authentification comme l'un des facteurs d'authentification, consultez la rubrique CTX224268.

EPA post-authentification à l'aide de l'EPA avancée

L'analyse EPA post-authentification se produit après la vérification des informations d'identification de l'utilisateur. Dans l'infrastructure de stratégie classique, l'EPA post-authentification a été configuré dans le cadre de la stratégie de session ou de l'action de session. Dans l'infrastructure de stratégie avancée, l'analyse EPA doit être configurée en tant que facteur EPA dans l'authentification nFactor. Pour plus d'informations sur la configuration de NetScaler Gateway pour l'authentification nFactor avec le scan EPA post-authentification comme l'un des facteurs d'authentification, consultez la rubrique CTX224303.

EPA de pré-authentification et de post-authentification à l'aide de stratégies avancées

L'EPA peut être effectuée avant l'authentification et la post-authentification. Pour plus d'informations sur la configuration de NetScaler Gateway pour l'authentification nFactor avec des analyses EPA avant et après authentification, consultez la rubrique CTX231362.

Analyse EPA périodique en tant que facteur d'authentification nFactor

Dans l'infrastructure de stratégie classique, une analyse EPA périodique a été configurée dans le cadre de l'action de stratégie de session. Dans l'infrastructure de stratégie avancée, il peut être configuré

dans le cadre du facteur EPA dans l'authentification nFactor.

Pour plus d'informations sur la configuration de l'analyse EPA périodique en tant que facteur d'authentification nFactor, cliquez sur la rubriqueCTX231361.

Résolution des problèmes :

Les points suivants doivent être gardés à l'esprit pour le dépannage.

- Les stratégies Classic et Advance du même type (par exemple, stratégie de session) ne peuvent pas être liées à la même entité/point de liaison.
- La priorité est obligatoire pour toutes les stratégies PI.
- La stratégie avancée pour le VPN peut être liée à tous les points de liaison.
- Une stratégie avancée avec la même priorité peut être liée à un seul point de liaison.
- Si aucune des stratégies d'autorisation configurées n'est sélectionnée, l'action d'autorisation globale configurée dans le paramètre VPN est appliquée.
- Dans la stratégie d'autorisation, l'action d'autorisation n'est pas annulée si la règle d'autorisation échoue.

Expressions équivalentes à la stratégie avancée couramment utilisées pour la stratégie classique :

Expressions de stratégie classiques	Expressions de stratégie avancée
ns_true	true
ns_false	false
REQ.HTTP	HTTP.REQ
RES.HTTP	HTTP.RES
HEADER “foo”	HEADER(“foo”)
CONTAINS ”bar”	.CONTAINS(“bar”) [Note use of “..”]
REQ.IP	CLIENT.IP
RES.IP	SERVER.IP
SOURCEIP	SRC
DESTIP	DST
REQ.TCP	CLIENT.TCP
RES.TCP	SERVER.TCP
SOURCEPORT	SRCPORT
DESTPORT	DSTPORT

Expressions de stratégie classiques	Expressions de stratégie avancée
STATUSCODE	STATUS
REQ.SSL.CLIENT.CERT	CLIENT.SSL.CLIENT_CERT

Configurer le serveur virtuel VPN DTLS à l'aide du serveur virtuel VPN SSL

March 27, 2024

Vous pouvez configurer un serveur virtuel VPN DTLS pour NetScaler Gateway en utilisant la même adresse IP et le même numéro de port qu'un serveur virtuel VPN SSL configuré. La configuration des serveurs virtuels VPN DTLS vous permet de lier les chiffrements et certificats DTLS avancés au trafic DTLS pour une sécurité renforcée.

> **Important :**
>
> - Par défaut, la fonctionnalité DTLS est définie sur ON pour le serveur virtuel VPN SSL existant. Désactivez la fonctionnalité du serveur avant de créer le serveur virtuel VPN DTLS.
> - Le serveur virtuel de passerelle SNI pour DTLS est pris en charge dans NetScaler Gateway version 13.0 build 64.x et versions ultérieures.
> - À partir de NetScaler version 13.0 build 79.x, le `helloverifyrequest` paramètre est activé par défaut. L'activation du paramètre `helloverifyrequest` sur le profil DTLS permet d'atténuer le risque qu'un attaquant ou des bots submerge le débit réseau, entraînant potentiellement un épuisement de la bande passante sortante. C'est-à-dire qu'il aide à atténuer l'attaque d'amplification DDoS DTLS. Pour plus d'informations sur le paramètre,`helloverifyrequest` consultez la section Profil DTLS.
> - Lors de la gestion du trafic UDP, la consommation de mémoire de l'appliance NetScaler augmente si les serveurs principaux acheminent un trafic important. Par conséquent, l'appliance NetScaler ne peut pas transférer ce trafic vers le client en raison de la connexion TCP MUX côté client. Dans ce cas, Citrix vous recommande d'utiliser le protocole DTLS.

Points à noter

- Le serveur virtuel VPN DTLS sur une appliance NetScaler Gateway peut être configuré à partir de la version 13.0 build 58.x.

- Avant de configurer un serveur virtuel VPN DTLS sur une appliance NetScaler Gateway, vous devez avoir configuré un serveur virtuel VPN SSL sur l'appliance.
- Le serveur virtuel VPN DTLS utilise l'adresse IP et le numéro de port du serveur virtuel VPN SSL configuré.
- Si la connexion DTLS échoue, la connexion revient au protocole TLS.
- Pour utiliser DTLS uniquement, vous pouvez désactiver le protocole TLS en liant uniquement les chiffrements DTLS au trafic DTLS.
- Le multiplexage DTLS n'est pas pris en charge lorsque le trafic TCP est tunnelisé sur VPN.

Configurer un serveur virtuel VPN DTLS à l'aide de l'interface graphique

1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Virtual Servers**.
2. Sur la page **Serveurs virtuels NetScaler Gateway**, sélectionnez le serveur virtuel VPN SSL existant et cliquez sur **Modifier**.
3. Sur la page **Serveur virtuel VPN**, cliquez sur l'icône Modifier et désactivez la case à cocher **DTLS**, puis cliquez sur **OK**.
4. Revenez à **NetScaler Gateway > Virtual Servers** et cliquez sur **Ajouter**.
5. Sous **Paramètres de base**, saisissez les valeurs des champs suivants, puis cliquez sur **OK**.
    - Nom : nom du serveur virtuel VPN DTLS
    - Protocole - Sélectionnez DTLS
    - Adresse IP —Entrez l'adresse IP du serveur virtuel VPN SSL
    - Port —Entrez le numéro de port du serveur virtuel VPN SSL
6. Sur la page **Serveurs virtuels NetScaler Gateway**, sélectionnez le serveur virtuel que vous avez ajouté précédemment et cliquez sur **Modifier**.
7. Sous **Certificats**, cliquez sur l'icône en forme de flèche pour sélectionner la clé de certificat requise.
8. Dans la section **Liaison des certificats de serveur > Sélectionner un certificat**de serveur, sélectionnez une clé de certificat SSL existante ou créez-en une.
9. Cliquez sur **Bind** dans la page **Liaison de certificat de serveur**.

> **Remarque :**
>
> - Pour utiliser DTLS 1.2, cliquez sur l'icône de modification sous Paramètres SSL et cochez la case **DTLS 1.2**.
> - L'indication de nom de serveur (SNI) est prise en charge pour les serveurs virtuels VPN de

> type DTLS.

Configurer un serveur virtuel VPN DTLS à l'aide de l'interface de ligne de commande

À l'invite de commandes, saisissez le jeu de commandes suivant :

```
set vpn vserver <ssl vpnvserver name> -dtls off
add vpn vserver <dtls vpnvserver name> dtls <ssl vpn vserver IP> <ssl vpn vserver port>
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key>
<!--NeedCopy-->
```

DTLS 1.0 fonctionne comme d'habitude. Pour utiliser DTLS 1.2, tapez la commande suivante :

```
set ssl vserver < dtls vpnvserver name > -dtls12 ENABLED
<!--NeedCopy-->
```

Exemple

```
set vpn vserver vpnvserver  -dtls off
add vpn vserver vpnvserver_dtls dtls 10.108.45.220 443
bind ssl vservser vpnvserver_dtls -certkeyName sslcertkey
set ssl vserver vpnvserver_dtls -dtls12 ENABLED
<!--NeedCopy-->
```

Pour activer le SNI pour le serveur virtuel VPN de type DTLS, tapez la commande suivante :

```
set ssl vserver <vServerName>@ [-SNIEnable ( ENABLED | DISABLED )
bind ssl vservser <dtls vpnvserver name> -certkeyName <existing ssl cert key or newly created cert key> <-SNICert>
<!--NeedCopy-->
```

Exemple

```
set ssl vserver _XD_10.106.40.225_443_DTLS -sniEnable eNABLED
bind ssl vserver _XD_10.106.40.225_443_DTLS -certkeyName "Insight/*.insight.net.cer_CERT_" -snICert

<!--NeedCopy-->
```

Paramètres de serveur virtuel VPN DTLS pris en charge

Seuls les paramètres suivants sont pris en charge pour le serveur virtuel VPN de type DTLS.

- Ipaddress
- Port
- État

- Double saut
- downstateflush
- Commentaire
- Appflowlog
- Icmpvsrresponse

Paramètres de serveur virtuel VPN DTLS non pris en charge

Les paramètres suivants ne sont pas pris en charge pour le serveur virtuel VPN de type DTLS.

- LinuxEPAPluginUpgrade
- WindowsEPAPluginUpgrade
- maxAAAUsers
- icaProxySessionMigration
- loginOnce
- cginfraHomePageRedirect
- logoutOnSmartcardRemoval
- l2Conn
- MacEPAPluginUpgradeRHIstate
- icaOnly
- maxLoginAttempts
- failedLoginTimeout
- vserverFqdn
- deviceCert
- rdpServerProfileName
- pcoipVserverProfileName
- tcpProfileName
- netProfile
- authnProfile
- Listenpriority
- Listenpolicy
- ipset
- certkeyNames

Configurer un serveur virtuel DTLS à l'aide de l'assistant XenApp et XenDesktop

1. Cliquez sur **XenApp et XenDesktop** sous **Intégrer aux produits Citrix**.
2. Dans l'assistant d'installation de XenApp et XenDesktop, sélectionnez **StoreFront** et cliquez sur **Continuer**.

3. Sur la page **Paramètres NetScaler Gateway**, activez la case à cocher **Configurer un écouteur DTLS pour ce vServer VPN** et cliquez sur **Continuer**.

   L'écouteur DTLS est maintenant configuré.

4. Dans Certificat de serveur, cliquez sur **Choisir un fichier** pour sélectionner un certificat de serveur, puis cliquez sur **Continuer**.
5. Spécifiez le fichier de certificat et le nom du fichier clé, puis cliquez sur **Continuer**.
6. Dans la section **StoreFront**, indiquez les valeurs des paramètres requis comme suit et cliquez sur **Continuer**.
7. Dans la section **Authentification**, saisissez les valeurs des paramètres requis comme suit et cliquez sur **Tester la connexion**.

   Assurez-vous que le serveur est accessible, indiquez la valeur de délai d'exécution et l'attribut de nom d'ouverture de session du serveur, puis cliquez sur **Continuer**.

8. Cliquez sur **OK** pour terminer la configuration.

Limitations

- DTLS 1.2 est pris en charge sur les clients Windows uniquement.
- Le serveur virtuel VPN avec DTLS ne prend pas en charge les adresses IPv6.
- La stratégie SSL et le profil SSL ne sont pas pris en charge sur un serveur virtuel VPN DTLS. De plus, la liaison de la stratégie de serveur virtuel VPN n'est pas prise en charge.
- Le serveur virtuel VPN NetScaler Gateway DTLS ne prend pas en charge les fonctionnalités suivantes. Toutefois, le serveur virtuel VPN SSL NetScaler Gateway prend en charge les fonctionnalités suivantes :
  - Unified Gateway avec serveur virtuel de commutation de contenu
  - UDP MUX
  - Vidéo UDP
  - Audio UDP
  - PCOIP
- La `stat vpn vserver` commande relative aux statistiques du serveur virtuel VPN DTLS n'est pas prise en charge.
- Les clés HSM ne sont pas prises en charge par le serveur virtuel DTLS.
- La configuration du cluster n'est pas prise en charge

Intégration aux produits NetScaler

March 27, 2024

Si vous êtes administrateur système responsable de l'installation et de la configuration de NetScaler Gateway, vous pouvez configurer l'appliance pour qu'elle prenne en charge Citrix Endpoint Management, StoreFront et l'interface Web.

Les utilisateurs peuvent se connecter directement à Endpoint Management depuis le réseau interne ou depuis un emplacement distant. Lorsque les utilisateurs se connectent, ils peuvent accéder à leurs applications Web, SaaS et mobiles. Ils peuvent également prendre en charge les documents situés dans ShareFile depuis n'importe quel appareil.

Pour autoriser les utilisateurs à se connecter à une batterie de serveurs via NetScaler Gateway, vous devez configurer les paramètres dans StoreFront ou dans l'interface Web, ainsi que sur NetScaler Gateway. Lorsque les utilisateurs se connectent, ils ont accès aux applications publiées et aux bureaux virtuels.

Les étapes de configuration pour intégrer NetScaler Gateway à Endpoint Management, StoreFront et à l'interface Web supposent ce qui suit :

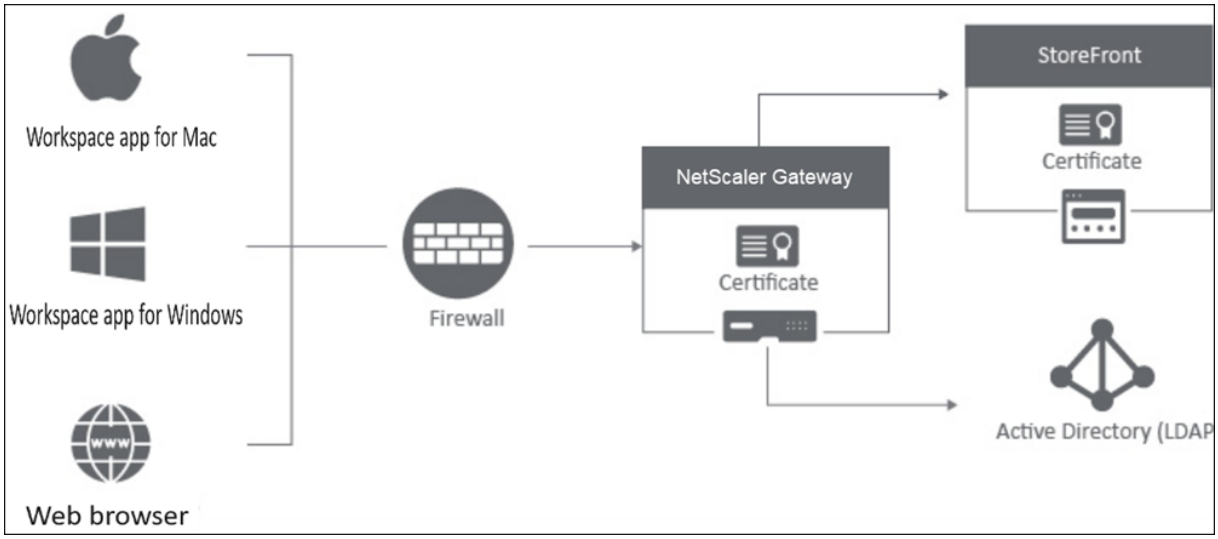
- NetScaler Gateway réside dans la zone démilitarisée et est connecté à un réseau existant.
- NetScaler Gateway est déployé en tant qu'appliance autonome et les utilisateurs distants se connectent directement à NetScaler Gateway.
- StoreFront, Endpoint Management, Citrix Virtual Apps, Citrix Virtual Desktops et l'interface Web résident dans le réseau sécurisé.
- ShareFile est configuré dans Endpoint Management. Pour plus d'informations sur ShareFile, consultez les rubriques ShareFile et Configuration de ShareFile pour l'accès utilisateur.

La façon dont vous déployez StoreFront et Endpoint Management dépend des applications que vous fournissez aux appareils mobiles. Si les utilisateurs ont accès aux applications MDX qui sont encapsulées avec le MDX Toolkit, Endpoint Management se trouve en face de StoreFront dans le réseau sécurisé. Si vous ne fournissez pas l'accès aux applications MDX, StoreFront se trouve devant Endpoint Management dans le réseau sécurisé.

Intégrer NetScaler Gateway à StoreFront

March 27, 2024

Cet article explique comment créer un serveur virtuel NetScaler Gateway pour accéder à distance à StoreFront, pour les utilisateurs qui utilisent l'application Citrix Workspace ou un navigateur Web.



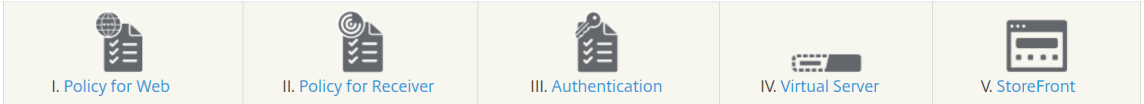
Les utilisateurs se connectent à NetScaler Gateway via un navigateur Web ou l'application Citrix Workspace.NetScaler Gateway authentifie les utilisateurs en fonction des stratégies configurées. Si l'authentification est réussie, NetScaler Gateway permet aux utilisateurs de s'identifier de manière unique au magasin et de transmettre le magasin StoreFront à l'utilisateur par proxy.

> **Important :**
>
> Nous vous recommandons de ne pas utiliser l'assistant Citrix Virtual Apps and Desktops pour intégrer NetScaler Gateway à StoreFront, car cela crée une configuration non valide à l'aide des stratégies d'authentification classiques (obsolète).

Configurer NetScaler Gateway pour l'utiliser avec StoreFront

Pour intégrer NetScaler Gateway à StoreFront, procédez comme suit :

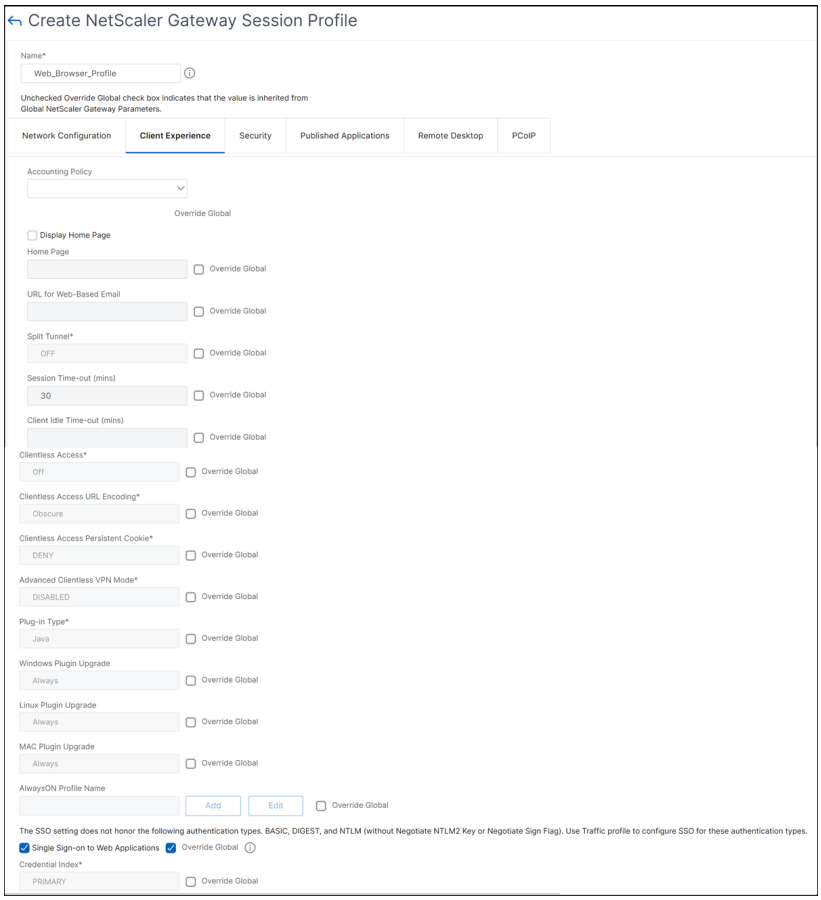
1. Créer une stratégie de session pour l'accès par navigateur Web
2. Créer une stratégie de session pour l'accès basé sur les applications Citrix Workspace
3. Créer un profil d'authentification
4. Création d'un serveur virtuel NetScaler Gateway
5. Ajoutez l'instance NetScaler Gateway sur StoreFront



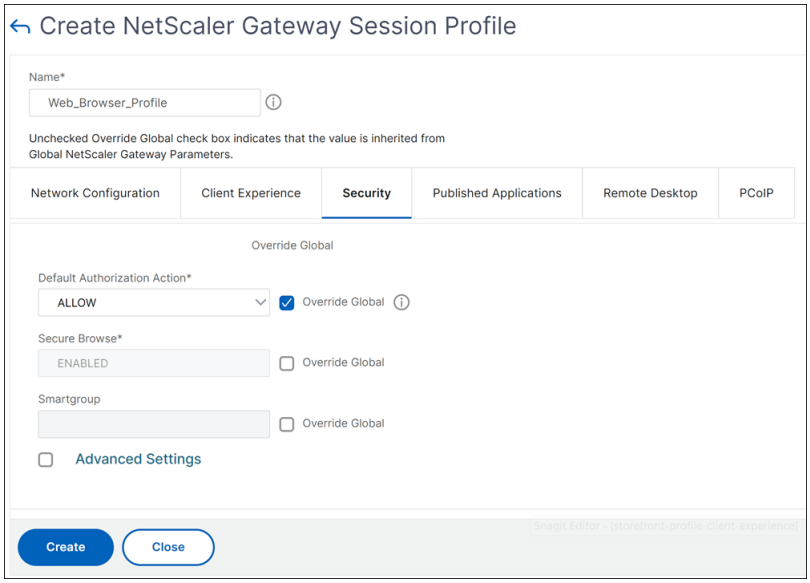
1. Créer une stratégie de session pour l'accès par navigateur Web

1. Accédez à **Configuration > NetScaler Gateway > Politiques**Session.

2. Dans l'onglet **Profils de session**, cliquez sur **Ajouter**.
3. Attribuez un nom au profil de session.
4. Dans l'onglet **Expérience client**, activez les paramètres suivants :
   - **Type**de plug-in : le type de plug-in est défini sur **Java**, par défaut. Bien que ce paramètre soit facultatif, il est recommandé aux utilisateurs qui souhaitent désactiver le VPN complet.
   - **Authentification unique à l'application**Web : en sélectionnant cette option, lorsqu'un utilisateur se connecte à NetScaler Gateway, il transmet les informations d'identification au site Web StoreFront. Ce paramètre évite aux utilisateurs d'avoir à saisir leurs informations d'identification deux fois. Toutefois, vous devez également activer la méthode d'authentification Pass-through depuis NetScaler Gateway sur StoreFront. Désactivez cette option si vous demandez aux utilisateurs de se connecter à NetScaler Gateway et au magasin StoreFront avec des informations d'identification différentes.

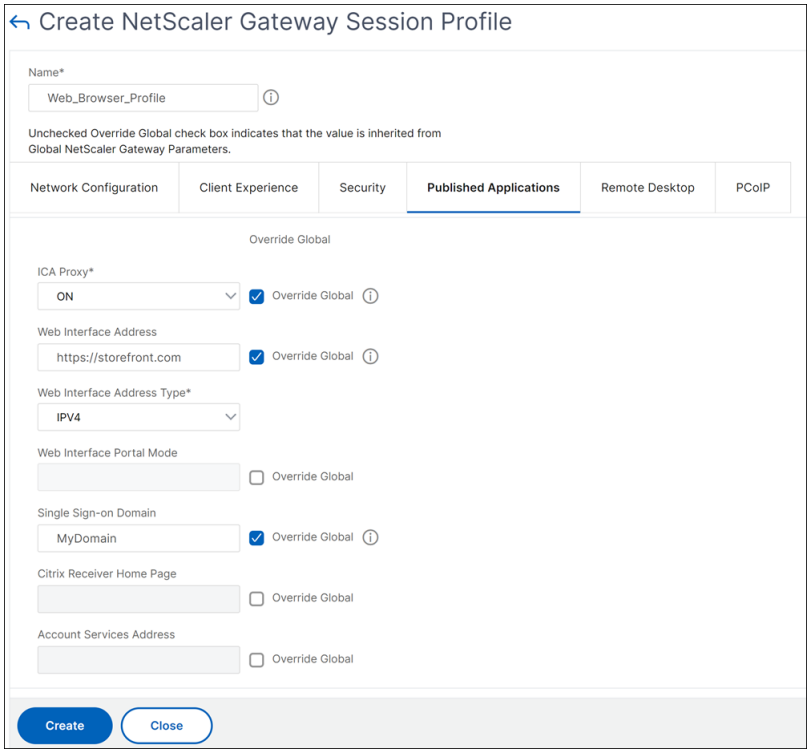


5. Dans l'onglet **Sécurité**, activez l'**action d'autorisation par défaut** et définissez-la sur **AUTORISER**.



6. Dans l'onglet **Applications publiées**, activez les paramètres suivants :

   - **Proxy ICA**: Réglez sur ON.
   - **Adresse**de l'interface Web : nom de domaine complet du serveur StoreFront suivi du chemin d'accès au site Web du magasin.
   - **Domaine**d'authentification unique : si vous n'utilisez qu'un seul domaine, entrez éventuellement le nom NetBIOS du domaine.

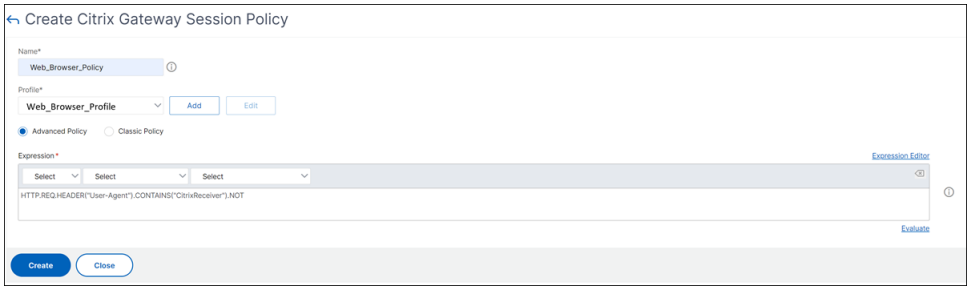


7. Cliquez sur **Créer**.

8. Dans l'onglet **Stratégies de session**, cliquez sur **Ajouter**. La stratégie de session est requise pour que NetScaler puisse différencier les connexions basées sur un navigateur Web et celles basées sur l'application Citrix Workspace. Cette stratégie s'applique aux connexions basées sur un navigateur Web.
9. Dans **Nom**, attribuez un nom à la stratégie de session.
10. Dans **Profil**, sélectionnez le profil de session que vous avez créé.
11. Cliquez sur l'option **Stratégie avancée** et entrez la syntaxe suivante sous **Expression** :

    ```
    HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT
    ```

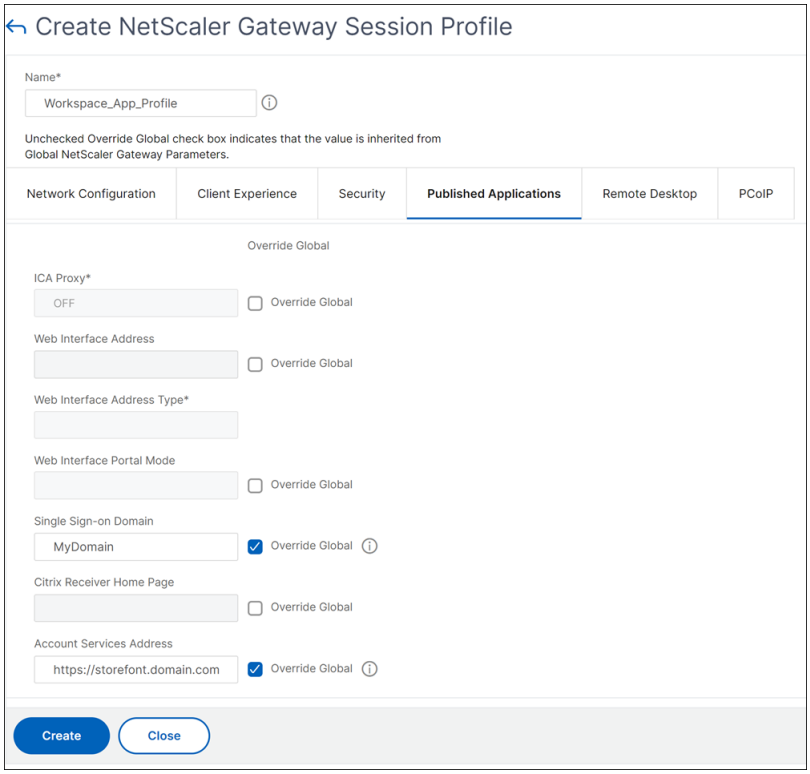
12. Cliquez sur **Créer**.



Pour plus d'informations sur les stratégies de session NetScaler Gateway, consultez la section Stratégies de session.

2. Créer une stratégie de session pour l'accès basé sur les applications Citrix Workspace

Répétez les étapes précédentes pour créer une stratégie de session et un profil de session pour l'accès basé sur l'application Citrix Workspace. Toutefois, dans l'onglet **Applications publiées**, au lieu de configurer l'adresse de l'interface Web, vous devez configurer le paramètre d'**adresse de service du compte**. Cette étape nécessite que vous fournissiez le nom de domaine complet du serveur StoreFront. L'application Citrix Workspace utilise cette adresse pour découvrir les magasins disponibles sur le serveur.



3. Créer un profil d'authentification

Créez un profil d'authentification sur NetScaler en fonction du type de méthode d'authentification que vous devez configurer.

Bien que cette étape soit facultative, il est recommandé d'utiliser NetScaler Gateway pour authentifier l'identité des utilisateurs avant d'accorder l'accès à StoreFront.

Reportez-vous à Authentification et autorisation pour plus de détails.

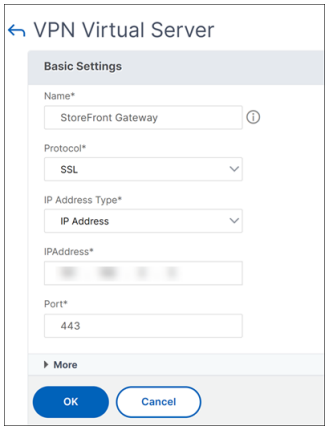
4. Création d'un serveur virtuel NetScaler Gateway

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Cliquez sur **Ajouter** pour ajouter un serveur virtuel NetScaler Gateway.
3. Attribuez un nom et une adresse au serveur virtuel.

   > **Remarque :**
   >
   > Si vous choisissez de ne pas utiliser NetScaler Gateway pour authentifier les utilisateurs, cliquez sur **Plus** et décochez la case **Activer l'authentification**.

4. Sous **Certificat**, cliquez sur **Certificat de serveur**.

5. Téléchargez un certificat de serveur et cliquez sur **Lier**.
6. Ajoutez les stratégies de session :
    a) Sous **Stratégies**, cliquez sur **+**.
    b) Dans la liste déroulante **Choisir une stratégie**, sélectionnez **Session**. Dans la liste déroulante **Type**, sélectionnez **Demande**, puis cliquez sur **Continuer**.
    c) Sous **Policy Binding**, cliquez sur **Select Policy** et sélectionnez la stratégie de session basée sur le navigateur Web et la stratégie de session basée sur l'application Citrix Workspace que vous avez précédemment créées, puis cliquez **sur**Lier pour lier les stratégies de session au serveur virtuel.
7. Sous **Applications publiées**, cliquez sur **Serveur STA**. Spécifiez au moins une URL de la Security Ticket Authority (STA). Si vous utilisez Citrix Virtual Apps and Desktops, entrez les URL des Desktop Delivery Controller. Si vous utilisez Citrix DAaS, entrez les URL des Citrix Cloud Connectors.
8. Sous **Profil d'authentification**, sélectionnez le profil d'authentification que vous avez créé. Cette étape est requise car les stratégies classiques ne sont plus prises en charge.
9. Cliquez sur **Terminé**.



5. Ajouter une instance NetScaler Gateway sur StoreFront

Pour savoir comment ajouter une instance NetScaler Gateway sur StoreFront, consultez la section Configurer NetScaler Gateways.

Références

Pour plus d'informations sur l'intégration entre StoreFront et NetScaler Gateway, consultez les rubriques suivantes :

- Ajouter NetScaler Gateway
- Conception de l'intégration entre StoreFront et NetScaler Gateway

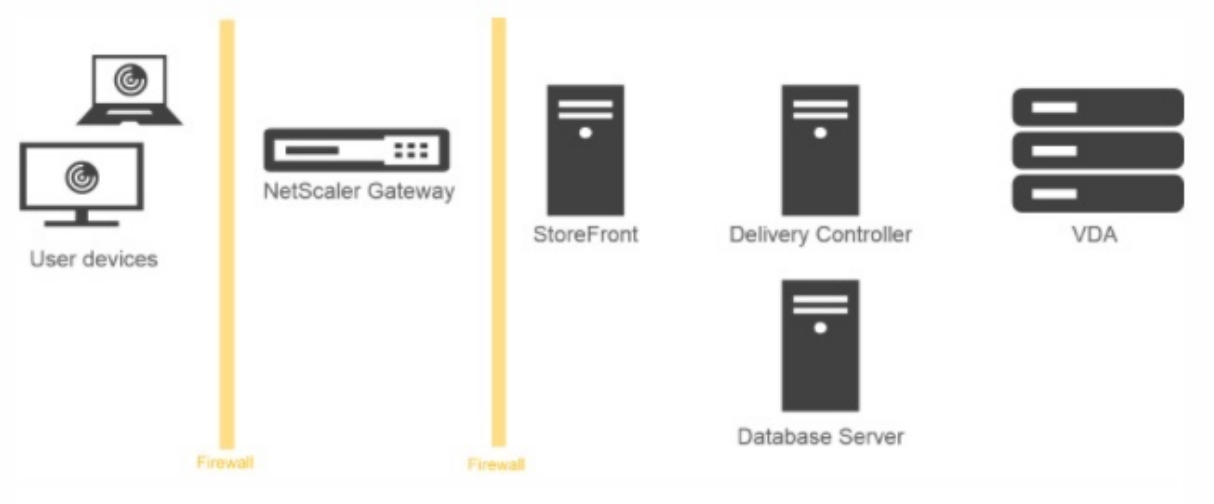
Intégrer NetScaler Gateway à Citrix Virtual Apps and Desktops

January 26, 2024

Les serveurs StoreFront sont déployés et configurés pour gérer l'accès aux données et ressources publiées. Pour un accès distant, il est recommandé d'ajouter NetScaler Gateway devant StoreFront.

> **Remarque**
>
> Pour connaître les étapes de configuration détaillées relatives à l'intégration de Citrix Virtual Apps and Desktops à NetScaler Gateway, consultez la documentation StoreFront.

Le diagramme suivant illustre un exemple d'un déploiement de Citrix simplifié qui inclut NetScaler Gateway. NetScaler Gateway communique avec StoreFront pour protéger les applications et les données fournies par Citrix Virtual Apps and Desktops. Les machines utilisateur exécutent l'application Citrix Workspace pour créer une connexion sécurisée et accéder à leurs applications, postes de travail et fichiers.



Les utilisateurs se connectent et s'authentifient à l'aide de NetScaler Gateway. NetScaler Gateway est déployé et sécurisé dans la DMZ. L'authentification à deux facteurs est configurée. En fonction des informations d'identification qu'ils saisissent, les utilisateurs recevront les ressources et applications auxquelles ils sont autorisés à accéder. Les applications et les données sont sur des serveurs appropriés (non illustrés dans le diagramme). Séparez les serveurs utilisés pour des applications et des données sensibles.

Déploiement avec Citrix Endpoint Management, Citrix Virtual Apps and Desktop

March 27, 2024

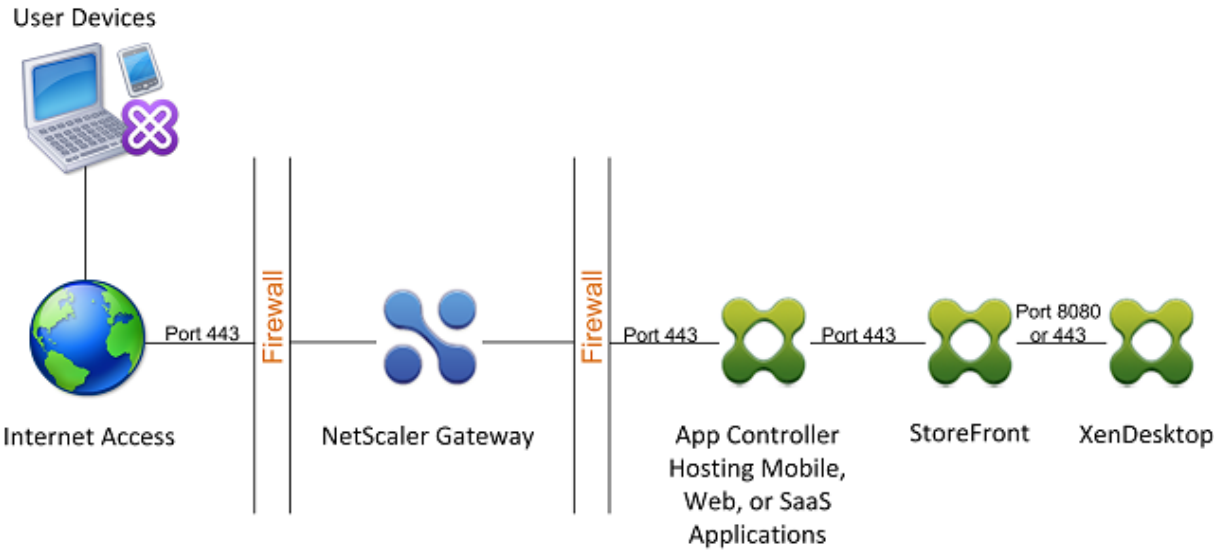
Vous pouvez permettre aux utilisateurs de se connecter à des applications Windows, Web, SaaS et mobiles et à des bureaux virtuels hébergés sur votre réseau. Vous pouvez fournir un accès à vos applications et bureaux à des utilisateurs distants et internes à l'aide de NetScaler Gateway, Citrix Endpoint Management et Citrix Virtual Apps and Desktops. NetScaler Gateway authentifie les utilisateurs puis leur permet d'accéder à leurs applications à l'aide de l'application Citrix Workspace ou de Secure Hub.

Les utilisateurs se connectent à leurs applications Windows publiées dans Citrix Virtual Apps et aux bureaux virtuels publiés dans Citrix Virtual Desktops à l'aide de l'application Citrix Workspace et de StoreFront.

Citrix Endpoint Management contient Citrix Endpoint Management, qui permet aux utilisateurs de se connecter à des applications Web, SaaS et MDX. Endpoint Management vous permet de gérer des applications Web, SaaS et MDX pour l'authentification unique (SSO), ainsi que des documents ShareFile. Vous installez Endpoint Management sur le réseau interne. Les utilisateurs distants se connectent à Endpoint Management via NetScaler Gateway pour accéder à leurs applications et aux données ShareFile. Les utilisateurs distants peuvent se connecter au client Citrix Secure Access, à l'application Citrix Workspace ou à Secure Hub pour accéder aux applications et à ShareFile. Les utilisateurs qui se trouvent dans le réseau interne peuvent se connecter directement à Endpoint Management à l'aide de l'application Citrix Workspace. La figure suivante montre NetScaler Gateway déployé avec Endpoint Management et StoreFront.

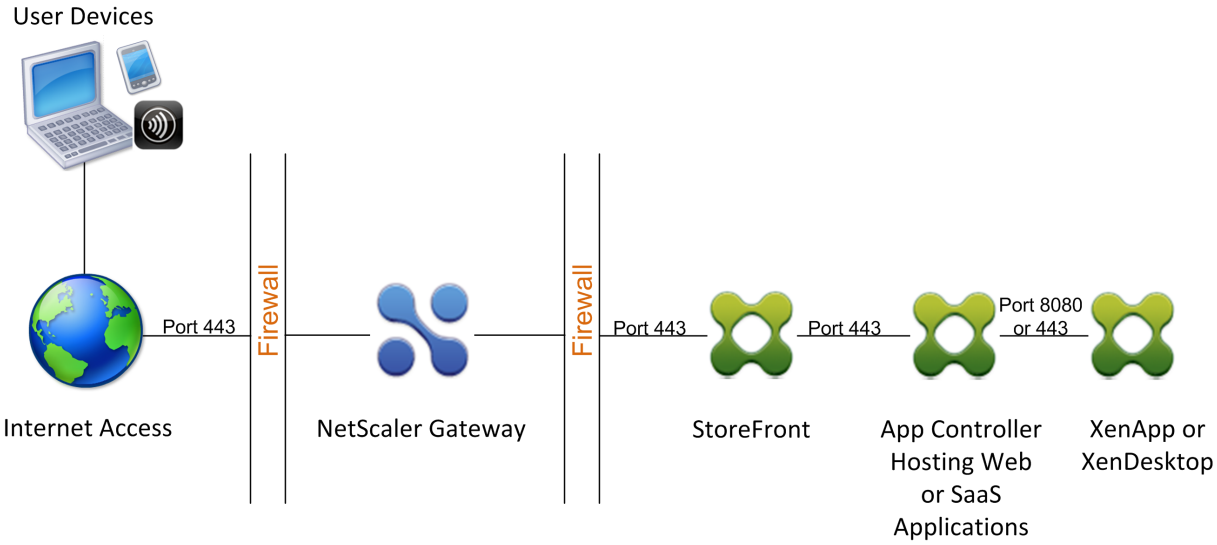
Si votre déploiement donne accès aux applications MDX depuis Endpoint Management et aux applications Windows depuis StoreFront, vous déployez Endpoint Management devant StoreFront, comme indiqué dans l'illustration suivante :

Figure 1. Déploiement de NetScaler Gateway avec Endpoint Management devant StoreFront



Si votre déploiement ne permet pas d'accéder aux applications MDX, StoreFront se trouve devant Endpoint Management, comme illustré dans l'illustration suivante :

Figure 2. Déploiement de NetScaler Gateway avec StoreFront dans Front of Endpoint Management



À chaque déploiement, StoreFront et Endpoint Management doivent résider dans le réseau interne et NetScaler Gateway doit se trouver dans la zone démilitarisée. Pour plus d'informations sur le déploiement d'Endpoint Management, consultez la rubrique Installation d'Endpoint Management. Pour plus d'informations sur le déploiement de StoreFront, consultez la rubrique StoreFront.

Configuration des paramètres de votre environnement Citrix Endpoint Management

March 27, 2024

L'assistant NetScaler pour Citrix Endpoint Management vous guide tout au long de la configuration des fonctionnalités de NetScaler pour votre déploiement Citrix Endpoint Management. Vous pouvez utiliser l'assistant pour effectuer les opérations suivantes :

- **Configurez un Micro VPN.** Dans ce scénario, les utilisateurs distants peuvent accéder aux applications et aux bureaux du réseau interne.
  - Pour le mode MAM de Citrix Endpoint Management uniquement, vous devez utiliser NetScaler Gateway pour l'authentification.
  - Pour les déploiements MDM, Citrix recommande NetScaler Gateway pour les appareils VPN mobiles.
  - Pour les déploiements ENT, si un utilisateur choisit de ne pas participer à l'inscription MDM, l'appareil fonctionne en mode MAM traditionnel et s'inscrit à l'aide du FQDN NetScaler Gateway.
- **Configurez l'authentification basée sur les certificats.** La configuration par défaut de Citrix Endpoint Management est l'authentification par nom d'utilisateur et mot de passe. Pour ajouter une autre couche de sécurité pour l'inscription et l'accès à l'environnement Citrix Endpoint Management, envisagez d'utiliser l'authentification basée sur certificat.
- **Équilibrez la charge des serveurs Citrix Endpoint Management.** L'équilibrage de charge NetScaler est requis pour tous les modes d'appareils Citrix Endpoint Management si vous possédez plusieurs serveurs Citrix Endpoint Management ou si Citrix Endpoint Management se trouve dans votre zone démilitarisée ou votre réseau interne (et donc le trafic circule des appareils vers NetScaler vers Citrix Endpoint Management). Dans ce scénario, l'appliance NetScaler se trouve dans la zone démilitarisée entre la machine utilisateur et les serveurs Citrix Endpoint Management afin d'équilibrer la charge des données chiffrées envoyées depuis les appareils mobiles vers les serveurs Citrix Endpoint Management.
- **Équilibrez la charge des serveurs Microsoft Exchange avec filtrage des e-mails** Dans ce scénario, l'appliance NetScaler se trouve entre la machine utilisateur et le Citrix Endpoint Management NetScaler Connector (XNC), et entre la machine utilisateur et les serveurs Microsoft Exchange CAS. Toutes les demandes provenant des machines utilisateur sont transmises à l'appliance NetScaler Gateway, qui communique ensuite avec le XNC pour récupérer des informations sur l'appareil. En fonction de la réponse du XNC, l'appliance NetScaler transmet la

demande d'un appareil sur liste blanche au serveur du réseau interne ou interrompt la connexion depuis un appareil sur liste noire.

- **Équilibrez la charge des connecteurs ShareFile StorageZones en fonction du type de contenu demandé.** Ce scénario vous invite à fournir des informations de base sur votre environnement StorageZones Controller, puis génère une configuration qui effectue les opérations suivantes :
  - Équilibre la charge du trafic entre les StorageZones Controller.
  - Fournit l'authentification des utilisateurs pour StorageZones Connector.
  - Valide les signatures URI pour les chargements et téléchargements ShareFile.
  - Met fin aux connexions SSL sur l'appliance NetScaler.

Pour plus d'informations sur la configuration de ShareFile, voir Configurer NetScaler pour StorageZonesController.

> **Important :**
>
> Avant d'utiliser l'assistant Citrix Endpoint Management, veillez à consulter les articles suivants sur le déploiement de Citrix Endpoint Management pour obtenir des informations et des recommandations sur la conception et le déploiement :
>
> Intégration de Citrix Endpoint Management
>
> Intégration avec NetScaler Gateway et NetScaler
>
> Considérations SSO et proxy pour les applications MDX
>
> Authentification
>
> Vous ne pouvez utiliser l'assistant NetScaler pour Citrix Endpoint Management qu'une seule fois. Si vous souhaitez disposer de plusieurs instances Citrix Endpoint Management, par exemple pour les environnements de test, de développement et de production, vous devez configurer NetScaler manuellement pour les environnements supplémentaires. Les articles de support suivants répertorient les commandes exécutées par l'assistant et fournissent des instructions pour les exécuter afin de créer une instance NetScaler :
>
> Commandes générées par Citrix Endpoint Management Wizard sur NetScaler - SSL Bridge
>
> Commandes générées par Citrix Endpoint Management Wizard sur NetScaler - SSL Offload

Exigences de licence pour les fonctionnalités de NetScaler

Vous devez installer des licences pour activer les fonctionnalités NetScaler suivantes :

- L'équilibrage de charge MDM de Citrix Endpoint Management nécessite une licence standard NetScaler.

- L'équilibrage de charge de ShareFile avec StorageZones nécessite une licence standard NetScaler.
- L'équilibrage de charge Exchange nécessite une licence NetScaler ou une licence Advanced avec l'ajout d'une licence de mise en cache intégrée.

Assistant NetScaler pour Citrix Endpoint Management

Cette section fournit un exemple d'utilisation de l'assistant NetScaler pour Citrix Endpoint Management pour :

- Configuration de l'accès micro VPN pour les connexions d'utilisateurs distants aux ressources gérées par Citrix Endpoint Management sur votre réseau interne
- Configurez l'authentification basée sur les certificats. Pour plus d'informations sur l'obtention et l'installation d'un certificat SSL public, consultez Installation et gestion des certificats.
- Configurez l'équilibrage de charge pour les serveurs Citrix Endpoint Management.

Pour utiliser l'assistant, procédez comme suit :

1. Dans l'interface graphique NetScaler, cliquez sur l'onglet **Configuration**, puis sur **XenMobile** dans la section **Intégrer aux produits Citrix**.
2. Sélectionnez votre version de Citrix Endpoint Management, puis cliquez sur **Démarrer**.
3. Sélectionnez les fonctionnalités que vous souhaitez configurer. Vous ne pouvez utiliser cet assistant qu'une seule fois.Vous devez donc effectuer la configuration suivante manuellement. Ces instructions supposent que vous sélectionnez les paramètres suivants : **Accès via NetScaler Gateway** (pour Citrix Endpoint Management exécuté en mode ENT ou MAM) et **Load Balance Citrix Endpoint Management Servers**.
4. Sur la page de **configuration de NetScaler Gateway**, entrez des valeurs pour l'adresse IP, le port et le nom du serveur virtuel NetScaler Gateway destinés à l'extérieur.
5. Sur la page **Certificat de serveur pour NetScaler Gateway**, dans **Fichier de certificat**, choisissez le fichier de certificat dans **Local** ou **Appliance**.

   - Local : sélectionnez le certificat sur votre ordinateur
   - Appliance : sélectionnez le certificat sur NetScaler Gateway (appliance).

6. Sur la page **Authentification**, dans **Méthode d'authentification principale**, sélectionnez **Certificat client**, puis entrez un nom pour le profil du certificat.

   Les étapes suivantes supposent que vous disposez déjà d'une stratégie de certificat.

   Si vous devez créer une stratégie de certification, cliquez sur Créer une stratégie de certification. Sur l'écran Citrix Endpoint Management Certificate, choisissez un certificat de serveur existant

ou installez un nouveau certificat. Si vous utilisez plusieurs serveurs Citrix Endpoint Management, vous ajoutez un certificat pour chacun d'entre eux. Pour l'attribut Nom de connexion au serveur, spécifiez UserPrincipalName ou SamAccountName, selon vos besoins.

7. Cliquez sur **Deux facteurs** pour activer l'authentification à deux facteurs, l'authentification par certificat client suivie par LDAP ou RADIUS comme type d'authentification secondaire.
8. Dans **Méthode d'authentification secondaire**, sélectionnez la méthode d'authentification secondaire.

    - Avec le certificat client comme type d'authentification principal, vous avez la possibilité de configurer LDPA (ou RADIUS) en tant que type d'authentification secondaire.

      Pour utiliser uniquement l'authentification par certificat client, laissez la **deuxième méthode d'authentification** sur **Aucune**, puis cliquez sur **Continuer**.

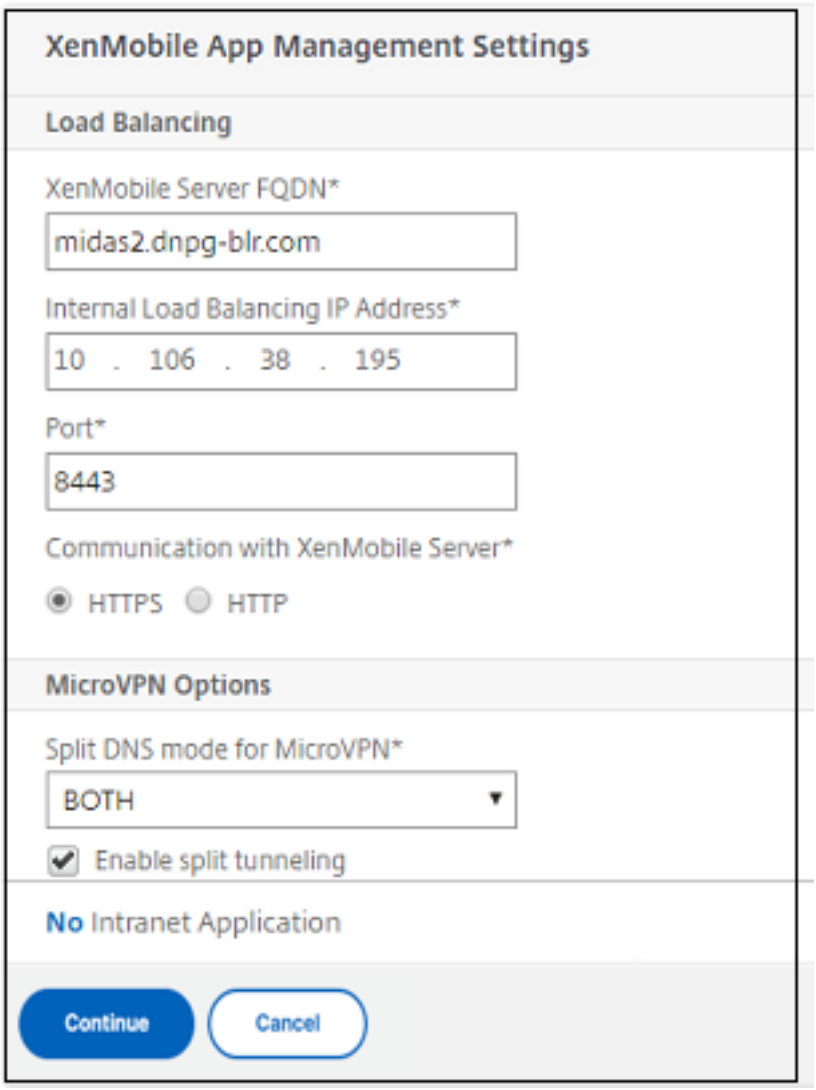
      Pour utiliser l'authentification LDAP (certificat client+domaine), remplacez la **méthode d'authentification secondaire** par **LDAP** et configurez les paramètres du serveur d'authentification.

9. Configurez les **paramètres de gestion des applications Citrix Endpoint Management**.

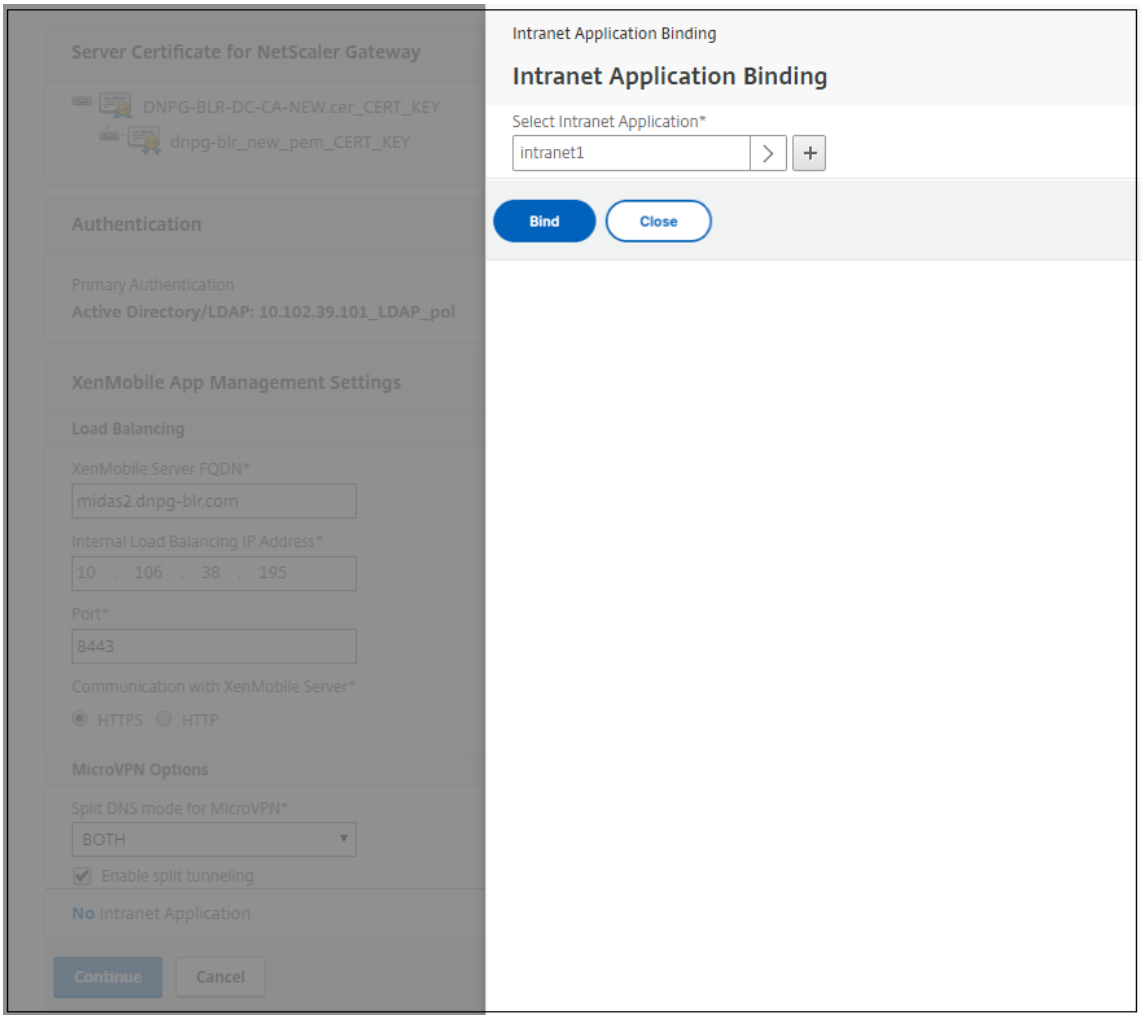
    - Entrez le nom de **domaine complet de Citrix Endpoint Management**.Il s'agit du nom de domaine complet d'équilibrage de charge pour MAM.
    - Entrez une **adresse IP d'équilibrage de charge interne**MAM uniquement pour le serveur virtuel qui équilibre la charge des serveurs Citrix Endpoint Management. NetScaler Gateway communique avec Citrix Endpoint Management via cette adresse IP virtuelle d'équilibrage de charge MAM.
    - Il s'agit d'un déploiement de déchargement SSL. Par conséquent, sélectionnez**HTTP**dans**Communicat**
      avec Citrix Endpoint Management Server.
    - Le champ**Split DNS mode for MicroVPN**est automatiquement défini sur LES**DEUX**.

    Si votre déploiement nécessite un split tunneling, sélectionnez **Activer le split tunneling**. Configurez ensuite la liaison d'application intranet si vous activez le split tunneling.

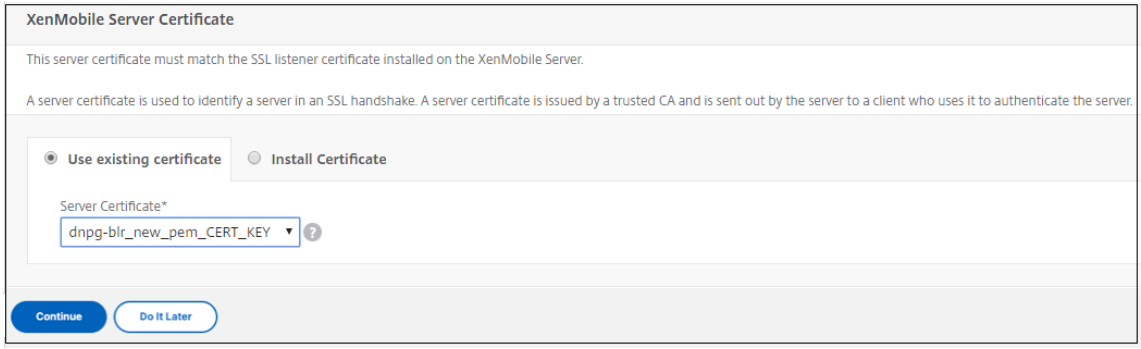
    Par défaut, l'accès Secure Web est canalisé vers le réseau interne, ce qui signifie que Secure Web utilise un tunnel VPN par application vers le réseau interne pour tous les accès au réseau et que l'appliance NetScaler utilise les paramètres du tunnel partagé.



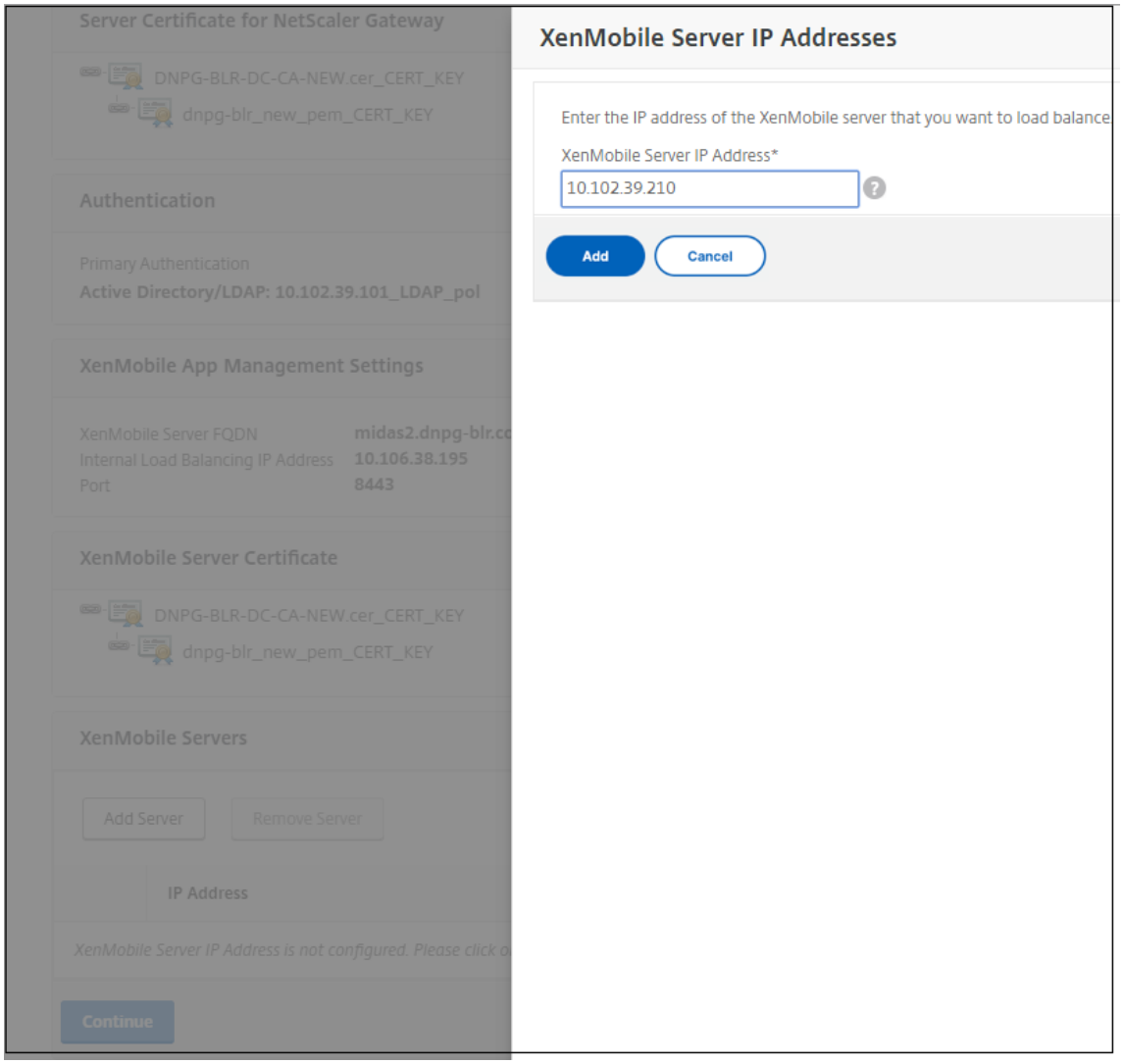
10. Pour configurer les règles d'interception pour les connexions utilisateur sur NetScaler Gateway, vous devez configurer **Intranet**Application Binding. Cliquez sur **+** pour ajouter une liaison.



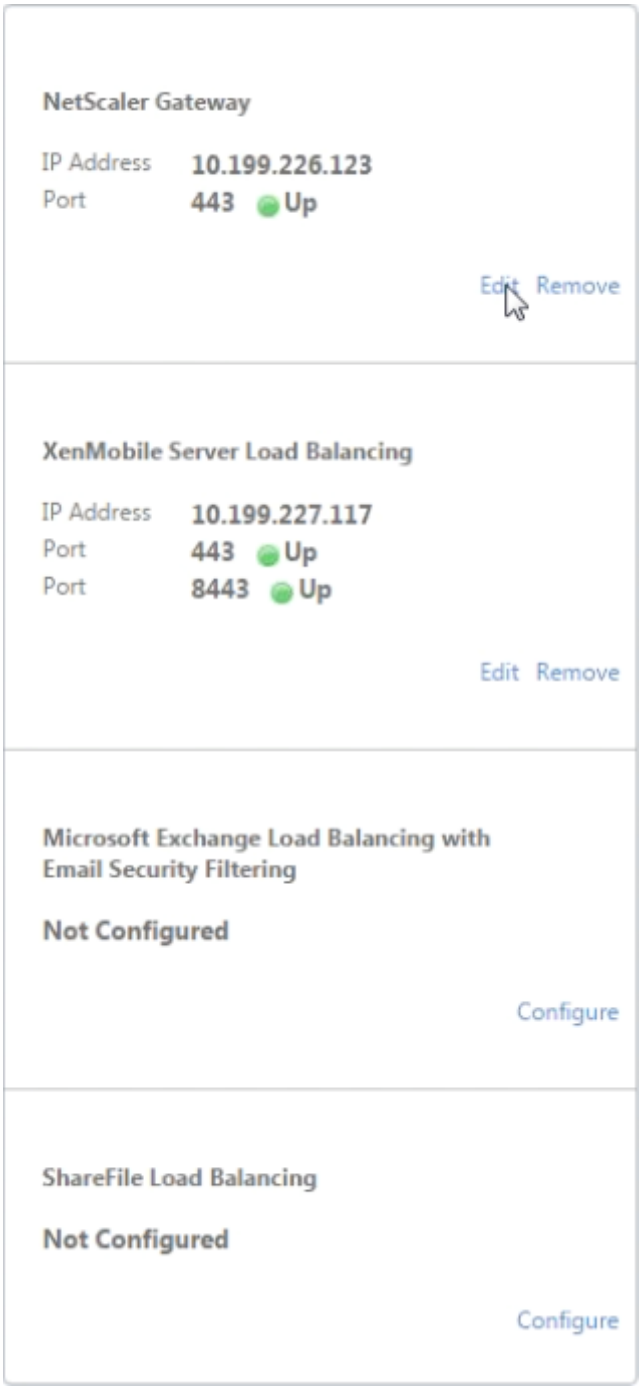
11. Renseignez les paramètres d'autorisation d'accès au réseau, puis cliquez sur **Créer**.
12. Ajoutez le certificat Citrix Endpoint Management. Il est utilisé pour le serveur virtuel d'équilibrage de charge MAM.



13. Sous **Citrix Endpoint Management Servers**, cliquez sur **Ajouter un serveur** pour ajouter l'**adresse IP Citrix Endpoint Management à lier à l'adresse**IP virtuelle d'équilibrage de charge.



Sur le tableau de bord NetScaler, vérifiez que l'équilibrage de charge NetScaler Gateway et Citrix Endpoint Management est configuré.



Si vous utilisez les attributs SamAccount dans les certificats utilisateur comme alternative au nom d'utilisateur principal (UPN), configurez le profil du certificat comme décrit dans Configuration manuelle de NetScaler Gateway pour l'authentification par certificat client.

Configuration des serveurs d'équilibrage de charge pour Citrix Endpoint Management ou Citrix XenMobile Server

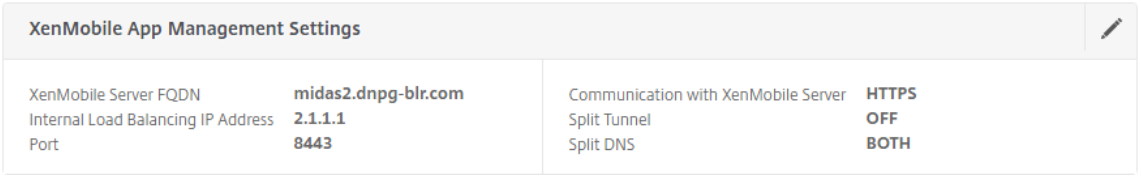
January 26, 2024

Après avoir utilisé l'assistant **NetScaler pour Citrix Endpoint Management** pour la configuration initiale, utilisez l'utilitaire de configuration NetScaler Gateway pour configurer l'équilibrage de charge, comme décrit dans cette section. Pour Citrix Endpoint Management, utilisez le déchargement SSL. Pour Citrix Endpoint Management Server, veillez à consulter les recommandations relatives aux modes d'équilibrage de charge dans la section « Résumé du déploiement » de la section Intégration à NetScaler Gateway et NetScaler.

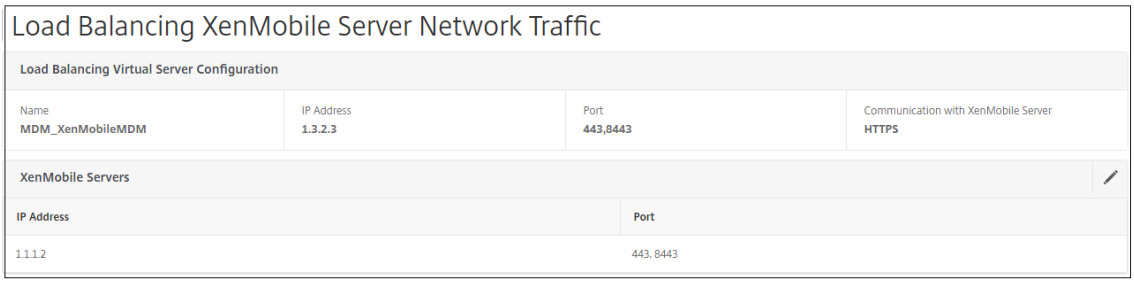
Pour utiliser le mode pont SSL pour les VIP de NetScaler

Utilisez le mode Pont SSL si Citrix Endpoint Management se trouve dans la zone démilitarisée. Lorsque vous équilibrez la charge de Citrix Endpoint Management avec les VIP de NetScaler en mode SSL Bridge, le trafic Internet circule directement vers le serveur Citrix Endpoint Management, où les connexions s'arrêtent. Le mode Pont SSL est le mode le plus simple à configurer et à résoudre.

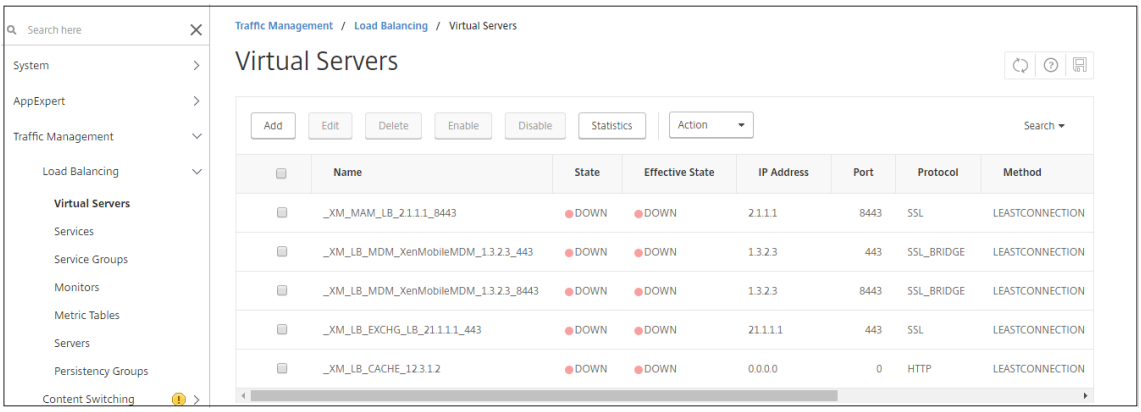
1. Avant de configurer le mode Pont SSL, accédez aux **paramètres de gestion des applications Citrix Endpoint Management** et vérifiez que **la communication avec Citrix Endpoint Management Server** est **HTTPS**.



2. Une fois que vous êtes connecté à l'utilitaire de configuration, sous l'onglet **Accueil**, dans **MDM Server LB**, cliquez sur **Configurer**.
3. Sous **Serveur virtuel LB pour la gestion des périphériques**, dans **Nom**, tapez un nom pour le serveur.
4. Dans **Adresse IP**, tapez l'adresse IP du serveur virtuel, puis cliquez sur **Continuer**.
5. Sur la page **Équilibrage de charge des serveurs MDM Citrix Endpoint Management**, répétez les étapes 3 et 4, puis cliquez sur **Créer**.
6. Vérifiez que les paramètres sont corrects, puis cliquez sur **Terminé**.



7. Pour vérifier la configuration de l'équilibrage de charge, accédez à **Gestion du trafic > Serveurs virtuels**.



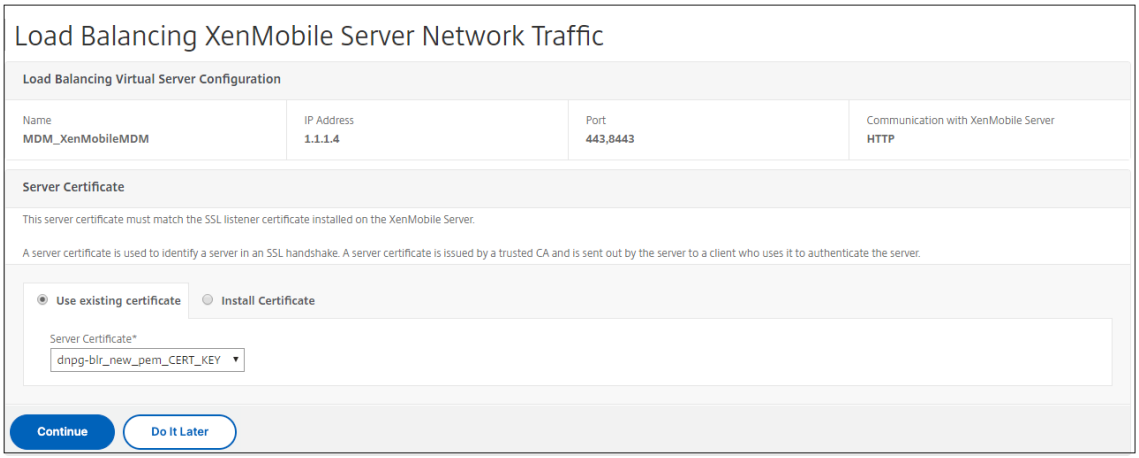
Pour utiliser le mode de déchargement SSL pour les VIP NetScaler

Utilisez le déchargement SSL pour Citrix Endpoint Management. Utilisez également le déchargement SSL, si nécessaire pour respecter les normes de sécurité, lorsque Citrix Endpoint Management sur site se trouve sur le réseau interne. Lorsque vous équilibrez la charge de Citrix Endpoint Management avec les VIP de NetScaler en mode SSL Offload, le trafic Internet circule directement vers l'appliance NetScaler, où les connexions s'arrêtent. NetScaler Gateway établit ensuite de nouvelles sessions entre l'appliance et Citrix Endpoint Management. Le mode de déchargement SSL est plus complexe lors de la configuration et du dépannage.

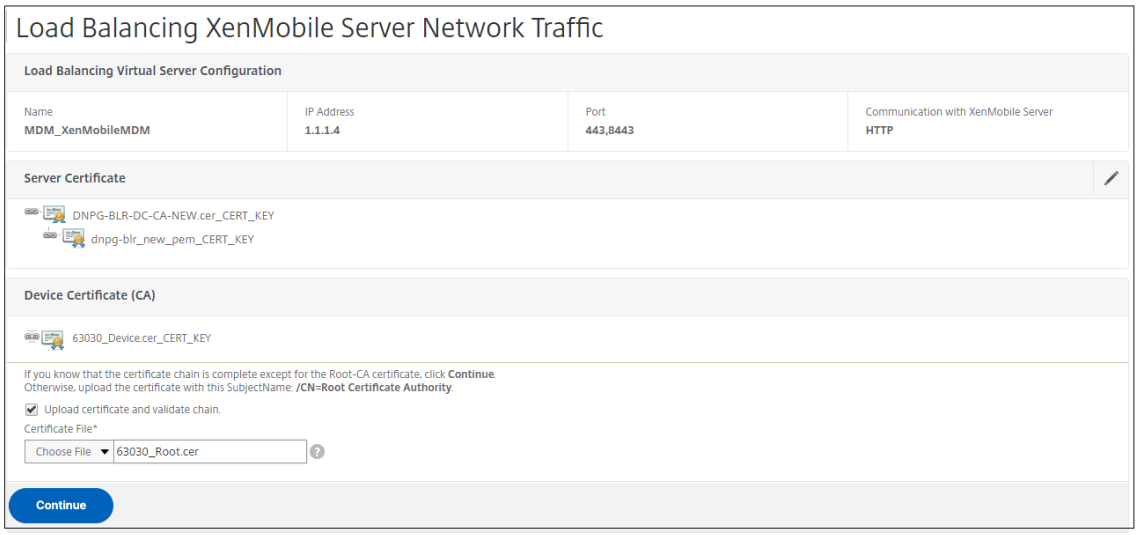
1. Avant de configurer le mode de déchargement SSL, accédez aux **paramètres de gestion des applications Citrix Endpoint Management** et vérifiez que **la communication avec Citrix Endpoint Management Server** est **HTTP**.

2. Ouvrez une session sur l'utilitaire de configuration. Dans l'onglet **Accueil**, dans **MDM Server LB**, cliquez sur **Configurer**.

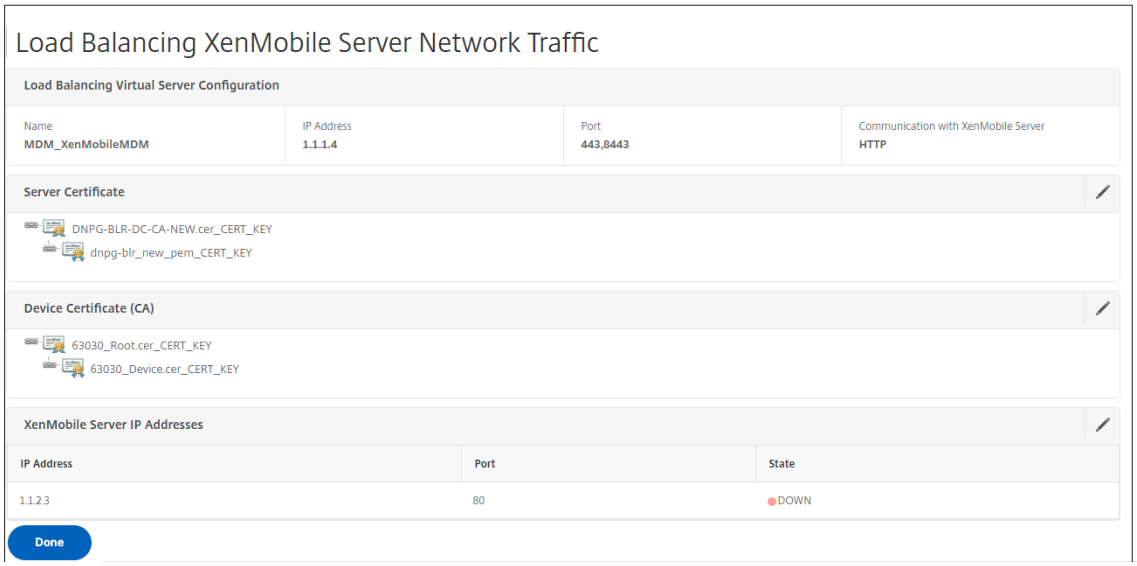
3. Sous **Serveur virtuel LB pour la gestion des périphériques**, dans **Nom**, tapez un nom pour le serveur.
4. Dans **Adresse IP**, tapez l'adresse IP du serveur virtuel, puis cliquez sur **Continuer**.
5. Sur la page **Équilibrage de charge des serveurs MDM Citrix Endpoint Management**, répétez les étapes 3 et 4, puis cliquez sur **Créer**.
6. Vérifiez les paramètres, puis cliquez sur **Terminé**.
7. Lorsque vous êtes invité à ajouter un certificat de serveur, choisissez le certificat de serveur et cliquez sur **Continuer**.



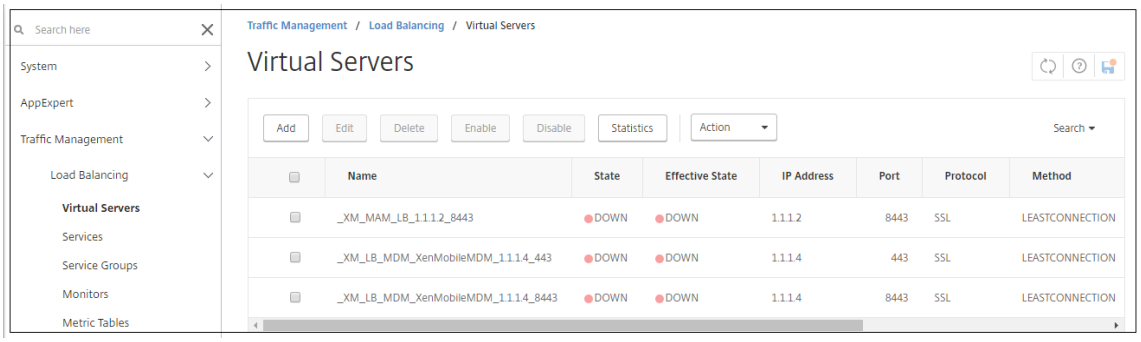
8. Spécifiez le certificat d'autorité de certification et cliquez sur **Continuer**.



9. Conservez la même adresse IP Citrix Endpoint Management. Cliquez sur **Terminé**.



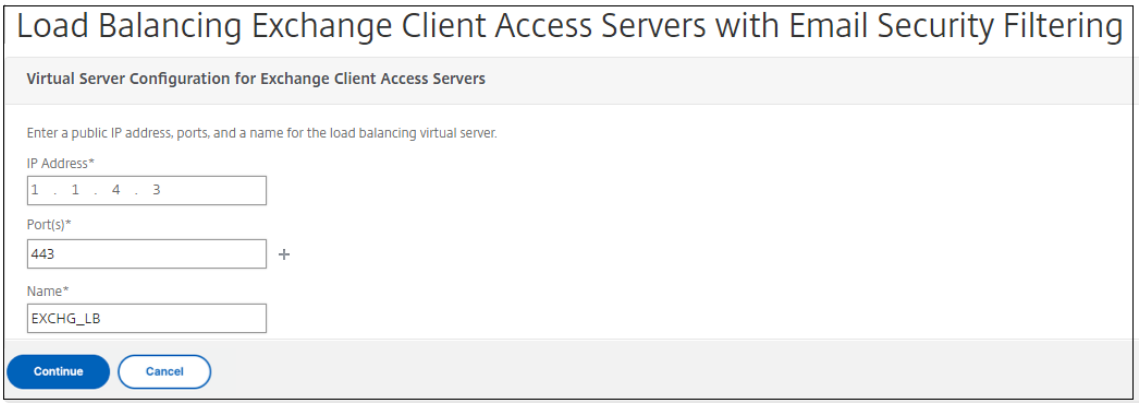
10. Pour vérifier la configuration de l'équilibrage de charge, accédez à **Gestion du trafic > Serveurs virtuels**.



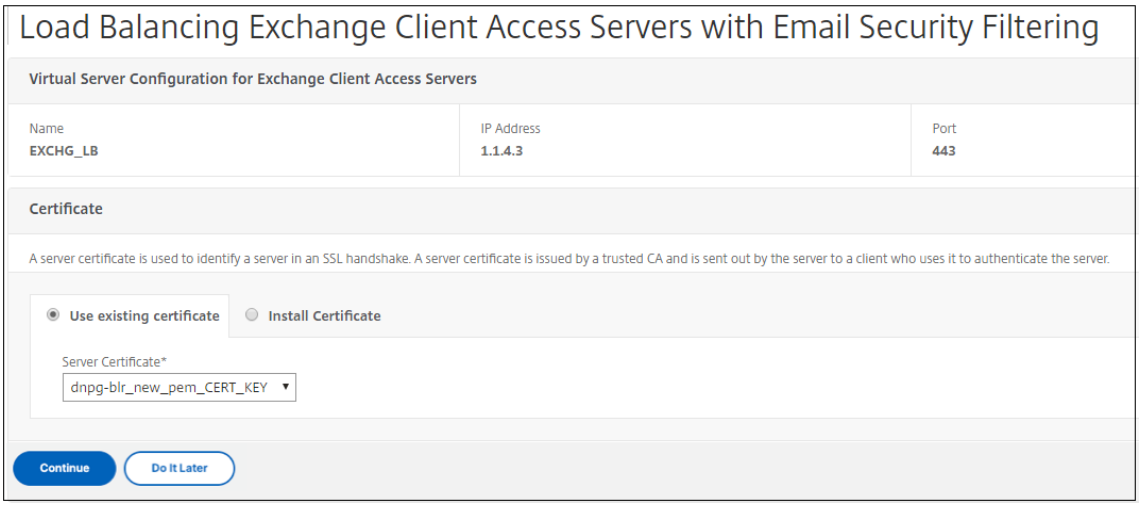
Configurer les serveurs d'équilibrage de charge pour Microsoft Exchange avec le filtrage de sécurité des e-mails

January 26, 2024

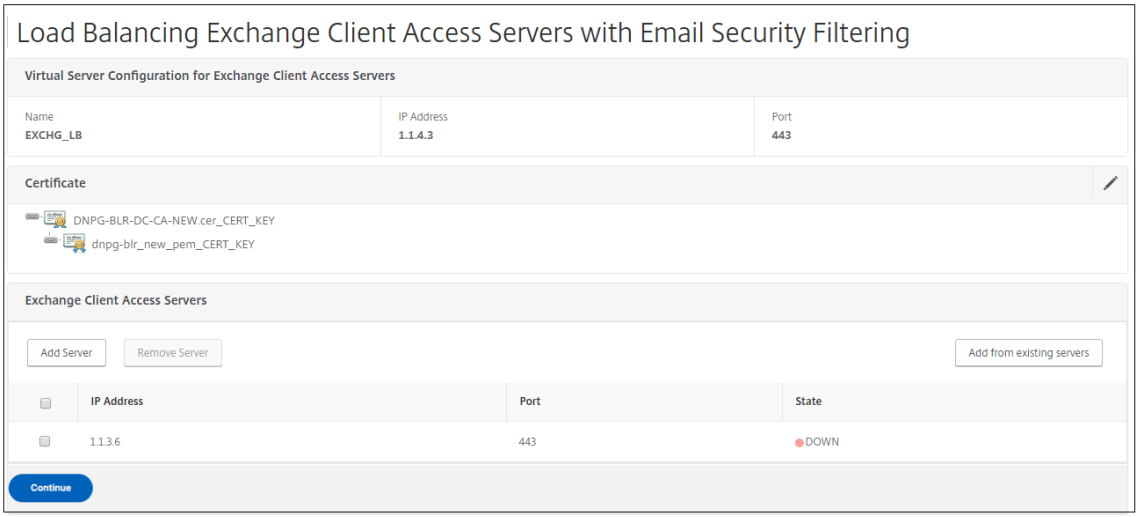
1. Dans l'onglet **Accueil**, dans **MDM Server LB**, cliquez sur **Configurer**.
2. Sous **Serveur virtuel LB pour Exchange CAS**, dans **Nom**, tapez un nom pour le serveur.
3. Dans **Adresse IP**, tapez l'adresse IP du serveur virtuel.
4. Dans **Port**, tapez le numéro de port. Pour ajouter d'autres ports, cliquez sur le signe plus (**+**), puis saisissez le numéro de port.
5. Cliquez sur **Continuer**.



6. Sous **Certificats**, choisissez un certificat existant ou installez-en un sur votre ordinateur (**local**) ou sur l'appliance NetScaler (**Appliance**).
7. Cliquez sur **Continuer**.



8. Sous **Instances du service Exchange Citrix Analytics**, tapez le nom, l'adresse IP et le numéro de port du serveur virtuel. Cliquez ensuite sur **Ajouter** et **continuer**.



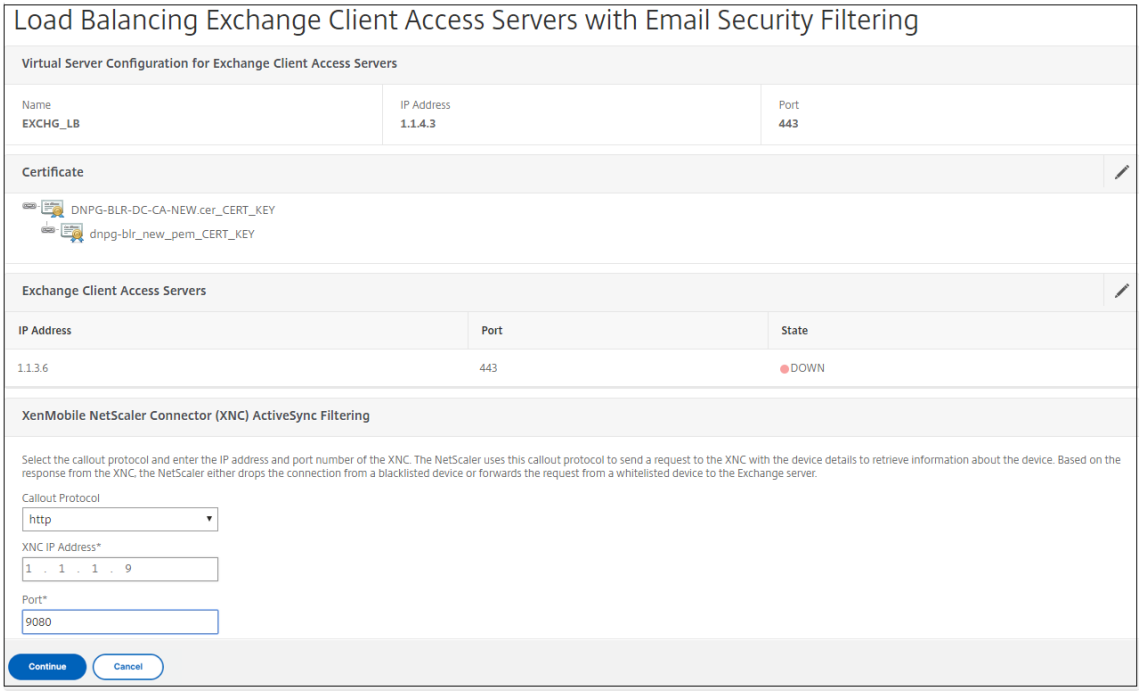
Lorsque vous cliquez sur **Terminé**, les champs de configuration du filtrage ActiveSync de Citrix Endpoint Management NetScaler Connector (XNC) apparaissent.

Configurer le filtrage ActiveSync Citrix Endpoint Management NetScaler Connector (XNC)

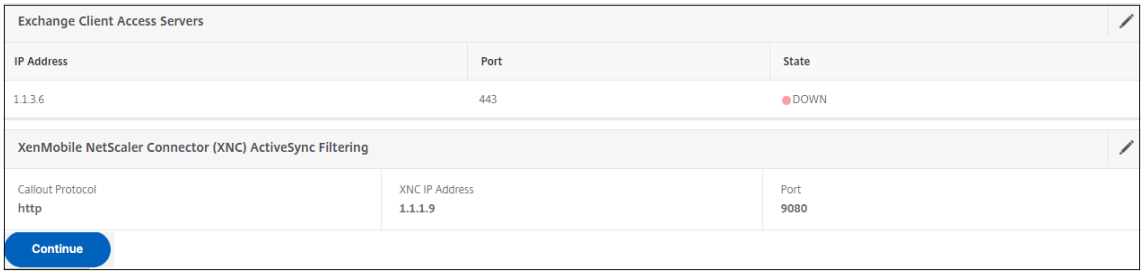
January 26, 2024

Le connecteur Citrix Endpoint Management NetScaler (XNC) fournit à NetScaler un service d'autorisation au niveau de l'appareil pour les clients ActiveSync qui agit comme un proxy inverse pour le protocole Exchange ActiveSync. La combinaison de stratégies définies dans Citrix Endpoint Management et de règles définies localement par le XNC contrôlent l'autorisation.

1. Sous **Citrix Endpoint Management NetScaler Connector (XNC) ActiveSync Filtering**, pour **Callout Protocol**, sélectionnez **http** ou **https**.
2. Dans **Adresse IP XNC, tapez l'adresse**IP du connecteur Citrix Endpoint Management NetScaler.
3. Dans **Port**, tapez **9080** pour le trafic réseau HTTP ou **9443** pour le trafic réseau HTTPS, puis cliquez sur **Continuer**.



Votre configuration s'affiche.



Autoriser l'accès à partir d'appareils mobiles avec Citrix Mobile Productivity Apps

March 27, 2024

L'assistant NetScaler for XenMobile configure les paramètres requis pour permettre aux utilisateurs de se connecter à partir d'appareils pris en charge via NetScaler Gateway à des applications mobiles et à des ressources du réseau interne. Les utilisateurs se connectent à l'aide de Secure Hub (anciennement Citrix Secure Hub), qui établit un tunnel Micro VPN. Lorsque les utilisateurs se connectent, un tunnel VPN s'ouvre vers NetScaler Gateway, puis est transmis à XenMobile sur le réseau interne. Les utilisateurs peuvent ensuite accéder à leurs applications Web, mobiles et SaaS à partir de XenMobile.

Pour garantir que les utilisateurs utilisent une seule licence universelle lorsqu'ils se connectent à NetScaler Gateway avec plusieurs appareils simultanément, vous pouvez activer le transfert de session sur le serveur virtuel. Pour plus de détails, consultez la section Configuration des types de connexion sur le serveur virtuel.

Si vous devez modifier votre configuration après avoir utilisé l'assistant NetScaler pour XenMobile, consultez les sections de cet article pour obtenir des conseils. Avant de modifier les paramètres, assurez-vous de bien comprendre les implications de vos modifications. Pour plus d'informations, reportez-vous aux articles XenMobile Deployment.

Configurer Secure Browse dans NetScaler Gateway

Vous pouvez modifier la Secure Browse dans le cadre des paramètres globaux ou dans le cadre d'un profil de session. Vous pouvez lier la stratégie de session aux utilisateurs, groupes ou serveurs virtuels. Lorsque vous configurez Secure Browse, vous devez également activer l'accès sans client. Toutefois, l'accès sans client ne nécessite pas l'activation de la Secure Browse. Lorsque vous configurez l'accès sans client, définissez **l'encodage d'URL d'accès sans client** sur **Effacer**.

Pour configurer Secure Browse globalement :

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans la boîte de dialogue **Paramètres globaux de NetScaler Gateway**, sous l'onglet **Sécurité**, cliquez sur **Secure Browse**, puis sur **OK**.

Pour configurer Secure Browse dans une stratégie et un profil de session :

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, effectuez l'une des opérations suivantes :
   - Si vous créez une nouvelle stratégie de session, cliquez sur **Ajouter**.
   - Si vous modifiez une politique existante, sélectionnez-en une, puis cliquez sur **Ouvrir**.
3. Dans la stratégie, créez un profil ou modifiez un profil existant. Pour ce faire, effectuez l'une des opérations suivantes :
   - À côté de **Demander un profil**, cliquez sur **Nouveau**.
   - À côté de **Demander un profil**, cliquez sur **Modifier**.
4. Dans l'onglet **Sécurité**, en regard de **Secure Browse**, cliquez sur **Override Global**, puis sélectionnez **Secure Browse**.
5. Procédez comme suit :
   - Si vous créez un nouveau profil, cliquez sur **Créer**, définissez l'expression dans la boîte de dialogue de stratégie, cliquez sur **Créer,** puis cliquez sur **Fermer**.
   - Si vous modifiez un profil existant, après avoir effectué la sélection, cliquez deux fois sur **OK** .

Pour configurer les stratégies de trafic pour Secure Web en mode Secure Browse :

Suivez les étapes suivantes pour configurer des stratégies de trafic afin d'acheminer le trafic Secure Web via un serveur proxy en mode Secure Browse.

1. Dans l'utilitaire de configuration, sous l'onglet **Configuration**, développez **NetScaler Gateway > Stratégies**, puis cliquez sur **Traffic**.
2. Dans le volet droit, cliquez sur l'onglet **Profils de trafic**, puis cliquez sur **Ajouter**.
3. Dans **Nom**, saisissez un nom pour le profil, sélectionnez **TCP** comme **protocole**et laissez les autres paramètres tels quels.
4. Cliquez sur **Créer**.
5. Cliquez sur l'onglet **Profils de trafic**, puis cliquez sur **Ajouter**.

6. Dans **Nom**, saisissez un nom pour le profil, puis sélectionnez **HTTP** comme **protocole**.
   Ce profil de trafic est destiné aux protocoles HTTP et SSL. Le trafic VPN sans client est un trafic HTTP par conception, quel que soit le port de destination ou le type de service. Par conséquent, vous spécifiez à la fois le trafic SSL et le trafic HTTP en tant que **HTTP** dans le profil de trafic.
7. Dans **Proxy**, saisissez l'adresse IP du serveur proxy. Dans **Port**, saisissez le numéro de port du serveur proxy.
8. Cliquez sur **Créer**.
9. Cliquez sur l'onglet **Stratégies de trafic**, puis sur **Ajouter**.
10. Entrez le **nom** de la stratégie de trafic et, pour **Demander un profil**, sélectionnez le profil de trafic que vous avez créé à l'étape 3. Entrez l'**expression** suivante, puis cliquez sur **Créer** :

    ```
    1 REQ.HTTP.HEADER HOST contains ActiveSyncServer || REQ.HTTP.HEADER
        User-Agent CONTAINS WorxMail || REQ.HTTP.HEADER User-Agent
        CONTAINS com.zenprise || REQ.HTTP.HEADER User-Agent CONTAINS
        Citrix Secure Hub || REQ.HTTP.URL CONTAINS AGServices || REQ.
        HTTP.URL CONTAINS StoreWeb
    2 <!--NeedCopy-->
    ```

    Cette règle effectue une vérification en fonction de l'en-tête de l'hôte. Pour contourner le trafic de synchronisation actif du proxy, remplacez-le **`ActiveSyncServer`** par le nom du serveur de synchronisation actif approprié.
11. Cliquez sur l'onglet **Stratégies de trafic**, puis sur **Ajouter**. Entrez le **nom** de la stratégie de trafic et, pour **Demander un profil**, sélectionnez le profil de trafic créé à l'étape 6. Entrez l'**expression** suivante, puis cliquez sur **Créer** :

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

12. Cliquez sur l'onglet **Stratégies de trafic**, puis sur **Ajouter**. Entrez le **nom** de la stratégie de trafic et, pour **Profil de demande**, sélectionnez le profil de trafic créé à l'étape 6. Entrez l'**expression** suivante, puis cliquez sur **Créer** :

(REQ.HTTP.HEADER User-Agent CONTAINS Mozilla	REQ.HTTP.HEADER User-Agent CONTAINS com.citrix.browser

13. Accédez à **NetScaler Gateway > Serveurs virtuels**, sélectionnez le serveur virtuel dans le volet droit, puis cliquez sur **Modifier**.
14. Sur la ligne **Stratégies**, cliquez sur **+**.
15. Dans le menu **Choisir une stratégie**, sélectionnez **Trafic**.

16. Cliquez sur **Continuer**.
17. Sous **Liaison de stratégie**, en face de **Sélectionner une stratégie**, cliquez sur **.
18. Sélectionnez la stratégie que vous avez créée à l'étape 10, puis cliquez sur **OK**.
19. Cliquez sur **Bind**.
20. Sous **Stratégies**, cliquez sur **Stratégie de trafic**.
21. Sous **Liaison de stratégie de trafic du serveur virtuel VPN**, cliquez sur **Ajouter une liaison**.
22. Sous **Liaison de stratégie**, en regard du menu **Sélectionner une stratégie**, cliquez sur ** pour afficher la liste des stratégies.
23. Sélectionnez la stratégie que vous avez créée à l'étape 11, puis cliquez sur **OK**.
24. Cliquez sur **Bind**.
25. Sous **Stratégies**, cliquez sur **Stratégies de trafic**.
26. Sous **Liaison de stratégie de trafic du serveur virtuel VPN**, cliquez sur **Ajouter une liaison**.
27. Sous **Liaison de stratégie**, en regard du menu **Sélectionner une stratégie**, cliquez sur ** pour afficher la liste des stratégies.
28. Sélectionnez la stratégie que vous avez créée à l'étape 12, puis cliquez sur **OK**.
29. Cliquez sur **Bind**.
30. Cliquez sur **Fermer**.
31. Cliquez sur **Terminé**.

Assurez-vous de configurer l'application Secure Web (WorxWeb) dans la console XenMobile. Accédez à **Configurer > Applications**, sélectionnez l'application Secure Web, cliquez sur **Modifier**, puis effectuez les modifications suivantes :

- Sur la page **d'informations de l'application**, modifiez le **mode VPN initial** sur **Secure Browse**.
- Sur la page **iOS**, modifiez le **mode VPN initial** sur **Secure Browse**.
- Sur la page **Android**, modifiez le **mode VPN préféré** sur **Secure Browse**.

Configuration des délais d'expiration des applications et des jetons MDX

Lorsque les utilisateurs ouvrent une session à partir d'un appareil iOS ou Android, un jeton d'application ou un jeton MDX est émis. Le jeton est similaire à la Secure Ticket Authority (STA).

Vous pouvez définir le nombre de secondes ou de minutes pendant lesquels les jetons sont actifs. Si le jeton expire, les utilisateurs ne peuvent pas accéder à la ressource demandée, telle qu'une application ou une page Web.

Les délais d'expiration des jetons sont des paramètres globaux. Lorsque vous configurez le paramètre, il s'applique à tous les utilisateurs qui se connectent à NetScaler Gateway.

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans la boîte de dialogue **Paramètres globaux de NetScaler Gateway**, sous l'onglet **Expérience client**, cliquez sur **Paramètres avancés**.
4. Dans l'onglet **Général**, dans **Délai d'expiration du jeton d'application (s)**, entrez le nombre de secondes avant l'expiration du jeton. La valeur par défaut est **de 100** secondes.
5. Dans **Délai d'expiration du jeton MDX (minutes)**, entrez le nombre de minutes avant l'expiration du jeton, puis cliquez sur **OK**. La valeur par défaut est de **10** minutes.

Désactiver Endpoint Analysis pour les appareils mobiles

Si vous configurez l'analyse des points de terminaison, vous devez configurer les expressions de stratégie afin que les analyses d'analyse des points de terminaison ne soient pas exécutées sur les appareils mobiles Android ou iOS. Les analyses d'analyse des points de terminaison ne sont pas prises en charge sur les appareils mobiles.

Si vous liez une stratégie d'analyse des points de terminaison à un serveur virtuel, vous devez créer un serveur virtuel secondaire pour les appareils mobiles. Ne liez pas les stratégies de pré-authentification ou de post-authentification au serveur virtuel de l'appareil mobile.

Lorsque vous configurez l'expression de stratégie dans une stratégie de pré-authentification, vous ajoutez la chaîne User-Agent pour exclure Android ou iOS. Lorsque les utilisateurs ouvrent une session à partir de l'un de ces appareils et que vous excluez le type d'appareil, l'analyse des points de terminaison ne s'exécute pas.

Par exemple, vous créez l'expression de stratégie suivante pour vérifier si l'agent utilisateur contient Android, si l'application virus.exe n'existe pas, et pour mettre fin au processus keylogger.exe s'il est exécuté à l'aide du profil de pré-authentification. L'expression de stratégie peut ressembler à ceci :

```
REQ.HTTP.HEADER User-Agent NOTCONTAINS Android &&
CLIENT.APPLICATION.PROCESS(keylogger.exe) contains
```

Après avoir créé la stratégie et le profil de pré-authentification, liez la stratégie au serveur virtuel. Lorsque les utilisateurs ouvrent une session à partir d'un appareil Android ou iOS, l'analyse ne s'exécute pas. Si les utilisateurs ouvrent une session à partir d'un appareil Windows, l'analyse est exécutée.

Pour plus d'informations sur la configuration des stratégies de pré-authentification, consultez Configuration des stratégies de point de terminaison.

Prise en charge des requêtes DNS en utilisant des suffixes DNS pour les appareils Android

Lorsque les utilisateurs établissent une connexion Micro VPN à partir d'un appareil Android, NetScaler Gateway envoie des paramètres DNS fractionnés à la machine utilisateur. NetScaler Gateway prend en charge les requêtes DNS fractionnées en fonction des paramètres DNS fractionnés que vous configurez. NetScaler Gateway peut également prendre en charge les requêtes DNS fractionnées en fonction des suffixes DNS que vous configurez sur l'appliance. Si les utilisateurs se connectent depuis un appareil Android, vous devez configurer les paramètres DNS sur NetScaler Gateway.

Le Split DNS fonctionne de la manière suivante :

- Si vous définissez le DNS fractionné sur **Local**, l'appareil Android envoie toutes les demandes DNS au serveur DNS local.
- Si vous définissez le DNS fractionné sur **Remote**, toutes les demandes DNS sont envoyées aux serveurs DNS configurés sur NetScaler Gateway (serveur DNS distant) pour résolution.
- Si vous définissez le DNS fractionné sur **Les deux**, l'appareil Android recherche le type de demande DNS.
  - Si le type de demande DNS n'est pas « A », il envoie le paquet de demande DNS aux serveurs DNS locaux et distants.
  - Si le type de requête DNS est « A », le plug-in Android extrait le nom de domaine complet de la requête et compare ce nom de domaine complet à la liste de suffixes DNS configurée sur l'appliance NetScaler. Si le nom de domaine complet de la demande DNS correspond, la demande DNS est envoyée au serveur DNS distant. Si le nom de domaine complet ne correspond pas, la demande DNS est envoyée aux serveurs DNS locaux.

Le tableau suivant récapitule le fonctionnement du DNS fractionné en fonction de l'enregistrement de type A et de la liste de suffixes.

Paramètre Split DNS	S'agit-il d'un enregistrement de type A ?	Est-ce que c'est dans la liste des suffixes ?	Où la demande DNS est envoyée
Stockage local	Oui ou Non	Oui ou Non	Stockage local
Distant	Oui ou Non	Oui ou Non	Distant
Les deux	Non	SO	Les deux
Les deux	Oui	Oui	Distant
Les deux	Oui	Non	Stockage local

Pour configurer un suffixe DNS, procédez comme suit :

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, sous **l'onglet Stratégies**, sélectionnez une stratégie de session, puis cliquez sur **Ouvrir**.
3. À côté de **Demander un profil**, cliquez sur **Modifier**.
4. Dans l'onglet **Configuration réseau**, cliquez sur **Avancé**.
5. À côté de **Suffixe DNS IP de l'intranet**, cliquez sur **Override Global**, saisissez le suffixe DNS, puis cliquez trois fois sur **OK**.

Pour configurer le DNS fractionné globalement sur NetScaler Gateway :

1. **Dans l'utilitaire de configuration, dans l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway**, puis cliquez sur Paramètres globaux.**
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres généraux**.
3. Dans l'onglet **Expérience client**, cliquez sur **Paramètres avancés**.
4. Sous l'onglet **Général**, dans **Split DNS**, sélectionnez **Les deux**, **Remote**ou **Local**, puis cliquez sur **OK**.

Pour configurer le DNS partagé dans une stratégie de session sur NetScaler Gateway :

1. **Dans l'utilitaire de configuration, sous l'onglet**Configuration**, dans le volet de navigation, développez**NetScaler Gateway > Policies**, puis cliquez sur Session.**
2. Dans le volet d'informations, dans l'onglet **Stratégies**, cliquez sur **Ajouter**.
3. Dans **Nom**, tapez le nom de la politique.
4. À côté de **Demander un profil**, cliquez sur **Nouveau**.
5. Dans **Nom**, saisissez le nom du profil.
6. Dans l'onglet **Expérience client**, cliquez sur **Paramètres avancés**.
7. Dans l'onglet **Général**, en regard de **Split DNS**, cliquez sur **Remplacer Global**, sélectionnez **Les deux**, **Remote**ou **Local**, puis cliquez sur **OK**.
8. Dans la boîte de dialogue **Créer une stratégie de session**, en regard de **Expressions nommées**, sélectionnez **Général**, sélectionnez **Vrai**, cliquez sur **Ajouter une expression**, cliquez sur **Créer,** puis cliquez sur **Fermer**.

Configurer l'authentification de domaine et de jeton de sécurité pour Citrix Endpoint Management

March 27, 2024

Vous pouvez configurer Citrix Endpoint Management de manière à obliger les utilisateurs à s'authentifier avec leurs informations d'identification LDAP plus un mot de passe à usage unique, à l'aide du

protocole RADIUS. Cette section décrit la configuration NetScaler Gateway requise pour ce type d'authentification à deux facteurs.

Pré-requis

Si vous n'avez pas encore exécuté l'assistant NetScaler pour Citrix Endpoint Management, consultez la section *NetScaler pour Citrix Endpoint Management Wizard* dans Configuration des paramètres de votre environnement CitrixEndpoint Management. Assurez-vous que votre configuration NetScaler inclut les éléments suivants :

- **Numéro de port LDAP** = **636** (port par défaut pour les connexions LDAP sécurisées)
- **Attribut du nom d'ouverture de session du serveur** = **SAMAccountName** ou **UserPrincipalName** selon vos besoins

Pour configurer l'authentification de domaine et de jeton de sécurité

1. Accédez à **NetScaler Gateway > Serveurs virtuels**. Sélectionnez le serveur virtuel, puis cliquez sur **Modifier**.
2. Cliquez sur **Aucun certificat d'autorité de certification.**
3. Dans **Sélectionner un certificat CA**, choisissez un certificat, cliquez sur **OK**, sur **Lier**, puis sur **Terminé**.
4. Accédez à **Stratégies > Session > Profils**de session, sélectionnez le profil et cliquez sur **Modifier**.
5. Cliquez sur l'onglet **Expérience client** .
6. Dans **Credential Index**, choisissez **SECONDAIRE**.
7. Cliquez sur **OK**.
8. Accédez à **Stratégies > Authentification > LDAP**, cliquez sur l'onglet **Stratégie LDAP**, puis sur **Modifier**.
9. Utilisez l'expression suivante pour utiliser des VIP NetScaler Gateway distincts pour Citrix Endpoint Management et Citrix Virtual Apps and Desktops.

   REQ.HTTP.HEADER User-Agent CONTAINS `CitrixReceiver`
10. Accédez à **Stratégies > Authentification > RADIUS**, puis cliquez sur l'onglet **Serveurs**.
11. Cliquez sur **Ajouter**, saisissez les détails du serveur RADIUS, puis cliquez sur **Créer**.
12. Accédez à **Stratégies**, puis cliquez sur **Ajouter**.

13. Entrez un **nom** pour la stratégie. Dans le menu déroulant **Serveur**, sélectionnez le nom du serveur RADIUS que vous avez créé.
14. Dans **Expression**, saisissez **REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver** et cliquez sur **Create**.
15. Sélectionnez le serveur virtuel, puis cliquez sur **Modifier**.
16. Sous **Authentification principale**, cliquez sur **Stratégie LDAP**.
17. Sélectionnez la stratégie, cliquez sur **Unbind (Délier)**, puis sur **Close (Fermer**).
18. Sur la ligne **Authentification**, cliquez sur **+** pour ajouter l'authentification RADIUS.
19. Sous **Choisir un type**, dans **Choisir une stratégie**, sélectionnez **RADIUS**.
20. Cliquez sur **Bind**.
21. Sélectionnez la stratégie d'authentification RADIUS que vous avez créée précédemment, puis cliquez sur **Insérer**.
22. Cliquez sur **OK**.
23. Pour ajouter LDAP en tant que stratégie d'authentification secondaire : sur la ligne **Authentification**, cliquez sur **+**.
24. Dans **Choose Policy**, choisissez **LDAP**.
25. Dans **Choisir le type**, choisissez **Secondaire**.
26. Dans **Sélectionner une stratégie**, choisissez la stratégie LDAP.
27. Sélectionnez la stratégie, puis cliquez sur **OK**.
28. Cliquez sur **Bind**.
29. Cliquez sur **Terminé**.
30. Vérifiez que les stratégies que vous avez créées ont la priorité la plus élevée. Cela garantit qu'ils ont la priorité la plus élevée, même si d'autres stratégies sont ajoutées pour les utilisateurs non mobiles. Pour plus d'informations, consultez la section Définition des priorités pour les stratégies d'authentification

Configurer le certificat client ou le certificat client et l'authentification du domaine

March 27, 2024

Vous pouvez utiliser l'assistant NetScaler pour Citrix Endpoint Management pour effectuer la configuration requise pour Citrix Endpoint Management lorsque vous utilisez l'authentification par certificat NetScaler uniquement ou l'authentification par certificat plus domaine. Vous ne pouvez exécuter l'assistant NetScaler pour Citrix Endpoint Management qu'une seule fois. Pour plus d'informations sur l'utilisation de l'Assistant, consultez Configuration des paramètres de votre environnement Citrix Endpoint Management.

Si vous avez déjà utilisé l'Assistant, suivez les instructions de cet article pour la configuration supplémentaire requise pour l'authentification par certificat client ou pour l'authentification par certificat client plus domaine.

Pour vous assurer que l'utilisateur d'un appareil en mode MAM uniquement ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil, consultez « Liste de révocation des certificats NetScaler (CRL) » plus loin dans cet article.

Configurer NetScaler Gateway pour l'authentification par certificat client à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel de type **SSL**et, dans la section **Paramètres SSL**, définissez **Activer la réutilisation de session surDÉSACTIVÉ**.
3. Accédez à **NetScaler Gateway > Serveurs virtuels**.
4. Sélectionnez le serveur virtuel de type **SSL**, puis cliquez sur **Modifier**.
5. Dans la section **Paramètres SSL**, cliquez sur l'icône de modification.
6. Sélectionnez **Authentification du client** et dans **Certificat client**, sélectionnez **Obligatoire**.
7. Créez une stratégie de certificat d'authentification afin que Citrix Endpoint Management puisse extraire le **nom d'utilisateur principal** ou le **SAMAccount** du certificat client fourni par Secure Hub à NetScaler Gateway.
8. Accédez à **NetScaler Gateway > Stratégies > Authentification > CERT**.
9. Cliquez sur l'onglet **Profils**, puis sur **Ajouter**.
10. Définissez les paramètres suivants pour le profil de certificat :

    Type d'authentification : **CERT**

    Deux facteurs : **OFF** (pour l'authentification par certificat uniquement)

    Champ Nom d'utilisateur : Objet : **CN**

    Champ Nom du groupe : **SubjectAltName :PrincipalName**

11. Liez uniquement la stratégie d'authentification par certificat en tant qu'**authentification principale** sur le serveur virtuel NetScaler Gateway.
12. Liez le certificat Root CA pour valider la fiabilité du certificat client présenté à NetScaler Gateway.

Configurer NetScaler Gateway pour le certificat client et l'authentification de domaine à l'aide de l'interface graphique

1. Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs virtuels**.
2. Sélectionnez le serveur virtuel de type **SSL**et, dans la section **Paramètres SSL**, définissez **Activer la réutilisation de session surDÉSACTIVÉ**.
3. Accédez à **NetScaler Gateway > Stratégies > Authentification > Cert**.
4. Cliquez sur l'onglet **Profils**, puis sur **Ajouter**.
5. Entrez le **nom** du profil, définissez **Deux facteurssur ON**, puis dans le**champ Nom d'utilisateur**, sélectionnez**SubjectAltNamePrincipalName**.
6. Cliquez sur l'onglet **Stratégies**, puis sur **Ajouter**.
7. Entrez le **nom** de la stratégie, dans **Serveur**, sélectionnez le profil de certificat, définissez l'**expression** et cliquez sur **Créer**.
8. Accédez à **Virtual Servers**, sélectionnez le serveur virtuel de type **SSL**, puis cliquez sur **Modifier**.
9. En regard de **Authentification**, cliquez sur **+** pour ajouter l'authentification du certificat.
10. Pour sélectionner la méthode d'authentification, dans **Choisir une stratégie**, sélectionnez **Certificat** et dans **Choisir un type**, sélectionnez **Principal**. Cela lie l'authentification par certificat en tant qu'authentification principale avec la même priorité que le type d'authentification LDAP.
11. Sous **Liaison de stratégie**, **cliquez sur Cliquez pour sélectionner** pour sélectionner la stratégie de certificat créée précédemment.
12. Sélectionnez la stratégie de certificat créée précédemment, puis cliquez sur **OK**.
13. Définissez la **priorité** sur **100**, puis cliquez sur **Liaison**. Utilisez le même numéro de priorité lorsque vous configurez la stratégie d'authentification LDAP dans les étapes suivantes.
14. Sur la ligne correspondant à la **stratégie LDAP**, cliquez sur **.
15. Sélectionnez la stratégie, puis, dans le menu déroulant **Modifier**, cliquez sur **Modifier la liaison**.
16. Entrez la même valeur de **priorité** que celle que vous avez spécifiée pour la stratégie de certificat. Cliquez sur **Bind**.

17. Cliquez sur **Fermer**.
18. Cliquez sur l'icône de modification dans la section **Paramètres SSL**.
19. Cochez la case **Authentification du client**, puis dans **Certificat client**, choisissez **Obligatoire**, puis cliquez sur **OK**.
20. Cliquez sur **Terminé**.

Liste de révocation de certificats (CRL) NetScaler

Citrix Endpoint Management prend en charge la liste de révocation de certificats (CRL) uniquement pour une autorité de certification tierce. Si vous avez configuré une autorité de certification Microsoft, Citrix Endpoint Management utilise NetScaler pour gérer la révocation. Lorsque vous configurez l'authentification basée sur un certificat client, vous devez décider si vous avez besoin de configurer le paramètre Liste de révocation de certificats (CRL) NetScaler, **Enable CRL Auto Refresh**. Cette étape garantit que l'utilisateur d'un appareil en mode MAM exclusif ne peut pas s'authentifier à l'aide d'un certificat existant sur l'appareil. Citrix Endpoint Management réémet un nouveau certificat, car il n'empêche pas un utilisateur de générer un certificat utilisateur si un certificat est révoqué. Ce paramètre renforce la sécurité des entités PKI lorsque la CRL vérifie la présence d'entités PKI expirées.

Intégration Microsoft Intune

January 26, 2024

L'intégration de Microsoft Intune à NetScaler Gateway fournit la meilleure solution d'accès aux applications et de protection des données proposée par NetScaler Gateway et Intune.

Vous bénéficiez de la suite la plus complète d'applications de productivité sécurisées, y compris la messagerie électronique, le calendrier, les contacts, la prise de notes, l'édition de documents et l'accès à distance, le tout pouvant être géré de manière centralisée sur différentes plates-formes. L'intégration d'Intune et de NetScaler Gateway fournit des fonctionnalités de gestion des appareils mobiles (MDM) de pointe, tandis que la technologie côté client Citrix Secure Access permet à ces applications éclairées d'Intune d'accéder aux données et aux applications de l'entreprise en toute sécurité via NetScaler Gateway.

L'intégration permet à NetScaler Gateway d'extraire les données de conformité d'Intune, ce qui permet d'appliquer des stratégies d'accès conditionnel. Les stratégies d'accès conditionnel donnent à NetScaler Gateway un contrôle plus précis sur la régulation de l'accès en fonction des fonctionnalités de l'appareil, etc. Par exemple, un administrateur peut créer une stratégie dans laquelle seuls les appareils dont l'option « Caméra » est désactivée sont autorisés à y accéder.

NetScaler Gateway prend en charge l'authentification par jeton des bibliothèques Azure Active Directory (ADAL) une fois que le serveur virtuel NetScaler Gateway est configuré. Lors de la configuration, une application mobile encapsulée avec le wrapper ou le SDK Citrix Network-Only accède à NetScaler Gateway à l'aide d'un jeton ADAL que l'application peut récupérer directement auprès d'AAD.

Intégration de Citrix Micro VPN avec Microsoft Endpoint Manager

Les clients de NetScaler Gateway peuvent utiliser un micro VPN avec Microsoft Endpoint Manager (Intune). L'intégration de Citrix Micro VPN avec Microsoft Endpoint Management permet à vos applications d'accéder aux ressources locales.

La technologie Citrix Micro VPN fournit un VPN à la demande qui réduit les coûts de transfert de données et simplifie la sécurité, car le tunnel VPN n'est pas toujours actif. Au lieu de cela, il n'est actif qu'en cas de besoin, ce qui réduit les risques et optimise les performances de l'appareil pour une meilleure expérience utilisateur. Cela contribue également à améliorer la durée de vie de la batterie mobile. La technologie micro VPN de NetScaler fournit aux utilisateurs mobiles un accès sécurisé aux ressources internes de l'entreprise tout en leur offrant la meilleure expérience utilisateur possible.

Micro VPN n'est pris en charge que pour les cas d'utilisation suivants :

- Gestion des applications mobiles (MAM) Intune uniquement
- Gestion des appareils mobiles (MDM) Intune et gestion des applications mobiles (MAM)

> **Important :**
>
> Pour la fonctionnalité VPN SSL, le micro VPN nécessite une édition NetScaler Gateway Advanced ou Premium (VPX 3000 ou version ultérieure) et un droit Citrix Endpoint Management. L'autorisation Citrix Endpoint Management garantit une prise en charge continue du SDK micro VPN sur un navigateur mobile Microsoft Edge (iOS et Android). Pour plus d'informations, contactez le représentant de votre service commercial, de votre compte ou de votre partenaire.

Pour plus d'informations sur la configuration de l'intégration du micro VPN Citrix à Microsoft Endpoint Manager, voir Configurer NetScaler Gateway pour utiliser le micro VPN avec Microsoft EndpointManager.

Quand utiliser la solution Intune MDM intégrée

January 26, 2024

Les scénarios suivants illustrent l'utilisation de la solution Intune MDM intégrée :

- Un nouveau client décide d'intégrer Intune au déploiement sur site de NetScaler Gateway

- Un utilisateur existant de NetScaler Gateway souhaite ajouter la gestion des appareils mobiles avec Intune
- Un utilisateur d'Intune existant souhaite autoriser les appareils mobiles ou les applications à accéder aux données situées au sein du réseau de l'entreprise à l'aide d'une appliance physique ou virtuelle NetScaler Gateway située dans la zone démilitarisée de l'entreprise

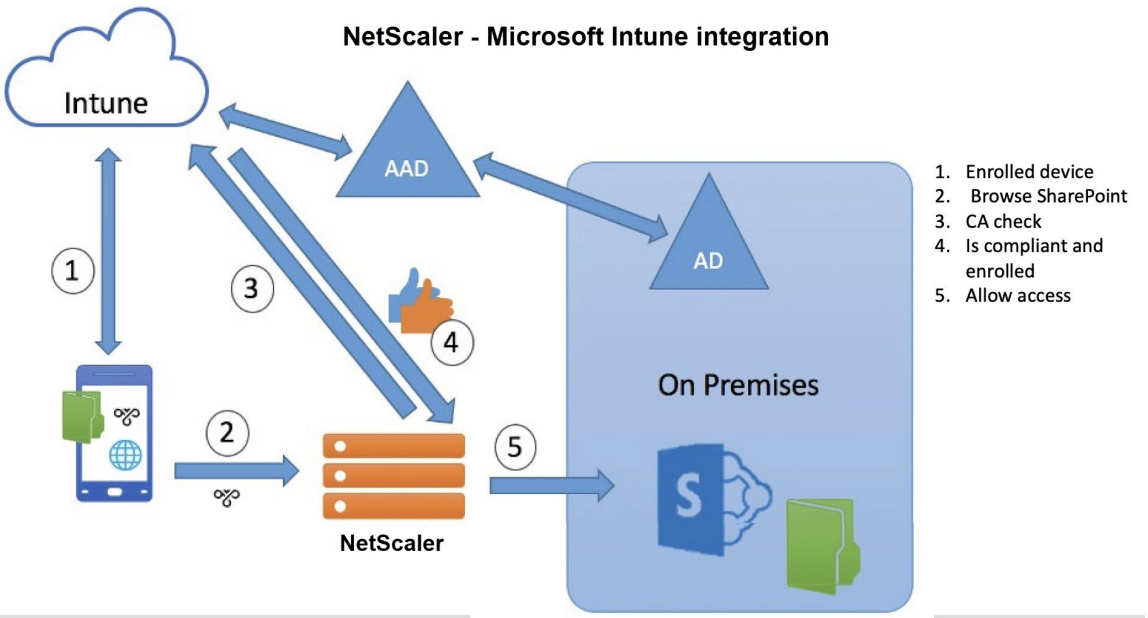
> **Remarque**
>
> Seuls les clients iOS et Android sont pris en charge.

Comprendre l'intégration de NetScaler Gateway MDM à Intune

January 26, 2024

Voici un exemple de flux d'événements dans le cadre d'une intégration MDM classique de NetScaler Gateway avec Intune :

1. Inscrivez un appareil mobile avec Intune.
2. Les applications et stratégies d'appareil approuvées par l'entreprise sont transmises à l'appareil.
3. Parcourez SharePoint (application locale) à partir de l'appareil.
4. La demande du navigateur est envoyée à NetScaler Gateway.
5. L'appliance NetScaler Gateway vérifie auprès d'Intune l'état d'inscription de l'appareil.
6. Si un appareil conforme est inscrit avec succès, l'accès SharePoint est accordé.



Lorsqu'un appareil ne répond pas à une stratégie d'accès conditionnel, le client VPN NetScaler Gateway affiche un message d'erreur. Le message fournit un lien entre l'appareil et une page hébergée par Intune qui donne à l'utilisateur la possibilité de s'inscrire ou de corriger l'état de conformité de l'appareil.

> **Remarque :**
>
> Les administrateurs doivent s'assurer des points suivants lorsqu'ils poussent les certificats vers Intune afin que les utilisateurs puissent différencier les différents certificats de leur appareil.

- Les certificats doivent comporter un résumé du sujet.
- Les résumés des sujets des différents certificats doivent être distincts.

Prise en charge des API Intune NAC v2

Dans le cadre de la prise en charge de l'API Intune NAC v2, vous devez lier un fichier d'autorité de certification (certificat CA) pour garantir que l'appliance NetScaler obtient un certificat valide depuis les appareils mobiles. Dans Intune NAC v2, les appareils mobiles envoient des ID d'appareil dans le cadre du certificat de l'autorité de certification. Le certificat d'autorité de certification lié ici doit être celui utilisé pour émettre des certificats clients sur les appareils iOS et Android des utilisateurs finaux. S'il existe des certificats intermédiaires, ceux-ci doivent également être liés ici.

Pour plus de détails, voir Prise en charge de l'API Intune NAC v2

Configurer la vérification du périphérique de contrôle d'accès réseau pour le serveur virtuel NetScaler Gateway pour une connexion à facteur unique

March 27, 2024

Cette rubrique fournit des informations sur la configuration de NetScaler Gateway pour se connecter à un réseau interne à partir d'un appareil mobile (iOS et Android) avec la sécurité Network Access Compliance (NAC) proposée par Microsoft Intune. Lorsqu'un utilisateur essaie de se connecter à NetScaler Gateway à partir d'un client VPN iOS ou Android, la passerelle vérifie d'abord auprès du service Intune si l'appareil est géré et conforme.

- Géré : l'appareil est inscrit à l'aide du client du portail d'entreprise Intune.
- Conformité : les stratégies requises envoyées depuis le serveur MDM Intune sont appliquées.

Ce n'est que si l'appareil est géré et conforme que la session VPN est établie et que l'utilisateur a accès aux ressources internes.

> **Remarque :**
>
> - Dans cette configuration, NetScaler Gateway du back-end communique avec le service Intune. Les profils SSL gèrent les connexions entrantes à NetScaler Gateway. La communication principale de NetScaler Gateway gère toutes les exigences SNI des services cloud principaux (Intune).
> - Le serveur virtuel de passerelle SNI pour DTLS est pris en charge dans NetScaler Gateway version 13.0 build 64.x et versions ultérieures.
> - La vérification NAC Intune, pour le VPN par application ou même le VPN à l'échelle de l'appareil, n'est prise en charge que lorsque le profil VPN est provisionné par le portail de gestion Intune (maintenant connu sous le nom de Microsoft Endpoint Manager). Ces fonctionnalités ne sont pas prises en charge pour les profils VPN ajoutés par l'utilisateur final. Le profil VPN de la machine de l'utilisateur final doit être déployé sur son appareil à partir de Microsoft Endpoint Manager par son administrateur Intune pour utiliser la vérification NAC.

Gestion des licences

Une licence Citrix Enterprise Edition est requise pour cette fonctionnalité.

Configuration système requise

- NetScaler Gateway version 11.1 build 51.21 ou ultérieure
- VPN iOS —10.6 ou version ultérieure
- VPN Android —2.0.13 ou version ultérieure
- Microsoft
  - Accès Azure AD (avec des privilèges de locataire et d'administrateur)
  - Locataire activé Intune
- Pare-feu
  Activer les règles de pare-feu pour tout le trafic DNS et SSL depuis l'adresse IP du sous-réseau vers `https://login.microsoftonline.com` et `https://graph.windows.net` (port 53 et port 443)

Pré-requis

- Toutes les stratégies d'authentification existantes doivent être converties des stratégies classiques aux stratégies avancées. Pour plus d'informations sur la conversion de stratégies clas-

siques en stratégies avancées, reportez-vous à la section https://support.citrix.com/article/CTX131024.

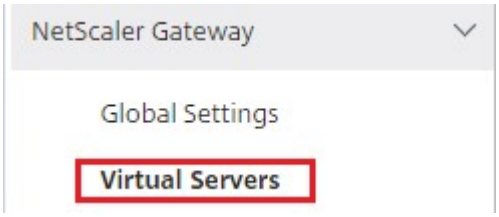
- Créez une application NetScaler Gateway sur le portail Azure. Pour plus de détails, consultez Configuration d'une application NetScaler Gateway sur le portail Azure.
- Configurez la stratégie OAuth sur l'application NetScaler Gateway que vous avez créée à l'aide des informations spécifiques à l'application suivantes.
  - ID client/ID de l'application
  - Secret client/ Clé d'application
  - ID de locataire Azure

Références

- Ce document capture la configuration de NetScaler Gateway. La plupart de la configuration du client Citrix SSO (iOS/Android) se fait du côté Intune. Pour plus d'informations sur la configuration du VPN Intune pour NAC, reportez-vous à la section https://docs.microsoft.com/en-us/mem/intune/protect/network-access-control-integrate.
- Pour configurer le profil VPN d'une application iOS, reportez-vous à la section https://docs.microsoft.com/en-us/mem/intune/configuration/vpn-settings-ios.
- Pour configurer l'application NetScaler Gateway sur le portail Azure, consultez la section Configuration d'une application NetScaler Gateway sur leportail Azure.

Pour ajouter un serveur virtuel NetScaler Gateway avec nFactor pour le déploiement de la passerelle

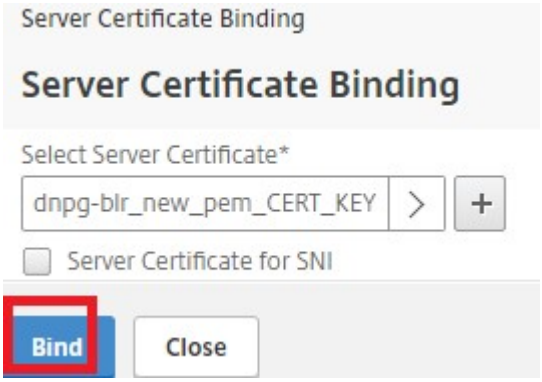
1. Accédez à **NetScaler Gateway > Serveurs virtuels**.



2. Cliquez sur **Ajouter**.
3. Indiquez les informations requises dans la zone **Paramètres de base**, puis cliquez sur **OK**.

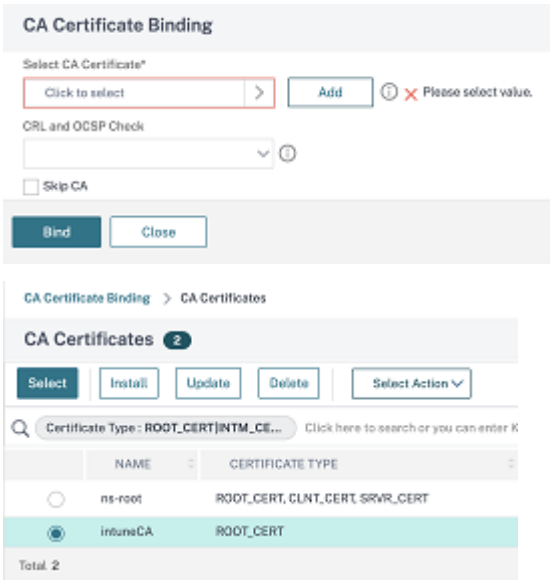
4. Sélectionnez **Certificat de serveur**.

5. Sélectionnez le certificat de serveur requis et cliquez sur **Liaison**.



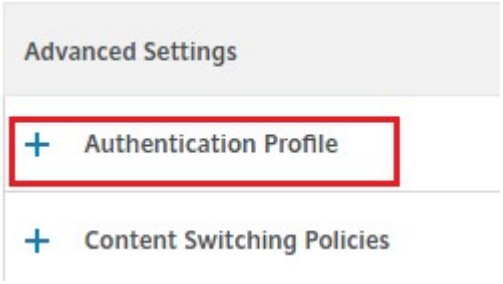
6. Dans le cadre de la prise en charge de l'API Intune NAC v2, vous devez lier un fichier d'autorité de certification (certificat CA) pour garantir que l'appliance NetScaler obtient un certificat valide depuis les appareils mobiles. Dans Intune NAC v2, les appareils mobiles envoient des ID d'appareil dans le cadre du certificat client. Le certificat d'autorité de certification lié ici doit être

celui utilisé pour émettre des certificats clients aux appareils iOS et Android des utilisateurs finaux. S'il existe des certificats intermédiaires, ceux-ci doivent également être liés ici. Pour en savoir plus sur la configuration d'Intune, consultez la section Configuration d'une application NetScaler Gateway sur leportail Azure. Pour prendre en charge l'API Intune NAC v2, sélectionnez le certificat d'autorité de certification requis et cliquez sur **Lier**.

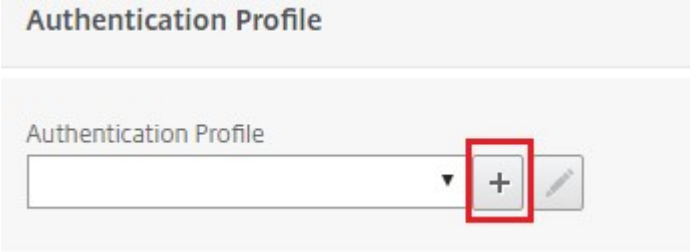


7. Cliquez sur **Continuer**.
8. Cliquez sur **Continuer**.
9. Cliquez sur **Continuer**.
10. Cliquez sur l'icône plus **[+]** en regard de **Stratégies** et sélectionnez **Session** dans la liste **Choisir une stratégie**, sélectionnez **Demande** dans la liste **Choisir un type**, puis cliquez sur **Continuer**.
11. Cliquez sur l'icône plus **[+]** en regard de **Sélectionner une stratégie**.
12. Sur la page **Create NetScaler Gateway Session Policy**, attribuez un nom à la stratégie de session.
13. Cliquez sur l'icône plus [+] à côté de **Profil** et sur la page **Créer un profil de session NetScaler Gateway, donnez un nom au profil** de session.
14. Dans l'onglet **Expérience client**, cochez la case en regard de **Accès sans client** et sélectionnez **Désactivé** dans la liste.
15. Cochez la case en regard de **Type de plug-in** et sélectionnez Windows/Mac OS X dans la liste.
16. Cliquez sur **Paramètres avancés**, cochez la case en regard de **Choix du client** et définissez sa valeur **sur ON**.
17. Dans l'onglet **Sécurité**, cochez la case en regard de **Action d'autorisation par défaut** et sélectionnez **Autoriser** dans la liste.

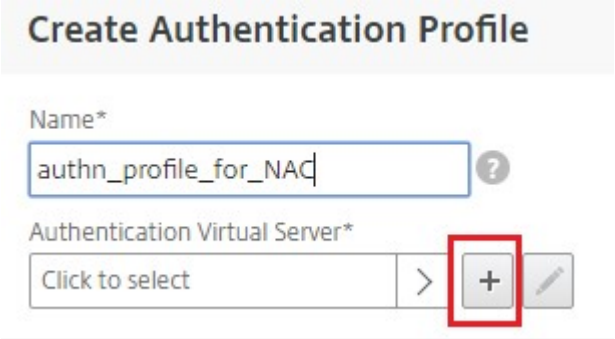
18. Dans l'onglet **Applications publiées**, cochez la case en regard de **Proxy ICA** et sélectionnez **DÉSACTIVÉ** dans la liste.
19. Cliquez sur **Créer**.
20. Sur la page **Create NetScaler Gateway Session Policy**, dans la zone **Expression, configurez l'expression** qualificative.
21. Cliquez sur **Créer**.
22. Cliquez sur **Bind**.
23. Sélectionnez **Profil d'authentification** dans **les paramètres avancés**.



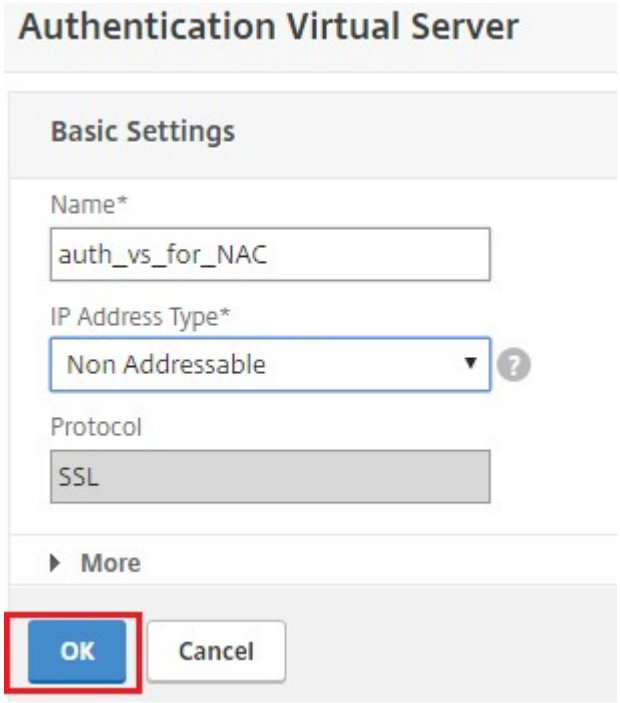
24. Cliquez sur l'icône plus **[+]** et saisissez un nom pour le profil d'authentification.



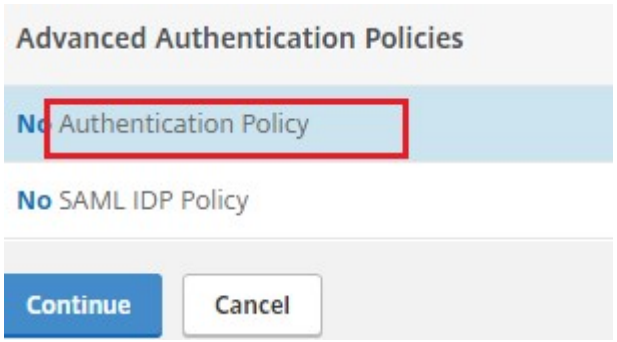
25. Cliquez sur l'icône plus **[+]** pour créer un serveur virtuel d'authentification.



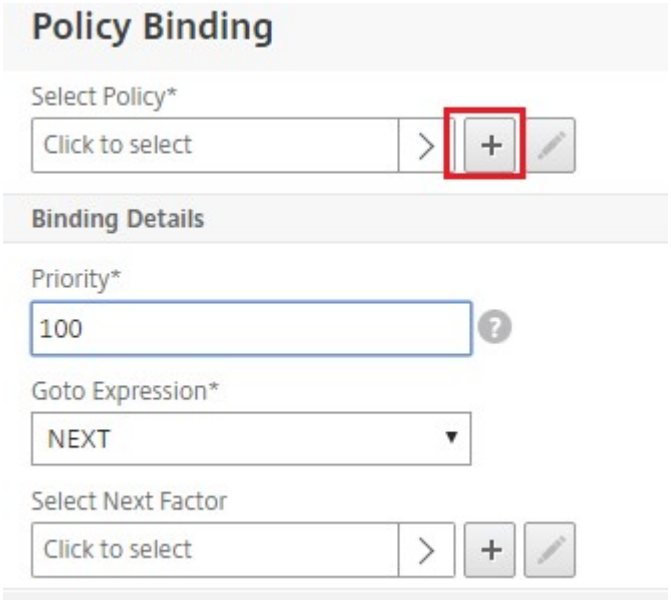
26. Spécifiez le nom et le type d'adresse IP du serveur virtuel d'authentification dans la zone **Paramètres de base**, puis cliquez sur **OK**. Le type d'adresse IP peut également être **non adressable**.



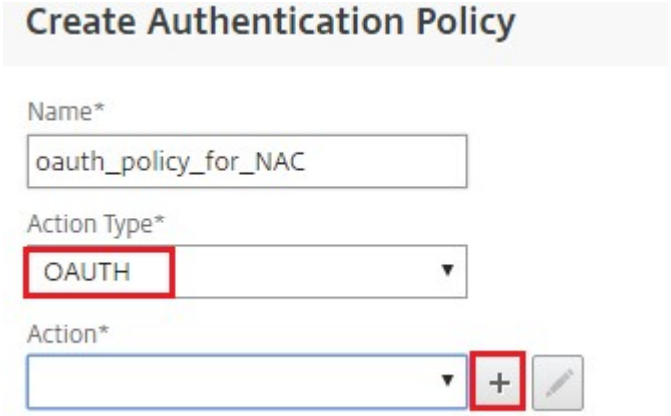
27. Cliquez sur **Stratégie d'authentification**.



28. Dans la vue Liaison de stratégie, cliquez sur l'icône plus **[+]** pour créer une stratégie d'authentification.



29. Sélectionnez **OAUTH** comme **type d'action** et cliquez sur l'icône plus **[+]** pour créer une action OAuth pour NAC.



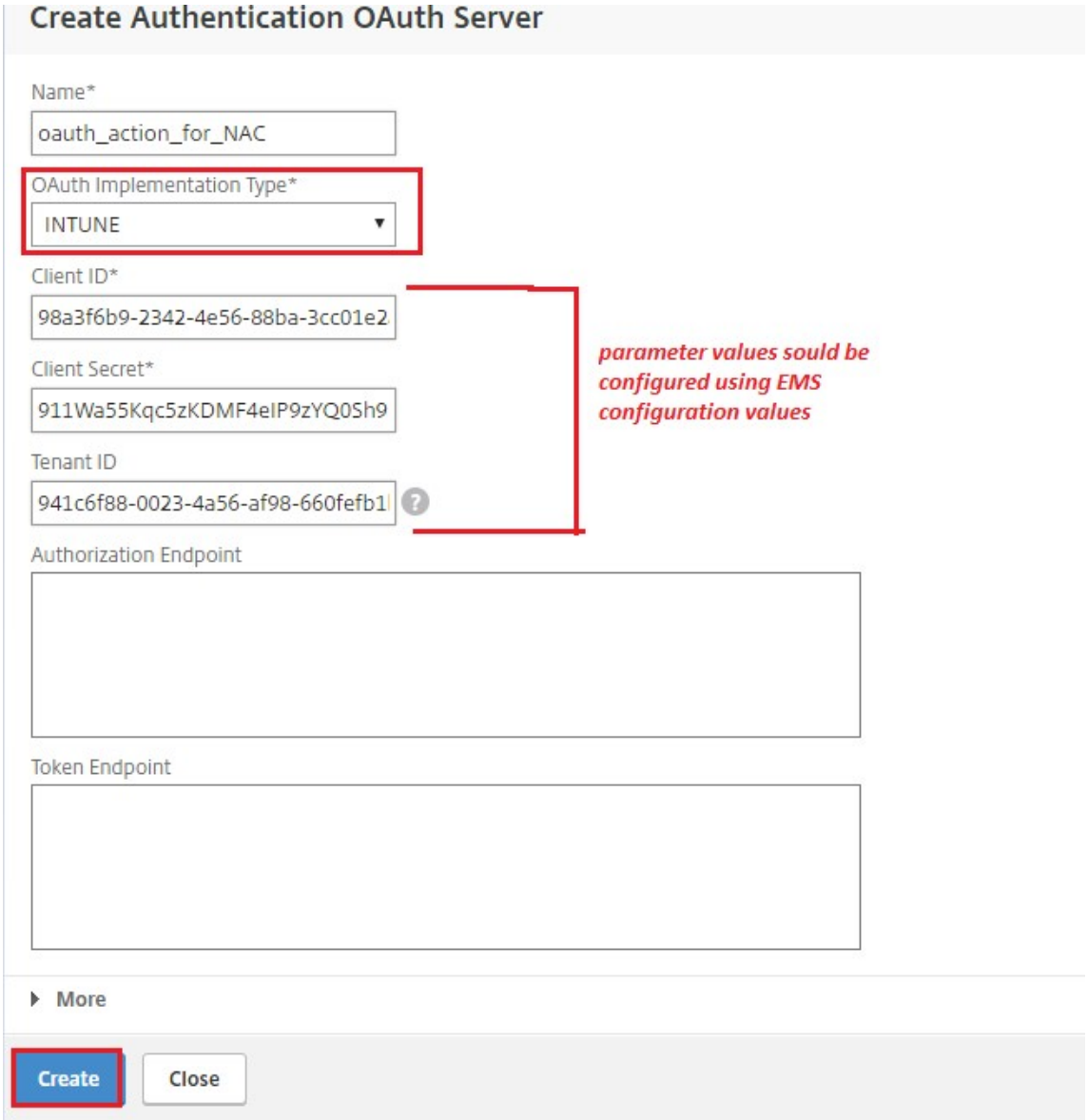
30. Créez une action OAuth à l'aide de l'**ID client**, **du secret client**et de l'**ID de locataire**.

> **Remarque :**
>
> - **L'ID client**, **le secret client** et l'**ID du locataire** sont générés après la configuration de l'application NetScaler Gateway sur le portail Azure.
> - Notez les informations relatives à l'ID client/à l'ID d'application, au secret du client/au secret d'application et à l'ID du locataire Azure, car elles sont requises lors de la création ultérieure d'une action OAuth sur NetScaler Gateway.

Assurez-vous que vous disposez d'un serveur de noms DNS approprié configuré sur votre appliance pour résoudre et atteindre ;
`https://login.microsoftonline.com/`,

-

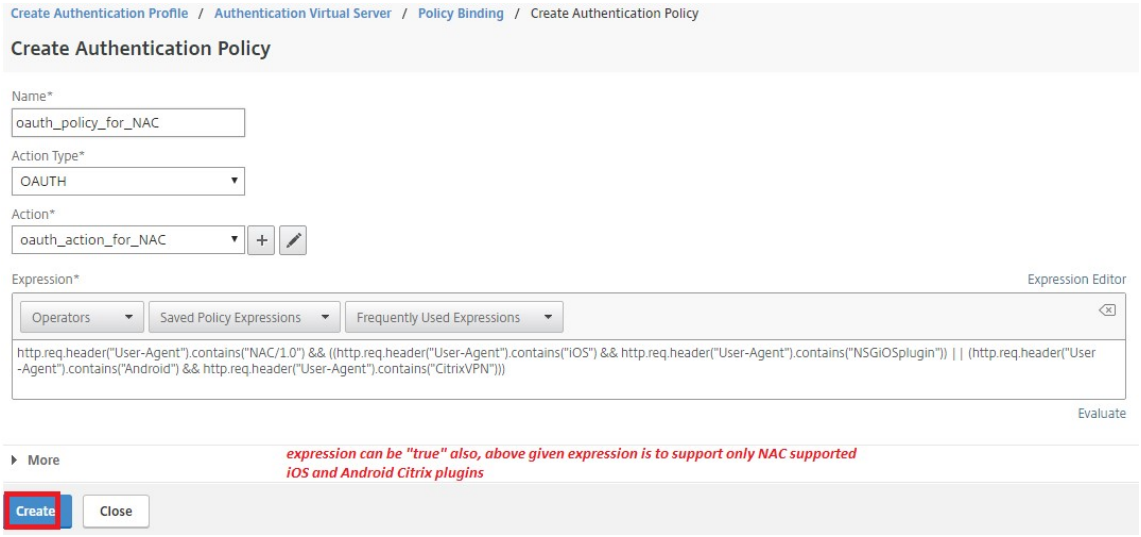
- `https://graph.windows.net/`, - *.manage.microsoft.com.



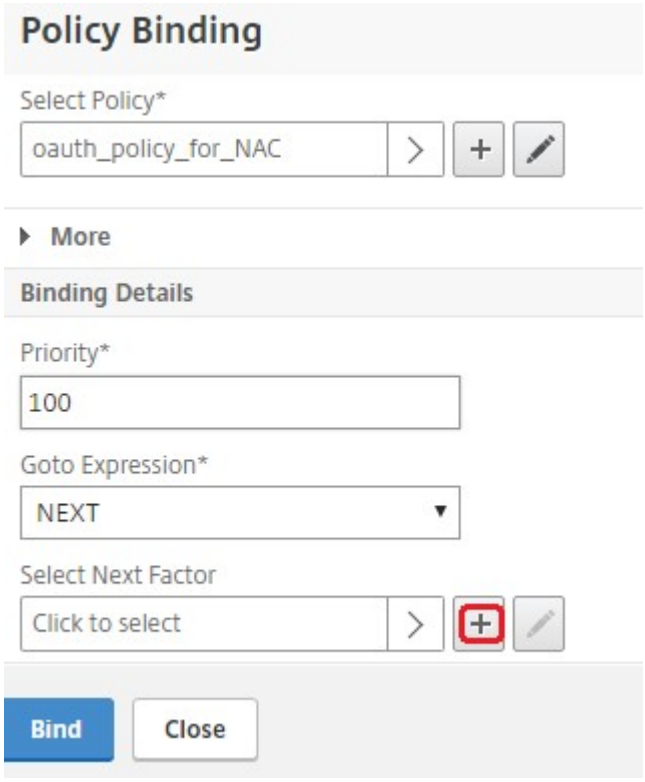
31. Créez une stratégie d'authentification pour **OAuth Action**.

Règle :

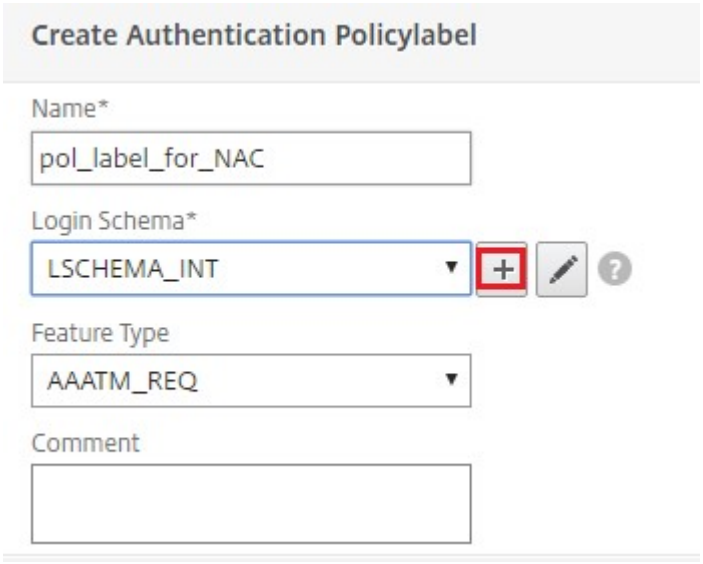
```
http.req.header("User-Agent").contains("NAC/1.0")&& ((http.req.
    header("User-Agent").contains("iOS") && http.req.header("User-
    Agent").contains("NSGiOSplugin")) || (http.req.header("User-
    Agent").contains("Android") && http.req.header("User-Agent").
    contains("CitrixVPN")))
<!--NeedCopy-->
```

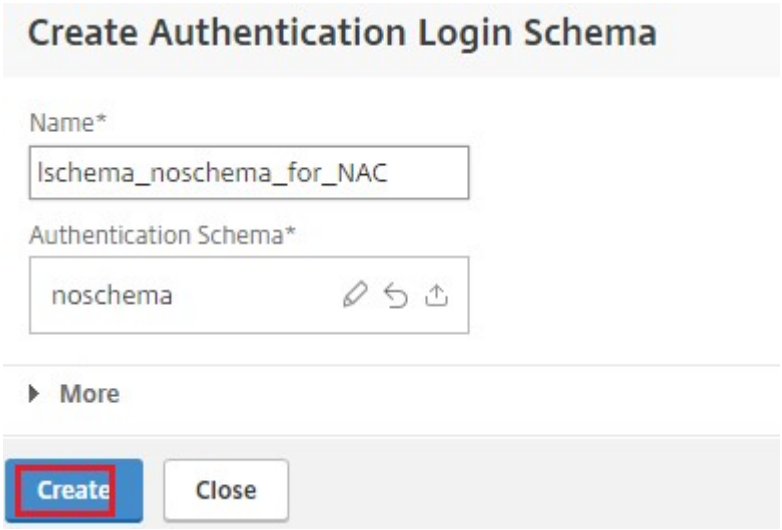
32. Cliquez sur l'icône plus **[+]** pour créer une étiquette de stratégie NextFactor.



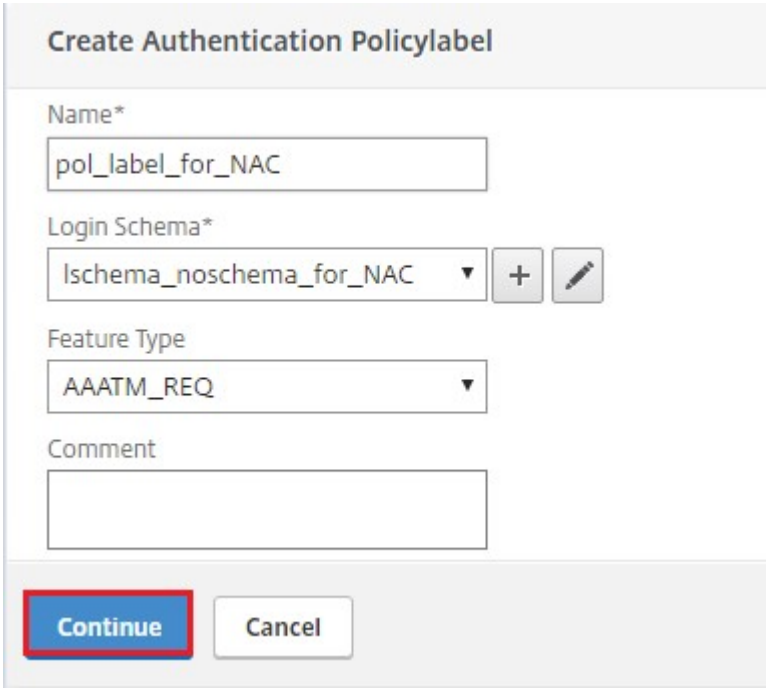
33. Cliquez sur l'icône plus **[+]** pour créer un schéma de connexion.



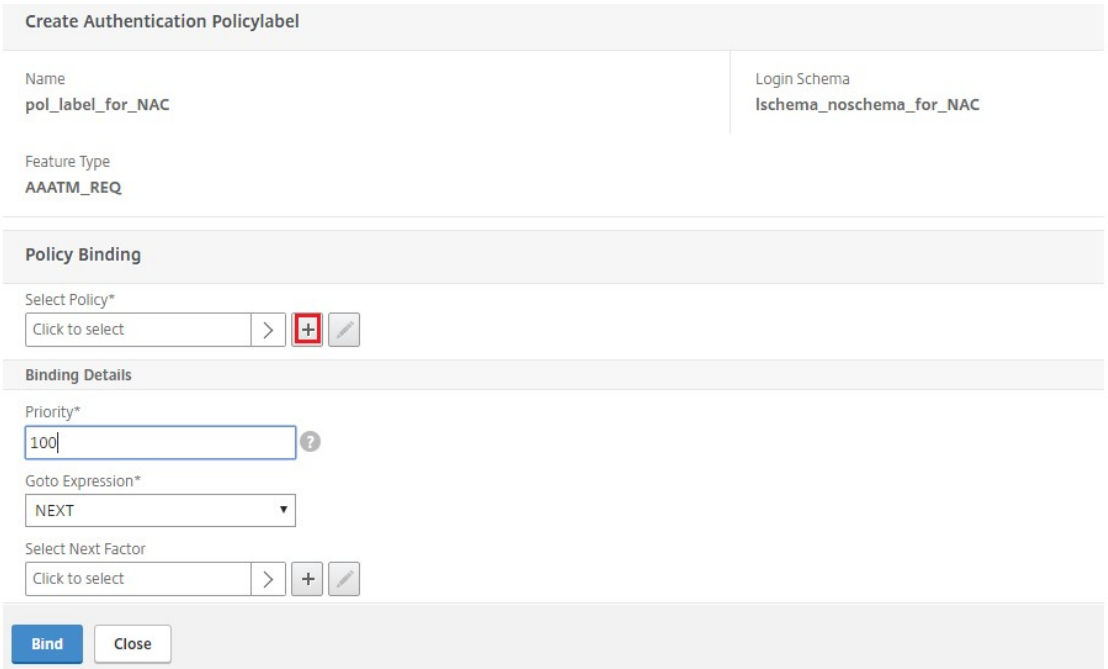
34. Sélectionnez **noschema** en tant que schéma d'authentification, puis cliquez sur **Créer**.



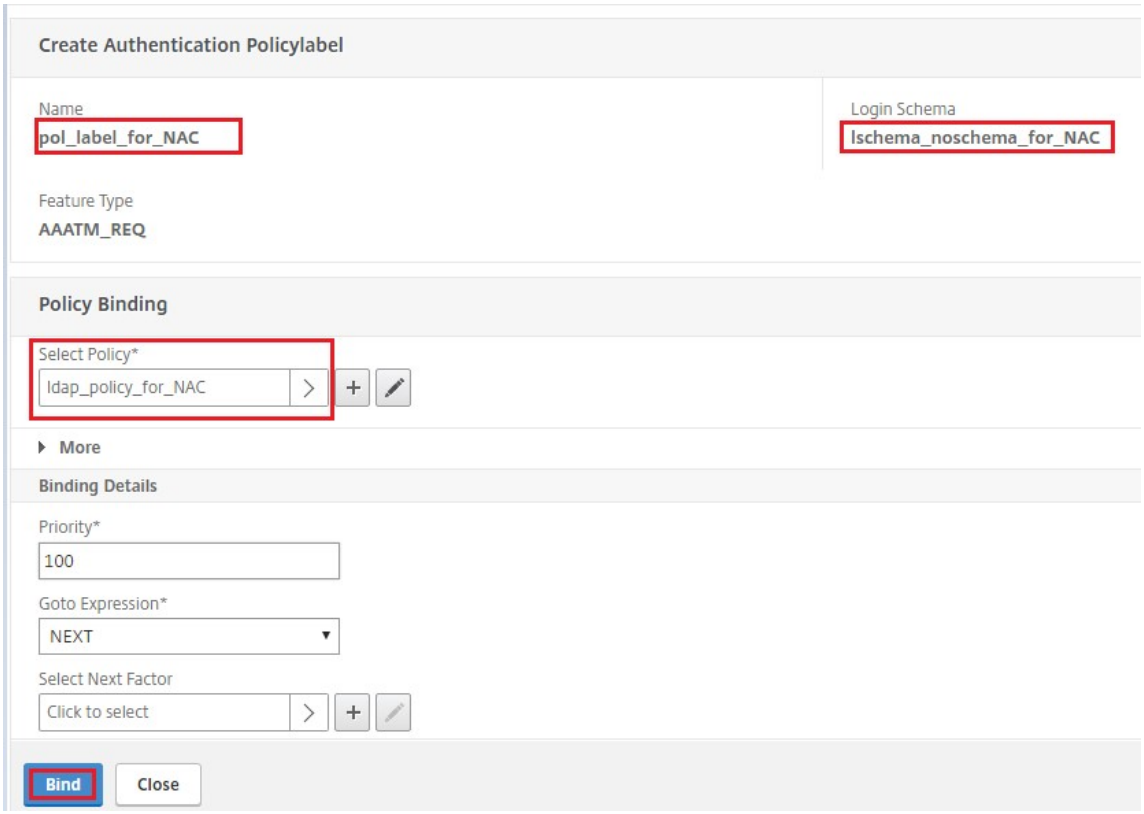
35. Après avoir sélectionné le schéma de connexion créé, cliquez sur **Continuer**.



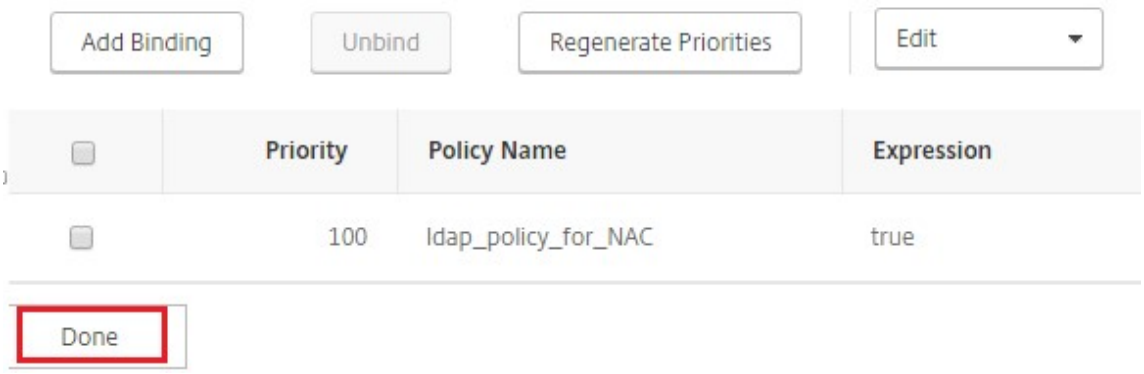
36. Dans **Sélectionner une stratégie**, sélectionnez une stratégie d'authentification existante pour la connexion de l'utilisateur ou cliquez sur l'icône plus **+** pour créer une stratégie d'authentification.
    Pour plus d'informations sur la création d'une stratégie d'authentification, consultez Configuration des stratégies d'authentification avancées et Configuration de l'authentification LDAP.



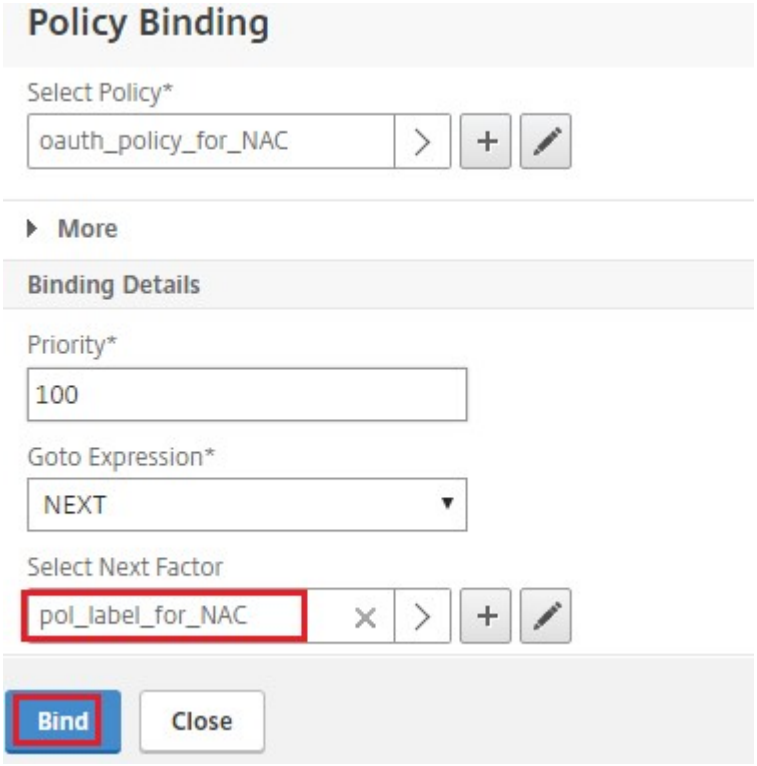
37. Cliquez sur **Bind**.



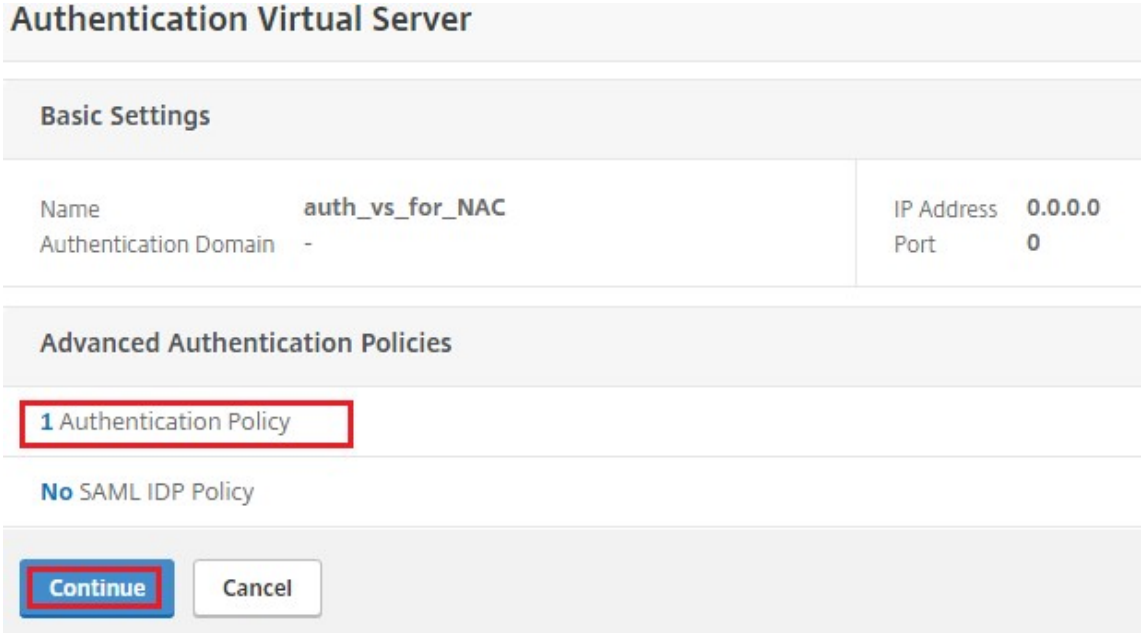
38. Cliquez sur **Terminé**.



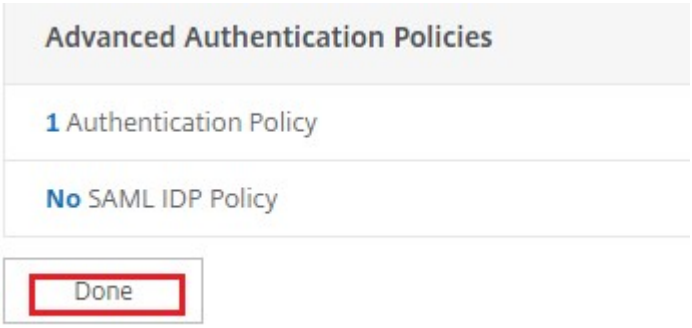
39. Cliquez sur **Bind**.



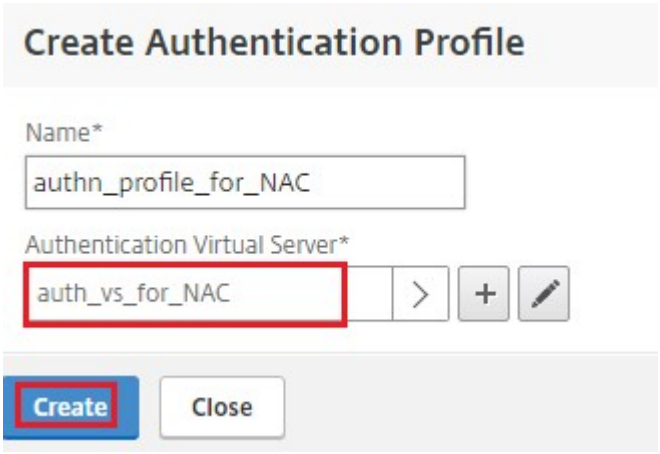
40. Cliquez sur **Continuer**.



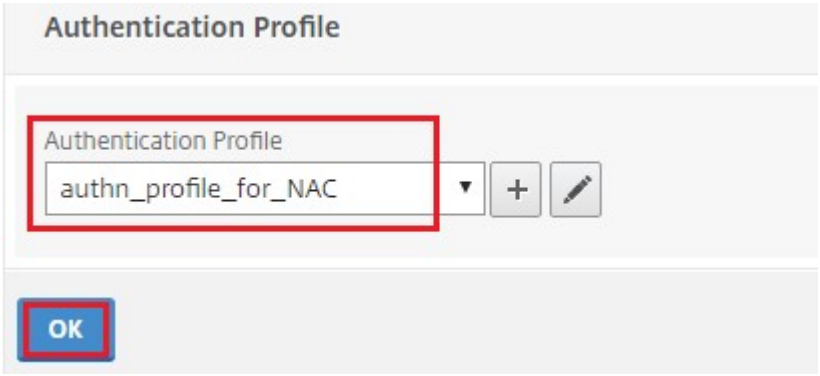
41. Cliquez sur **Terminé**.



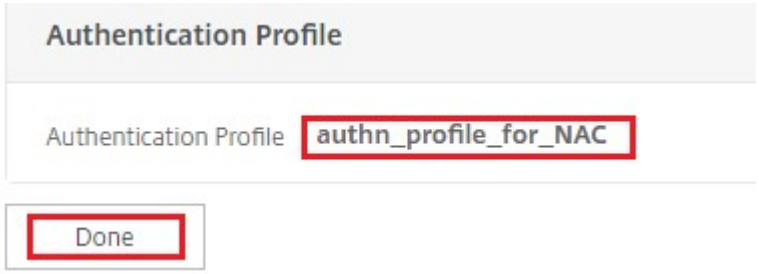
42. Cliquez sur **Créer**.



43. Cliquez sur **OK**.



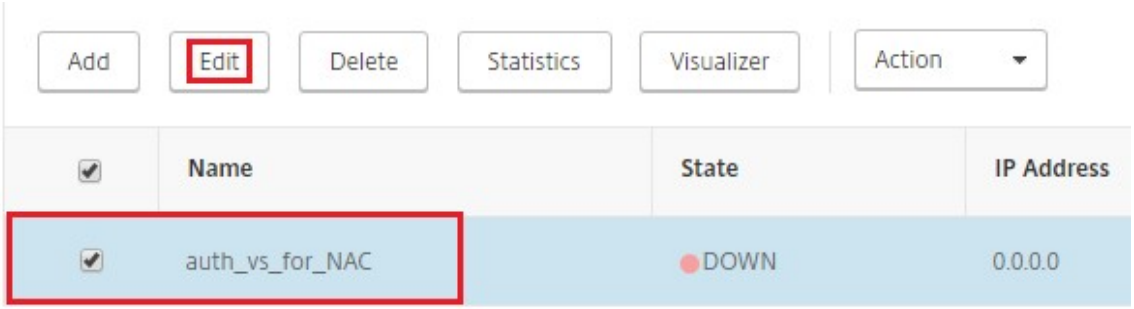
44. Cliquez sur **Terminé**.



Pour lier le schéma de connexion d'authentification au serveur virtuel d'authentification afin d'indiquer que les plug-ins VPN doivent envoyer l'ID de périphérique dans le cadre de la demande /cgi/login

1. Accédez à **Sécurité** > **AAA - Trafic des applications** > **Serveurs virtuels**.

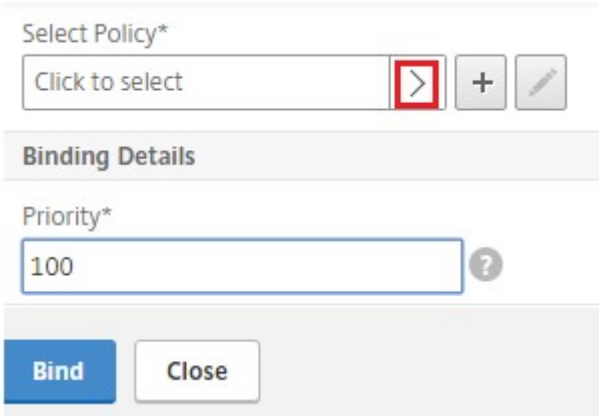
2. Sélectionnez le serveur virtuel précédemment sélectionné, puis cliquez sur **Modifier**.



3. Cliquez sur **Schémas de connexion** sous **Paramètres avancés**.

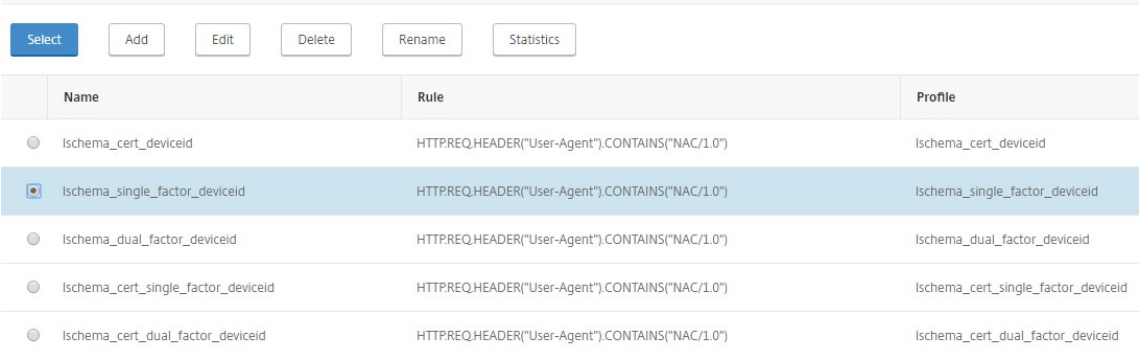
4. Cliquez sur **Schémas de connexion** à lier.

5. Cliquez sur **[>]** pour sélectionner et lier les stratégies de schéma de connexion intégrées existantes pour la vérification des périphériques NAC.

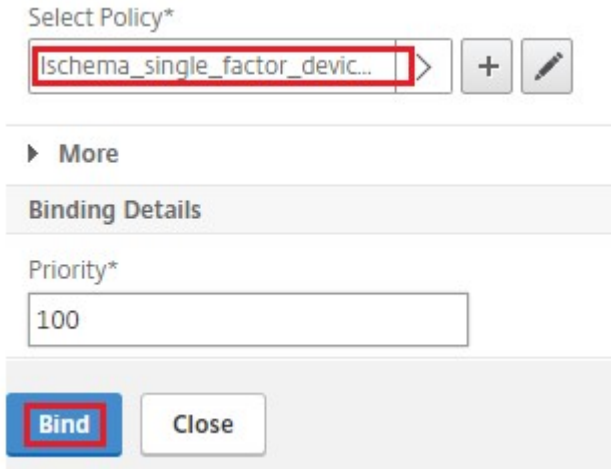


6. Sélectionnez la stratégie de schéma de connexion requise appropriée à votre déploiement d'authentification, puis cliquez sur **Sélectionner**.

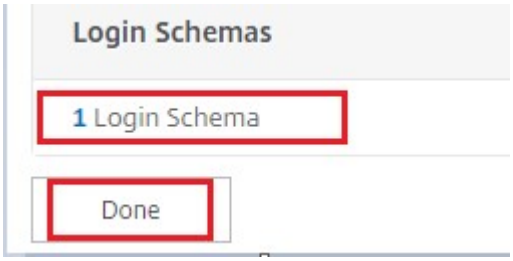
   Dans le déploiement expliqué précédemment, l'authentification à facteur unique (LDAP) ainsi qu'une stratégie d'action OAuth NAC sont utilisées. Par conséquent, **lschema_single_factor_deviceid** est sélectionné.



7. Cliquez sur **Bind**.



8. Cliquez sur **Terminé**.



Prise en charge des API Intune NAC v2

Dans le cadre de la prise en charge de l'API Intune NAC v2, vous devez lier un fichier d'autorité de certification (certificat CA) pour garantir que l'appliance NetScaler obtient un certificat valide depuis les appareils mobiles. Dans Intune NAC v2, les appareils mobiles envoient des ID d'appareil dans le cadre du certificat de l'autorité de certification. Le certificat d'autorité de certification lié ici doit être celui utilisé pour émettre des certificats clients sur les appareils iOS et Android des utilisateurs finaux. S'il existe des certificats intermédiaires, ceux-ci doivent également être liés ici.

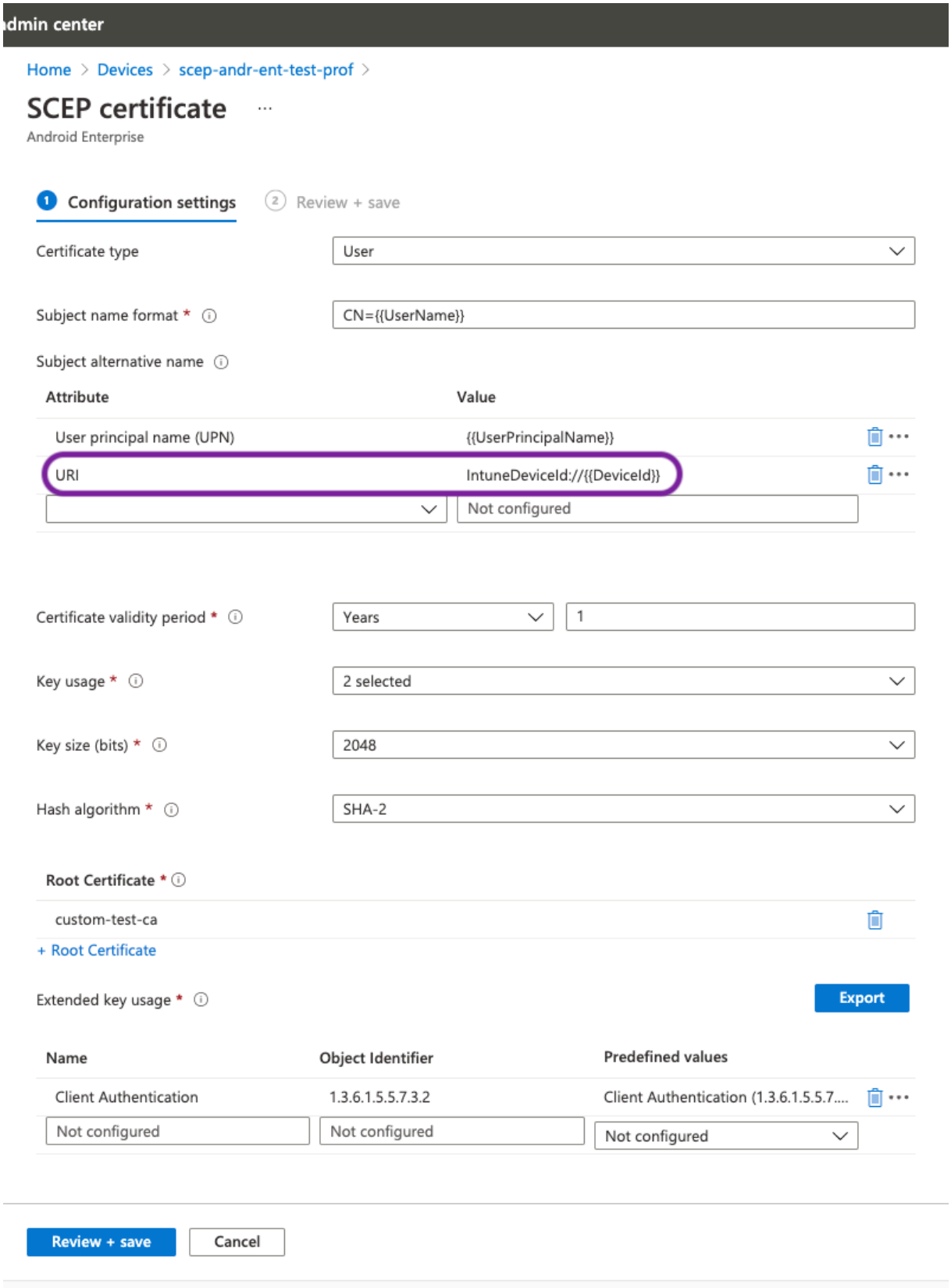
Vous pouvez utiliser l'exemple de commande suivant pour lier votre certificat d'autorité de certification.

```
bind ssl vserver intune_nac_check_443 -certkeyName clientca -CA -
    ocspCheck Optional
<!--NeedCopy-->
```

Important :

- La prise en charge de l'API Intune NAC v2 est disponible dans les versions 13.1 build 12.50 ou ultérieure de NetScaler Gateway et 13.0 build 84.11 ou version ultérieure.
- Vous devez activer l'authentification basée sur un certificat client `clientAuth` en définissant sur ACTIVÉ et `clientCert` sur FACULTATIF sur les serveurs virtuels VPN et d'authentification. Le paramètre `clientCert` est défini sur FACULTATIF afin que les autres points de terminaison qui n'ont pas besoin de la vérification NAC Intune puissent s'authentifier via le même serveur virtuel sans fournir le certificat client. Les appareils Android et iOS doivent fournir le certificat client. Sinon, la vérification du NAC Intune échoue.
- Vous devez vous assurer que les certificats clients provisionnés via Intune sur l'appareil mobile doivent avoir un ID d'appareil Intune dans le champ SAN de type URI, comme indiqué dans le document Nouveau service Microsoft Intune pour le contrôle d'accès réseau. Pour plus de détails, consultez https://techcommunity.microsoft.com/t5/intune-customer-success/new-microsoft-intune-service-for-network-access-control/ba-p/2544696.
  Le format du champ de valeur URI doit être identique à celui indiqué dans la figure suivante.

> En outre, l'application Citrix SSO doit utiliser le même certificat pour s'authentifier auprès de la passerelle.



Dépannage

Problèmes d'ordre général

Problème	Résolution
Le message « Ajouter une stratégie requise » s'affiche lorsque vous ouvrez une application	Ajouter des stratégies dans l'API Microsoft Graph
Il y a des conflits de stratégie	Une seule stratégie par application est autorisée
Votre application ne peut pas se connecter aux ressources internes	Assurez-vous que les ports de pare-feu appropriés sont ouverts, que l'ID de locataire est correct, etc.

Problèmes liés à NetScaler Gateway

Problème	Résolution
Les autorisations requises pour être configurées pour l'application passerelle sur Azure ne sont pas disponibles.	Vérifiez si une licence Intune appropriée est disponible. Essayez d'utiliser le portail manage.windowsazure.com pour voir si l'autorisation peut être ajoutée. Contactez le support technique Microsoft si le problème persiste.
NetScaler Gateway ne peut pas atteindre. `login.microsoftonline.comandgraph.windows.net`	À partir de NS Shell, vérifiez si vous êtes en mesure d'accéder au site Web Microsoft suivant : cURL -v -k https://login.microsoftonline.com. Vérifiez ensuite si le DNS est configuré sur NetScaler Gateway. Vérifiez également que les paramètres du pare-feu sont corrects (dans le cas où les demandes DNS sont pare-feu).
Une erreur apparaît dans ns.log après la configuration de OAuthAction.	Vérifiez si la licence Intune est activée et si l'application de passerelle Azure dispose des autorisations appropriées.
La commande `Sh OAuthAction` n'affiche pas l'état OAuth comme étant terminé.	Vérifiez les paramètres DNS et les autorisations configurées sur l'application de passerelle Azure.
L'appareil Android ou iOS n'affiche pas l'invite d'authentification double.	Vérifiez si l'ID d'appareil à double facteur LogonSchema est lié au serveur virtuel d'authentification.

État et état d'erreur de NetScaler Gateway OAuth

État	Condition d'erreur
AADFORGRAPH	Secret non valide, URL non résolue, expiration de la connexion
MDMINFO	*manage.microsoft.comest en panne ou inaccessible
GRAPH	Le point de terminaison graphique est inaccessible
CERTFETCH	Communication impossible avec Token Endpoint: https://login.microsoftonline.com en raison d'une erreur DNS. Pour valider cette configuration, accédez à l'invite Shell et tapez cURL https://login.microsoftonline.com. Cette commande doit être validée.

Remarque : Lorsque l'état OAuth est réussi, l'état est affiché comme COMPLETE.

Vérification de la configuration Intune

Assurez-vous de cocher la case **J'accepte** dans **Configuration VPN iOS de base pour Citrix SSO > Activer le contrôle d'accès réseau (NAC)**. Sinon, la vérification NAC ne fonctionne pas.

Configuration d'une application NetScaler Gateway sur le portail Azure

March 27, 2024

La section suivante répertorie les étapes à suivre pour configurer une application NetScaler Gateway sur le portail Azure.

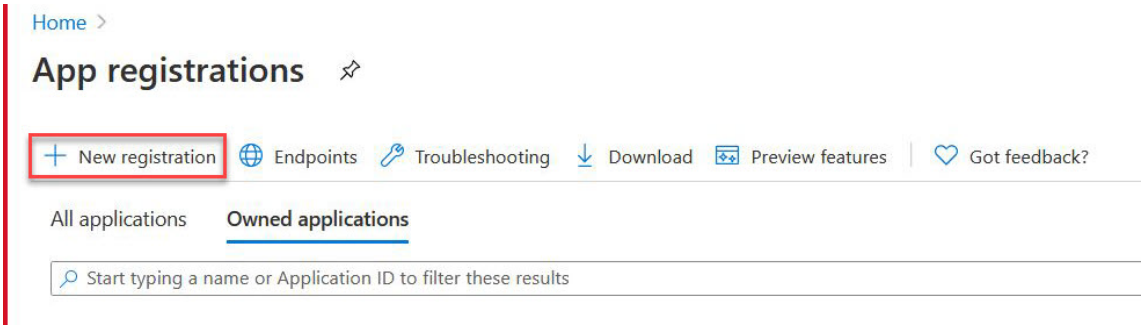
Pré-requis

- Informations d'identification Azure Global Admin
- Les licences Intune sont activées
- Pour l'intégration Intune, vous devez créer une application NetScaler Gateway sur le portail Azure.

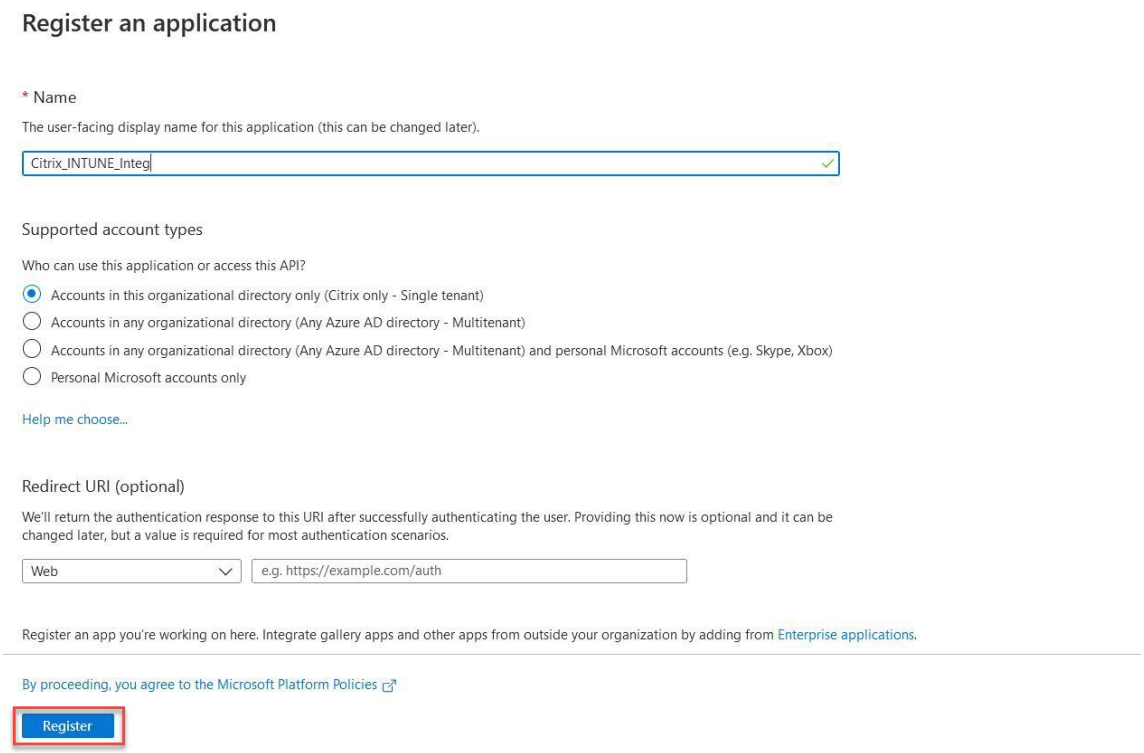
- Une fois l'application NetScaler Gateway créée, configurez la stratégie OAuth sur NetScaler Gateway à l'aide des informations spécifiques à l'application suivantes :
  - ID client/ID de l'application
  - Secret client/clé d'application
  - ID de locataire Azure
- NetScaler Gateway utilise l'identifiant client de l'application et le secret du client pour communiquer avec Azure et vérifier la conformité au NAC.

Pour créer une application NetScaler Gateway sur Azure

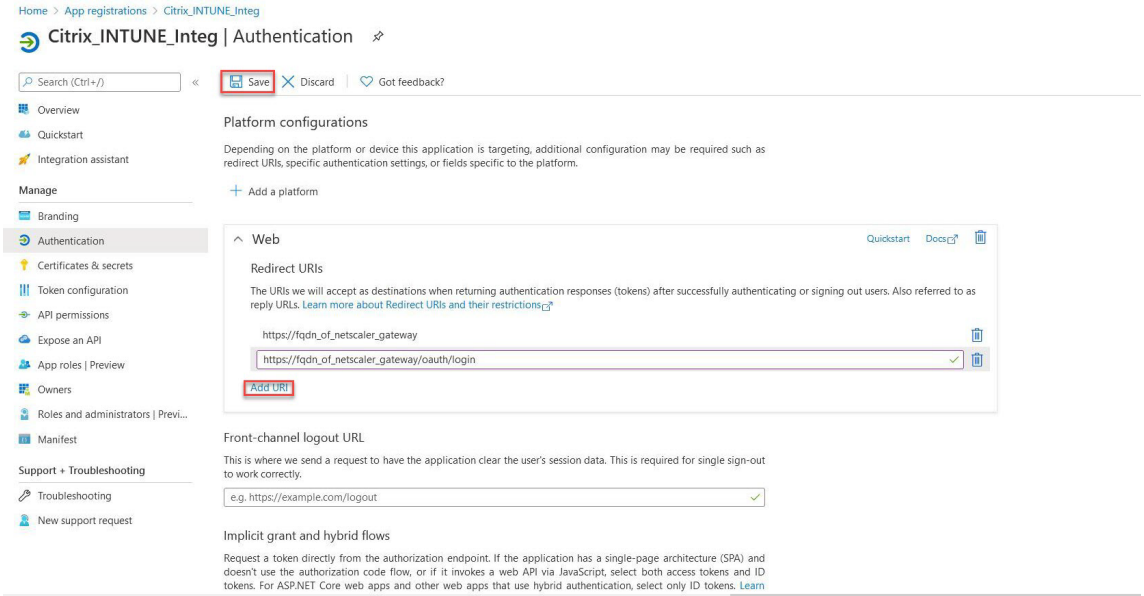
1. Connectez-vous à portal.azure.com
2. Cliquez sur **Azure Active Directory**.
3. Cliquez sur **Enregistrements d'applications**, puis sur **Nouvel enregistrement**.



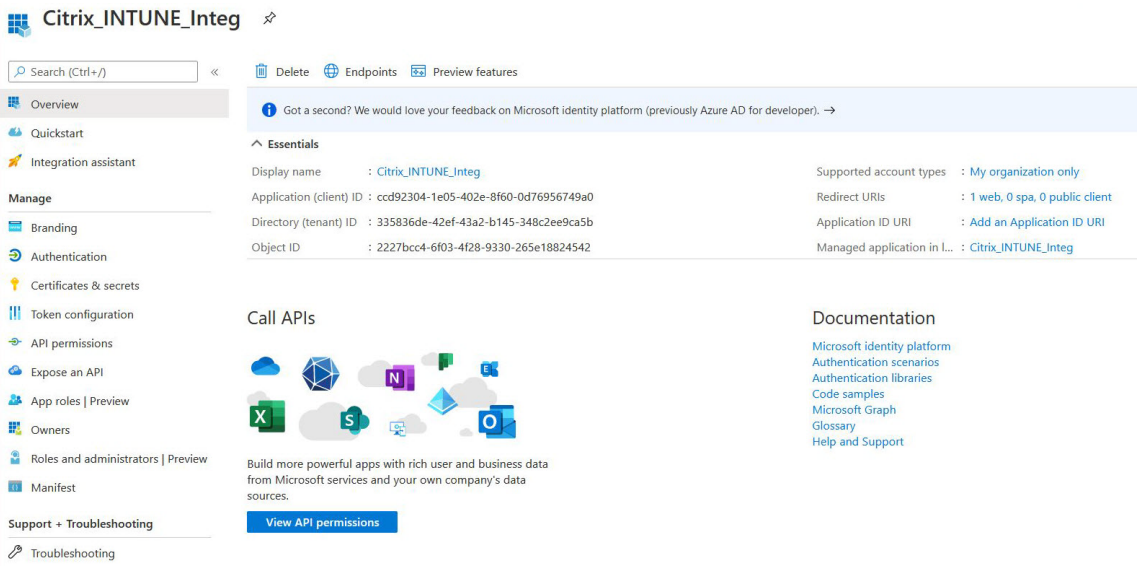
4. Sur la page **Enregistrer une application**, saisissez le nom d'une application et cliquez sur **Enregistrer**.



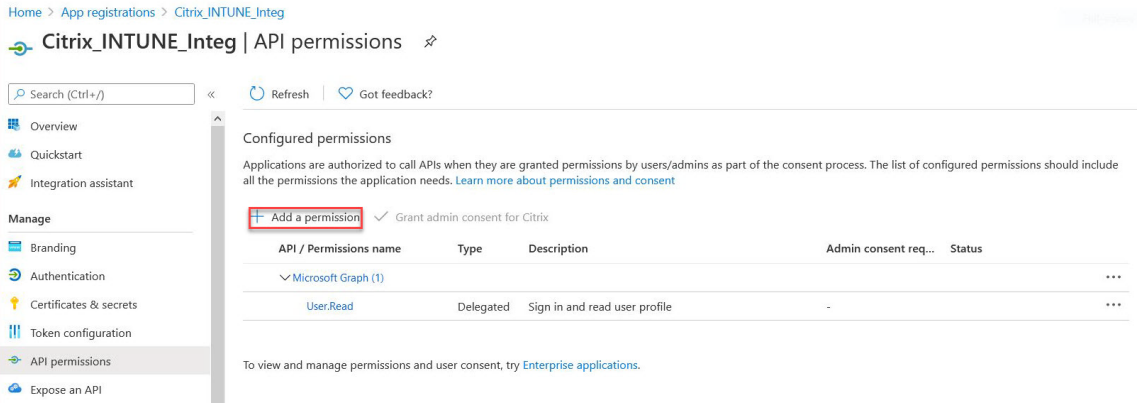
5. Accédez à **Authentification**, cliquez sur **Ajouter un URI**, saisissez FDQN pour NetScaler Gateway, puis cliquez sur **Enregistrer**.



6. Accédez à la page **Vue d'ensemble** pour obtenir l'ID client, l'ID de client et l'ID d'objet.



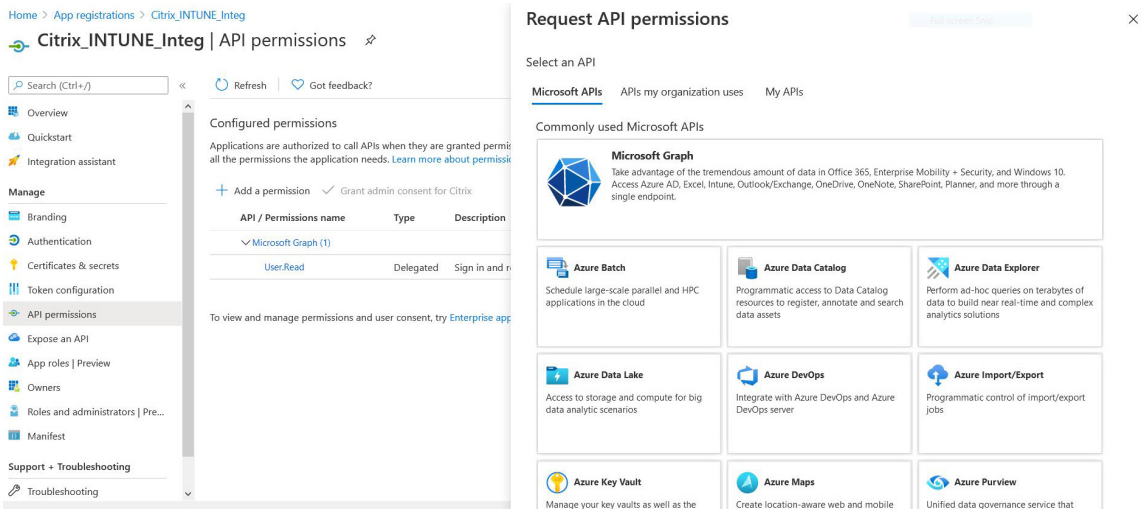
7. Accédez à **Autorisations API** et cliquez sur **Ajouter une autorisation**.



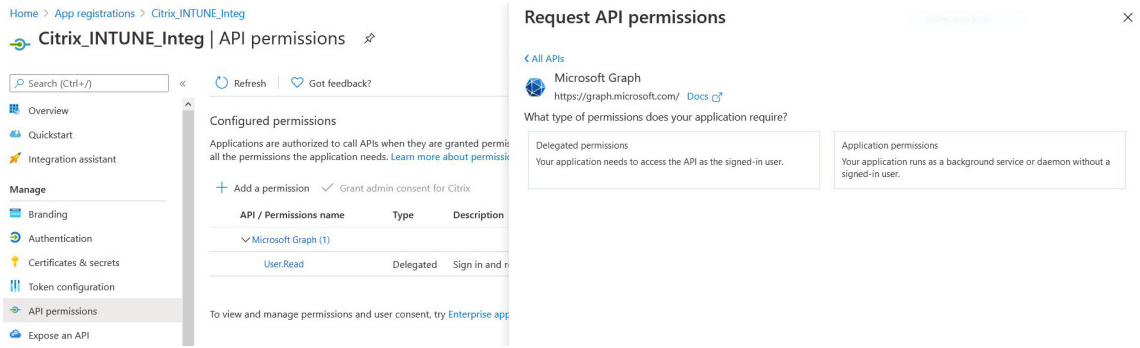
> **Remarque :**
>
> Toutes les applications Azure AD qui appellent les points de terminaison de service,`https://login.microsoftonline.com`,`https://graph.microsoft.com` ou `https://graph.windows.net` nécessitent que l'autorisation d'API soit attribuée pour que la passerelle puisse appeler l'API NAC. Les autorisations API disponibles sont les suivantes :
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> L'autorisation préférée est **Application.Read.All**.
>
> Pour plus de détails, consultez https://techcommunity.microsoft.com/t5/intune-cust

> omer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040

8. Cliquez sur la vignette **Microsoft Graph** pour configurer les autorisations d'API pour Microsoft Graph.

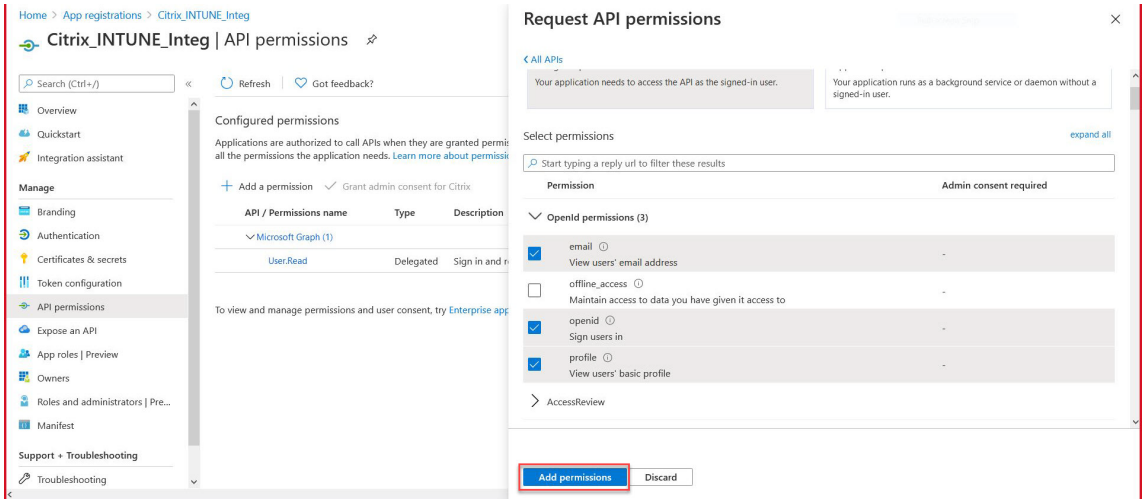


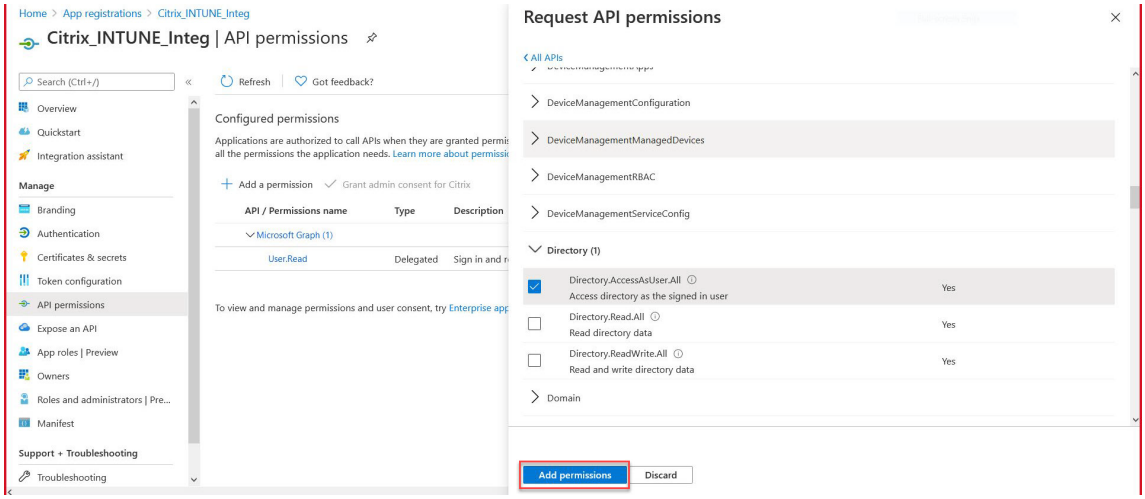
9. Cliquez sur la vignette **Autorisations déléguées**.

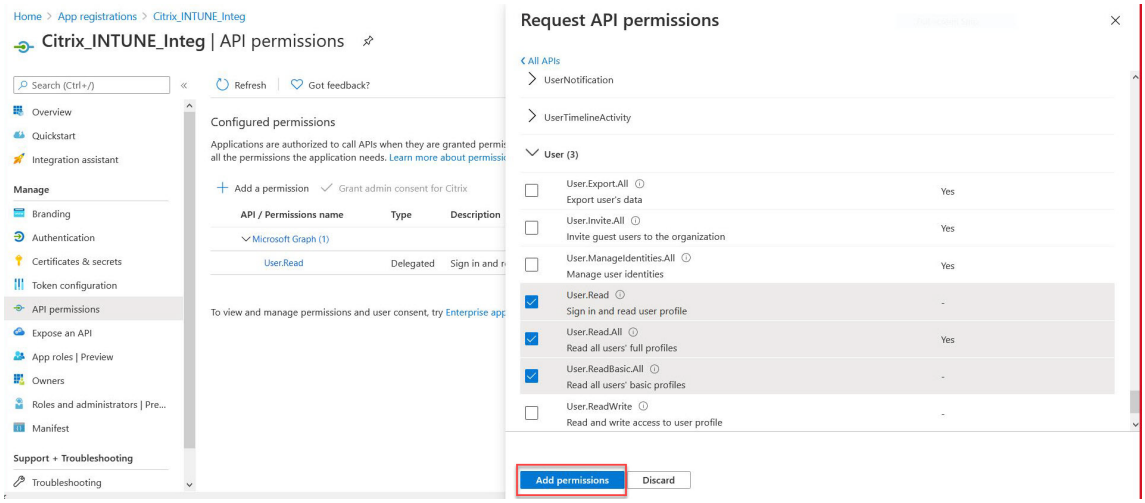


10. Sélectionnez les autorisations suivantes, puis cliquez sur **Ajouter des autorisations**.

    - E-mail
    - `openid`
    - Profile
    - Directory.AccessAsUser.All
    - User.Read
    - User.Read.All
    - User.ReadBasic.All



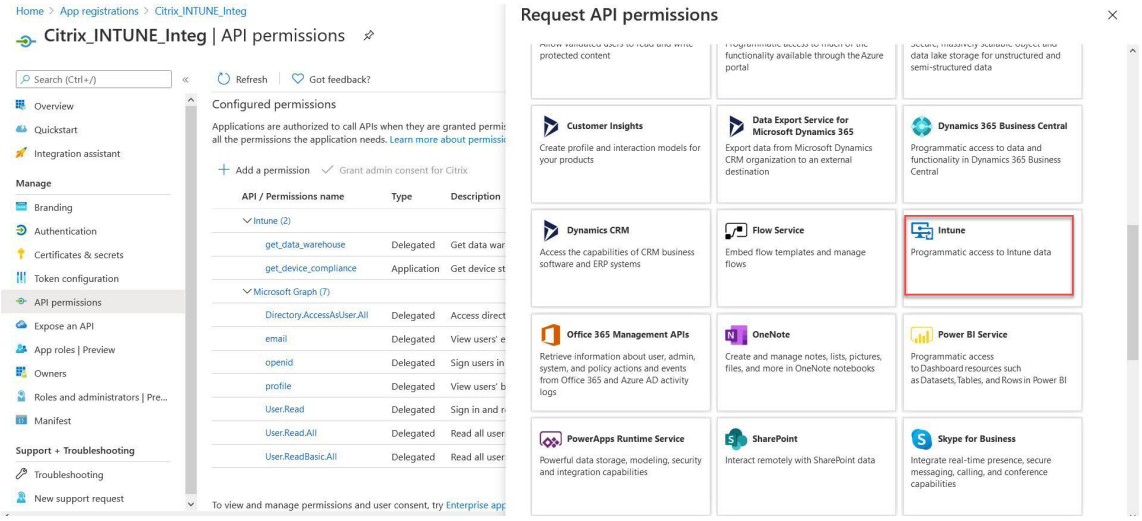




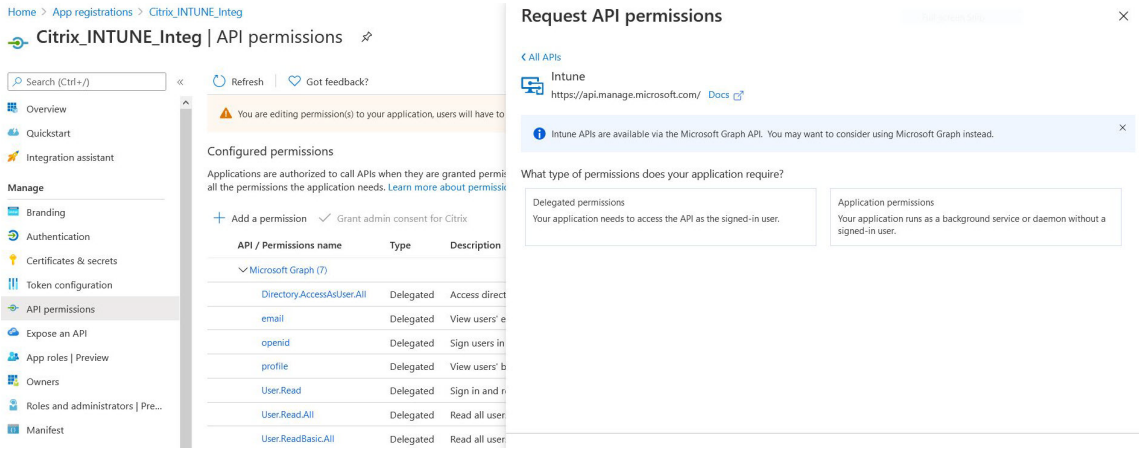
> **Autorisations pour la vérification NAC Intune :**
>
> toutes les applications Azure AD qui appellent les points de terminaison du service,`https://login.microsoftonline.com` `https://graph.microsoft.com` ou

> `https://graph.windows.net` nécessitent l'autorisation d'API à attribuer pour que la passerelle puisse appeler l'API NAC. Les autorisations API disponibles sont les suivantes :
>
> - Application.Read.All
> - Application.ReadWrite.All
> - Application.OwnedBy
> - Directory.Read.All
>
> L'autorisation préférée est **Application.Read.All**.
>
> Pour plus de détails, voir https://techcommunity.microsoft.com/t5/intune-customer-success/support-tip-intune-service-discovery-api-endpoint-will-require/ba-p/2428040
>
> **Remarque :**
>
> si un client utilise uniquement la vérification Intune Action pour NAC, la seule autorisation requise est **Application.Read.All** dans Microsoft Graph.

11. Cliquez sur la vignette **Intune** pour configurer les autorisations d'API pour Intune.



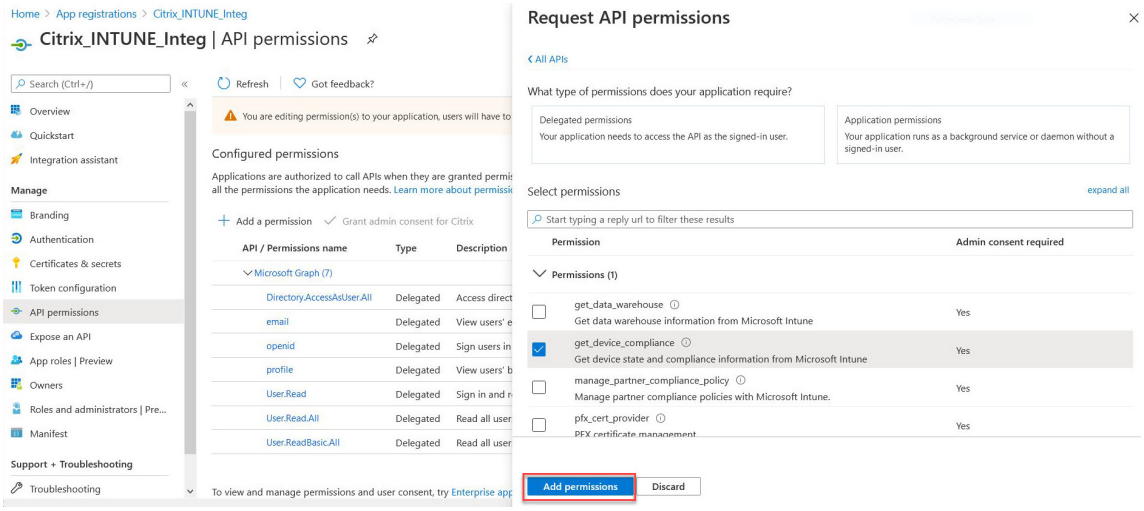
12. Cliquez sur la vignette **Autorisations de l'application** et sur la vignette **Autorisations déléguées** pour ajouter des autorisations pour Get_Device_Compliance et Get_Data_Warehouse respectivement.

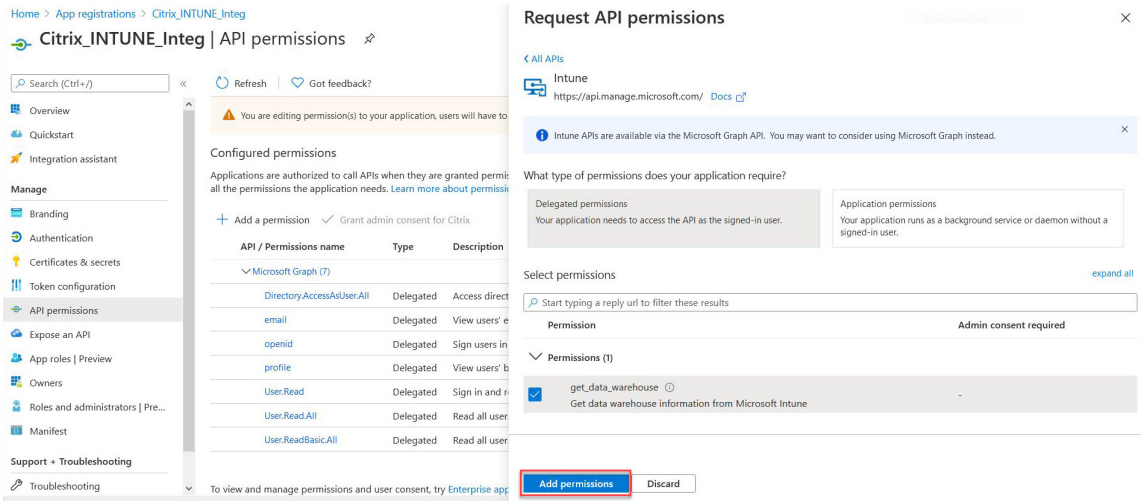


13. Sélectionnez les autorisations suivantes, puis cliquez sur **Ajouter des autorisations**.

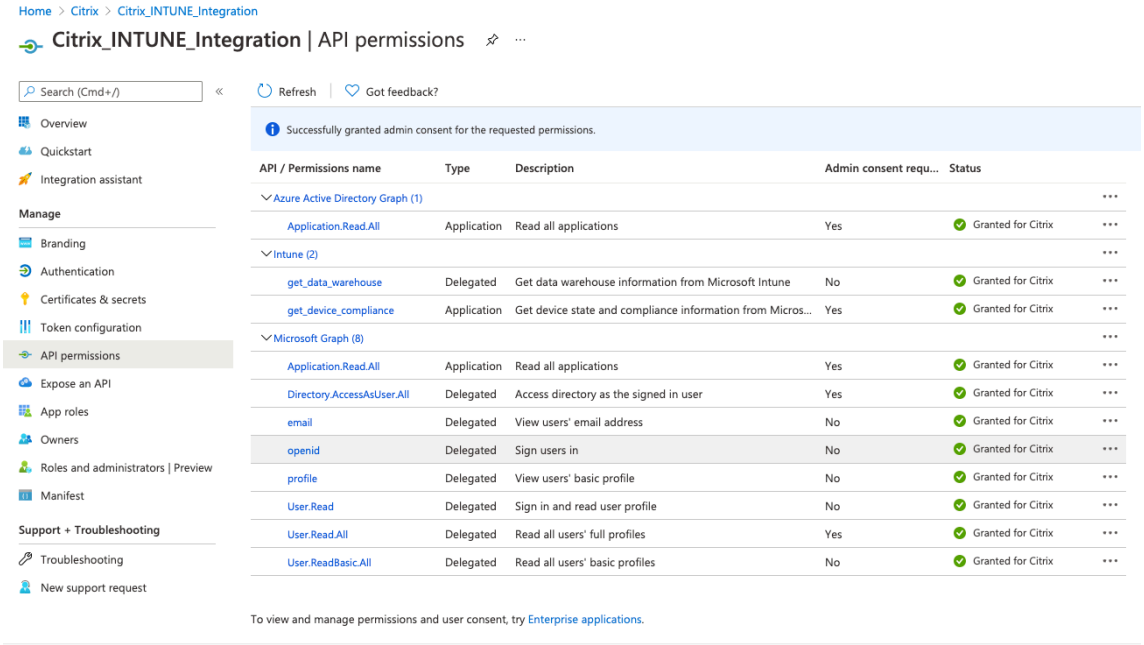
    - Get_Device_Compliance - Autorisations des applications
    - Get_Data_Warehouse - Autorisations déléguées

> **Remarque :**
>
> Pour la vérification NAC Intune, la seule autorisation requise est **Get_Device_Compliance**.

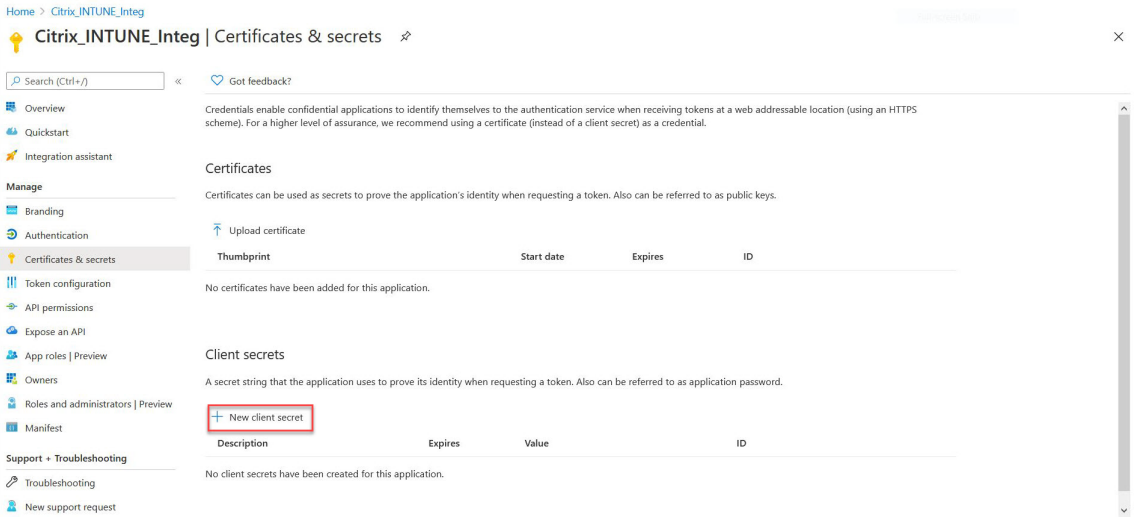




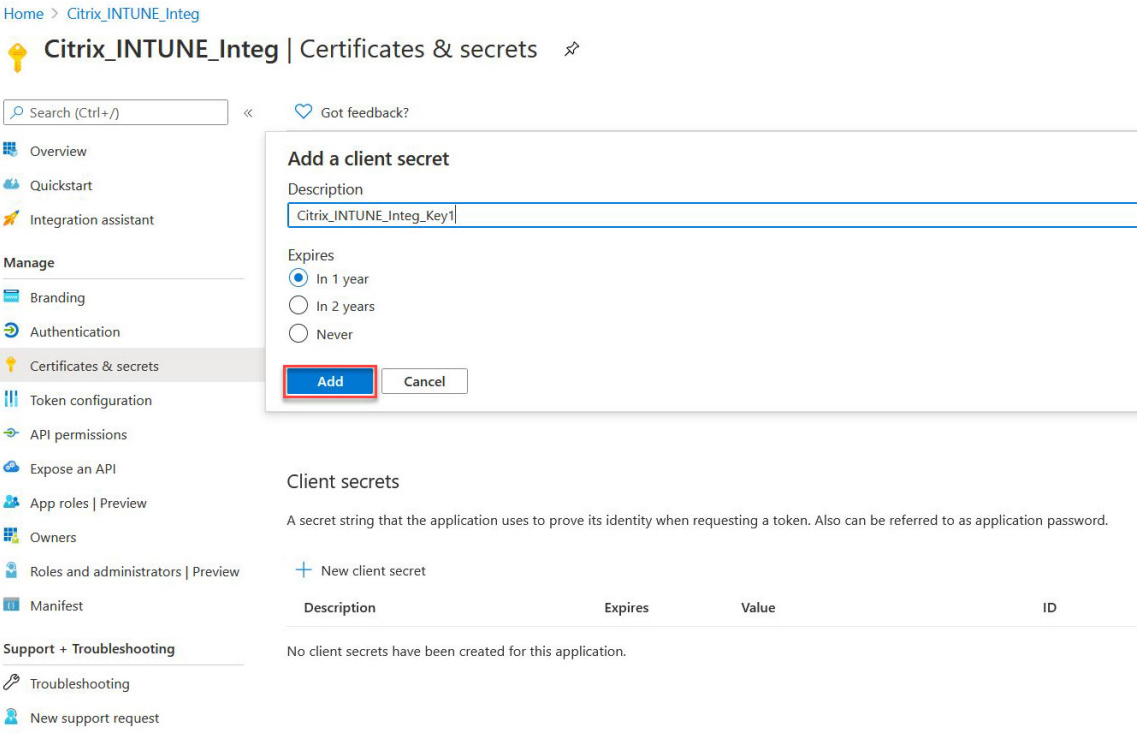
14. La page suivante répertorie les autorisations API configurées.



15. Accédez à **Certificats et secrets**, puis cliquez sur **Nouveau secret client**.

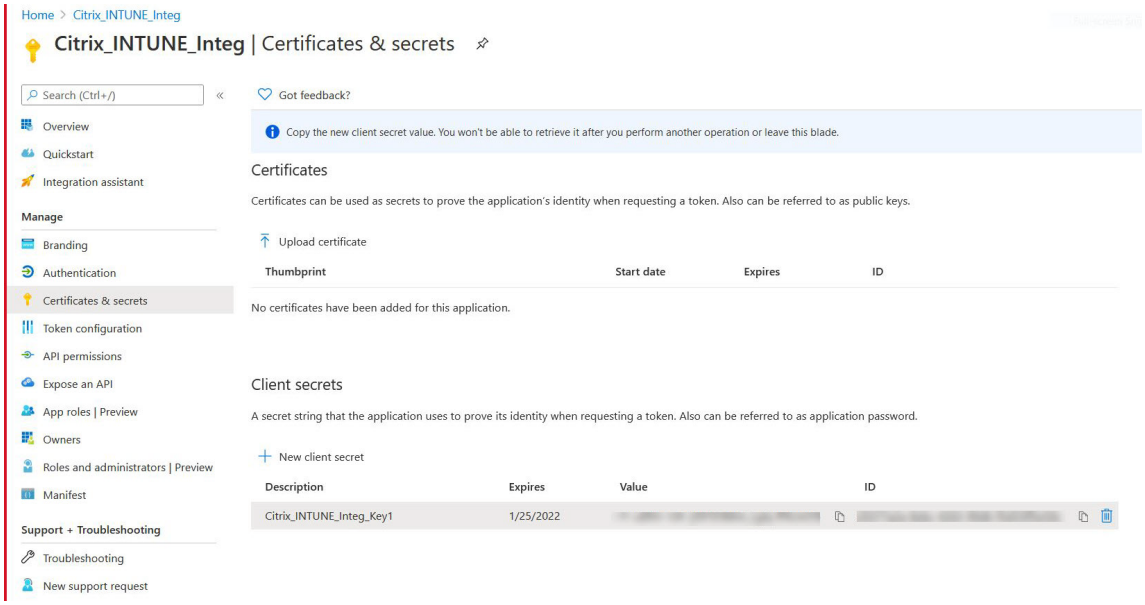


16. Dans la page **Ajouter un secret client**, saisissez une description, sélectionnez expiration, puis cliquez sur **Ajouter**.



17. L'écran suivant affiche le secret client configuré.

> **Remarque**
>
> Le secret client n'est affiché qu'une seule fois lors de sa génération. Copiez localement le secret client affiché. Utilisez le même secret client ainsi que l'ID client associé à l'application nouvellement enregistrée lors de la configuration de l'action OAuth sur l'appliance NetScaler Gateway pour Intune.



La configuration de l'application sur le portail Azure est maintenant terminée.

Présentation de l'authentification par jeton Azure ADAL

March 27, 2024

Voici le déroulement des événements d'une authentification par jeton ADAL classique entre NetScaler Gateway-Microsoft :

1. Lorsqu'une application est lancée sous iOS ou Android, elle contacte Azure. L'utilisateur est invité à ouvrir une session avec ses informations d'identification. Une fois l'ouverture de session réussie, l'application reçoit un jeton ADAL.

2. Ce jeton ADAL est présenté à un NetScaler Gateway, qui a été configuré pour valider le jeton ADAL.

3. NetScaler Gateway valide la signature du jeton ADAL avec le certificat correspondant de Microsoft.

4. Après une validation réussie, NetScaler Gateway extrait le nom principal (UPN) de l'utilisateur et accorde à l'application un accès VPN aux ressources internes.

Configuration du serveur virtuel NetScaler Gateway pour l'authentification par jeton Microsoft ADAL

March 27, 2024

Pour configurer un serveur virtuel NetScaler Gateway afin de surveiller l'authentification par jeton Microsoft ADAL, vous avez besoin des informations suivantes :

- **CertEndpoint** : URL du point de terminaison qui contient la clé Web JSON (JWK) pour la vérification du jeton ADAL.
- **Public** : FQDN du serveur virtuel NetScaler auquel l'application envoie le jeton ADAL.
- **Emetteur** : nom de l'émetteur AAD. Cette propriété est renseignée par défaut.
- **TenanTid** : ID de locataire pour l'enregistrement Azure ADAL.
- **ClientID** : ID unique attribué à l'application Gateway dans le cadre de l'enregistrement ADAL.
- **ClientSecret :** clé secrète transmise à l'application Gateway dans le cadre de l'enregistrement ADAL.
- **ResourceURI** : paramètre facultatif pour capturer l'URI de la ressource. S'il n'est pas configuré, NetScaler utilise l'URI de la ressource commerciale Azure.

Effectuez les étapes suivantes à l'aide de l'interface de ligne de commande :

1. Créez une action OAuth.

```
1 add authentication OAuthAction <oauth-action-name> -OAuthType <
    INTUNE>  – clientid <clientID> -clientsecret <client-secret> -
    audience <audience name> -tenantid <tenantID> -issuer <issuer-
    name> -userNameField <upn> -certEndpoint <certEndpoint-name> -
    resourceURI <name of resource URI>
2 <!--NeedCopy-->
```

2. Créez une stratégie d'authentification à associer à l'action OAuth nouvellement créée.

```
1 add authentication Policy <policy-name> -rule <true> -action <
    oauth intune action>
2 <!--NeedCopy-->
```

3. Liez l'OAuth nouvellement créé à AuthVS.

```
1 bind authentication vserver <auth-vserver> -policy <oauth-intune-
    policy> -priority 2 -gotoPriorityExpression END
2 <!--NeedCopy-->
```

4. Créez un schéma de connexion.

```
1 add authentication loginSchema <loginSchemaName> -
    authenticationSchema <authenticationSchema ” location ” >
```



```
2 add authentication loginSchemaPolicy <loginSchemaPolicyName> -rule
      true -action <loginSchemaName>
3 <!--NeedCopy-->
```

5. Liez AuthVS avec LoginSchema.

```
1 bind authentication vserver <auth-vs> -policy <oauth-pol> -
     priority 2 -gotoPriorityExpression END
2 <!--NeedCopy-->
```

6. Ajoutez un profil d'authentification et attribuez-le à un serveur virtuel VPN.

```
1 add authnprofile <nfactor-profile-name> -authnvsName <authvserver>
2 set vpn vserver <vserver-name> -authnprofile <nfactor-profile-name
      >
3 <!--NeedCopy-->
```

Exemple de configuration

```
1  add authentication OAuthAction tmp-action -OAuthType INTUNE -clientid
      id 1204 -clientsecret a -audience "[http://hello](http://hello/)" -
      tenantid xxxx -issuer "[https://hello](https://hello/)" -
      userNameField upn -certEndpoint https://login.microsoftonline.com/
      common/discovery/v2.0/keys --resourceURI htpps://api.manage.
      microsoft.com
2
3  add authentication Policy oauth-intune-pol -rule true -action tmp-
      action
4  bind authentication vserver auth-vs-for-gw1-intune -policy oauth-pol -
      priority 2 -gotoPriorityExpression END
5
6  add authentication loginSchema oauth-loginschema -authenticationSchema
      "/nsconfig/loginschema/LoginSchema/OnlyOAuthToken.xml"
7
8  add authentication loginSchemaPolicy oauth-loginschema-pol -rule true -
      action oauth-loginschema `
9
10 bind authentication vserver auth-vs-for-gw1-intune -policy oauth-
      loginschema-pol -priority 2 -gotoPriorityExpression END
11
12 add authnprofile nfactor-prof-intune -authnvsName auth-vs-for-gw1-
      intune
13
14 set vpn vserver gw1-intune-authnprofile nfactor-prof-intune
15 <!--NeedCopy-->
```


Configurer NetScaler Gateway pour utiliser un micro VPN avec Microsoft Endpoint Manager

March 27, 2024

L'intégration de Citrix Micro VPN avec Microsoft Endpoint Management permet à vos applications d'accéder aux ressources locales. Pour plus d'informations, consultez la section Intégration de Citrix Micro VPN avec Microsoft Endpoint Manager.

Configuration système requise

- Versions de NetScaler Gateway
  - 13.1
  - 13.0
  - 12.1.50.x ou version ultérieure
  - 12.0.59.x ou version ultérieure

  Vous pouvez télécharger la dernière version de NetScaler Gateway depuis la page de téléchargement de NetScaler Gateway.
- Un bureau Windows exécutant Windows 7 ou version ultérieure (pour encapsuler les applications Android uniquement)
- Microsoft
  - Accès Azure AD (avec privilèges d'administrateur de locataires)
  - Locataire activé par Intune
- Règles de pare-feu
  - Activer une règle de pare-feu pour le trafic SSL provenant d'une adresse IP de sous-réseau NetScaler Gateway vers,`*.manage.microsoft.com` `https://login.microsoftonline.com` et `https://graph.windows.net` (port 443)
  - NetScaler Gateway doit être capable de résoudre de manière externe les URL précédentes.

Pré-requis

- **Environnement Intune :** si vous n'avez pas d'environnement Intune, configurez-en un. Pour obtenir des instructions, consultez la documentation Microsoft.

- **Application Edge Browser :** Le SDK Micro VPN est intégré à l'application Microsoft Edge et à l'application Intune Managed Browser pour iOS et Android. Pour plus d'informations sur Managed Browser, consultez la page Managed Browser de Microsoft.
- **Droits Citrix Endpoint Management : assurez-vous de disposer d'un droit**Citrix Endpoint Management actif pour bénéficier d'une prise en charge continue du SDK micro VPN sur un navigateur mobile Microsoft Edge (iOS et Android). Pour plus d'informations, contactez le représentant de votre service commercial, de votre compte ou de votre partenaire.

Accorder des autorisations d'application Azure Active Directory (AAD)

1. Consentement à l'application Citrix multitenant AAD pour permettre à NetScaler Gateway de s'authentifier auprès du domaine AAD. L'administrateur global Azure doit visiter l'URL suivante et donner son consentement :

   https://login.windows.net/common/adminconsent?client_id=b6a53a76-5d50-499e-beb3-c8dbdad5c40b&redirect_uri=https://www.citrix.com&state=consent.

2. Autorisation à l'application Citrix multitenant AAD d'autoriser les applications mobiles à s'authentifier avec le micro VPN NetScaler Gateway. Ce lien n'est requis que si l'administrateur mondial Azure a modifié la valeur par défaut pour que les utilisateurs puissent inscrire des applications de Oui à Non.
   Ce paramètre se trouve dans le portail Azure sous **Azure Active Directory > Utilisateurs > Paramètres utilisateur**.
   L'administrateur global Azure doit visiter l'URL suivante et donner son consentement (ajoutez votre ID de
   locataire) https://login.microsoftonline.com/%5Btenant_id%5D/adminconsent?client_id=9215b80e-186b-43a1-8aed-9902264a5af7.

Configuration de NetScaler Gateway pour un micro VPN

Pour utiliser un micro VPN avec Intune, vous devez configurer NetScaler Gateway pour vous authentifier auprès d'Azure AD. Un serveur virtuel NetScaler Gateway existant ne fonctionne pas pour ce cas d'utilisation.
Tout d'abord, configurez Azure AD pour qu'il se synchronise avec le répertoire Active Directory local. Cette étape est nécessaire pour garantir que l'authentification entre Intune et NetScaler Gateway s'effectue correctement.

Télécharger le script : Le fichier .zip inclut un fichier Lisez-moi contenant des instructions pour implémenter le script. Vous devez saisir manuellement les informations requises par les scripts et exécuter le script sur NetScaler Gateway pour configurer le service. Vous pouvez télécharger le fichier script depuis la page de téléchargement de NetScaler.

> **Important :** Une fois que vous avez terminé la configuration de NetScaler Gateway et si vous voyez un état OAuth différent de COMPLETE, consultez la section Résolution des problèmes.

Configuration du navigateur Microsoft Edge

1. Connectez-vous à,https://endpoint.microsoft.com/ puis accédez à **Intune > Applications mobiles**.
2. Publiez l'application Edge comme vous le faites normalement, puis ajoutez une stratégie de configuration d'application.
3. Sous **Gérer**, cliquez sur **Stratégies de configuration des applications**.
4. Cliquez sur **Ajouter**, puis entrez un nom pour la stratégie que vous souhaitez créer. Dans **Type d'inscription de l'appareil**, sélectionnez **Applications gérées**.
5. Cliquez sur **Application associée.**
6. Sélectionnez les applications auxquelles vous souhaitez appliquer la stratégie (navigateur géré Microsoft Edge ou Intune), puis cliquez sur **OK**.
7. Cliquez sur **Paramètres de configuration**.
8. Dans le champ **Nom**, saisissez le nom de l'une des stratégies répertoriées dans le tableau suivant.
9. Dans le champ **Valeur**, entrez la valeur à appliquer pour cette stratégie. Cliquez sur le champ pour ajouter la stratégie à la liste. Vous pouvez ajouter plusieurs stratégies.
10. Cliquez sur **OK**, puis sur **Ajouter**.

La stratégie est ajoutée à votre liste de stratégies.

Nom (iOS /Android)	Valeur	Description
—	—	—
MvpnGatewayAddress	`https://external.companyname.com`	URL externe de votre NetScaler Gateway
MvpnNetworkAccess	MvpnNetworkAccessTunneledWebSSOor Unrestricted	MvpnNetworkAccessTunneledWebSS est la valeur par défaut pour le tunneling.
MvpnExcludeDomains	Liste des noms de domaine à exclure, séparés par des virgules	Facultatif. Default=Blank
TunnelExcludeDomains	Utilisez cette propriété client pour remplacer la liste par défaut des domaines exclus. Défaut=`app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream.launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com`

> **Remarque :** L'SSO Web est le nom de la Secure Browse dans les paramètres. Le comportement est le même.

- **MvpnNetworkAccess** : MvpnNetworkAccessTunneledWebSSO permet la redirection HTTP/HTTPS via Netscaler Gateway, également connue sous le nom de Tunneled-Web SSO. La passerelle répond aux défis de l'authentification HTTP en ligne, offrant ainsi une expérience d'authentification unique (SSO). Pour utiliser l'SSO Web, définissez cette stratégie sur **MvpnNetworkAccessTunneledWebSSO**. La redirection complète du tunnel n'est actuellement pas prise en charge. Utilisez l'**option Sans restriction** pour désactiver le tunneling micro VPN.
- **MVPNExcludeDomains** : liste séparée par des virgules de noms d'hôtes ou de domaines à exclure du routage via le proxy Web inverse NetScaler Gateway. Les noms d'hôte ou de domaine sont exclus même si les paramètres DNS fractionnés configurés par NetScaler Gateway pourraient autrement sélectionner le domaine ou l'hôte.

  > **Remarque :**
  >
  > - Cette stratégie n'est appliquée que pour les connexions **MVPNNetworkAccessTunneledWebSSO**. Si cette `MvpnNetworkAccess` option **n'est pas restreinte**, cette stratégie est ignorée.
  > - Cette stratégie s'applique uniquement au mode Tunneled-Web SSO avec NetScaler Gateway configuré pour le split tunneling inversé.

- **TunnelExcludeDomains** - Par défaut, MDX exclut certains points de terminaison de service du tunneling micro VPN. Les kits SDK des applications mobiles et les applications utilisent ces points de terminaison de service pour diverses fonctionnalités. Par exemple, les points de terminaison des services incluent des services qui ne nécessitent pas de routage via les réseaux d'entreprise, tels que Google Analytics, les services Citrix Cloud et les services Active Directory. Utilisez cette propriété client pour remplacer la liste par défaut des domaines exclus.

  Pour configurer cette politique client globale, sur la console Microsoft Endpoint Management, accédez à **Paramètres > Propriétés du client**, ajoutez la clé personnalisée **TUNNEL_EXCLUDE_DOMAINS**et définissez la valeur.

  Valeur : pour remplacer la liste par défaut par les domaines que vous souhaitez exclure du tunneling, saisissez une liste de suffixes de domaines séparés par des virgules. Pour inclure tous les domaines dans le tunneling, entrez none. La valeur par défaut est :

  ```
  app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis
  -test.citrix.com,clientstream.launchdarkly.com,crashlytics.com
  ,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com,
  hockeyapp.net,mobile.launchdarkly.com,pushreg.xm.citrix.com,rttf
  ```



```
.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.
google-analytics.com,stream.launchdarkly.com
```

Dépannage

Problèmes d'ordre général

Problème	Résolution
Le message « Ajouter une stratégie requise » s'affiche lorsque vous ouvrez une application	Ajouter des stratégies dans l'API Microsoft Graph
Il y a des conflits de stratégie	Une seule stratégie par application est autorisée
Le message « Échec du package de l'application » s'affiche lors de l'encapsulation d'une application. Pour obtenir le message complet, reportez-vous au tableau suivant	L'application est intégrée au SDK Intune. Il n'est pas nécessaire d'encapsuler l'application avec Intune
Votre application ne peut pas se connecter aux ressources internes	Assurez-vous que les ports de pare-feu appropriés sont ouverts, que vous avez corrigé l'ID de locataire, etc.

Message d'erreur Echec du package de l'application :

Échec de la mise en package de l'application. com.microsoft.Intune.mam.AppPackager.utils.AppPackagerException :
le
SDK MAM est déjà intégré à cette application.
com.microsoft.intune.mam.apppackager.AppPackager.packageApp(AppPackager.java:113)
com.microsoft.intune.mam.apppackager.PackagerMain.mainInternal(PackagerMain.java:198)
com.microsoft.intune.mam.apppackager.PackagerMain.main(PackagerMain.java:56)
The application cannot be wrapped.

Problèmes liés à NetScaler Gateway

Problème	Résolution
Les autorisations requises pour être configurées pour l'application passerelle sur Azure ne sont pas disponibles.	Vérifiez si une licence Intune appropriée est disponible. Essayez d'utiliser le portail manage.windowsazure.com pour voir si l'autorisation peut être ajoutée. Contactez le support technique Microsoft si le problème persiste.
NetScaler Gateway ne peut pas atteindre. `login.microsoftonline.com and graph.windows.net`	À partir de NS Shell, vérifiez si vous êtes en mesure d'accéder au site Web Microsoft suivant : cURL -v -k https://login.microsoftonline.com. Vérifiez ensuite si le DNS est configuré sur NetScaler Gateway. Vérifiez également que les paramètres du pare-feu sont corrects (dans le cas où les demandes DNS sont pare-feu).
Une erreur apparaît dans ns.log après la configuration de OAuthAction.	Vérifiez si la licence Intune est activée et si l'application de passerelle Azure dispose des autorisations appropriées.
La commande Sh OAuthAction n'affiche pas l'état OAuth comme terminé.	Vérifiez les paramètres DNS et les autorisations configurées sur l'application de passerelle Azure.
L'appareil Android ou iOS n'affiche pas l'invite d'authentification double.	Vérifiez si l'ID d'appareil à double facteur LogonSchema est lié au serveur virtuel d'authentification.

État et état d'erreur de NetScaler Gateway OAuth

État	Condition d'erreur
AADFORGRAPH	Secret non valide, URL non résolue, expiration de la connexion
MDMINFO	`*manage.microsoft.com`est en panne ou inaccessible
GRAPH	Le point de terminaison graphique est inaccessible

État	Condition d'erreur
CERTFETCH	Communication impossible avec Token Endpoint: https://login.microsoftonline.com en raison d'une erreur DNS. Pour valider cette configuration, accédez à l'interpréteur de commandes et tapez cURL https://login.microsoftonline.com. Cette commande doit être validée.

Remarque : Lorsque l'état OAuth est réussi, l'état est affiché comme COMPLETE.

Prise en charge étendue d'Azure AD Graph

March 27, 2024

Comme Azure AD Graph est obsolète, les clients qui déclenchent une nouvelle application ne peuvent pas utiliser les autorisations précédentes qui étaient disponibles avec le graphe Azure AD. Toutefois, les clients disposant d'applications existantes qui souhaitent utiliser les anciennes autorisations d'Azure AD Graph pendant un certain temps peuvent continuer à le faire en apportant des modifications de configuration sur l'appliance Gateway. Cette configuration est prise en charge dans les versions 13.1-27.xx et ultérieures de NetScaler Gateway.

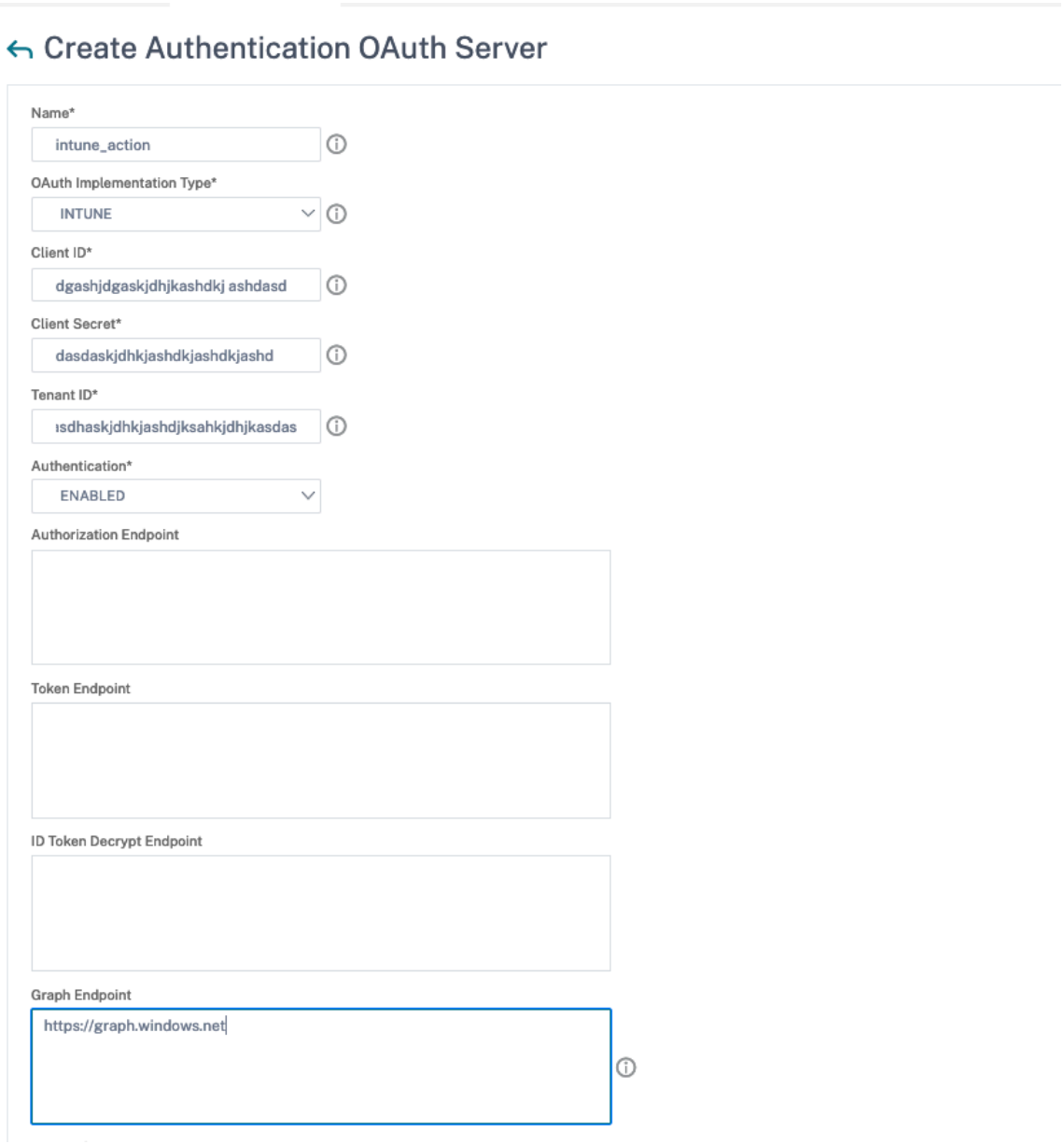
Effectuez les modifications de configuration suivantes sur l'appliance NetScaler Gateway :

1. Dans l'invite de commandes, exécutez la commande suivante.

```
shell nsapimgr_wr.sh -ys call=”ns_intune_enable_old_endpoints”
<!--NeedCopy-->
```

2. Accédez à **Sécurité > Trafic des applications AAA > Stratégies > Authentification > Stratégies avancées > Actions > Actions OAUTH**.

   a) Sélectionnez un serveur OAuth existant.
   b) Cliquez sur **Plus**.
   c) Dans **Graph Endpoint**, assurez-vous que l'URL ressemble à celle affichée sur la figure.



Prise en charge du transport de données éclairé HDX

January 26, 2024

La prise en charge du Enlightened Data Transport (EDT) pour NetScaler Gateway garantit aux utilisateurs exécutant l'application Citrix Workspace une expérience utilisateur haute définition en cours de session sur des bureaux virtuels.

De plus, le chiffrement de bout en bout avec DTLS 1.0 pour la terminaison EDT entre l'application

Citrix Workspace et le VDA est facilité. Pour plus d'informations, consultez la section Prise en charge du protocole DTLS.

NetScaler Gateway compatible EDT offre une bonne expérience utilisateur sur les réseaux locaux et étendus. Avec EDT, vous n'avez besoin d'aucune configuration administrative ou utilisateur lorsque vous passez de l'un à l'autre en itinérance. L'avantage est particulièrement visible dans les réseaux à latence élevée avec une perte de paquets modérée, où l'expérience utilisateur est généralement en retard par rapport aux autres solutions.

Quand utiliser la prise en charge du Enlightened Data Transport

March 27, 2024

Les scénarios suivants illustrent l'utilisation de NetScaler Gateway compatible EDT.

- Un utilisateur souhaite bénéficier d'une expérience aussi bonne que dans un environnement LAN tout en accédant à distance aux ressources de l'entreprise.
- Un utilisateur souhaite bénéficier d'une expérience utilisateur riche en applications virtuelles et en poste de travail sur les réseaux Wi-Fi et cellulaires où la qualité du réseau est médiocre en raison de la congestion, des pertes de paquets élevées et de la latence élevée.

Les points suivants doivent être gardés à l'esprit lorsque vous utilisez EDT.

- Le bouton DTLS au niveau du serveur virtuel est activé par défaut.
- IPv6 avec DTLS n'est pas pris en charge.
- L'appliance peut désormais être configurée pour la fonctionnalité de double saut pour le trafic EDT entre Receiver et VDA. Pour plus d'informations, cliquez sur Déploiement dans une zone démilitarisée à double saut.

Remarque : EDT est pris en charge sur la plate-forme MPX FIPS dans la version 12.1 build 49.xx et ultérieure. Sur les périphériques MPX dotés d'une puce SSL Intel Coleto, EDT est pris en charge à partir de la version 12.1 build 51.16 et ultérieure.

Configurer NetScaler Gateway pour prendre en charge le Enlightened Data Transport et HDX Insight

March 27, 2024

Le trafic EDT via Gateway bénéficie désormais d'une visibilité de bout en bout. La disponibilité de données de visibilité en temps réel et historiques permet à NetScaler ADM de prendre en charge un large éventail de cas d'utilisation.

Les scénarios suivants sont pris en charge :

Scénario	Prise en charge EDT
NetScaler Gateway	Oui
NetScaler Gateway avec haute disponibilité	Oui
NetScaler Gateway avec optimisation de la haute disponibilité (HA)	Oui
NetScaler avec Unified Gateway	Oui
NetScaler Gateway avec GSLB	Oui
NetScaler Gateway avec cluster	Oui
Chiffrement DTLS de l'application Citrix Workspace vers NetScaler Gateway	Oui
Double Secure Ticket Authority (STA) sur NetScaler Gateway	Oui
Délai d'expiration de la session ICA de NetScaler Gateway	Oui
ICA multiflux NetScaler Gateway	Non
Fiabilité des sessions NetScaler Gateway (Port 2598)	Oui
NetScaler Gateway à double saut	Oui
Chiffrement DTLS entre NetScaler et VDA	Oui
HDX Insight	Oui
NetScaler Gateway en mode IPv6	Non
SOCKS NetScaler Gateway (port 1494)	Non
Proxy LAN NetScaler pure (voir remarque)	Non

> **Remarque :**
>
> EDT n'est pas pris en charge si le proxy LAN NetScaler est configuré en mode utilisateur du réseau local ou en mode transparent. Cependant, le protocole TCP est pris en charge. Pour plus d'informations, consultez :

- Configuration du proxy ICA sortant
- Collecte d'analyses HDX Insight pour les utilisateurs de réseaux locaux avec NetScaler à l'aide de SOCKS

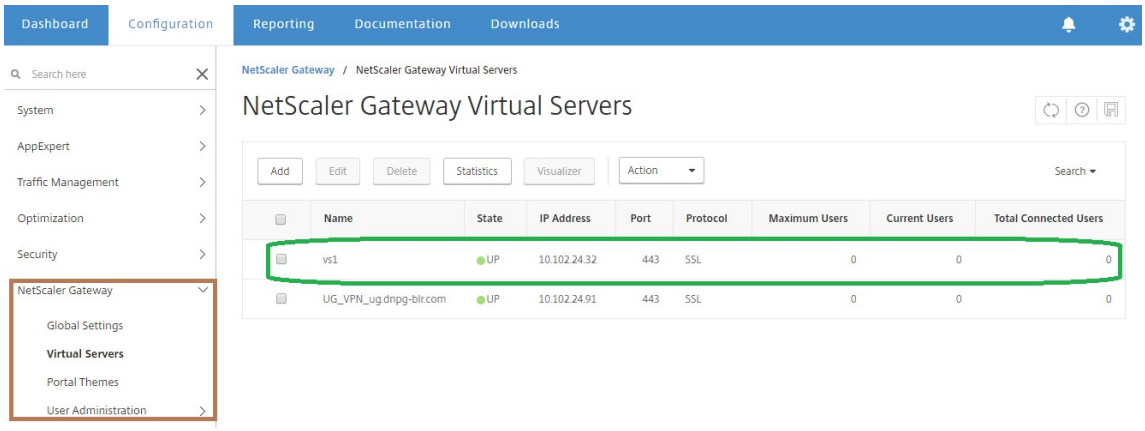
Configurer NetScaler Gateway pour prendre en charge le Enlightened Data Transport

Si vous utilisez Enlightened Data Transport (EDT), Datagram Transport Layer Security (DTLS) doit être activé pour chiffrer la connexion UDP utilisée par EDT. Le paramètre DTLS doit être activé au niveau du serveur virtuel Gateway VPN. De plus, les composants Citrix Virtual Apps and Desktops doivent être correctement mis à niveau et configurés pour obtenir un trafic chiffré entre le serveur virtuel Gateway VPN et la machine utilisateur.

> **Remarque :** Le port UDP (par exemple le port 443) configuré pour le serveur virtuel frontal NetScaler Gateway doit être ouvert dans la DMZ pour que le serveur virtuel reçoive les connexions DTLS. DTLS et CGP sont des conditions préalables à la compatibilité d'EDT avec NetScaler Gateway.

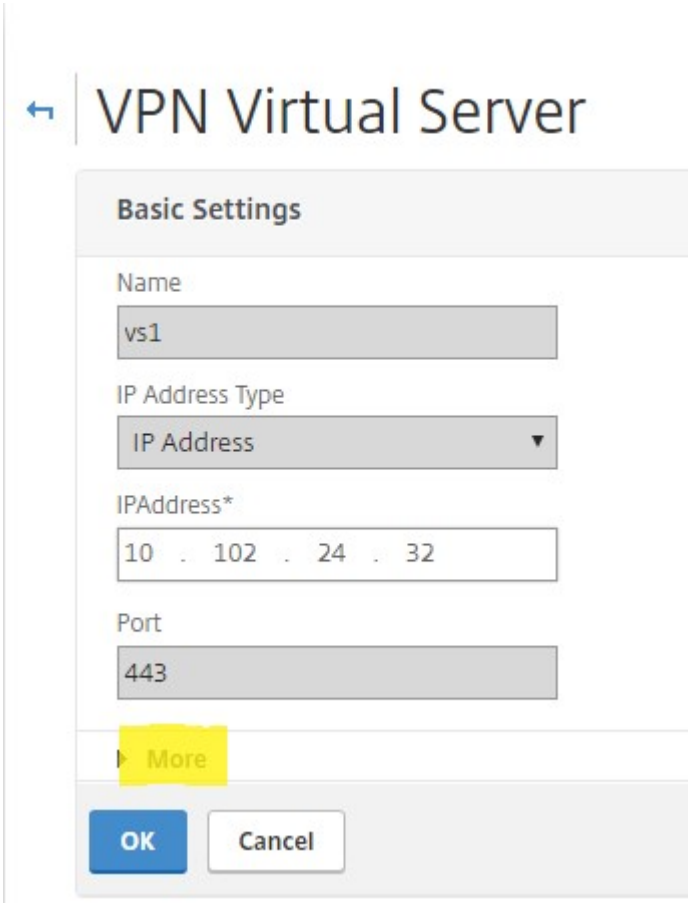
Pour configurer NetScaler Gateway afin qu'il prenne en charge l'EDT à l'aide de l'interface graphique

1. Déployez et configurez NetScaler Gateway pour communiquer avec StoreFront et authentifier les utilisateurs pour Citrix Virtual Apps and Desktops.
2. Dans l'onglet Configuration de l'interface graphique de NetScaler, développez NetScaler **Gateway** et sélectionnez **Virtual Servers**.

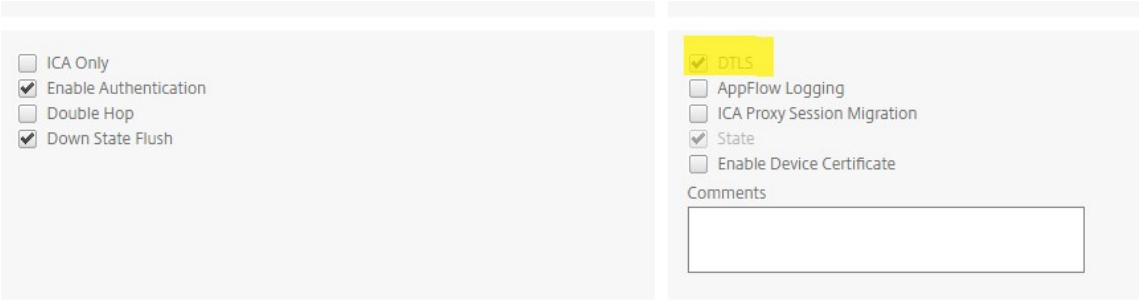


3. Cliquez sur **Modifier** pour afficher les paramètres de base du serveur virtuel VPN, puis vérifiez l'état du paramètre DTLS.

4. Cliquez sur **Plus** pour afficher d'autres options de configuration.



5. Sélectionnez **DTLS** pour assurer la sécurité des communications pour les protocoles de datagramme. Cliquez sur **OK**. La zone **Paramètres de base** du serveur virtuel VPN indique que l'indicateur DTLS est défini sur **True**.



Pour configurer NetScaler Gateway pour le support EDT à l'aide de l'interface de ligne de commande

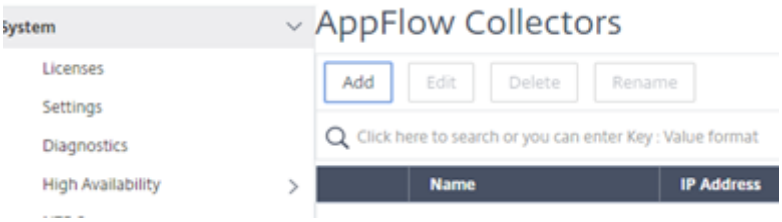
```
set vpn vserver vs1 -DTLS ON
```

Configurer NetScaler Gateway pour prendre en charge HDX Insight

HDX Insight fournit une visibilité de bout en bout du trafic HDX vers les applications et les postes de travail virtuels via NetScaler. Il permet également aux administrateurs d'afficher en temps réel les mesures de latence client et réseau, les rapports historiques, les données de performances de bout en bout et de résoudre les problèmes de performances.

Pour configurer NetScaler Gateway afin qu'il prenne en charge HDX Insight à l'aide de l'interface graphique

1. Dans l'onglet **Configuration**, accédez à **Système > AppFlow>Collecteurs**, puis cliquez sur **Ajouter**.



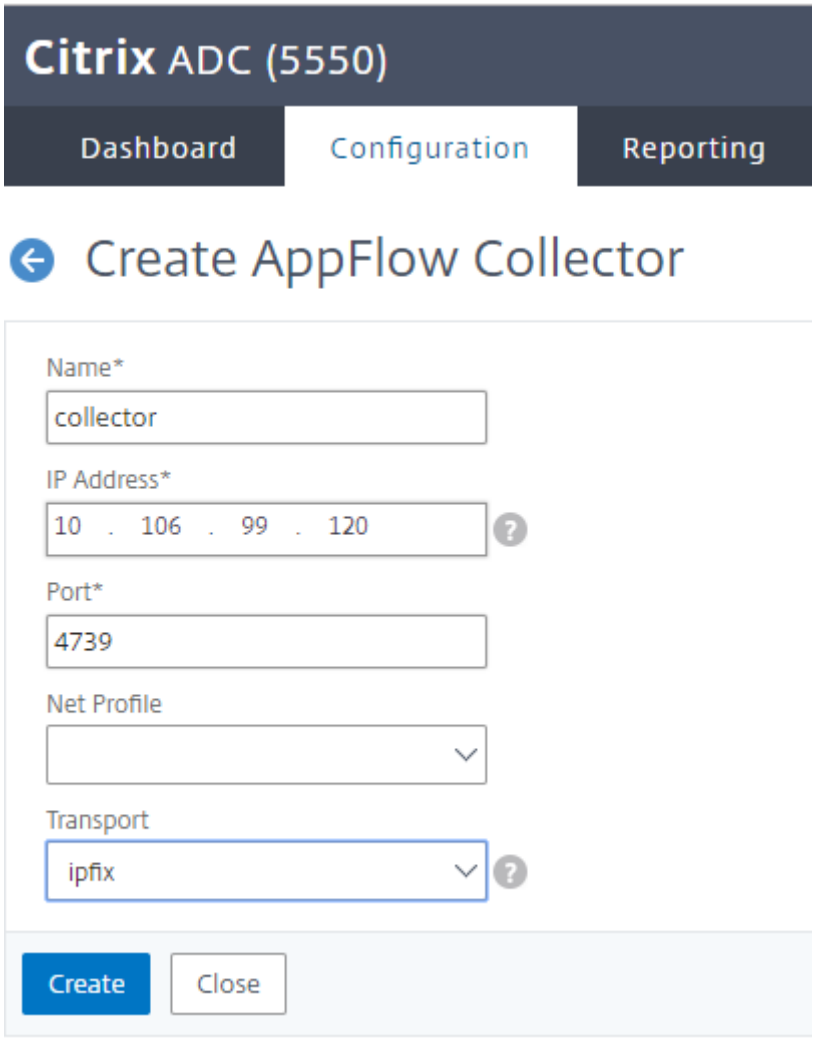
2. Sur la page **Créer un collecteur AppFlow**, renseignez les champs suivants, puis cliquez sur **Créer**.
   Name : nom du collecteur

Adresse IP : adresse IPv4 du collecteur

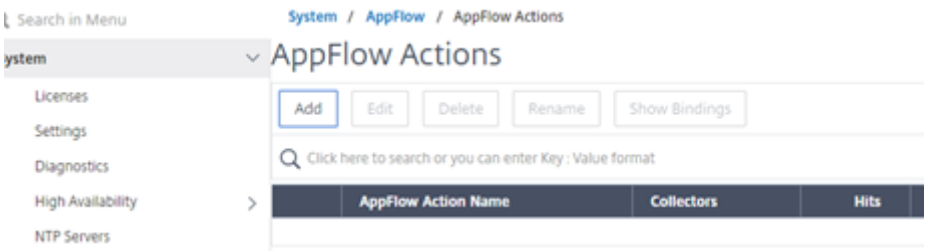
Port : port sur lequel le collecteur écoute

Profil réseau : profil de réseau à associer au collecteur. L'adresse IP définie dans le profil est utilisée comme adresse IP source pour le trafic AppFlow pour ce collecteur. Si vous ne définissez pas ce paramètre, l'adresse IP NetScaler (NSIP) est utilisée comme adresse IP source.

Transport —Type de collecteur de transport.



3. Accédez à **Système > AppFlow>Actions**, puis cliquez sur **Ajouter**.

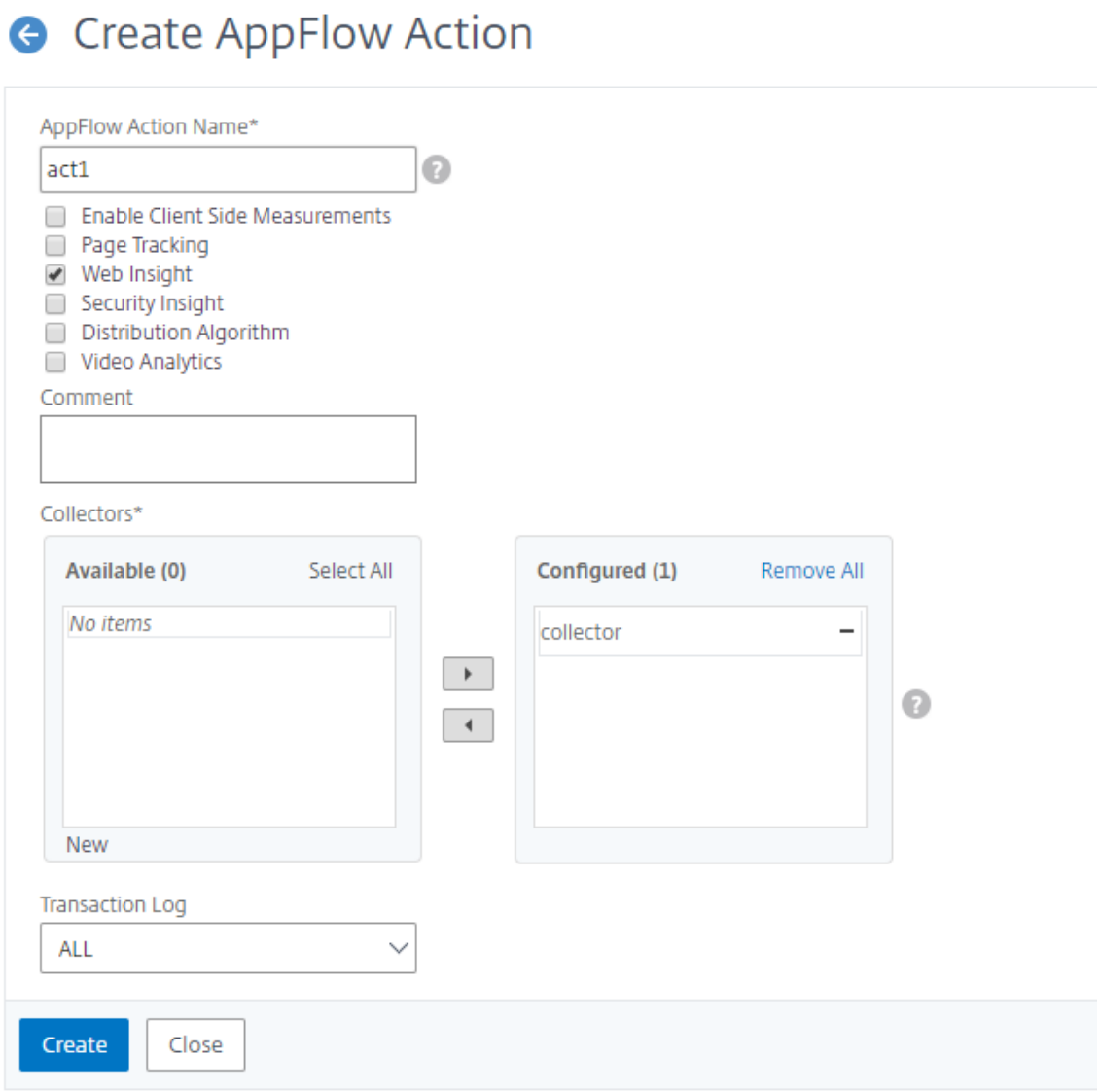


4. Sur la page **Créer une action AppFlow**, renseignez les champs suivants, puis cliquez sur **Créer**.
   Nom de l'action AppFlow : nom de l'action

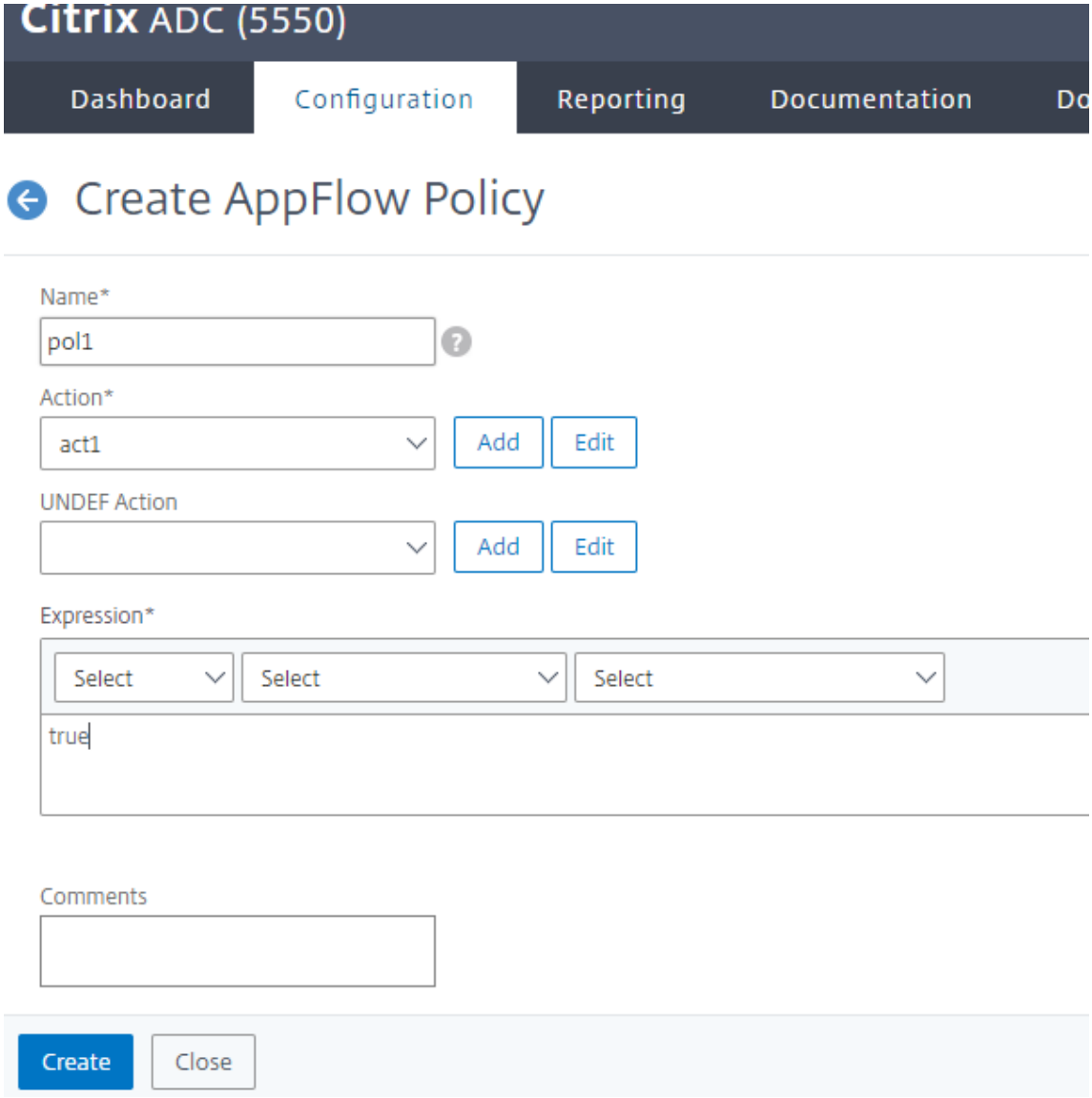
   Commentaire : tout commentaire concernant l'action

   Collecteur : sélectionnez les noms des collecteurs à associer à l'action AppFlow.

   Journal des transactions : type de transactions à consigner.



5. Accédez à **Système > AppFlow > Stratégies**, puis cliquez sur **Ajouter**.



6. Sur la page **Créer une stratégie AppFlow**, remplissez les champs suivants, puis cliquez sur **Créer**.

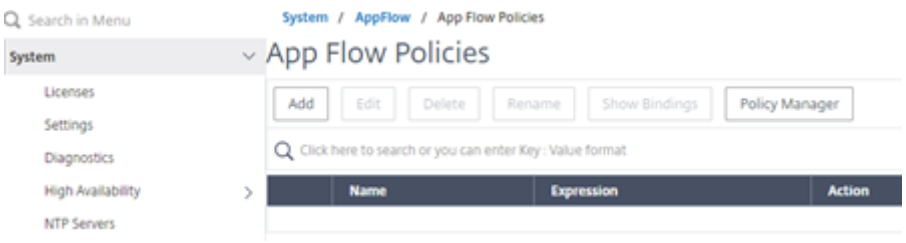
   Nom : nom de la stratégie.

   Action : nom de l'action à associer à la stratégie.

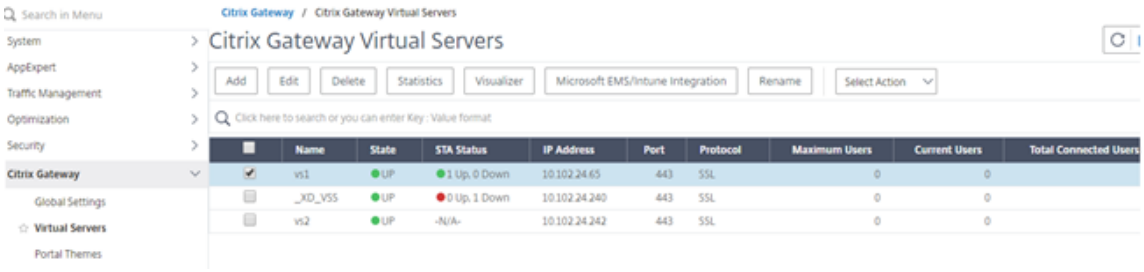
   UNDEF : nom de l'action AppFlow à associer à cette stratégie lorsqu'un événement indéfini se produit.

   Expression : expression ou autre valeur par rapport à laquelle le trafic est évalué. Il doit s'agir d'une expression booléenne.

   Commentaires : tout commentaire concernant cette stratégie.

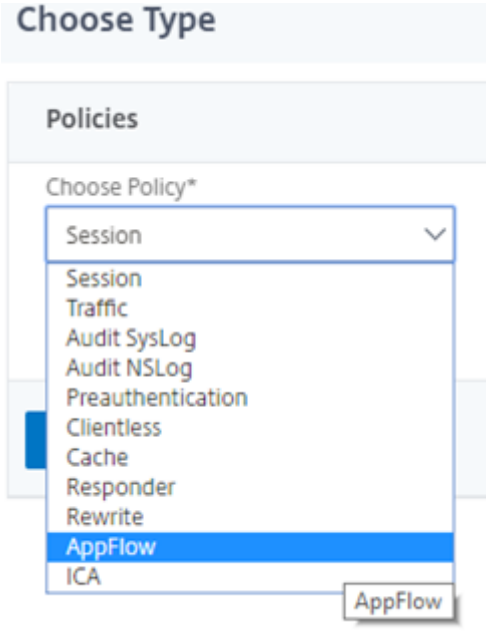


7. Accédez à **NetScaler Gateway>Serveurs virtuels**, sélectionnez le serveur virtuel et cliquez sur **Modifier**.

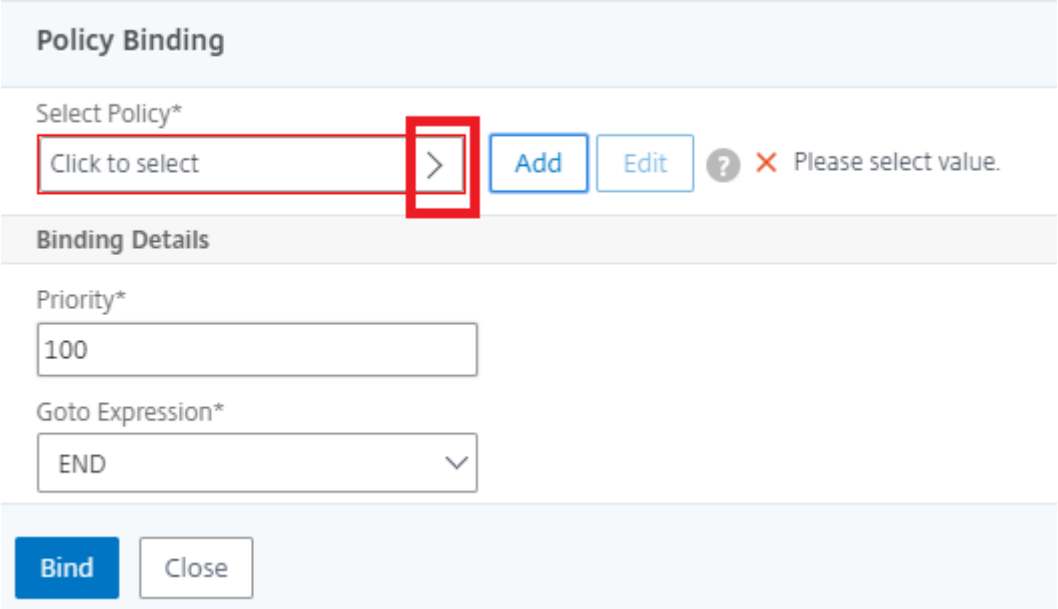


8. Faites défiler la page **Serveur virtuel VPN** vers le bas et sous la section **Stratégies**, cliquez sur **+**.

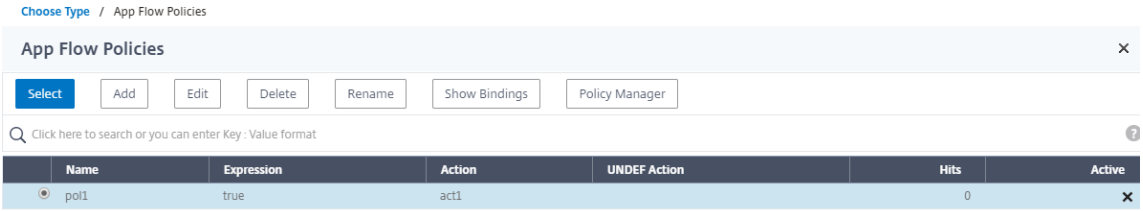
9. Sur l'écran **Choisir un type**, dans le menu déroulant **Choisir une stratégie**, sélectionnez **AppFlow**. Dans le menu déroulant **Choisir un type**, choisissez **Demande ou DemandeICA**, puis cliquez sur**Continuer**.



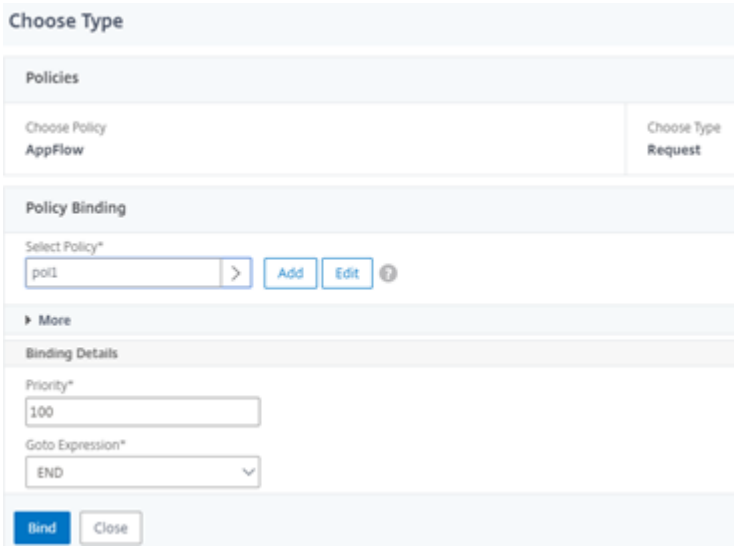
10. Cliquez sur la flèche en surbrillance sous **Sélectionner une stratégie**.



11. Sélectionnez la **stratégie AppFlow**, puis cliquez sur **Sélectionner**.



12. Enfin, cliquez sur **Bind**.



Pour configurer le support de NetScaler Gateway pour HDX Insight à l'aide de l'interface de ligne de commande, tapez la commande suivante

```
add appflow collector col3 -IPAddress<ip_mas>
add appflow action act1 <action_name>
add appflow policy <policy_name> true <action_name>
bind vpn Vserver <vserver_name>  -pol <policy_name> - priority101 END -
    type <ICA_Request>
```

Désactiver HDX Insight pour une session HDX non-NSAP

Dans une appliance NetScaler, vous pouvez désormais désactiver HDX Insight pour les sessions HDX autres que NSAP.

À l'invite de commandes, tapez :

```
set ica parameter HDXInsightNonNSAP (YES | NO )
<!--NeedCopy-->
```

Par défaut, la session HDX Insight pour non-NSAP est activée.

Découverte du PMTUD et propagation des bits DF pour EDT via NetScaler Gateway

March 27, 2024

À partir de la version 13.1 build 17.x, l'appliance NetScaler Gateway prend en charge l'application des bits DF pour la découverte du maximum d'unités de transmission (PMTUD) sur le chemin EDT. La découverte du MTU du chemin permet de déterminer dynamiquement l'unité de transmission maximale (MTU) lors de l'établissement d'une session. L'application des bits DF empêche la fragmentation EDT qui pourrait entraîner une dégradation des performances ou l'échec de l'établissement d'une session.

Dans les versions précédentes, NetScaler Gateway prenait en charge le chemin EDT MTUD mais ne prenait pas en charge l'application des bits DF.

Pour plus de détails, consultez la section Découverte MTU EDT.

Activez le support PMTUD à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
set ica parameter [-EnableSRonHAFailover ( YES | NO )] [-
    HDXInsightNonNSAP ( YES | NO )] [-EDTPmtudDF ( ENABLED | DISABLED )]
     [-EDTPmtudDFTimeout <positive_integer>] [-L7LatencyFrequency <
    positive_integer>]
<!--NeedCopy-->
```

Exemple:

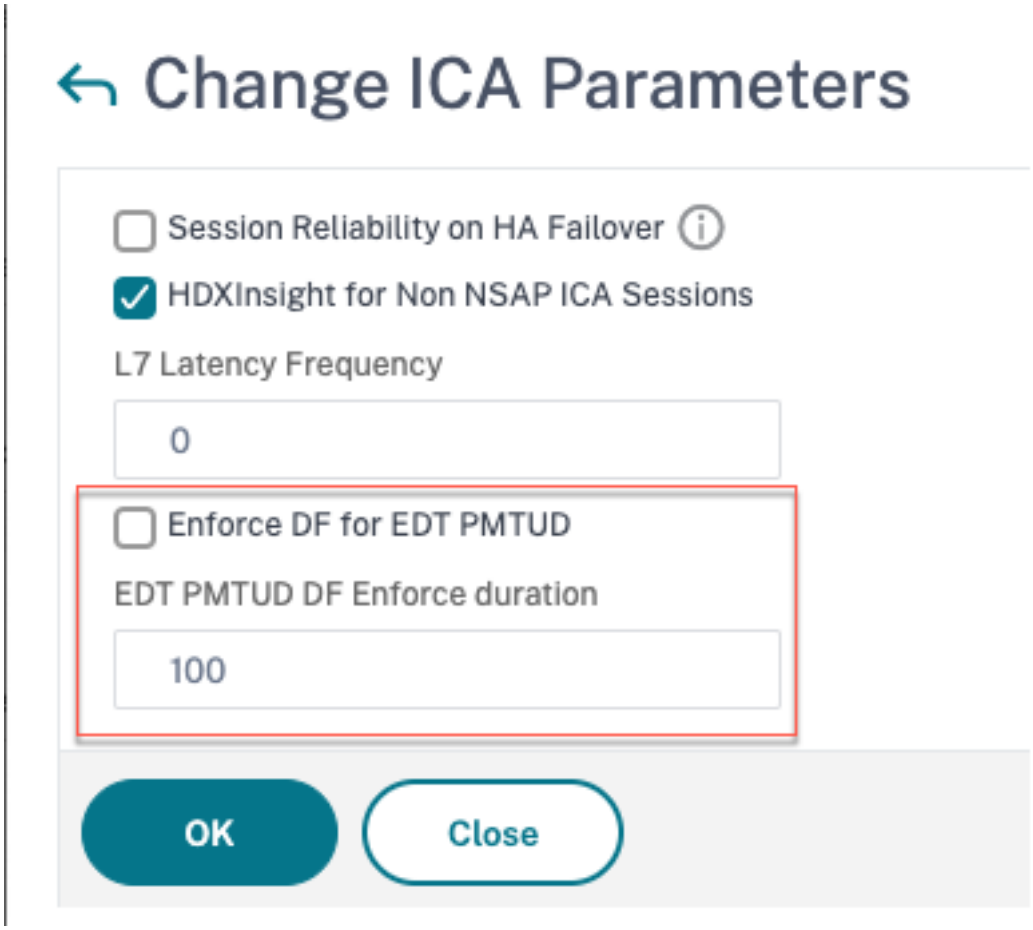
```
set ica parameter -EnableSRonHAFailover YES -EDTPmtudDF ENABLED -
    EDTPmtudDFTimeout 100
<!--NeedCopy-->
```

> **Remarque :**
>
> À partir de la version 13.1 build 42.x et des versions ultérieures, le paramètre EdTPMTUDDF est activé par défaut. Auparavant, cette option était désactivée par défaut.

Activez le support PMTUD à l'aide de l'interface graphique

1. Accédez à **Système > Paramètres > Modifier les paramètres ICA**.
2. Dans **Durée EDT PMTUD DF Enforce**, entrez le délai d'expiration en secondes pour l'application PMTUD DF Enforce.

> **Remarque :**
>
> À partir de la version 13.1 build 42.x et des versions ultérieures, l'option **PMTUD Enforce DF for EDT** est activée par défaut. Auparavant, cette option était désactivée par défaut.



Seuil de latence L7

January 26, 2024

La fonctionnalité de seuil de latence L7 de HDX Insight détecte activement les problèmes de latence réseau de bout en bout au niveau de l'application et prend des mesures proactives. La fonction de seuil de latence L7 effectue une surveillance de la latence en direct pour détecter les pics et envoie des notifications à HDX Insight si la latence dépasse la latence minimale observée.

Auparavant, les valeurs moyennes de latence L7 côté client et côté serveur étaient envoyées toutes les 60 secondes à HDX Insight. Tous les pics observés dans cet intervalle ont été calculés en moyenne et n'ont donc pas été détectés. De plus, il n'y avait pas de surveillance de la latence en direct pour détecter ces pics.

En quoi la latence de niveau 7 est-elle différente de la latence de niveau 4

Les latences réseau sont également capturées et affichées au niveau L4. Ces latences sont calculées à partir de la couche TCP et ne nécessitent pas d'analyse du trafic ICA. Par conséquent, ils sont relativement faciles à obtenir et consomment moins d'UC. Cependant, le principal inconvénient de la latence de niveau 4 est la compréhension de la latence de bout en bout. S'il y a des proxys TCP dans le chemin, la latence L4 capture uniquement la latence entre NetScaler et le proxy TCP. Cela peut entraîner des informations incomplètes et donc des difficultés de débogage du problème.

La latence L7 est calculée en analysant le trafic ICA. Le calcul de la latence L7 est effectué au niveau de la couche ICA. Par conséquent, les proxys intermédiaires n'entraînent pas de valeurs de latence incomplètes. Ainsi, fournit une détection de la latence de bout en bout.

Les figures suivantes présentent un type de déploiement avec et sans proxy TCP.

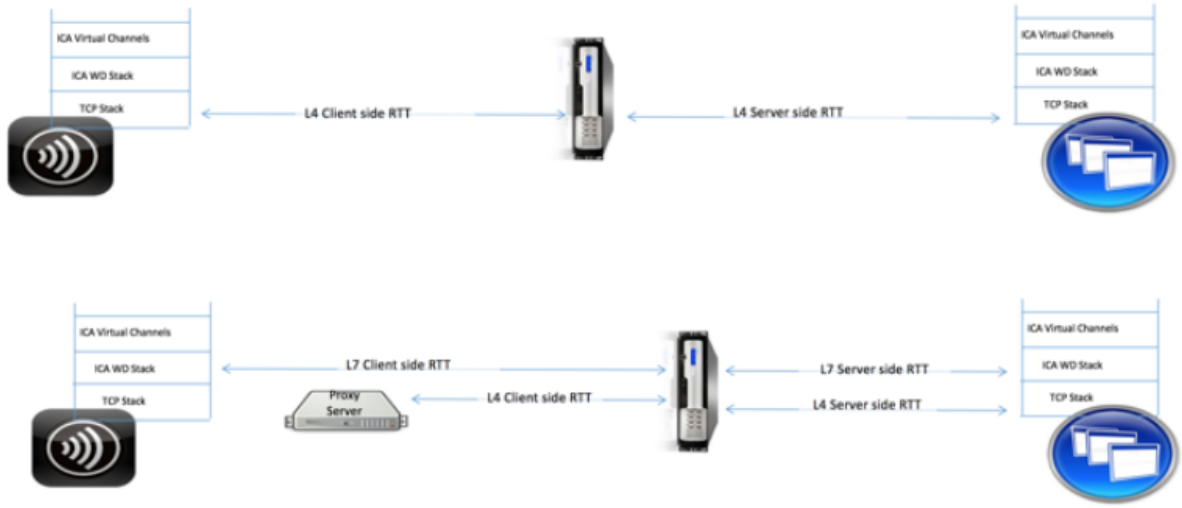


Fig 2. Deployment with TCP Proxies

Différence entre les calculs de latence ICA RTT et L7

ICA RTT représente le temps total aller-retour entre l'application Citrix Workspace et le Virtual Delivery Agent (VDA). La latence L7 fournit des détails détaillés concernant les latences côté client et côté serveur. La latence du client L7 est la latence entre l'application Citrix Workspace et NetScaler Gateway. La latence du serveur L7 est la latence entre NetScaler Gateway et VDA.

> **Remarque** : Le calcul de la latence L7 côté serveur pour le serveur est pris en charge uniquement pour les versions 7.13 et ultérieures de Citrix Virtual Apps and Desktops.

Configuration du seuil de latence L7 à l'aide de l'interface de ligne de commande

1. Ajoutez un profil de latence ICA.

```
add ica latencyprofile <name> [-l7LatencyMonitoring ( ENABLED |
    DISABLED )] [-l7LatencyThresholdFactor <positive_integer>] [-
    l7LatencyWaitTime <positive_integer>] [-l7LatencyNotifyInterval
     <positive_integer>] [-l7LatencyMaxNotifyCount <
    positive_integer>]
<!--NeedCopy-->
```

2. Ajoutez une action ICA.

```
add ica action <name> [-latencyprofileName <string>]
<!--NeedCopy-->
```

3. Ajoutez une stratégie ICA.

```
add ica policy <name> -rule <expression> -action <string> [-
    comment<string>] [-logAction <string>
<!--NeedCopy-->
```

4. Liez la stratégie ICA au serveur VPN ou au point de liaison global ICA.

```
bind ica global -policyName <string> -priority <positive_integer>
    [-gotoPriorityExpression <expression>] [-type (
    ICA_REQ_OVERRIDE | ICA_REQ_DEFAULT )]
<!--NeedCopy-->
```

Ou

```
bind vpn vserver <name> -policy <string>  [-priority <
    positive_integer>]
<!--NeedCopy-->
```

Ou

```
bind cr vserver <name> -policy <string> [-priority <positive
    _integer>]
<!--NeedCopy-->
```

Arguments

- **Surveillance de la latence** : paramètre permettant d'activer ou de désactiver la surveillance du seuil L7. Lorsque ce paramètre est activé, des notifications sont envoyées à HDX Insight lorsque les conditions définies sont remplies.

  Valeur par défaut : DISABLED

- **LatencyThresholdFactor** : Facteur selon lequel la latence active doit être supérieure à la latence minimale observée pour conclure que le seuil est dépassé. Par conséquent, une notification doit être envoyée à HDX Insight.

  Valeur par défaut : 4

  Valeur minimale : 2

  Valeur maximale : 65535

- **LatencyWaitTime** : durée en secondes d'attente de l'appliance après le dépassement du seuil de latence pour envoyer une notification à HDX Insight.

  Valeur par défaut : 20

  Valeur minimale : 1

  Valeur maximale : 65535

- **LatencyNotifyInterval** : intervalle de temps en secondes pendant lequel l'appliance envoie les notifications suivantes à HDX Insight une fois le temps d'attente écoulé.

  Valeur par défaut : 20

  Valeur minimale : 1

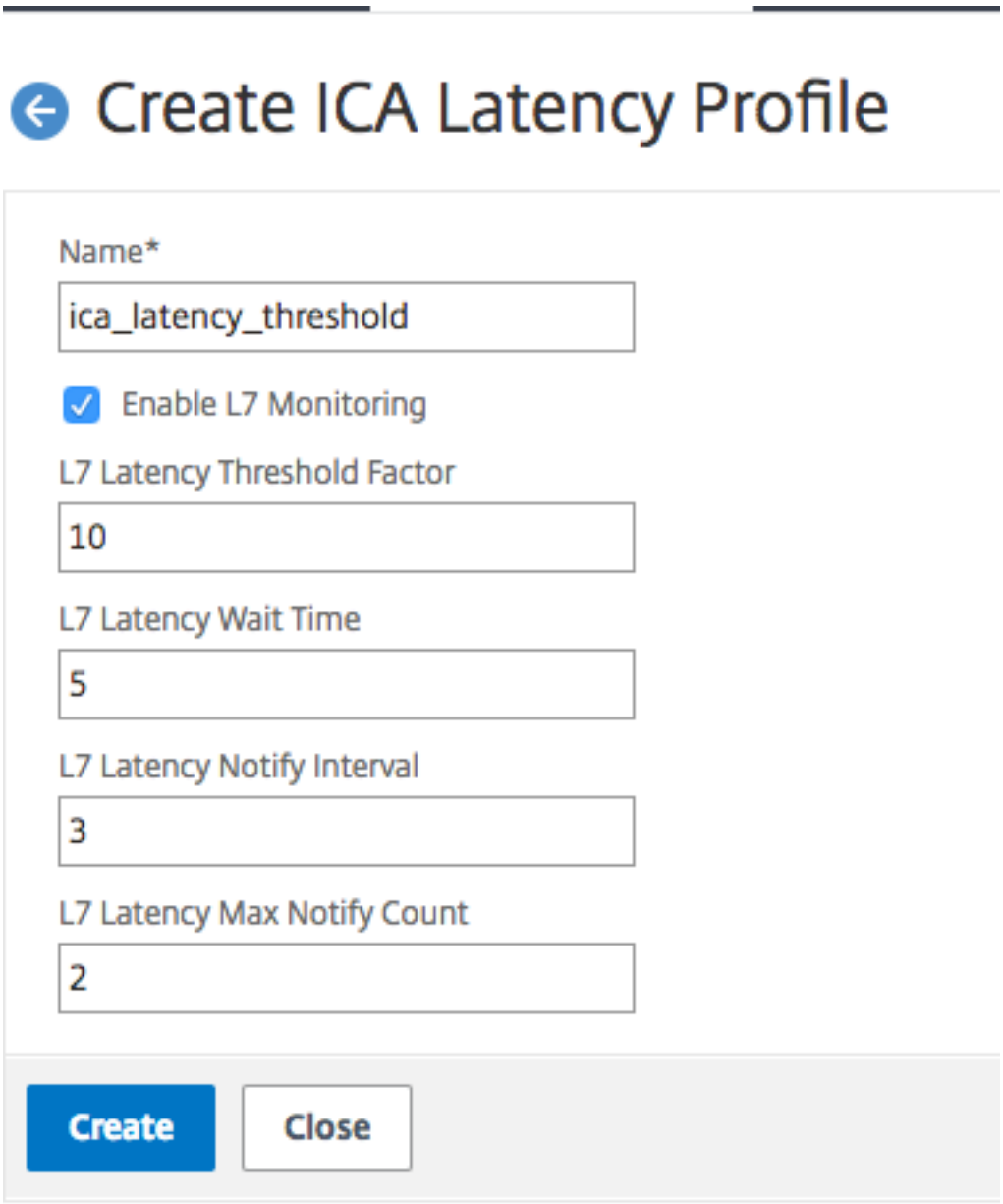
  Valeur maximale : 65535

- **LatencyMaxNotifyCount** : nombre maximal de notifications pouvant être envoyées à HDX Insight dans un intervalle où la latence est supérieure au seuil.

  Valeur par défaut : 5

Configurer le seuil de latence L7 à l'aide de l'interface graphique

1. Accédez à **Configuration** > **NetScaler Gateway** > **Stratégies** > **ICA**.
2. Sélectionnez l'onglet **Profils de latence ICA**, puis cliquez sur **Ajouter**.
3. Dans la page **Créer un profil de latence ICA**, effectuez les opérations suivantes.



- Sélectionnez Surveillance de **la latence L7 pour activer la surveillance** du seuil de niveau 7.
- Dans **Facteur de seuil L7**, entrez la valeur par laquelle la latence active doit dépasser la latence minimale observée pour envoyer une notification à HDX Insight.
- Dans la zone **Latency Wait Time (Temps d'attente de latence de niveau 7**), entrez la durée en secondes pendant laquelle l'appliance doit attendre après le dépassement du seuil pour envoyer une notification à HDX Insight.
- Dans **Intervalle de notification de latence L7**, entrez le temps en secondes pendant lequel l'appliance doit envoyer les notifications suivantes à HDX Insight une fois le temps d'attente écoulé.

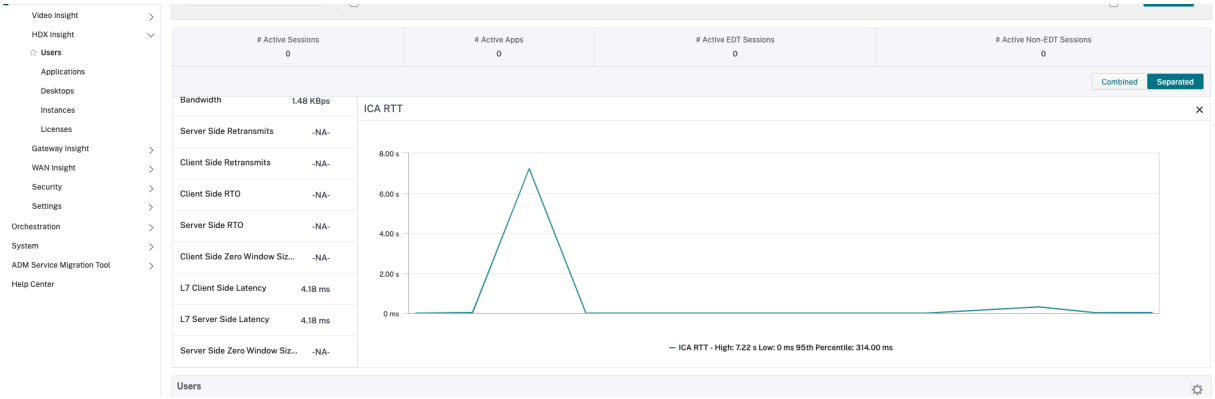
- Dans la zone **L7 Latency Maximum Notify Count**, entrez le nombre maximal de notifications pouvant être envoyées à HDX Insight dans un intervalle où la latence est supérieure au seuil.
  Remarque : Le nombre maximal de notifications de latence L7 est applicable une fois que le seuil est dépassé et est réinitialisé lorsque la latence active tombe en dessous du seuil. La périodicité de ces notifications est régie par l'intervalle de notification.

4. Cliquez sur **Créer**.

> **Important :**
>
> Après avoir configuré les paramètres de seuil de latence L7, vous devez configurer HDX Insight. Pour plus de détails, consultez la section Configurer NetScaler Gateway pour prendre en charge HDX Insight.

Afficher les paramètres de latence L7 dans NetScaler ADM

Pour afficher les paramètres de latence L7 dans NetScaler ADM, accédez à **Analytics > HDX Insight > Applications ou Analytics > HDX Insight> Utilisateurs**.

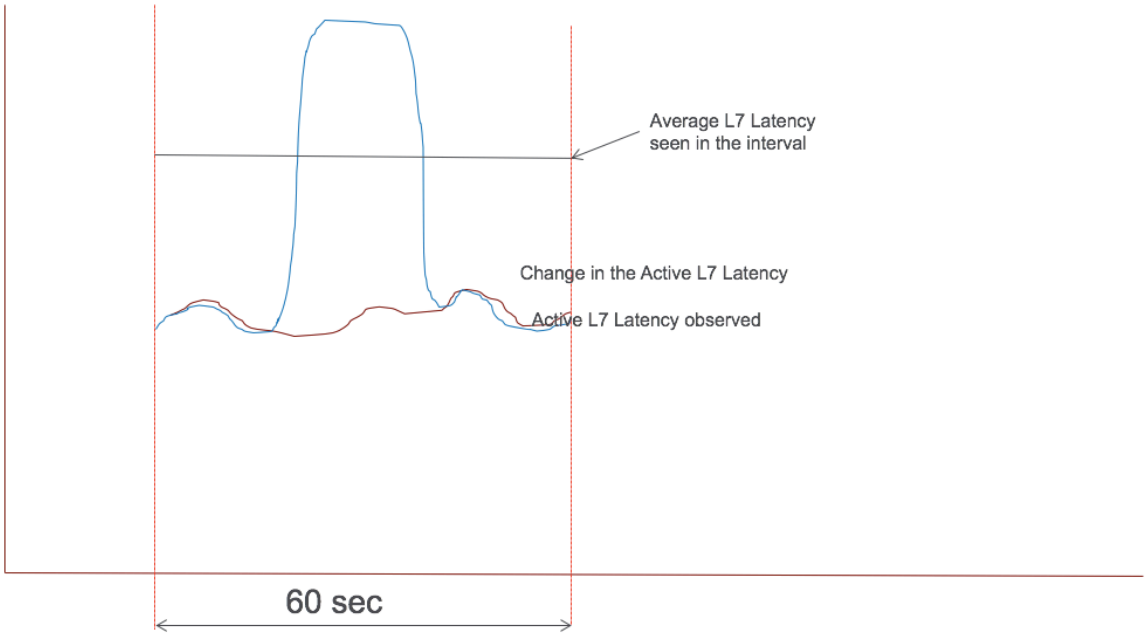


Le modèle de mesure de latence L7 par rapport au modèle de reporting du seuil de latence L7

Le modèle de mesure de latence L7

Dans le module de mesure de latence L7, les valeurs moyennes de latence L7 côté client et côté serveur sont envoyées à HDX Insight toutes les 60 secondes. Par conséquent, les pics observés dans cet intervalle sont calculés en moyenne et ne sont donc pas détectés. De plus, le module de mesure de latence L7 n'a pas la capacité de surveillance de la latence en direct.

La figure suivante illustre un exemple de modèle de mesure de la latence L7.

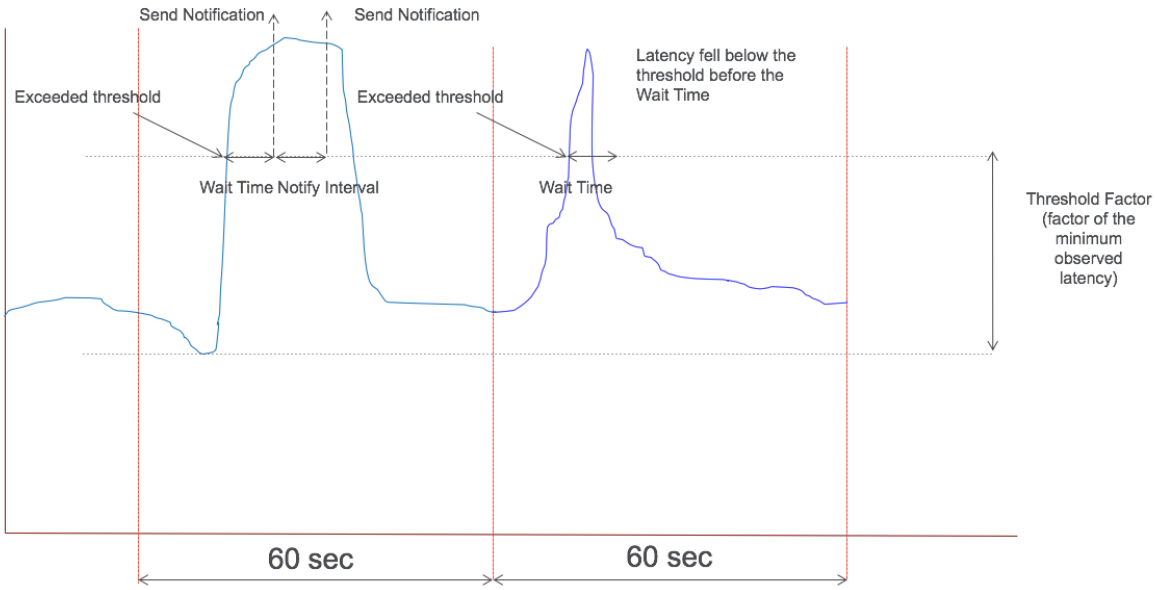


Modèle de rapport de seuil de latence L7

Le modèle de rapport de seuil de latence L7 dispose de la capacité de surveillance de la latence en direct pour détecter les pics. Les notifications sont envoyées à HDX Insight si la latence dépasse la latence minimale observée.

Chaque fois qu'un facteur de seuil est dépassé, l'augmentation de latence est détectée. Une fois le délai d'attente de seuil configuré expiré, une notification est envoyée à HDX Insight. Une notification ultérieure est envoyée à HDX Insight une fois que le temps d'attente a expiré et que le facteur de seuil est toujours dépassé.
Si la valeur de latence tombe en dessous du facteur de seuil avant l'expiration du temps d'attente, aucune notification n'est envoyée à HDX Insight.

La figure suivante illustre un exemple de modèle de rapport de seuil de latence L7.



Les paramètres suivants peuvent être configurés au moment de l'exécution :

- Surveillance des seuils (ON/OFF)
- Facteur de seuil
- Temps d'attente seuil
- Intervalle de
- Nombre maximal de notifications

Proxy RDP

March 27, 2024

La fonctionnalité de proxy RDP est fournie dans le cadre de NetScaler Gateway. Dans un déploiement standard, le client RDP s'exécute sur la machine d'un utilisateur distant. L'appliance NetScaler Gateway est déployée dans la zone démilitarisée et la batterie de serveurs RDP se trouve dans le réseau interne de l'entreprise.

L'utilisateur distant ;

1. se connecte à l'adresse IP publique de NetScaler Gateway
2. établit une connexion VPN SSL
3. authentifie
4. accède aux postes de travail distants via l'appliance NetScaler Gateway

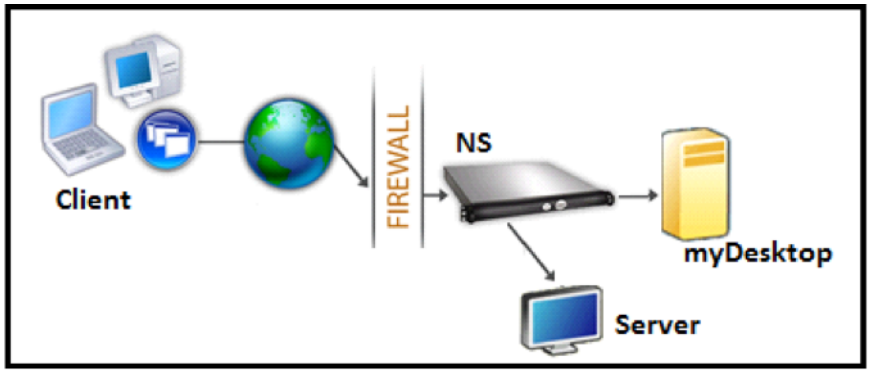
La fonctionnalité RDP-proxy est prise en charge en mode VPN sans client et proxy ICA.

> **Remarque :**
>
> NetScaler Gateway ne prend pas en charge l'hôte de session de bureau à distance (RDSH), l'application distante, le mode multiutilisateur RDS, les sessions RDP ou les applications RDP.

Les fonctionnalités de proxy RDP suivantes permettent d'accéder à une batterie de postes de travail distants via NetScaler Gateway.

- Sécurisez le trafic RDP via un VPN sans client ou un mode proxy ICA (sans tunnel complet).
- SSO (authentification unique) vers les serveurs RDP via NetScaler Gateway. Fournit également une option permettant de désactiver l'SSO si nécessaire.
- Fonction d'application (SmartAccess), dans laquelle les administrateurs de NetScaler peuvent désactiver certaines fonctionnalités RDP via la configuration de NetScaler Gateway.
- Solution de passerelle unique/sans état (double) pour tous les besoins (VPN/ICA/RDP/Citrix Endpoint Management).
- Compatibilité avec le client Windows MSTSC natif pour RDP sans avoir besoin de clients personnalisés.
- Utilisation d'un client RDP fourni par Microsoft sur MACOSX, iOS et Android.

La figure suivante présente une vue d'ensemble du déploiement :



Déploiement via un VPN sans client

Dans ce mode, les liens RDP sont publiés sur la page d'accueil ou le portail de la passerelle, sous forme de signets, via la `add vpn url` configuration ou via un portail externe. L'utilisateur peut cliquer sur ces liens pour accéder au Bureau à distance.

Déploiement via le proxy ICA

Dans ce mode, une page d'accueil personnalisée est configurée sur le VIP de passerelle à l'aide du paramètre `wihome`. Cette page d'accueil peut être personnalisée avec la liste des ressources Bureau

à distance auxquelles l'utilisateur est autorisé à accéder. Cette page personnalisée peut être hébergée sur NetScaler ou, si elle est externe, elle peut être un iFrame dans la page du portail Gateway existante.

Dans les deux modes, une fois que l'utilisateur clique sur le lien ou l'icône RDP provisionné, une demande HTTPS pour la ressource correspondante parvient à NetScaler Gateway. La passerelle génère le contenu du fichier RDP pour la connexion demandée et le pousse vers le client. Le client RDP natif est appelé et il se connecte à un écouteur RDP sur la passerelle. Gateway effectue une connexion unique vers le serveur RDP en prenant en charge l'application (SmartAccess). La passerelle bloque l'accès du client à certaines fonctionnalités RDP, en fonction de la configuration de NetScaler, puis elle transmet par proxy le trafic RDP entre le client RDP et le serveur.

Détails de l'application

L'administrateur de NetScaler peut configurer certaines fonctionnalités RDP via la configuration de NetScaler Gateway. NetScaler Gateway fournit la fonctionnalité « Application du protocole RDP » pour les paramètres importants du protocole RDP. NetScaler veille à ce que le client ne puisse pas activer les paramètres bloqués. Si les paramètres bloqués sont activés, la fonctionnalité d'application RDP remplace les paramètres activés pour le client et ils ne sont pas respectés.

> **Important :** La fonctionnalité d'application n'est applicable que si l'authentification unique est activée.

Paramètres RDP pris en charge pour l'application

L'application des paramètres de redirection suivants est prise en charge. Ces paramètres sont configurables dans le cadre d'un profil client RDP.

- Redirection du presse-papiers
- Redirection des imprimantes
- Redirection des unités de disque
- Redirection des ports COM
- Redirection des périphériques PNP

Flux de connexion

Le flux de connexion peut être divisé en deux étapes :

- Énumération des ressources RDP et téléchargement de fichiers RDP.

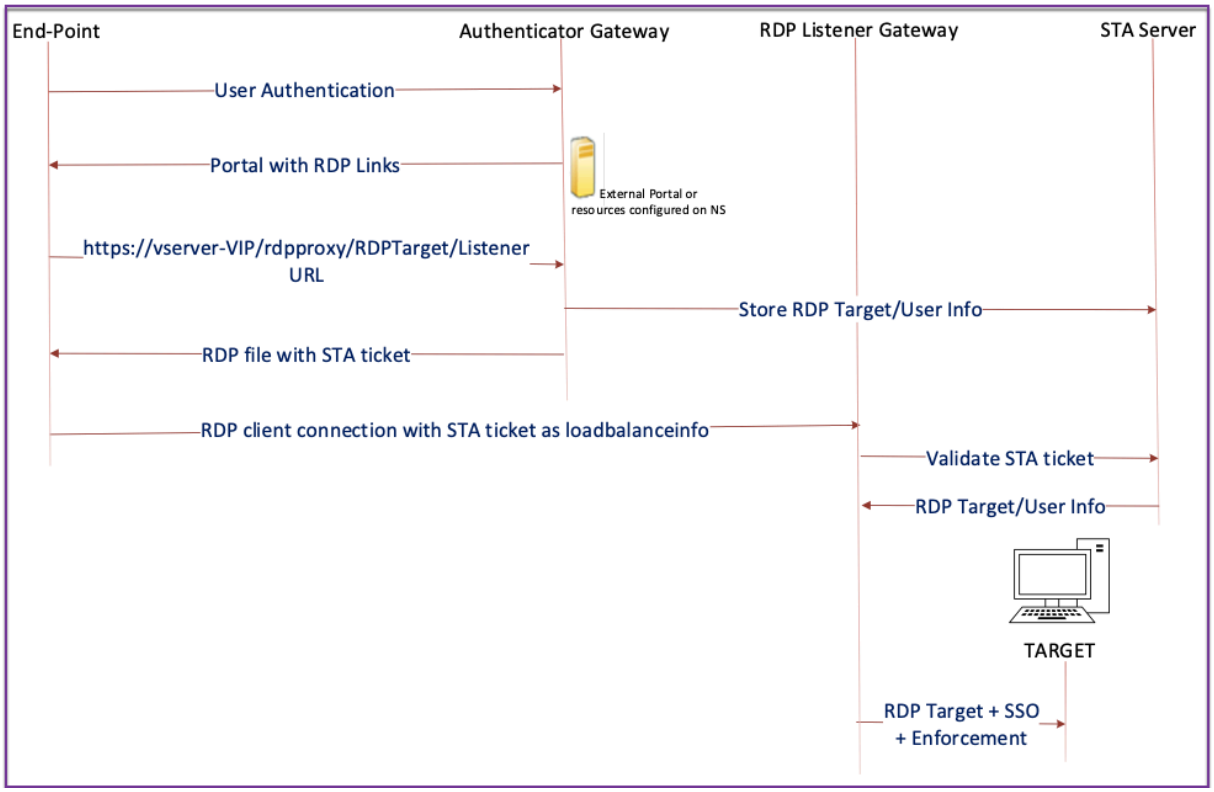
- Lancement de la connexion RDP.

Sur la base du flux de connexion précédent, il existe deux solutions de déploiement :

- Solution de passerelle sans état (double) : l'énumération des ressources RDP et le téléchargement du fichier RDP s'effectue via la passerelle d'authentification, mais le lancement de la connexion RDP s'effectue via la passerelle d'écoute RDP.
- Solution de passerelle unique : l'énumération des ressources RDP, le téléchargement de fichiers RDP et le lancement de la connexion RDP se produisent via la même passerelle.

Compatibilité avec la passerelle sans état (double)

La figure suivante illustre le déploiement :



- Un utilisateur se connecte à la VIP Authenticator Gateway et fournit les informations d'identification.
- Une fois la connexion réussie à la passerelle, l'utilisateur est redirigé vers la page d'accueil ou le portail externe, qui énumère les ressources du poste de travail distant auxquelles l'utilisateur peut accéder.
- Une fois que l'utilisateur a sélectionné une ressource RDP, la VIP Authenticator Gateway reçoit la demande au format `https://vserver-vip/rdpproxy/rdptarget/listener` in-

diquant la ressource publiée sur laquelle l'utilisateur a cliqué. Cette demande contient les informations relatives à l'adresse IP et au port du serveur RDP sélectionné par l'utilisateur.

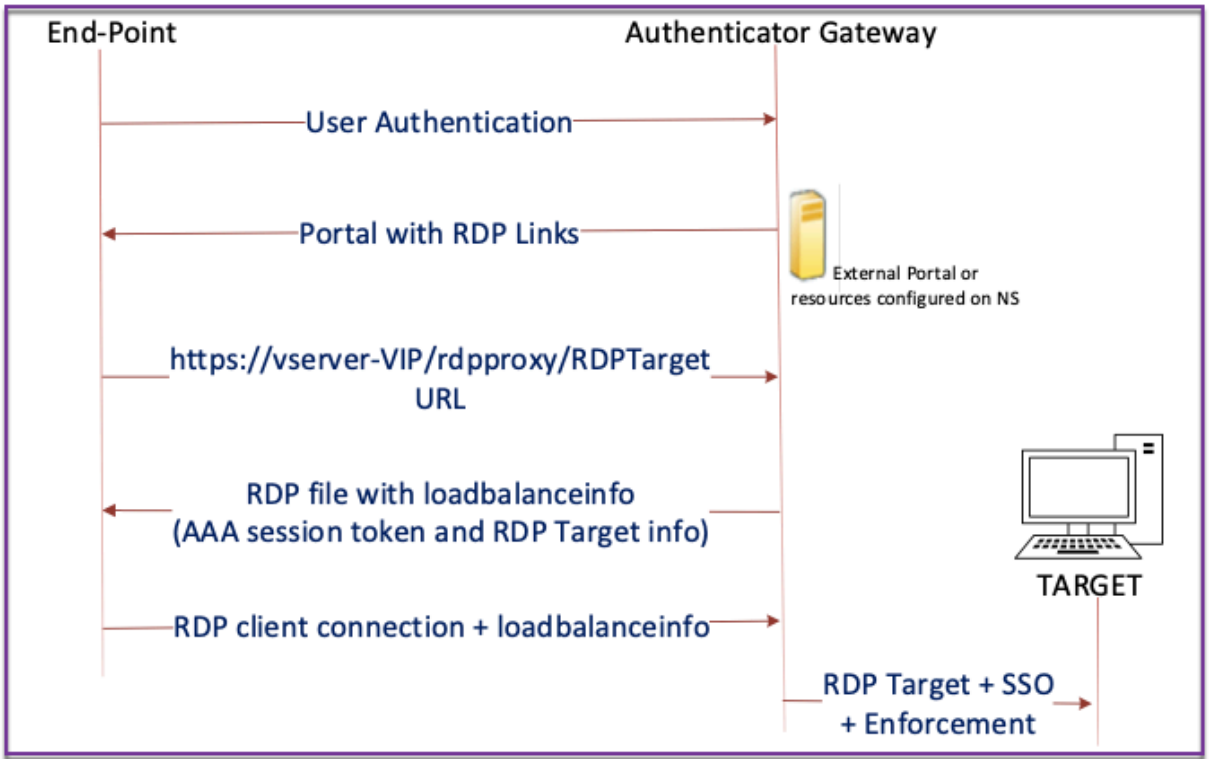
- La passerelle d'authentification traite la demande /rdpproxy/. Étant donné que l'utilisateur est déjà authentifié, cette demande est accompagnée d'un cookie Gateway valide.
- Les `RDPUser` informations `RDPTarget` et sont stockées sur le serveur STA, et un ticket STA est généré. Les informations stockées sur le serveur STA sont cryptées à l'aide de la clé prépartagée configurée. La passerelle Authenticator utilise l'un des serveurs STA configurés sur le serveur virtuel de passerelle.
- Les informations 'Listener'obtenues dans la requête /rdpproxy/ sont placées dans le `.rdp file` « `fulladdress` » et le ticket STA (pré-ajouté avec l'AuthID STA) est placé dans `.rdp file` comme « `loadbalanceinfo` ».
- Le paramètre `.rdp file` est renvoyé au point de terminaison du client.
- Le client RDP natif se lance et se connecte au `RDPListener Gateway`. Il envoie le ticket STA dans le paquet initial.

  La passerelle `RDPListener` valide le ticket STA et obtient les informations `RDPTarget` et `RDPUser`. Le serveur STA à utiliser est récupéré à l'aide du 'AuthID'présent dans le `loadbalanceinfo`.
- Une session de passerelle est créée pour stocker les stratégies d'autorisation/d'audit. Si une session existe pour l'utilisateur, elle est réutilisée.
- La passerelle `RDPListener` se connecte à `RDPTarget` et ouvre une session unique à l'aide de CREDSSP.

> **Important :**
>
> - Pour le proxy RDP sans état, le serveur STA valide le ticket STA, envoyé par le client RDP, pour obtenir les informations `RDPTarget`/`RDPUser`. Vous devez lier le serveur STA en plus du serveur virtuel VPN.

Compatibilité avec une passerelle unique

La figure suivante illustre le déploiement :



> **Important :**
>
> Dans le cas d'un déploiement de passerelle unique, le serveur STA n'est pas nécessaire. La passerelle d'authentification code le `RDPTarget` en toute sécurité le cookie de session d'authentification, d'autorisation et d'audit NetScaler et les envoie en tant que `loadbalanceinfo` dans le `.rdp file`. Lorsque le client RDP envoie ce jeton dans le paquet initial, la passerelle d'authentification décode les informations,`RDPTarget` recherche la session et se connecte au `RDPTarget`.

Prise en charge de Single Listener

- Un seul écouteur pour le trafic RDP et SSL.
- Le téléchargement du fichier RDP et le trafic RDP peuvent être gérés via le même tuple 2 (c'est-à-dire IP et port) sur l'appliance NetScaler.

Exigences de licence pour le proxy RDP

Édition Premium, édition avancée

> **Remarque :**
>
> La fonction de proxy RDP n'est pas disponible pour les clients disposant uniquement d'une li-

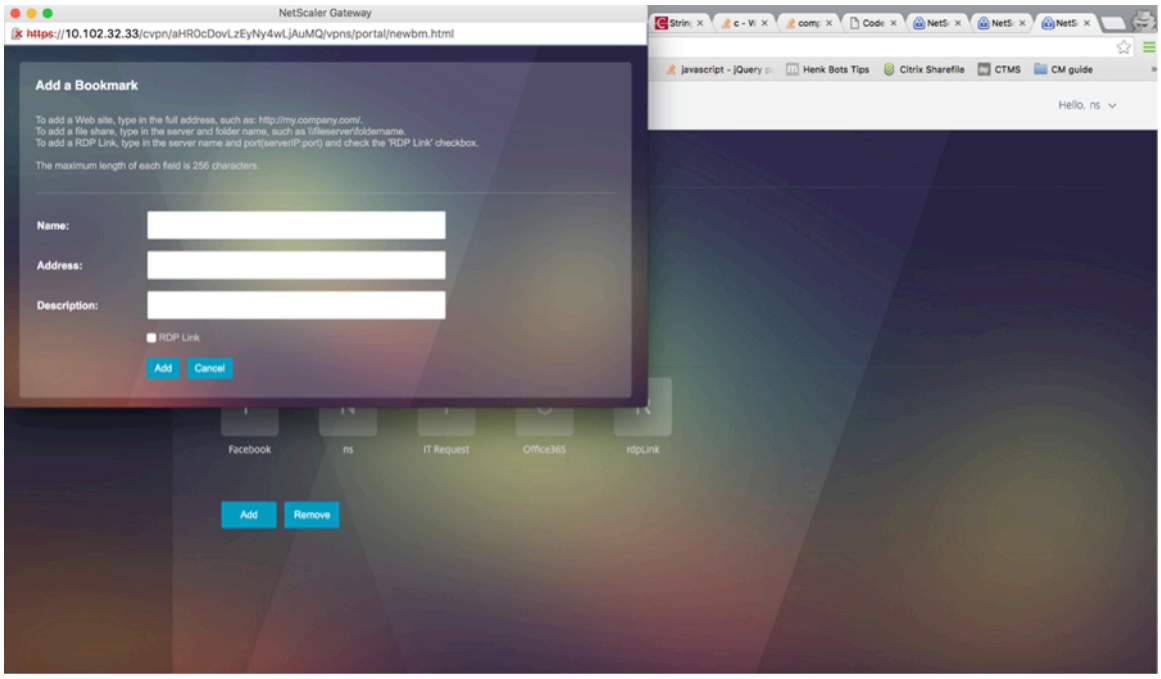
> cence de plate-forme Gateway ou uniquement de l'édition Standard.

Vous pouvez utiliser la commande suivante pour activer le proxy RDP.

```
enable feature rdpProxy
<!--NeedCopy-->
```

Signet

Génération de liens RDP via Portal. Au lieu de configurer les liens RDP pour l'utilisateur ou de publier les liens RDP via un portail externe, vous pouvez donner aux utilisateurs la possibilité de générer leurs propres URL en fournissant `targerIP:Port`. Pour un déploiement proxy RDP sans état, l'administrateur peut inclure des informations sur l'écouteur RDP dans le format FQDN : Port dans le profil du client RDP. Cela se fait sous l'option `rdpListener`. Cette configuration est utilisée pour la génération de liens RDP via le portail en mode Dual Gateway.



Créer des signets

1. Créez des signets sur la page du portail pour accéder aux ressources RDP : (L'URL actuelle commence par `rdp`://).
2. Ajouter une URL VPN `<urlName> <linkName> <actualURL>`
    - L'URL doit être au format suivant : `rdp://<TargetIP:Port>`.

- Pour le mode proxy RDP sans état, l'URL doit être au format suivant : `rdp://<TargetIP:Port>/<ListenerIP:Port>`
- L'URL est publiée sur le portail au format suivant :
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>`
  `https://<VPN-VIP>/rdpproxy/<TargetIP:Port>/<ListenerIP:Port>`

3. Liez les signets à l'utilisateur ou au groupe, au serveur virtuel VPN ou au VPN global.

Fonctionnalités et modes à activer pour le proxy RDP

```
- enable ns feature ssl

- enable ns feature sslvpn

- enable ns feature rdpproxy

- enable mode usnip
<!--NeedCopy-->
```

Étapes de configuration de haut niveau du proxy RDP

Les étapes de haut niveau suivantes impliquées dans la configuration du proxy RDP sans état.

- Créer un profil de serveur RDP
- Créer un profil client RDP
- Création et liaison d'un serveur virtuel
- Créer un signet
- Créer ou modifier un profil ou une stratégie de session
- Liez un signet

Configuration d'un profil client

Configurez le profil client sur la passerelle d'authentification. Voici un exemple de configuration :

```
add rdpClient profile <name> [-addUserNameInRdpFile ( YES | NO )] [-
    audioCaptureMode ( ENABLE | DISABLE )] [-keyboardHook <keyboardHook
    >] [-multiMonitorSupport ( ENABLE | DISABLE )] [-psk <string>] [-
    rdpCookieValidity <positive_integer>] [-rdpCustomParams <string>] [-
    rdpFileName <string>] [-rdpHost <optional FQDN that will be put in
    the RDP file as ' fulladdress>] [-rdpUrlOverride ( ENABLE | DISABLE
    )] [-redirectClipboard ( ENABLE | DISABLE )] [-redirectComPorts (
    ENABLE | DISABLE )] [-redirectDrives ( ENABLE | DISABLE )] [-
    redirectPnpDevices ( ENABLE | DISABLE )] [-redirectPrinters ( ENABLE
     | DISABLE )] [-videoPlaybackMode ( ENABLE | DISABLE )]
```



```
<!--NeedCopy-->
```

Associez le profil du client RDP au serveur virtuel VPN.

Cela peut être fait en configurant une SessionAction+SessionPolicy ou en définissant le paramètre VPN global.

Exemple:

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
   prioritynumber>
<!--NeedCopy-->
```

OU

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

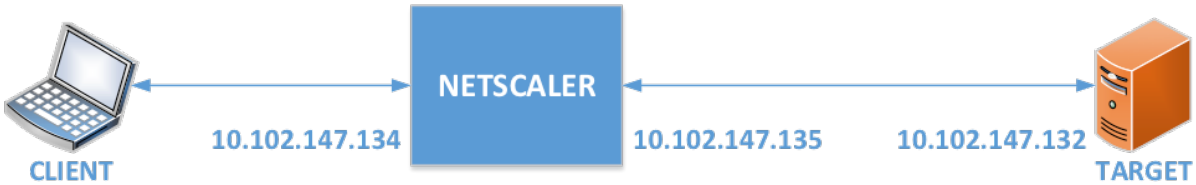
Configurer un profil de serveur

Configurez le profil de serveur sur la passerelle d'écoute.

```
add rdp ServerProfile <profilename> -rdpIP <IPV4 address of the RDP
   listener> -rdpPort <port for terminating RDP client connections> -
   psk <key to decrypt RDPTarget/RDPUser information, needed while
   using STA>`
<!--NeedCopy-->
```

Le `rdp ServerProfile` doit être configuré sur le serveur virtuel VPN.

```
add vpn vserver v1 SSL <publicIP> <portforterminatingvpnconnections> -
   rdpServerProfile <rdpServer Profile>`
<!--NeedCopy-->
```



Configuration du proxy RDP à l'aide de l'interface de ligne de commande

Voici un exemple de configuration du proxy RDP à l'aide de l'interface de ligne de commande.

- Ajoutez l'URL VPN de l'utilisateur avec les informations de la cible.

```
add aaa user Administrator  –password freebsd123$%^

add vpn url rdp RdpLink rdp://rdpserverinfo

add dns addrec rdpserverinfo 10.102.147.132

bind aaa user Administrator   –urlName rdp
<!--NeedCopy-->
```

- Configurez le profil client et serveur RDP pour la connexion VPN.

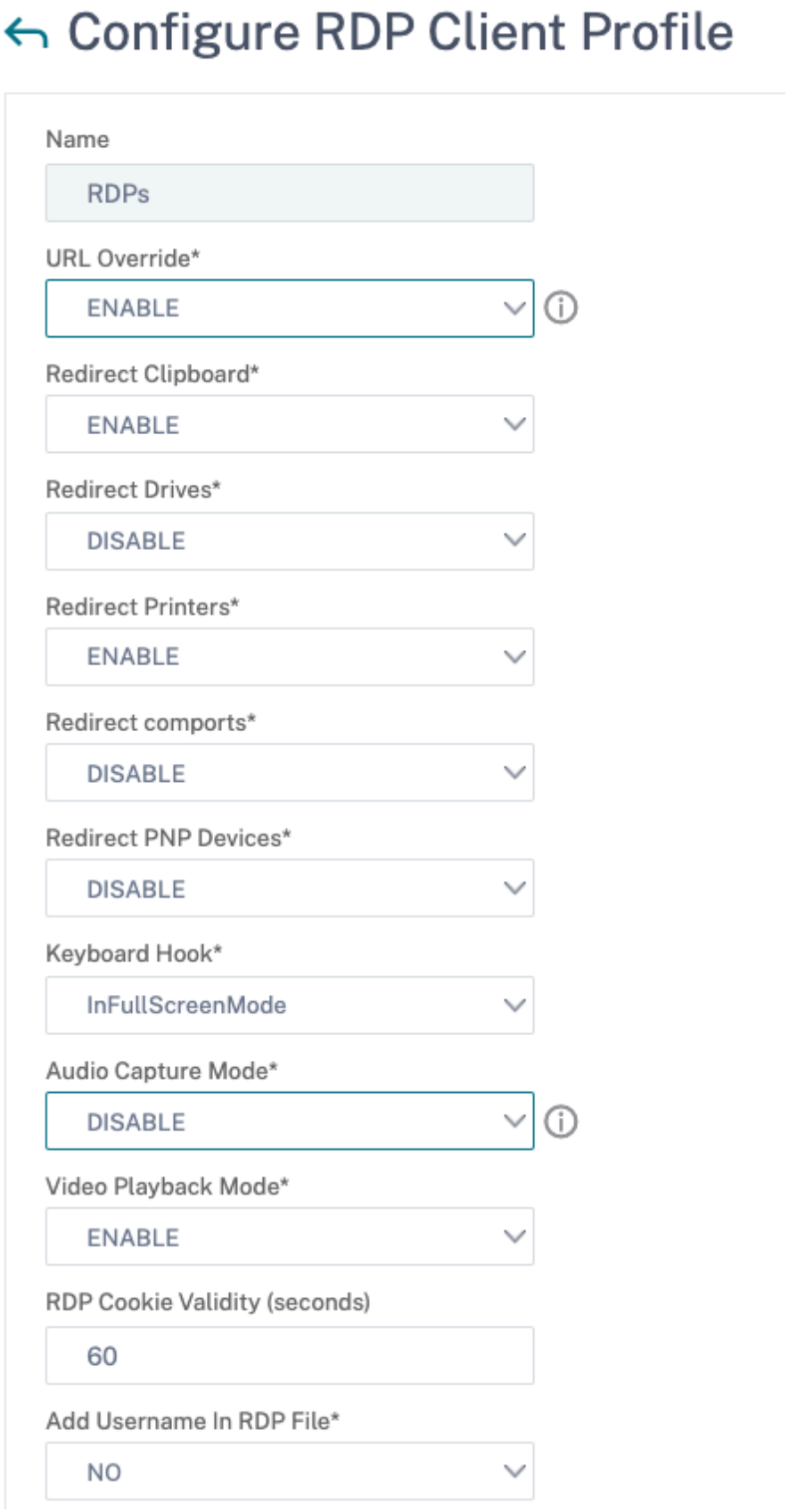
```
add rdp clientprofile p1  –psk citrix -redirectClipboard ENABLE

add rdp serverprofile p1 -rdpIP 10.102.147.134 -psk citrix

add vpn vserver mygateway SSL  10.102.147.134 443  –
   rdpserverprofile p1

set vpn parameter -clientlessVpnMode ON -
   defaultAuthorizationAction ALLOW -rdpClientProfileName p1

add ssl certKey gatewaykey -cert rdp_rootcert.pem  -key
   rdp_rootkey

bind ssl vserver mygateway -certkeyName gatewaykey
<!--NeedCopy-->
```

- AJOUTEZ UN SNIP pour la connexion entre NetScaler et la cible.

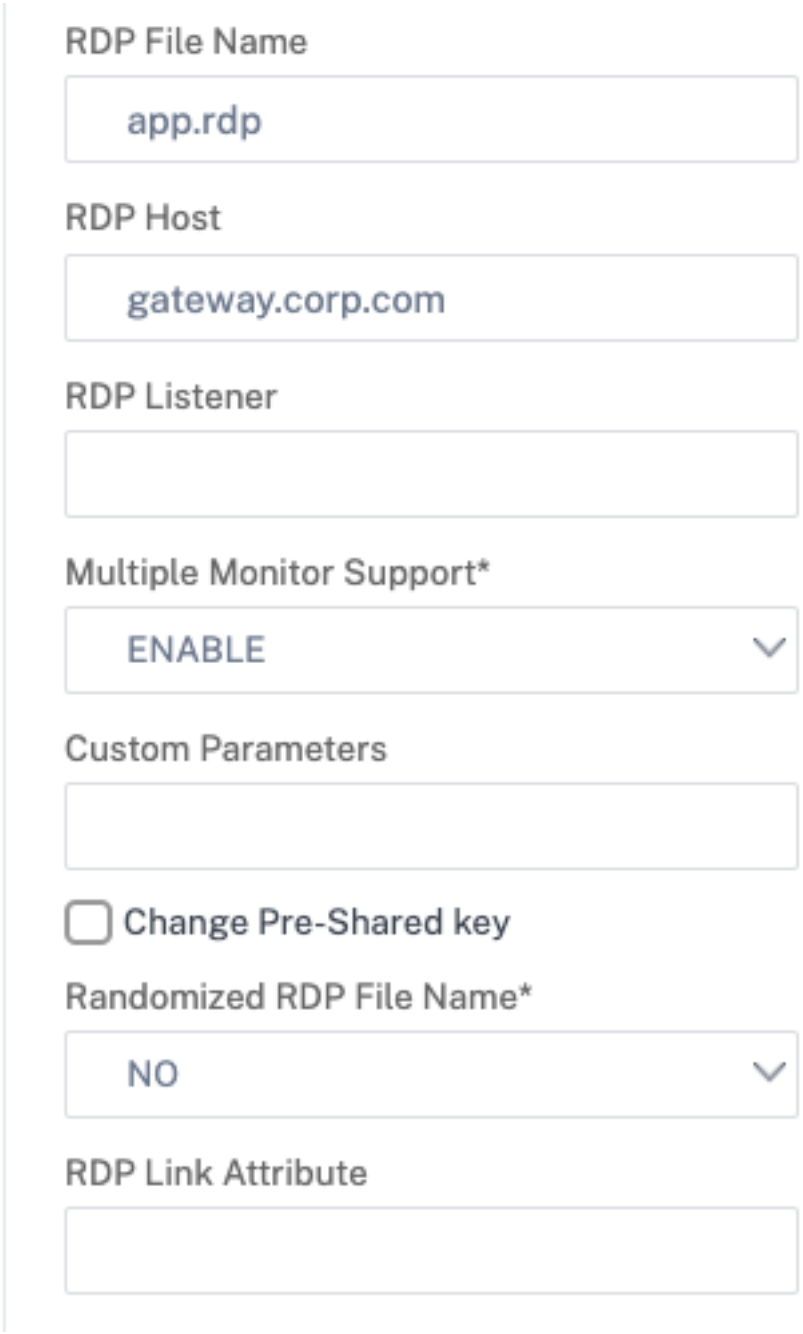
```
add ns ip 10.102.147.135  255.255.255.0  –type SNIP
<!--NeedCopy-->
```

Configuration du proxy RDP à l'aide de l'interface graphique

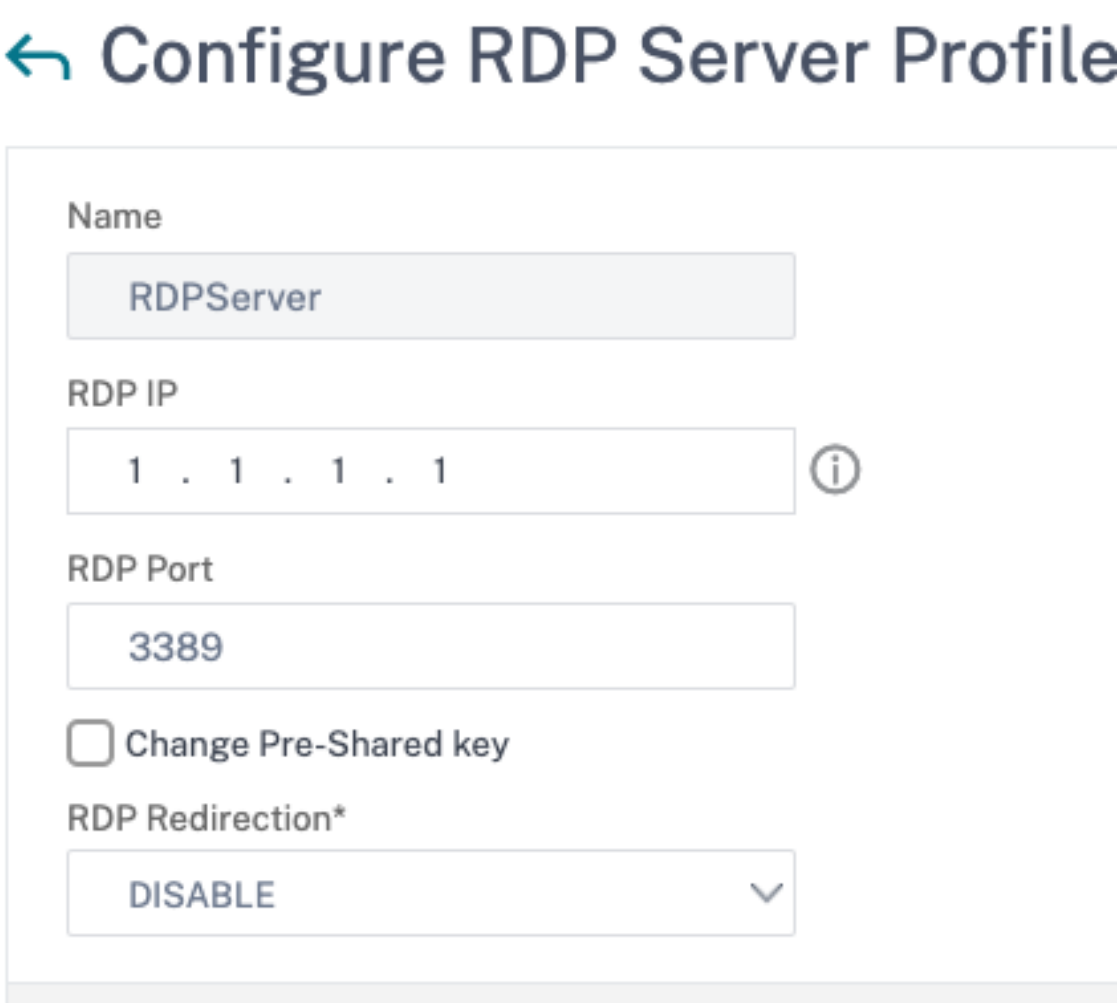
1. Accédez à **NetScaler Gateway > Stratégies**, cliquez avec le bouton droit sur **RDP**, puis cliquez sur **Activer la fonctionnalité**.
2. Cliquez sur RDP dans le volet de navigation. Sur la droite, sélectionnez l'onglet **Profils client**, puis cliquez sur **Ajouter**.
3. Entrez un nom pour le profil client et configurez-le.



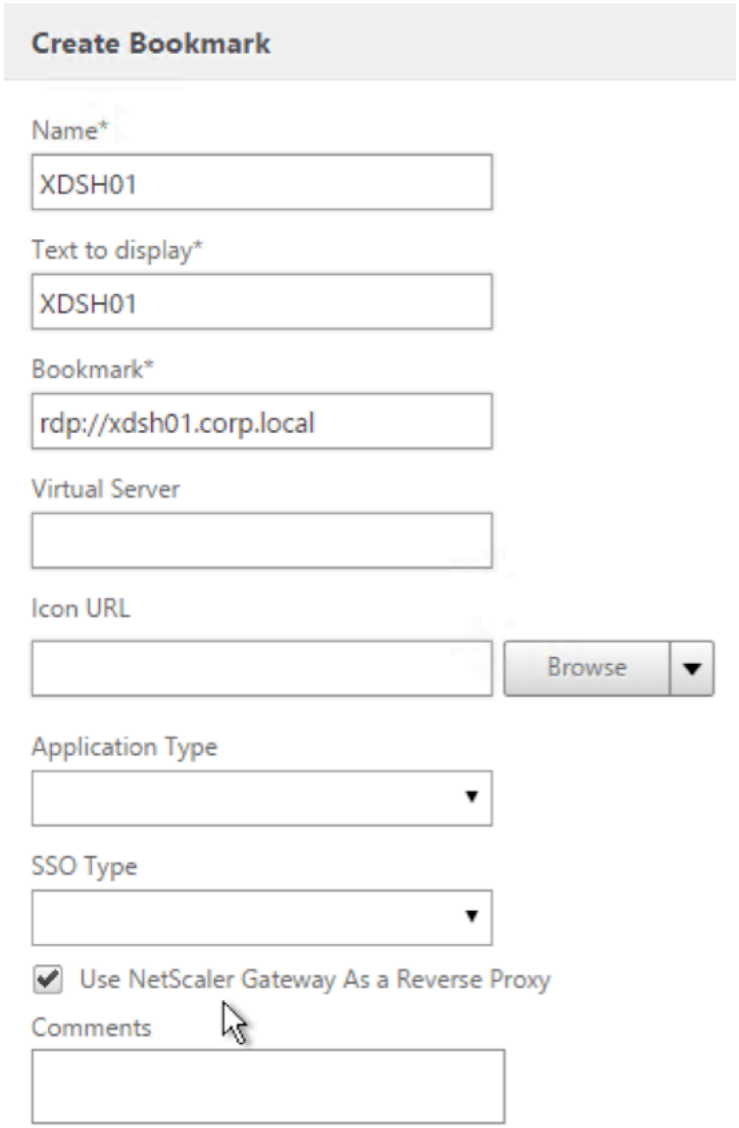
4. Dans le champ Hôte RDP, entrez le nom de domaine complet correspondant à l'écouteur proxy RDP, qui est généralement le même que le FDQN de l'appliance NetScaler Gateway.
5. Dans **Clé pré-partagée**, saisissez un mot de passe et cliquez sur **OK**.



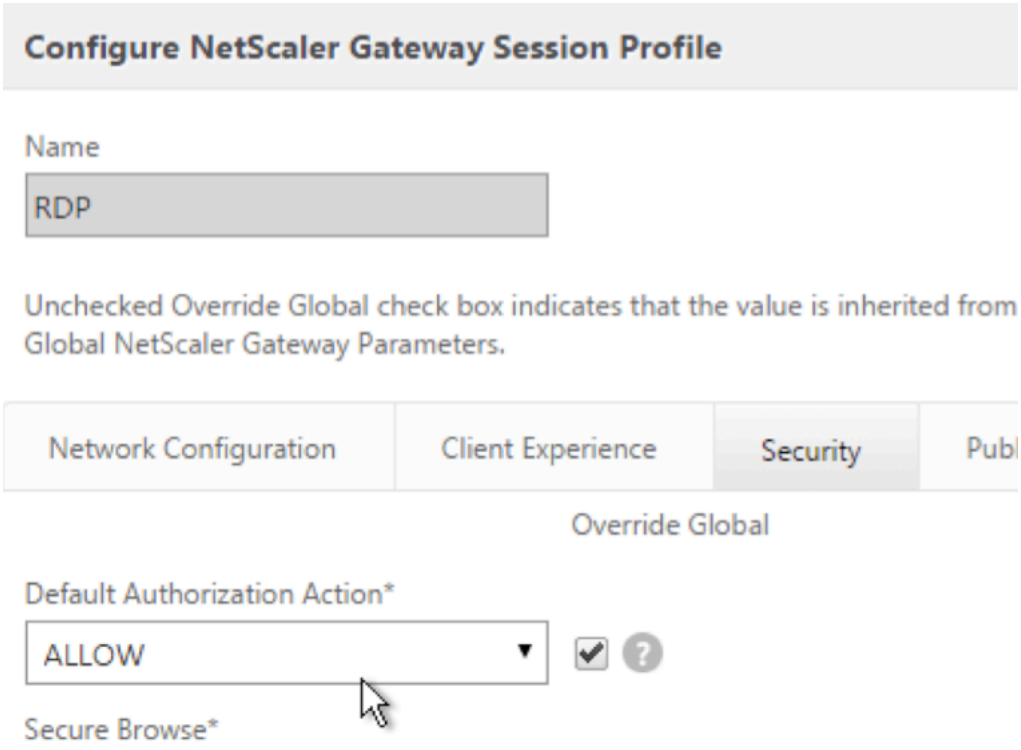
6. Entrez un nom pour le profil de serveur.
7. Entrez l'adresse IP du serveur virtuel de passerelle auquel vous allez lier ce profil.
8. Entrez la même clé prépartagée que celle que vous avez configurée pour le profil client RDP. Cliquez sur **Créer**.



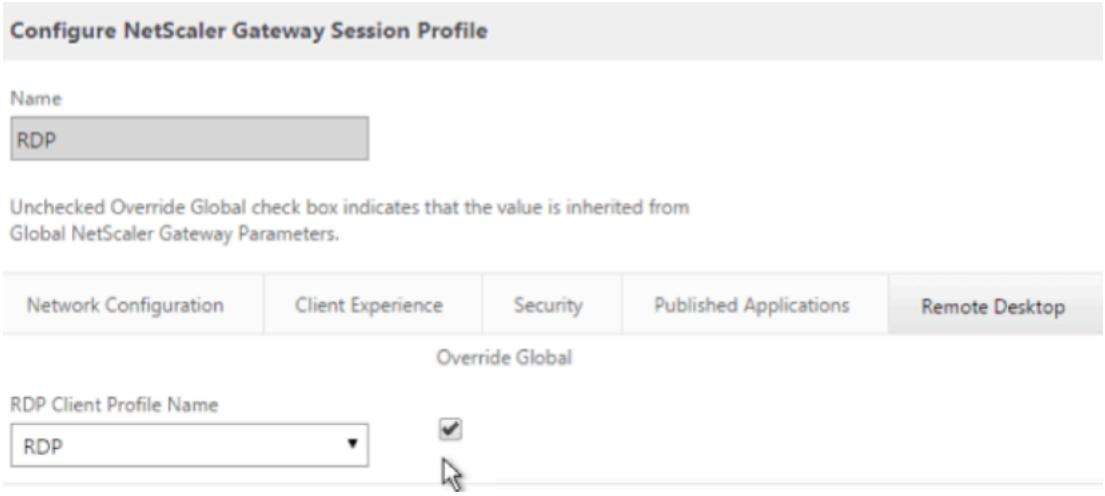
9. Si vous souhaitez ajouter des signets RDP sur la page du portail Accès sans client, sur la gauche, développez **NetScaler Gateway**, développez **Ressources**, puis cliquez sur **Signets**.
10. Sur la droite, cliquez sur **Ajouter**.
11. Donnez un nom au signet.
12. Pour l'URL, saisissez **rdp : //MyRDPServer en utilisant IP ou DNS**.
13. Sélectionnez Utiliser **NetScaler Gateway en tant que proxy inverse**, puis cliquez sur **Créer**.
14. Créez des signets selon vos besoins.



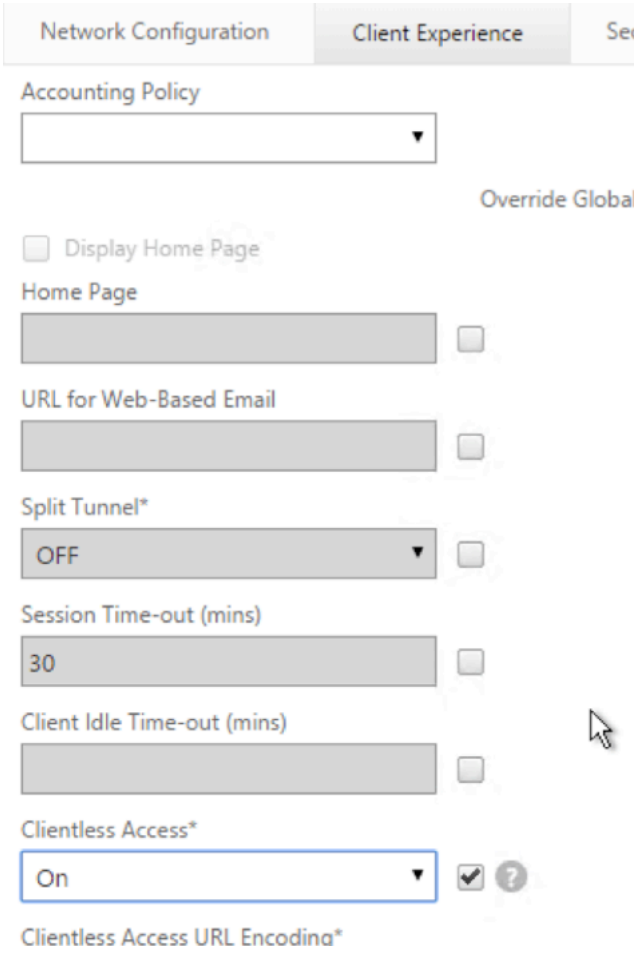
15. Créez ou modifiez un profil de session. Accédez à **NetScaler Gateway > Stratégies**Session.
16. Dans l'onglet Sécurité, définissez l'**action d'autorisation par défaut** sur **AUTORISER**. Vous pouvez également utiliser des stratégies d'autorisation pour contrôler l'accès.



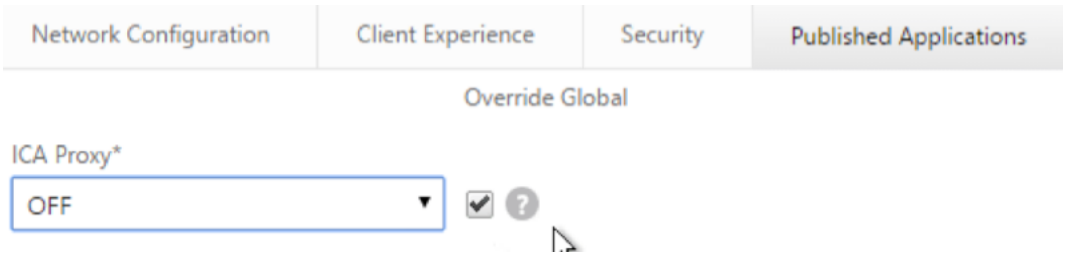
17. Dans l'onglet Bureau à distance, sélectionnez le profil de client RDP que vous avez créé précédemment.



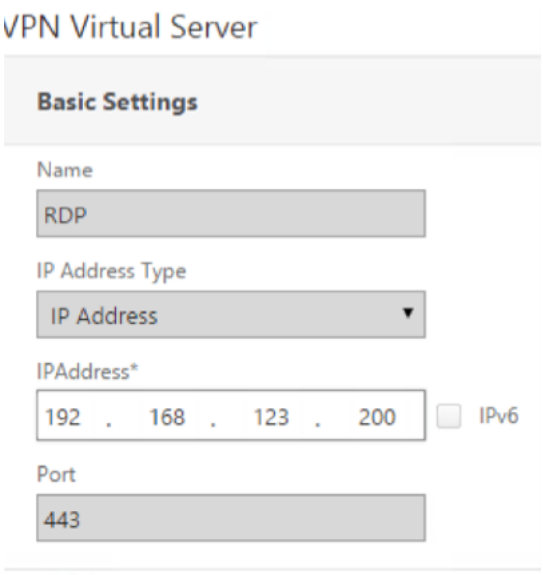
18. Si vous souhaitez utiliser des signets, sous l'onglet **Expérience client**, définissez **Accès sans clientsur On**.



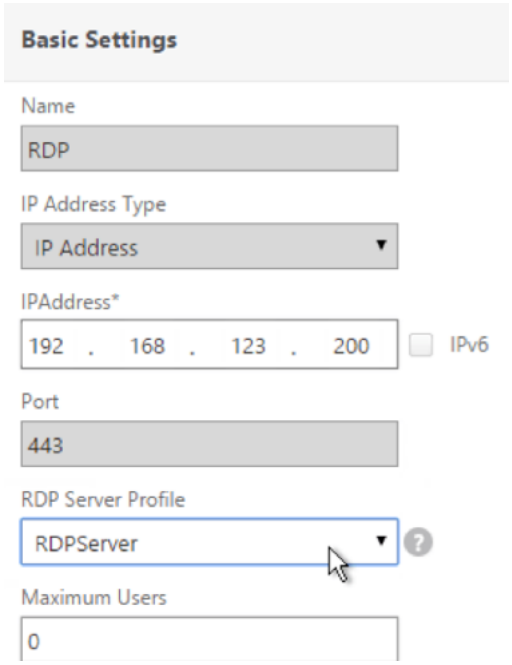
19. Dans l'onglet **Applications publiées**, assurez-vous que le proxy ICA est **désactivé**.



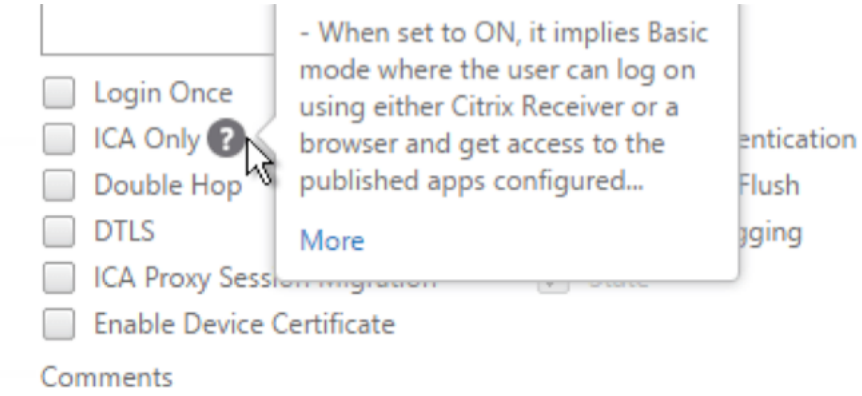
20. Modifiez ou créez votre serveur virtuel de passerelle.
21. Dans la section **Paramètres de base**, cliquez sur **Plus**.



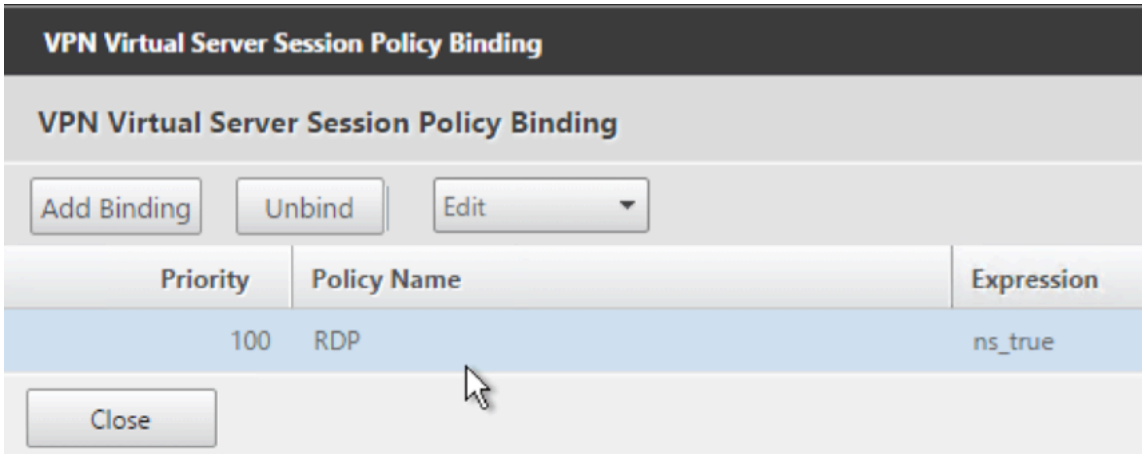
22. Utilisez la liste des profils de serveur RDP pour sélectionner le profil de serveur RDP que vous avez créé précédemment.



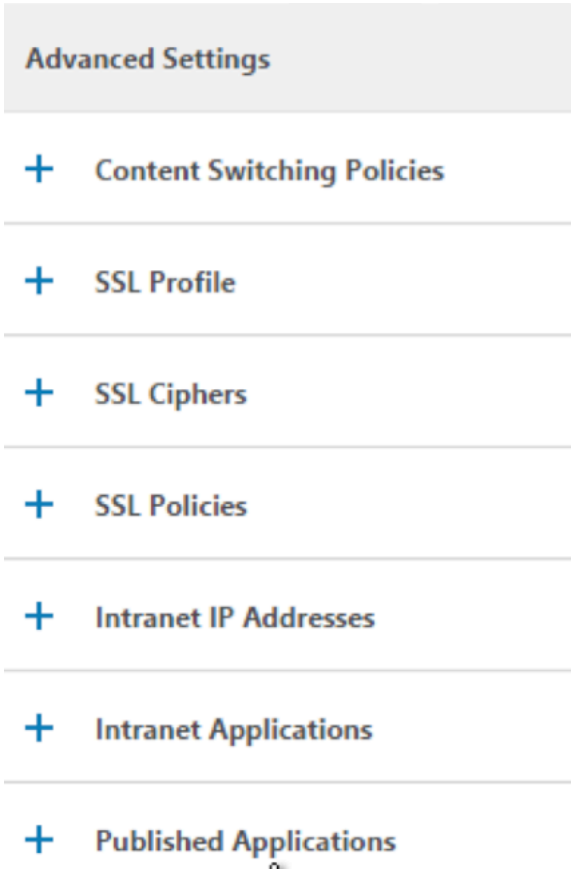
23. Faites défiler vers le bas. Assurez-vous que l'option **ICA uniquement n'** est pas cochée.



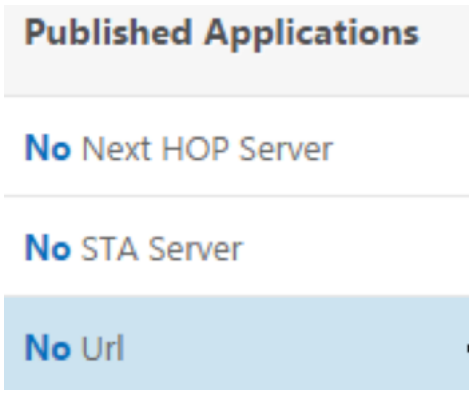
24. Liez un certificat.
25. Lier les stratégies d'authentification.
26. Liez la stratégie/le profil de session sur lequel le profil client RDP est configuré.



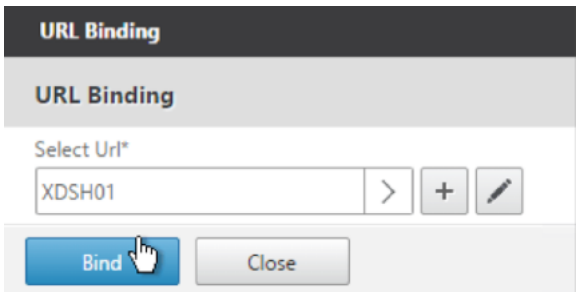
27. Vous pouvez lier des signets au serveur virtuel NetScaler Gateway ou à un groupe d'authentification, d'autorisation et d'audit. Pour établir une liaison avec le serveur virtuel NetScaler Gateway, sur la droite, dans la section Paramètres avancés, cliquez sur Applications **publiées**.



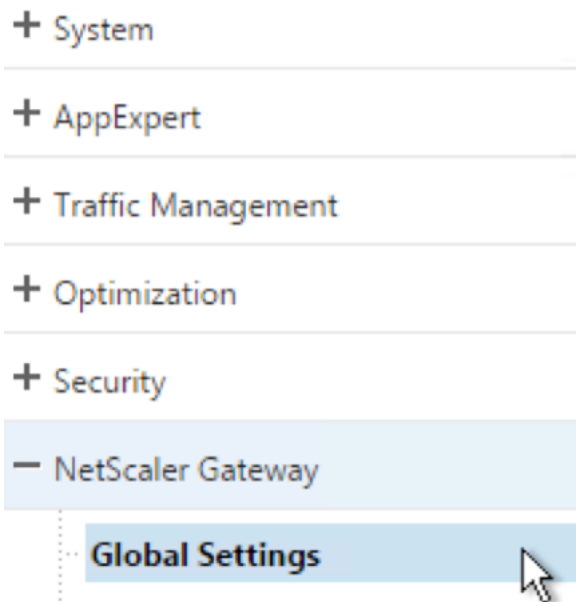
28. Sur la gauche, dans la section **Applications publiées**, cliquez sur **Aucune URL**.



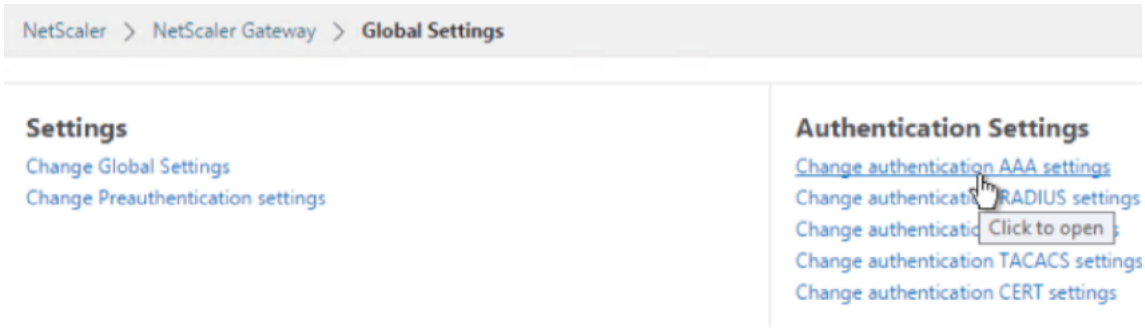
29. Liez vos signets.



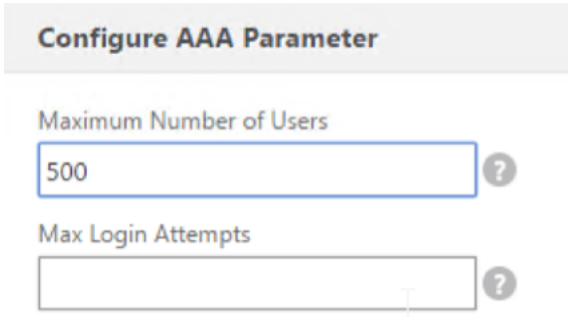
30. Comme ICA Only n'est pas spécifié pour ce serveur virtuel NetScaler Gateway, assurez-vous que vos licences NetScaler Gateway Universal sont correctement configurées. Sur la gauche, développez **NetScaler Gateway** et cliquez sur Paramètres **généraux**.



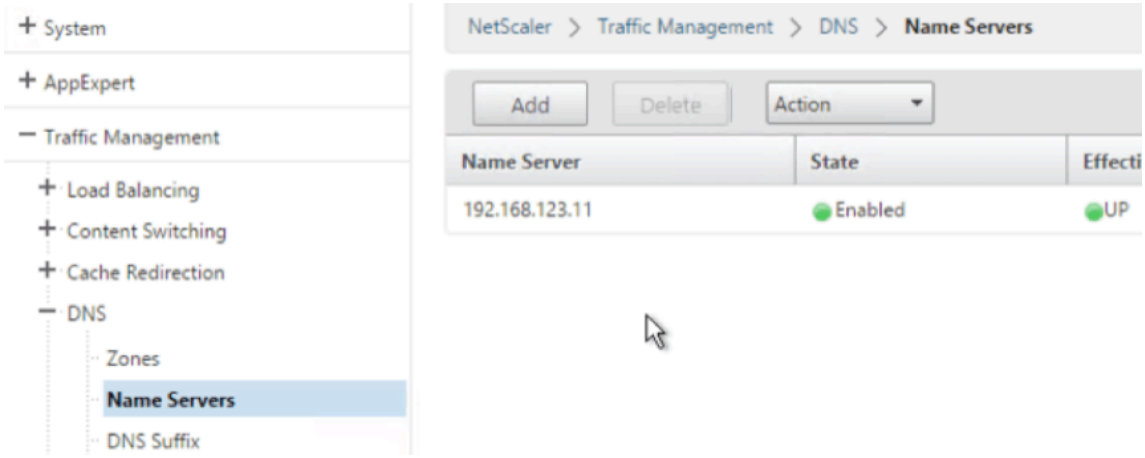
31. Sur la droite, cliquez sur **Modifier les paramètres AAA d'authentification**.



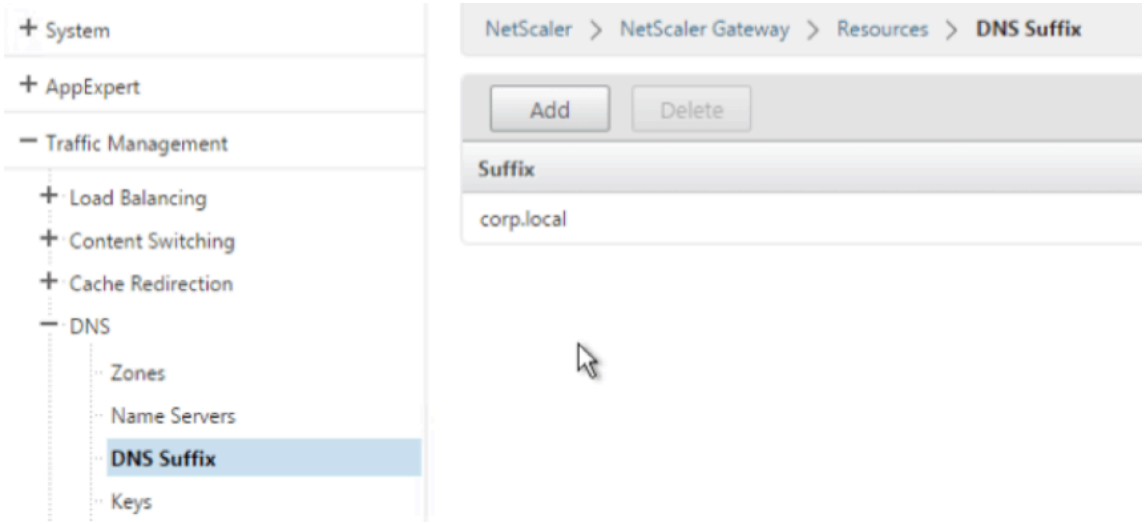
32. Modifiez le **nombre maximal d'utilisateurs** en fonction de votre limite de licence.



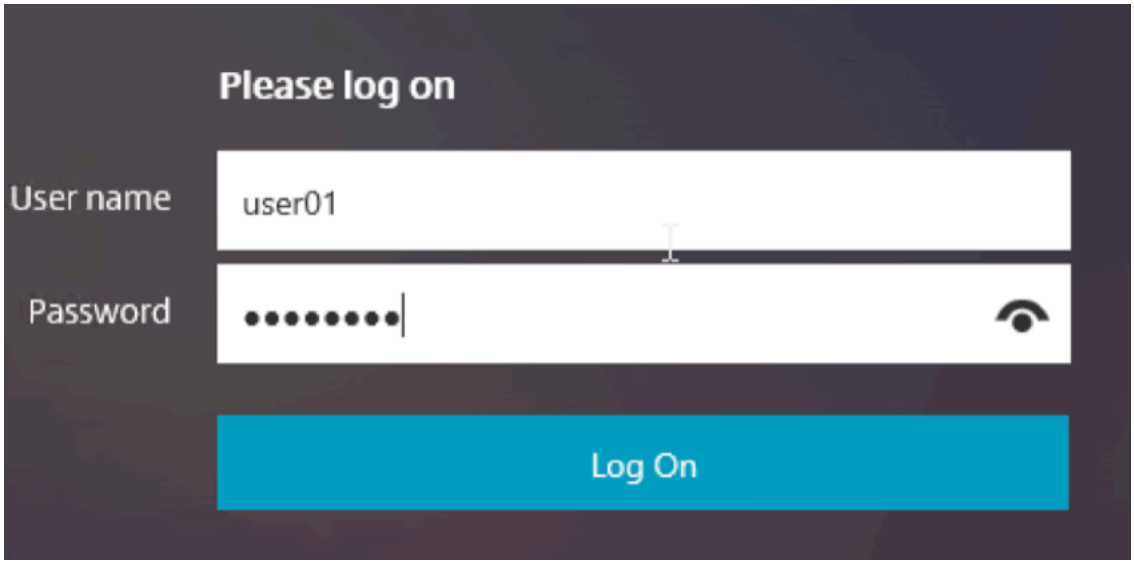
33. Si vous souhaitez vous connecter aux serveurs RDP à l'aide du DNS, assurez-vous que les serveurs DNS sont configurés sur l'appliance (**Gestion du trafic > DNS > Serveurs de noms)**.



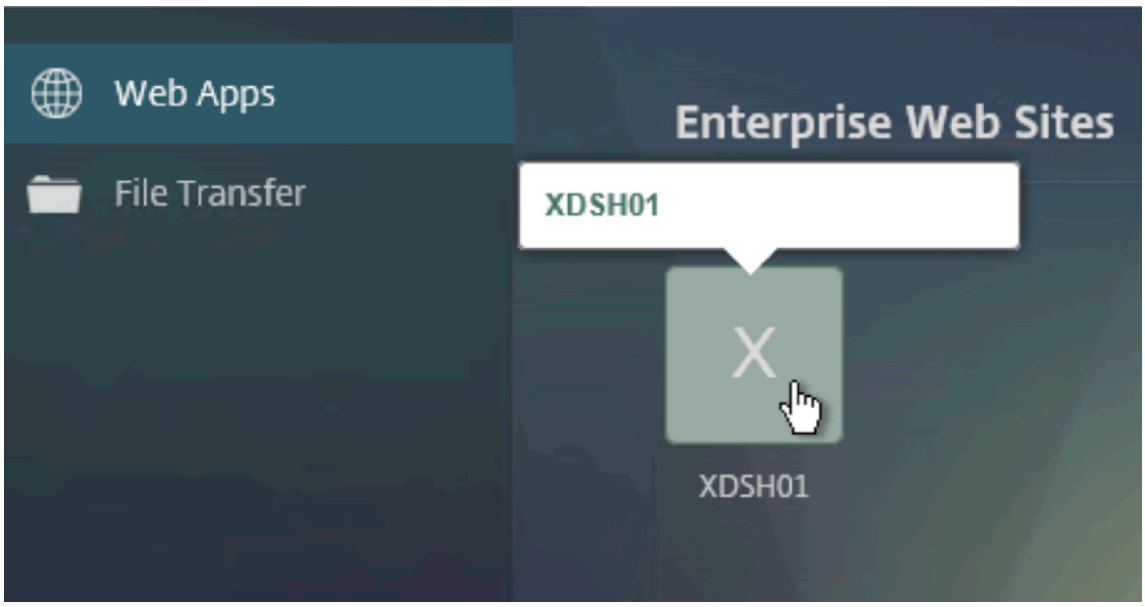
34. Si vous souhaitez utiliser les noms courts au lieu des noms complets, ajoutez un **suffixe DNS (Gestion du trafic > DNS > Suffixe DNS)**.



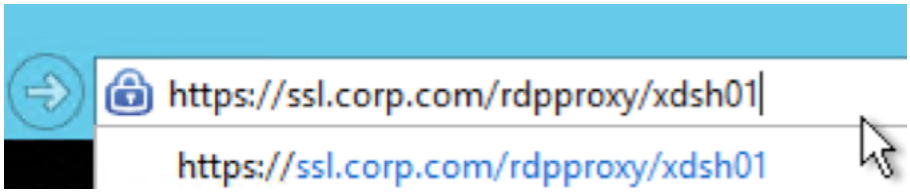
35. Connectez-vous à votre passerelle et ouvrez une session.



36. Si vous avez configuré des **signets**, cliquez sur le **signet**.

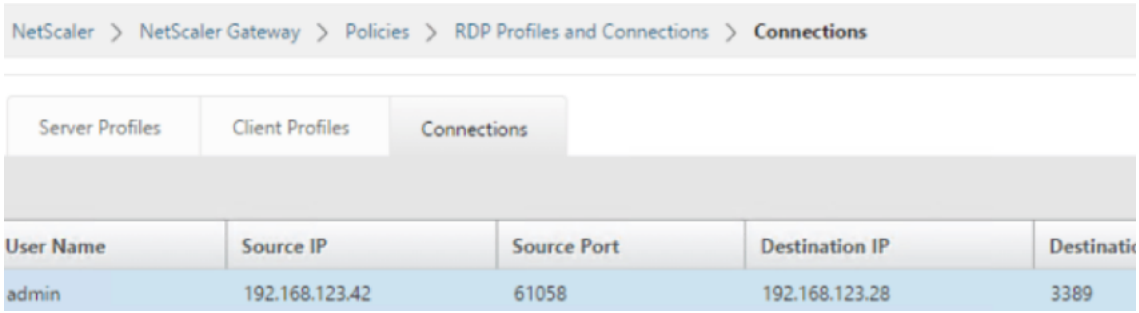


37. Vous pouvez modifier la barre d'adresse en **/RDPProxy/MyRDPServer**. Vous pouvez entrer une adresse IP (par exemple rdpproxy/192.168.1.50) ou un nom DNS (/rdpproxy/monserveur).



38. Ouvrez le fichier téléchargé `.rdp file`.

39. Vous pouvez consulter les utilisateurs actuellement connectés en accédant à **NetScaler Gateway Policies**RDP. Sur la droite se trouve l'onglet **Connexions**.



Option de désactivation de l'SSO

La fonctionnalité SSO (authentification unique) avec le proxy RDP peut être désactivée en configurant les stratégies de trafic NetScaler afin que l'utilisateur soit toujours invité à fournir des informations d'identification. Lorsque l'accès SSO est désactivé, l'application RDP (SmartAccess) ne fonctionne pas.

Exemple:

```
add vpn trafficaction <TrafficActionName> HTTP -SSO OFF
<!--NeedCopy-->
```

La stratégie de trafic peut être configurée conformément aux exigences. Voici deux exemples :

- Pour désactiver l'accès SSO pour tout le trafic, procédez comme suit :

```
add vpn trafficpolicy <TrafficPolicyName>  "url contains rdpproxy
   " <TrafficActionName>
<!--NeedCopy-->
```

- Pour désactiver l'accès unique en fonction de l'adresse IP source/destination/nom de domaine complet

```
add vpn trafficPolicy <TrafficPolicyName>  "HTTP.REQ.URL.CONTAINS
   ("rdpproxy") && CLIENT.IP.SRC.EQ(<IP>)" <TrafficActionName>
bind vpnvserver rdp -policy <TrafficPolicyName> -priority 10
<!--NeedCopy-->
```

Proxy RDP sans état

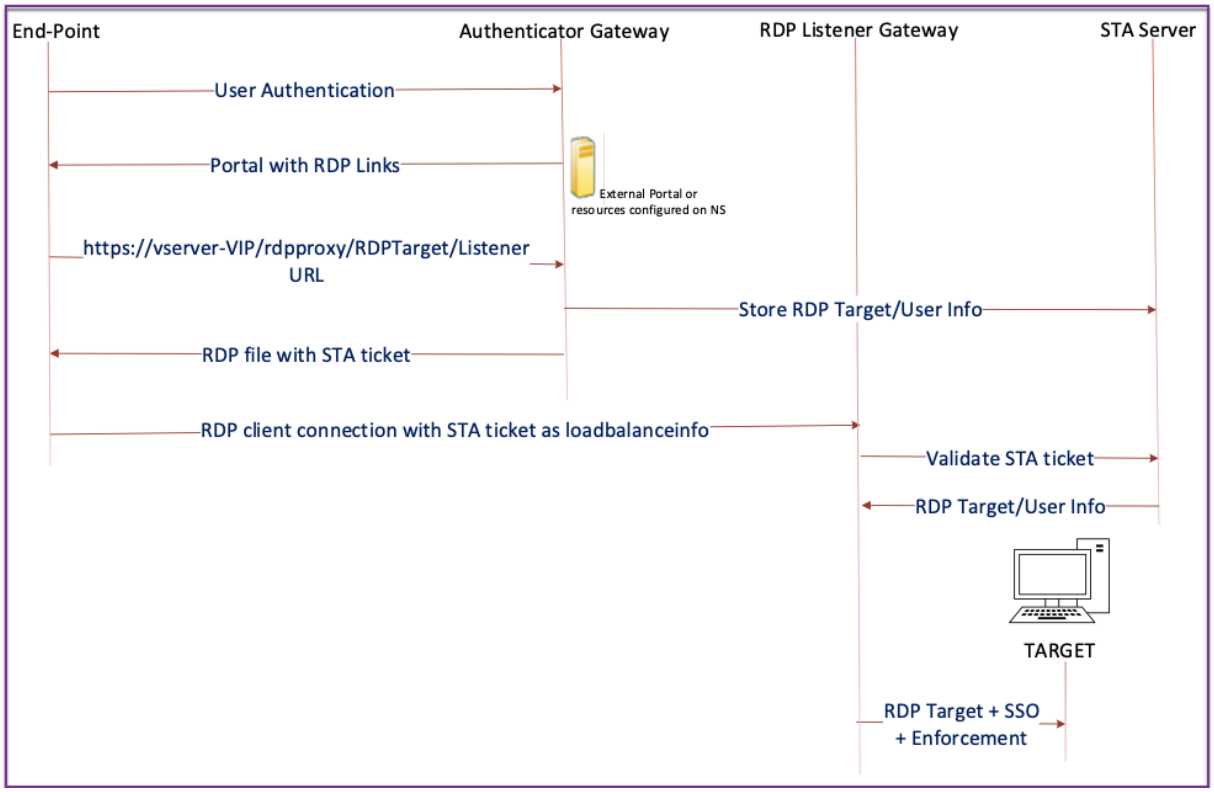
March 27, 2024

Le proxy RDP sans état accède à un hôte RDP. L'accès est accordé via NetScaler Gateway lorsque l'utilisateur s'authentifie sur un authentificateur NetScaler Gateway distinct. `RDPListener` Les informations requises par le `RDPListener` for NetScaler Gateway sont stockées de manière sécurisée sur un serveur STA. Un serveur STA peut être placé n'importe où tant que NetScaler Gateway et les serveurs d'énumération d'applications peuvent y accéder. Pour plus de détails, reportez-vous à https://support.citrix.com/article/CTX101997.

Flux de connexion

Deux connexions sont impliquées dans le flux proxy RDP. La première connexion est la connexion VPN SSL de l'utilisateur au NetScaler Gateway VIP et l'énumération des ressources RDP.

La deuxième connexion est la connexion native du client RDP à l'écouteur RDP (configuré à l'aide de RDPip et RDPport) sur NetScaler Gateway, et la transmission ultérieure du client RDP vers les paquets du serveur en toute sécurité.



1. L'utilisateur se connecte à la VIP Authenticator Gateway et fournit les informations d'identification.
2. Une fois la connexion réussie à la passerelle, l'utilisateur est redirigé vers la page d'accueil/portail externe qui énumère les ressources du poste de travail distant auxquelles l'utilisateur peut accéder.

3. Une fois que l'utilisateur a sélectionné une ressource RDP, une demande est reçue par le VIP Authenticator Gateway, dans le format `https://AGVIP/rdpproxy/ip:port/rdptargetproxy` indiquant la ressource publiée sur laquelle l'utilisateur a cliqué. Cette demande contient les informations relatives à l'adresse IP et au port du serveur RDP sélectionné par l'utilisateur.
4. La passerelle d'authentification traite la demande /rdpproxy/. Étant donné que l'utilisateur est déjà authentifié, cette demande est accompagnée d'un cookie de passerelle valide.
5. Les `RDPUser` informations `RDPTarget` et sont stockées sur le serveur STA et un ticket STA est généré. Les informations sont stockées sous la forme d'un objet blob XML qui est éventuellement chiffré à l'aide de la clé pré-partagée configurée. S'il est chiffré, le blob est codé et stocké en base64. La passerelle Authenticator utilise l'un des serveurs STA configurés sur le serveur virtuel de passerelle.
6. Le blob XML est au format suivant :

```
<Value name="IPAddress">ipaddr</Value>\n<Value name="Port">
    port</Value>n

<Value name="`Username`">username</Value>\n<Value name="
    Password">pwd</Value>
<!--NeedCopy-->
```

7. Le fichier `rdptargetproxy` obtenu dans la requête /rdpproxy/ est placé en tant que `fulladdress`" et le ticket STA (pré-ajouté avec l'AuthID STA) est placé `loadbalanceinfo` dans le fichier .rdp.
8. Le `.rdp` fichier est renvoyé au point de terminaison du client.
9. Le client RDP natif se lance et se connecte au `RDPListener Gateway`. Il envoie le ticket STA dans le paquet initial x.224.
10. Le `RDPListener Gateway` valide le ticket STA et obtient les `RDPUser` informations `RDPTarget` et. Le serveur STA à utiliser est récupéré à l'aide du 'AuthID'présent dans le `loadbalanceinfo`.
11. Une session de passerelle est créée pour stocker les stratégies d'autorisation/d'audit. Si une session existe pour l'utilisateur, elle est réutilisée.
12. Le `RDPListener Gateway` se connecte au `RDPTarget` et se connecte à l'aide de CREDSSP.

Pré-requis

- L'utilisateur est authentifié sur l'authentificateur NetScaler Gateway.
- L'URL /rdpproxy initiale et le client RDP sont connectés à un autre `RDPListener NetScaler Gateway`.

- La passerelle Authenticator utilisant un serveur STA transmet les `RDPListener Gateway` informations en toute sécurité.

Configurez le proxy RDP sans état à l'aide de l'interface de ligne de commande

- Ajoutez un `rdpServer` profil. Le profil de serveur est configuré sur le `RDPListener Gateway`.

  Remarque :

  - Une fois que le profil RDPServer est configuré sur le serveur virtuel VPN, il ne peut pas être modifié. De plus, le même ServerProfile ne peut pas être réutilisé sur un autre serveur virtuel VPN.

```
1  add rdpServer Profile [profilename] -rdpIP [IPV4 address of the
      RDP listener] -rdpPort [port for terminating RDP client
      connections] -psk [key to decrypt RDPTarget/RDPUser
      information, needed while using STA].
2  <!--NeedCopy-->
```

  Configurez le profil du serveur RDP sur le serveur virtuel VPN à l'aide de la commande suivante :

```
1  add vpn vserver v1 SSL [publicIP] [
      portforterminatingvpnconnections] -rdpServerProfile [rdpServer
       Profile]
2  <!--NeedCopy-->
```

  Exemple

```
1  add vpn vserver v1 SSL 1.1.1.1 443 -rdpServerProfile
      rdp_server_prof
2  <!--NeedCopy-->
```

  Important :

  - Le même serveur STA doit être lié à la fois à la passerelle d'authentification RDP et à la passerelle d'écoute.
  - Pour un proxy RDP apatride, le serveur STA valide le ticket STA envoyé par le client RDP pour obtenir les informations du serveur cible RDP et de l'utilisateur RDP. Vous devez lier le serveur STA en plus du serveur virtuel VPN. Dans l'exemple suivant, le serveur cible RDP est 1.1.1.0 et le serveur virtuel de passerelle d'écoute RDP 1.1.1.2.

```
1       add vpn url url4 RDP2 "rdp://1.1.1.0/1.1.1.2:443"
2   <!--NeedCopy-->
```

Configurez le profil client sur la passerelle d'authentification à l'aide de la commande suivante :


```
add rdpClient profile <name> -rdpHost <optional FQDN that will be put
    in the RDP file as ' fulladdress '> [-rdpUrlOverride ( ENABLE |
    DISABLE )] [-redirectClipboard ( ENABLE | DISABLE )] [-
    redirectDrives ( ENABLE | DISABLE )]

        [-redirectPrinters ( ENABLE | DISABLE )] [-keyboardHook <
            keyboardHook>] [-audioCaptureMode ( ENABLE | DISABLE )] [-
            videoPlaybackMode ( ENABLE | DISABLE )]

        [-rdpCookieValidity <positive_integer>][-multiMonitorSupport (
            ENABLE | DISABLE )] [-rdpCustomParams <string>]
<!--NeedCopy-->
```

La configuration —RDPHHost est utilisée dans un déploiement de passerelle unique. Seul `psk` est un argument obligatoire et il doit s'agir du même PSK que celui ajouté dans le profil du serveur RDP dans la passerelle d'écoute RDP.

- Associez le profil RDP au serveur virtuel VPN.

Vous pouvez associer un profil RDP en configurant une SessionAction+SessionPolicy ou en définissant le paramètre VPN global.

Exemple :

```
add vpn sessionaction <actname> -rdpClientprofile <rdpprofilename>

add vpn sessionpolicy <polname> NS_TRUE <actname>

bind vpn vserver <vservername> -policy <polname> -priority <
    prioritynumber>
<!--NeedCopy-->
```

OU

```
set vpn parameter  – rdpClientprofile <name>
<!--NeedCopy-->
```

Configurez le proxy RDP sans état à l'aide de l'interface graphique

Les étapes de haut niveau suivantes sont impliquées dans la configuration du proxy RDP sans état. Pour connaître les étapes détaillées, reportez-vous à la section Configuration du proxy RDP.

- Créer un profil de serveur RDP
- Créer un profil client RDP
- Créer un serveur virtuel
- Créer un signet
- Créer ou modifier un profil ou une stratégie de session

- Liez un signet

> **Important :**
>
> Pour le proxy RDP sans état, vous devez lier un serveur STA en plus du serveur virtuel VPN.

Compteur de connexion

Un nouveau compteur de connexions ns_rdp_tot_curr_active_conn a été ajouté, qui conserve l'enregistrement du nombre de connexions actives en cours d'utilisation. Il peut être considéré comme faisant partie de la `nsconmsg` commande sur le shell NetScaler. La commande CLI pour afficher ces compteurs devrait être ajoutée ultérieurement.

Notes de mise

Le RDPip et le port RDPport, qui étaient précédemment configurés sur le serveur virtuel VPN, font partie du profil RDPServerProfile. Le paramètre `rdp Profile` est renommé `rdp ClientProfile` et le paramètre ClientSSL est supprimé. Par conséquent, la configuration précédente ne fonctionne pas.

Redirection de connexion RDP

March 27, 2024

Une appliance NetScaler Gateway prend désormais en charge la redirection de connexion RDP en présence d'un broker de connexion ou d'un répertoire de sessions. Une communication proxy RDP ne nécessite plus d'URL exclusive pour chaque connexion entre le client et le serveur. Au lieu de cela, le proxy utilise une URL unique pour se connecter à une batterie de serveurs RDP, ce qui réduit les frais de maintenance et de configuration pour un administrateur.

Point à noter:

- La redirection de connexion RDP n'est prise en charge que lorsque l'authentification unique est activée et est prise en charge en mode passerelle unique et sans état ou double passerelle avec application (SmartAccess).
- La fonctionnalité de proxy RDP est prise en charge uniquement avec la redirection basée sur des jetons prenant en charge les cookies IP. Les jetons de routage basés sur IP « msts= » sont remis par le broker de session Windows ou le courtier de connexion lorsque la fonctionnalité **Utiliser la redirection d'adresse IP** est désactivée.

- Vous pouvez désactiver le paramètre **Utiliser la redirection d'adresse IP** pour activer la redirection basée sur des jetons à l'emplacement suivant.
  `Computer Configuration > Policies > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > RD Connection Broker`.
- Désactivez le paramètre Utiliser la redirection d'adresses IP sur les machines RDSH et non sur la machine du broker de connexion.
- Des redirecteurs dédiés pour la connexion proxy RDP peuvent être configurés.

Pré-requis

- Créez un profil de serveur RDP pour activer l'écouteur 3389 sur le serveur virtuel NetScaler Gateway.
  Si la machine que vous souhaitez utiliser RDP n'est membre d'aucune infrastructure de broker de connexion RDS, vous n'avez pas besoin de l'écouteur 3389.
- Activez la redirection de connexion RDP sur l'appliance NetScaler Gateway pour prendre en charge le proxy RDP en présence d'un broker de connexion.

Déployer le proxy RDP en présence d'un broker de connexion

Le proxy RDP en présence d'un broker de connexion peut être déployé de deux manières différentes.

- Avec les serveurs hôtes de session Bureau à distance participant à l'équilibrage de charge du broker de connexion Bureau à distance.
- En présence de la fonctionnalité d'équilibrage de charge RDP.

Avec les serveurs hôtes de session Bureau à distance participant à l'équilibrage de charge du broker de connexion Bureauà distance :

Dans ce cas, le lien URL RDP peut être configuré pour pointer vers l'un des serveurs RDP en tant que serveur de destination, qui agit en tant que redirecteur. Il est également possible d'avoir l'un des serveurs RDP de la batterie de serveurs en tant que serveur de destination (dans ce cas, le serveur n'accepte aucune session RDP).

En présence de la fonctionnalité d'équilibrage de charge RDP :

Lorsque l'équilibrage de charge du broker de connexion n'est pas activé, la fonctionnalité d'équilibrage de charge RDP peut être disponible sur NetScaler pour effectuer l'équilibrage de charge requis des sessions RDP en présence d'un broker de connexion. Dans ce cas, le lien URL RDP doit être configuré pour que l'équilibreur de charge RDP soit utilisé comme serveur de destination. L'équilibreur

de charge RDP peut se trouver sur le même dispositif NetScaler Gateway que le proxy RDP. Pour plus d'informations, consultez la section Équilibrage de chargement des serveurs RDP.

Configurez le proxy RDP en présence d'un broker de connexion à l'aide de l'interface de ligne de commande

À l'invite de commande, tapez ;

```
add rdpserverprofile <Name> -psk <string> -rdpRedirection ( ENABLE |
    DISABLE )

add rdpserverprofile serverProfileName -psk " secretString " -
    rdpRedirection ENABLE
<!--NeedCopy-->
```

Configurer la redirection de connexion RDP à l'aide de l'interface graphique NetScaler

1. Accédez à **NetScaler Gateway > Politiques > RDP**.
2. Cliquez avec le bouton droit de la souris sur **RDP** pour **activer** ou **désactiver** la fonctionnalité de redirection RDP.

Renseigner les URL RDP en fonction de l'attribut LDAP

March 27, 2024

Vous pouvez configurer une appliance NetScaler Gateway pour récupérer une liste de serveurs RDP (IP/FQDN) à partir d'un attribut de serveur LDAP. En fonction de la liste récupérée, l'appliance affiche les URL RDP des serveurs auxquels un utilisateur peut accéder.

Pour renseigner les URL RDP en fonction de l'attribut LDAP à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add rdpclientprofile <Name>  – rdpUrlLinkAttribute <string>

add rdpclientprofile clientProfileName  – rdpUrlLinkAttribute
    rdpServerAttribute

<!--NeedCopy-->
```


Dans l'exemple précédent, RDPServerAttribute correspond aux détails du serveur RDP pour un utilisateur donné sur le serveur LDAP.

Remarque : Pour récupérer les détails de l'attribut LDAP à partir du serveur LDAP, l'action LDAP doit être configurée avec la même chaîne que celle qui est configurée `pUrlLinkAttribute` comme suit.

```
add authentication ldapAction dnpg_ldap -serverIP <IP address>-ldapBase
     <"domain name"> -ldapBindDn <username> -ldapLoginName
    sAMAccountName -ldapbindDnpassword <password>

add authentication ldapAction dnpg_ldap -serverIP 10.102.39.101 -
    ldapBase "dc=dnpg-blr,dc=com" -ldapBindDn sqladmin@dnpg-blr.com -
    ldapLoginName sAMAccountName -ldapbindDnpassword xxxx

add authentication ldapPolicy dnpg_ldap_pol ns_true dnpg_ldap

bind vpn vs vserver<name> -pol dnpg_ldap_pol

set ldapaction dnpg_ldap -attributes "rdpServerAttribute"

set rdpclientprofile ldap -rdpLinkAttribute rdpServerAttribute
<!--NeedCopy-->
```

Configuration du serveur LDAP

Sur le serveur LDAP, effectuez les opérations suivantes :

1. Accédez à un **utilisateur**particulier.
2. Dans **Utilisateurs et ordinateurs AD**, cliquez sur **Afficher**, puis sur **Détails.**
3. Cliquez avec le bouton droit sur **le nom d'utilisateur** et cliquez sur **Éditeur d'attributs**
4. Modifiez la valeur de l'attribut requis (DisplayName) et cliquez sur **OK.**

Pour renseigner les URL RDP en fonction de l'attribut LDAP à l'aide de l'interface graphique

1. Accédez à **NetScaler Gateway > Politiques > RDP**.
2. Sur la page **Profils et connexions RDP**, cliquez sur l'onglet **Profils client** et sélectionnez le profil client dans lequel vous souhaitez configurer l'attribut de lien RDP.
3. Dans la page **Configurer le profil du clientRDP, dans Attribut de lien RDP**, entrez le nom de l'attribut LDAP.

   Remarque : La valeur de l'attribut LDAP peut être une liste séparée par des virgules.

Randomiser le nom du fichier RDP avec le proxy RDP

March 27, 2024

Lorsque vous cliquez sur une URL RDP, un fichier RDP est téléchargé. Lorsque vous cliquez à nouveau sur **l'URL** RDP, un nouveau fichier RDP portant le même nom est téléchargé, ce qui entraîne l'affichage d'une fenêtre contextuelle permettant de remplacer le nouveau fichier par le fichier existant. Pour éviter cela, l'administrateur peut opter pour une attribution aléatoire du nom du fichier RDP. Le nom de fichier est maintenant aléatoire en ajoutant la sortie de la fonction time () au format <rdpFileName>_<outputof time()>.rdp. Ce faisant, l'appliance génère un nom de fichier RDP unique chaque fois que vous téléchargez un fichier.

Configuration de la prise en charge de la randomisation du nom de fichier RDP avec le proxy RDP

Pour configurer la prise en charge de la randomisation du nom de fichier RDP avec le proxy RDP à l'aide de l'interface de ligne de commande à l'invite de commande, tapez :

```
1     add rdpclientprofile <profileName> -rdpfileName <filename> -
          randomizeRDPFilename <YES/NO>
2
3     add rdpclientprofile clientProfileName -rdpfileName testRDP -
          randomizeRDPFilename YES
4 <!--NeedCopy-->
```

Pour configurer la prise en charge de la randomisation du nom de fichier RDP avec le proxy RDP à l'aide de l'interface graphique NetScaler :

1. ****Accédez à **NetScaler Gateway > Politiques > RDP** .**
2. Sur la page **Profils et connexions RDP**, cliquez sur l'onglet **Profils client** et sélectionnez le profil client dans lequel vous souhaitez configurer la fonctionnalité de nom de fichier RDP aléatoire.
3. Sur la page **Configurer le profil du client RDP**, sélectionnez **OUI** dans le menu en regard du champ **Nom de fichier RDP aléatoire**.

Configurer le nom des fichiers RDP

March 27, 2024

Lors du téléchargement d'un fichier RDP, il peut être stocké localement avec le nom de fichier configuré.

Configurer un nom pour les fichiers RDP

Pour configurer un nom pour les fichiers RDP à l'aide de l'interface de ligne de commande, tapez :**

```
set rdpclientprofile <Name> -rdpfilename <filename>.rdp
<!--NeedCopy-->
```

Pour configurer un nom pour les fichiers RDP à l'aide de l'interface graphique :

1. ****Accédez à **NetScaler Gateway > Politiques > RDP** .**
2. Sur la page **Profils et connexions RDP**, cliquez sur l'onglet **Profils client**. Sélectionnez le profil client dans lequel vous souhaitez configurer une fonctionnalité de nom de fichier RDP aléatoire.
3. Sur la page **Configurer le profil du client RDP**, entrez un nom pour le profil RDP dans le champ **Nom du fichier RDP**. Le nom du fichier doit être au format suivant : . Un maximum de 31 caractères sont autorisés pour le nom.

Prise en charge du proxy ICA sortant

January 26, 2024

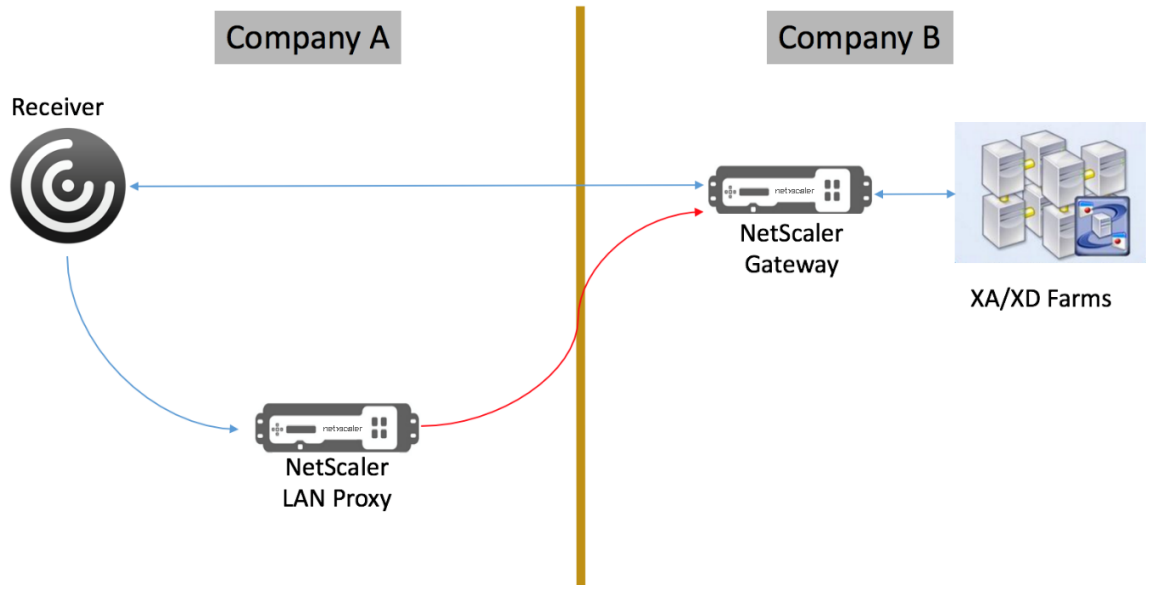
La prise en charge du proxy ICA sortant pour NetScaler Gateway permet aux administrateurs réseau de bénéficier des fonctionnalités SmartControl même lorsque Receiver et NetScaler Gateway sont déployés dans différentes organisations.

Le scénario suivant illustre l'utilisation de la solution de proxy ICA sortant :

Un administrateur réseau doit contrôler les fonctionnalités liées aux sessions ICA lorsque Receiver et NetScaler Gateway sont déployés dans différentes organisations.

Présentation de la prise en charge du proxy ICA sortant

Pour apporter la fonctionnalité SmartControl à l'organisation de l'entreprise, la société A, qui possède le récepteur, nous devons ajouter une appliance NetScaler qui fait office de proxy LAN. Le proxy réseau NetScaler applique SmartControl et transmet le trafic par proxy au NetScaler Gateway de la société B. Dans ce scénario de déploiement, le récepteur transmet le trafic au proxy réseau NetScaler LAN, ce qui permet à l'administrateur réseau de l'entreprise A d'appliquer SmartControl. Le déploiement est illustré dans la figure suivante.



Dans ce scénario, le trafic entre le proxy LAN et NetScaler Gateway passe par SSL.

> **Remarque :** N'activez pas l'authentification basée sur un certificat client sur NetScaler Gateway.

Support SSL sur le proxy NetScaler LAN

À partir de la version 13.0 build xx.xx, le trafic entre l'application Citrix Workspace et le proxy réseau NetScaler est également pris en charge via SSL. L'application Citrix Workspace chiffre le trafic qu'elle envoie au proxy LAN via SSL. La prise en charge SSL sur le proxy LAN peut coexister avec le déploiement existant.

Pour activer le chiffrement du trafic via SSL entre l'application Citrix Workspace et le proxy réseau NetScaler, vous devez effectuer les opérations suivantes sur le proxy réseau NetScaler :

- Désactivez l'authentification et activez le double saut sur le serveur virtuel VPN.
- Définissez l'hôte sur le client Windows sur l'adresse IP du serveur virtuel VPN.
- Activez la validation du SNI et du certificat.
- Ajoutez les certificats d'autorité de certification appropriés et activez-les globalement.

Configuration du proxy ICA sortant

March 27, 2024

La configuration du proxy ICA sortant implique la configuration du proxy réseau NetScaler et de NetScaler Gateway.

Configurer le proxy réseau NetScaler pour le proxy sortant ICA

Vous pouvez effectuer les étapes suivantes pour configurer le proxy ICA sortant à l'aide de l'interface de ligne de commande.

- Ajoutez un serveur virtuel VPN.

```
add vpn vserver <name> <serviceType> [<IPAddress> [-range <
    positive_integer>] [-ipset <string>]] [<port>] [-state (
    ENABLED | DISABLED )] [-authentication ( ON | OFF )] [-
    doubleHop ( ENABLED |DISABLED )]
<!--NeedCopy-->
```

- Définissez les paramètres du VPN.

```
set vpn parameter[-backendServerSni ( ENABLED | DISABLED )][-
    backendCertValidation ( ENABLED | DISABLED )]
<!--NeedCopy-->
```

- Ajoutez une paire de clés de certificat SSL.

```
add ssl certKey ca_cert_verify -cert <certificate name>
<!--NeedCopy-->
```

- Liez la paire de clés de certificat SSL à l'échelle mondiale.

```
bind vpn global -cacert ca_cert_verify
<!--NeedCopy-->
```

Exemple :

```
- add vpn vserver ssl_lan_proxy SSL 65.219.17.34 443 -authentication
    OFF - doubleHop ENABLED

- set vpn parameter backendserverSni ENABLED backendcertValidation
    ENABLED

- add ssl certKey dnpg_ca -cert dnpg_ca_cert.cer

- bind vpn global -cacert dnpg_ca

<!--NeedCopy-->
```

> **Remarque :**
>
> Pour la prise en charge du protocole SSL sur le proxy NetScaler LAN, aucune modification n'est requise dans la configuration de NetScaler Gateway.

Support du proxy PCoIP compatible avec NetScaler Gateway pour VMware Horizon View

January 26, 2024

NetScaler Gateway 12.0 prend en charge le protocole PC-over-IP (PCoIP), qui est le protocole d'affichage à distance pour plusieurs solutions VDI autres que Citrix, notamment VMware Horizon View. PCoIP est analogue au protocole Citrix HDX/ICA et au protocole Microsoft RDP. PCoIP utilise le port UDP 4172.

Lorsque PCoIP est transmis par proxy via NetScaler Gateway, NetScaler Gateway peut remplacer les solutions d'accès à distance PCoIP traditionnelles, telles que View Security Server ou VMware Access Point.

Les scénarios suivants illustrent l'utilisation de la solution VMware Horizon View compatible avec NetScaler Gateway.

- Utilisateurs de VMware Horizon PCoIP ayant besoin d'accéder à distance à des pools de postes de travail et à des pools d'applications VMware Horizon View via NetScaler Gateway sans déployer un serveur de sécurité Horizon View ou un point d'accès VMware.
- Les utilisateurs PCoIP accèdent à distance à d'autres solutions de bureau virtuel basées sur PCoIP via NetScaler Gateway.

> **Remarque**
>
> NetScaler Gateway est déployé en tant que solution d'accès à distance.

Configurer le proxy PCoIP compatible avec NetScaler Gateway pour VMware Horizon View

March 27, 2024

Pré-requis

Version : NetScaler 12.0 ou version ultérieure

Licence universelle : le proxy PCoIP utilise la fonctionnalité d'accès sans client de NetScaler Gateway, ce qui signifie que chaque connexion NetScaler Gateway doit être autorisée pour NetScaler Gateway

Universal. Sur le serveur virtuel NetScaler Gateway, assurez-vous que l'option **ICA Only est désactivée**.

Infrastructure Horizon View : infrastructure Horizon View interne fonctionnelle. Assurez-vous de pouvoir vous connecter aux agents Horizon View en interne sans NetScaler Gateway. Assurez-vous que le **tunnel sécurisé HTTP (S) d'Horizon View et la SecureGateway PCoIP** ne sont pas activés sur les serveurs de connexion View auxquels NetScaler fournira des connexions proxy.
Les versions suivantes de VMware Horizon View sont prises en charge.

- Serveur de connexion : 7.0.1 et supérieur
- Horizon Client : 4.2.0 et versions ultérieures (Windows et Mac)

Ports de pare-feu :

Vérifiez les points suivants.

- Les protocoles UDP 4172 et TCP 443 doivent être ouverts depuis les clients Horizon View vers NetScaler Gateway VIP.
- L'UDP 4172 doit être ouvert à partir du NetScaler SNIP à tous les agents Horizon View internes.
- Le proxy PCoIP est pris en charge sur NetScaler déployé derrière NAT. Voici les points importants à prendre en compte :
  - La prise en charge est basée sur le paramètre FQDN du serveur virtuel VPN
  - Prise en charge uniquement du nom de domaine complet accessible publiquement et non de l'adresse IP
  - Prise en charge uniquement des ports 443 et 4172
  - Il doit s'agir d'un NAT statique

Certificat : certificat valide pour le serveur virtuel NetScaler Gateway.

Authentification : stratégie/serveur d'authentification LDAP utilisant une syntaxe avancée.

Unified Gateway (facultatif) : si Unified Gateway, créez Unified Gateway avant d'ajouter la fonctionnalité PCoIP.

Thème du portail RFWebUI : pour accéder à Horizon View par navigateur Web, le serveur virtuel NetScaler Gateway doit être configuré avec le thème RFWebUI.

Horizon View Client : le client Horizon View doit être installé sur l'appareil client, même si vous accédez aux icônes publiées par Horizon via le portail NetScaler RFWebUI.

Pour configurer NetScaler Gateway afin qu'il prenne en charge le proxy PCoIP pour VMware Horizon View :

1. Accédez à **Configuration > NetScaler Gateway**Policies > PCoIP.
2. Créez un profil de serveur virtuel et un profil PCoIP sur la page **Profils et connexions PCoIP**.

a) Pour créer un profil de serveur virtuel, sous l'onglet **Profils vServer**, cliquez sur **Ajouter**.

b) Entrez le nom du profil de serveur virtuel.

c) Entrez un nom de domaine Active Directory utilisé pour l'authentification unique au Serveur de connexion View, puis cliquez sur **Créer.**
Remarque : Un seul domaine Active Directory est pris en charge par serveur virtuel NetScaler Gateway. De plus, le nom de domaine spécifié ici est affiché dans Horizon View Client.

d) Cliquez sur **Connexion**.

e) Pour créer un profil PCoIP, sous l'onglet **Profils**, cliquez sur **Ajouter**.

   i. Entrez le nom du profil PCoIP.

   ii. Entrez l'URL de connexion du serveur de connexion VMware Horizon View interne, puis cliquez sur **Créer**.

f) Accédez à **Configuration > NetScaler Gateway > Politiques**Session.

g) Sur la droite, sélectionnez l'onglet **Profils de session**.

h) Sur la page **Stratégies et profils de session NetScaler Gateway**, créez ou modifiez un profil de session NetScaler Gateway.

   i. Pour créer un profil de session NetScaler Gateway, cliquez sur **Ajouter**et donnez un nom.

   ii. **Pour modifier un profil de session NetScaler Gateway, sélectionnez le profil et cliquez sur Modifier.**

i) Dans l'onglet **Expérience client**, vérifiez que la valeur **Accès sans client** est définie **sur On**.

j) Dans l'onglet **Sécurité**, assurez-vous que la valeur de l'**action d'autorisation par défaut** est définie sur **ALLOW**.

k) Dans l'onglet **PCoIP**, sélectionnez le profil PCoIP requis, puis cliquez sur **Créer**. Vous pouvez également créer ou modifier des profils PCoIP à partir de cet onglet.

l) Cliquez sur **Créer** ou sur **OK** pour terminer la création ou la modification du profil de session.

m) Si vous avez créé un profil de session, vous devez également créer une stratégie de session correspondante.

   i. Accédez à **Configuration > NetScaler Gateway > Politiques**Session.

   ii. sélectionnez l'onglet **Stratégies de session**, puis cliquez sur **Ajouter**.

   iii. Sur la page Create NetScaler Gateway Session Policy, entrez le nom de la stratégie.

iv. Dans **Profil**, sélectionnez un profil existant ou cliquez sur **Ajouter** et créez un profil.

v. Ajoutez une expression.

A. Cliquez sur **Stratégie avancée**, puis sur **Éditeur d'expression**.
B. Dans **Expression**, sélectionnez l'expression selon vos besoins.

vi. Cliquez sur **OK.**

n) Liez le profil de serveur virtuel PCoIP et la stratégie de session créés à un serveur virtuel NetScaler Gateway.

i. Accédez à **NetScaler Gateway > Serveurs virtuels**.

ii. Sur la droite, **ajoutez** un nouveau serveur virtuel NetScaler Gateway ou **modifiez** un serveur virtuel NetScaler Gateway existant.

iii. Si vous modifiez un serveur virtuel NetScaler Gateway existant, dans la section **Paramètres de base**, cliquez sur l'icône en forme de crayon.

iv. Pour l'ajout et la modification, dans la section **Paramètres de base**, cliquez sur **Plus**.

v. Utilisez le menu **Profil vServer PCoIP pour sélectionner le profil** de serveur virtuel PCoIP requis.

vi. Faites défiler l'écran vers le bas et assurez-vous que l'ICA uniquement est désactivée. Cliquez ensuite sur **OK** pour fermer la section **Paramètres de base**.

vii. Si vous créez un serveur virtuel NetScaler Gateway, liez un **certificat**et liez une stratégie d'authentification LDAP.

viii. Faites défiler la page jusqu'à la section **Stratégies** et cliquez sur l'icône Plus.

ix. La page **Choisir un type** est définie par défaut sur **Session** et **Demande**. Cliquez sur **Continuer**.

x. Dans la section **Liaison de stratégie**, cliquez **sur Cliquez pour sélectionner**.

xi. Sélectionnez la stratégie de session requise pour laquelle le profil PCoIP est configuré, puis cliquez sur **Sélectionner**.

xii. Dans la page **Liaison de stratégie**, cliquez sur **Liaison**.

xiii. Si vous souhaitez utiliser un navigateur Web pour vous connecter à VMware Horizon View, sous **Paramètres avancés**, ajoutez la section **Thèmes du portail**. Si vous utilisez uniquement Horizon View Client pour vous connecter à NetScaler Gateway, vous n'avez pas à effectuer cette étape.

xiv. Utilisez le menu **Thème du portail** pour sélectionner **RFWebUI** et cliquez sur **OK**.

xv. Les icônes publiées Horizon View sont ajoutées au portail RFWebUI.

> **Remarque :** VMware utilise deux protocoles ou plus lorsqu'il utilise un protocole autre que RDP. Cela peut entraîner l'équilibrage de charge des demandes sur deux serveurs principaux différents. Vous pouvez résoudre ce problème en configurant un groupe de persistance unique sur tous les protocoles, en veillant à ce que toutes les connexions restent sur le même serveur virtuel Citrix.

Étapes à suivre pour activer la redirection USB

Les périphériques USB connectés à la machine cliente sont accessibles depuis les bureaux et applications virtuels. Voici les étapes à suivre pour activer la redirection USB :

1. Connectez-vous à la console VMware Horizon Administrator.
2. Accédez à **Inventaire > Afficher les serveurs de configuration**.
3. Sélectionnez l'onglet **Serveurs de connexion**.
4. Sélectionnez un serveur de connexion répertorié et cliquez sur **Modifier**.
5. Sous l'onglet **Général**, sélectionnez l'option **Utiliser la connexion Secure Tunnel à la machine** sous **HTTP (S) Secure Tunnel**. Indiquez l'URL externe de NetScaler Gateway dans le champ **URL externe**.

Mise à jour de l'expression de commutation Unified Gateway contenu pour

Si votre serveur virtuel NetScaler Gateway se trouve derrière une Unified Gateway (serveur virtuel de commutation de contenu), vous devez mettre à jour l'expression de commutation de contenu pour inclure les chemins d'URL PCoIP.

1. Dans l'interface graphique de NetScaler, accédez à **Configuration > Gestion du trafic > Commutation de contenu**Stratégies.
2. Ajoutez l'expression suivante dans la zone **Expression**, puis cliquez sur **OK**.

	http.req.url.path.eq (« /broker/xml »)	http.req.url.path.contains (« /broker/resources »)	http.req.url.path.eq (« /pcoip-client »)

Utiliser la passerelle PCoIP

1. Pour vous connecter, Horizon View Client doit être installé sur l'appareil client. Une fois installé, vous pouvez soit utiliser l'interface utilisateur du client Horizon View pour vous connecter à NetScaler Gateway, soit utiliser la page du portail NetScaler Gateway RFWebUI pour afficher les icônes publiées depuis Horizon.

2. Pour afficher les connexions PCoIP actives, accédez à **NetScaler Gateway** > PCoIP.
3. Sur la droite, accédez à l'onglet **Connexions**. Les sessions actives sont affichées avec les données suivantes : nom d'utilisateur, adresse IP du client Horizon View et adresse IP de destination d'Horizon View Agent.
4. Pour mettre fin à une connexion, cliquez avec le bouton droit sur l'onglet **Connexion**, puis cliquez **sur Supprimer la connexion** Ou cliquez sur **Kill All Connections** pour mettre fin à toutes les connexions PCoIP.

Configuration du serveur de connexion VMware Horizon View

March 27, 2024

Pour prendre en charge le proxy PCoIP via NetScaler Gateway :

1. Connectez-vous à la **console VMware Horizon Administrator**.

2. Accédez à I**Inventory** —> **View Configuration** —> **Servers**.

3. Sélectionnez l'onglet **Serveurs de connexion**.

4.Sélectionnez un serveur de connexion répertorié et cliquez sur **Modifier**.

5. Sous l'onglet **Général**, désélectionnez l'option **Utiliser la connexion Secure Tunnel** à la machine sous HTTP (S) Secure Tunnel.

6. Cliquez sur **OK** pour fermer la fenêtre **Modifier les paramètres du serveur de connexion**.

7. Exécutez les étapes 4 à 6 sur tous les serveurs de connexion répertoriés.

Configuration automatique du proxy pour la prise en charge du proxy sortant pour NetScaler Gateway

March 27, 2024

Lorsque vous configurez l'appliance NetScaler Gateway pour qu'elle prenne en charge la configuration automatique du proxy (PAC), l'URL d'un fichier PAC est transmise au navigateur client. Le trafic provenant du client est ensuite redirigé vers les proxys respectifs tels que déterminés par les conditions définies dans le fichier PAC.

Voici quelques cas d'utilisation courants de PAC pour le proxy sortant :

- Pour configurer plusieurs serveurs proxy qui gèrent le trafic client.

- Pour équilibrer la charge du trafic proxy sur les sous-réseaux.

Configurer les paramètres globaux de NetScaler Gateway pour prendre en charge le PAC pour le proxy sortant à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
set vpn parameter -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Configurer NetScaler Gateway pour prendre en charge le PAC dans un profil de session à l'aide de l'interface de ligne de commande

À l'invite de commandes, tapez :

```
add vpn sessionAction <name> -proxy BROWSER -autoProxyUrl <URL>
<!--NeedCopy-->
```

Où ?

- **URL** : URL du serveur proxy
- **Name** : nom du VPN SessionAction

Configurer les paramètres globaux de NetScaler Gateway pour prendre en charge le PAC pour le proxy sortant à l'aide de l'interface graphique

1. Accédez à **Configuration > NetScaler Gateway > Paramètres généraux**.
2. Sur la page**Paramètres globaux**, cliquez sur**Modifier les paramètres globaux**, puis sélectionnez l '**onglet Expérience client**.
3. Dans l'onglet**Expérience client**, sélectionnez**Paramètres avancés**, puis l'**onglet Proxy**.
4. Dans l'**onglet Proxy** , sélectionnez**Navigateur**, puis sélectionnez**Utiliser la configuration automatique**.
5. Dans le champ**URL vers le fichier de configuration du proxy automatique**, tapez l'URL du fichier PAC requis.
6. Cliquez sur**Créer**.

Configurer NetScaler Gateway pour prendre en charge le PAC sur le profil de session à l'aide de l'interface graphique

1. Accédez à **Configuration > NetScaler Gateway > Stratégies**Session .

2. Sur la page **Stratégies et profils de session NetScaler Gateway, créez un profil**de session NetScaler Gateway.
3. Sélectionnez l'onglet **Profils de session**, cliquez sur **Ajouter**, puis saisissez un nom.
4. Dans l'onglet**Expérience client**, sélectionnez **Paramètres avancés**, puis l'onglet **Proxy**.
5. Dans l'onglet**Proxy**, sélectionnez **Navigateur**, puis **Utiliser la configuration automatique**.
6. Dans le champ**URL vers le fichier de configuration du proxy automatique**, tapez l'URL du fichier PAC requis.
7. Cliquez sur**Créer**.
8. Cliquez sur**Créer**.

Prise en charge de la configuration de l'attribut de cookie SameSite

March 27, 2024

L'attribut `SameSite` indique au navigateur si le cookie peut être utilisé pour un contexte intersite ou uniquement pour un contexte de même site. Si une application a l'intention d'être accessible dans le contexte intersite, elle ne peut le faire que via la connexion HTTPS. Pour plus de détails, consultez la RFC6265.

Jusqu'en février 2020, l'attribut `SameSite` n'était pas défini explicitement dans l'appliance NetScaler. Le navigateur a pris la valeur par défaut (Aucun). La non-définition de l'attribut `SameSite` n'a pas eu d'impact sur les déploiements de NetScaler Gateway et NetScaler AAA.

La mise à niveau de certains navigateurs, tels que Google Chrome 80, modifie le comportement par défaut des cookies entre domaines. L'attribut `SameSite` peut être défini sur l'une des valeurs suivantes. La valeur par défaut de Google Chrome est définie sur Lax. Pour certaines versions d'autres navigateurs, la valeur par défaut de l'attribut `SameSite` peut toujours être définie sur Aucun.

- **Aucun** : indique au navigateur qu'il doit utiliser le cookie dans un contexte intersite uniquement sur les connexions sécurisées.
- **Lax** : indique que le navigateur doit utiliser le cookie pour les demandes sur le contexte du même site. Dans le contexte inter-site, seules les méthodes HTTP sûres comme la requête GET peuvent utiliser le cookie.
- **Strict** : utilisez le cookie uniquement dans le même contexte de site.

S'il n'y a pas d'attribut `SameSite` dans le cookie, Google Chrome assume la fonctionnalité de `SameSite` = Lax.
Par conséquent, pour les déploiements au sein d'une iframe avec un contexte intersite nécessitant l'insertion de cookies par le navigateur, Google Chrome ne partage pas les cookies intersites. Par conséquent, il se peut que l'iframe du site Web ne se charge pas.

Configurer l'attribut de SameSite cookie

Un nouvel attribut de cookie nommé SameSite est ajouté aux serveurs virtuels VPN et NetScaler AAA. Cet attribut peut être défini au niveau global et au niveau du serveur virtuel.

Pour configurer l'attribut,SameSite vous devez effectuer les opérations suivantes :

1. Définir l'attribut SameSite du serveur virtuel
2. Liez les cookies au patset (si le navigateur supprime les cookies intersites sont déposés par le navigateur)

Définition de l'attribut SameSite à l'aide de l'interface de ligne de commande

Pour définir l'attribut SameSite au niveau du serveur virtuel, utilisez les commandes suivantes.

```
set vpn vserver VP1 -SameSite  [ STRICT | LAX | None ]
set aaa vserver VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Pour définir l'attribut SameSite au niveau global, utilisez les commandes suivantes.

```
set vpn param VP1 -SameSite  [ STRICT | LAX | None ]
set aaa param VP1 -SameSite  [ STRICT | LAX | None ]
<!--NeedCopy-->
```

Remarque : Le paramètre de niveau du serveur virtuel est prioritaire sur le paramètre de niveau global. Citrix recommande de définir l'attribut de SameSite cookie au niveau du serveur virtuel.

Liaison des cookies à patset à l'aide de l'interface de ligne de commande

Si le navigateur supprime les cookies intersites, vous pouvez lier cette chaîne de cookies au ns_cookies_SameSite patset existant afin que l'attribut SameSite soit ajouté au cookie.

Exemple :

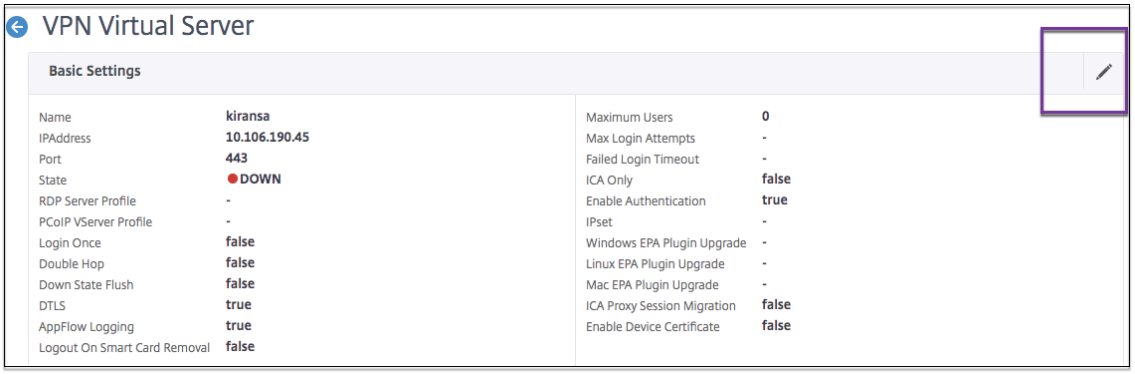
```
bind patset ns_cookies_SameSite "NSC_TASS"
bind patset ns_cookies_SameSite "NSC_TMAS"
<!--NeedCopy-->
```

Définition de l'attribut SameSite à l'aide de l'interface graphique

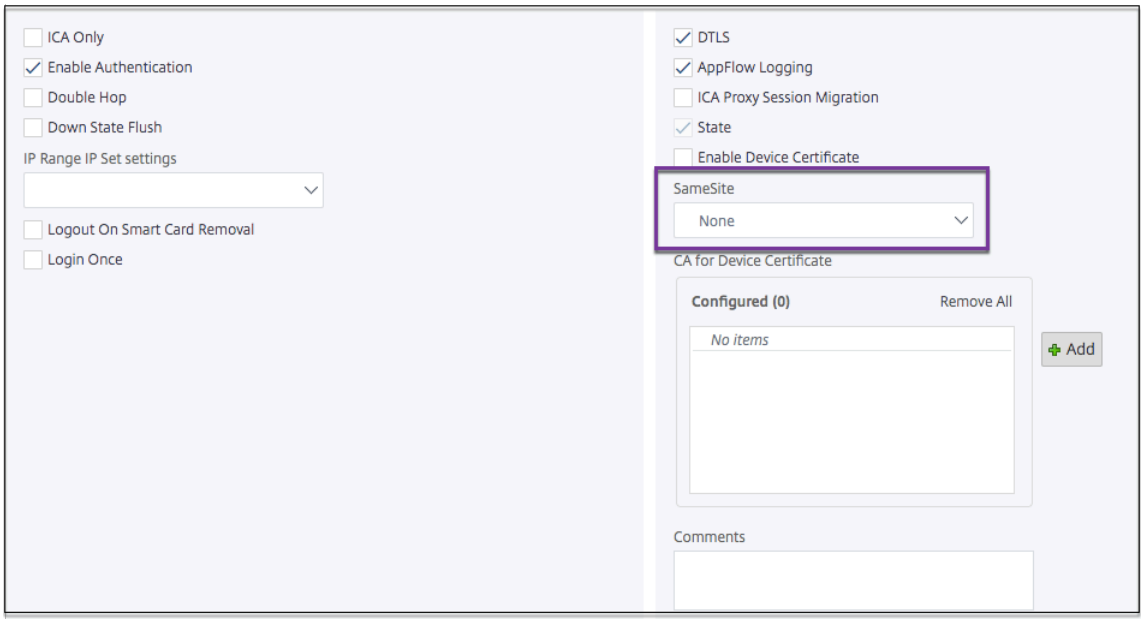
Pour définir l'attribut SameSite au niveau du serveur virtuel, procédez comme suit :

1. Accédez à **NetScaler Gateway > Serveurs virtuels**.
2. Sélectionnez un serveur virtuel et cliquez sur **Modifier**.

3. Sélectionnez l'icône de modification dans la section **Paramètres de base**, puis cliquez sur **Plus**.

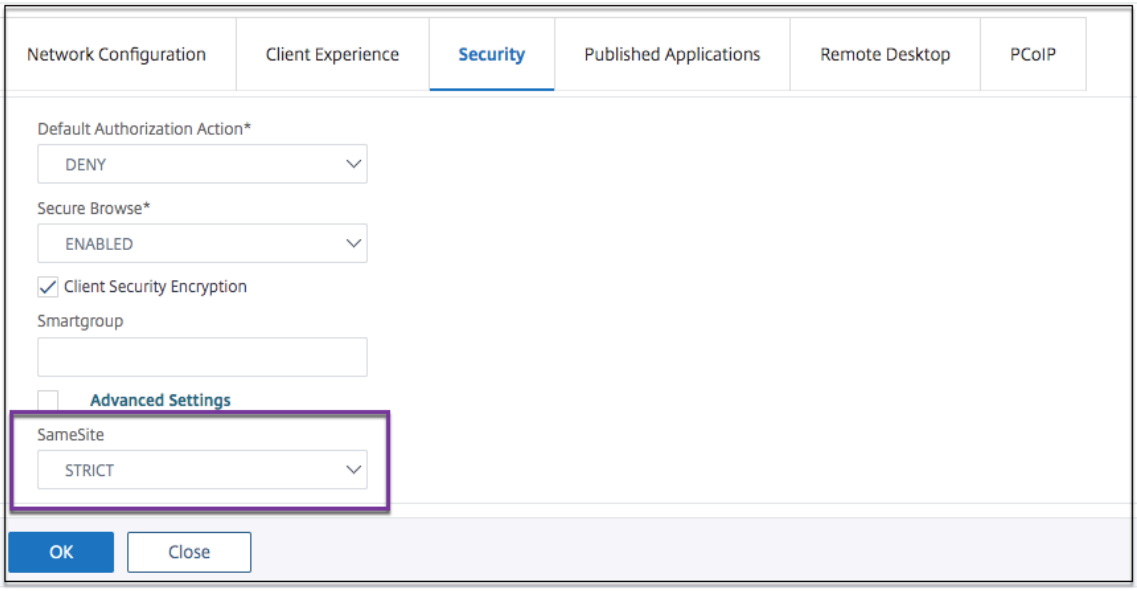


4. Dans **SameSite**, sélectionnez l'option si nécessaire.



Pour définir l'attribut `SameSite` au niveau global, procédez comme suit :

1. Accédez à **NetScaler Gateway > Paramètres globaux > Modifier les paramètres globaux .**
2. Cliquez sur l'onglet **Sécurité**.
3. Dans,**`SameSite`** sélectionnez l'option si nécessaire.



Configuration de RFWebUI Persona on Gateway UX

March 27, 2024

RFWebUI Persona est un thème qui fournit une nouvelle page de connexion et de portail pour les utilisateurs de NetScaler Gateway qui se connectent via NetScaler Gateway. Le portail présente aux utilisateurs Receiver, StoreFront et Citrix Endpoint Management avec la même interface graphique que lorsqu'ils accèdent directement à l'un de ces produits.

Quand utiliser RFWebui Persona

Utilisez le personnage RFWebUI dans NetScaler Gateway lorsque vous avez besoin d'une vue à volet unique de toutes les applications fournies par différents produits NetScaler, telles que les applications Web et SaaS (Software as a Service), les applications Windows virtuelles et les postes de travail.

Les scénarios suivants illustrent l'utilisation de RFWebUI Persona.

- Un utilisateur accède à StoreFront à l'aide de Gateway et trouve une interface graphique différente de celle qu'il voit lorsqu'il accède au produit sans passerelle.
  Solution : Lorsque l'utilisateur accède à StoreFront à l'aide de la passerelle, le thème RFWebUI fournit une interface utilisateur similaire à celle qu'il voit lorsqu'il accède au produit sans utiliser la passerelle.
- Un utilisateur accède à l'application Citrix Workspace, StoreFront et aux applications Citrix Endpoint Management à l'aide de Gateway et a du mal à localiser les applications souhaitées

car les applications ne sont pas regroupées de manière logique.
Solution : Le persona RFWebUI fournit une expérience utilisateur à panneau unique en créant un regroupement logique d'applications fournies par différents produits, tels que Receiver, StoreFront, Citrix Endpoint Management, etc.

Fonctionnalités fournies par RFWebui Persona

La nouvelle RFWebUI offre les fonctionnalités suivantes :

- ALLER
- Agrégation des applications
- Liens proxy RDP (Remote Desktop Protocol) configurés par l'
- Applications préférées

ALLER

GO : La fonctionnalité Go permet d'accéder aux pages Web via un VPN sans client. L'utilisateur saisit simplement l'URL dans la section **URL** de l'onglet **Favoris** et clique sur **GO**.

Actuellement, la fonctionnalité **GO** prend uniquement en charge les URL Outlook Web Application (OWA) et SharePoint.

> **Remarque**
> L'onglet **GO** n'est visible que si le `clientlessAccessVPNMode` paramètre de la stratégie de session est **activé**.

Agrégation des applications

Agrégation des applications : le thème RFWebUI fournit une vue à panneau unique en regroupant les applications fournies par différents produits sous des bannières descriptives. Par exemple, toutes les URL VPN configurées par un administrateur NetScaler se trouvent dans un ensemble appelé **Applications Web et SaaS**, et les signets Web spécifiques à l'utilisateur se trouvent sous **Favoris personnels**. Si les ensembles d'applications Citrix Virtual Apps and Desktops sont configurés dans StoreFront, l'affichage à volet unique de NetScaler Gateway répertorie également ces ensembles.

Liens proxy RDP configurés par l'utilisateur

Les utilisateurs peuvent ajouter un lien proxy RDP en tant que signets personnels. Les signets personnels apparaissent sous l'onglet **Postes de travail**.

Les modes RDP suivants sont pris en charge :

- Passerelle unique
- Passerelle Stateless (double)

> **Remarque :** Un utilisateur peut ajouter des liens proxy RDP uniquement s'il `RDPclientprofile` est configuré. Pour plus d'informations sur les configurations RDP, consultez la documentation du proxy RDP .

Applications préférées

Les utilisateurs peuvent ajouter les applications souhaitées répertoriées sous **Application Web et SaaS** et sous **Signets personnels** à l'onglet **FAVORIS** en cliquant sur le lien **Ajouter aux favoris** présent en regard du nom de l'application. Les applications ajoutées sont visibles sous l'onglet **FAVORIS**. La même chose peut également être supprimée de l'onglet **FAVORIS** en cliquant sur le lien **SUPPRIMER** présent en regard de l'application dans l'onglet **FAVORIS**.

Considérations relatives à l'activation de RFWebUI Persona

Le persona RFWebUI ne prend pas entièrement en charge les éléments suivants :

Fonctionnalité de**partage de fichiers : La fonctionnalité** de partage de fichiers, permettant d'accéder aux partages de fichiers SMB, n'est pas prise en charge.
Email Home : le paramètre VPN **Email Home** n'est pas disponible en tant que vue intégrée pour le portail NetScaler Gateway. Il est accessible en tant qu'application dans le bundle **Web et SaaS Apps sous** l'onglet **APPS** de RFWebUI.
Client Java : Le client Java basé sur un navigateur pour établir un tunnel SSL n'est pas disponible dans ce thème.

Configuration de RFWebUI Persona

Pour appliquer le RFWeBui Persona :

1. Dans l'interface NetScaler, accédez à **Configuration > Thèmes du portail NetScaler Gateway**.
2. Sur la page **Thèmes du portail**, cochez la case **RFWebUI**.
3. Cliquez sur l'icône **Enregistrer** dans le coin supérieur droit de la page **Thèmes du portail**.
4. Dans la boîte de dialogue **Enregistrer la confirmation**, cliquez sur **Oui**.

Paramètres de configuration RFWebUI

March 27, 2024

Le comportement général du portail NetScaler Gateway est influencé par deux fichiers de configuration : le fichier de configuration local de NetScaler Gateway et le fichier StoreFront.

En fonction de votre déploiement, vous pouvez modifier le comportement du portail NetScaler Gateway en modifiant les propriétés du fichier « plugins.xml ». Ce fichier apparaît sous la forme d'un fichier de configuration dans le navigateur qui fait l'objet de la demande `/var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

Lors de l'ouverture de session, les fichiers de configuration de NetScaler Gateway sont utilisés. Mais lorsqu'il est connecté à StoreFront, StoreFront envoie une nouvelle configuration et la configuration précédente est écrasée. Ce comportement est différent pour les VPN et ICA sans client.

Pour ICA, la configuration de StoreFront est toujours prioritaire, mais certains comportements du VPN sans client qui sont influencés par la configuration de NetScaler Gateway sont conservés même après la mise à jour de la nouvelle configuration depuis StoreFront.

Le tableau suivant répertorie les paramètres décrivant la configuration qui a priorité sur le VPN et l'ICA sans client.

Type de configuration	type de sous-configuration	Paramètre	VPN sans client	ICA	Description
Session pour VPN sans client/Auth-Manager for ICA	-	loginFormTimeout	NetScaler Gateway	-	Définit la durée en minutes du délai d'expiration de la page d'ouverture de session
Assistant Plug-in	-	enabled	StoreFront	StoreFront	Activer ou désactiver l'assistant de plug-in
Assistant Plug-in	-	upgradeAtLogin	StoreFront	StoreFront	Demande la mise à niveau du plug-in lors de la connexion
Assistant Plug-in	-	showAfterLogin	NetScaler Gateway	StoreFront	Affiche l'invite du plug-in après la connexion

Type de configuration	type de sous-configuration	Paramètre	VPN sans client	ICA	Description
Assistant Plug-in	-	showOnlyIfRequiredByApps	NetScaler Gateway	StoreFront	Affiche l'invite du plug-in après la connexion, si les applications l'exigent
Assistant Plug-in	macOS/win32	path	NetScaler Gateway	StoreFront	Définit le chemin de téléchargement pour les plug-ins
Assistant Plug-in	protocolHandler	enabled	NetScaler Gateway	StoreFront	Basculer la page du gestionnaire de protocole avant de lancer le plug-in
Assistant Plug-in	protocolHandler	plateformes	NetScaler Gateway	StoreFront	Identifie la plate-forme prise en charge pour le plug-in
Assistant Plug-in	-	skipDoubleHopCheckWhenDisabled	NetScaler Gateway	StoreFront	Activez la vérification à double saut de la configuration de NetScaler Gateway pour le transfert ICA
Interface utilisateur	-	frameOptions	SO	SO	-

Type de configuration	type de sous-configuration	Paramètre	VPN sans client	ICA	Description
Interface utilisateur		autoLaunchDesktop	StoreFront	StoreFront	Activer ou désactiver le lancement du bureau
Interface utilisateur	workspaceControl	enabled	StoreFront	StoreFront	Activer ou désactiver le contrôle de l'espace de travail
Interface utilisateur	workspaceControl	autoReconnectAtLogon	StoreFront	StoreFront	Basculer pour reconnecter automatiquement la session précédente si disponible
Interface utilisateur	workspaceControl	logoffAction	StoreFront	StoreFront	Définit le comportement de fermeture de session de Citrix Workspace
Interface utilisateur	workspaceControl	showReconnectButton	StoreFront	StoreFront	Afficher ou masquer le bouton de **reconnexion**
Interface utilisateur	workspaceControl	showDisconnectButton	StoreFront	StoreFront	Afficher ou masquer le bouton de **déconnexion**
Interface utilisateur	workspaceControl	showDesktopsView	StoreFront	StoreFront	Afficher ou masquer la vue Bureaux
Interface utilisateur	workspaceControl	showAppsView	StoreFront	StoreFront	Afficher ou masquer la vue Applications

Type de configuration	type de sous-configuration	Paramètre	VPN sans client	ICA	Description
Interface utilisateur	workspaceControl	defaultView	StoreFront	StoreFront	Sélectionnez la vue Bureau ou la vue Application
Interface utilisateur	receiverConfiguration	enabled	StoreFront	StoreFront	Basculer la configuration du Receiver
Interface utilisateur	receiverConfiguration	showOnlyIfRequiredByApps	NetScaler Gateway	NetScaler Gateway	Afficher l'invite du Receiver si nécessaire par les applications
Interface utilisateur	receiverConfiguration	downloadURL	StoreFront	StoreFront	Téléchargez l'URL du Receiver
Interface utilisateur	appShortcuts	enabled	StoreFront	StoreFront	Activer ou désactiver l'onglet de raccourci de l'application
Interface utilisateur	appShortcuts	allowSessionReconnect	StoreFront	StoreFront	Autoriser la reconnexion de sessions

Personnalisation du portail de passerelle à l'aide de plug-ins personnalisés

March 27, 2024

Le framework NetScaler Gateway RFWebUI permet d'ajouter des plug-ins personnalisés pour personnaliser leur portail de passerelle. Ces plug-ins personnalisés peuvent être utilisés pour ajouter des fonctionnalités importantes à la passerelle, par exemple si vous souhaitez ajouter une nouvelle page entière dans le flux de la passerelle. Pour d'autres cas d'utilisation, le code peut être ajouté au fichier

de script personnalisé fourni pour les thèmes de passerelle à l'emplacement /var/netscaler/logon/themes/<custom_theme>/script.js.

1. Pour ajouter un plug-in personnalisé, créez le fichier JavaScript à l'emplacement correspondant /var/netscaler/logon/LogonPoint/plugins/ns-gateway/. Par exemple, vous trouverez les plug-ins suivants dans /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.

   - ns-nfactor.js
   - nsg-epa.js
   - nsg-setclient.js

   Il est recommandé d'entrer le nom du plug-in au format <plugin_name>.js.

   Tous ces fichiers de plug-in sont récupérés par le framework RFWebUI requis par la fonctionnalité.

2. Après avoir créé le fichier de plug-in, utilisez le code suivant comme exemple pour enregistrer le plug-in dans le framework RFWebUI.

```
1          (function ($) {
2
3                      CTXS.ExtensionAPI.addPlugin( {
4
5                                  Name : " plugin name " ,
6                                  initialize: function() {
7    }
8
9                       }
10  );
11              }
12  )(jQuery);
13 <!--NeedCopy-->
```

   où

   name est le nom donné au plug-in. Il est utilisé comme identifiant du plug-in.

   initialize prend la fonction comme paramètre utilisé pour initialiser le plug-in.

3. Entrez le nom du plug-in et la fonction d'initialisation dans la CTXS.ExtensionAPI.addPlugin() fonction d'enregistrement du plug-in.
   Le nom et l'emplacement du plug-in ajoutés doivent être enregistrés dans le fichier plugins.xml à cet emplacement /var/netscaler/logon/themes/<custom_theme>/plugins.xml.

4. Après avoir écrit le code du plug-in, le nom et l'emplacement du plug-in nouvellement ajouté doivent être enregistrés avec le plugins.xml fichier à cet emplacement /var/netscaler

/logon/themes/<custom_theme>/plugins.xml. Le plug-in doit être enregistré avec la plug-in balise.

```
<plugins>
<plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js"/>
<plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
   .js"/>
<plugin name="ns-nfactorn" src="plugins/ns-gateway/ns-nfactor.js"
   />
</plugins>
<!--NeedCopy-->
```

5. Entrez un nom et un src pour le plug-in afin que RFWebUI puisse identifier et récupérer le plug-in.

Exemple de configuration

Les exemples de configuration suivants peuvent être utilisés pour ajouter un plug-in personnalisé afin d'ajouter un pied de page à la page de connexion de NetScaler Gateway.

1. Créez le fichier de plug-in JavaScript à l'emplacement, /var/netscaler/logon/LogonPoint/plugins/ns-gateway/.
2. Nommez le plug-in en tant que ns-footer.js /var/netscaler/logon/LogonPoint/plugins/ns-gateway/ns-footer.js
3. Ajoutez le code suivant au plug-in enregistré à la RFWebUI et dans la fonction d'initialisation, ajoutez le pied de page à la passerelle.

```
(function ($) {

CTXS.ExtensionAPI.addPlugin({

    name: "ns-footer", // Name of plugin - must match name sent in
        configuration
    initialize: function () {

        CTXS.Extensions.beforeLogon = function (callback) {

            $("#customExplicitAuthBottom").append("<div style='
               text-align:center;color:white;font-size:15px;'><br>
               Disclaimer<BR><BR>"+
                " Access to this website is restricted to
                   employees of Login Consultants<BR></div>");
            callback();
         }
;
     }

}
```

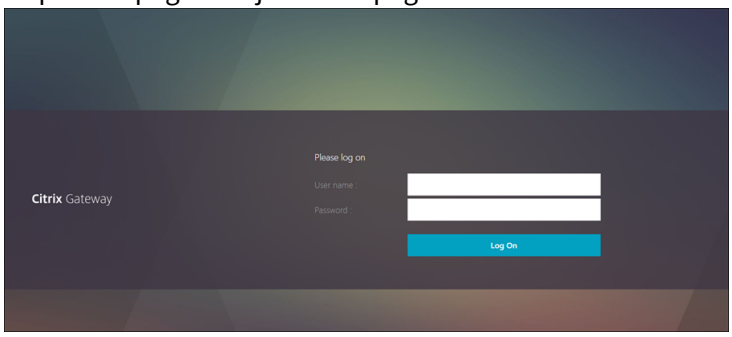


```
18   );
19   }
20   )(jQuery);
21  <!--NeedCopy-->
```

4. Enregistrez le fichier.
5. Ajoutez le nom et le src dans le fichier plugins.xml à l'emplacement `var/netscaler/logon/themes/<custom_theme>/plugins.xml`.

```
1  <plugins>
2  <plugin name="nsg-epa" src="plugins/ns-gateway/nsg-epa.js" />
3  <plugin name="nsg-setclient" src="plugins/ns-gateway/nsg-setclient
       .js" />
4  <plugin name="ns-nfactor" src="plugins/ns-gateway/ns-nfactor.js"
       />
5  <plugin name="ns-footer" src="plugins/ns-gateway/ns-footer.js" />
6  </plugins>
7  <!--NeedCopy-->
```

6. Configurez le thème personnalisé pour lequel le plug-in est ajouté.
7. Videz le cache à l'aide de la commande `flush cache contentgroup loginstaticobjects` .
8. Rechargez l'écran du portail.
   Le pied de page est ajouté à la page de connexion de NetScaler Gateway.



Création et personnalisation du schéma de connexion

January 26, 2024

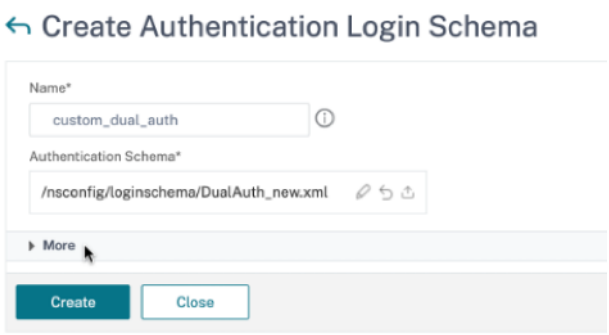
Le schéma de connexion est le fichier XML qui fournit la structure de l'authentification basée sur un formulaire.
Les utilisateurs peuvent utiliser un large éventail de formulaires d'authentification à l'aide d'un ensemble de constructions d'interface utilisateur similaires aux formulaires HTML de base.

Dans les authentifications nFactor, les facteurs d'authentification sont enchaînés. Chaque facteur peut avoir des pages ou des fichiers de schéma de connexion différents. Dans certains scénarios d'authentification, plusieurs écrans d'ouverture de session peuvent être présentés aux utilisateurs. Vous pouvez également faire en sorte qu'un schéma de connexion collecte les informations qui peuvent être transmises à plusieurs facteurs afin que ces derniers n'aient pas à afficher un autre schéma de connexion.

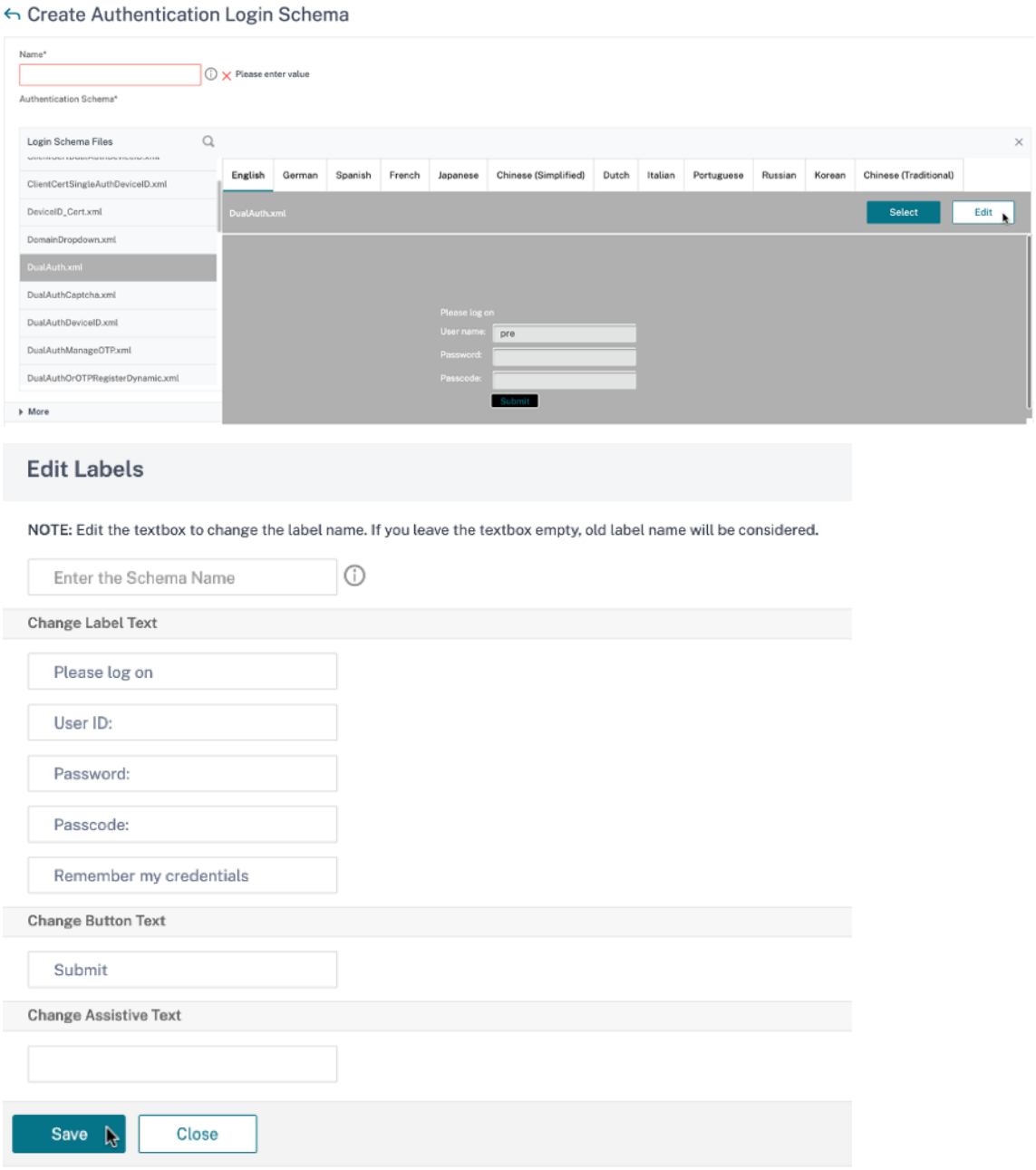
Les fichiers XML du schéma de connexion sont inclus avec l'appliance NetScaler dans. `/nsconfig/loginschema/LoginSchema`

Créer un profil de schéma de connexion

1. Accédez à **Sécurité > AAA > Schéma de connexion**.
2. Cliquez sur l'onglet **Profils**, puis cliquez sur **Ajouter**.
3. Dans le **schéma d'authentification**, cliquez sur l'icône en forme de crayon.



4. Cliquez sur le dossier **LoginSchema** pour afficher les fichiers qu'il contient.
5. Sélectionnez l'un des fichiers et effectuez les modifications nécessaires.
    - Modifiez les étiquettes en cliquant sur le bouton Modifier en haut à droite.
    - Modifiez le schéma en sélectionnant la langue.

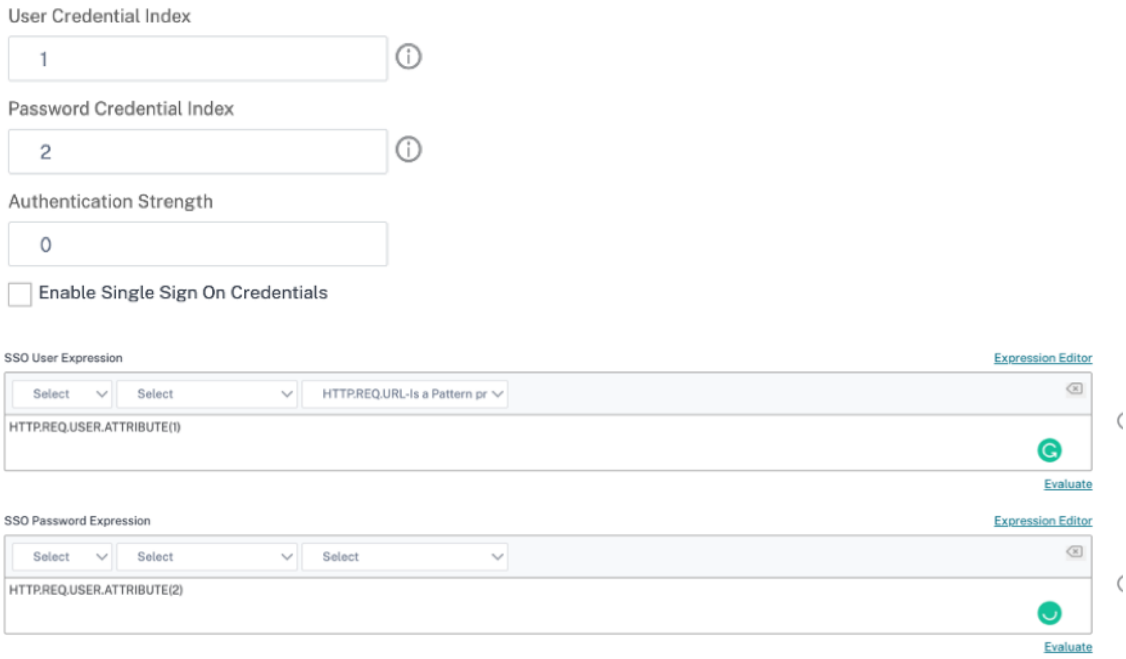


Remarque : Lorsque vous enregistrez les modifications après modification, un nouveau fichier XML de schéma est créé avec les modifications.

6. En haut à droite, cliquez sur **Sélectionner** pour sélectionner le code XML du schéma modifié.
7. Entrez un nom de schéma de connexion, puis cliquez sur **Plus**.

   Remarque : Vous pouvez utiliser les informations d'identification déjà entrées ailleurs. Par exemple, vous pouvez utiliser le nom d'utilisateur et l'un des mots de passe pour l'authentification unique à StoreFront. Vous pouvez cliquer sur **Plus** et entrer des valeurs uniques pour les index. Ces valeurs peuvent être comprises entre 1 et 16. Vous pouvez référencer ces valeurs d'

index dans une stratégie ou un profil de trafic à l'aide de l'expression REQ.USER.ATTRIBUTE (#).



8. Cliquez sur **Créer** pour créer le profil de schéma de connexion.

Liaison d'un profil de schéma de connexion à un serveur virtuel d'authentification, d'autorisation et d'audit

Pour lier un profil de schéma de connexion à un serveur virtuel d'authentification, d'autorisation et d'audit, vous devez d'abord créer une stratégie de schéma de connexion. Les stratégies de schéma de connexion ne sont pas requises lors de la liaison du profil de schéma de connexion à une étiquette de stratégie d'authentification.

Pour créer et lier une stratégie de schéma de connexion, procédez comme suit :

1. Accédez à **Sécurité > AAA > Schéma de connexion**.
2. Cliquez sur l'onglet **Stratégies**, puis cliquez sur **Ajouter**.
3. Dans **Profil**, sélectionnez le profil de schéma de connexion créé précédemment.
4. Dans **Règle**, saisissez l'expression de syntaxe par défaut, puis cliquez sur **Créer**.

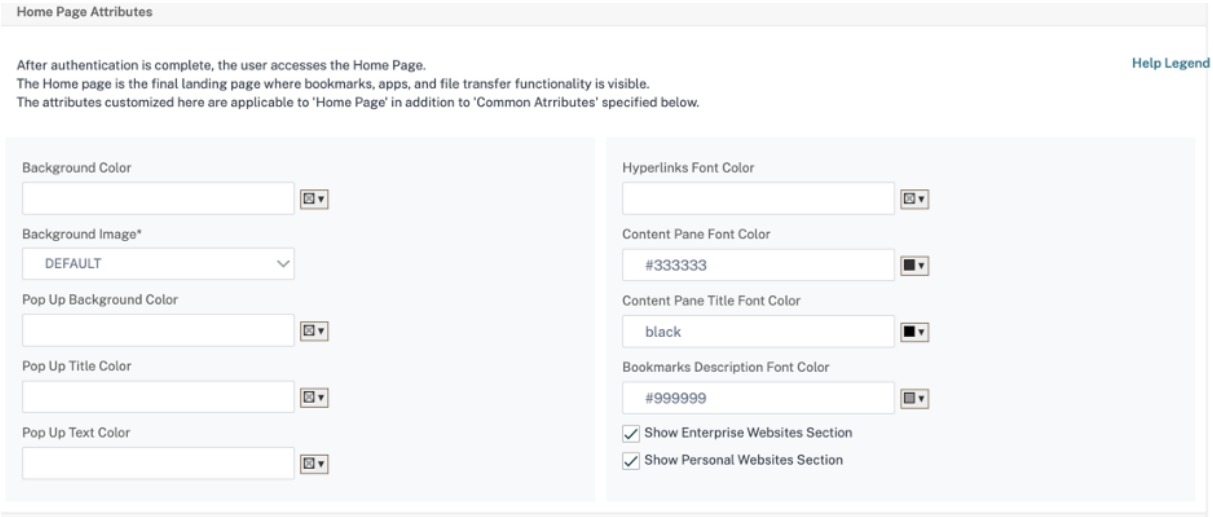
Personnalisations du portail depuis l'interface utilisateur d'administration

January 26, 2024

Les administrateurs peuvent personnaliser les thèmes du portail en créant des thèmes personnalisés afin d'obtenir l'aspect et la convivialité personnalisés du portail utilisateur. Des thèmes personnalisés peuvent être créés sur la base des thèmes RFWebUI, Default, X1 et GreenBubble.

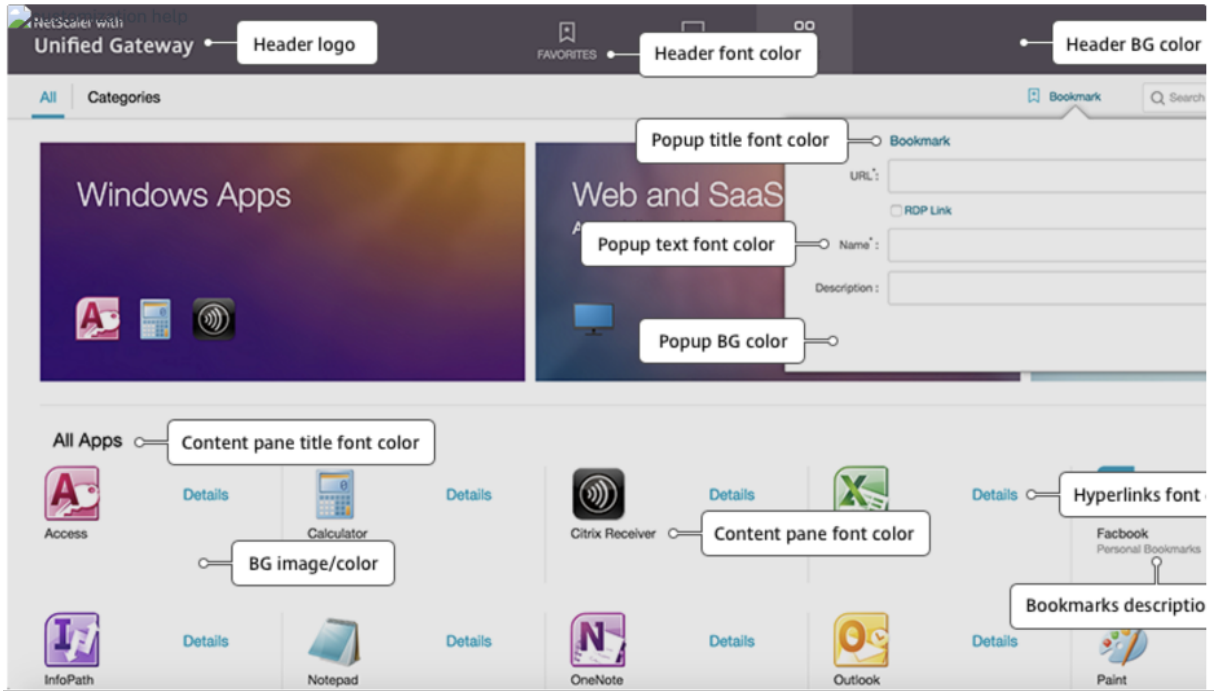
Pour créer les thèmes personnalisés :

1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Thèmes du portail** et cliquez sur **Ajouter**.
2. Entrez un nom pour le nom du thème personnalisé.
3. Dans **Thème du modèle**, sélectionnez le thème de base, selon vos besoins. **RFWebUI** est sélectionné par défaut.
4. Cliquez sur **OK**.
5. Dans la section **Apparence et convivialité**, modifiez les attributs selon vos besoins pour la page d'accueil et cliquez sur **OK**.



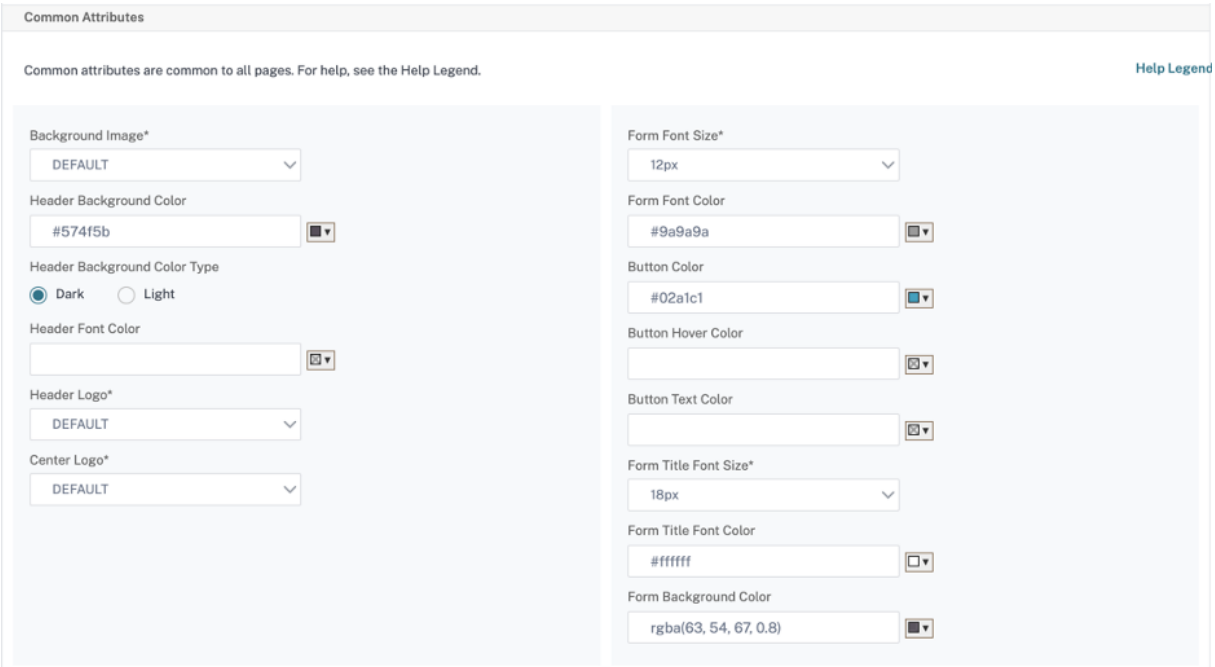
La figure suivante montre le thème personnalisé basé sur l'interface utilisateur RFWebUI.

Le lien **Légende de l'aide** affiche la page graphique avec les noms de section pour vous aider à choisir ce que vous voulez modifier.

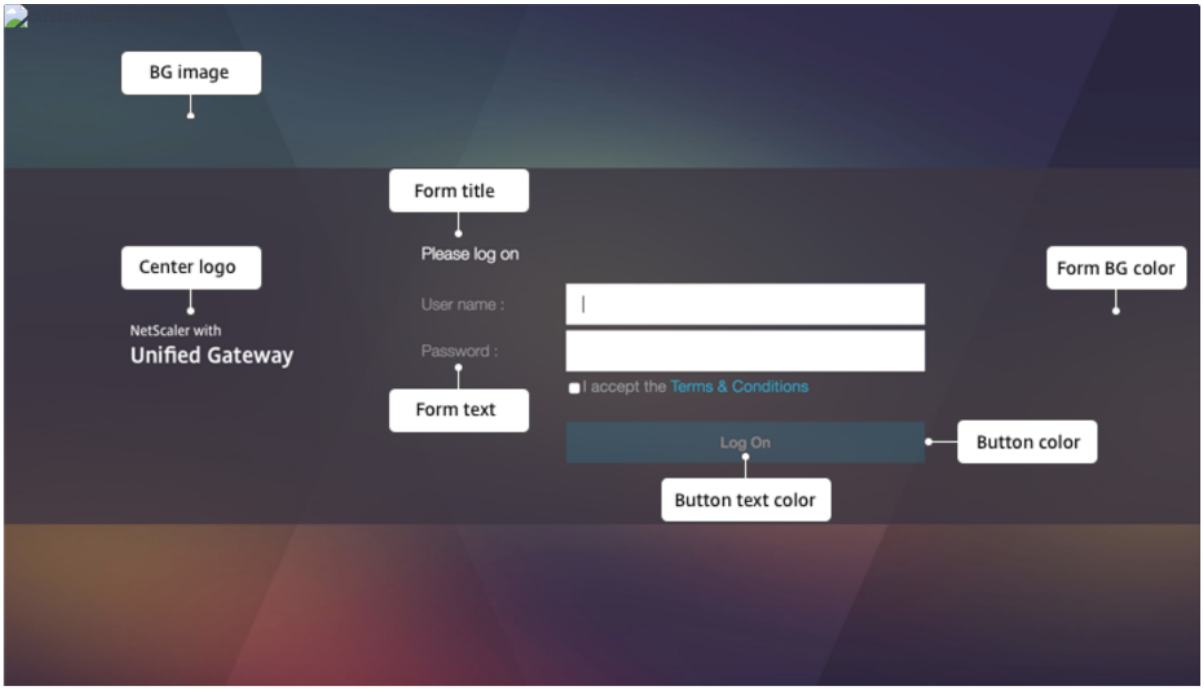


Attributs communs

La section **Attributs communs** fournit les paramètres configurables communs à toutes les pages d'ouverture de session de NetScaler Gateway.

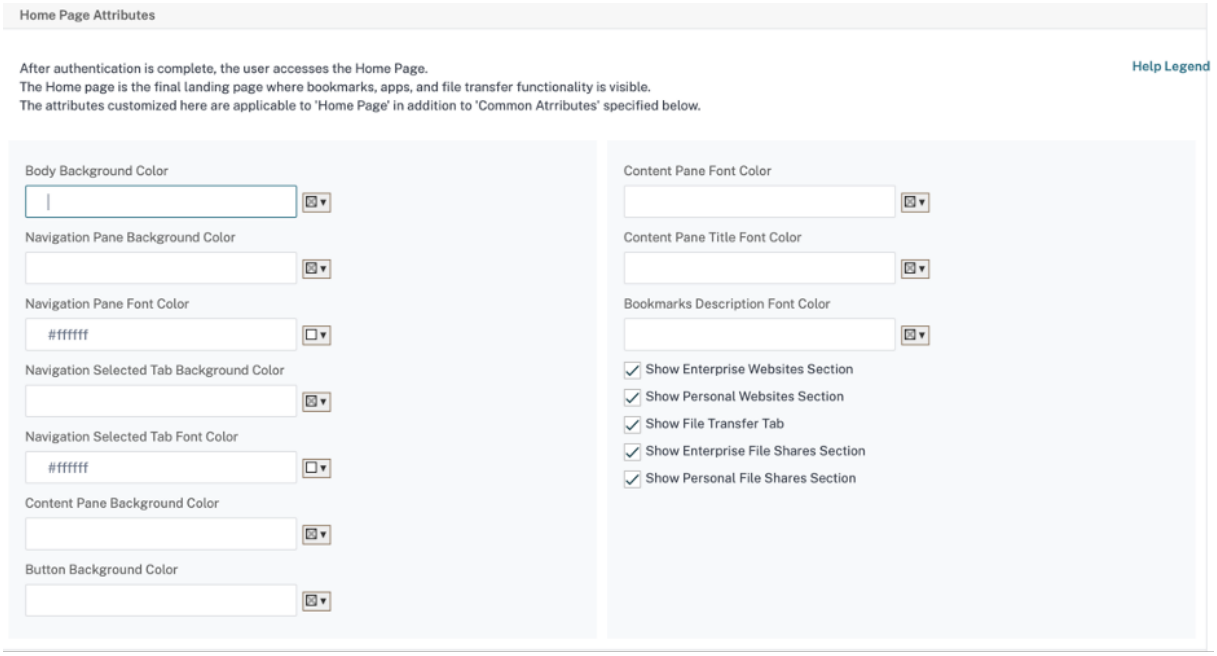


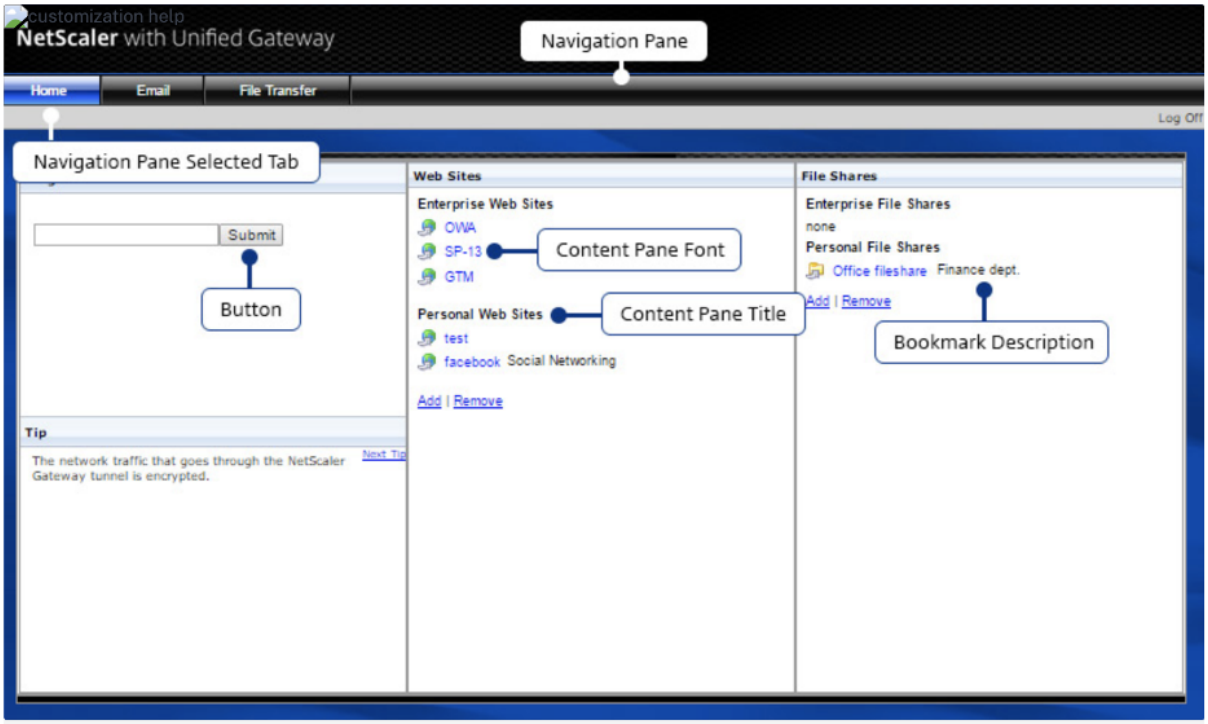
Cliquez sur le lien **Légende de l'aide** pour afficher chaque paramètre configurable courant.

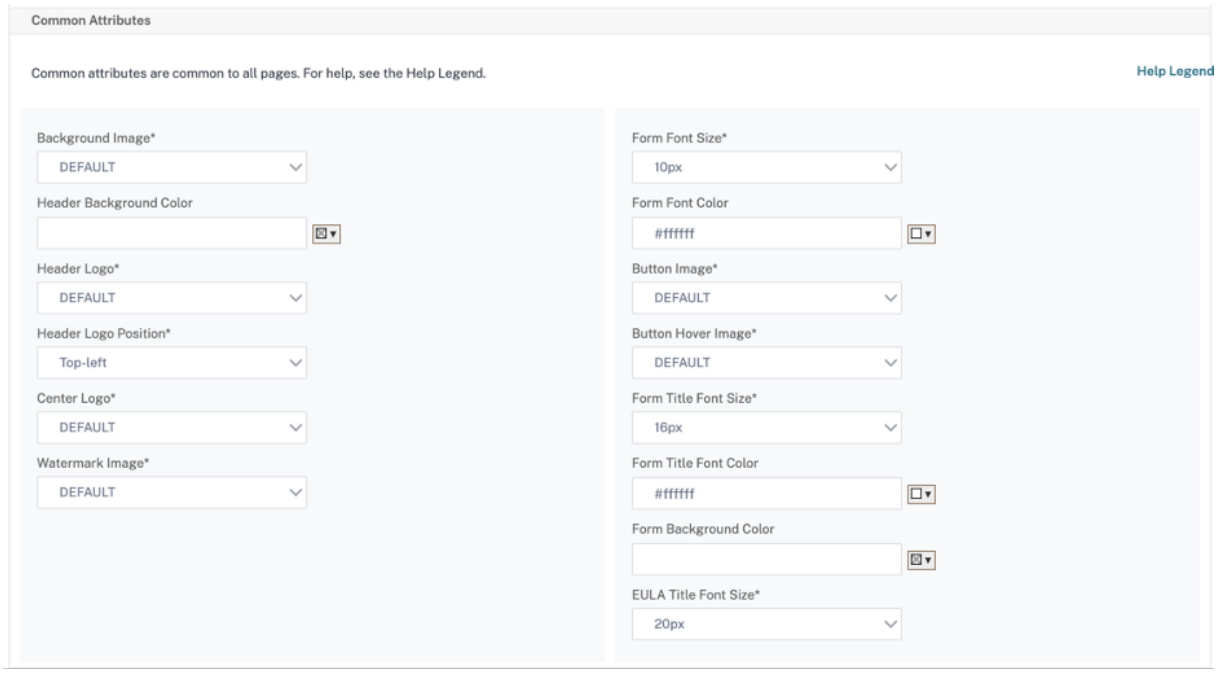


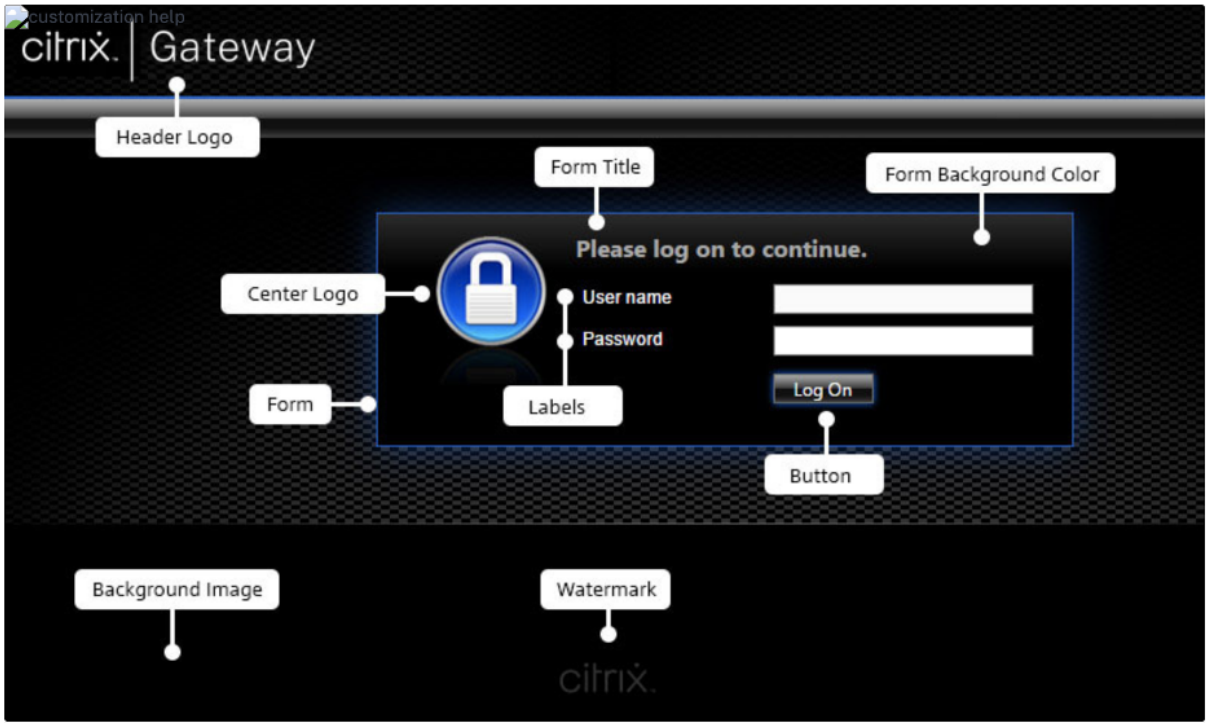
De même, pour le thème personnalisé basé sur la **valeur par défaut**, la figure suivante affiche la configuration disponible pour la page d'accueil.

Remarque : Cette configuration est différente pour le x1 et GreenBubble.







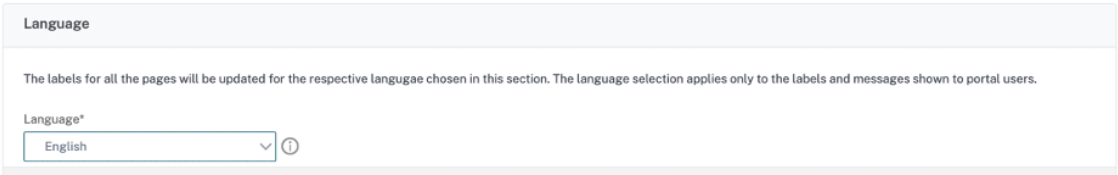


Personnalisations de chaînes

Outre l'aspect et l'aspect des pages d'accueil du portail de la passerelle, l'interface utilisateur d'administration permet également la personnalisation des chaînes sur toutes les pages.

Effectuez les étapes suivantes pour personnaliser les chaînes :

1. Sélectionnez la langue pour laquelle vous souhaitez modifier la chaîne. Les chaînes sont affichées dans la langue sélectionnée. L'anglais est sélectionné par défaut.

   Remarque : La langue que vous sélectionnez ne définit pas la langue du thème du portail. Il s'agit de la langue pour laquelle les chaînes sont personnalisées.

2. Sur la droite, dans **Paramètres avancés**, les pages disponibles pour la personnalisation de chaîne sont répertoriées.

   - Page de connexion
   - Page de l'EPA
   - Page d'erreur EPA

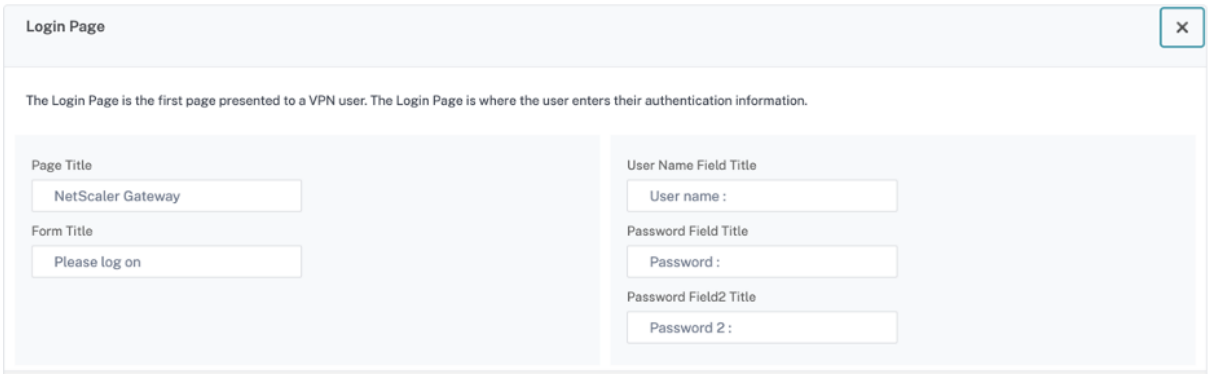
- Page post-EPA
- Page de connexion VPN
- Page d'accueil

3. Sélectionnez la page dont vous souhaitez personnaliser les chaînes, puis cliquez sur l'icône de modification. Un formulaire avec des personnalisations de chaîne préremplies s'affiche.
4. Sélectionnez le champ et ajoutez ou modifiez la chaîne selon vos besoins.
5. Cliquez sur **Terminé** pour terminer la création du thème de portail personnalisé. Vous pouvez modifier les thèmes ultérieurement depuis **NetScaler Gateway > Thèmes du portail**.

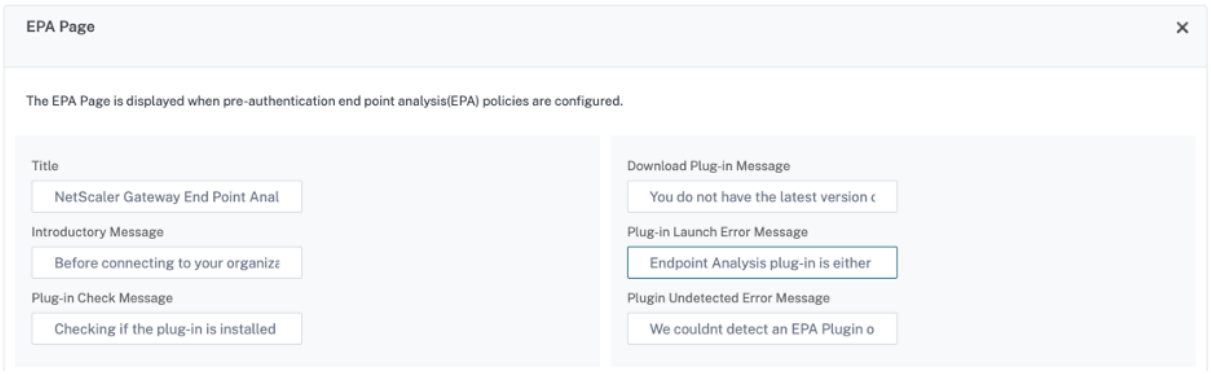
Remarque : Si la section affiche toujours les chaînes dans la langue précédemment sélectionnée, il se peut que la section était déjà ouverte lorsque la langue a été modifiée. Dans ce cas, fermez la section, sélectionnez la langue et ouvrez à nouveau la page dans **Paramètres avancés**.

Les captures d'écran suivantes affichent l'ensemble de chaînes personnalisables disponibles pour chaque page.

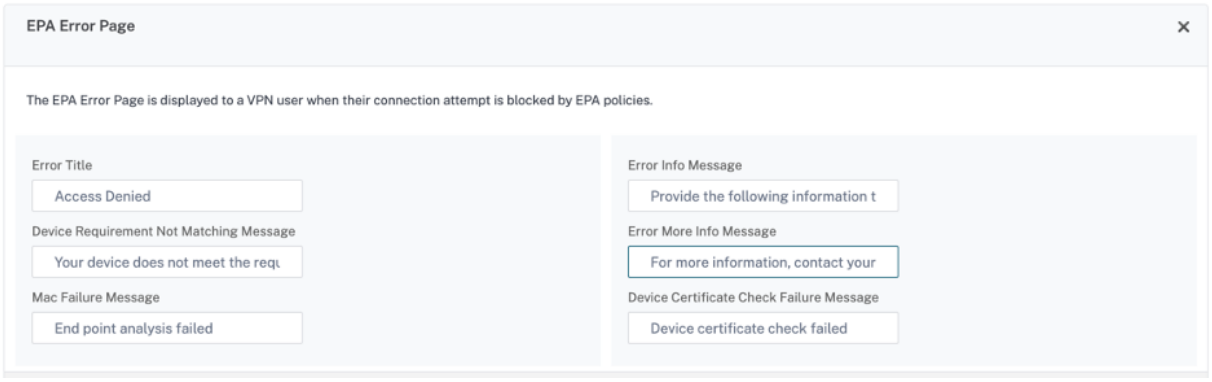
Page de connexion :



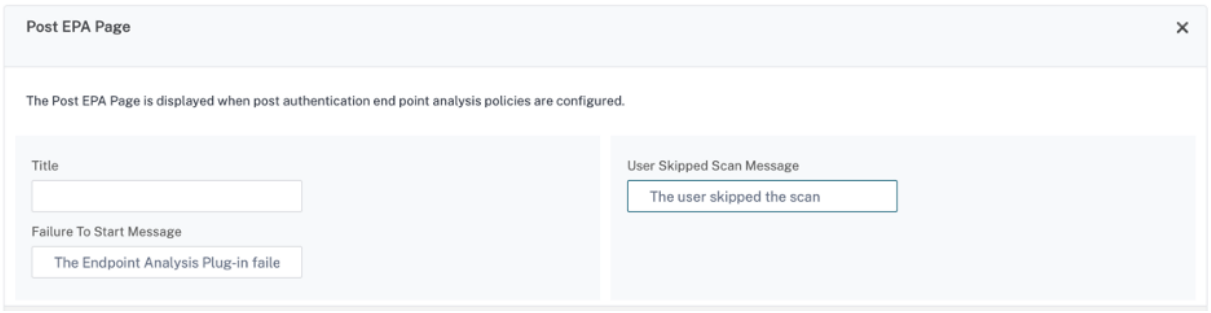
Page de l'EPA :



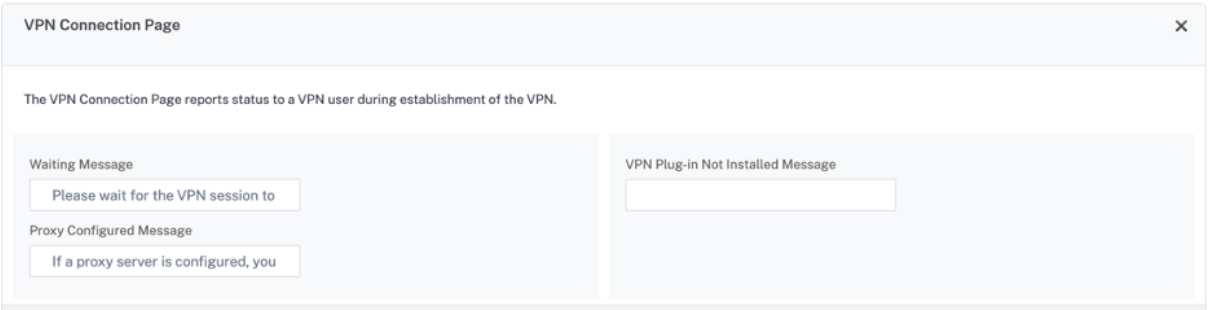
Page d'erreur EPA :



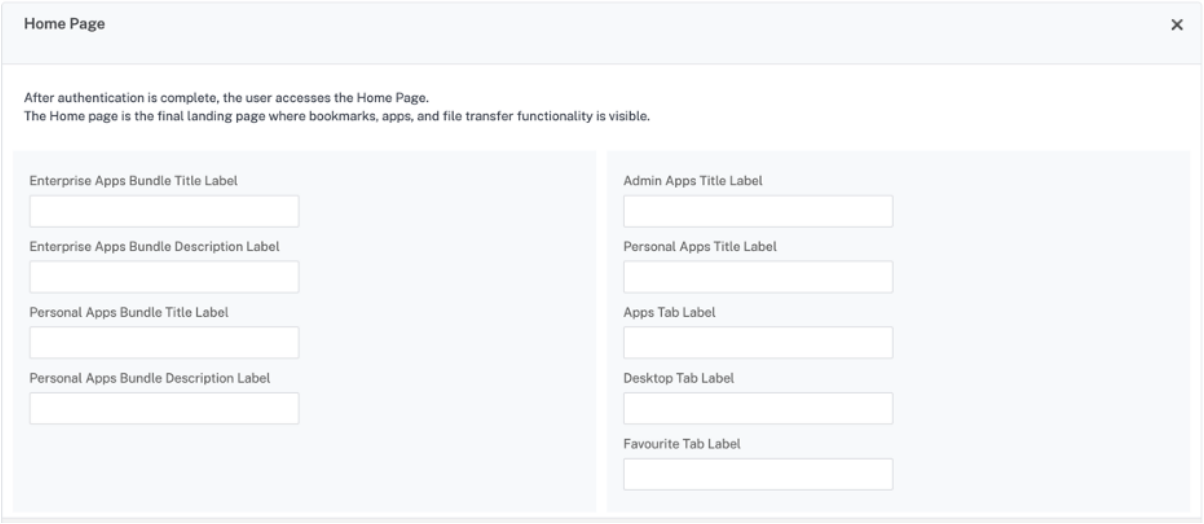
Page post-EPA :



Page de connexion VPN :



Page d'accueil :



Optimisation du tunnel partagé VPN NetScaler Gateway pour Office365

March 27, 2024

Étant donné que les entreprises s'adaptent plus rapidement aux options de travail à distance qu'auparavant, l'infrastructure d'accès à distance doit être optimisée pour faciliter une connectivité transparente dans des conditions de charge de trafic accrue.

> **Important :**
>
> Microsoft recommande d'exclure le trafic destiné aux principaux services Office 365 de la portée de la connexion VPN en configurant le split tunneling à l'aide de plages d'adresses IPv4 et IPv6 publiées. Pour de meilleures performances et une utilisation optimale de la capacité du VPN, le trafic vers les plages d'adresses IP dédiées associées aux applications suivantes doit être acheminé directement, en dehors du tunnel VPN :
>
> - Office 365 Exchange en ligne
> - SharePoint Online
> - Microsoft Teams (désignée sous le nom de catégorie Optimize dans la documentation Microsoft)
>
> Reportez-vous aux directives de Microsoft pour obtenir des informations plus détaillées sur cette recommandation.

La recommandation de Microsoft dans NetScaler Gateway est réalisée en acheminant la liste d'adresses IP fournie par Microsoft directement vers Internet pour le trafic O365 en utilisant la configuration inverse du tunnel partagé.

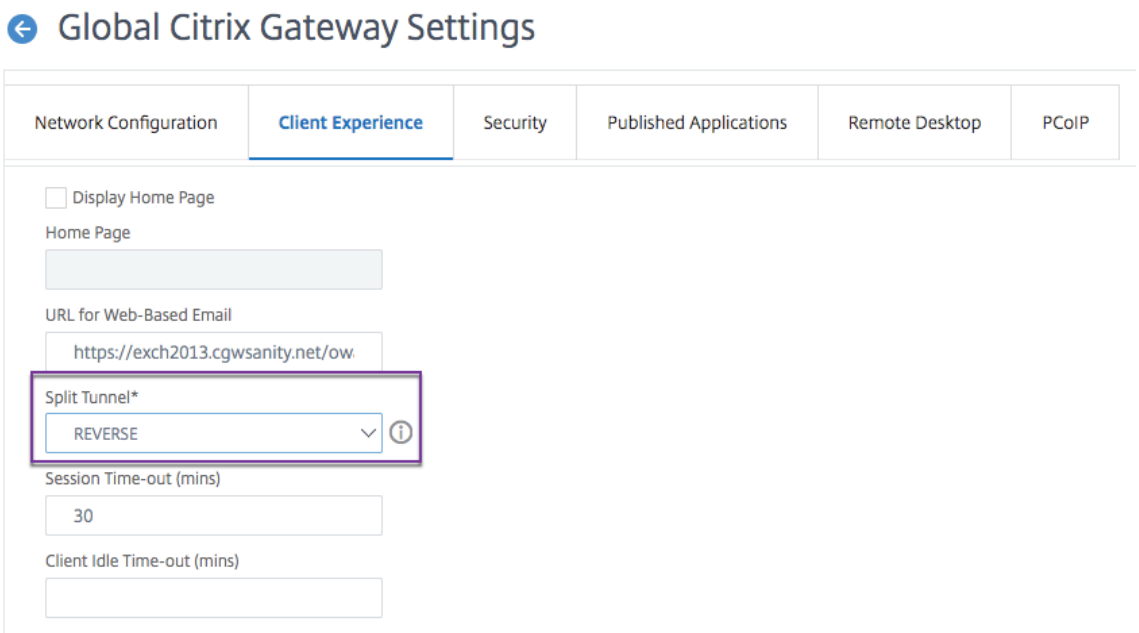
La configuration implique les opérations suivantes, qui peuvent être effectuées manuellement à l'aide de l'interface graphique ou de la CLI :

- Configurez le tunnel divisé pour une configuration inverse. Pour plus de détails, consultez la section Options de tunneling fractionné.
- Configurez les applications intranet pour l'accès des utilisateurs aux ressources.

Configuration à l'aide de l'interface graphique

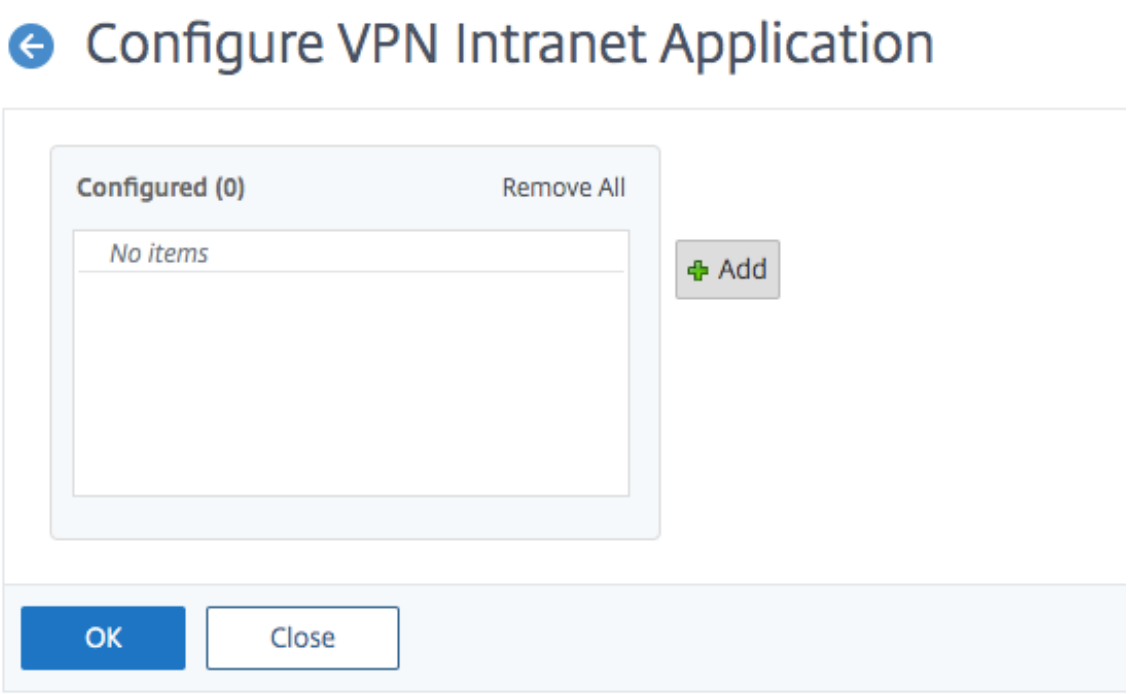
Pour configurer le split tunneling à l'aide de l'interface graphique

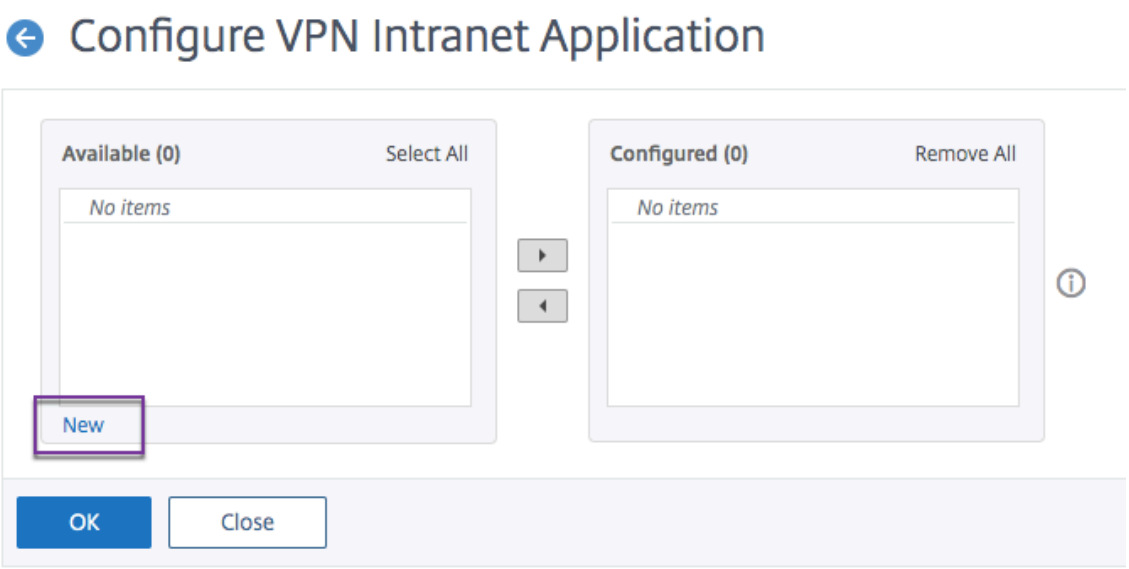
1. Dans l'onglet Configuration, accédez à **NetScaler Gateway > Paramètres** généraux.
2. Dans le volet d'informations, sous **Paramètres**, cliquez sur **Modifier les paramètres globaux**.
3. Dans l'onglet **Expérience client**, dans **Split Tunnel**, sélectionnez **Inverser**.
4. Cliquez sur **OK**.



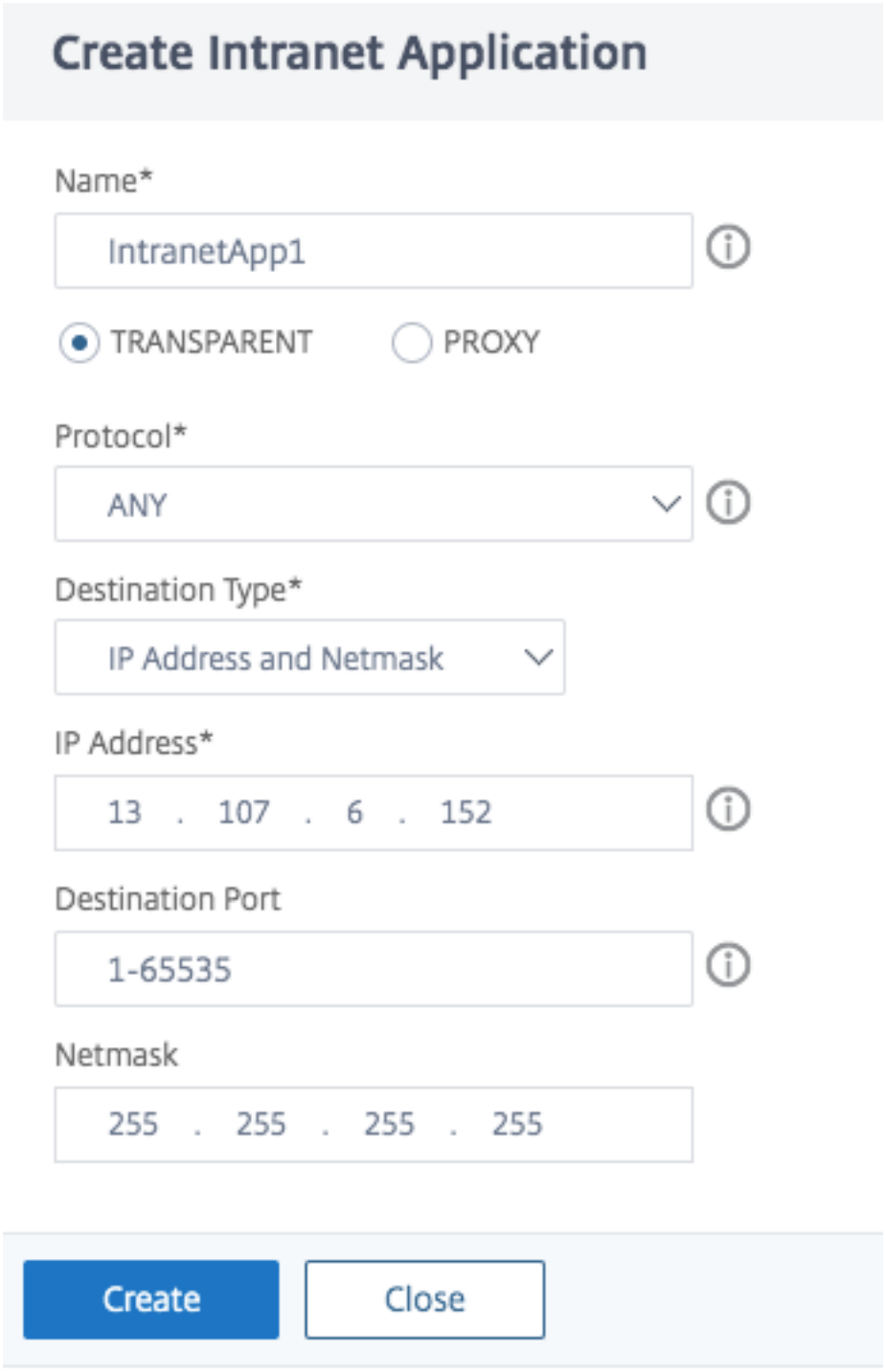
Pour créer une application intranet VPN à l'aide de l'interface graphique

1. Dans l'onglet Configuration, accédez à**Citrix Gateway > Paramètres généraux.**
2. Dans le volet d'informations, sous **Applications intranet**, cliquez sur le lien.
3. Dans la page **Configurer l'application intranet VPN**, cliquez sur **Ajouter**, puis sur **Nouveau**.





4. Dans **Nom**, saisissez le nom du profil.
5. Dans **Protocole**, sélectionnez le protocole qui s'applique à la ressource réseau.
6. Dans **Type de destination**, sélectionnez **Adresse IP et masque réseau**.
7. Dans **Adresse IP**, saisissez l'adresse IP qui doit être acheminée directement vers Internet pour le trafic O365. Pour obtenir la liste des adresses IP, reportez-vous à la section Liste des adresses IP.
8. Dans **Masque de réseau**, saisissez l'adresse IP du masque de réseau.



9. Cliquez sur **Create**, puis cliquez sur **Close**.

Remarque : Répétez cette procédure pour toutes les adresses IP.

Configuration à l'aide de l'interface de ligne de commande

- Pour définir le split tunnel sur l'inverse, à l'invite de commandes, tapez :

```
set vpn parameter -splitTunnel REVERSE
<!--NeedCopy-->
```

- Pour ajouter une application intranet VPN, à l'invite de commandes, tapez :

```
add vpn intranetApplication intranetapp1 ANY 13.107.6.152 -netmask
   255.255.255.254 -destPort 1-65535 -interception TRANSPARENT
<!--NeedCopy-->
```

Remarque : Répétez cette procédure pour toutes les adresses IP.

- Pour lier l'application intranet, à l'invite de commande, tapez :

```
bind vpn global -intranetApplication intranetapp1
<!--NeedCopy-->
```

Liste des adresses IP des services Office 365 (EXO, SPO et Microsoft Teams)

Référence : https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges

> **Remarque de Microsoft :**
>
> Dans le cadre de la réponse de Microsoft à la situation liée à la COVID-19, Microsoft a déclaré un moratoire temporaire sur certains changements d'URL et d'adresses IP prévus. Ce moratoire vise à fournir aux équipes informatiques des clients la confiance et la simplicité dans la mise en œuvre des optimisations réseau recommandées pour les scénarios Office 365 de travail à domicile. Du 24 mars 2020 au 30 juin 2020, ce moratoire mettra fin aux modifications apportées aux principaux services Office 365 (Exchange Online, SharePoint Online et Microsoft Teams) aux plages d'adresses IP et aux URL incluses dans la catégorie Optimiser.

Plage d'adresses IPv4

104.146.128.0/17
13.107.128.0/22
13.107.136.0/22
13.107.18.10/31
13.107.6.152/31
13.107.64.0/18
131.253.33.215/32

132.245.0.0/16
150.171.32.0/22
150.171.40.0/22
191.234.140.0/22
204.79.197.215/32
23.103.160.0/20
40.104.0.0/15
40.108.128.0/17
40.96.0.0/13
52.104.0.0/14
52.112.0.0/14
52.96.0.0/14
52.120.0.0/14

Plage d'adresses IPv6

2603:1006::/40
2603:1016::/36
2603:1026::/36
2603:1036::/36
2603:1046::/36
2603:1056::/36
2603:1096::/38
2603:1096:400::/40
2603:1096:600::/40
2603:1096:a00::/39
2603:1096:c00::/40
2603:10a6:200::/40
2603:10a6:400::/40
2603:10a6:600::/40
2603:10a6:800::/40
2603:10d6:200::/40
2620:1ec:4::152/128
2620:1ec:4::153/128
2620:1ec:c::10/128
2620:1ec:c::11/128
2620:1ec:d::10/128
2620:1ec:d::11/128
2620:1ec:8f0::/46

2620:1ec:900::/46
2620:1ec:a92::152/128
2620:1ec:a92::153/128
2a01:111:f400::/48
2620:1ec:8f8::/46
2620:1ec:908::/46
2a01:111:f402::/48

Type de service pris en charge pour le trafic UDP

January 26, 2024

La prise en charge du type de service (ToS) pour l'UDP garantit qu'une fois qu'une valeur ToS est configurée pour un paquet UDP par un expéditeur, NetScaler Gateway conserve la valeur jusqu'à ce que le paquet atteigne sa destination. Sur la base de la valeur configurée et de la configuration du réseau de destination, le réseau de destination place le paquet UDP dans une file d'attente sortante priorisée.

> **Remarque**
> À l'aide des informations de l'équipe de service, vous pouvez attribuer une priorité à chaque paquet IP et demander un traitement spécifique, tel qu'un débit élevé, une fiabilité élevée, une faible latence, etc.

Configuration de l'extension d'indication de nom de serveur

January 26, 2024

Une appliance NetScaler Gateway peut désormais être configurée pour inclure une extension SNI (indication du nom du serveur) dans le paquet SSL « client hello » envoyé au serveur principal. L'extension SNI aide le serveur principal à identifier le nom de domaine complet demandé lors de la connexion SSL et à répondre avec les certificats respectifs.

> **Remarque**
>
> Activez la prise en charge SNI lorsque plusieurs domaines SSL sont hébergés sur le même serveur.

Pour configurer NetScaler Gateway afin qu'il prenne en charge le SNI à l'aide de l'interface graphique :

1. Dans l'interface graphique de NetScaler, accédez à **Configuration > NetScaler**Paramètres généraux.
2. Cliquez sur le lien **Modifier les paramètres globaux** et, dans le menu **SNI du serveur principal**, sélectionnez **Activé**.

Pour configurer NetScaler Gateway afin qu'il prenne en charge le SNI à l'aide de l'interface de ligne de commande, tapez :

```
set vpn parameter backendServerSni <ENABLED><DISABLED>
<!--NeedCopy-->
```

Validation du certificat de serveur lors d'une connexion SSL

March 27, 2024

L'appliance NetScaler Gateway peut désormais être configurée pour valider le certificat de serveur fourni par le serveur principal lors d'une connexion SSL.

Pour configurer les paramètres globaux de NetScaler Gateway afin de prendre en charge le PAC pour le proxy sortant à l'aide de l'utilitaire de configuration

Liez le certificat de l'autorité de certification

1. Accédez à **Configuration** >**NetScaler Gateway** > **NetScaler Gateway Policy Manager** > **Liaisons de certificats**.**
2. Dans l'écran **Liaisons de certificats**, cliquez sur l'icône **+**.
3. Dans l'écran **Liaison de certificat (s) d'autorité** de certification, cliquez sur **Ajouter une liaison**, puis sur **Installer**.
4. Sélectionnez le nom du fichier de certificat dans le champ **Nom du fichier de certificat**, puis cliquez sur **Installer**.
5. Dans l'écran **Liaison de certificat (s) d'autorité de certification**, sélectionnez le certificat et cliquez sur **Liaison**.
6. Cliquez sur **Terminé**.

Activation de la validation du certificat :

1. Accédez à **NetScaler Gateway > Paramètres généraux**.
2. Cliquez sur **Modifier les paramètres globaux**.**
3. Sélectionnez **Activé** dans le menu déroulant **Validation du certificat du serveur principal**, puis cliquez sur **OK**.

Pour configurer les paramètres globaux de NetScaler Gateway afin qu'ils prennent en charge le certificat de serveur à l'aide de la ligne de commande

À l'invite de commandes, tapez les commandes suivantes :

```
    bind vpn global cacert DNPGCA1

    set vpn parameter backendcertValidation ENABLED
<!--NeedCopy-->
```

Configuration simplifiée des applications SaaS à l'aide d'un modèle

March 27, 2024

La configuration des applications SaaS avec authentification unique sur NetScaler Gateway est simplifiée par la mise en service d'un modèle de menu déroulant pour les applications SaaS les plus populaires. L'application SaaS à configurer peut être sélectionnée dans le menu. Le modèle préremplit une grande partie des informations nécessaires à la configuration des applications. Toutefois, les informations spécifiques au client doivent toujours être fournies.

> **Remarque :**
>
> Pour configurer et publier des applications SaaS, configurez et publiez sur NetScaler Gateway, puis sur le serveur d'applications.
>
> Les étapes décrites dans la section suivante vous aident à configurer et à publier des applications sur NetScaler Gateway à l'aide d'un modèle. Passez ensuite à la section qui explique comment configurer et publier sur le serveur d'applications.

Configuration et publication d'applications à l'aide d'un modèle - Configuration spécifique à NetScaler Gateway

La configuration suivante utilise l'application AWS Console comme exemple de configuration et de publication d'une application à l'aide d'un modèle.

Avant de commencer, vous avez besoin des éléments suivants :

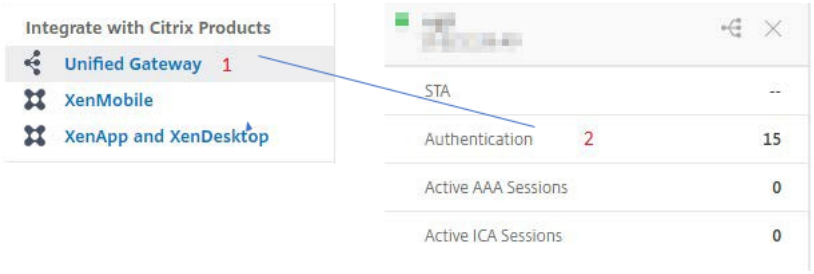
- Un compte d'administrateur pour la console AWS
- Un compte administrateur pour NetScaler Gateway

Les étapes de configuration de la console AWS sont les suivantes :

1. Configurez la console AWS avec le catalogue d'applications.
2. Exportez les métadonnées IdP de la console AWS depuis NetScaler.
3. Configurez le fournisseur d'identité dans AWS Console.

ÉTAPE 1 : Configurer AWS Console avec App Catalog

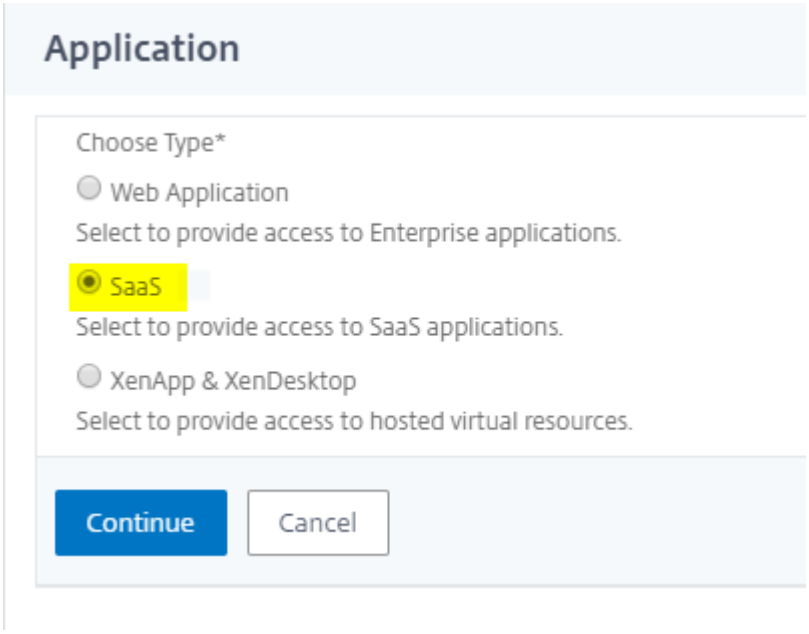
1. Cliquez sur **Unified Gateway > Authentification**.



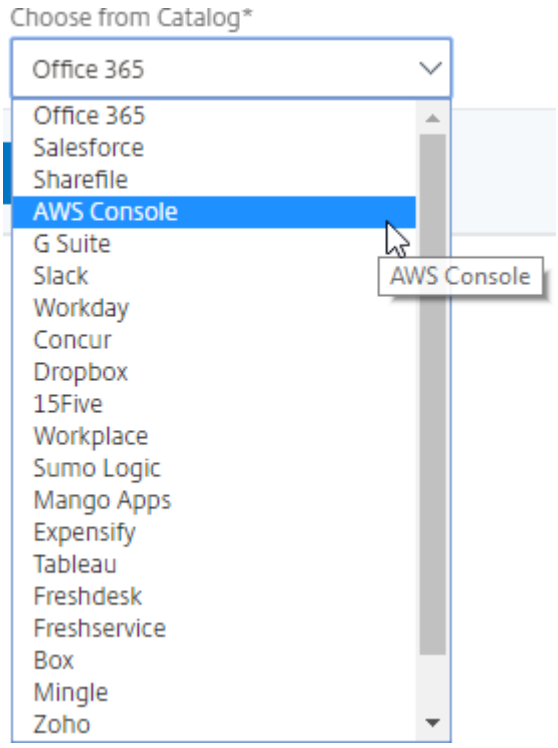
   L'écran de configuration d'Unified Gateway apparaît.

2. Dans la section **Applications**, cliquez sur l'icône Modifier. Maintenant, cliquez sur l'icône Plus. La fenêtre Application apparaît.

3. Sélectionnez **SaaS** dans le type d'application.

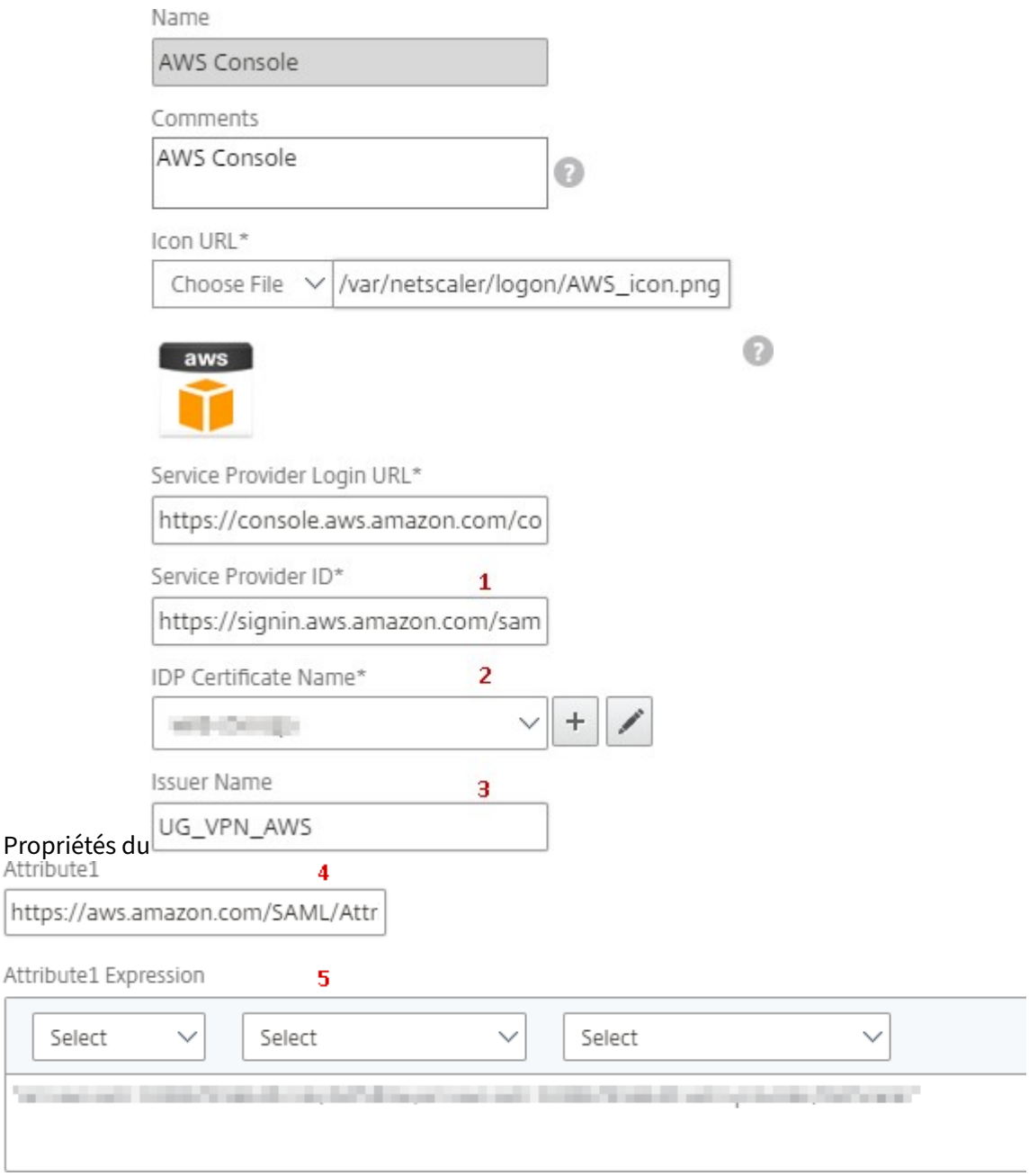


4. Sélectionnez **AWS Console** dans la liste déroulante.



5. Remplissez le modèle d'application avec les valeurs appropriées.

Propriétés du



6. Entrez les détails de configuration SAML suivants, puis cliquez sur **Continuer**.

   ID du fournisseur de services —https://signin.aws.amazon.com/saml

   Nom du certificat de signature : le certificat IdP doit être sélectionné

   Nom de l'émetteur : le nom de l'émetteur peut être renseigné selon votre choix

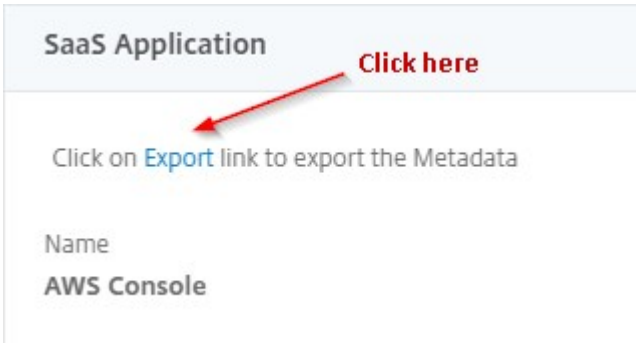
   Attribut 1 —`https://aws.amazon.com/SAML/Attributes/Role`

   Expression Attribute1, – `Role ARN`, `IdP ARN` comme indiqué à l'étape 3

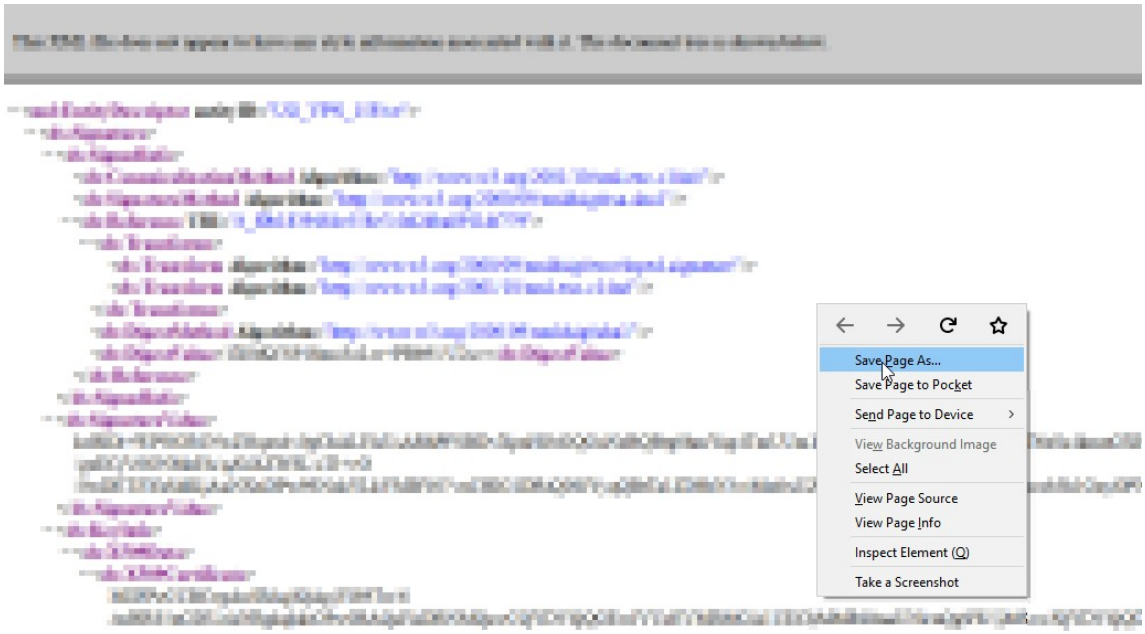
7. Cliquez sur **Terminé**.

ÉTAPE 2 : Exportez les métadonnées de l'IdP de la console AWS depuis NetScaler Gateway.

1. Cliquez sur **Unified Gateway > Authentification**.
2. Faites défiler l'écran vers le bas et cliquez sur modèle **AWS Console**. La fenêtre de l'application SaaS apparaît. Cliquez sur le lien **Exporter**.



3. **Les métadonnées** s'ouvrent dans une autre fenêtre. Enregistrer le fichier de **métadonnées du fournisseur d'identité**



ÉTAPE 3 : Configurez le fournisseur d'identité dans AWS Console.

Configuration et publication d'applications à l'aide d'un modèle - Configuration spécifique au serveur d'applications

Les liens suivants ouvrent des documents PDF qui fournissent des conseils spécifiques pour la configuration et la publication d'applications SaaS populaires à l'aide de modèles.

- 15Five

- Absorb
- Accompa
- Adobe Captivate Prime
- Adobe Creative Cloud
- Aha
- AlertOps
- Allocadia
- Ariba
- Assembla
- AWS Console
- BambooHR
- Base CRM
- BitaBIZ
- BlueJeans
- Blissbook
- Bonusly
- Box
- Bugsnag
- Buildkite
- CakeHR
- Cardboard
- Cedexis
- Celoxis
- Cisco Meraki
- ClearSlide
- CloudCheckr
- ConceptShare
- Concur
- Confluence

- Contactzilla
- Convo
- Circonus
- Dashlane
- Datadog
- Deskpro
- Deputy
- DigiCert
- DocuSign
- Domo
- Dropbox
- Duo
- eFront
- Ekarda
- Envoy
- ERP
- Expensify
- EZOfficeInventory
- EZRentOut
- Favro
- Federated Directory
- Feedly
- Fivetran
- Flatter Files
- Flowdock
- Freshdesk
- Front
- G-Suite
- GitHub

- GlassFrog
- GotoMeeting
- HappyFox
- Helpjuice
- Help Scout
- Hoshinplan
- Humanity
- Igloo
- Illumio
- Image Relay
- iMeet Central
- InteractGo
- iQualify One
- Jira
- Kanban Tool
- Keeper Security
- Kentik
- Kentik
- Kissflow
- KnowBe4
- KnowledgeOwl
- Kudos
- LaunchDarkly
- Lifesize
- Litmos
- LiquidPlanner
- LogDNA
- Mango
- Manuscript

- Marketo
- Mingle
- Mixpanel
- MuleSoft
- MyWebTimesheets
- New Relic
- Nmbrs
- Nuclino
- Office365
- OneDesk
- OpsGenie
- Orginio
- PagerDuty
- Panorama9
- ParkMyCloud
- Peakon
- People HR
- Pingboard
- Pipedrive
- PlanMyLeave
- PlayVox
- Podio
- ProdPad
- Proto.io
- Proxyclick
- PurelyHR
- Quandora
- Rackspace
- RealtimeBoard

- Remedyforce
- Robin
- Rollbar
- Salesforce
- Samanage
- Samepage
- Sentry
- ServiceDesk Plus
- ServiceNow
- Shufflrr
- Skeddly
- Skills Base
- Slack
- Slemma
- Sli.do
- Smartsheet
- Spoke
- Spotinst
- SproutVideo
- StatusCast
- Status Hero
- StatusHub
- Statuspage
- Sumo Logic
- Supermood
- Syncplicity
- Tableau
- Targetprocess
- Teamphoria

- Testable
- TestFairy
- TextExpander
- TextMagic
- ThousandEyes
- Thycotic Secret server
- Tinfoil Security
- Trisotech
- Trumba
- TwentyThree
- UniFi
- UserEcho
- UserVoice
- Velpic
- VictorOps
- VIDIZMO
- Visual Paradigm
- Weekdone
- Wepow
- When I Work
- Workday
- Workpath
- Workplace
- Workstars
- Workteam
- XaitPorter
- Ximble
- XMatters
- Yodeck

- Zendesk
- ZIVVER
- Zoho One
- ZIVVER
- Zoom