Citrix SD-WAN WANOP 11.3

Machine translated content

Disclaimer

La version officielle de ce document est en anglais. Certains contenus de la documentation Cloud Software Group ont été traduits de façon automatique à des fins pratiques uniquement. Cloud Software Group n'exerce aucun contrôle sur le contenu traduit de façon automatique, qui peut contenir des erreurs, des imprécisions ou un langage inapproprié. Aucune garantie, explicite ou implicite, n'est fournie quant à l'exactitude, la fiabilité, la pertinence ou la justesse de toute traduction effectuée depuis l'anglais d'origine vers une autre langue, ou quant à la conformité de votre produit ou service Cloud Software Group à tout contenu traduit de façon automatique, et toute garantie fournie en vertu du contrat de licence de l'utilisateur final ou des conditions d'utilisation des services applicables, ou de tout autre accord avec Cloud Software Group, quant à la conformité du produit ou service à toute documentation ne s'applique pas dans la mesure où cette documentation a été traduite de façon automatique. Cloud Software Group ne pourra être tenu responsable de tout dommage ou problème dû à l'utilisation de contenu traduit de façon automatique.

Contents

À propos de Citrix SD-WAN WANOP

December 14, 2022

Les appliances Citrix SD-WAN WANOP optimisent vos liaisons WAN, offrant ainsi à vos utilisateurs un maximum de réactivité et de débit à n'importe quelle distance. Une appliance Citrix SD-WAN WANOP est facile à déployer, car elle fonctionne de manière transparente. Une installation de vingt minutes accélère votre trafic WAN sans autre configuration requise. Vous n'avez pas à modifier vos applications, serveurs, clients ou infrastructure réseau. Vous pouvez toutefois les modifier après l'installation de Citrix SD-WAN WANOP sans affecter l'accélération du trafic. Une appliance Citrix SD-WAN WANOP doit être reconfigurée uniquement lorsque vos liaisons WAN changent.

Les appliances Citrix SD-WAN WANOP prennent en charge une gamme complète d'optimisations, notamment :

- Compression multi-sessions avec des rapports de compression allant jusqu'à 10 000:1.
- Accélération du protocole pour les systèmes de fichiers réseau Windows (CIFS), les applications virtuelles (ICA et CGP, y compris la nouvelle norme *ICA multisession*), Microsoft Outlook (MAPI) et SSL.
- Traffic shaping pour garantir que le trafic hautement prioritaire et interactif a priorité sur le trafic de faible priorité ou en vrac.
- Accélération avancée du protocole TCP, qui réduit les retards sur les liaisons congestionnées ou à latence élevée.
- Mise en cache vidéo.

Comment fonctionne Citrix SD-WAN WANOP ?

Les produits Citrix SD-WAN WANOP fonctionnent par paires, un à chaque extrémité d'une liaison, pour accélérer le trafic sur la liaison. Les transformations effectuées par l'expéditeur sont inversées par le destinataire.

Toutefois, une appliance (ou appliance virtuelle) peut gérer de nombreux liens, de sorte que vous n'avez pas à consacrer une paire à chaque connexion.

Une entreprise dispose généralement d'une appliance Citrix SD-WAN WANOP par site (appliances plus grandes sur des sites plus importants, plus petites sur des sites plus petits), bien qu'une entreprise disposant de nombreuses succursales puisse disposer de plusieurs appliances dans son centre de données central.

Lien d'un site doté d'une appliance Citrix SD-WAN WANOP vers un site qui n'a pas d'appliance Citrix SD-WAN WANOP fonctionne normalement, mais son trafic n'est pas accéléré.

Les fonctionnalités Citrix SD-WAN WANOP incluent une compression robuste pour des performances rapides sur des liaisons relativement lentes, et un contrôle de débit sans perte pour faire face à la congestion. Les optimisations TCP surmontent les principales limites des liens problématiques, et l'optimisation des applications supporte les limites des applications conçues pour les réseaux locaux à grande vitesse. Une fonction d'autodétection rend le déploiement rapide et facile.

Caractéristiques et avantages de Citrix SD-WAN WANOP

Tout temps que les travailleurs passent à attendre que leurs ordinateurs répondent est perdu du temps, ce qui entraîne une perte de productivité. Lorsque les utilisateurs travaillent à distance ou utilisent des ressources hors site, leur productivité dépend de la réactivité de leurs connexions réseau. La sauvegarde de la réactivité de leurs connexions nécessite une accélération avancée du réseau.

La gamme de produits Citrix SD-WAN WANOP protège votre productivité en fournissant des performances de connexion WAN et Internet fiables grâce à un ensemble d'optimisations multiples, qui renforcent chacune les autres. Pour assurer une productivité maximale dans l'ensemble de votre entreprise, il existe des produits Citrix SD-WAN WANOP pour tous les besoins, du plus grand datacenter jusqu'à la plus petite succursale et même l'ordinateur portable individuel.

Citrix SD-WAN WANOP offre une facilité d'utilisation robuste même avec des liaisons sous-dimensionnées ou dégradées.

Caractéristiques en un coup d'œil :

Pour plus d'informations, consultez le tableau

Caractéristiques et avantages :

Voici quelques-uns des principaux avantages de notre gamme de produits Citrix SD-WAN WANOP.

La**compression surmonte les faibles vitesses de liaison**. Le problème le plus évident avec les liaisons de réseau étendu (WAN) et les liaisons Internet est leur faible bande passante par rapport aux réseaux locaux (LAN). Un réseau étendu de 1 Mbps ne possède que 1 % du débit d'un réseau local de 100 Mbps. Comment surmonter la faible bande passante des liaisons ? Avec compression. Un taux de compression de 100:1 permet à une liaison de 1 Mbps de transférer des données aussi rapidement qu'un 100 Mbps. Ce facteur d'accélération est atteint lorsque les critères suivants sont remplis :

- L'algorithme de compression doit être capable de fournir des rapports de compression élevés.
- L'algorithme de compression doit être très rapide (beaucoup plus rapide que la bande passante du lien, et idéalement aussi rapide que le LAN).
- Les segments LAN de la liaison doivent avoir un contrôle de flux indépendant du segment WAN, car les différents segments traitent les données à des débits différents.

- Plusieurs moteurs de compression doivent être utilisés pour répondre aux différents besoins des différents types de trafic. Le trafic interactif nécessite relativement peu de bande passante, mais est très sensible au retard, tandis que les transferts en vrac sont très sensibles à la bande passante mais ne sont pas sensibles au retard.

L'**accélération du protocole TCP surmonte la congestion**. Toute tentative d'envoi de trafic plus rapide que la vitesse de liaison entraîne une congestion, ce qui entraîne de nombreux problèmes causés par des pertes de paquets élevées et une forte latence de file d'attente.

Contrôle du débit sans perte. Le protocole TCP/IP n'a aucun contrôle de flux pour ralentir directement les expéditeurs, et l'absence de ce mécanisme de contrôle nécessaire rend normales les pertes de paquets et les retards excessifs de file d'attente, même sur les liaisons stratégiques. (Si quelque chose, ce problème s'aggrave avec le temps, comme l'attestent les documents sur le phénomène de **bufferbloat**.)

Un dispositif Citrix SD-WAN WANOP résout ce problème en fournissant le contrôle de flux qui a été omis dans le protocole TCP/IP. Contrairement aux solutions ordinaires de qualité de service (QoS), qui réallouent simplement la perte de paquets, Citrix SD-WAN WANOP fournit un contrôle de flux sans perte qui contrôle la vitesse à laquelle les expéditeurs de points de terminaison transmettent les données, au lieu de permettre aux expéditeurs de transmettre les données à toute vitesse qu'ils souhaitent, et de supprimer les paquets lorsqu'ils envoient Trop. Chaque expéditeur transmet seulement autant de données que Citrix SD-WAN WANOP lui permet d'envoyer, sans jamais laisser tomber un paquet, et ces données sont placées sur le lien à la bonne vitesse pour garder le lien complet sans débordement. En éliminant les données excédentaires, Citrix SD-WAN WANOP n'est pas obligé de les rejeter. Sans Citrix SD-WAN WANOP, les paquets abandonnés doivent être envoyés à nouveau, provoquant des retards inutiles. Le contrôle du débit sans perte élimine également les retards causés par un tampon excessif. Le contrôle du débit sans perte est la clé d'une réactivité maximale sur une liaison occupée, permettant à une liaison qui était autrefois encombrée au point d'inutilisabilité à 40 % d'utilisation de rester productive et réactive à 95 % d'utilisation.

Éliminer l'iniquité fondée sur la distance. Les liens avec une latence élevée ou des pertes de paquets sont difficiles à utiliser à pleine bande passante, en particulier avec les variantes TCP ordinaires telles que TCP Reno. Les conséquences sont des retards excessifs et de la difficulté à obtenir la bande passante que vous payez. Plus la distance de liaison est longue, plus le problème devient grave.

L'accélération du protocole SD-WAN WANOP TCP de Citrix minimise ces effets, permettant aux liaisons intercontinentales et même satellites de fonctionner à pleine vitesse.

Le traffic shaping gère automatiquement la bande passante. Du côté de la sortie, un algorithme de type fair-queuing-like garantit que chaque connexion est mise en file d'attente indépendamment et compte tenu de sa juste part de la bande passante du lien. Les stratégies de traffic shaping permettent d'accorder une priorité plus élevée ou moins élevée à différents services.Optimisations des applications Surmonter les limitations de conception

Les applications et les protocoles conçus pour être utilisés sur les réseaux locaux sont notoires pour leurs performances médiocres sur les réseaux étendus, car les concepteurs n'ont pas tenu compte des effets des longs retards de la vitesse de la lumière sur leurs protocoles. Par exemple, une simple opération de système de fichiers Windows (CIFS) peut prendre jusqu'à 50 allers-retours à mesure que les messages passent d'un bout à l'autre du réseau. Dans un réseau étendu avec un temps aller-retour de 100 ms, 50 aller-retour entraînent un retard de cinq secondes.

Bien que les retards de vitesse de lumière soient une limitation fondamentale, les optimisations d'applications peuvent effectuer les mêmes opérations dans un plus petit nombre d'aller-retour, généralement par le biais d'opérations spéculatives. Lorsque l'application originale émettrait une commande à la fois et attendrait qu'elle se termine avant d'émettre la suivante, il est souvent parfaitement sûr d'émettre une série de commandes sans attendre. En outre, les transferts de données peuvent être accélérés grâce à une combinaison d'opérations de pré-extraction, de lecture anticipée et d'écriture arrière. En regroupant autant d'opérations que possible en un seul aller-retour, les performances peuvent être multipliées par dix ou plus.

Les optimisations Citrix SD-WAN WANOP sont particulièrement efficaces sur CIFS/SMB (le système de fichiers Windows), MAPI (le protocole Outlook/Exchange) et HTTP.

Plusieurs optimisations améliorent les performances des Applications virtuelles/bureaux virtuels (Citrix HDX). Les appliances WANOP Citrix SD-WAN étant des produits Citrix, elles sont particulièrement efficaces pour accélérer les protocoles Citrix, tels que Citrix Virtual Apps and Desktops. Tous les aspects de l'accélération Citrix SD-WAN WANOP entrent en jeu avec ces protocoles pour rendre l'expérience utilisateur à distance aussi productive que possible.

Les appliances WANOP SD-WAN Citrix négocient des options de session avec les serveurs Citrix Virtual Apps and Desktops. Cela permet à l'appliance Citrix SD-WAN WANOP d'appliquer les améliorations suivantes :

- Il remplace la compression native du serveur par une compression Citrix SD-WAN WANOP plus performante.
- Il base la priorité de mise en forme du trafic de la connexion sur les bits prioritaires incorporés dans chaque connexion Citrix Virtual Apps and Desktops. Cela permet à la priorité de la connexion de varier en fonction du type de trafic. Par exemple, les tâches interactives sont des tâches hautement prioritaires et les tâches d'impression sont des tâches de faible priorité.
- Il rassemble et rapporte des statistiques basées sur les applications virtuelles ou les applications Virtual Desktops utilisées.
- Il maintient le chiffrement de bout en bout de la connexion d'origine.

Détection automatique pour une configuration minimale. Étant donné que la solution est à double extrémité, exigeant qu'un produit Citrix SD-WAN WANOP soit présent aux deux extrémités de la liaison, le déploiement semble imposer un fardeau aux bureaux distants, en particulier ceux qui n'ont pas de

personnel informatique spécialisé. Cependant, Citrix SD-WAN WANOP est conçu pour être très facile à installer et à entretenir. Une installation typique prend environ vingt minutes. Les seuls paramètres nécessaires sont les paramètres réseau habituels (tels que l'adresse IP et le masque de sous-réseau), l'adresse d'un serveur de licences Citrix et la vitesse d'envoi et de réception de la liaison.

Seul un niveau minimal de configuration est possible grâce à l'autodétection, grâce à laquelle un serveur Citrix SD-WAN WANOP détermine quelles connexions peuvent être accélérées (et celles qui ne peuvent pas), sans configuration manuelle. Un serveur Citrix SD-WAN WANOP à l'autre extrémité de la liaison est automatiquement détecté, et la connexion est ensuite accélérée. Vous pouvez ajouter des appliances Citrix SD-WAN WANOP à votre réseau de manière ad hoc. Vous n'avez même pas à informer les appareils existants de l'arrivée d'un nouveau. Ils le découvrent par eux-mêmes.

Un Citrix SD-WAN WANOP utilise les options d'en-tête TCP pour signaler sa présence et négocier les paramètres d'accélération avec le Citrix SD-WAN WANOP distant car les options d'en-tête TCP font partie de la norme TCP, cette méthode fonctionne très bien, sauf dans les cas où les pare-feu sont programmés pour rejeter tous les options. De tels pare-feu existent, mais ils peuvent être configurés pour permettre la transmission des options utilisées par Citrix SD-WAN WANOP.

Les opérations Citrix SD-WAN WANOP sont transparentes pour l'expéditeur et le destinataire. Les autres périphériques de votre réseau ne savent pas que Citrix SD-WAN WANOP
existe. Ils continuent à travailler comme ils l'ont fait avant l'installation de Citrix SD-WAN WANOP. Cette transparence élimine également tout besoin d'installer des logiciels spéciaux sur vos serveurs ou clients afin de bénéficier de l'accélération Citrix SD-WAN WANOP. Tout fonctionne de manière transparente.

Fonctionnalités de la gamme de produits :

Chaque produit de la gamme de produits Citrix SD-WAN WANOP fournit des fonctionnalités d'accélération WANOP de base Citrix SD-WAN. La plupart des modèles ont également des fonctionnalités supplémentaires, telles que :

- Mise en cache de vidéo
- Ponts accélérés multiples avec fonction de dérivation Ethernet
- Surveillance et gestion via l'interface graphique, l'interface de ligne de commande, SNMP, AppFlow et Citrix ADM.

Différents produits Citrix SD-WAN WANOP ont des capacités différentes. Les produits qui prennent en charge des bandes passantes WAN plus élevées prennent également en charge un plus grand nombre d'utilisateurs et ont généralement plus de ressources : plus de CPU de puissance, plus de mémoire, plus de disques et plus de ponts accélérés.

Les fonctionnalités des produits qui s'exécutent sur votre propre matériel, tels que le plug-in Citrix SD-WAN WANOP et Citrix SD-WAN WANOP VPX, dépendent de la vitesse du matériel et de la quantité de ressources système que vous consacrez à l'accélération.

Pour obtenir des spécifications à jour, reportez-vous à la Fiche technique SD-WAN de Citrix.

Architecture Citrix SD-WAN WANOP

Les appliances Citrix SD-WAN WANOP accélèrent le trafic sur vos liaisons WAN. Pour accélérer un WAN, vous avez besoin d'au moins deux appliances Citrix SD-WAN WANOP, un pour chaque site que vous souhaitez accélérer.

L'appliance Citrix SD-WAN WANOP côté de l'envoyeur applique une série d'optimisations et de transformations à votre trafic, telles que la compression et le chiffrement. De nombreuses opérations nécessitent que le serveur Citrix SD-WAN WANOP côté récepteur effectue une opération inverse, telle que la décompression ou le déchiffrement, pour restaurer le trafic à son état d'origine.

Ainsi, la plupart des optimisations nécessitent que le trafic passe par deux appliances Citrix SD-WAN WANOP. Certaines optimisations sont effectuées à une seule extrémité et sont effectuées par l'appliance locale agissant seul. Ces optimisations incluent le traffic shaping et la mise en cache vidéo.

Les appliances Citrix SD-WAN WANOP sont largement transparentes pour le réseau. L'appliance elle-même semble être un pont, et non un routeur, une Gateway ou un proxy. Cette invisibilité permet d'installer l'appliance sans configurer d'autres matériels. Les optimisations de l'appliance sont également transparentes, détectées uniquement par l'appliance partenaire à l'autre extrémité du lien.

Les appliances Citrix SD-WAN WANOP peuvent être ajoutées au réseau à volonté, car leurs fonctions de détection automatique et de négociation automatique garantissent qu'une nouvelle appliance sur le réseau est immédiatement détectée par d'autres appliances et que l'accélération commence immédiatement.

Bien que le diagramme ci-dessus montre un réseau avec seulement deux appliances, une seule appliance Citrix SD-WAN WANOP peut communiquer avec n'importe quel nombre de sites partenaires. Les réseaux point à point, en étoile et maillés sont tous pris en charge.

Outre les appliances autonomes, les produits d'accélération Citrix SD-WAN WANOP incluent des machines virtuelles (la série Citrix SD-WAN WANOP VPX) et un service d'accélération installable pour les systèmes Windows (le plug-in Citrix SD-WAN WANOP).

Ce que signifie l'accélération

Dans la terminologie WANOP SD-WAN de Citrix, « accélération » est la réduction du temps de transaction, ce qui réduit le temps d'attente des utilisateurs. Étant donné que le temps que les utilisateurs passent en attente représente une perte de productivité directe, le principal avantage de l'accélération est l'augmentation de la productivité.

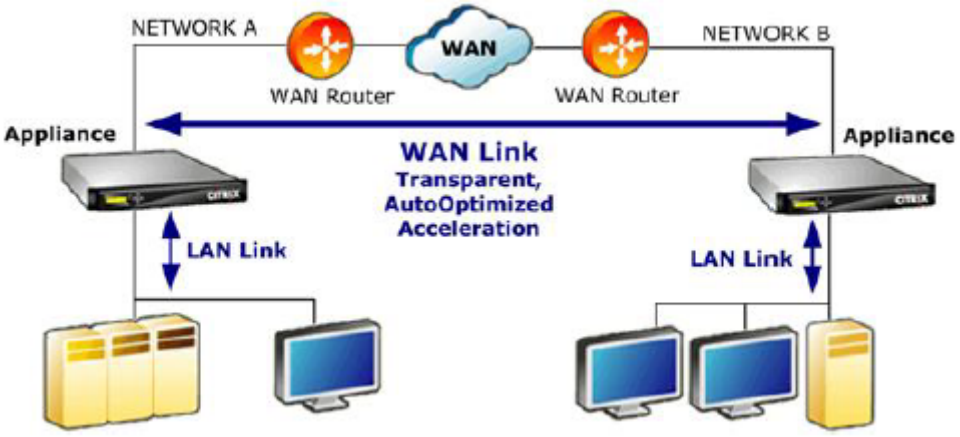
Dans le trafic réseau, une transaction va de très petite taille (un seul octet de données dans une session de terminal telnet ou SSH) à très grande taille, comme pour les transferts FTP, dont la taille dé-

passe souvent un gigaoctet. Un accélérateur pratique doit accélérer toute la gamme des tailles de transaction, du trafic interactif au trafic en vrac, offrant les meilleures performances et l'expérience utilisateur à tous les niveaux. La technologie Citrix SD-WAN WANOP y parvient de diverses façons.

Fonctionnement de l'accélération : Le pipeline

Pour voir comment fonctionne l'appliance Citrix SD-WAN WANOP, consultez de près le diagramme du pipeline de flux de trafic. Comme vous pouvez le voir, il y a deux pipelines :

1. Le pipeline d'envoi, qui accélère l'entrée des données dans le WAN à partir du LAN local.
2. Le pipeline de réception, qui accélère les données sortant du WAN et entrant dans le LAN local.



Envoyer le pipeline

Pour comprendre l'appliance, considérez le pipeline d'envoi une unité à la fois.

1. Tampon d'entrée. Les paquets du réseau local sont reçus par l'appliance. Étant donné que le trafic non-TCP/IP est optimisé uniquement par le régulateur du trafic, les paquets non-TCP sont détournés directement vers le régulateur du trafic. Le trafic TCP/IP (appelé trafic TCP à partir de maintenant) traverse le reste du pipeline.
2. Cache vidéo. Si le trafic TCP correspond aux paramètres du cache vidéo, la demande est transmise à l'unité de cache vidéo.
3. Détection automatique côté LAN. Outre le traffic shaping, les optimisations côté envoyeur nécessitent une appliance distante ainsi que l'appliance locale. Toutes les connexions qui ne passent pas par une appliance distante sont détournées vers le régulateur du trafic. Cette action est effectuée par la logique de détection automatique côté LAN. Le test réel d'une appliance distante est effectué par l'unité de détection automatique côté WAN.

4. Contrôle de flux côté LAN .CITRIX SD-WAN WANOP agit comme un proxy TCP transparent, recevant et accusant réception des paquets de l'expéditeur du point de terminaison pour le compte du récepteur du point de terminaison. Cela permet à l'appliance d'accepter de grandes quantités de données de l'expéditeur local très rapidement, à pleine vitesse du réseau local, quelle que soit la lenteur du trafic sur le réseau étendu. (TCP normal utilise le contrôle de la vitesse de bout en bout, ce qui n'est pas assez agile pour permettre des performances maximales.) En outre, le contrôle de flux de Citrix SD-WAN WANOP est sans perte, ce qui signifie que l'expéditeur local ne voit jamais un paquet abandonné, ce qui augmente la fiabilité et l'efficacité.
5. Moteurs applications.Citrix SD-WAN WANOP effectue des optimisations spécifiques pour plusieurs protocoles, notamment :

   - Citrix Virtual Apps and Desktops, à l'aide des protocoles ICA et CGP.
   - Système de fichiers Windows (CIFS, y compris les versions SMB1 et SMB2)
   - Outlook/Exchange (MAPI)

   Ces optimisations réduisent le temps de transaction. Cela se fait en réécrivant, combinant et réordonnant des commandes, en utilisant la lecture anticipée et l'écriture derrière, en utilisant une connaissance du protocole pour un traffic shaping plus avancé et des conseils de compression.
6. Moteur de compression. La compression réduit les transactions, ce qui réduit le temps nécessaire pour transférer les données sur le lien. Le compresseur Citrix SD-WAN WANOP utilise plusieurs algorithmes de compression, certains très efficaces pour les petites transactions, certains optimisés pour les transactions en vrac et d'autres pour les transactions de taille moyenne. Les rapports de compression de 10 000:1 sont facilement obtenus par le compresseur Citrix SD-WAN WANOP. Le compresseur est très rapide, ce qui permet de maintenir des rapports de compression élevés à pleine vitesse WAN. Avec le traitement Citrix SD-WAN WANOP, un fichier qui compresse à un rapport de 100:1 peut facilement être envoyé via une liaison de 1 Mbit/s avec un débit global de 100 Mbit/s.
7. Moteur de sécurité. Certaines fonctionnalités Citrix SD-WAN WANOP nécessitent que les deux appliances entretiennent une relation d'homologue sécurisée entre elles et avec le serveur d'origine. Le moteur de sécurité authentifie cette relation d'homologue et chiffre les connexions de données accélérées entre eux. Une relation homologue sécurisée permet l'utilisation de la compression SSL et l'accélération du trafic crypté Apps/Virtual Desktops (ICA/CGP), Windows Filesystem (CIFS) et Outlook/Exchange (MAPI).
8. Contrôle du débit côté WAN-Side et détection automatique. La liaison WAN est l'endroit où les ralentissements du trafic se produisent, et si la liaison est congestionnée, les paquets sont perdus et doivent être retransmis. La retransmission des paquets provoque toujours un retard important, parfois plus d'une seconde. L'unité de contrôle de débit côté WAN utilise des éléments

de retransmission avancés et un protocole TCP/IP avancé pour des performances maximales dans les liaisons « propres » et « perturbées ». L'unité de détection automatique identifie la présence d'une unité WANOP SD-WAN partenaire Citrix sur une base connexion par connexion, ce qui empêche l'utilisation des optimisations là où elles ne sont pas souhaitées et permet de détecter de nouveaux matériels par les appliances existantes dès qu'ils sont ajoutés au réseau. La détection automatique utilise des options dans le champ d'en-tête TCP. Ceci est normalement transparent mais peut être bloqué par certains pare-feu, qui doivent être reconfigurés.

9. Classificateur d'applications. Cette unité examine tout le trafic circulant via Citrix SD-WAN WANOP et identifie l'application ou le protocole auquel il appartient. Ces informations sont utilisées dans les rapports et par le régulateur du trafic.
10. Régulateur de trafic. Pour éviter la congestion, les files d'attente excessives et d'autres sources de retards évitables, le régulateur de trafic injecte du trafic sur le WAN à un taux légèrement inférieur au débit de données du WAN, afin de garantir que le WAN ne soit jamais dépassé. Un algorithme de mise en file d'attente équitable pondérée est utilisé pour s'assurer que tout le trafic obtient sa juste part de la bande passante du lien. Les politiques de traffic shaping permettent à différents types de trafic de recevoir des poids différents, de sorte que certains trafic obtiennent plus de bande passante que d'autres.

Canalisation de réception

Le pipeline dans la direction de réception est similaire à la direction d'envoi, sauf qu'au lieu de chiffrer, il décrypte, et au lieu de compresser, nous avons des décompresses. Notez également qu'il y a également un régulateur du trafic dans la direction de réception, appliquant des stratégies de traffic shaping au trafic WAN entrant, de sorte que les deux directions sont réglementées.

Détection automatique et transformation au niveau des paquets

L'algorithme de détection automatique insère les options d'en-tête TCP pour annoncer la présence d'une appliance Citrix SD-WAN WANOP et faciliter la négociation. Ces options sont dans la gamme de 24-31. Les transformations de niveau paquet suivantes sont utilisées :

- Sur le paquet initial de la connexion (le paquet SYN), l'appliance émettrice attache des options d'en-tête qui s'identifient comme une appliance Citrix SD-WAN WANOP et déclarent également d'autres fonctionnalités, telles que la compression. C'est ce qu'on appelle un « paquet SYN taggé ».
- Lors de la réception d'un paquet SYN taggé, l'appliance réceptrice attache les options d'en-tête au paquet SYN-ACK, s'identifiant à son tour et annonçant ses capacités.

- Une fois que l'appliance émettrice reçoit le paquet SYN-ACK taggé, la connexion peut être accélérée en fonction des capacités partagées par les deux appliances. Par exemple, la connexion est compressée si les deux appliances déclarent la prise en charge de la compression.
- Les numéros de séquence initiale TCP (iSNS) dans les deux directions sont modifiés en ajoutant 2 000 000 000 aux valeurs d'origine. Il s'agit d'une précaution qui empêche la connexion de se poursuivre en cas de défaillance d'une appliance ou de modification de routage qui l'empêche de voir tout le trafic dans la connexion. Une fois qu'une connexion est accélérée, elle doit rester accélérée tout au long de sa durée de vie.
- La valeur MSS est réduite, généralement à 1380 octets, pour garantir que chaque paquet a de la place pour les options d'en-tête Citrix SD-WAN WANOP TCP insérées.
- Les adresses IP et les numéros de port de la connexion restent inchangés.

Pré-accusé de réception

Les paquets SYN et SYN-ACK circulent de bout en bout :

- Le paquet SYN circule du client de point de terminaison, via l'appliance côté client, via le WAN, via l'appliance côté serveur et enfin vers le serveur.
- Le paquet SYN-ACK circule du serveur, par le biais de l'appliance côté serveur, sur le WAN, via l'appliance côté client et enfin vers le client.

Il en va de même pour les paquets finaux de la connexion, les paquets FIN, FIN-ACK et RST.

D'autres paquets, cependant, sont pré-reconnus. Par exemple, lorsque l'appliance côté serveur reçoit un paquet du serveur, elle le reconnaît immédiatement sur le réseau local et le met en mémoire tampon pour une éventuelle transmission sur le réseau étendu. Cela permet de remplir très rapidement les tampons de l'appliance côté serveur, de sorte qu'elle a toujours beaucoup de données à utiliser pour la compression et d'autres optimisations. (Ceci est très différent de l'opération TCP normale, où tous les accusés de réception proviennent du côté opposé du WAN, ce qui rend l'accusé de réception très lent, et forçant chaque segment de la connexion à se déplacer pas plus rapidement que le segment le plus lent, ce qui réduit considérablement l'efficacité de l'accélération.)

Déplacer le trafic entrant et sortant de l'appliance

Les appliances Citrix SD-WAN WANOP disposent d'un certain nombre de « modes de transfert ». Un mode de transfert est une méthode permettant d'obtenir le trafic entrant et sortant de l'appliance. Le plus commun est le mode en ligne, où le serveur Citrix SD-WAN WANOP semble être un périphérique de pont. Les paquets entrant sur un port de pont semblent quitter l'autre. Bien sûr, Citrix SD-WAN

WANOP transforme les données de différentes manières, donc dans de nombreux cas, le paquet quittant le deuxième port n'est pas identique à celui qui est entré dans le premier port, mais c'est ainsi qu'il apparaît pour le reste du réseau.

Lorsque le mode en ligne n'est pas pratique, plusieurs autres méthodes sont disponibles, notamment le mode WCCP. Ce sont des modes « à un bras », utilisant un seul câble d'interface.

> **Conseil**
>
> Vous pouvez gérer et surveiller vos appliances WANOP Citrix SD-WAN à l'aide de Citrix ADM. Pour plus d'informations, reportez-vous à la section Gestion des instances Citrix SD-WAN à l'aide de Citrix ADM.

Prise en main de Citrix SD-WAN WANOP

April 9, 2021

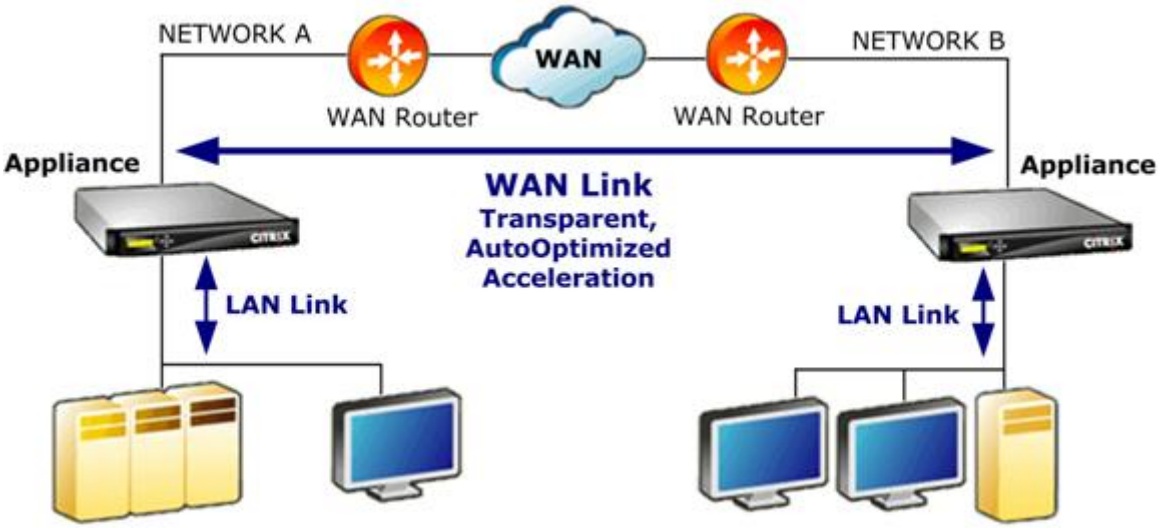
Le déploiement des appliances Citrix SD-WAN WANOP n'est pas difficile, mais des déploiements inappropriés peuvent causer des problèmes et fournir une accélération inadéquate. Veillez à sélectionner des appliances ayant une capacité suffisante pour que les liens que vous souhaitez qu'elles accélèrent. La sélection des produits est également l'un des facteurs à prendre en compte lorsque vous décidez de la meilleure façon d'adapter les appliances à votre topologie.

Les critères de déploiement les plus élémentaires sont les suivants :

- Tous les paquets de la connexion TCP doivent passer par une combinaison prise en charge de deux *unités d'accélération* (appliances Citrix SD-WAN WANOP ou plug-ins).
- La circulation doit passer par les deux unités d'accélération dans les deux sens.

Lorsque ces critères sont remplis, l'accélération est automatique.

L'accélération améliore les performances lorsque le trafic passe par deux appliances



Pour les sites disposant d'un seul réseau WAN, ces critères peuvent être respectés en plaçant l'appliance Citrix SD-WAN WANOP en ligne avec le WAN. Dans les sites plus complexes, d'autres options sont disponibles. Certains, tels que le support WCCP, sont disponibles sur tous les modèles. D'autres sont disponibles sur certains modèles seulement. Par conséquent, les besoins d'un site plus complexe peuvent limiter votre choix d'appliances.

Lors de l'évaluation de vos options, tenez compte de l'importance de maintenir les différents segments de votre réseau opérationnel en cas de défaillance d'un périphérique ou de nécessité de désactiver. Pour les déploiements en ligne, Citrix recommande une *carte de contournement Ethernet*. Cette carte, qui est facultative sur les appliances Citrix SD-WAN WANOP, dispose d'un relais qui se ferme en cas de défaillance de l'appliance, ce qui permet aux paquets de passer même si l'alimentation est perdue ou supprimée.

La redondance est une considération pour tous les types de déploiements. Les appliances Citrix SD-WAN WANOP offrent différents types de redondance :

- Les appareils SD-WAN WANOP 4000/5000 ont deux alimentations.
- Les appliances SD-WAN WANOP 4000/5000 disposent d'unités de disque redondantes.
- Les appliances peuvent être utilisées en mode haute disponibilité (deux appliances redondantes avec basculement automatique). Ce mode est pris en charge sur tous les modèles.

> **Remarque**
>
> Pour plus d'informations sur les appliances Citrix SD-WAN WANOP et les modes de déploiement, reportez-vous à la sectionDocumentation de la plateforme WANOP SD-WAN.

Sélectionner une appliance en fonction de la capacité

April 9, 2021

Pour un bon fonctionnement, votre appliance Citrix SD-WAN WANOP doit disposer de ressources adéquates pour prendre en charge le nombre de liaisons WAN que vous souhaitez accélérer et pour prendre en charge tous les utilisateurs de ces liaisons. Trois capacités sont importantes lors de la sélection d'une
appliance Citrix SD-WAN WANOP : capacité de liaison (bande passante), capacité utilisateur et capacité disque.

Capacité de liaison

Lors de la sélection d'une appliance Citrix SD-WAN WANOP, le facteur le plus important est qu'elle prend en charge vos liaisons WAN. Si votre site dispose d'une liaison WAN unique, votre appliance doit prendre en charge votre vitesse de liaison. Par exemple, un Citrix SD-WAN WANOP 2000-010 peut prendre en charge des liaisons allant jusqu'à 10 Mbps, ce qui serait approprié pour une liaison de 8 Mbps mais pas une liaison de 12 Mbps. Si votre site comporte plusieurs liens qui doivent être accélérés par une seule appliance, celle-ci doit prendre en charge la vitesse totale de toutes ces liaisons WAN ajoutées ensemble.

La vitesse maximale prise en charge est déterminée par une combinaison du matériel de l'appliance et de la licence de produit. La limite de bande passante sous licence est la vitesse maximale de liaison prise en charge par la licence.

Produit	Gamme WAN BW sous licence
Produits actuels	
Plug-in SD-WAN WANOP	S.O.
SD-WAN WANOP 400	2-6 Mbit/s
SD-WAN WANOP 800	2-10 Mbit/s
SD-WAN WANOP 2000, 2000WS	10-50 Mbit/s
SD-WAN WANOP 3000	5 0-155
SD-WAN WANOP 4000	310-1 000 Mbit/s
SD-WAN WANOP 5000	1 500-2 000 Mbit/s
SD-WAN WANOP VPX	1-45 Mbit/s

Tableau 1. Limites de bande passante sous licence par gamme de produits

Capacité utilisateur des applications virtuelles/bureaux virtuels

Chaque appliance est évaluée pour un nombre maximal d'utilisateurs XenApp ou Virtual Desktops. Cette valeur ne doit pas être dépassée lorsque votre déploiement utilise des applications virtuelles ou des bureaux virtuels. Si vous n'utilisez pas d'applications virtuelles ou de bureaux virtuels, considérez ce nombre comme un guide approximatif du nombre d'utilisateurs d'autres applications.

Produit	Nombre maximal d'utilisateurs
Plug-in SD-WAN WANOP	1
SD-WAN WANOP 400	10-30
SD-WAN WANOP 800	20-100
SD-WAN WANOP 2000, 2000WS	100-300
SD-WAN WANOP 3000	300-500
SD-WAN WANOP VPX	20-350
SD-WAN WANOP 4000	750-2,500
SD-WAN WANOP 5000	3,500-5,000

Tableau 2. Capacité utilisateur des applications virtuelles/postes de travail virtuels

Taille du disque

L'espace disque est principalement utilisé pour l'historique de compression, et plus d'espace disque se traduit par des performances de compression plus élevées.

La série SD-WAN WANOP 4000/5000 offre une capacité de disque allant de 1,8 To à 2,4 To. Cela se compare à 2,1 To pour le SD-WAN WANOP 3000, 470 Go pour le SD-WAN WANOP 2000, 80 Go pour le SD-WAN WANOP 800 et 40 Go pour le SD-WAN WANOP 400. SD-WAN WANOP VPX a une capacité de disque de 100-500 Go. Idéalement, une appliance doit avoir une capacité disque supérieure à la durée de cycle des données de la liaison. Par exemple, une liaison transportant principalement du trafic de mise à jour quotidien devrait avoir une capacité de disque de 24 heures ou plus. Avec un lien portant principalement des sessions utilisateur, cette fenêtre peut être plus petite. (Un lien de 1 Mbps peut transférer environ 10 Go par jour à pleine vitesse.)

Tableau 3. Exemples de durée de vie des données pour les tailles de disque

Modèle d'appliance	Vitesse de liaison 1 Mbit/s	Vitesse de liaison - 10 Mbps	Vitesse de liaison - 100 Mbps	Vitesse de liaison 1000 Mbps
Durée de vie des données à 33 % d'utilisation des liaisons				
SD-WAN WANOP 800	23 jours	2.3 jours	SO	SO
SD-WAN WANOP 2000, 2000WS	141 jours	14 jours	SO	SO
SD-WAN WANOP 5000	717 jours	72 jours	7.2 jours	17 heures
Durée de vie des données à 100 % d'utilisation des liens				
SD-WAN WANOP 800	8 jours	19 heures	SO	SO
SD-WAN WANOP 2000, 2000WS	47 jours	4.7 jours	SO	SO
SD-WAN WANOP 5000	239 jours	24 jours	2,4 jours	6 heures

Sélectionner le mode de déploiement en fonction de la topologie du centre de données

April 9, 2021

L'appliance peut être placée en ligne avec votre liaison WAN. L'appliance utilise deux ports Ethernet pontés pour le mode Inline. Les paquets entrent dans un port Ethernet et sortent par l'autre. Ce mode place l'appliance entre votre routeur WAN et votre LAN. Pour le reste du réseau, c'est comme si l'appliance n'était pas là du tout. Son fonctionnement est complètement transparent.

Le mode Inline présente les avantages suivants par rapport aux autres modes de déploiement :

- Performances maximales.

- Configuration très facile, en utilisant uniquement la page Installation rapide.
- Aucune reconfiguration de votre autre équipement réseau.

D'autres modes (WCCP, virtuel en ligne, redirecteur) sont moins pratiques à configurer, nécessitant généralement que vous reconfigurez votre routeur, et ils ont des performances légèrement inférieures.

Une considération de base en matière de déploiement est de savoir si votre site dispose d'un seul routeur WAN ou de plusieurs routeurs WAN. Vous devez également penser à quelles fonctionnalités peuvent être utilisées dans quels modes. L'obligation de prendre en charge les VPN affecte le placement de l'appliance dans votre réseau.

Les appliances Access Gateway prennent en charge les optimisations de Citrix SD-WAN WANOP TCP, ce qui permet d'accélérer les connexions VPN lorsque les appliances Citrix SD-WAN WANOP sont déployées avec Access Gateway.

Présentation des modes de déploiement

L'appliance peut être déployée dans les modes suivants :

Modes de transfert

- Mode**Inline : le mode**le plus transparent et le plus performant. Les données sont entrées sur un port Ethernet accéléré et sortent sur l'autre. Ne nécessite aucune reconfiguration du routeur de quelque nature que ce soit.
- **Inline with dual bridges (Inline with dual bridges**) : identique à la ligne, mais avec deux ponts accélérés indépendants.
- **Mode WCCP** : recommandé lorsque le mode en ligne n'est pas pratique. Pris en charge par la plupart des routeurs. Nécessite seulement trois lignes de configuration du routeur. Pour utiliser le mode WCCP sur un routeur Cisco, le routeur doit exécuter au moins IOS version 12.0 (11) S ou 12.1 (3) T. (WCCP signifie Web Cache Communications Protocol, mais le protocole a été considérablement élargi avec la version 2.0 pour prendre en charge une grande variété de périphériques réseau.)
- **Mode virtuel en ligne** : similaire au mode WCCP. Utilise le routage basé sur des stratégies. Nécessite généralement un port LAN dédié sur le routeur. Non recommandé sur les unités sans carte de contournement Ethernet. Pour utiliser le mode virtuel en ligne sur un routeur Cisco, le routeur doit exécuter IOS version 12.3 (4) T ou ultérieure.
- **Mode Groupe** : utilisé avec au moins deux appliances en ligne, une par lien, au sein d'un site. Recommandé uniquement lorsque plusieurs ponts, WCCP et modes inline virtuels sont tous impraticables.

- **Mode haute disponibilité** : combine de manière transparente deux appliances inline ou virtuelle en une paire primaire/secondaire. L'appliance principale gère tout le trafic. En cas de défaillance, l'appliance secondaire prend le relais. Ne nécessite aucune configuration de routeur. Nécessite une appliance dotée d'une carte de contournement Ethernet.
- **Mode transparent : mode**recommandé pour la communication avec le plug-in Citrix SD-WAN WANOP. En mode transparent, le plug-in initie les connexions de la même manière que l'appliance Citrix SD-WAN WANOP, en conservant l'adresse IP et le numéro de port d'origine de la connexion et en ajoutant les options Citrix SD-WAN WANOP aux en-têtes TCP/IP des paquets sélectionnés. En revanche, en mode redirecteur (non recommandé), le plug-in modifie l'adresse IP de destination et les numéros de port des paquets pour qu'ils correspondent à l'adresse IP de signalisation (et au port) de l'appliance.
- **Mode redirecteur** (non recommandé) : utilisé par le plug-in Citrix SD-WAN WANOP pour transférer le trafic vers l'appliance. Peut être utilisé comme mode autonome ou combiné avec l'un des autres déploiements. Ne nécessite aucune configuration de routeur.

Modes d'accélération

- **Mode Softboost** : variante TCP haute performance recommandée pour la plupart des liens. Bien qu'il offre moins de performances que le mode Boost, il fonctionne avec n'importe quel déploiement. Agit comme TCP normal, mais plus rapide.
- **Mode Boost** : variante TCP très agressive et limitée à la bande passante, utile pour les liaisons à grande vitesse, les liaisons intercontinentales, les liaisons satellites et d'autres liaisons à vitesse fixe pour lesquelles il est difficile d'atteindre une vitesse de liaison complète. Recommandé pour les liaisons point à point à vitesse fixe où le traffic shaping n'est pas requis.

> **Remarque**
>
> Pour plus d'informations sur les appliances Citrix SD-WAN WANOP et les modes de déploiement, reportez-vous à la sectionDocumentation de la plateforme Citrix SD-WAN WANOP.

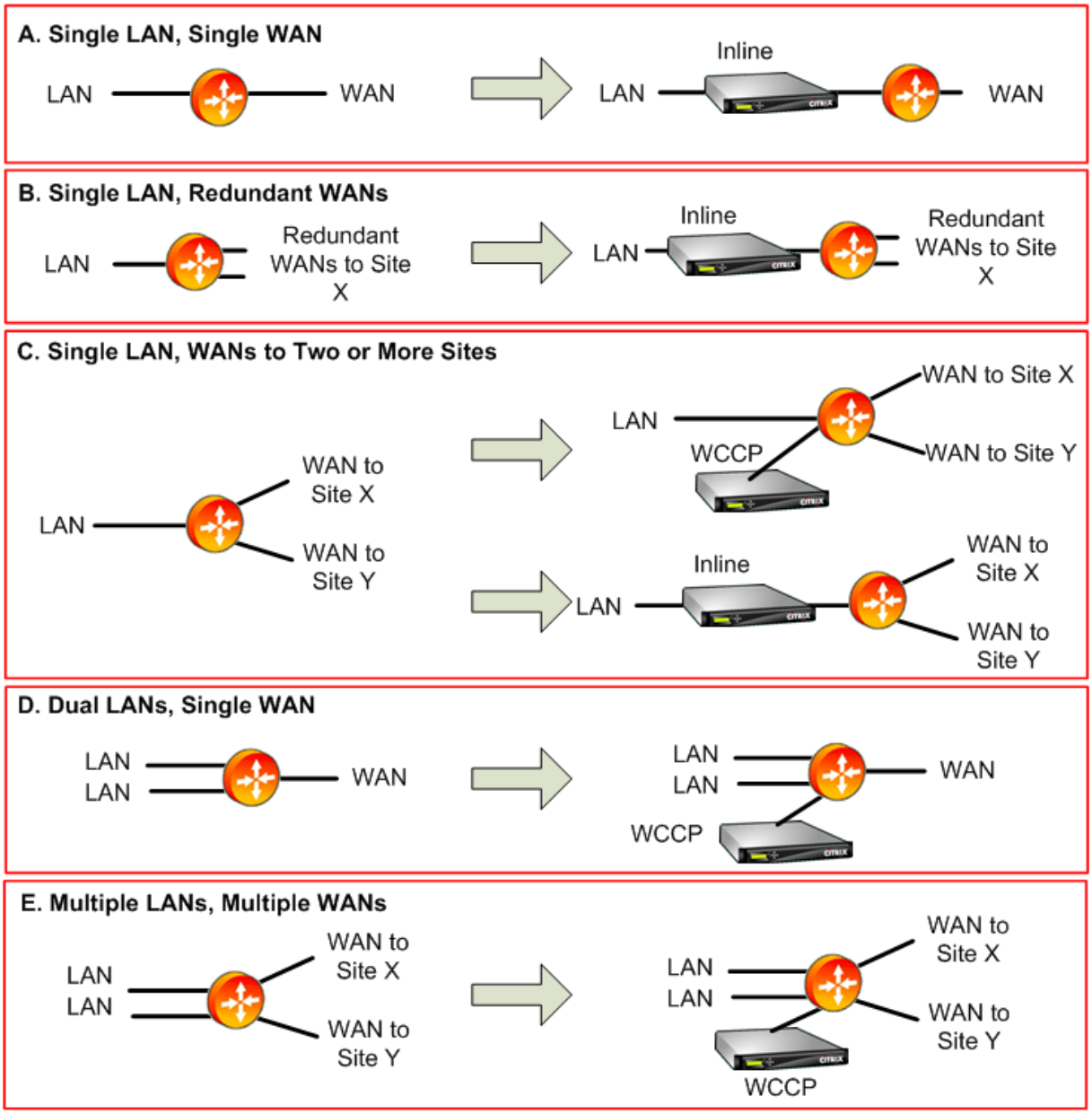
Sites avec un routeur WAN

April 9, 2021

Pour un site avec un seul routeur WAN, le principal problème dans le déploiement est de permettre à l'appliance Citrix SD-WAN WANOP de fonctionner en harmonie avec le routeur. La figure suivante

montre les modes de déploiement recommandés pour un routeur unique. Comparez-le au câblage de votre routeur pour trouver le meilleur mode pour votre environnement.

Modes de déploiement recommandés, basés sur la topologie du routeur WAN



Commentaires sur les modes de déploiement recommandés :

1. **LAN unique, WAN unique : mode Inline.** Le routeur dispose d'une seule interface LAN active et d'une seule interface WAN active. Le mode recommandé pour ce cas est le mode en ligne, qui fournit l'installation la plus simple, le plus de fonctionnalités et la plus haute performance de n'importe quel mode.
2. **LAN unique, WAN redondants : mode Inline.** Le mode Inline est également le meilleur pour

cette configuration.

3. **LAN unique, multiples WAN : Inline ou WCCP.** Cette topologie se répartit en deux catégories : hub-and-spoke ou multihop. Dans un déploiement en étoile, les connexions sont principalement entre un site en étoile et le site en étoile. Dans un déploiement multi-hop, de nombreuses connexions se font entre deux sites en rayon, les données passant par le site hub. Une seule connexion multi-hop peut donc impliquer jusqu'à trois appliances, selon les détails de l'emplacement de l'appliance du site concentrateur dans le flux de trafic.

   Pour un traffic shaping correct du trafic dans les déploiements à plusieurs sauts, tout le trafic WAN sur le routeur WAN du site hub doit également passer par l'appliance, au lieu d'être transmis directement par le routeur entre les interfaces WAN. Dans ce cas, WCCP est le mode préféré. Si le déploiement est en étoile et que la plupart du trafic se termine sur le site du concentrateur, un déploiement en ligne est préférable.

4. **LAN double, WAN unique : Inline (avec double ponts) ou WCCP.** Ce mode est pris en charge par les ponts doubles accélérés, le mode WCCP ou le mode virtuel en ligne.

5. **LAN multiples, WAN multiples : Inline (double ponts) ou WCCP.** Ceci est similaire au cas C, mais compliqué par la présence de plusieurs interfaces LAN ainsi que de plusieurs WAN. WCCP peut toujours être utilisé ici. Dans le cas de deux réseaux locaux, une appliance dotée de deux ponts peut également être utilisée en mode Inline.

   Pour plus d'informations, consultez le tableau

Sites avec plusieurs routeurs WAN

April 9, 2021

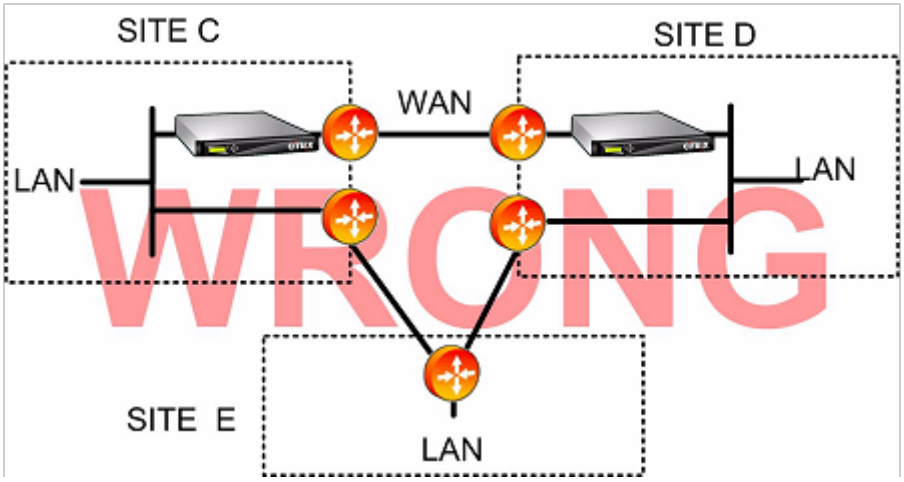
Plus d'un routeur WAN sur le même site soulève la possibilité d'un *routage asymétrique.* Normalement, les réseaux IP ne sont pas affectés par le chemin emprunté par les paquets, tant qu'ils arrivent à leur destination. Toutefois, l'appliance s'appuie sur l'affichage de chaque paquet dans la connexion. Les paquets « End-around » ne sont pas acceptables.

Dans un site avec un seul routeur WAN, le routage asymétrique n'est pas un problème, car l'appliance peut être placée dans le chemin entre le routeur et le reste du site, de sorte que le trafic entrant ou sortant du routeur passe également par l'appliance. Mais avec deux routeurs WAN, le routage asymétrique peut devenir un problème.

Des problèmes de routage asymétrique peuvent apparaître pendant l'installation ou une version ultérieure, à la suite d'un basculement vers une liaison secondaire ou d'autres formes de routage dynamique et d'équilibrage de charge. La figure suivante illustre un exemple de sites susceptibles de souffrir d'un routage asymétrique. Si les sites C et D utilisent toujours le chemin direct, C-D ou

D-C, lors de l'envoi de trafic les uns aux autres, tout va bien. Toutefois, les paquets qui prennent le chemin le plus long, C-E-D ou D-E-C, contournent les appliances, entraînant la non-accélération des nouvelles connexions et le blocage des connexions existantes.

Routage asymétrique

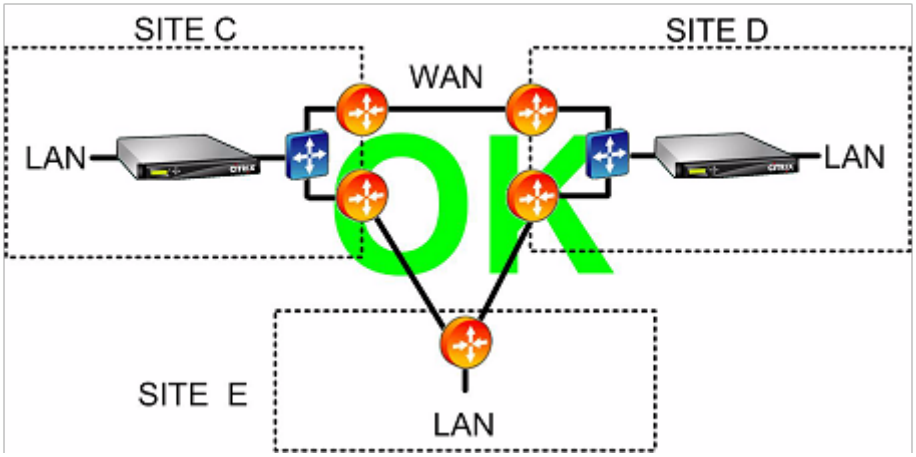


Le routage asymétrique peut être résolu par la configuration du routeur, le placement de l'appliance ou la configuration de l'appliance.

Si le routeur est configuré pour s'assurer que tous les paquets d'une connexion donnée passent toujours par l'appliance dans les deux sens, il n'y a pas d'asymétrie.

Si l'appliance est positionnée après le point où tous les flux WAN sont combinés, l'asymétrie est évitée et tout le trafic est accéléré, comme illustré dans la figure suivante.

Éviter le routage asymétrique grâce au bon positionnement de l'appliance



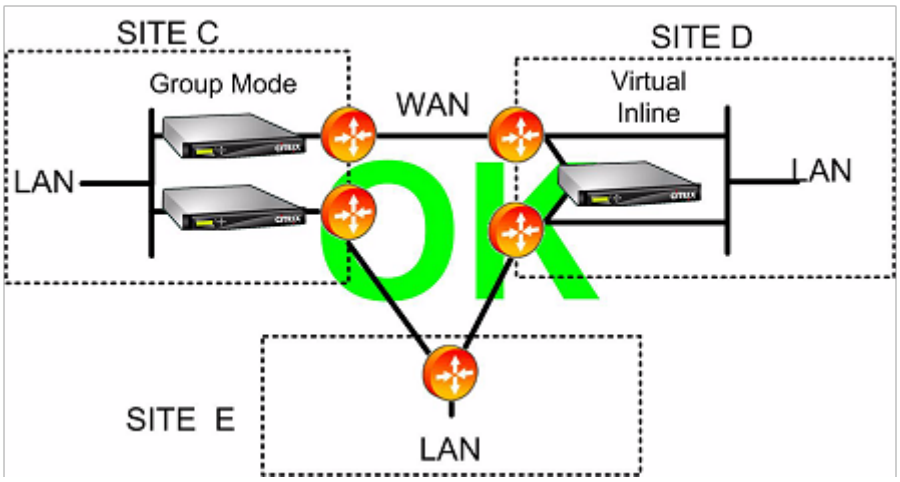
La configuration de l'appliance pour qu'elle utilise l'un des modes de transfert résistant à l'asymétrie suivants peut éliminer le problème :

- *Ponts multiples.* Une appliance dotée de deux ponts accélérés, ou de *paires accélérées* (par exemple, apA et apB), permet d'accélérer deux liaisons en mode Inline. Les deux liens peuvent

être entièrement indépendants, équilibrés de charge ou des liens principaux/de sauvegarde.

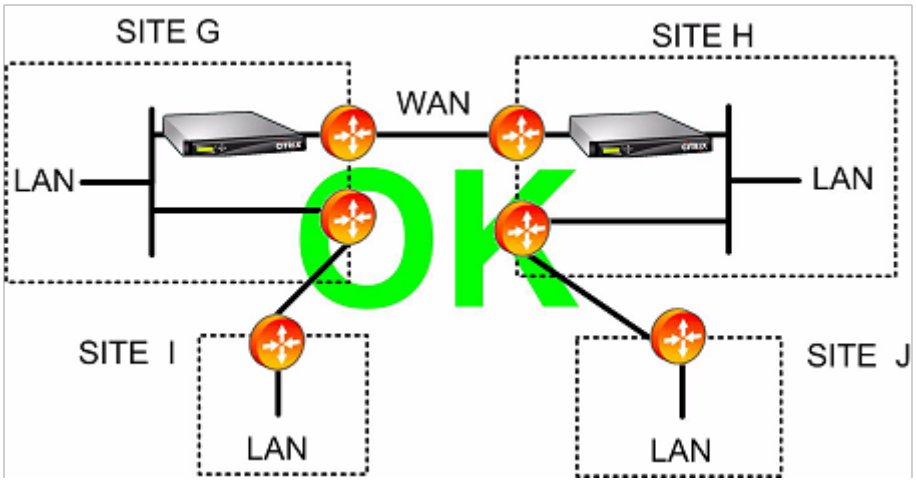
- Le*mode WCCP* permet de partager un seul matériel entre plusieurs routeurs WAN, ce qui lui permet de gérer tout le trafic WAN, quel que soit le lien sur lequel il arrive.
- *Le mode virtuel en ligne* permet de partager une seule appliance entre plusieurs routeurs WAN, ce qui lui permet de gérer tout le trafic WAN, quelle que soit la liaison sur laquelle elle arrive.
- *Le mode Groupe* permet à deux appliances en ligne ou plus de partager le trafic entre elles, en veillant à ce que le trafic qui arrive sur le mauvais lien soit transmis correctement. Étant donné que le mode groupe nécessite plusieurs appliances, il s'agit d'une solution coûteuse qui convient le mieux aux installations où les liaisons accélérées ont une grande séparation physique, ce qui rend les autres alternatives difficiles. Par exemple, si les deux liaisons WAN se trouvent sur des bureaux différents dans la même ville (mais que les campus sont connectés par une liaison à vitesse LAN), le mode groupe peut être le seul choix.

Élimination du routage asymétrique à l'aide du mode Groupe ou du mode Inline virtuel



> **Remarque**
>
> Une extrémité du lien peut utiliser le mode virtuel en ligne tandis que l'autre extrémité utilise le mode groupe. Les deux extrémités d'un lien n'ont pas besoin d'utiliser le même mode de transfert.

Les sites avec une seule liaison WAN ne peuvent pas avoir de problèmes de routage asymétrique



Défaillance de l'appliance gérée dans différents modes de déploiement

April 9, 2021

Les appliances Citrix SD-WAN WANOP offrent des garanties contre la perte de connectivité en cas de panne logicielle, matérielle et d'alimentation. Ces garanties dépendent du mode.

En **mode Inline**, les appliances assurent la continuité du réseau en cas de panne matérielle, logicielle ou d'alimentation. Le cas échéant, le relais de contournement de l'appliance se ferme en cas de perte d'alimentation ou de panne. Les appareils en ligne sans carte de contournement bloquent généralement le trafic en cas de défaillance grave, mais ils continuent à transférer le trafic dans certaines conditions, à savoir lorsque la pile réseau est en cours d'exécution mais que le logiciel d'accélération a été désactivé ou s'est arrêté en raison d'erreurs persistantes.

Les connexions accélérées existantes ne répondent généralement pas après une panne et finissent par être interrompues par l'application ou la pile réseau à l'un des points d'arrivée. Certaines connexions accélérées peuvent continuer en tant que connexions non accélérées après l'échec. Les nouvelles connexions s'exécutent en mode non accéléré.

Lorsque l'appliance revient en ligne, les connexions existantes continuent en tant que connexions non accélérées. Les nouvelles connexions sont accélérées.

En mode WCCP, le routeur contourne une appliance qui cesse de répondre et rouvre la connexion lorsque l'appliance recommence à répondre.** Le protocole WCCP comporte un contrôle de santé intégral.

Si l'option « verify-availability » est utilisée avec le mode virtuel en ligne, le routeur se comporte comme il le fait avec le mode WCCP, en contournant l'appliance lorsqu'elle n'est pas disponible et en se reconnectant lorsqu'elle l'est.** Si « verify-availability » n'est pas utilisé, tous les paquets transférés à l'appliance sont supprimés si celle-ci n'est pas disponible.

En **mode groupe**, une appliance peut être configurée pour échouer « ouvert » (pontage désactivé) ou « fermé » (pontage ou contournement activé).

En mode **haute disponibilité**, si une appliance HA tombe en panne, l'autre prend automatiquement le relais. Les cartes de contournement des appareils sont désactivées en mode HA. Par conséquent, si les appareils HA sont en mode Inline et que les deux appareils échouent, la connectivité est perdue.

En **mode redirecteur**, le plug-in Citrix SD-WAN WANOP effectue une vérification de l'état des appliances en mode redirecteur et contourne les appliances qui ne répondent pas, envoyant du trafic directement aux serveurs de point de terminaison.

Matrice des fonctionnalités et modes pris en charge

April 9, 2021

En général, tous les modes sont simultanément actifs. Toutefois, certaines combinaisons ne doivent pas être utilisées ensemble, comme le montre le tableau suivant.

Combinaisons prises en charge, unités avec cartes de contournement Ethernet							
Config.	**Inline**	**Virtuel Inline**	**WCCP-GRE**	**WCCP-L2**	**Multiple Bridges**	**High Avail.**	**Mode Group**
Plug-in Citrix SD-WAN WANOP	**O**	**O**	**O**	**O**	**O**	**O**	N
Inline	**O**	N	N	N	**O**	**O**	**O**
Virtuel Inline		**O**	**O**	**O**	**O**	**O**	N

Combinaisons prises en charge, unités avec cartes de con-tourne-ment Ethernet							
WCCP-GRE			**O**	**O**	**O**	**O**	N
WCCP-L2				**O**	**O**	**O**	N
Multiple Bridges					**O**	**O**	N
High Avail.						**O**	**O**
Combinaisons prises en charge, unités SANS cartes de con-tourne-ment Ethernet							
Config.	**Inline**	**Virtuel Inline**	**WCCP-GRE**	**WCCP-L2**	**Multiple Bridges**	**High Avail.**	**Mode Group**
Plug-in Citrix SD-WAN WANOP	N	N	N	N	N	N	N
Inline	**O**	N	N	N	N	N	N
Virtuel Inline		**O**	**O**	**O**	N	N	N

Combinaisons prises en charge, unités avec cartes de con-tourne-ment Ethernet					
WCCP-GRE	**O**	**O**	N	N	N
WCCP-L2		**O**	N	N	N
Multiple Bridges			N	N	**O**
High Avail.				N	N

O/Y = Oui, pris en charge. N = Non pris en charge.

Configurer le plug-in Citrix SD-WAN WANOP avec des VPN Access Gateway

April 9, 2021

Le VPN Access Gateway Standard Edition prend en charge l'accélération du plug-in Citrix SD-WAN WANOP, à condition qu'une appliance Citrix SD-WAN WANOP soit déployée avec l'appliance Access Gateway et que l'appliance Access Gateway soit configurée pour la prendre en charge.

Pour obtenir la prise en charge de Citrix SD-WAN WANOP Plug-in avec d'autres VPN, consultez la documentation de votre VPN ou contactez votre représentant Citrix.

Pour configurer la prise en charge de Citrix SD-WAN WANOP, utilisez l'outil d'administration Access Gateway, comme suit :

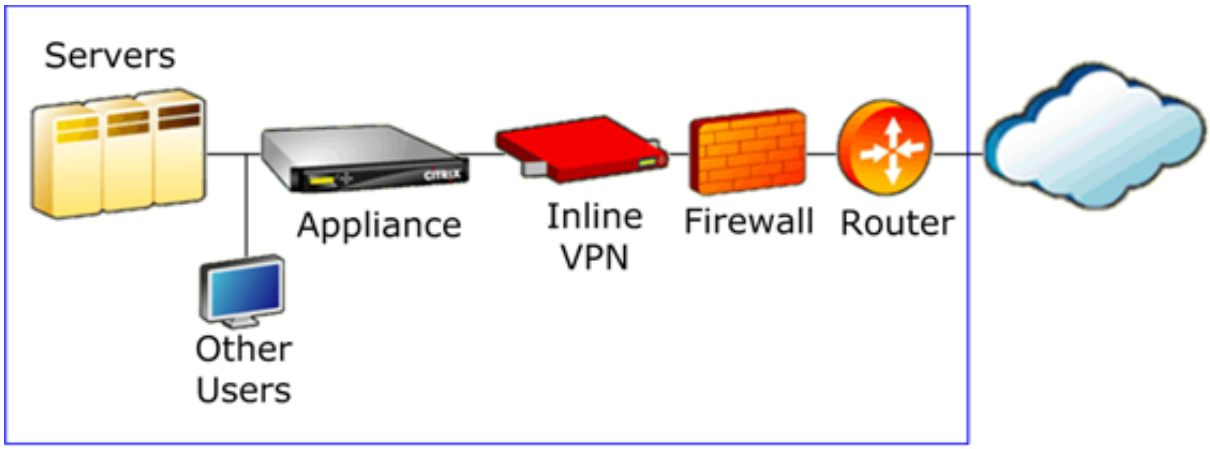
1. Dans la page Stratégies globales de cluster, sous Options avancées, **activez la case à cocher Activer l'optimisation TCP avec Citrix SD-WAN WANOP Plug-in**.

2. Assurez-vous que l'accès aux adresses IP utilisées par Citrix SD-WAN WANOP (adresse IP de redirecteur et adresse IP de gestion) est activé dans la section Ressources réseau de la page Gestionnaire de stratégies d'accès.
3. Pour chacune de ces adresses, activez tous les protocoles (TCP, UDP, ICMP) et activez Conserver les options TCP.
4. Assurez-vous que ces mêmes adresses sont incluses dans Groupes d'utilisateurs : Par défaut : Stratégies réseau dans la page Gestionnaire de stratégies d'accès.

Options de prise en charge VPN

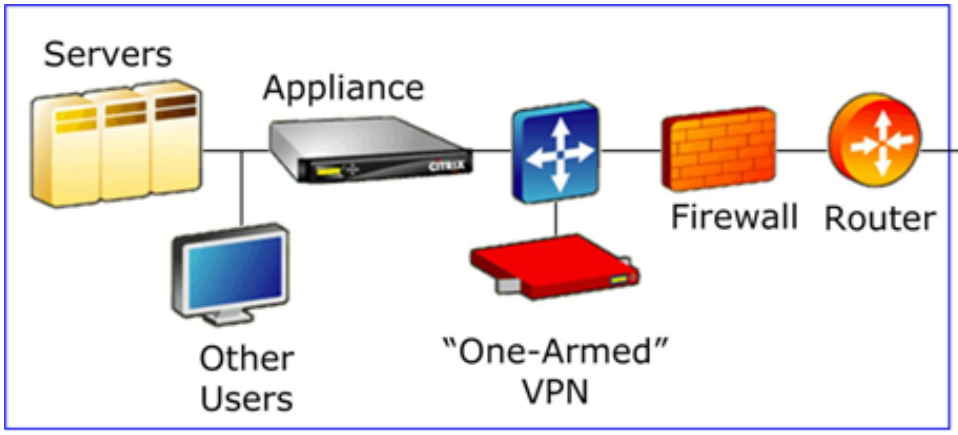
La prise en charge du VPN consiste simplement à placer l'appliance du côté LAN du VPN, comme le montre la figure suivante. Ce placement garantit que l'appliance reçoit et transmet la version décapsulée, déchiffrée et en texte brut du trafic de liaison, ce qui permet à la compression et à l'accélération de l'application de fonctionner. (L'accélération et la compression des applications n'ont aucun effet sur le trafic chiffré. Cependant, l'accélération du protocole TCP fonctionne sur le trafic crypté.)

Câblage VPN pour un VPN en ligne



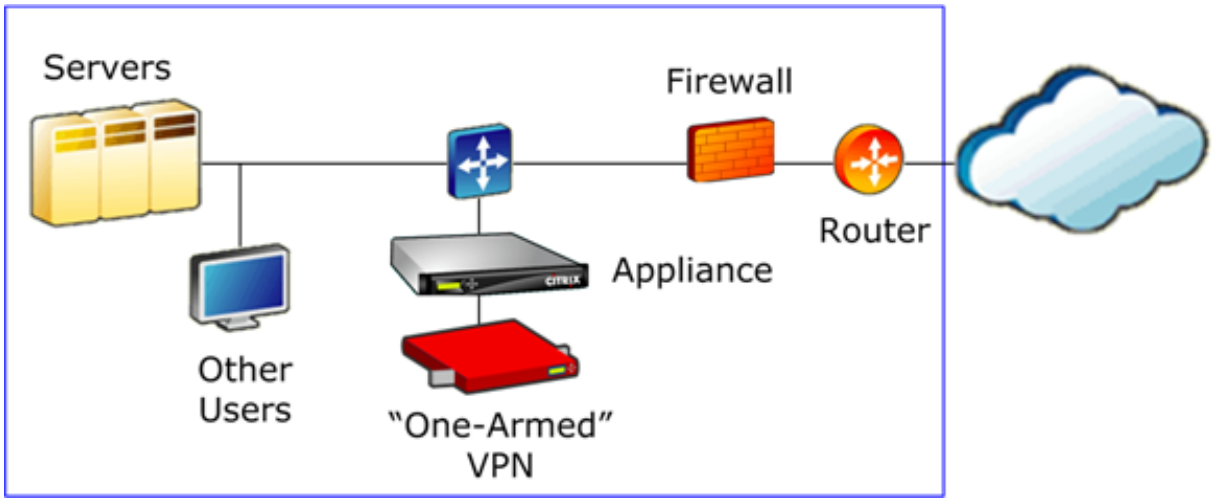
La figure suivante montre une option pour accélérer les VPN à un bras. L'appliance se trouve du côté serveur du VPN. Tout le trafic VPN avec une destination locale est accéléré. Le trafic VPN avec une destination distante n'est pas accéléré. Le trafic non-VPN peut également être accéléré.

Accélération VPN à un bras, option A



La figure suivante montre une autre option pour accélérer les VPN à un bras. L'appliance se trouve du côté serveur du VPN. Tout le trafic VPN avec une destination locale est accéléré. Le trafic VPN avec une destination distante n'est pas accéléré. Le trafic non-VPN peut également être accéléré.

Accélération VPN à un bras, Option B



> **Important**
>
> Pour que l'accélération soit efficace, le VPN doit conserver les options d'en-tête TCP. La plupart des VPN le font.

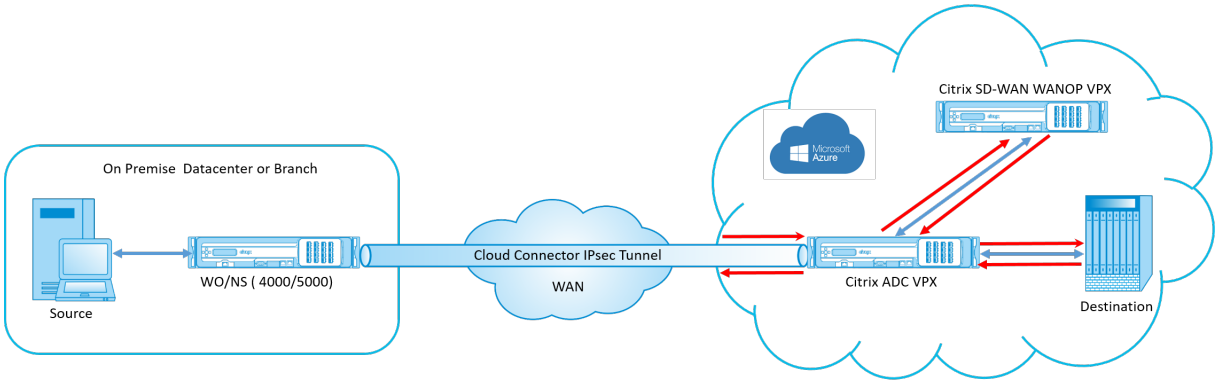
Déployer SD-WAN WANOP VPX sur Microsoft Azure

April 9, 2021

Citrix SD-WAN WANOP Edition est désormais disponible sur le marché Azure, ce qui permet d'optimiser le réseau étendu entre le datacenter/la succursale d'entreprise et le cloud Azure. Étant donné que la prise en charge du mode L2 n'est pas disponible sur les infrastructures cloud, vous ne pouvez

pas déployer Citrix SD-WAN WANOP en tant que VPX autonome dans Azure Cloud. Toutefois, vous pouvez déployer Citrix SD-WAN WANOP VPX avec Citrix ADC VPX dans l'infrastructure cloud Azure. Le Citrix ADC utilise un connecteur cloud pour créer un tunnel IPSec, tandis que le Citrix SD-WAN WANOP VPX accélère les connexions, offrant des performances de type LAN pour les applications.

Citrix SD-WAN WANOP dans la topologie du cloud Azure



Le diagramme topologique montre un Citrix SD-WAN 4000/5000 déployé dans les locaux du centre de données ou de la succursale. Vous pouvez également déployer Citrix SD-WAN WANOP et Citrix ADC en mode à deux boîtes ou il peut s'agir de VPX. Sur le VNET cloud Azure, le Citrix SD-WAN WANOP VPX est déployé en mode monobras (PBR) avec Citrix ADC VPX.

Vue d'ensemble du déploiement

Pour déployer SD-WAN WANOP sur Microsoft Azure :

1. Déployez une instance Citrix ADC VPX sur le cloud Azure. Pour de plus amples informations, consultez la section Déployer une instance de Citrix ADC VPX sur Microsoft Azure. Configurez quatre interfaces réseau dans quatre sous-réseaux différents et activez le transfert IP sur toutes les interfaces réseau. Les quatre interfaces réseau sont utilisées comme :
    - Interface de gestion
    - Interface WAN, pour tunnel IPSec
    - Interface côté LAN, pour se connecter au serveur
    - Interface de communication WANOP, pour communiquer avec le Citrix SD-WAN WANOP VPX sur le cloud Azure.
2. Déployez un Citrix SD-WAN WANOP VPX sur le cloud Azure. Pour plus d'informations, consultez la procédure de déploiement ci-dessous.

> **Remarque** : Activez le transfert IP sur l'interface WANOP.

3. Configurez un tunnel IPSec entre l'appliance sur site et Citrix ADC VPX sur le cloud Azure, à l'aide de l'adresse IP publique de l'interface WAN Citrix ADC. Pour plus d'informations sur la configuration des tunnels IP, consultez,Tunnels IP.
4. Configurez Citrix ADC VPX pour rediriger les paquets vers Citrix SD-WAN WANOP VPX. Utilisez l'adresse IP privée de l'interface de communication WANOP et créez un serveur virtuel d'équilibrage de charge. Pour de plus amples informations, consultez la section Créer un serveur virtuel d'équilibrage de charge.
5. Configurez les tables de routage suivantes sur Azure :
    - Table de routage pour l'interface WANOP sur Citrix ADC VPX —Les entrées de table de routage doivent avoir une adresse source et de destination en tant que sous-réseaux client et serveur respectivement. L'adresse IP de l'interface WANOP de Citrix ADC VPX est le saut suivant.
    - Table de routage pour l'interface Citrix SD-WAN WANOP - Les entrées de table de routage doivent avoir une adresse source et une adresse de destination en tant que sous-réseaux client et serveur respectivement. L'adresse IP de l'interface WANOP SD-WAN de Citrix est le saut suivant.

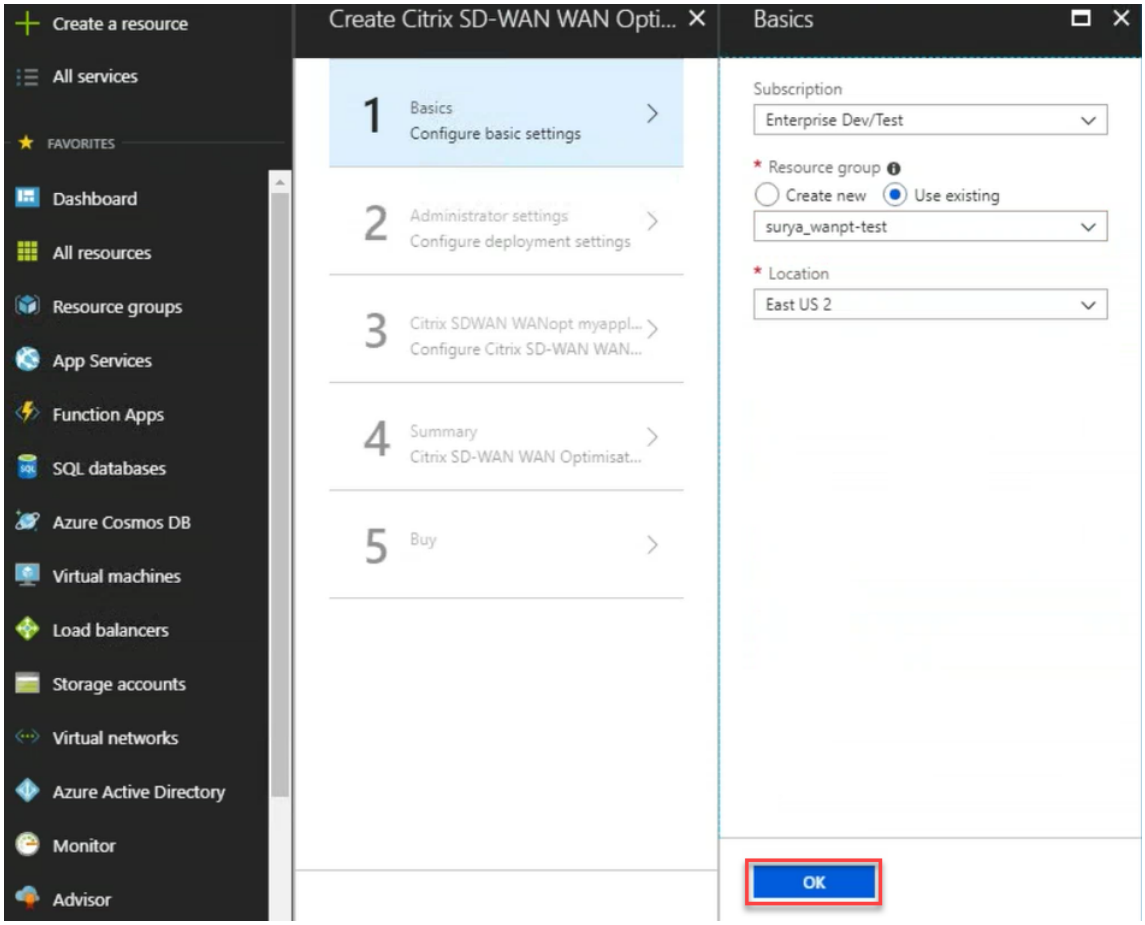
Dans l'exemple ci-dessus, lorsque la source tente d'accéder à une application sur la destination du cloud, les paquets passent par le tunnel IPsec établi. À l'extrémité VNET du cloud Azure, le Citrix ADC VPX reçoit les paquets, les déchiffre et les transmet au Citrix SD-WAN WANOP VPX. Le Citrix SD-WAN WANOP VPX traite les paquets, les optimise et les renvoie à Citrix ADC VPX. Le Citrix ADC VPX envoie le paquet à la destination. Sur le chemin de retour, le Citrix ADC VPX transfère les paquets à Citrix SD-WAN WANOP VPX pour optimisation. Les paquets optimisés sont transmis à la source via le tunnel IPsec établi.

Déployer Citrix SD-WAN WANOP VPX sur Microsoft Azure

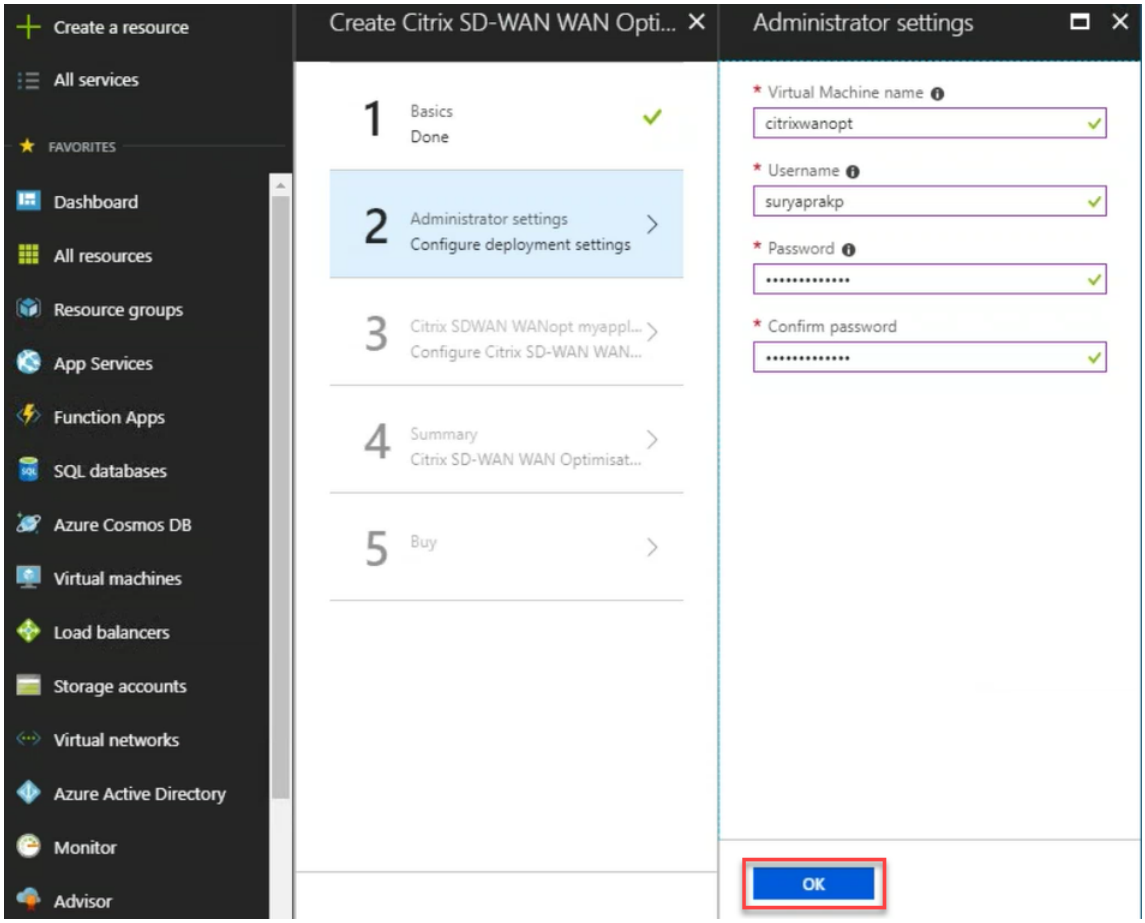
Pour déployer Citrix SD-WAN WANOP VPX sur Microsoft Azure :

1. Dans Microsoft Azure, accédez à **Accueil** > **Marketplace** > **Mise en réseau**, recherchez **Citrix SD-WAN WANOP** et installez-le.
2. Sur la page OP de réseau étendu SD-WAN Citrix, dans la liste déroulante, sélectionnez **Gestionnaire de ressources** et cliquez sur **Créer**. La page **Créer Citrix SD-WAN Optimization** s'affiche.
3. Dans la section **Bases**, sélectionnez le type d'abonnement, le groupe de ressources et l'emplacement. Cliquez sur OK.

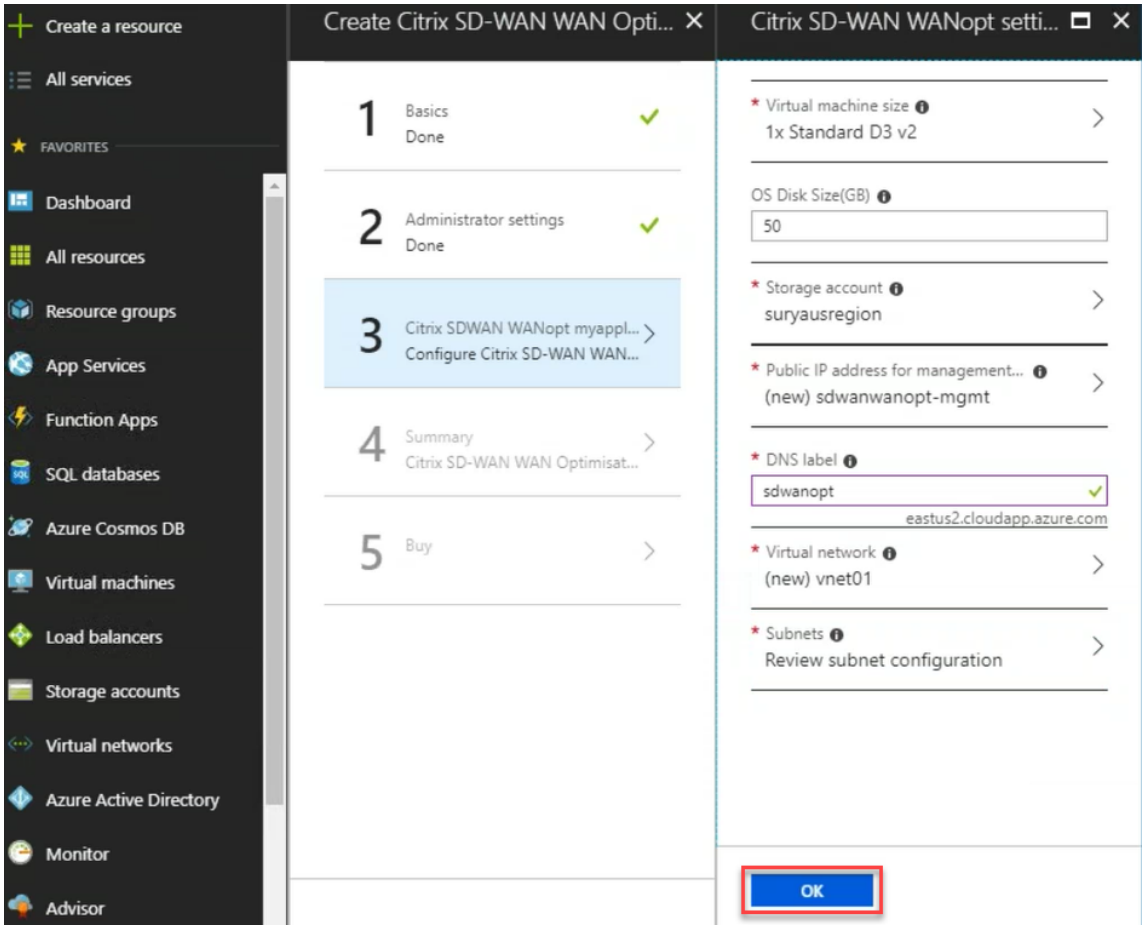
> **Remarque** :
>
> Vous pouvez choisir de créer un groupe de ressources. Un groupe de ressources est un conteneur qui contient des ressources associées pour une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe.



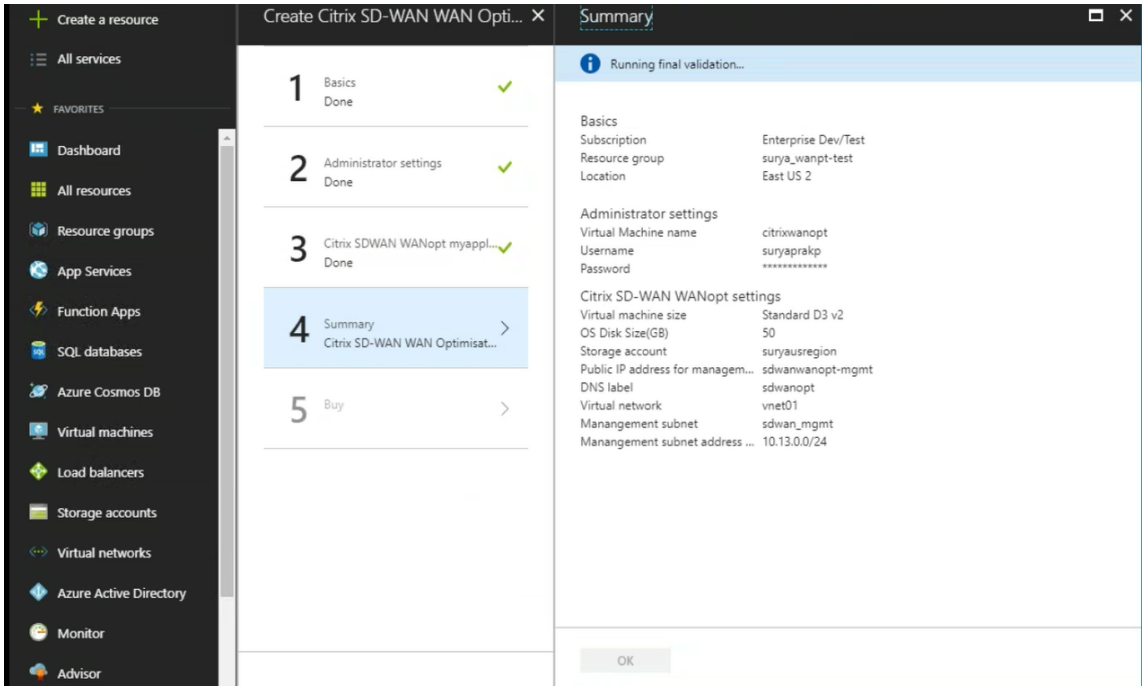
4. Dans la section **Administrateur**, entrez le nom et les informations d'identification de la machine virtuelle Citrix SD-WAN WANOP. Cliquez sur **OK**.



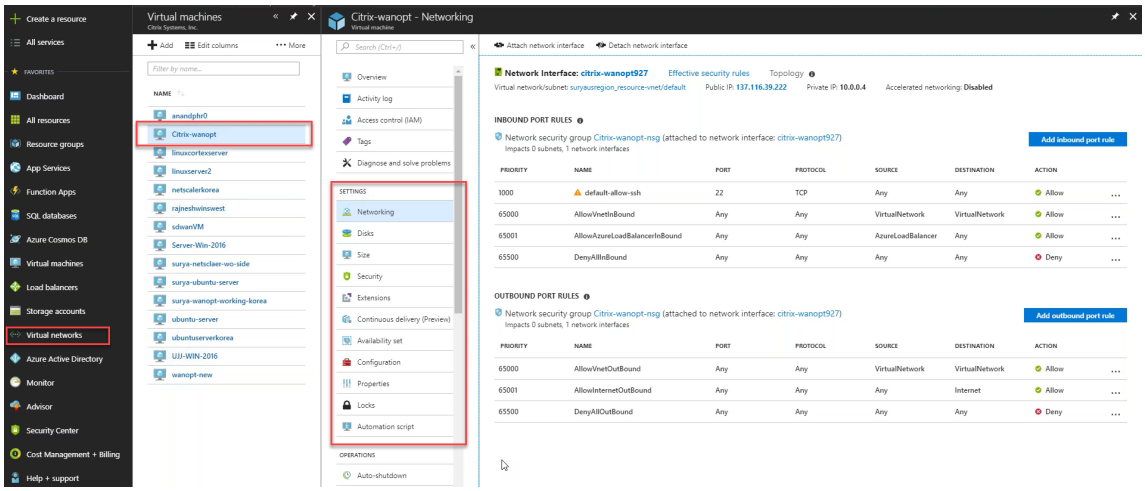
5. Dans la **section Paramètres Citrix SD-WAN WANOP**, configurez le paramètre pour Citrix SD-WAN WANOP VPX conformément à vos exigences. Cliquez sur **OK**.



6. La configuration que vous avez fournie lors des étapes précédentes est validée et appliquée. Si vous avez configuré correctement, le message de validation passé s'affiche. Cliquez sur **OK**.



7. Après le déploiement réussi, accédez à **Virtual Networks** pour afficher le Citrix SD-WAN WANOP VPX. Vous pouvez configurer davantage les paramètres de la machine virtuelle à l'aide de l'option Paramètres.



Procédure de mise à niveau de SD-WAN WANOP

December 14, 2022

Cette section fournit des informations sur le téléchargement et la mise à niveau des packages logiciels Citrix SD-WAN WAN Optimization (WANOP).

> **Remarque** :
>
> Avant de télécharger le logiciel, vous devez obtenir et enregistrer une licence de logiciel Citrix SD-WAN. Pour plus d'informations, consultez l'article Licences.

Télécharger les progiciels

Pour télécharger les packages logiciels Citrix SD-WAN WANOP, accédez à l'URL ; téléchargements de produits. Les instructions pour télécharger le logiciel sont fournies sur ce site.

Pour télécharger le package logiciel Citrix SD-WAN WANOP :

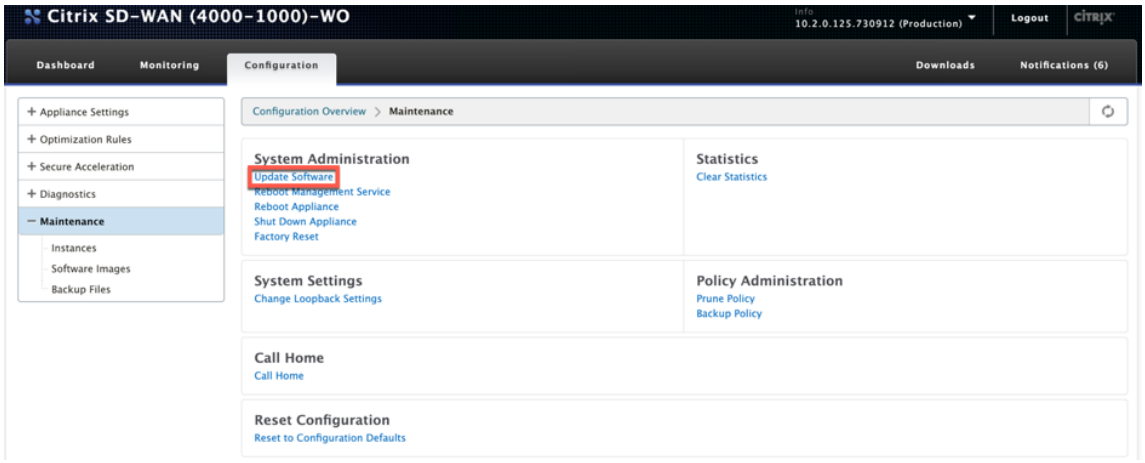
1. Connectez-vous à citrix.com à l'aide de vos informations d'identification.
2. Accédez à la page Téléchargements et sélectionnez le produit (Citrix SD-WAN) dans la liste déroulante.
3. Développez l'**édition Citrix SD-WAN WANOP** et sélectionnez la version logicielle requise.
4. Les options de téléchargement suivantes sont disponibles. Téléchargez le logiciel requis.
    - Téléchargez le fichier de mise à niveau .upg pour les appliances SD-WAN WANOP 4100/5100.
    - Téléchargez le fichier de mise à niveau .bin pour les appliances SD-WAN WANOP VPX.

Pour plus d'informations sur les plateformes prises en charge par le SD-WAN WANOP, consultez les modèles de plateformes SD-WAN et les packages logiciels.

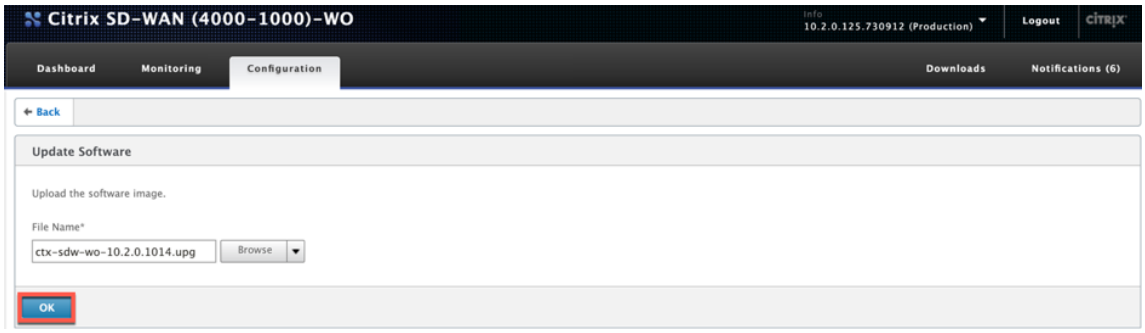
Procédure de mise à niveau

Pour mettre à jour le logiciel, procédez comme suit :

1. Accédez à **Configuration > Maintenance > Administration du système**, puis cliquez sur **Mettre à jour le logiciel**.

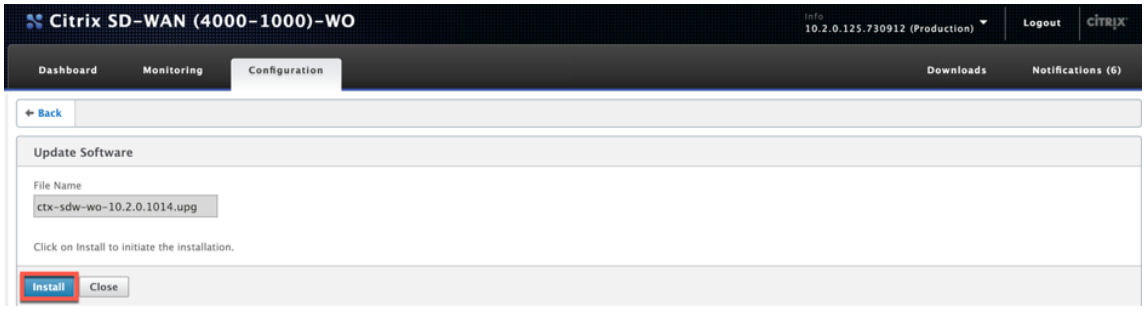


2. Cliquez sur **Parcourir** pour fournir le fichier **ctx-SDW-WO-10.2.x.upg** . Cliquez sur **OK**.



Vous pouvez voir la barre d'état du téléchargement.

3. Lorsqu'un message annonce la réussite du téléchargement, cliquez sur **Installer**.



4. L'appliance effectue la mise à niveau, qui prend de 10 à 40 minutes selon le modèle de plate-forme. Il affiche une série de messages d'état, commençant par **Préparation à la mise à niveau** et se terminant par **Mise à niveau terminée avec succès**.
5. Cliquez sur **OK** pour afficher l'interface utilisateur mise à jour.

Configuration initiale

April 9, 2021

Après avoir vérifié les connexions, vous êtes prêt à déployer les appliances SD-WAN sur le réseau.

Les adresses IP par défaut de l'appliance expédiée à partir de Citrix sont configurées. Pour déployer l'appliance sur le réseau, vous devez configurer les adresses IP appropriées sur l'appliance afin d'

accélérer le trafic réseau.

La configuration initiale comprend les tâches suivantes :

- Identifiez les conditions préalables à la configuration initiale.
- Enregistrez les différentes valeurs requises dans la procédure de configuration initiale.
- Configurez l'appliance en la connectant au port Ethernet.
- Attribuez l'adresse IP de gestion via la console série.

Par défaut, la configuration initiale déploie l'appliance en mode Inline.

Conditions préalables

April 9, 2021

Pour déployer une appliance Citrix SD-WAN 4100 ou 5100, vous devez effectuer la configuration préalable suivante avant de la configurer.

Versions logicielles

Ce document traite de la publication du logiciel SD-WAN. Voir les notes de version pour les versions recommandées du logiciel NetScaler correspondant à la version souhaitée du logiciel SD-WAN. N' utilisez jamais d'autres versions que celles recommandées pour les appareils SD-WAN 4100 et 5100.

Fichier de licences

Le nombre d'appliances accélérateur dépend de la plate-forme matérielle et du type de licence que vous appliquez à l'appliance. La liste suivante affiche le nombre d'accélérateurs qui sont provisionnés automatiquement par l'Assistant Configuration :

- Modèle 310 : Deux
- Modèle 500 : Trois
- Modèles 1000 et 1500 : Six
- Modèle 2000 : Huit

Avant de commencer à provisionner l'appliance, Citrix vous recommande d'avoir le fichier de licence avec vous, car cela est nécessaire au début du processus de configuration Pour télécharger un fichier de licence, suivez la procédure décrite dans le Guide de l'utilisateur de My Account All Licensing Tools - My Account All Licensing Tools.

Installation du matériel

Après avoir reçu l'appliance matérielle de Citrix, vous devez l'installer sur le réseau. Pour installer le matériel SD-WAN 4100/5100, suivez la procédure d'installation à l'adresseInstallation du matériel.

Fiche de déploiement

April 9, 2021

> **Remarque**
>
> Utilisez cette feuille de calcul uniquement lorsque vous provisionnez une appliance de réinitialisation d'usine à l'aide de l'assistant de configuration version 9.3. Si vous mettez simplement à niveau un système précédemment configuré vers la version 9.3, votre appliance conserve sa configuration précédente, qui sera différente.

L'appliance utilise au moins deux ports : le port de gestion (généralement 0/1) et le port de trafic (comme 10/1). Le mode Inline utilise des ports de trafic par paires, tels que les ports 10/1 et 10/2. Les ports doivent être sélectionnés à l'avance, car la configuration dépend de leur identité.

L'appliance utilise directement trois sous-réseaux : le sous-réseau de gestion, le sous-réseau de trafic externe et le sous-réseau de trafic interne. Plusieurs adresses IP sont utilisées sur chaque sous-réseau. Chaque sous-réseau doit être spécifié avec le masque de sous-réseau correct.

La figure suivante est une feuille de calcul pour ces paramètres. Il prend en charge les modes en ligne et WCCP, avec et sans haute disponibilité. Le tableau ci-dessous décrit ce que chaque entrée signifie.

Tableau 1.Paramètres de la fiche de déploiement

	Paramètre	Exemple	Votre valeur	Description
Sous-réseau de gestion				
M2.	Adresse IP de la passerelle	10.199.79.254		Gateway par défaut desservant le sous-réseau de gestion.

	Paramètre	Exemple	Votre valeur	Description
M3.	Masque de sous-réseau	255.255.255.128		Masque de sous-réseau pour le sous-réseau de gestion.
M4.	Adresse IP de l'hyperviseur Xen	10.199.79.225		Adresse IP de l'hyperviseur Xen.
M5.	Adresse IP de la machine virtuelle de service	10.199.79.226		Adresse IP de la machine virtuelle Management Service, qui contrôle la configuration.
M6.	Interface utilisateur de l'accélérateur	10.199.79.227		L'interface graphique de l'accélérateur, également appelée interface utilisateur Broker, qui gère les instances en tant qu'unité.
M7.	Adresse IP de NetScaler Management	10.199.79.245		Adresse IP des interfaces GUI et CLI de l'instance NetScaler.
Sous-réseau de trafic externe				
T1.	Adresse IP du routeur	172.17.17.1		Adresse IP du routeur sur le sous-réseau de trafic externe.
T2.	Masque de sous-réseau	255.255.255.0		Masque de sous-réseau du sous-réseau de trafic externe.

	Paramètre	Exemple	Votre valeur	Description
T3.	Adresse IP de NetScaler	172.17.17.2		Adresse IP NetScaler sur le sous-réseau de trafic externe.
T4.	Adresse IP de signalisation externe	172.17.17.10		Le trafic vers cette adresse IP est équilibré entre les adresses IP de signalisation des accélérateurs.
T5.	Adresse IP WCCP externe #1	172.17.17.11		Cartes par NAT à WCCP VIP sur l'accélérateur #1.
T6.	Adresse IP WCCP externe #2	172.17.17.12		Cartes par NAT à WCCP VIP sur l'accélérateur #2.
T7.	Sous-réseaux LAN locaux	10.200.0.0/16		Sous-réseau LAN local à accélérer. C'est le seul sous-réseau qui reçoit une accélération.
T8.	ID d'hôte du routeur GRE	SO		WCCP-GRE uniquement. ID hôte du routeur GRE.
T9.	Port de trafic	10/1		Port utilisé pour le trafic accéléré.
T10+.	(en ligne) plus Port de trafic			Autre port de trafic en paire.

	Paramètre	Exemple	Votre valeur	Description
T11, T12	(WCCP) Groupes de services : TCP, UDP	71, 72		Groupes de services utilisés par l'accélérateur #1 pour WCCP. La première concerne le trafic TCP, la seconde est pour UDP.
T13, T14	(Non utilisé)			
T15, T16	Ports (Inline) utilisés par link #2	10/5, 10/6		Si plusieurs liens sont utilisés avec le mode Inline, ces ports sont utilisés pour le lien #2.
T17, T18	Ports (Inline) utilisés par link #3	10/7, 10/8		Si plusieurs liens sont utilisés avec le mode Inline, ces ports sont utilisés pour le lien #3.
VLAN1.1, VLAN1.2, VLAN1.3, VLAN1.4	VLAN externes pour Bridge #1	412		Lorsque le trunking de VLAN est utilisé, ceux-ci sont taggés VLAN traversant le pont #1.
VLAN2.1, VLAN2.2, VLAN2.3, VLAN2.4				Lorsque le trunking de VLAN est utilisé, ceux-ci sont taggés VLAN traversant le pont #2.

	Paramètre	Exemple	Votre valeur	Description
VLAN3.1, VLAN3.2, VLAN3.3, VLAN3.4	VLAN externes pour Bridge #1			Lorsque le trunking de VLAN est utilisé, ceux-ci sont taggés VLAN traversant le pont #3.

Configuration de l'appliance

April 9, 2021

Avant de commencer à configurer l'appliance, vous devez modifier l'adresse IP du service de gestion par celle de votre réseau de gestion, afin que vous puissiez accéder à l'appliance via le réseau. Vous pouvez modifier l'adresse IP de gestion en connectant un ordinateur à l'appliance via le port Ethernet ou la console série.

Affectation d'une adresse IP de gestion via le port Ethernet

April 9, 2021

Suivez la procédure suivante pour la configuration initiale de chaque appliance SD-WAN 1000 ou 2000 avec Windows Server. La procédure exécute les tâches suivantes :

- Configurez l'appliance pour une utilisation sur votre site.
- Installez la licence Citrix.
- Activer l'accélération.
- Activer le traffic shaping (mode Inline uniquement).

Avec les déploiements en ligne, cette configuration peut être tout ce dont vous avez besoin, car la plupart des fonctionnalités d'accélération sont activées par défaut et ne nécessitent aucune configuration supplémentaire.

Si vous souhaitez configurer l'appliance en la connectant à l'ordinateur via la console série, affectez l'adresse IP du service de gestion à partir de votre feuille de calcul en effectuant laAffectation d'une adresse IP de gestion via la console sérieprocédure, puis exécutez étapes 4 à 15 de la procédure suivante.

> **Remarque** :
>
> Vous devez avoir un accès physique à l'appliance.

Pour configurer l'appliance en connectant un ordinateur au port Ethernet 0/1 de l'appliance SD-WAN

1. Définissez l'adresse du port Ethernet d'un ordinateur (ou d'un autre périphérique équipé d'un navigateur doté d'un port Ethernet) sur 192.168.100.50, avec un masque réseau de 255.255.0.0. Sur un périphérique Windows, cela se fait en modifiant les propriétés Internet Protocol Version 4 de la connexion LAN, comme indiqué ci-dessous. Vous pouvez laisser les champs de Gateway et de serveur DNS vides.

2. À l'aide d'un câble Ethernet, connectez cet ordinateur au port PRI de l'appliance SD-WAN.
3. Allumez l'appliance. À l'aide du navigateur Web de l'ordinateur, accédez à l'appliance à l'aide de l'adresse IP du service de gestion par défaut, qui est http://192.168.100.1.
4. Sur la page de connexion, utilisez les informations d'identification par défaut suivantes pour vous connecter à l'appliance :

- **Nom d'utilisateur** : nsroot
- **Mot de passe** : nsroot

1. Démarrez l'assistant de configuration en cliquant sur **Démarrer**.
2. Dans la page **Configuration de la plate-forme**, saisissez les valeurs respectives de votre feuille de calcul, comme illustré dans l'exemple suivant :

3. Cliquez sur **Terminé**. Un écran affichant le message Installation en cours…s'affiche. Ce processus prend environ 2 à 5 minutes, selon la vitesse de votre réseau.
4. Un message IP Redirection vers un nouveau système de gestion s'affiche.
5. Cliquez sur **OK**.
6. Débranchez votre ordinateur du port Ethernet et connectez le port à votre réseau de gestion.
7. Réinitialisez l'adresse IP de votre ordinateur à son paramètre précédent.
8. À partir d'un ordinateur du réseau de gestion, connectez-vous à l'appliance en entrant la nouvelle adresse IP du service de gestion, par exemple`https://<Managemnt_IP_Address>`, dans un navigateur Web.
9. Pour poursuivre la configuration, acceptez le certificat et continuez. L'option de continuer varie en fonction du navigateur Web que vous utilisez.
10. Connectez-vous à l'appliance à l'aide du nom d'utilisateur **nsroot** et du mot de passe de votre feuille de calcul.
11. Pour terminer le processus de configuration, reportez-vous à la section Provisionnement de l'appliance.

Affectation d'une adresse IP de gestion via le port série

April 9, 2021

Si vous ne souhaitez pas modifier les paramètres de votre ordinateur, vous pouvez configurer l'appliance en le connectant à votre ordinateur à l'aide d'un câble de modem série null. Vous devez disposer d'un accès physique à l'appliance.

Pour configurer l'appliance via la console série

1. Connectez un câble série null modem au port console de l'appliance.
2. Connectez l'autre extrémité du câble au port COM série d'un ordinateur exécutant un émulateur de terminal, tel que Microsoft HyperTerminal, avec les paramètres 9600, N,8,1, p.
3. Dans la sortie HyperTerminal, appuyez sur **Entrée**. L'écran du terminal affiche l'invite d'ouverture de session. **Remarque** : vous devrez peut-être appuyer deux ou trois fois sur **Entrée**, selon le programme terminal que vous utilisez.
4. À l'invite d'ouverture de session, connectez-vous à l'appliance avec les informations d'identification par défaut suivantes :

- **Nom d'utilisateur** : nsroot
- **Mot de passe** : nsroot

1. À l'invite **$**, exécutez la commande suivante pour passer à l'invite shell de l'appliance :`$ ssh 169.254.0.10`
2. Entrez **Oui** pour continuer à vous connecter au service de gestion.
3. Connectez-vous à l'invite de shell de l'appliance avec les informations d'identification par défaut suivantes :
   Mot de passe : nsroot.
4. À l'invite d'ouverture de session, exécutez la commande suivante pour ouvrir le menu Configuration initiale de l'adresse réseau du service de gestion :`# networkconfig`
5. Tapez **1** et appuyez sur **Entrée** pour sélectionner l'option 1 et spécifiez une nouvelle adresse IP de gestion pour le service de gestion.
6. Tapez **2** et appuyez sur **Entrée** pour sélectionner l'option 2 et spécifiez une nouvelle adresse IP de gestion pour Citrix Hypervisor.
7. Tapez **3** et appuyez sur **Entrée** pour sélectionner l'option 3, puis spécifiez le masque réseau pour les adresses IP.
8. Tapez **4** et appuyez sur **Entrée** pour sélectionner l'option 4, puis spécifiez la Gateway par défaut pour l'adresse IP du service de gestion.
9. Tapez **8** et appuyez sur **Entrée** pour enregistrer les paramètres et quitter.

10. Accédez à l'appliance SD-WAN en saisissant la nouvelle adresse IP du service de gestion de l'appliance`https://<Management_Service_IP_Address>`, par exemple dans un navigateur Web d'un ordinateur du réseau de gestion.
11. Pour poursuivre la configuration, acceptez le certificat et continuez. L'option de continuer varie en fonction du navigateur Web que vous utilisez.
12. Pour terminer le processus de configuration, reportez-vous à la section Provisionnement de l'appliance.

Provisionnement de l'appliance

April 9, 2021

Après avoir attribué une adresse IP au service de gestion, vous êtes prêt à provisionner les instances NetScaler et d'accélérateur. Lorsque vous ouvrez une session sur l'appliance, l'assistant de configuration apparaît.

Lorsque vous utilisez l'assistant de configuration, gardez à l'esprit les points suivants :

- La procédure suivante suppose que vous avez déjà rempli la feuille de calcul de configuration.
- Si vous modifiez les adresses IP du réseau de gestion ou si vous modifiez la Gateway par défaut en une adresse qui ne se trouve pas sur le réseau de gestion, vous perdez la connectivité à l'appliance, sauf si vous êtes sur le même segment Ethernet que le port de gestion.
- Lorsque vous utilisez l'assistant de configuration, vérifiez attentivement vos entrées. L'Assistant n'a pas de bouton Précédent. Si vous devez modifier l'écran précédent, utilisez le bouton **Précédent** de votre navigateur. Cela vous amène à la page d'ouverture de session, puis à l'écran précédent.
- L'assistant de configuration s'affiche uniquement lorsque vous vous connectez à l'appliance pour la première fois pour la configurer. Une fois la configuration terminée, cet Assistant devient inaccessible et ne réapparaîtra qu'après une réinitialisation d'usine. Vérifiez attentivement vos entrées.

Cet assistant vous guide dans une nouvelle configuration de l'appliance.

> **Note** :
>
> Si vous recevez une erreur #SESS_CORRUPTED à tout moment au cours de ces procédures, cliquez sur
> **Se déconnecter**, vider le cache de votre navigateur, fermez votre navigateur et ouvrez-le à nouveau.

Pour configurer l'appliance à l'aide de l'assistant de configuration :

1. Sur la page Bienvenue, cliquez sur **Démarrer**.

   > **Note** :
   >
   > Toutes les pages qui suivent la page Mise en route comportent un en-tête indiquant « Mode de déploiement : mode inline/L2 », mais cet Assistant est utilisé pour tous les modes de déploiement.

2. Procédez comme suit pour configurer un système entièrement conforme à la norme 7.3 :

   - Acquérir les distributions de logiciels de version 7.3 suivantes à partir de la page de téléchargement de version 7.3 sur My Citrix :
     - Service de gestion (sous forme de fichier .tgz)
     - VM NetScaler (sous forme de fichier .xva)
     - Machine virtuelle de l'accélérateur (sous forme de fichier .xva)
     - Mettre à niveau le bundle (en tant que fichier .upg)
   - Accédez à la page **Système > Configuration > Service de gestion > Images logicielles**, puis sélectionnez **Télécharger** dans la liste Action.
   - Téléchargez une image du service de gestion version 7.3 (distribuée sous la forme d'un fichier .tgz).
   - Accédez à la page **Système > Configuration > NetScaler \ > Images logicielles**, puis téléchargez une image NetScaler XVA version 7.3.
   - Accédez à la page **Système > Configuration > SD-WAN > Images logicielles**, puis téléchargez l'image XVA de l'accélérateur.
   - Accédez à la page **Système > Configuration > Service de gestion**, puis cliquez sur le lien **Service de gestion de mise à niveau**.
   - Sélectionnez l'image du service de gestion que vous avez récemment chargée et cliquez sur **OK**.
   - Lorsque le coin inférieur gauche de l'écran affiche « Service de gestion mis à jour avec succès », déconnectez-vous et effacez le cache de votre navigateur. Ouvrez une session après le redémarrage du service de gestion (quelques minutes).
   - Dans l'écran de **bienvenue**, cliquez sur **Démarrer**.

3. Pour Paramètres d'accès à la gestion, spécifiez des valeurs pour les différents champs en fonction des paramètres réseau. La capture d'écran suivante affiche des exemples de valeurs utilisées dans cette documentation. Entrez les valeurs comme suit :

   - **Adresse IP Citrix Hypervisor**—(élément M4 de votre feuille de calcul, ou H4 s'il s'agit de la deuxième appliance d'une paire de haute disponibilité.) Adresse de gestion de l'hyperviseur Citrix Hypervisor intégré. Il doit s'agir d'une adresse valide sur le réseau de gestion.

- **Adresse IP du service de gestion** : (Article M5 de votre feuille de calcul, ou H5 s'il s'agit de la deuxième appliance d'une paire haute disponibilité). Adresse de la machine virtuelle de service de gestion que vous utilisez pour effectuer la plupart des tâches de gestion du système. Il doit s'agir d'une adresse valide sur le réseau de gestion.
- **Masque réseau**—(élément M3 de votre feuille de calcul). Masque de sous-réseau du réseau de gestion.
- **Passerelle**—(Article M2 sur votre feuille de calcul). Gateway par défaut du réseau de gestion.
- **Serveur DNS**—Adresse IP du serveur DNS. Il s'agit d'un paramètre obligatoire.
- **Serveur NTP** : adresse IP ou FQDN de votre serveur de temps. Cela sera utilisé par toutes les machines virtuelles de l'appliance. > **Notez** que si vous utilisez une accélération CIFS ou MAPI avancée, l'heure système de l'appliance doit être proche de celle du serveur de domaine Windows. Choisissez donc un serveur NTP qui maintient une relation étroite avec l'heure sur votre Windows. serveur de domaine.

  > **Note** :
  >
  > Sauf si le serveur NTP est spécifié en tant qu'adresse IP, il n'est pas utilisé par l'accélérateur.

- **Fuseau horaire**—Sélectionnez votre fuseau horaire dans le menu déroulant.
- **Changer le mot de passe**—Activez cette case à cocher et tapez deux fois un nouveau mot de passe nsroot pour modifier le mot de passe. Ce même mot de passe est utilisé sur le service de gestion et l'instance NetScaler pour le compte nsroot, et sur l'accélérateur pour le compte admin. Si le mot de passe n'est pas modifié, il reste défini sur nsroot (valeur par défaut).
  Figure 1.Exemples de valeurs pour les champs de la page Paramètres d'accès à la gestion de la configuration

4. Vérifiez vos paramètres et cliquez sur **Continuer**.
5. Dans la section **Gérer les licences**, voir si une licence appropriée est déjà répertoriée dans le champ **Nom**. Si c'est le cas, sélectionnez-le et passez à l'étape 8.
6. Cliquez sur **Télécharger** dans la section **Mettre à jour les licences**.
7. Accédez au dossier contenant le fichier de licence et ouvrez le fichier.
8. Cliquez sur **Ajouter une licence** et téléchargez le fichier de licence fourni par Citrix. La licence est ajoutée à l'appliance, comme illustré dans la figure suivante.
   Figure 2. Exemple de licence ajouté à l'appliance sur la page Gérer les fichiers de licence de l'

Assistant Configuration

Vous pouvez également obtenir un fichier de licence à partir du site Web Citrix.com en cliquant sur le bouton **ici** et en utilisant vos informations d'identification My Citrix.

9. Sélectionnez la licence dans le champ **Nom** et cliquez sur **Continuer**. La page Configuration du SD-WAN s'affiche. Remplissez les champs comme suit :

   a) **Paramètres réseau** : cette section informe les accélérateurs du réseau de gestion.

      - **Adresse IP SD-WAN Accelerator** : saisissez la valeur de M6 dans votre feuille de calcul. Ceci est l'adresse IP de l'accélérateur
      - **Adresse IP NetScaler** : entrez la valeur de M7 dans votre feuille de calcul. Il s'agit de l'adresse IP de l'interface graphique de NetScaler.
      - **Utiliser le masque réseau et la Gateway système** : sélectionnez cette option si vous souhaitez utiliser le masque réseau et les adresses IP de passerelle que vous avez spécifiées dans la page Configuration de la plate-forme.
      - **Masque réseau** : saisissez la valeur M3 dans votre feuille de calcul. Il s'agit du masque de sous-réseau (masque de réseau) du réseau de gestion (notez que vous l'avez déjà entré, sur une page précédente).
      - **Gateway**—Saisissez à nouveau la valeur M2 de votre feuille de calcul.
      - **Signalisation IP Address** : saisissez la valeur T4 dans votre feuille de calcul. Il s'agit de l'adresse IP de signalisation externe de l'accélérateur, utilisée par les plug-ins SD-WAN pour se connecter à l'appliance.
      - **Masque de réseau de signalisation** : saisissez la valeur de T2 dans votre feuille de calcul. Il s'agit du masque de sous-réseau (masque de réseau) du réseau de trafic externe.

   b) **Fichiers XVA**—Cette section vous permet de spécifier les fichiers XVA précédemment téléchargés (machines virtuelles Xen) pour les instances NetScaler et d'accélérateur. Sélectionnez les images XVA que vous avez téléchargées dans le cadre de l'étape 2.
   Figure 3. Page Configuration du SD-WAN

10. Cliquez sur **Continuer**. L'Assistant commence à Provisioning les instances requises, comme illustré dans la figure suivante.
    Figure 4. Indicateur
    de progression du provisionnement

11. Une fois les instances configurées, ajoutez l'un de vos sous-réseaux LAN locaux à la section **Configuration des liens** de la liste T7 de votre feuille de calcul, comme illustré dans la figure suivante. Ce sous-réseau est ajouté en tant que sous-réseau LAN local dans l'accélérateur. Si vous disposez de plusieurs sous-réseaux LAN, vous pouvez les ajouter à la définition de **lien LAN** dans l'interface graphique de l'accélérateur une fois l'assistant de configuration terminé.

Cliquez sur **Ajouter** pour ajouter le sous-réseau.
Figure 5. La configuration du lien se trouve au bas de cette page

12. Déconnectez-vous, puis reconnectez-vous. Si vous voyez un message « Incompatibilité de version détectée », installez le bundle de mise à niveau que vous avez téléchargé à l'étape 2.

La configuration de base est terminée. Ensuite, effectuez une configuration spécifique au mode de déploiement (par exemple pour le mode WCCP).

> **Note** :
>
> Une fois l'Assistant terminé, l'appliance est configurée pour la configuration de base. Pour configurer l'appliance pour un scénario de déploiement spécifique, reportez-vous à la section Modes de déploiement.

Modes de déploiement

April 9, 2021

Une appliance SD-WAN agit comme une Gateway virtuelle. Ce n'est ni un point de terminaison TCP ni un routeur. Comme n'importe quelle Gateway, son travail consiste à mettre en mémoire tampon les paquets entrants et à les placer sur le lien sortant à la bonne vitesse. Ce transfert de paquets peut se faire de différentes manières, telles que le mode Inline, le mode Inline virtuel et le mode WCCP. Bien que ces méthodes soient appelées *modes*, vous n'avez pas à désactiver un mode de transfert pour en activer un autre. Si votre déploiement prend en charge plusieurs modes, le mode utilisé par l'appliance est déterminé automatiquement par le format Ethernet et IP de chaque paquet.

Étant donné que l'appliance prend en charge différents modes de transfert et différents types de connexions non transférées, elle a besoin d'un moyen de distinguer un type de trafic d'un autre. Il le fait en examinant l'adresse IP de destination et l'adresse Ethernet de destination (adresse MAC), comme indiqué dans le tableau ci-dessous. Par exemple, en mode Inline, l'appliance agit comme un pont. Contrairement à d'autres types de trafic, les paquets pontés sont adressés à un système au-delà de l'appliance, et non à l'appliance elle-même. Les champs d'adresse ne contiennent ni l'adresse IP de l'appliance ni l'adresse MAC Ethernet de l'appliance.

Outre les modes de transfert pur, l'appliance doit prendre en compte d'autres types de connexions, y compris les connexions de gestion à l'interface graphique et le signal de pulsation qui passe entre les membres d'une paire haute disponibilité. Par souci d'exhaustivité, ces modes de trafic supplémentaires sont également répertoriés dans le tableau ci-dessous.

Tableau 1. Comment les adresses Ethernet et IP déterminent le mode

Adresse IP de destination	Adresse Ethernet de destination	Mode
Non appliance	Non appliance	Inline ou Pass-through
Non appliance	Boîtier	Virtual Inline ou L2 WCCP
Boîtier	Boîtier	Direct (accès à l'interface utilisateur)
Appareil (VIP)	Boîtier	Haute disponibilité. Mode proxy
Appliance (paquet WCCP GRE)	Boîtier	Mode WCCP GRE
Appliance (IP de signalisation)	Boîtier	Connexion de signalisation (Plugin SD-WAN Connexion de signalisation (Plugin SD-WAN, Secure Peer) ou Connexion en mode redirecteur (Plugin SD-WAN)

Tous les modes peuvent être actifs simultanément. Le mode utilisé pour un paquet donné est déterminé par les en-têtes Ethernet et IP.

Les modes de transfert sont les suivants :

- **Mode en ligne,** dans lequel l'appliance accélère de manière transparente le trafic entre ses deux ports Ethernet. Dans ce mode, l'appliance apparaît (pour le reste du réseau) comme un pont Ethernet. Le mode Inline est recommandé, car il nécessite le moins de configuration.
- **Mode WCCP,** qui utilise le protocole WCCP v. 2.0 pour communiquer avec le routeur. Ce mode est facile à configurer sur la plupart des routeurs. WCCP a deux variantes : WCCP-GRE et WCCP-L2. WCCP-GRE encapsule le trafic WCCP dans les tunnels d'encapsulation de routage générique (GRE). WCCP-L2 utilise le transport réseau de couche 2 (Ethernet) non encapsulé.
- **Mode virtuel en ligne,** dans lequel un routeur envoie du trafic WAN à l'appliance et le renvoie au routeur. Dans ce mode, l'appliance semble être un routeur, mais elle n'utilise aucune table de routage. Il envoie le trafic de retour au routeur réel. Le mode virtuel en ligne est recommandé lorsque le mode en ligne et le fonctionnement WCCP haute vitesse ne sont pas pratiques.
- **Mode groupe,** qui permet à deux appliances de fonctionner ensemble pour accélérer une paire de liaisons WAN largement séparées.
- **Mode haute disponibilité,** qui permet aux appliances de fonctionner comme une paire haute disponibilité active/veille. En cas de défaillance de l'appliance principale, l'appliance secondaire prend le relais.

D'autres types de trafic sont répertoriés ici pour être complets :

- Le**trafic pass-through** fait référence à tout trafic que l'appliance ne tente pas d'accélérer. Il s'agit d'une catégorie de trafic, pas d'un mode de transfert.
- **Accès direct,** où l'appliance agit comme un serveur ou un client ordinaire. L'interface graphique et l'interface de ligne de commande sont des exemples d'accès direct, à l'aide des protocoles HTTP, HTTPS, SSH ou SFTP. Le trafic d'accès direct peut également inclure les protocoles NTP et SNMP.
- **Communication Appliance-to-Appliance**, qui peut inclure des connexions de signalisation (utilisées dans l'appairage sécurisé et par le plugin SD-WAN), des pulsations VRRP (utilisées en mode haute disponibilité) et des tunnels GRE chiffrés (utilisées en mode groupe).
- **Modes obsolètes.** Le mode proxy et le mode redirecteur sont des modes de transfert hérités qui ne doivent pas être utilisés dans les nouvelles installations.

Les appliances SD-WAN 4100/5100 ont deux modes de déploiement recommandés : WCCP et Inline. Ces modes sont couramment utilisés sans haute disponibilité (haute disponibilité), et moins fréquemment avec haute disponibilité.

Actuellement, Citrix recommande le mode WCCP, avec un seul routeur et sans haute disponibilité, pour la plupart des déploiements. Utilisez le mode Inline lorsque WCCP n'est pas disponible.

Bien que tous les modes suivants ne soient pas recommandés actuellement, ils sont tous pris en charge :

- Mode WCCP avec un seul routeur
- Mode WCCP avec un seul routeur et haute disponibilité
- Cascade de deux appliances ou plus en mode WCCP avec une appliance NetScaler MPX
- Cascade de deux appliances ou plus en mode WCCP avec une appliance NetScaler MPX en haute disponibilité
- Mode Inline
- Mode Inline en haute disponibilité
- Mode virtuel en ligne
- Mode virtuel en ligne en haute disponibilité

> **Remarque**
>
> Bien que les modes autres que WCCP et en ligne soient pris en charge, ils sont incomplètement documentés et ne sont pas recommandés pour les installations typiques. Veuillez contacter votre représentant Citrix lorsque vous envisagez l'un de ces modes.

Personnalisation des ports Ethernet

April 9, 2021

Une appliance standard dispose de quatre ports Ethernet : deux ports pontés accélérés, appelés *paire accélérée A* (apA.1 et apA.2), avec un relais de contournement (fail-to-wire), et deux ports de carte mère non accélérés, appelés Primary et Aux1. Les ports pontés assurent une accélération, tandis que les ports de la carte mère sont parfois utilisés à des fins secondaires. La plupart des installations utilisent uniquement les ports pontés.

Certaines unités SD-WAN n'ont que les ports de la carte mère. Dans ce cas, les deux ports de la carte mère sont pontés.

L'interface utilisateur de l'appliance est accessible par un réseau VLAN ou non VLAN. Vous pouvez affecter un VLAN à l'un des ports pontés ou des ports de carte mère de l'appliance à des fins de gestion.

Figure 1. Ports Ethernet

Liste des ports

Les ports sont nommés comme suit :

Port Ethernet	Nom
Port de la carte mère 1	Primaire (ou apA.1 si aucune carte de contournement n'est présente)
Port carte mère 2	Auxiliaire1 ou Aux1 (ou apA.2 si aucune carte de contournement n'est présente)
Pont #1	Paire A accélérée (apA, avec ports apA.1 et apA.2)
Pont #2	Paire B accélérée (apB, avec ports apB.1 et apB.2)

Tableau 1. Noms de ports Ethernet

Paramètres de port

April 9, 2021

Chaque port de pont et de carte mère peut être :

- Activé ou désactivé
- Affecté d'une adresse IP et d'un masque de sous-réseau
- Attribué à une Gateway par défaut
- Affecté à un VLAN
- Régler sur 1000 Mbit/s, 100 Mbit/s ou 10 Mbit/s
- Réglage sur duplex intégral, semi-duplex ou automatique (sur les appliances SD-WAN WANOP 4000/5000, certains ports peuvent être réglés sur 10 Gbit/s)

Tous ces paramètres, à l'exception du paramètre speed/duplex, sont définis sur la page Configuration : Adresse IP. Les paramètres de vitesse/duplex sont définis sur la page Configuration : Interface.

> **Remarques** sur les paramètres :

- Les ports désactivés ne répondent à aucun trafic.
- L'interface utilisateur basée sur le navigateur peut être activée ou désactivée indépendamment sur tous les ports.
- Pour sécuriser l'interface utilisateur sur les ports dotés d'adresses IP, sélectionnez HTTPS au lieu de HTTP dans la page Configuration : Interface Administrateur : Accès Web.
- Le mode Inline fonctionne même si un pont n'a pas d'adresse IP. Tous les autres modes nécessitent qu'une adresse IP soit attribuée au port.
- Le trafic n'est pas routé entre les interfaces. Par exemple, une connexion sur le pont ApA ne traverse pas les ports principal ou Aux1, mais reste sur le pont ApA. Tous les problèmes de routage sont laissés à vos routeurs.

Ponts accélérés (apA et apB)

April 9, 2021

Chaque appliance dispose d'au moins une paire de ports Ethernet qui fonctionnent comme un pont accéléré, appelé *apA* (pour la *paire accélérée A*). Un pont peut agir en mode en ligne, fonctionnant comme un pont transparent, comme s'il s'agissait d'un commutateur Ethernet. Les paquets circulent dans un port et sortent de l'autre. Les ponts peuvent également agir en mode d'un bras, dans lequel les paquets circulent dans un port et sortent le même port.

Une appliance dotée d'une carte de contournement assure la continuité du réseau en cas de dysfonctionnement d'un pont ou d'une appliance.

Certaines unités ont plus d'une paire accélérée, et ces paires accélérées supplémentaires sont appelées APB, APC, etc.

Carte de contournement

Si l'appliance perd de l'alimentation ou tombe en panne d'une autre manière, un relais interne se ferme et les deux ports pontés sont connectés électriquement. Cette connexion maintient la continuité du réseau mais rend les ports du pont inaccessibles. Par conséquent, vous pouvez utiliser l'un des ports de la carte mère pour l'accès à la gestion.

Attention : N'activez pas le port principal s'il n'est pas connecté à votre réseau. Sinon, vous ne pouvez pas accéder à l'appliance, comme expliqué dans Contournement d'Ethernet et propagation de déconnexion

Les cartes de contournement sont de série sur certains modèles et en option sur d'autres. Citrix vous recommande d'acheter des appliances dotées de cartes de contournement pour tous les déploiements en ligne.

La fonction de contournement est câblée comme si un câble croisé reliait les deux ports, ce qui est le bon comportement dans les installations correctement câblées.

Important : Les installations de dérivation doivent être testées - Un câblage incorrect peut fonctionner en fonctionnement normal, mais pas en mode de dérivation. Les ports Ethernet tolèrent un câblage incorrect et s'y adaptent souvent silencieusement. Le mode de dérivation est câblé et n'a pas une telle adaptabilité. Testez les installations en ligne avec l'appliance désactivée pour vérifier que le câblage est correct pour le mode de contournement.

Utilisation de plusieurs ponts

Si l'appliance est équipée de deux ponts accélérés, ils peuvent être utilisés pour accélérer deux liaisons différentes. Ces liens peuvent être entièrement indépendants ou être des liens redondants se connectant au même site. Les liens redondants peuvent être soit équilibrés de charge, soit utilisés comme lien principal et lien de basculement.

Figure 1. Utilisation de ponts doubles

Lorsqu'il est temps pour l'appliance d'envoyer un paquet pour une connexion donnée, le paquet est envoyé sur le même pont à partir duquel l'appliance a reçu le paquet d'entrée le plus récent pour cette connexion. Ainsi, l'appliance respecte les décisions de liaison prises par le routeur et suit automatiquement en temps réel l'algorithme d'équilibrage de charge ou de liaison principale/lien de basculement. Pour les liaisons non équilibrées, ce dernier algorithme garantit également que les paquets utilisent toujours le pont correct.

Modes WCCP et Virtual Inline

Plusieurs ponts sont pris en charge à la fois en mode WCCP et en mode virtuel en ligne. L'utilisation est la même que dans le cas d'un pont unique, sauf que WCCP a la limitation supplémentaire selon

laquelle tout le trafic d'un groupe de services WCCP donné doit arriver sur le même pont.

Haute disponibilité avec plusieurs ponts

Deux unités avec plusieurs ponts peuvent être utilisées dans une paire haute disponibilité. Il suffit de faire correspondre les ponts de sorte que tous les liens passent par les deux appareils.

Ports de carte-mère

April 9, 2021

Bien que les ports Ethernet d'une carte de dérivation soient inaccessibles lorsque le relais de dérivation est fermé, les ports de la carte mère restent actifs. Vous pouvez parfois accéder à une appliance défaillante via les ports de la carte mère si les ports pontés sont inaccessibles.

Le port principal

Si le port principal est activé et qu'une adresse IP lui est attribuée, l'appliance utilise cette adresse IP pour s'identifier aux autres unités d'accélération. Cette adresse est utilisée en interne à diverses fins et est la plus visible pour les utilisateurs en tant que champ Unité partenaire de la page Surveillance : Optimisation : Connexions. Si aucun port de carte mère n'est activé, l'appliance utilise l'adresse IP de la paire accélérée A.

Le port principal est utilisé pour :

- Administration via l'interface utilisateur Web
- Un canal arrière pour le mode groupe
- Un canal arrière pour le mode haute disponibilité

Le port Aux1

Le port Aux1 est identique au port principal. Si le port Aux1 est activé et que le port principal ne l'est pas, l'appliance prend son identité à partir de l'adresse IP du port Aux1. Si les deux sont activés, l'adresse IP du port principal est l'identité de l'unité

Prise en charge de VLAN

April 9, 2021

Un réseau local virtuel (VLAN) utilise une partie de l'en-tête Ethernet pour indiquer à quel réseau virtuel appartient une trame Ethernet donnée. Les appliances SD-WAN prennent en charge le groupement VLAN dans tous les modes de transfert (mode Inline, WCCP, virtuel Inline et groupe). Le trafic avec n'importe quelle combinaison de balises VLAN est géré et accéléré correctement.

Par exemple, si un flux de trafic passant par le pont accéléré est adressé à 10.0.0.1, VLAN 100, et un autre à 10.0.0.1, VLAN 111, l'appliance sait qu'il s'agit de deux destinations distinctes, même si les deux VLAN ont la même adresse IP.

Vous pouvez affecter un VLAN à tous, à certains ou à aucun des ports Ethernet de l'appliance. Si un VLAN est affecté à un port, les interfaces de gestion (GUI et CLI) écoutent uniquement le trafic sur ce VLAN. Si aucun VLAN n'est attribué, les interfaces de gestion écoutent uniquement le trafic sans VLAN. Cette sélection est effectuée dans l'onglet Configuration : Paramètres de l'appliance : Cartes réseau : Adresses IP.

Personnalisation des ports Ethernet

April 9, 2021

Une appliance standard dispose de quatre ports Ethernet : deux ports pontés accélérés, appelés *paire accélérée A* (apA.1 et apA.2), avec un relais de contournement (fail-to-wire), et deux ports de carte mère non accélérés, appelés Primary et Aux1. Les ports pontés assurent une accélération, tandis que les ports de la carte mère sont parfois utilisés à des fins secondaires. La plupart des installations utilisent uniquement les ports pontés.

Certaines unités SD-WAN n'ont que les ports de la carte mère. Dans ce cas, les deux ports de la carte mère sont pontés.

L'interface utilisateur de l'appliance est accessible par un réseau VLAN ou non VLAN. Vous pouvez affecter un VLAN à l'un des ports pontés ou des ports de carte mère de l'appliance à des fins de gestion.

Figure 1. Ports Ethernet

Liste des ports

Les ports sont nommés comme suit :

Port Ethernet	Nom
Port de la carte mère 1	Primaire (ou apA.1 si aucune carte de contournement n'est présente)
Port carte mère 2	Auxiliaire1 ou Aux1 (ou apA.2 si aucune carte de contournement n'est présente)
Pont #1	Paire A accélérée (apA, avec ports apA.1 et apA.2)
Pont #2	Paire B accélérée (apB, avec ports apB.1 et apB.2)

Tableau 1. Noms de ports Ethernet

Contournement d'Ethernet et propagation de déconnexion

April 9, 2021

Remarque : La propagation Link-Down a été ajoutée aux appliances SD-WAN (anciennement SD-WAN) 1000, 2000, 3000, 4000 et 5000 avec la version 7.2.1.

La plupart des modèles d'appliance incluent une fonction de « basculement vers fil » (bypass Ethernet) pour le mode en ligne. En cas de panne d'alimentation, un relais se ferme et les ports d'entrée et de sortie sont connectés électriquement, ce qui permet au signal Ethernet de passer d'un port à l'autre comme si l'appareil n'était pas là. En mode Fail-to-wire, l'appliance ressemble à un câble croisé reliant les deux ports.

Toute défaillance du matériel ou du logiciel de l'appliance ferme également le relais. Lorsque l'appliance est redémarrée, le relais de contournement reste fermé jusqu'à ce que l'appliance soit entièrement initialisée, ce qui assure la continuité du réseau en tout temps. Cette fonctionnalité est automatique et ne nécessite aucune configuration utilisateur.

Lorsque le relais de contournement est fermé, les ports de pont de l'appliance sont inaccessibles.

Si le transporteur est perdu sur l'un des ports de pont, le transporteur est abandonné sur l'autre port de pont pour s'assurer que la condition de liaison est propagée au périphérique de l'autre côté de l'appliance. Les unités qui surveillent l'état de liaison (comme les routeurs) sont ainsi informées des conditions de l'autre côté du pont.

La propagation de liaison vers le bas comporte deux modes de fonctionnement :

- Si le port principal n'est pas activé, l'état de liaison vers le bas sur un port de pont est brièvement mis en miroir sur l'autre port de pont, puis le port est réactivé. Cela permet d'atteindre l'

appliance via le port encore connecté pour la gestion, la fréquence cardiaque haute disponibilité et d'autres tâches.

- Si le port principal est activé, l'appliance suppose (sans vérifier) que le port principal est utilisé pour la gestion, les pulsations de haute disponibilité et d'autres tâches. La condition de liaison vers le bas sur un port de pont est constamment mise en miroir sur l'autre port, jusqu'à ce que le transporteur soit restauré ou que l'unité soit redémarrée. Cela est vrai même si le port principal est activé dans l'interface graphique mais n'est pas connecté à un réseau, le port principal doit donc être désactivé (par défaut) lorsqu'il n'est pas utilisé.

Accélération d'un site entier

April 9, 2021

Mode en ligne, accélération de tout le trafic sur un WANprésente une configuration typique pour le mode Inline. Pour les deux sites, les appliances sont placées entre le LAN et le WAN, de sorte que tout le trafic WAN pouvant être accéléré est accéléré. C'est la méthode la plus simple pour mettre en œuvre l'accélération, et elle devrait être utilisée lorsque cela est pratique.

Étant donné que tout le trafic de liaison circule à travers les appliances, les avantages d'une mise en file d'attente et d'un contrôle de flux équitables empêchent la liaison d'être dépassée.

Dans les réseaux IP, la Gateway goulot d'étranglement détermine le comportement de file d'attente pour l'ensemble du lien. En devenant la Gateway goulot d'étranglement, l'appliance prend le contrôle de la liaison et peut la gérer intelligemment. Ceci est fait en définissant la limite de bande passante légèrement inférieure à la vitesse de liaison. Lorsque cela est fait, les performances de liaison sont idéales, avec une latence et une perte minimales, même à l'utilisation complète de la liaison.

Accélération partielle du site

April 9, 2021

Pour réserver la bande passante accélérée de l'appliance à un groupe particulier de systèmes, tels que des serveurs de sauvegarde distants, vous pouvez installer l'appliance sur un réseau de succursales qui inclut uniquement ces systèmes. Ceci est montré dans la figure suivante.

Figure 1. Mode Inline, Accélération des systèmes sélectionnés uniquement

Le traffic shaping SD-WAN repose sur le contrôle de l'intégralité de la liaison. Le traffic shaping n'est donc pas efficace avec cette topologie, car l'appliance ne voit qu'une partie du trafic de liaison. Le

contrôle de la latence est à la hauteur de la Gateway goulot d'étranglement, et la réactivité interactive peut en souffrir.

Mode WCCP

April 23, 2021

Le protocole WCCP (Web Cache Communication Protocol) est un protocole de routage dynamique introduit par Cisco. Initialement destiné uniquement à la mise en cache web, WCCP version 2 est devenu un protocole plus général, adapté à une utilisation par des accélérateurs tels que les appliances Citrix SD-WAN.

Le mode WCCP est le moyen le plus simple d'installer une appliance SD-WAN lorsque le fonctionnement en ligne n'est pas pratique. Il est également utile lorsque le routage asymétrique se produit, c'est-à-dire lorsque des paquets de la même connexion arrivent sur différentes liaisons WAN. En mode WCCP, les routeurs utilisent le protocole WCCP 2.0 pour détourner le trafic via l'appliance. Une fois reçu par l'appliance, le trafic est traité par le moteur d'accélération et le régulateur du trafic comme s'il était reçu en mode Inline.

> **Remarque**
>
> - Aux fins de la présente discussion, la version 1 du WCCP est considérée comme obsolète et seule la version 2 du WCCP est présentée.
> - La documentation WCCP standard appelle les clients WCCP « caches ». Pour éviter toute confusion avec les caches réels, Citrix évite généralement d'appeler un client WCCP un « cache ». Au lieu de cela, les clients WCCP sont généralement appelés « appliances ».
> - Cette discussion utilise le terme « routeur » pour indiquer les routeurs compatibles WCCP et les commutateurs compatibles WCCP. Bien que le terme « routeur » soit utilisé ici, certains commutateurs haut de gamme prennent également en charge WCCP et peuvent être utilisés avec des appareils SD-WAN.
>
> Les appliances SD-WAN prennent en charge deux modes WCCP :
>
> - WCCP est l'offre WCCP SD-WAN originale prise en charge depuis la version 3.x. Il prend en charge un seul groupe de services d'appliance (pas de mise en cluster).
> - La mise en cluster WCCP, introduite dans la version 7.2, permet à votre routeur d'équilibrer le trafic entre plusieurs appliances.

Fonctionnement du mode WCCP

Le mode physique pour le déploiement WCCP d'une appliance SD-WAN est le mode à un bras dans lequel l'appliance est connectée directement à un port dédié sur le routeur WAN. La norme WCCP inclut une négociation de protocole dans laquelle l'appliance s'enregistre auprès du routeur, et les deux négocient l'utilisation des fonctionnalités qu'ils prennent en charge en commun. Une fois cette négociation réussie, le trafic est routé entre le routeur et l'appliance selon les règles de routeur WCCP et de redirection définies sur le routeur.

Une appliance en mode WCCP ne requiert qu'un seul port Ethernet. L'appliance doit être déployée sur un port de routeur dédié (ou port de commutateur compatible WCC) ou isolée d'un autre trafic via un VLAN. Ne mélangez pas les modes en ligne et WCCP.

La figure suivante montre comment un routeur est configuré pour intercepter le trafic sur les interfaces sélectionnées et le transférer à l'appliance compatible WCCP. Chaque fois que l'appliance compatible WCCP n'est pas disponible, le trafic n'est pas intercepté et est transféré normalement.

Figure 1. Flux de trafic WCCP

Encapsulation du trafic

WCCP permet de transférer le trafic entre le routeur et l'appliance dans l'un des modes suivants :

- Mode L2 : nécessite que le routeur et l'appliance soient sur le même segment L2 (généralement un segment Ethernet). Le paquet IP n'est pas modifié, et seule l'adressage L2 est modifié pour transférer le paquet. Dans de nombreux périphériques, le transfert L2 est effectué sur la couche matérielle, ce qui lui donne les performances maximales. En raison de son avantage de performances, le transfert L2 est le mode préféré, mais tous les périphériques compatibles WCCP ne le prennent pas en charge.
- Mode GRE : l'encapsulation de routage générique (GRE) est un protocole routé et l'appliance peut en théorie être placée n'importe où, mais pour des performances, elle doit être placée près du routeur, sur un chemin rapide et non congestionné qui traverse le plus petit nombre possible de commutateurs et de routeurs. GRE est le mode WCCP d'origine. Un en-tête GRE est créé et le paquet de données y est ajouté. Le périphérique de réception supprime l'en-tête GRE. Avec l'encapsulation, l'appliance peut se trouver sur un sous-réseau qui n'est pas directement connecté au routeur. Cependant, le processus d'encapsulation et le routage ultérieur ajoutent la surcharge CPU au routeur, et l'ajout de l'en-tête GRE de 28 octets peut conduire à la fragmentation des paquets, ce qui ajoute des frais supplémentaires.

Le mode WCCP prend en charge plusieurs routeurs et GRE vs. Transfert L2. Chaque routeur peut avoir plusieurs liaisons WAN. Chaque lien peut avoir son propre groupe de services WCCP.

Le traffic shaping n'est pas efficace à moins que l'appliance ne gère le trafic UDP ainsi que le trafic TCP. Un deuxième groupe de services, avec un groupe de services UDP pour chaque liaison WAN, est recommandé si le traffic shaping est souhaité.

Inscription et mises à jour de statut

Un client WCCP (une appliance) utilise le port UDP 2048 pour s'enregistrer auprès du routeur et négocier quel trafic doit lui être envoyé, ainsi que quelles fonctionnalités WCCP doivent être utilisées pour ce trafic. L'appliance opère sur ce trafic et transfère le trafic résultant au point de terminaison d'origine. L'état d'une appliance est suivi via le processus d'enregistrement WCCP et un protocole de pulsation cardiaque. L'appliance contacte d'abord le routeur via le canal de contrôle WCCP (port UDP 2048), et l'appliance et le routeur échangent des informations avec des paquets nommés respectivement « Here_I_Am » et « I_See_You ». Par défaut, ce processus est répété toutes les 10 secondes. Si le routeur ne reçoit pas de message de la part de l'appliance pendant trois de ces intervalles, il considère que l'appliance a échoué et arrête de lui transférer le trafic jusqu'à ce que le contact soit rétabli.

Services et groupes de services

Différents appareils utilisant le même routeur peuvent fournir différents services. Pour suivre les services affectés aux appliances, le protocole WCCP utilise un identificateur de groupe de services, un entier d'un octet. Lorsqu'une appliance s'enregistre auprès d'un routeur, elle inclut également des numéros de groupe de services.

- Une seule appliance peut prendre en charge plusieurs groupes de services.
- Un seul routeur peut prendre en charge plusieurs groupes de services.
- Une seule appliance peut utiliser le même groupe de services avec plusieurs routeurs.
- Un seul routeur peut utiliser le même groupe de services avec plusieurs appliances. Pour les appliances SD-WAN, plusieurs appliances sont prises en charge en mode cluster WCCP et une seule appliance est prise en charge en mode WCCP.
- Chaque appliance spécifie un « type de retour » (L2 ou GRE) indépendamment pour chaque direction et chaque groupe de services. Les appliances SD-WAN 4000/5000 spécifient toujours le même type de retour pour les deux directions. D'autres appliances SD-WAN permettent au type de retour d'être différent.

Figure 2. Utilisation de différents groupes de services WCCP pour différents services

Plusieurs groupes de services peuvent être utilisés avec WCCP sur la même appliance. Par exemple, l'appliance peut recevoir du trafic du groupe de services 51 à partir d'une liaison WAN et du trafic du groupe de services 62 à partir d'une autre liaison WAN. L'appliance prend également en charge plusieurs routeurs. Il est indifférent de savoir si tous les routeurs utilisent le même groupe de services ou si différents routeurs utilisent différents groupes de services.

Suivi des groupes de services. Si un paquet arrive sur un groupe de services, les paquets de sortie pour la même connexion sont envoyés sur le même groupe de services. Si des paquets arrivent pour la même connexion sur plusieurs groupes de services, les paquets de sortie suivent le groupe de services le plus récemment vu pour cette connexion.

Comportement de haute disponibilité

Lorsque WCCP est utilisé avec le mode haute disponibilité, l'appliance principale envoie sa propre adresse IP de gestion apA ou apB, et non l'adresse virtuelle de la paire haute disponibilité, lorsqu'elle contacte le routeur. En cas de basculement sur incident, le nouveau dispositif principal contacte automatiquement le routeur, rétablissant le canal WCCP. Dans la plupart des cas, le délai d'expiration WCCP et le temps de basculement haute disponibilité se chevauchent. Par conséquent, la panne du réseau est inférieure à la somme des deux retards.

Le WCCP standard n'autorise qu'une seule appliance dans un groupe de services WCCP. Si une nouvelle appliance tente de contacter le routeur, elle découvre que l'autre appliance gère le groupe de services, et la nouvelle appliance définit une alerte. Il vérifie périodiquement si le groupe de services est toujours actif avec l'autre appliance et que la nouvelle appliance gère le groupe de services lorsque l'autre appliance devient inactive. La mise en cluster WCCP permet plusieurs appliances par groupe de services.

Topologie de déploiement

La figure suivante montre un déploiement WCCP simple, adapté pour L2 ou GRE. Le port de trafic (1/1) est connecté directement à un port de routeur dédié (Gig 4/12).

Figure 3. Déploiement WCCP simple

Dans cet exemple, le SD-WAN 4000/5000 est déployé en mode à un bras, le port de trafic (1/1) et le port de gestion (0/1) se connectant chacun à son propre port de routeur dédié.

Sur le routeur, WCCP est configuré avec la redirection ip wccp identique dans les instructions sur les ports WAN et LAN. Deux groupes de services sont utilisés, 71 et 72. Le groupe de services 71 est utilisé pour le trafic TCP et le groupe de services 72 est utilisé pour le trafic UDP. L'appliance n'accélère pas le trafic UDP, mais peut lui appliquer des stratégies de traffic shaping.

> **Remarque** : la spécification WCCP ne permet pas de transférer des protocoles autres que TCP et UDP, de sorte que des protocoles tels que ICMP et GRE contournent toujours l'appliance.

Clustering WCCP

Les appliances SD-WAN prennent en charge la mise en cluster WCCP, ce qui permet à votre routeur d'équilibrer votre trafic entre plusieurs appliances. Pour plus d'informations sur le déploiement d'appliances SD-WAN en tant que cluster, reportez-vous à la section Clustering WCCP.

Spécifications WCCP

Pour plus d'informations sur WCCP, voir Web Cache Communication Protocol V2, révision 1, http://tools.ietf.org/html/draft-mclaggan-wccp-v2rev1-00.

> **Remarque**
>
> Lors du déploiement de SD-WAN dans WCCP pour la redondance des commutateurs, nous pouvons connecter le commutateur 2 à apB. Créez un SG différent pour apB, donnez-lui une priorité inférieure à celle du SG pour Apa. Si Apa SG plus élevé est en place, cela sera utilisé pour la redirection. Si ce n'est pas le cas, apB SG sera utilisé. Notez que ApA et apB doivent être sur un sous-réseau différent.

Mode WCCP (non clusterisé)

April 9, 2021

Le mode WCCP n'autorise qu'une seule appliance dans un groupe de services WCCP. Si une nouvelle appliance tente de contacter le routeur, elle découvre que l'autre appliance gère le groupe de services, et la nouvelle appliance définit une alerte. Il vérifie périodiquement si le groupe de services est toujours actif avec l'autre appliance et que la nouvelle appliance gère le groupe de services lorsque l'autre appliance devient inactive.

> **Remarque : La**mise en cluster
> WCCP permet de multiplier les appliances par groupe de services.

Limites et pratiques exemplaires

Voici les limitations et les meilleures pratiques pour le mode WCCP (non clusterisé) :

- Sur les appliances avec plus d'une paire accélérée, tout le trafic d'un groupe de services WCCP donné doit arriver sur la même paire accélérée.

- Ne mélangez pas le trafic en ligne et le trafic WCCP sur la même appliance. L'appliance n'applique pas cette directive, mais sa violation peut entraîner des difficultés d'accélération. (Les modes WCCP et virtuel en ligne peuvent être mélangés, mais seulement si le WCCP et le trafic virtuel en ligne proviennent de différents routeurs.)
- Pour les sites avec un routeur WAN unique, utilisez WCCP chaque fois que le mode en ligne n'est pas pratique.
- Une seule appliance est prise en charge par groupe de services. Si plusieurs solutions matérielles tentent de se connecter au même routeur avec le même groupe de services, la négociation ne réussira que pour la première appliance.
- Pour les sites avec plusieurs routeurs WAN gérés par la même appliance, WCCP peut être utilisé pour prendre en charge un, certains ou tous vos routeurs WAN. D'autres routeurs peuvent utiliser le mode virtuel en ligne.

Prise en charge du routeur pour WCCP

La configuration du routeur pour WCCP est très simple. La prise en charge de WCCP version 2 est incluse dans tous les routeurs modernes. Elle été ajoutée à Cisco IOS à la version 12.0(11)S et 12.1(3)T. La meilleure stratégie de configuration du routeur est déterminée par les caractéristiques de votre routeur et de vos commutateurs. Le traffic shaping nécessite deux groupes de services.

Si votre routeur prend en charge la retransmission par le chemin inverse (RPF), vous devez la désactiver sur tous les ports, car elle peut confondre le trafic WCCP avec le trafic usurpé. Cette fonctionnalité se trouve dans les routeurs Cisco plus récents tels que le Cisco 7600.

Stratégies de configuration du routeur

Il existe deux approches de base pour rediriger le trafic du routeur vers l'appliance :

Sur le port WAN uniquement, ajoutez une instruction « WCCP redirection in » et une instruction « WCCP redirection out ».
Sur chaque port du routeur, à l'exception du port attaché à l'appliance, ajoutez une instruction « WCCP redirection in ».

La première méthode redirige uniquement le trafic WAN vers l'appliance, tandis que la seconde redirige tout le trafic routeur vers l'appliance, qu'il soit lié ou non au réseau étendu. Sur un routeur doté de plusieurs ports LAN et d'un trafic LAN à LAN important, l'envoi de tout le trafic vers l'appliance peut surcharger son segment LAN et surcharger l'appliance de cette charge inutile. Si GRE est utilisé, le trafic inutile peut également surcharger le routeur.

Sur certains routeurs, le chemin de « redirection » est plus rapide et met moins de charge sur le processeur du routeur que le chemin de « redirection ». Si nécessaire, cela peut être déterminé par

expérimentation directe sur votre routeur : Essayez les deux méthodes de redirection sous pleine charge réseau pour voir lequel offre les taux de transfert les plus élevés.

Certains routeurs et commutateurs compatibles WCCP ne prennent pas en charge la « redirection WCCP », donc la deuxième méthode doit être utilisée. Pour éviter de surcharger le routeur, il est recommandé d'éviter de rediriger un grand nombre de ports du routeur via l'appliance, peut-être en utilisant deux routeurs, l'un pour le routage WAN et l'autre pour le routage LAN vers LAN.

En général, la méthode 1 est plus simple, tandis que la méthode 2 peut fournir une plus grande performance.

Traffic shaping et WCCP

Un groupe de services peut être TCP ou UDP, mais pas les deux. Pour que le régulateur du trafic soit efficace, les deux types de trafic WAN doivent passer par l'appliance. Par conséquent :

L'accélération nécessite un groupe de services, pour le trafic TCP.
Le Traffic shaping nécessite deux groupes de services, l'un pour le trafic TCP et l'autre pour le trafic UDP. La différence entre les deux est configurée sur l'appliance et le routeur accepte cette configuration.

Configurer le routeur

L'appliance négocie automatiquement WCCP-GRE ou WCCP-L2. Le choix principal est entre une *opération de monodiffusion* (dans laquelle l'appliance est configurée avec l'adresse IP de chaque routeur) ou une *opération de multidiffusion* (dans laquelle l'appliance et les routeurs sont configurés avec l'adresse de multidiffusion).

Opération normale (Unicast) : pour un fonctionnement normal, la procédure consiste à déclarer WCCP version 2 et l'ID de groupe WCCP pour le routeur dans son ensemble, puis à activer la redirection sur chaque interface WAN. Voici un exemple Cisco IOS :

```
config term
ip wccp version 2
! We will configure the appliance to use group 51 for TCP and 52 for
   UDP.
ip wccp 51
ip wccp 52

! Repeat the following three lines for each WAN interface
! you wish to accelerate:
interface your_wan_interface
! If Reverse Path Forwarding is enabled (with an ip verify unicast
! source reachable" statement), delete or comment out the statement:
! ip verify unicast source reachable-via any
! Repeat on all ports.
```



```
14
15 ip wccp 51 redirect out
16 ip wccp 51 redirect in
17 ip wccp 52 redirect out
18 ip wccp 52 redirect in
19
20 ! If the appliance is inline with one of the router interfaces
21 ! (NOT SUPPORTED), add the following line for that interface
22 ! to prevent loops:
23 ip wccp redirect exclude in
24 ^Z
25 <!--NeedCopy-->
```

Si plusieurs routeurs doivent utiliser la même appliance, chacun est configuré comme indiqué ci-dessus, en utilisant les mêmes groupes de services ou différents.

Opération de multidiffusion : lorsque vous attribuez à l'appliance et à chaque routeur une adresse de multidiffusion, la configuration est légèrement différente de celle du fonctionnement normal. Voici un exemple Cisco IOS :

```
1  config term
2  ip wccp version 2
3  ip wccp 51 group-address 225.0.0.1
4
5  ! Repeat the following three lines for each WAN interface
6  ! you wish to accelerate:
7  interface your_wan_interface
8  ! If Reverse Path Forwarding is enabled (with an ip verify unicast
9  ! source reachable " statement), delete or comment out the statement:
10 ! ip verify unicast source reachable-via any
11
12 ip wccp 51 redirect out
13 ip wccp 51 redirect in
14 !
15 ! The following line is needed only on the interface facing the other
      router,
16 ! if there is another router participating in this service group.
17 ip wccp 51 group-listen
18
19 !If the appliance is inline with one of the router interfaces,
20 !(which is supported but not recommended), add
21 !the following line for that interface to prevent loops:
22 ip wccp redirect exclude in
23 ^Z
24 <!--NeedCopy-->
```

Procédure de configuration de base du mode WCCP sur l'appliance SD-WAN

Pour la plupart des sites, vous pouvez utiliser la procédure suivante pour configurer le mode WCCP sur l'appliance. La procédure vous permet de définir plusieurs paramètres sur des valeurs par défaut

sensibles. Les déploiements avancés peuvent nécessiter que vous définissez ces paramètres sur d'autres valeurs. Par exemple, si le groupe de services WCCP 51 est déjà utilisé par votre routeur, vous devez utiliser une valeur différente pour l'appliance.

Pour configurer le mode WCCP sur l'appliance :

1. Sur la page Configuration : Paramètres de l'appliance : WCCP.
2. Si aucun groupe de services n'a été défini, la page Sélectionner le mode apparaît. Les options sont Single SD-WAN et Cluster (Multiple SD-WAN). Sélectionnez Single SD-WAN. Vous êtes dirigé vers la page WCCP.
   Remarque : Les étiquettes de mode sont trompeuses. Le mode « Single SD-WAN » est également utilisé pour les paires SD-WAN haute disponibilité.
3. Si le mode WCCP n'est pas activé, cliquez sur **Activer**.
4. Cliquez sur **Ajouter un groupe de services**.
5. Les valeurs par défaut de l'interface (apA), du protocole (TCP), de la priorité WCCP (0), de la communication du routeur (monodiffusion), (mot de passe vide) et de la durée de vie (1) n'ont généralement pas à être modifiées pour le premier groupe de services que vous créez, mais si c'est le cas, tapez de nouvelles valeurs dans les champs fournis.
6. Dans le champ Adresse du **routeur** (si vous utilisez la monodiffusion) ou le champ **Adresse de multidiffusion** (si vous utilisez la multidiffusion), tapez l'adresse IP du routeur. Utilisez l'adresse IP du port du routeur utilisé pour la communication WCCP avec l'appliance.
7. Si plusieurs routeurs utilisent WCCP pour communiquer avec cette appliance, ajoutez d'autres routeurs maintenant.
8. Si vos routeurs ont des exigences particulières, définissez les champs Redirection du routeur (Auto/GRE/Level-2), Retour du paquet du routeur (Auto/GRE/Level-2) et Affectation du routeur (Masque/Hash) en conséquence. Les valeurs par défaut produisent des résultats optimaux avec la plupart des routeurs.
9. Cliquez sur **Ajouter**.
10. Répétez les étapes précédentes pour créer un autre groupe de services, pour le trafic UDP (par exemple, ID 52 du groupe de services et protocole UDP).
11. Accédez à la page Surveillance : Performances de l'appliance : WCCP. Le champ **Statut** doit passer à Connecté dans les 60 secondes.
12. Envoyez du trafic sur le lien et, sur la page Connexions, vérifiez que les connexions arrivent et sont en cours d'accélération.

Détails de configuration du groupe de services WCCP

Dans un groupe de services, un routeur WCCP et un dispositif SD-WAN (« cache WCCP » dans la terminologie WCCP) négocient les attributs de communication (capacités). Le routeur annonce ses capacités dans le message « I See You ». Les attributs de communication sont les suivants :

- Méthode de transfert : GRE ou niveau 2
- Méthode de retour de paquets (multidiffusion uniquement) : GRE ou niveau 2
- Méthode d'affectation : hachage ou masque
- Mot de passe (aucune valeur par défaut)

L'appliance déclenche une alerte si elle détecte une incompatibilité entre ses attributs et ceux du routeur. L'appliance peut être incompatible en raison d'un attribut spécifique d'un groupe de services (tel que GRE ou Level-2). Plus rarement, dans un groupe de services de multidiffusion, une alerte peut être déclenchée lorsque la sélection « Auto » choisit un attribut particulier avec un routeur particulier connecté, mais l'attribut est incompatible avec un routeur ultérieur.

Voici les règles de base pour les attributs de communication au sein d'une appliance SD-WAN.

Pour le transfert de routeur :

- Lorsque « Auto » est sélectionné, la préférence est pour le niveau 2, car il est plus efficace pour le routeur et l'appliance. Le niveau 2 est négocié si le routeur le prend en charge et que le routeur se trouve sur le même sous-réseau que l'appliance.
- Les routeurs d'un groupe de services monodiffusion peuvent négocier différentes méthodes si « Auto » est sélectionné.
- Les routeurs d'un groupe de services multidiffusion doivent tous utiliser la même méthode, qu'ils soient forcés avec « GRE » ou « Niveau 2 » ou, avec « Auto », comme déterminé par le premier routeur du groupe de services à se connecter.
- Pour une incompatibilité, une alerte annonce que le routeur « a un transfert de routeur incompatible ».

Pour l'affectation du routeur :

- La valeur par défaut est Hash.
- Lorsque « Auto » est sélectionné, le mode est négocié avec le routeur.
- Tous les routeurs d'un groupe de services doivent prendre en charge la même méthode d'affectation (Hash ou Masque).
- Pour tout groupe de services, si cet attribut est configuré comme « Auto », l'appliance sélectionne « Hash » ou « Masque » lorsque le premier routeur est connecté. « Hash » est choisi si le routeur le prend en charge. Sinon, « Masque » est sélectionné. Le problème de l'incompatibilité des routeurs suivants avec la méthode sélectionnée automatiquement peut être réduit en sélectionnant manuellement une méthode commune à tous les routeurs du groupe de services.
- Pour une incompatibilité, une alerte annonce que le routeur « a une méthode d'attribution de routeur incompatible ».
- Avec l'une ou l'autre des méthodes, l'appliance unique du groupe de services demande à tous les routeurs du groupe de services de diriger tous les paquets TCP ou UDP vers l'appliance. Les

routeurs peuvent modifier ce comportement avec des listes d'accès ou en sélectionnant les interfaces à rediriger vers le groupe de services.

Pour la méthode Mask, l'appliance négocie le masque « adresse IP source ». L'appliance ne fournit aucun mécanisme permettant de sélectionner « adresse IP de destination » ou les ports pour la source ou la destination. Le masque « adresse IP source » n'identifie pas spécifiquement une adresse IP ou une plage spécifique. Le protocole ne fournit pas un moyen de spécifier une adresse IP spécifique. Par défaut, étant donné qu'il n'y a qu'une seule appliance dans le groupe de services, un masque à un bit est utilisé pour conserver les ressources du routeur. (La version 6.0 utilisait un masque plus grand.)

Pour Mot de passe :

- Si le routeur requiert un mot de passe, le mot de passe défini sur l'appliance doit correspondre. Si le routeur ne nécessite pas de mot de passe, le champ de mot de passe de l'appliance doit être vide.

Test et dépannage de WCCP

Lorsque vous travaillez avec WCCP, l'appliance fournit différentes façons de surveiller l'état de l'interface WCCP, et votre routeur doit également fournir des informations.

Surveillance : Performances de l'appliance : page WCCP : la page WCCP signale l'état actuel du lien WCCP et signale la plupart des problèmes.

Entrées de journaux : la page Surveillance : performances de l'appliance : journalisation affiche une nouvelle entrée chaque fois que le mode WCCP est défini ou perdu.

Figure 1. Entrées du journal WCCP (le format varie quelque peu en fonction de la version)

Router Status—Sur le routeur, la commande « show ip wccp » affiche l'état du lien WCCP :

```
Router>enable
Password:
Router#show ip wccp
Global WCCP information:
    Router information:
        Router Identifier:                  172.16.2.4
        Protocol Version:                   2.0

    Service Identifier: 51
        Number of Cache Engines:            0
        Number of routers:                  0
        Total Packets Redirected:           19951
        Redirect access-list:               -none-
        Total Packets Denied Redirect:      0
        Total Packets Unassigned:           0
        Group access-list:                  -none-
```



```
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
<!--NeedCopy-->
```

Vérifier le mode WCCP

Vous pouvez surveiller la configuration WCCP à partir de l'interface graphique SD-WAN.

Pour surveiller la configuration WCCP

1. Accédez à la page **Surveillance > Performances de l'appliance > WCCP**.
2. Sélectionnez un cache et cliquez sur **Obtenir des informations**. Une page État du cache affiche la configuration WCCP, comme illustré dans la figure suivante.
3. Démarrez le trafic qui doit être transféré via l'appliance SD-WAN et surveillez la connexion sur la page **Surveillance > Optimisation > Connexions**.
    - Si les connexions sont affichées sous l'onglet **Connexions accélérées**, cela indique que tout fonctionne.
    - Si les connexions se trouvent dans l'onglet **Connexions non accélérées**, consultez la colonne **Détails**. Un message détecté asymétrie de routage implique que l'une des lignes de redirection ip wccp sur le routeur est manquante ou comporte une erreur, ou que différents chemins sont empruntés par le trafic client-serveur et serveur-client.
    - Si aucune connexion n'est affichée, mais que l'appliance signale qu'elle est connectée au routeur et que la page de surveillance WCCP ne présente aucune erreur, le problème est probablement lié à la configuration du routeur.

Clustering WCCP

December 14, 2022

La fonctionnalité de clustering WCCP vous permet de multiplier votre capacité d'accélération en affectant plusieurs appliances SD-WAN aux mêmes liaisons. Vous pouvez regrouper jusqu'à 32 appliances identiques, jusqu'à 32 fois la capacité. Parce qu'il utilise la norme WCCP 2.0, le clustering WCCP fonctionne sur la plupart des routeurs et certains commutateurs intelligents, y compris probablement ceux que vous utilisez déjà.

Parce qu'il utilise un protocole décentralisé, la mise en cluster WCCP permet d'ajouter ou de supprimer des appliances SD-WAN à volonté. En cas de défaillance d'une appliance, son trafic est réacheminé vers les appliances survivantes.

Contrairement à la haute disponibilité SD-WAN, une paire active/passive qui utilise deux appliances pour fournir les performances d'une seule appliance, les mêmes appliances déployées en tant que cluster WCCP offrent deux fois plus de performances qu'une seule appliance, ce qui permet à la fois de redondance et d'améliorer les performances.

En plus d'ajouter des appliances à mesure que les besoins de votre site augmentent, vous pouvez utiliser la fonctionnalité « Pay as You Grow » de Citrix pour augmenter les capacités de vos appareils grâce à des mises à niveau de licence.

CitrixCommand Centerest recommandé pour la gestion des clusters WCCP. La figure suivante illustre un réseau de base d'un cluster d'appliances SD-WAN en mode WCCP, administré à l'aide de Citrix Command Center.

Figure 1. Cluster SD-WAN administré à l'aide de Citrix Command Center

Clusters WCCP à charge équilibrée

Le protocole WCCP prend en charge jusqu'à 32 appliances dans une baie équilibrée de charge tolérante aux pannes appelée cluster. Dans l'exemple ci-dessous, trois appliances identiques (même modèle, même version logicielle) sont câblées de manière identique et configurées de manière identique, à l'exception de leurs adresses IP. Les appliances utilisant les mêmes groupes de services avec le même routeur peuvent devenir un cluster WCCP à charge équilibrée. Lorsqu'une nouvelle appliance s'enregistre auprès du routeur, elle peut rejoindre le pool existant d'appliances et recevoir sa part de trafic. Si une appliance quitte le réseau (comme indiqué par l'absence de signaux de pulsation cardiaque), le cluster est rééquilibré de sorte que seules les solutions matérielles restantes soient utilisées.

Figure 2. Un cluster WCCP à charge équilibrée avec trois appliances

Une appliance du cluster est sélectionnée comme cache désigné et contrôle le comportement d'équilibrage de charge des appliances du cluster. Le cache désigné est l'appliance dont l'adresse IP est la plus basse. Étant donné que les appliances ont des configurations identiques, peu importe lequel est le cache désigné. Si le cache désigné actuel est hors connexion, une autre appliance devient le cache désigné.

Le cache désigné détermine comment le trafic équilibré de charge est alloué et informe le routeur de ces décisions. Le routeur partage des informations avec tous les membres du cluster, de sorte que le cluster peut fonctionner même si le cache désigné est hors connexion.

> **Remarque** : Comme normalement configuré, une appliance SD-WAN 4000/5000 apparaît sous la forme de deux caches WCCP sur le routeur.

Algorithme d'équilibrage de charge

L'équilibrage de charge dans WCCP est statique, sauf lorsqu'une appliance entre ou quitte le cluster, ce qui entraîne le rééquilibrage du cluster entre ses membres actuels.

La norme WCCP prend en charge l'équilibrage de charge basé sur un masque ou un hachage. Par exemple, la mise en cluster SD-WAN WCCP utilise la méthode du masque uniquement, en utilisant un masque de 1 à 6 bits de l'adresse IP 32 bits. Ces bits d'adresse peuvent être non consécutifs. Toutes les adresses donnant le même résultat lorsqu'elles sont masquées sont envoyées à la même appliance. L'efficacité de l'équilibrage de charge dépend du choix d'une valeur de masque appropriée : un mauvais choix de masque peut entraîner un mauvais équilibrage de charge ou même aucun, avec tout le trafic envoyé à une seule appliance.

Topologie de déploiement

Selon la topologie de votre réseau, vous pouvez déployer un cluster WCCP avec un seul routeur ou plusieurs routeurs. Qu'elle soit connectée à un routeur ou à plusieurs routeurs, chaque appliance du cluster doit être connectée de manière identique à tous les routeurs utilisés.

Déploiement d'un seul routeur

Dans le diagramme suivant, trois appliances SD-WAN accélèrent le réseau étendu de 200 Mbps du datacenter. Le site prend en charge 750 utilisateurs d'applications virtuelles.

Comme indiqué sur le Fiche technique SD-WAN, un SD-WAN 3000-100 peut prendre en charge 100 Mbps et 400 utilisateurs, donc une paire de ces appliances prend en charge 200 Mbps et 800 utilisateurs, ce qui répond aux exigences du datacenter d'une liaison 200 Mbps et 750 utilisateurs.

Toutefois, en ce qui concerne la tolérance aux pannes, le cluster WCCP doit continuer à fonctionner sans être surchargé en cas de défaillance d'une appliance. Cela peut être réalisé en utilisant trois appliances lorsque les calculs exigent deux. C'est ce qu'on appelle la règle N+1.

La défaillance est un événement inhabituel, donc généralement les trois appliances sont en fonctionnement. Dans ce cas, chaque appliance ne prend en charge que 67 Mbps et 250 utilisateurs, ce qui laisse beaucoup de marge de manœuvre et fait bon usage du fait que le cluster a trois fois la puissance CPU et trois fois l'historique de compression d'un seul appareil.

Sans la mise en cluster WCCP, la capacité et la tolérance aux pannes nécessiteraient une paire d'appliances SD-WAN 4000-500 en mode haute disponibilité. Un seul de ces appareils est actif à la fois.

Déploiements multiples de routeurs

L'utilisation de plusieurs routeurs WAN est similaire à l'utilisation d'un seul routeur WAN. Si l'exemple précédent est modifié pour inclure deux liaisons de 100 Mbit/s au lieu d'un lien de 200 Mbit/s, la topologie change, mais les calculs ne le font pas.

Limitations

La configuration des appliances dans un cluster WCCP comporte les limitations suivantes :

- Toutes les appliances d'un cluster doivent être du même modèle et utiliser la même version logicielle.
- La synchronisation des paramètres entre les appliances du cluster n'est pas automatique. Utilisez Command Center pour gérer les appliances en tant que groupe.
- Le traffic shaping SD-WAN n'est pas efficace, car il repose sur le contrôle de la liaison entière en tant qu'unité, et aucune des appliances n'est en mesure de le faire. La QoS du routeur peut être utilisée à la place.
- Les algorithmes d'équilibrage de charge basés sur WCCP ne varient pas dynamiquement avec la charge, donc obtenir un bon équilibre de charge peut nécessiter un certain réglage.
- La méthode de hachage de l'affectation du cache n'est pas prise en charge. L'affectation de masque est la méthode prise en charge.
- Alors que la norme WCCP autorise des longueurs de masque de 1 à 7 bits, l'appliance prend en charge des masques de 1 à 6 bits.
- Les groupes de services de multidiffusion ne sont pas pris en charge. Seuls les groupes de services monodiffusion sont pris en charge.
- Tous les routeurs utilisant la même paire de groupes de services doivent prendre en charge la même méthode de transfert (GRE ou L2).
- La méthode de transfert et de retour négociée avec le routeur doit correspondre : les deux doivent être GRE ou les deux doivent être L2. Certains routeurs ne prennent pas en charge L2 dans les deux sens, ce qui entraîne une erreur de « décalage de capacité d'avance ou de retour ou d'affectation du routeur. » Dans ce cas, le groupe de services doit être configuré comme GRE.
- SD-WAN VPX ne prend pas en charge le clustering WCCP.
- L'appliance prend en charge (et négocie) uniquement les affectations de cache non pondérées (égales). Les affectations pondérées ne sont pas prises en charge.
- Certains appareils plus anciens, tels que le SD-WAN 700, ne prennent pas en charge le clustering WCCP.
- (SD-WAN 4000/5000 uniquement) Deux instances d'accélérateur sont requises par interface en mode L2. Trois interfaces sont prises en charge par appliance (puis uniquement sur les appliances avec six instances d'accélérateur ou plus).

- (SD-WAN 4000/5000 uniquement) Les paquets de contrôle WCCP du routeur doivent correspondre à l'une des adresses IP du routeur configurées sur l'appliance pour le groupe de services. En pratique, l'adresse IP du routeur pour l'interface qui le connecte à l'appliance doit être utilisée. L'IP de bouclage du routeur ne peut pas être utilisée.

Limites de la feuille de calcul de déploiement et du cluster

Dans la feuille de calcul suivante, vous pouvez calculer le nombre d'appliances nécessaires à votre installation et la taille de champ de masque recommandée. La taille de masque recommandée est de 1 à 2 bits supérieure à la taille minimale du masque pour votre installation.

Paramètre	Valeur	Remarques
Modèle d'appliance utilisé		—
Utilisateurs Citrix Virtual Apps and Desktops pris en charge par appliance	Uspec =	À partir de la fiche technique
Utilisateurs Citrix Virtual Apps and Desktops sur WAN Link	Uwan =	—
Facteur de surcharge utilisateur	Uoverload = Uwan/Uspec =	—
Nombre de BW pris en charge par appliance	BWspec =	À partir de la fiche technique
Liaison WAN BW	BWwan =	—
Facteur de surcharge BW	BWoverload = BWwan/BWspec =	—
Nombre d'appareils requis	N = max(Uoverload, BWoverload) +1 =	Comprend une pièce de rechange —
Nombre minimal de paquets	Bmin = N, arrondi une puissance de 2 =	—
Si SD-WAN 4000 ou 5000,	Bmin = 2N, arrondi à une puissance de 2 =	—
Valeur recommandée	B = 4 Bmin si Bmin <= 16, sinon 2 Bmin =	—
Nombre de bits « un » dans le masque d'adresse	M = log2 (B)	Si B=16, M=4.

Valeur du masque : La valeur du masque est un masque d'adresse 32 bits avec plusieurs bits « un » égaux à M dans la feuille de calcul fournie précédemment. Souvent, ces bits peuvent être les bits les moins significatifs du masque de sous-réseau WAN utilisé par vos sites distants. Si les masques de vos sites distants varient, utilisez le masque médian. (Exemple : Avec les sous-réseaux /24, les bits les moins significatifs du sous-réseau sont 0x00 00 nn 00. Le nombre de bits à définir sur un est log2 (taille du masque) : si la taille du masque est 16, définissez 4 bits sur un. Donc, avec une taille de masque de 16 et un sous-réseau /24, définissez la valeur du masque sur 0x00 00 0f 00.)

Les recommandations ci-dessus ne fonctionnent que si le champ de sous-réseau sélectionné est réparti uniformément dans votre trafic, c'est-à-dire que chaque bit d'adresse sélectionné par le masque est un pour la moitié des hôtes distants et un zéro pour l'autre moitié. Sinon, l'équilibrage de la charge est altéré. Cette distribution uniforme peut être vraie pour seulement quelques bits dans le champ réseau (seulement 2 bits). Si c'est le cas avec votre réseau, au lieu de masquer des bits dans la zone incriminée du champ de sous-réseau, déplacer ces bits vers une partie du champ d'adresse hôte qui possède la propriété 50/50. Par exemple, si seulement trois bits de sous-réseau dans un sous-réseau /24 ont la propriété 50/50 et que vous utilisez quatre bits de masque, un masque de 0x00 00 07 10 évite le bit fautif à 0x00 00 0800 et le déplace à 0x00 00 00 10, une partie du champ d'adresse qui est susceptible d'avoir la propriété 50/50 si vos sous-réseaux distants utilisent généralement au moins 32 adresses IP chacune.

Paramètre	Valeur	Remarques
Valeur finale du masque		—
Pont accéléré		Habituellement apA
Groupe de services WAN		Un groupe de services qui n'est pas déjà utilisé sur votre routeur (51-255)
Groupe de services LAN		Un autre groupe de services inutilisé
Adresse IP du routeur		Adresse IP de l'interface du routeur sur le port faisant face à l'appliance
Protocole WCCP (généralement « Auto »)		—

Algorithme DC	Utilisez « Déterministe » si vous n'avez que deux appliances ou si vous utilisez un équilibrage de charge dynamique comme HSRP ou GSLB. Sinon, utilisez « Moins perturbateur ».

La configuration des appliances dans un cluster WCCP comporte les limitations suivantes :

- Toutes les appliances d'un cluster doivent être du même modèle et utiliser la même version logicielle.
- La synchronisation des paramètres entre les appliances du cluster n'est pas automatique. Utilisez Command Center pour gérer les appliances en tant que groupe.
- Le traffic shaping SD-WAN n'est pas efficace, car il repose sur le contrôle de la liaison entière en tant qu'unité, et aucune des appliances n'est en mesure de le faire. La QoS du routeur peut être utilisée à la place.
- Les algorithmes d'équilibrage de charge basés sur WCCP ne varient pas dynamiquement avec la charge, donc obtenir un bon équilibre de charge peut nécessiter un certain réglage.
- La méthode de hachage de l'affectation du cache n'est pas prise en charge. L'affectation de masque est la méthode prise en charge.
- Alors que la norme WCCP autorise des longueurs de masque de 1 à 7 bits, l'appliance prend en charge des masques de 1 à 6 bits.
- Les groupes de services de multidiffusion ne sont pas pris en charge ; seuls les groupes de services de monodiffusion sont pris en charge.
- Tous les routeurs utilisant la même paire de groupes de services doivent prendre en charge la même méthode de transfert (GRE ou L2).
- La méthode de transfert et de retour négociée avec le routeur doit correspondre : les deux doivent être GRE ou les deux doivent être L2. Certains routeurs ne prennent pas en charge L2 dans les deux sens, ce qui entraîne une erreur de « décalage de capacité d'avance ou de retour ou d'affectation du routeur. » Dans ce cas, le groupe de services doit être configuré comme GRE.
- SD-WAN VPX ne prend pas en charge le clustering WCCP.
- L'appliance prend en charge (et négocie) uniquement les affectations de cache non pondérées (égales). Les affectations pondérées ne sont pas prises en charge.
- Certains appareils plus anciens, tels que le SD-WAN 700, ne prennent pas en charge le clustering WCCP.
- (SD-WAN WANOP 4000/5000 uniquement) Deux instances d'accélérateur sont requises par interface en mode L2. Trois interfaces ne sont pas prises en charge par appliance (puis sur les

appliances comportant au moins six instances d'accélérateur).
- (SD-WAN 4000/5000 uniquement) Les paquets de contrôle WCCP du routeur doivent correspondre à l'une des adresses IP du routeur configurées sur l'appliance pour le groupe de services. En pratique, l'adresse IP du routeur pour l'interface qui le connecte à l'appliance doit être utilisée. L'IP de bouclage du routeur ne peut pas être utilisée.

Test et dépannage

La page **Surveillance** > **Appliance** > **Performances de l'application** > **WCCP** affiche l'état actuel non seulement de l'appliance locale, mais également de toutes les autres appliances ayant rejoint le cluster. Sélectionnez un cache WCCP et cliquez sur **Obtenir des informations**.

l'onglet État du cache affiche l'état de l'appliance locale. Quand tout va bien, le statut est « 25 : a une affectation ». Vous devez actualiser la page manuellement pour surveiller les changements d'état. Si l'appliance n'atteint pas le statut « 25 : a une affectation » dans un délai d'expiration, d'autres messages d'état d'information s'affichent.

Des informations supplémentaires s'affichent lorsque vous cliquez sur les onglets **Groupe de services ou Routeurs**.

L'onglet Récapitulatif du cluster affiche des informations sur le cluster WCCP dans son ensemble. En tant qu'effet secondaire du protocole WCCP, chaque membre du cluster dispose d'informations sur tous les autres, de sorte que ces informations peuvent être surveillées à partir de n'importe quelle appliance du cluster.

Votre routeur peut également fournir des informations d'état. Consultez la documentation de votre routeur.

Configurer le clustering WCCP

Après avoir finalisé la topologie de déploiement, pris en compte toutes les limitations et rempli la feuille de calcul de déploiement, vous êtes prêt à déployer vos appliances dans un cluster WCCP. Pour configurer le cluster WCCP, vous devez effectuer les tâches suivantes :

- Configuration des instances NetScaler
- Configuration du routeur
- Configuration de l'appliance

Mode Virtual Inline

April 9, 2021

> **Remarque** :
>
> Utilisez le mode virtuel en ligne uniquement lorsque le mode en ligne et le mode WCCP ne sont pas pratiques. Ne mélangez pas les modes Inline et Virtual Inline au sein de la même appliance. Toutefois, vous pouvez mélanger les modes virtuel en ligne et WCCP au sein de la même appliance. Citrix ne recommande pas le mode virtuel en ligne avec des routeurs qui ne prennent pas en charge la surveillance de l'intégrité.

En mode virtuel en ligne, le routeur utilise des règles de routage basées sur des stratégies (PBR) pour rediriger le trafic WAN entrant et sortant vers l'appliance pour une accélération, et l'appliance transfère les paquets traités au routeur. Presque toutes les tâches de configuration sont effectuées sur le routeur. La seule chose à configurer sur l'appliance est la méthode de transfert, et la méthode par défaut est recommandée.

Tout comme WCCP, le déploiement virtuel en ligne ne nécessite aucun recâblage et aucun temps d'arrêt, et il fournit une solution pour les problèmes de routage asymétrique rencontrés dans un déploiement avec deux liaisons WAN ou plus. Contrairement à WCCP, il ne contient aucune surveillance d'état intégrée ni vérification de l'état, ce qui rend le dépannage difficile. WCCP est donc le mode recommandé, et virtuel inline n'est recommandé que lorsque les modes inline et WCCP sont tous deux impraticables.

Exemple

La figure suivante illustre un réseau simple dans lequel tout le trafic destiné ou reçu du site distant est redirigé vers l'appliance. Dans cet exemple, le site local et le site distant utilisent le mode virtuel en ligne.

Figure 1. Exemple virtuel en ligne

Voici quelques détails de configuration pour le réseau dans cet exemple :

- Les passerelles des systèmes de terminaison sont définies sur le routeur local (qui n'est pas unique au mode virtuel en ligne).
- Chaque routeur est configuré pour rediriger le trafic WAN entrant et sortant vers l'appliance locale.
- Chaque appliance traite le trafic reçu de son routeur local et le transfère au routeur.
- Les règles PBR configurées sur le routeur empêchent les boucles de routage en autorisant les paquets à effectuer un seul trajet vers et depuis l'appliance. Les paquets que l'appliance transfère au routeur sont envoyés à leur destination d'origine (locale ou distante).
- La Gateway par défaut de chaque appliance est définie sur l'adresse du routeur local, comme d'habitude (sur la page **Configuration : cartes réseau**). Les options de transfert de paquets vers le routeur sont Retourner à l'expéditeur Ethernet et Envoyer à la passerelle.

Configuration du transfert de paquets sur l'appliance

April 9, 2021

Le mode virtuel en ligne offre deux options de transfert de paquets :

Revenir à l'expéditeur Ethernet (par défaut) : ce mode permet à plusieurs routeurs de partager une appliance. L'appliance transfère les paquets de sortie en ligne virtuels vers leur provenance, comme indiqué par l'adresse Ethernet du paquet entrant. Si deux routeurs partagent une seule appliance, chacun récupère son propre trafic, mais pas celui de l'autre routeur. Ce mode fonctionne également avec un seul routeur.

Send to Gateway (non recommandé) : dans ce mode, les paquets de sortie en ligne virtuels sont transférés vers la passerelle par défaut pour remise, même s'ils sont destinés à des hôtes sur le sous-réseau local. Cette option est généralement moins souhaitable que l'option Retour à l'expéditeur Ethernet, car elle ajoute un élément de complexité facilement oublié à la structure de routage.

Pour spécifier l'option de transfert de paquets—Sur la page Configuration : Règles d'optimisation : Réglage, en regard de Virtual Inline, sélectionnez Retourner à l'expéditeur Ethernet ou Envoyer à la passerelle.

Configuration du routeur

April 23, 2021

Le routeur a trois tâches lors de la prise en charge du mode virtuel en ligne :

1. Il doit transférer à la fois le trafic WAN entrant et sortant vers l'appliance SD-WAN.
2. Il doit transférer le trafic SD-WAN vers sa destination (WAN ou LAN).
3. Il doit surveiller l'état de l'appliance afin qu'elle puisse être contournée en cas de défaillance.

Règles basées sur des règles

En mode virtuel en ligne, les méthodes de transfert de paquets peuvent créer des boucles de routage si les règles de routage ne font pas la distinction entre un paquet qui a été transféré par l'appliance et un autre qui ne l'a pas fait. Vous pouvez utiliser n'importe quelle méthode qui fait cette distinction.

Une méthode typique consiste à consacrer l'un des ports Ethernet du routeur à l'appliance et à créer des règles de routage basées sur le port Ethernet sur lequel les paquets arrivent. Les paquets qui arrivent sur l'interface dédiée à l'appliance ne sont jamais renvoyés à l'appliance, mais les paquets arrivant sur n'importe quelle autre interface peuvent l'être.

L'algorithme de routage de base est :

- Ne pas retransférer les paquets de l'appliance vers l'appliance.
- Si le paquet arrive du WAN, le transmettre à l'appliance.
- Si le paquet est destiné au WAN, le remettre à l'appliance.
- Ne pas transférer le trafic LAN vers LAN sur l'appliance.
- Le traffic shaping n'est pas efficace à moins que tout le trafic WAN passe par l'appliance.

> **Remarque** : lorsque vous envisagez les options de routage, gardez à l'esprit que les données renvoyées, et pas seulement les données sortantes, doivent circuler à travers l'appliance. Par exemple, placer l'appliance sur le sous-réseau local et la désigner comme routeur par défaut pour les systèmes locaux ne fonctionne pas dans un déploiement virtuel en ligne. Les données sortantes circuleraient à travers l'appliance, mais les données entrantes les contourneraient. Pour forcer les données à travers l'appliance sans reconfiguration du routeur, utilisez le mode en ligne.

Surveillance de la santé

Si l'appliance échoue, les données ne doivent pas être acheminées vers elle. Par défaut, le routage basé sur des stratégies Cisco n'effectue aucune surveillance de l'intégrité. Pour activer la surveillance de l'intégrité, définissez une règle pour surveiller la disponibilité de l'appliance et spécifiez l'option « verify-availability » pour la commande « set ip next-hop ». Avec cette configuration, si l'appliance n'est pas disponible, la route n'est pas appliquée et l'appliance est contournée.

Important : Citrix recommande le mode virtuel en ligne uniquement lorsqu'il est utilisé avec la surveillance de l'intégrité. De nombreux routeurs qui prennent en charge le routage basé sur des stratégies ne prennent pas en charge le contrôle de l'état. La fonction de surveillance de la santé est relativement nouvelle. Il est devenu disponible dans Cisco IOS version 12.3 (4) T.

Voici un exemple de règle permettant de surveiller la disponibilité de l'appliance :

“‘ pre codeblock
!- Use a ping (ICMP echo) to see if appliance is connected track 123 rtr 1 reachabilit y ! rtr 1 type echo protocol IpIcmpecho 192.168.1.200 schedule 1 life forever start-time now

```
Cette règle envoie une commande ping régulièrement à l'appliance sur
   192.168.1.200. Vous pouvez tester par rapport à 123 pour voir si l'
   unité est en service.

## Exemples de routage

Les exemples suivants illustrent la configuration des routeurs Cisco
   pour les sites locaux et distants illustrés dans [Exemple virtuel en
    ligne](/fr-fr/citrix-sd-wan-wanop/current-release/cb-deployment-
   modes-con/br-adv-virt-inline-mode-con.html). Pour illustrer la
   surveillance de l'intégrité, la configuration pour le site local
```



```
    inclut la surveillance de l'intégrité, mais pas la configuration
    pour le site distant.

Remarque : La configuration du site local suppose qu'un moniteur ping a
    déjà été configuré.

Les exemples sont conformes à l'interface de ligne de commande Cisco
    IOS. Ils peuvent ne pas s'appliquer aux routeurs d'autres
    fournisseurs.

Site local, vérification de l'état activée :

``` pre codeblock
!
! For health-checking to work, do not forget to start
! the monitoring process.
!
! Original configuration is in normal type.
! appliance-specific configuration is in bold.
!
ip cef
!
interface FastEthernet0/0
ip address 10.10.10.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 172.68.1.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.1.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.1.1
!
ip access-list extended client_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
!- Now set the appliance as the next hop, if it ' s up.
set ip next-hop verify-availability 192.168.1.200 20 track 123
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop verify-availability 192.168.1.200 10 track 123
<!--NeedCopy-->
```

Site distant (aucune vérification de l'état) :


```

“‘ pre codeblock
! This example does not use health-checking.
! Remember, health-checking is always recommended,
! so this is a configuration of last resort.
!
!
ip cef
!
interface FastEthernet0/0
ip address 20.20.20.5 255.255.255.0
ip policy route-map client_side_map
!
interface FastEthernet0/1
ip address 171.68.2.5 255.255.255.0
ip policy route-map wan_side_map
!
interface FastEthernet1/0
ip address 192.168.2.5 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 171.68.2.1
!
ip access-list extended client_side
permit ip 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
ip access-list extended wan_side
permit ip 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
!
route-map wan_side_map permit 20
match ip address wan_side
set ip next-hop 192.168.2.200
!
route-map client_side_map permit 10
match ip address client_side
set ip next-hop 192.168.2.200
!_

```
1 Chacun des exemples ci-dessus applique une liste d'accès à une carte d'
       itinéraire et attache la carte d'itinéraire à une interface. Les
       listes d'accès identifient tout le trafic provenant d'un site accélé
       ré et se terminant à l'autre (IP source 10.10.10.0/24 et destination
        20.20.20.0/24 ou vice versa). Consultez la documentation de votre
```


```
      routeur pour obtenir les détails des listes d'accès et des cartes de
       routage.
2
3 Cette configuration redirige tout le trafic IP correspondant vers les
     appliances. Si vous souhaitez rediriger uniquement le trafic TCP,
     vous pouvez modifier la configuration de la liste d'accès comme suit
      (seule la configuration du côté distant est affichée ici) :
4
5 ``` pre codeblock
6 !
7  ip access-list extended client_side
8  permit tcp 10.16.20.0 0.0.0.255 10.10.10.0 0.0.0.255
9  ip access-list extended wan_side
10 permit tcp 10.10.10.0 0.0.0.255 10.16.20.0 0.0.0.255
11 !
12 <!--NeedCopy-->
```

Notez que, pour les listes d'accès, les masques ordinaires ne sont pas utilisés. Les masques génériques sont utilisés à la place. Notez que lors de la lecture d'un masque générique en binaire, « 1 » est considéré comme un bit « quelconque ».

Virtual Inline pour environnements WAN multiples

April 9, 2021

Les entreprises ayant plusieurs liaisons WAN ont souvent des stratégies de routage asymétriques, ce qui semble exiger qu'une appliance en ligne se trouve à deux endroits à la fois. Le mode virtuel en ligne résout le problème de routage asymétrique en utilisant la configuration du routeur pour envoyer tout le trafic WAN via l'appliance, quelle que soit la liaison WAN utilisée. La figure ci-dessous illustre un exemple simple de déploiement de liaison multiréseau.

Les deux routeurs côté local redirigent le trafic vers l'appliance locale. Les ports FE 0/0 des deux routeurs se trouvent dans le même domaine de diffusion que l'appliance. L'appliance locale doit utiliser la configuration virtuelle en ligne par défaut (Retourner à l'expéditeur Ethernet).

Figure 1. Mode virtuel en ligne avec deux routeurs WAN

Mode Virtual Inline et haute disponibilité

April 9, 2021

Le mode virtuel Inline peut être utilisé dans une configuration haute disponibilité (haute disponibilité). La figure ci-dessous illustre un déploiement simple de haute disponibilité. En mode virtuel en

ligne, une paire d'appliances agit comme une seule appliance virtuelle. La configuration du routeur est la même pour une paire haute disponibilité qu'avec une seule appliance, sauf que l'adresse IP virtuelle de la paire haute disponibilité, et non l'adresse IP d'une appliance individuelle, est utilisée dans les tables de configuration du routeur. Dans cet exemple, les appliances locales doivent utiliser la configuration virtuelle en ligne par défaut (Retour à l'expéditeur Ethernet).

Figure 1. Exemple de haute disponibilité

Surveillance et dépannage

April 9, 2021

En mode virtuel en ligne, contrairement au mode WCCP, l'appliance ne fournit aucune surveillance virtuelle spécifique à la ligne. Pour résoudre les problèmes liés à un déploiement virtuel en ligne, connectez-vous à l'appliance et utilisez la page Tableau de bord pour vérifier que le trafic entre et en sort. Les échecs de transfert de trafic sont généralement causés par des erreurs dans la configuration du routeur.

Si les pages Surveillance : Utilisation ou Surveillance : Connexions indiquent que le trafic est transféré mais qu'aucune accélération n'est en cours (en supposant qu'une appliance est déjà installée à l'autre extrémité du lien WAN), vérifiez que le trafic WAN entrant et le trafic WAN sortant sont transférés vers l'appliance. Si une seule direction est orientée, l'accélération ne peut pas avoir lieu.

Pour tester la vérification de l'état, mettez l'appareil hors tension. Le routeur doit arrêter le transfert de trafic après l'expiration de l'algorithme de vérification de la santé.

Mode Group

April 9, 2021

En mode groupe, deux appliances ou plus deviennent une appliance virtuelle unique. Ce mode est une solution au problème du routage asymétrique, qui est défini comme n'importe quel cas dans lequel certains paquets d'une connexion donnée passent par une appliance donnée, mais d'autres ne le font pas. Une limitation de l'architecture de l'appliance est que l'accélération ne peut pas avoir lieu à moins que tous les paquets d'une connexion donnée passent par les deux mêmes appliances. Le mode Groupe surmonte cette limitation.

Le mode Groupe peut être utilisé avec des liens multiples ou redondants sans reconfigurer vos routeurs.

> **Remarque**
>
> Le mode Groupe n'est pas pris en charge sur les appliances SD-WAN 4000 ou 5000.

Le mode Groupe s'applique uniquement aux appliances situées d'un côté de la liaison WAN ; les appliances locales ne savent pas si les appliances distantes utilisent le mode Groupe, et ne s'en soucient pas.

Le mode Groupe utilise un mécanisme de pulsation pour vérifier que les autres membres du groupe sont actifs. Les paquets sont transférés uniquement aux membres actifs du groupe.

Éviter le routage asymétrique est la principale raison d'utiliser le mode groupe, mais le mode groupe n'est pas la seule méthode disponible à cet effet. Si vous décidez qu'il s'agit de la meilleure méthode pour votre environnement, vous pouvez l'activer en définissant quelques paramètres. Si le mécanisme par défaut permettant de déterminer quelle appliance est responsable d'une connexion particulière ne fournit pas une accélération optimale, vous pouvez modifier les règles de transfert.

Figure 1. Mode Groupe avec liens redondants

Figure 2. Mode Groupe avec liens non redondants avec possibilité de routage asymétrique

Figure 3. Mode Groupe sur les campus à proximité

Quand utiliser le mode Group

April 9, 2021

Utilisez le mode groupe dans les circonstances suivantes :

- Vous avez plusieurs liens WAN.
- Il y a un risque de routage asymétrique (un paquet sur une connexion donnée peut circuler sur l'un ou l'autre des liens).
- Le mode groupe semble plus simple et plus pratique que les alternatives qui utilisent un seul appareil.

Les solutions de rechange sont les suivantes :

- Mode WCCP, dans lequel le trafic provenant de deux liaisons ou plus est envoyé à la même appliance par des routeurs WAN, au moyen du protocole WCCP.
- Mode virtuel en ligne, dans lequel vos routeurs envoient du trafic à partir de deux liens ou plus via la même appliance (ou paire haute disponibilité).
- Plusieurs ponts, où chaque liaison passe par un pont accéléré différent dans la même appliance.
- Agrégation au niveau du réseau local, qui place une appliance (ou une paire haute disponibilité) plus proche du réseau local, avant le point où le trafic WAN est divisé en deux chemins ou plus.

Fonctionnement du mode Group

April 9, 2021

En mode groupe, les appliances faisant partie du groupe prennent chacune possession d'une partie des connexions du groupe. Si une appliance donnée est propriétaire d'une connexion, elle prend toutes les décisions d'accélération concernant cette connexion et est responsable de la compression, du contrôle de flux, de la retransmission de paquets, etc.

Si une appliance reçoit un paquet pour une connexion dont elle n'est pas propriétaire, elle transfère le paquet à l'appliance qui en est le propriétaire. Le propriétaire examine le paquet, prend les décisions d'accélération appropriées et transfère tous les paquets de sortie à l'appliance non propriétaire. Ce processus préserve la sélection de liens effectuée par le routeur, tout en permettant à tous les paquets de la connexion d'être gérés par l'appliance propriétaire. Pour les routeurs, l'introduction des appliances n'a pas de conséquences. Il n'est pas nécessaire de reconfigurer les routeurs et les appliances n'ont pas besoin de comprendre le mécanisme de routage. Ils acceptent simplement les décisions de transmission des routeurs.

Figure 1. Côté émetteur du trafic en mode groupe

Figure 2. Côté de réception du flux de trafic en mode groupe

Le mode Groupe comporte deux modes de défaillance sélectionnables par l'utilisateur, qui contrôlent la façon dont les membres du groupe interagissent les uns avec les autres si l'un d'eux échoue. Le mode de défaillance détermine également si la carte de contournement de l'appliance défaillante s'ouvre (bloquant le trafic à travers l'appliance) ou reste fermée (permettant au trafic de passer). Les modes de défaillance sont les suivants :

Continuer à accélérer - En cas de défaillance d'un membre du groupe, sa carte de contournement est ouverte et aucun trafic ne passe par l'appliance défaillante. Le résultat est probablement un basculement si des liens redondants sont utilisés. Sinon, le lien est tout simplement inaccessible. Les autres appliances du groupe continuent de s'accélérer. L'algorithme de hachage habituel gère les conditions modifiées. (Autrement dit, l'ancien algorithme de hachage est utilisé, et si l'unité défaillante est indiquée comme propriétaire, un algorithme de hachage basé sur le nouveau groupe plus petit est appliqué. Cela préserve autant de connexions anciennes que possible.)

Ne pas accélérer - Si un membre du groupe tombe en panne, sa carte de contournement se ferme, ce qui permet au trafic de passer sans accélération. Étant donné qu'un chemin non accéléré introduit un routage asymétrique, les autres membres du groupe passent également en mode pass-through lorsqu'ils détectent l'échec.

Activation du mode Group

April 9, 2021

Pour activer le mode groupe, créez un groupe de deux appliances ou plus. Une appliance peut être membre d'un seul groupe. Les membres du groupe sont identifiés par l'adresse IP et le nom commun SSL dans la licence de l'appliance.

Tous les paramètres du mode groupe se trouvent sur la page Paramètres : Mode groupe, dans le tableau Configurer les paramètres : Mode groupe.

Figure 1. Page Mode de groupe

Pour activer le mode de groupe

1. Sélectionnez l'adresse à utiliser pour la communication de groupe. En haut de la table Configuration du mode groupe sous l'onglet Configuration : Déploiements avancés : Mode groupe, la cellule du tableau sous Membre VIP contient l'adresse de gestion du port utilisé pour communiquer avec les autres membres du groupe. Utilisez le menu déroulant (non étiqueté) pour sélectionner l'adresse correcte (par exemple, pour utiliser le port Aux1, sélectionnez l'adresse IP que vous avez affectée au port Aux1). Ensuite, cliquez sur Modifier VIP.
2. Ajoutez au moins un membre de groupe supplémentaire à la liste. (Les groupes de trois personnes ou plus sont pris en charge mais sont rarement utilisés.) Dans la cellule suivante de la colonne VIP membre, tapez l'adresse IP du port utilisé par l'autre appliance pour la communication en mode groupe.
3. Tapez le nom commun SSL de l'autre membre du groupe dans la colonne Nom commun SSL. Le nom commun SSL est répertorié dans l'onglet Configurer : Déploiements avancés : Haute disponibilité de l'autre appliance. Si l'autre membre du groupe est une paire haute disponibilité, le nom indiqué est le nom commun SSL de l'appliance principale.

   > **Remarque** :
   >
   > si l'appliance locale ne fait pas partie d'une paire haute disponibilité, la première cellule du nom commun SSL secondaire haute disponibilité est vide. Si l'autre membre du groupe est une paire haute disponibilité, spécifiez le nom commun SSL de l'appliance secondaire haute disponibilité dans le disponibilité Colonne du nom commun SSL secondaire.

4. Cliquez sur Ajouter.
5. Répétez les étapes 2 à 4 pour les appliances supplémentaires ou les paires haute disponibilité du groupe.

6. Les trois boutons de la liste des membres du groupe sont des bascules, de sorte que chacun est étiqueté comme étant le contraire de son paramètre actuel :

    a) Le bouton supérieur indique : **Ne pas accélérer lorsque l'échec du membre est détecté** ou **Continuer pour accélérer lorsque l'échec du membre est détecté**. Le paramètre « Ne pas accélérer… » fonctionne toujours et ne bloque pas le trafic, mais si un membre échoue, les autres membres du groupe passent en mode de contournement, ce qui provoque une perte complète d'accélération. Avec l'option « Continuer à accélérer », le pont de l'appliance défaillante devient un circuit ouvert et la liaison échoue. Cette option est appropriée si le routeur WAN répond en provoquant un basculement. Les nouvelles connexions et les connexions ouvertes appartenant aux appliances survivantes sont accélérées.
    b) Le bouton du bas doit maintenant être étiqueté Désactiver le mode de groupe. Si ce n'est pas le cas, activez le mode groupe en cliquant sur le bouton.

7. Actualisez l'écran. Le haut de la page doit répertorier les partenaires du mode groupe, mais afficher des avertissements sur leur statut, car ils n'ont pas encore été configurés pour le mode groupe. Par exemple, cela peut indiquer que le partenaire est introuvable ou qu'il exécute une autre version de logiciel.

8. Répétez cette procédure avec les autres membres du groupe. Dans les 20 secondes suivant l'activation du dernier membre du groupe, la ligne État du mode groupe doit afficher NORMAL, et les autres membres du mode groupe doivent être répertoriés avec Status : On-Line et Configuration : OK.

Règles de transfert

April 9, 2021

Par défaut, le *propriétaire* d'une connexion en mode groupe est défini par un hachage des adresses IP source et destination. Chaque appliance du groupe utilise le même algorithme pour déterminer quel membre du groupe possède une connexion donnée. Cette méthode ne nécessite aucune configuration. Le propriétaire peut éventuellement être spécifié via des règles configurables par l'utilisateur.

Étant donné que le hachage en mode groupe n'est pas identique à celui utilisé par les équilibreurs de charge, environ la moitié du trafic a tendance à être transféré à l'appliance propriétaire dans un groupe à deux appareils. Dans le pire des cas, le transfert entraîne le doublement de la charge sur l'interface côté LAN, ce qui réduit de moitié le taux de transfert maximal de l'appliance pour le trafic WAN réel.

Cette pénalité de vitesse peut être réduite si les ports Ethernet principal ou Aux1 sont utilisés pour le trafic entre les membres du groupe. Par exemple, si vous disposez d'un groupe de deux appliances,

vous pouvez utiliser un câble Ethernet pour connecter les ports principaux des deux unités, puis spécifier le port principal sur la page Mode groupe de chaque unité. Toutefois, les performances maximales sont atteintes si la quantité de trafic transférée entre les membres du mode groupe est réduite au minimum.

Le propriétaire peut éventuellement être défini selon des règles IP/port spécifiques. Ces règles doivent être identiques sur toutes les appliances du groupe. Chaque membre du groupe vérifie que sa configuration en mode groupe est identique aux autres. Si toutes les configurations ne sont pas identiques, aucune des appliances membres n'entre en mode groupe.

Si le trafic arrive en premier sur l'appliance propriétaire de la connexion, il est accéléré et transmis normalement. S'il arrive d'abord à une autre appliance du groupe, il est transmis à son propriétaire via un tunnel GRE, ce qui l'accélère et la renvoie à l'appliance d'origine pour qu'elle soit transférée. Ainsi, le mode groupe laisse la sélection de lien du routeur inchangée.

L'utilisation de règles de transfert explicites basées sur IP peut réduire la quantité de transfert en mode groupe. Ceci est particulièrement utile dans les scénarios de lien primaire/lien de sauvegarde, où chaque lien gère une plage particulière d'adresses IP, mais peut servir de sauvegarde lorsque l'autre lien est en panne.

Figure 1. Sélection de propriétaire basée sur IP

Les règles de transfert peuvent garantir que les membres du groupe traitent uniquement leur trafic « naturel ». Dans de nombreuses installations, où le trafic est généralement acheminé sur sa liaison normale et ne traverse que rarement l'autre, ces règles peuvent réduire considérablement les frais généraux.

Les règles sont évaluées dans l'ordre, de haut en bas, et la première règle de correspondance est utilisée. Les règles sont mises en correspondance par rapport à une paire optionnelle d'adresse IP/-masque (comparée aux adresses source et de destination) et par rapport à une plage de ports facultative.

Quel que soit l'ordre des règles, si l'appliance partenaire n'est pas disponible, le trafic n'y est pas transféré, qu'une règle corresponde ou non.

Par exemple, dans la figure ci-dessous, le membre 172.16.1.102 est le propriétaire de tout le trafic vers ou depuis son propre sous-réseau (172.16.1.0/24), tandis que le membre 172.16.0.184 est le propriétaire de tout autre trafic.

Si un paquet arrive à l'unité 172.16.1.102 et qu'il n'est pas adressé vers/depuis net 172.16.1.0/24, il est transmis à 172.16.0.184.

Toutefois, si l'unité 172.16.0.184 échoue, l'unité 172.16.1.102 ne transmet plus les paquets. Il tente de gérer le trafic lui-même. Ce comportement peut être inhibé en cliquant sur **Ne pas accélérer lorsque l'échec du membre est détecté** dans l'onglet Mode de groupe.

Dans une configuration avec une liaison WAN principale et une liaison WAN de sauvegarde, écrivez les règles de transfert pour envoyer tout le trafic vers l'appliance sur la liaison principale. Si la liaison WAN principale échoue, mais que l'appliance principale ne le fait pas, le routeur WAN échoue et envoie du trafic sur la liaison secondaire. L'appliance sur la liaison secondaire transfère le trafic vers la solution matérielle-liaison principale, et l'accélération se poursuit sans perturbations. Cette configuration maintient les connexions accélérées après le basculement de liaison.

Figure 2. Règles de transfert

Surveillance et dépannage du mode Group

April 9, 2021

Deux choses doivent être vérifiées dans une installation en mode groupe :

- Que les deux appliances sont entrées en mode groupe, ce qui peut être déterminé sur la page Configuration : Déploiements avancés : Mode groupe.
- Que le comportement de la paire de mode groupe est tel que souhaité lorsque l'autre membre échoue et lorsque l'une des liaisons échoue, comme déterminé en désactivant l'autre appliance et en déconnectant temporairement l'une des liaisons, respectivement.

Personnalisation des ports Ethernet

April 9, 2021

Une appliance standard dispose de quatre ports Ethernet : deux ports pontés accélérés, appelés *paire accélérée A* (apA.1 et apA.2), avec un relais de contournement (fail-to-wire), et deux ports de carte mère non accélérés, appelés Primary et Aux1. Les ports pontés assurent une accélération, tandis que les ports de la carte mère sont parfois utilisés à des fins secondaires. La plupart des installations utilisent uniquement les ports pontés.

Certaines unités SD-WAN n'ont que les ports de la carte mère. Dans ce cas, les deux ports de la carte mère sont pontés.

L'interface utilisateur de l'appliance est accessible par un réseau VLAN ou non VLAN. Vous pouvez affecter un VLAN à l'un des ports pontés ou des ports de carte mère de l'appliance à des fins de gestion.

Figure 1. Ports Ethernet

Liste des ports

Les ports sont nommés comme suit :

Port Ethernet	Nom
Port de la carte mère 1	Primaire (ou apA.1 si aucune carte de contournement n'est présente)
Port carte mère 2	Auxiliaire1 ou Aux1 (ou apA.2 si aucune carte de contournement n'est présente)
Pont #1	Paire A accélérée (apA, avec ports apA.1 et apA.2)
Pont #2	Paire B accélérée (apB, avec ports apB.1 et apB.2)

Tableau 1. Noms de ports Ethernet

Fonctionnement du mode High-Availability

April 9, 2021

Dans une paire haute disponibilité (haute disponibilité), une appliance est principale et l'autre est secondaire. L'appliance principale surveille son propre statut et celui de l'appliance secondaire. Si elle détecte un problème, le traitement du trafic échoue vers l'appliance secondaire. Les connexions TCP existantes sont terminées. Pour garantir le succès du basculement sur incident, les deux appliances conservent leurs configurations synchronisées. Dans une configuration haute disponibilité en mode WCCP, l'appliance qui traite le trafic maintient la communication avec le routeur en amont.

Surveillance de l'état Lorsque la haute disponibilité est activée, l'appliance principale utilise le protocole VRRP pour envoyer un signal de pulsation à l'appliance secondaire une fois par seconde. En outre, l'appliance principale surveille l'état de l'opérateur de ses ports Ethernet. La perte de transporteur sur un port précédemment actif implique une perte de connectivité.

Basculement Si le signal de pulsation de l'appliance principale doit échouer ou si l'appliance principale perd son opérateur pendant cinq secondes sur un port Ethernet précédemment actif, l'appliance secondaire prend le relais et devient le principal. Lorsque l'appliance défaillante redémarre, elle devient la solution secondaire. La nouvelle primaire s'annonce sur le réseau avec une diffusion ARP. L'usurpation MAC n'est pas utilisée. Le pontage Ethernet est désactivé sur l'appliance secondaire, laissant la solution principale comme seul chemin d'accès pour le trafic en ligne. Le défaut de connexion au fil est inhibé sur les deux appareils afin d'éviter les boucles.

> **Avertissement**
>
> La fonction de contournement Ethernet est désactivée en mode haute disponibilité. Si les deux appliances d'une paire haute disponibilité en ligne perdent de l'énergie, la connectivité est perdue. Si une connectivité WAN est nécessaire lors de coupures de courant, au moins une appliance doit être connectée à une source d'alimentation de secours.
>
> **Remarque**
>
> l'appliance secondaire de la paire haute disponibilité a un de ses ports de pont, le port apA.1, désactivé pour empêcher les boucles de transfert. Si l'appliance dispose de deux ponts, apB.1 est également désactivé. Dans une installation à un bras, utilisez le port apA.2. Sinon, l'appliance secondaire devient inaccessible lorsque la haute disponibilité est activée.

Affectation primaire/secondaire : si les deux appliances sont redémarrées, la première à s'initialiser complètement devient la principale. Autrement dit, les appliances n'ont pas de rôle assigné, et le premier à devenir disponible prend le relais en tant que principal. L'appliance dont l'adresse IP est la plus élevée sur l'interface utilisée pour le rythme cardiaque VRRP est utilisée comme disjoncteur si les deux sont disponibles en même temps.

Fin de la connexion pendant le basculement : les connexions TCP accélérées et non accélérées sont arrêtées en tant qu'effet secondaire du basculement. Les sessions non TCP ne sont pas affectées, à l'exception du délai causé par la brève période (plusieurs secondes) entre la panne de l'appliance principale et le basculement vers l'appliance secondaire. Les utilisateurs connaissent la fermeture des connexions ouvertes, mais ils peuvent ouvrir de nouvelles connexions.

Synchronisation de la configuration : les deux appliances synchronisent leurs paramètres pour s'assurer que le secondaire est prêt à prendre en charge le principal. Si la configuration de la paire est modifiée via l'interface basée sur le navigateur, l'appliance principale met immédiatement à jour l'appliance secondaire.

la haute disponibilité ne peut pas être activée à moins que les deux appliances exécutent la même version logicielle.

haute disponibilité en mode WCCP : lorsque WCCP est utilisé avec une paire haute disponibilité, l'appliance principale établit la communication avec le routeur. L'appliance utilise son adresse IP de gestion sur apA ou apB, et non son adresse IP virtuelle, pour communiquer avec le routeur. Lors du basculement, le nouveau dispositif principal établit la communication WCCP avec le routeur.

Exigences de câblage

April 9, 2021

Les deux appliances de la paire haute disponibilité sont installées sur le même sous-réseau dans un arrangement parallèle ou un arrangement à un bras, tous deux illustrés dans la figure suivante. Dans un arrangement à un bras, utilisez le port apA.2 (et, éventuellement, le port apB.2), pas le port apA.1. Certains modèles nécessitent un réseau local de gestion distinct, qu'il s'agisse d'un déploiement en ligne ou d'un seul bras. Ceci est représenté uniquement dans le diagramme du milieu.

Figure 1. Câblage pour paires haute disponibilité

Ne cassez pas la topologie ci-dessus avec des commutateurs supplémentaires. Les arrangements de commutateurs aléatoires ne sont pas pris en charge. Chacun des commutateurs doit être un seul commutateur monolithique, un seul commutateur logique ou une partie du même châssis.

Si le protocole spanning-tree (STP) est activé sur les ports du routeur ou du commutateur connectés aux appliances, le basculement fonctionnera, mais le temps de basculement peut passer à environ trente secondes. Sans STP, le temps de basculement est d'environ cinq secondes. Ainsi, pour atteindre l'intervalle de basculement le plus court possible, désactivez STP sur les ports se connectant aux appliances.

Autres exigences

April 9, 2021

Les deux appliances d'une paire haute disponibilité doivent répondre aux critères suivants :

- Avoir un matériel identique, comme indiqué dans l'entrée Matériel système de la page Tableau de bord.
- Exécutez exactement la même version de logiciel.
- Être équipé de cartes de contournement Ethernet. Pour déterminer ce qui est installé dans vos appliances, consultez la page Tableau de bord.

Les appliances qui ne prennent pas en charge la haute disponibilité affichent un avertissement sur la page Configuration : Haute disponibilité.

Gestion de l'accès à la paire haute disponibilité

April 9, 2021

Lors de la configuration d'une paire haute disponibilité (haute disponibilité), vous lui attribuez une adresse IP virtuelle (VIP) qui vous permet de gérer les deux appliances comme s'il s'agissait d'une seule unité. Après avoir activé le mode haute disponibilité, la gestion de l'appliance secondaire via

son adresse IP est généralement désactivée, la plupart des paramètres étant grisés. Un message d'avertissement affiche la raison sur chaque page. Utilisez le VIP haute disponibilité pour toutes les tâches de gestion. Vous pouvez toutefois désactiver l'état de haute disponibilité de l'appliance secondaire à partir de son interface utilisateur de gestion.

Configuration de la paire haute disponibilité

April 9, 2021

Vous pouvez configurer deux appliances nouvellement installées en tant que paire haute disponibilité ou créer une paire haute disponibilité en ajoutant une seconde appliance à une installation existante.

Conditions préalables : Installation physique et procédures de configuration de base

Pour configurer la haute disponibilité

1. Assurez-vous qu'au plus une appliance est connectée aux réseaux de trafic (sur les ponts accélérés). Si les deux sont connectés, déconnectez un câble de pont des ponts actifs de la seconde appliance. Cela empêchera les boucles de transfert.
2. Dans la page Fonctionnalités de la première appliance, désactivez le traitement du trafic. Cela désactive l'accélération jusqu'à ce que la paire haute disponibilité soit configurée.
3. Répétez l'opération pour la deuxième appliance.
4. Sur la première appliance, accédez à l'onglet Configuration : Déploiements avancés : Haute disponibilité, voir ci-dessous.
5. Activez la case à cocher Activé.
6. Cliquez sur le lien Configurer l'adresse IP virtuelle haute disponibilité et attribuez une adresse IP virtuelle à l'interface apA. Cette adresse sera utilisée ultérieurement pour contrôler les deux appliances en tant qu'unité.
7. Revenez à la page Haute disponibilité et, dans le champ VRID VRRP, affectez un ID VRRP à la paire. Bien que la valeur par défaut soit zéro, la plage valide des numéros d'identification VRRP est de 1 à 255. Dans cette plage, vous pouvez spécifier n'importe quelle valeur qui n'appartient pas à un autre périphérique VRRP de votre réseau.
8. Dans le champ Nom commun SSL du partenaire, tapez le nom commun SSL de l'autre appliance, qui s'affiche sous l'onglet Configuration : Déploiements avancés : Haute disponibilité, dans le champ Nom commun SSL du partenaire. Les informations d'identification SSL utilisées ici sont installées en usine.
9. Cliquez sur Update.
10. Répétez les étapes 3 à 8 sur la seconde appliance. Si vous gérez l'appliance via un pont accéléré (tel qu'apA), vous devrez peut-être reconnecter le câble Ethernet que vous avez retiré à l'étape

1 pour vous connecter à la seconde appliance. Si tel est le cas, branchez ce câble et déconnectez le câble correspondant sur le premier appareil.

11. Avec votre navigateur, accédez à l'adresse IP virtuelle de la paire haute disponibilité. Activez le traitement du trafic sur la page Fonctionnalités. Toute autre configuration sera effectuée à partir de cette adresse virtuelle.
12. Branchez le câble qui a été déconnecté.
13. Sur chaque appliance, la page Configuration : Déploiements avancés : Haute disponibilité doit désormais indiquer que la haute disponibilité est active, qu'une appliance est la principale et que l'autre est la seconde. Si ce n'est pas le cas, une bannière d'avertissement apparaît en haut de l'écran, indiquant la nature du problème.

Figure 1. Page de configuration haute disponibilité

Mise à jour du logiciel sur une paire haute disponibilité

April 9, 2021

La mise à jour du logiciel SD-WAN sur une paire haute disponibilité provoque un basculement à un moment donné pendant la mise à jour.

Remarque : Cliquer sur le bouton Mettre à jour met fin à toutes les connexions TCP ouvertes.

Pour mettre à jour le logiciel sur une paire haute disponibilité

1. Ouvrez une session sur les deux appliances.
2. Sur l'appliance secondaire, mettez à jour le logiciel et redémarrez. Après le redémarrage, l'appliance reste la solution secondaire. Vérifiez que l'installation a réussi. L'appliance principale doit indiquer que l'appliance secondaire existe mais que la synchronisation automatique des paramètres ne fonctionne pas, en raison d'une incompatibilité de version.
3. Sur l'appliance principale, mettez à jour le logiciel, puis redémarrez. Le redémarrage entraîne un basculement sur incident et l'appliance secondaire devient la principale. Une fois le redémarrage terminé, la haute disponibilité doit être pleinement établie, car les deux appliances exécutent le même logiciel.

Sauvegarde et restauration des paramètres d'une paire haute disponibilité

April 9, 2021

La fonction Maintenance du système : Sauvegarde/Restauration peut être utilisée pour enregistrer et restaurer les paramètres d'une paire haute disponibilité comme suit :

Pour sauvegarder les paramètres

Utilisez la fonction de sauvegarde comme d'habitude. Autrement dit, connectez-vous à l'interface graphique via l'adresse VIP haute disponibilité (comme c'est normal lors de la gestion de la paire haute disponibilité) et, sur la page Gestion du système : Sauvegarde/Restaurer, cliquez sur Paramètres de téléchargement.

Pour restaurer les paramètres

1. Désactivez la haute disponibilité sur les deux appliances en désactivant la case à cocher Activé de l'onglet Configuration : Déploiements avancés : Haute disponibilité (haute disponibilité).
2. Débranchez un câble réseau du pont d'une appliance. (Appelez-le « Appliance A. »)
3. Débranchez le cordon d'alimentation de l'appliance A.
4. Restaurez les paramètres de l'autre appliance (Appliance B) en téléchargeant un jeu de paramètres précédemment enregistré sur la page Maintenance du système : Sauvegarde/Restaurer, puis en cliquant sur Restaurer les paramètres. (L'exécution de cette opération nécessite un redémarrage, ce qui réactive la haute disponibilité).
5. Attendez le redémarrage de l'appliance B. Il devient le primaire.
6. Redémarrez l'appliance A.
7. Connectez-vous à l'interface graphique de l'appliance A et réactivez la haute disponibilité sous l'onglet Configuration : Déploiements avancés : Haute disponibilité (haute disponibilité). L'appliance obtient ses paramètres à partir du système principal.
8. Branchez le câble réseau retiré à l'étape 2.

Les deux appliances sont désormais restaurées et synchronisées.

Dépannage des paires haute disponibilité

April 9, 2021

Si les appliances signalent un échec d'entrée en mode haute disponibilité, le message d'erreur en notera également la cause. Voici quelques problèmes qui peuvent interférer avec le mode haute disponibilité :

- L'autre appliance n'est pas en cours d'exécution.
- Les paramètres de haute disponibilité des deux appliances ne sont pas identiques.
- Les deux appliances n'exécutent pas la même version logicielle.
- Les deux appareils n'ont pas le même numéro de modèle.
- Un câblage incorrect ou incomplet entre les appliances ne permet pas aux pulsations de haute disponibilité de passer entre elles.
- Les certificats SSL en mode groupe haute disponibilité/haute disponibilité sur une ou les deux appliances sont endommagés ou manquants.

Mode deux appliances

April 9, 2021

Le mode Two Box est un déploiement WCCP basé sur un bras où l'appliance SD-WAN SE agit comme un routeur WCCP et les appliances SDWAN-WANOP (4000/5000) agissent en tant que clients WCCP et aident à établir la convergence WCCP. De cette façon, tous les paquets TCP orientés chemin d'accès virtuel/service Intranet atteignant l'appliance SD-WAN SE sont redirigés vers l'appliance SDWAN-WANOP pour des avantages d'optimisation en offrant des avantages à la fois SD-WAN SE et WANOP pour le trafic client.

Le mode Two Box n'est pris en charge que sur les modèles d'appliance suivants :

- Appliances SD-WAN SE —4000, 4100 et 5100
- Appareils WANOP SD-WAN —4000, 4100, 5000 et 5100

> **Remarque**
>
> Les modes de déploiement haute disponibilité et WCCP ne sont pas accessibles lorsque le mode Two Box est activé. Toutefois, ces modes de déploiement sont disponibles pour l'utilisateur à administrer.
>
> **Important**
>
> - Bien que le déploiement WCCP hérité soit désactivé lorsque le mode Two Box est activé, la convergence des groupes de services ne peut être vérifiée qu'à partir de la page de surveillance WCCP. Il n'y a pas de page GUI distincte dans la section Surveillance pour le mode Two Box.

- Si le processus WCCP exécuté sur l'appliance Standard Edition redémarre plusieurs fois dans un court laps de temps, par exemple, 3 fois par minute, le groupe de service s'arrête automatiquement. Dans un tel scénario, pour obtenir la convergence WCCP sur l'appliance WANOP, réactivez la fonctionnalité WCCP dans l'interface graphique Web de l'appliance WANOP.
- En cas de modification de la configuration WCCP ou de l'optimisation WAN liée à la configuration sur l'appliance Standard Edition, l'appliance WANOP externe redémarre. Par exemple, l'activation ou la désactivation de la case WCCP dans le groupe d'interface de l'éditeur de configuration suivi du processus de gestion des modifications redémarre également l'appliance WANOP.

Remarque

Notez également les points suivants à prendre en compte lors de la mise en œuvre du mode à deux boîtes :

- Lorsqu'un domaine de routage est sélectionné pour être redirigé vers l'appliance WANOP à partir de l'éditeur de configuration, il doit être ajouté dans le groupe d'interface pour lequel WCCP est activé.
- Le trafic du même domaine de routage doit également être sélectionné sur le site partenaire. Par exemple, **MCN** > **Branch01** pour observer les avantages de l'optimisation WAN.
- Si un domaine de routage est sélectionné dans le groupe d'interface sur lequel WCCP est activé, un autre groupe d'interface contenant les interfaces pontées doit avoir le même domaine de routage configuré. Ce n'est que si le groupe d'interface WCCP a configuré le domaine de routage qu'il ne suffit pas de transmettre le trafic de bout en bout avec des avantages d'optimisation WAN.

Citrix SD-WAN édition standard

Pour configurer une solution en mode deux boîtes dans l'appliance Standard Edition sur le site de contrôleur de domaine ou de succursale :

1. Dans l'interface de gestion Web SD-WAN SE, accédez à **Configuration** > **Réseau étendu virtuel** > **Éditeur de configuration**. Ouvrez un package de configuration existant ou créez un package.
2. Dans le package de configuration choisi, accédez à l'onglet **Avancé** pour afficher les détails de configuration.
3. Ouvrez Paramètres **globaux** et développez **Domaines de routage** pour afficher que la case **Redirection vers WANOP** est activée.
4. Développez contrôleur de domaine pour activer **WCCP** pour l'**interface virtuelle** sous Paramètres **du groupe d'interface** qui indiquent l'interface réseau virtuelle pour laquelle l'

appliance est activée.

5. Développez **Sites+ Ajouter** pour afficher le domaine de routage de branche et les paramètres du groupe d'interface. Sous le site de la succursale, la case à cocher **Rediriger vers WANOP** est activée pour les domaines de routage.

> **Remarque**
>
> L'écouteur WCCP doit être activé uniquement pour les interfaces réseau virtuelles pour lesquelles une seule interface Ethernet est configurée. N'activez pas l'écouteur WCCP sur une paire BRIDGED. Il est destiné à être activé sur l'interface ONE-ARM entre les appliances SD-WAN SE et SD-WAN WANOP.

Configuration de Citrix SD-WAN WANOP

Pour configurer le mode de déploiement bibox dans l'interface graphique Web de l'appliance WANOP SD-WAN :

1. Dans l'interface de gestion Web WANOP SD-WAN, accédez à **Configuration** > **Paramètres de l'appliance** > **Déploiements avancés** > **Solution à deux boîtes**.
2. Cliquez sur l'icône **Modifier** pour modifier les paramètres du mode à deux cases. La boîte de dialogue d'informations sur **les adresses IP du cache** s'affiche. Cliquez sur **OK**.
3. Activez la **case à cocher Deux cases activées**.
4. Entrez l'**adresse IP homologue**. L'adresse IP homologue est l'adresse IP de l'appliance SD-WAN Standard Edition.
5. Entrez les informations d'identification de l'utilisateur et cliquez sur **Appliquer**.

Configuration et facilité de gestion en mode Two Box

Voici quelques-uns des deux points de configuration et de gérabilité en mode boîte à prendre en compte pour le déploiement :

- Les configurations WANOP SD-WAN mentionnées ci-dessous peuvent être configurées à partir de l'éditeur de configuration SD-WAN SE sous la forme d'un volet unifié
  - CLASSE DE SERVICE
  - CLASSIFICATEUR D'APPLICATIONS
  - FONCTIONNALITÉS
  - RÉGLAGE DU SYSTÈME

Surveillance

Vous pouvez surveiller le trafic WANOP SD-WAN directement à l'aide de la page Surveillance de l'interface Web de l'appliance SD-WAN SE. Cela permet de surveiller à la fois les appliances SDWAN-SE et SDWAN-WO lors du traitement du trafic de données. Vous pouvez afficher les détails de connexion, les détails des partenaires sécurisés, etc., sous le nœud d'optimisation WAN dans l'interface utilisateur SDWAN-SE.

Configuration

Vous pouvez configurer APPFLOW directement à partir de la page **Configuration** SDWAN-SE sous le nœud **APPFLOW**. Cela permet à SDWAN-SE d'agir comme un seul volet pour la configuration d'APPFLOW et d'autres attributs de configuration de traitement des données tels que Classe de service et Classificateurs d'applications. La configuration effectuée sur SDWAN-SE reflète sur la configuration SDWAN-WO, en maintenant la prise en charge transparente des fonctionnalités APPFLOW.

Le WANOP SD-WAN déjà découvert par Citrix Application Delivery Management (ADM), s'il est utilisé en mode Two Box, doit être isolé et non configuré à l'aide de Citrix ADM tant que ce mode n'est pas désactivé. Cela est dû au fait que la configuration de WANOP pour le traitement du trafic est gérée par l'appliance SD-WAN SE en mode Two Box.

Les optimisations avancées ou l'accélération sécurisée doivent être configurées directement sur l'appliance SDWAN-SE comme nous le ferions sur l'appliance SDWAN-WO. Cela permet de maintenir un seul volet de configuration de configurations telles que la jointure de domaine ou la création de profils Secure Acceleration/SSL pour les optimisations avancées ou le proxy SSL.

- Les licences doivent être gérées séparément pour chacune des appliances SD-WAN SE et SD-WAN WANOP.
- La mise à niveau logicielle doit être gérée séparément pour chacune des appliances SD-WAN SE et SD-WAN WANOP avec les progiciels correspondants. Par exemple, tar.gz pour SD-WAN SE et mise à niveau upg pour SD-WAN WANOP.
- L'intégration des chemins de données doit être configurée entre les appliances SD-WAN SE et WANOP externes via le mode de déploiement WCCP.
    - Au niveau du chemin de données, les fonctionnalités WCCP et Virtual WAN sont offertes grâce à l'intégration de chemin de données entre WANOP et SE en externe en mode mono-bras pour obtenir des avantages d'optimisation.

Configuration et surveillance unifiées

Lorsque vous activez le mode deux boîtiers avec les appliances SD-WAN SE et SDWAN-WANOP, vous pouvez afficher la configuration dans l'appliance SD-WAN SE de la même manière que la configuration à deux boîtiers avec l'appliance SD-WAN-EE.

1. Accédez à **Configuration** > **Réseau étendu virtuel** > **Optimisation WAN**
2. Nœud Appflow sous **Configuration** > **Paramètres de l'appliance**
3. Nœud d'optimisation WAN sous Configuration.

   Ces informations sont redirigées depuis l'appliance WANOP SD-WAN qui est en mode Deux boîtes avec l'appliance SD-WAN SE.

   La configuration liée à WANOP, telle que SSL Acceleration et AppFlow, peut désormais être effectuée à partir de l'interface graphique Web SD-WAN SE.

   Les statistiques relatives au trafic, telles que Connexions, Compression, CIFS/SMB, ICA Advanced, MAPI et partenaires, peuvent désormais être surveillées à partir de l'interface graphique Web SD-WAN SE sous **Monitoring** > **Optimisation WAN**, similaire à l'appliance SD-WAN Premium (Enterprise) edition.

Changement d'adresse IP de gestion pour l'appliance WANOP SD-WAN en mode deux boîtes

Pour modifier l'adresse IP de gestion de l'appliance SDWAN-WANOP en mode Deux boîtes :

1. Exécutez la commande *clear_wo_sync* sur l'appliance SD-WAN SE. Il garantit que les informations d'adresse IP WANOP SD-WAN sont effacées pour la redirection de l'interface graphique.
2. Désactivez et activez la configuration en mode deux boîtes sur l'appliance WANOP SD-WAN. La nouvelle adresse IP (IP modifiée) de l'appliance WANOP SD-WAN est envoyée à SD-WAN SE. La nouvelle adresse IP modifiée est affichée dans les pages de redirection d'URL.

L'adresse IP de gestion est utilisée pour la configuration de l'adresse IP homologue.

Désactiver le mode deux boîtes sur le dispositif WANOP SD-WAN

Pour désactiver ou dissocier les appliances SD-WAN WANOP et SD-WAN SE du mode Two Box :

1. Désactivez le mode Two Box de l'appliance WANOP SD-WAN.
2. Il est prévu que l'appliance SD-WAN WANOP affiche deux pages en mode boîte dans l'interface graphique Web SD-WAN SE. Pour effacer ces pages, exécutez la commande : *clear_wo_sync*.

Questions fréquentes

April 23, 2021

Accélération

April 9, 2021

L'accélération utilise-t-elle un tunnel ?

Non, l'accélération est transparente et utilise les mêmes adresses IP et numéros de port que la connexion d'origine. Cela permet à vos méthodes de surveillance actuelles de continuer à fonctionner normalement.

Comment l'accélération modifie-t-elle le flux de paquets ?

Avec les connexions non compressées, l'accélération ajoute des options à l'en-tête TCP du paquet, mais laisse la charge utile du paquet intacte. Ces options permettent aux périphériques Citrix SD-WAN WANOP à chaque extrémité de la connexion de communiquer entre eux. En outre, le numéro de séquence TCP est ajusté pour empêcher les problèmes de routage ou les défaillances de l'appliance de mélanger des paquets accélérés et des paquets non accélérés dans la même connexion.

Avec les connexions compressées, la charge utile est compressée et la sortie du compresseur est accumulée en paquets de taille réelle. Le résultat est que, par exemple, la compression 3:1 entraîne la transmission d'un tiers du nombre de paquets, plutôt que le même nombre de paquets, chacun étant réduit à un tiers de taille. La compression utilise également les options d'en-tête TCP de Citrix SD-WAN WANOP et l'ajustement du numéro de séquence.

Quelles sont les exigences de base de l'accélération ?

L'accélération nécessite un périphérique Citrix SD-WAN WANOP aux deux extrémités de la connexion, la connexion doit utiliser le protocole TCP et tous les paquets de la connexion doivent passer par les deux périphériques Citrix SD-WAN WANOP.

CIFS et MAPI

April 23, 2021

Quelles conditions préalables sont requises avant de configurer MAPI et SMB Signé sur une appliance Citrix SD-WAN WANOP ?

Vous devez satisfaire aux conditions suivantes avant de configurer MAPI et SMB signé sur un dispositif Citrix SD-WAN WANOP :

- L'option Secure Peer doit être définie sur True sur le matériel côté client et serveur.
- Un utilisateur délégué doit être ajouté à l'appliance côté centre de données et son état doit être marqué comme « Succès ».
- L'appliance côté centre de données doit joindre le domaine avec succès.
- L'adresse IP DNS configurée sur l'appliance côté serveur doit être accessible.

  Pour de plus amples informations, consultez la section Configurer une appliance Citrix SD-WAN WANOP pour optimiser la sécurité du trafic Windows.

Que dois-je configurer sur le Controller de domaine pour un utilisateur délégué ?

Vous devez créer un utilisateur sur le contrôleur de domaine avant de configurer la délégation pour l'utilisateur sur une appliance Citrix SD-WAN WANOP.

Dois-je configurer quelque chose sur le serveur DNS ?

Oui. Sur le serveur DNS, vous devez configurer les recherches avant et inversées pour toutes les adresses IP des contrôleurs de domaine.

Que dois-je vérifier avant de faire de l'appliance Citrix SD-WAN WANOP pour rejoindre le domaine ?

Avant d'associer l'appliance au domaine, vérifiez les éléments suivants :

- Les adresses IP configurées sur les serveurs DNS principaux ou secondaires doivent être accessibles.
- Le domaine doit être joignable.
- Les adresses IP du domaine résolu doivent être accessibles.
- Eventuellement, l'état de l'utilitaire de vérification de jointure avant domaine doit passer.

Comment puis-je vérifier si l'appliance Citrix SD-WAN WANOP est prête à ajouter un utilisateur en tant qu'utilisateur délégué ?

Vous pouvez vérifier l'utilisateur à l'aide de l'utilitaire Vérifier l'utilisateur délégué sur la page domaine Windows. Si l'état de tous les paramètres ne comporte aucun message d'erreur, l'appliance est prête à ajouter l'utilisateur en tant qu'utilisateur délégué.

Si l'utilitaire affiche des échecs, vous devez les corriger avant d'ajouter un utilisateur en tant qu'utilisateur délégué. Vous pouvez vous référer au journal pour comprendre les résultats du test.

Existe-t-il des exigences pour le nom d'hôte et la longueur du nom d'hôte de l'appliance Citrix SD-WAN WANOP côté serveur ?

Du côté serveur de l'appliance Citrix SD-WAN WANOP, assurez-vous que le nom d'hôte est unique au sein du réseau. En outre, la longueur du nom d'hôte ne doit pas dépasser 15 caractères.

Puis-je configurer l'approbation unidirectionnelle dans le domaine ?

Non. Le client et le serveur doivent être les membres d'un domaine qui a une approbation bidirectionnelle avec le domaine de l'appliance Citrix SD-WAN WANOP côté serveur. L'appliance ne prend pas en charge l'approbation unidirectionnelle.

Puis-je utiliser le client Macintosh Outlook et bénéficier des avantages d'accélération de l'appliance Citrix SD-WAN WANOP ?

Non. Macintosh Outlook n'utilise pas MAPI comme protocole de communication. Par conséquent, vous ne pouvez pas utiliser Macintosh Outlook dans ce programme d'installation.

Dois-je faire en sorte que l'appliance Citrix SD-WAN WANOP côté succursale rejoigne le domaine pour accélérer le chiffrement MAPI ?

Non. Vous n'avez pas besoin de faire en sorte que l'appliance Citrix SD-WAN WANOP côté succursale rejoigne le domaine pour accélérer le chiffrement MAPI.

Puis-je configurer une appliance Citrix SD-WAN WANOP 2000 avec Windows-Server côté datacenter pour une interface MAPI chiffrée ?

Oui. Vous pouvez configurer une appliance Citrix SD-WAN WANOP 2000 avec Windows-Server côté datacenter pour une interface MAPI chiffrée.

Lorsque j'utilise une appliance Citrix SD-WAN WANOP pour rejoindre un domaine et qu'un serveur NTP configuré avec un fuseau horaire différent existe sur le réseau, l'appliance synchronise-t-elle l'heure avec le contrôleur de domaine ou le serveur NTP ?

Lorsque vous associez l'appliance Citrix SD-WAN WANOP à un domaine, l'appliance synchronise toujours son heure avec le contrôleur de domaine et non avec le serveur NTP.

Sur l'appliance Citrix SD-WAN WANOP, quelle est la durée par défaut pour effacer la connexion répertoriée noire ?

Par défaut, les connexions répertoriées en noir sont effacées en 900 secondes.

Quels mécanismes d'authentification Outlook sont pris en charge sur une appliance Citrix SD-WAN WANOP ?

À partir de la version 6.2.4, l'appliance prend en charge l'authentification Negotiate (par défaut) et NTLM v2 Outlook, mais l'authentification Kerberos n'est pas prise en charge. Toutefois, les versions 6.2.3 et antérieures prennent uniquement en charge l'authentification Negotiate Outlook.

Citrix SD-WAN WANOP prend-il en charge Outlook Anywhere, RPC sur HTTPS ?

Oui, à partir de la version 7.3.

Compression

April 9, 2021

Quel est l'avantage de la compression Citrix SD-WAN WANOP ?

Alors que le mécanisme de base de la compression est de réduire les flux de données, l'avantage de cela est de rendre les choses plus rapides. Un fichier plus petit (ou une transaction plus petite) prend moins de temps à transférer. La taille n'a pas d'importance : le point de compression est la vitesse.

Comment les avantages de compression sont-ils mesurés ?

Il existe deux façons de mesurer les avantages de la compression : le temps et le rapport de compression. Les deux sont liés lorsque la liaison WAN est le goulot d'étranglement dominant. Parce que le compresseur Citrix SD-WAN WANOP est très rapide, comprimant les données en temps réel, un fichier qui compresse de 5:1 transfère en un cinquième du temps. Cela reste vrai jusqu'à ce qu'un goulot d'étranglement secondaire soit rencontré. Par exemple, si le client est trop lent pour gérer un transfert à pleine vitesse, un taux de compression de 5:1 offre moins d'une accélération de 5:1.

Comment fonctionne la compression ?

Le moteur de compression conserve les données précédemment transférées sur la liaison, les données les plus récentes étant conservées en mémoire et une quantité beaucoup plus importante sur

le disque. Lorsqu'une chaîne qui a été transférée auparavant est à nouveau rencontrée, elle est remplacée par une référence à la copie précédente. Cette référence est envoyée sur le WAN au lieu de la chaîne réelle, et l'appliance située à l'autre extrémité recherche la référence et la copie dans le flux de sortie.

Quel est le taux de compression maximal réalisable ?

Le taux de compression maximal atteint sur une appliance Citrix SD-WAN WANOP est d'environ 10 000:1.

Quel est le taux de compression attendu ?

Le ratio de compression global est la moyenne de toutes les tentatives de compression des flux de données sur le lien. Certains compresse mieux que d'autres, et d'autres ne se compriment jamais du tout. L'appliance utilise des classes de service pour empêcher l'envoi de flux manifestement non compressibles au compresseur. L'effet de la compression sur différents types de données varie comme suit :

Les données compressées ou chiffrées ponctuelles —les flux qui ne seront plus jamais vus et qui ont déjà été compressés ou chiffrés, tels que les tunnels SSH chiffrés et la surveillance en temps réel des caméras vidéo —ne sont pas compressés, car leurs flux de données ne sont jamais les mêmes deux fois.

Les données binaires compressées ou chiffrées qui sont vues plus d'une fois se compriment très bien sur le deuxième transfert et les transferts suivants, avec des rapports de compression de l'ordre de centaines à milliers pour un sur ces transferts ultérieurs. Lors du premier transfert, ils ne se compriment pas. Le taux de compression moyen de ces données dépend de la fréquence à laquelle les données sont vues plus d'une fois. Alors que les transferts individuels montrent parfois des rapports de compression supérieurs à 1 000:1, les moyennes pour les données binaires compressées sur la liaison se situent entre 1.5:1 et 5:1 sur la plupart des liaisons, avec des moyennes supérieures à 10:1 sur certaines liaisons, selon la nature du trafic.

Les flux de texte et les données binaires non compressées/non chiffrées se compriment même lors de la première passe. Les flux de texte se compriment bien car même les textes non liés ont de nombreuses sous-chaînes en commun. Ceci est vrai pour les documents, le code source, les pages HTML, etc. La compression du premier passage de l'ordre de 1.5:1 à 4:1 sont courantes. Lors de la deuxième et des passes suivantes, ils compriment presque aussi bien les données binaires compressées (100:1 ou plus). Les données binaires non compressées sont variables, mais elles sont souvent mieux comprimées que le texte. Des exemples de données binaires non compressées incluent des images de CD, des fichiers exécutables et des formats image, audio et vidéo non compressés. Lors de la deuxième et des passes suivantes, ils compriment aussi bien les données binaires compressées.

Les données Citrix Virtual Apps and Desktops se compriment particulièrement bien avec les transferts de fichiers, la sortie d'imprimante et la vidéo, à condition que les mêmes flux de données aient déjà traversé le lien. En raison de la surcharge du protocole, la compression maximale est d'environ 40:1,

et la compression moyenne est probablement proche de 3:1. Les flux de données interactifs, tels que les mises à jour d'écran), donnent des résultats de compression de l'ordre de 2:1.

Quelle est la différence entre la mise en cache et la compression ?

La mise en cache enregistre des objets nommés entiers sur l'appliance côté client. Le nom peut être un chemin d'accès et un nom de fichier dans le cas de la mise en cache du système de fichiers, ou une URL dans le cas de la mise en cache Web. Si vous transférez un objet identique avec un nom différent, le cache n'offre aucun avantage. Si vous transférez un objet portant le même nom qu'un objet mis en cache, mais avec de légères différences de contenu, le cache n'offre aucun avantage. Si l'objet peut être servi à partir du cache, il n'est pas récupéré à partir du serveur.

La compression, d'autre part, n'a pas de concept de noms d'objets, et a fourni un avantage chaque fois qu'une chaîne dans le transfert correspond à une chaîne qui est déjà dans l'historique de compression. Cela signifie que si vous téléchargez un fichier, modifiez 1% de son contenu et téléchargez le nouveau fichier, vous pouvez obtenir une compression de 99:1 sur le téléchargement. Si vous téléchargez un fichier et que vous le téléchargez dans un autre répertoire sur le site distant, vous pouvez également obtenir un taux de compression élevé. La compression ne nécessite pas de verrouillage des fichiers et ne souffre pas d'obsolescence. L'objet est toujours récupéré à partir du serveur et est donc toujours correct octet pour octet.

RPC sur HTTPS

April 9, 2021

Est-il obligatoire de créer une classe de service pour accélérer les connexions RPC sur HTTPS ?

La création d'une nouvelle classe de services est une tâche facultative. Vous pouvez utiliser une classe de service HTTPS existante. Toutefois, pour créer des rapports spécifiquement pour les connexions RPC sur HTTPS, vous devez créer une nouvelle classe de service et y lier le profil SSL. Si vous ne souhaitez pas créer de classe de service pour les connexions RPC sur HTTPS, vous pouvez lier le profil SSL que vous avez créé à la classe de service Web (Private-Secure).

Je n'ai créé aucune classe de service pour le RPC sur les applications HTTPS. Comment cela affectera-t-il le rapport du RPC sur les connexions HTTPS ?

Lorsque vous mettez à niveau l'appliance vers la version 7.3, les applications RPC sur HTTPS créées n'appartiennent à aucune classe de service. Par conséquent, toutes les connexions RPC sur HTTPS sont répertoriées en tant que connexions TCP Other dans les rapports. Si vous souhaitez classer ces connexions en tant que connexions RPC sur HTTPS, vous devez créer une classe de service pour ces applications.

Existe-t-il une classe de service par défaut pour RPC sur HTTPS sur l'appliance ?

Non. L'appliance ne comporte que des applications par défaut, et non des classes de service par défaut. Vous devez créer la classe de service pour une application.

L'appliance offre-t-elle des avantages de compression SSL au RPC par rapport aux connexions HTTPS ?

Non. L'appliance ne fournit aucun avantage de compression SSL au RPC par rapport aux connexions HTTP. Les avantages de compression ne sont disponibles que pour le chiffrement et le déchiffrement du trafic HTTPS.

Semblable à MAPI, l'appliance optimise la latence pour les connexions RPC sur HTTPS ?

Non. L'appliance n'optimise pas la latence pour RPC sur HTTPS.

MAPI sur HTTP est-il différent de RPC sur HTTPS ?

Oui. MAPI sur HTTP est un nouveau protocole pris en charge sur Microsoft Exchange Server 2013 SP1 ou version ultérieure.

Quelle est la différence entre les paramètres RPC sur HTTPS sur les appliances Citrix SD-WAN WANOP côté client et côté serveur ?

À l'exception de la création d'une classe de service et de l'ajout d'applications RPC sur HTTPS, vous n'avez pas besoin de configuration supplémentaire sur une appliance Citrix SD-WAN WANOP côté client.

Que se passe-t-il si je configure le profil SSL en mode proxy transparent ?

Certains serveurs Exchange nécessitent la prise en charge des tickets de session TLS. Pour accélérer les connexions à ces serveurs, vous devez créer un profil SSL avec proxy divisé, car le mode proxy transparent ne prend pas en charge les tickets de session TLS.

Si une configuration d'équilibrage de charge est utilisée pour Microsoft Exchange Server, quelle adresse IP de destination dois-je ajouter à la règle de filtre lors de la création d'une classe de service RPC sur HTTPS ?

Si vous utilisez un dispositif d'équilibrage de charge, ajoutez son adresse IP virtuelle (VIP) à la règle de filtre lors de la création d'une classe de service RPC sur HTTP.

Comment puis-je faire la différence entre le trafic MAP et RPC sur HTTPS dans la page Outlook (MAPI) ?

Vous pouvez différencier le trafic en fonction des applications affichées sur la page Outlook (MAPI). Par exemple, MAPI et RPC sur HTTPS sont utilisés pour les applications suivantes :

- **MAPI** : MAPI et eMAPI
- **RPC sur HTTPS** : HTTP MAPI, HTTP eMAPI, HTTPS MAPI et HTTPS eMAPI

SCPS

April 9, 2021

Qu'est-ce que le protocole SCPS ?

Le protocole SCPS (Space Communications Protocol Standard) est une variante du protocole TCP.

Quelle est l'utilisation du protocole SCPS ?

Le protocole SCPS est utilisé dans les communications par satellite et des applications similaires.

Le**protocole SCPS est-il pris en charge sur une appliance Citrix SD-WAN WANOP** ?

Oui. L'appliance Citrix SD-WAN WANOP prend en charge le protocole SCPS et accélèrent les données transférées à l'aide de ce protocole.

Puis-je utiliser une appliance SCPS avec une appliance non compatible SCPS ?

Oui. Si vous devez mélanger des appliances compatibles SCPS avec des appliances non compatibles SCPS, déployez-les de manière à éviter les incohérences. Vous pouvez utiliser des règles de classe de service basées sur IP ou organiser le déploiement de sorte que chaque chemin d'accès ait des appliances correspondantes.

Que se passe-t-il si j'utilise une appliance SCPS à une extrémité une appliance non compatible SCPS à l'autre extrémité du lien ?

Si SCPS est activé sur l'appliance à une extrémité de la connexion et que ce n'est pas le cas, les performances de retransmission en souffrent. Cette condition provoque également une alerte « Discordance du mode SCPS ».

Quelle est la différence entre le comportement d'une appliance compatible SCPS et celui d'une appliance par défaut ?

La principale différence entre un dispositif activé SCPS et le comportement par défaut est que les « accusés de réception négatifs sélectifs » (SNACK) de type SCPS sont utilisés à la place des accusés de réception sélective standard (SACK).

Peering sécurisé

April 9, 2021

Quelles fonctionnalités Citrix SD-WAN WANOP nécessitaient un appairage sécurisé ?

Vous devez établir un appairage sécurisé entre les appliances Citrix SD-WAN WANOP à deux extrémités de la liaison lorsque vous envisagez d'utiliser l'une des fonctionnalités suivantes :

- Compression SSL
- Prise en charge CIFS signée
- Prise en charge des MAPI chiffrées

Dois-je envisager quelque chose avant de configurer un tunnel sécurisé ?

Oui. Vous devez commander et recevoir une licence de crypto avant de pouvoir configurer un tunnel sécurisé entre les appliances Citrix SD-WAN WANOP aux extrémités du lien.

Que se passe-t-il lorsque vous activez l'appairage sécurisé sur une appliance à une extrémité de la liaison ?

Lorsque vous activez l'appairage sécurisé sur une appliance Citrix SD-WAN WANOP à une extrémité de la liaison, l'autre appliance la détecte et tente d'ouvrir un tunnel de signalisation SSL. Si les deux appliances s'authentifient mutuellement via ce tunnel, les appliances disposent d'une relation d'appairage sécurisée. Toutes les connexions accélérées entre les deux appliances sont chiffrées et la compression est activée.

Que se passe-t-il lorsque je n'active pas l'appairage sécurisé sur l'appliance partenaire ?

Lorsqu'une appliance a activé le peering sécurisé, les connexions avec un partenaire pour lequel elle n'a pas de relation homologue sécurisée ne sont ni chiffrées ni compressées, bien que l'accélération du contrôle de flux TCP soit toujours disponible. La compression est désactivée pour garantir que les données stockées dans l'historique de compression des partenaires sécurisés ne peuvent pas être partagées avec des partenaires non sécurisés.

Pourquoi ai-je besoin d'un mot de passe de keystore ?

Vous avez besoin d'un mot de passe de keystore pour accéder aux paramètres de sécurité. Ce mot de passe est différent du mot de passe de l'administrateur et permet de séparer l'administration de la sécurité des autres tâches. Si le mot de passe du keystore est réinitialisé, toutes les données cryptées et les clés privées existantes sont perdues.

Pour protéger les données, même en cas de vol de l'appliance, le mot de passe du magasin de clés doit être réentré chaque fois que l'appliance est redémarrée. Jusqu'à ce que cela soit fait, le peering sécurisé et la compression sont désactivés.

l'appliance Citrix SD-WAN WANOP que j'ai reçue de Citrix contient-elle des clés et un certificat permettant de configurer un tunnel sécurisé ?

Non. Les produits Citrix SD-WAN WANOP sont expédiés sans les clés et certificats requis pour le tunnel de signalisation SSL. Vous devez les générer vous-même.

Accélération SSL

April 9, 2021

L'accélération utilise-t-elle un tunnel ?

Non, l'accélération est transparente et utilise les mêmes adresses IP et numéros de port que la connexion d'origine. Cela permet à vos méthodes de surveillance actuelles de continuer à fonctionner normalement.

Comment l'accélération modifie-t-elle le flux de paquets ?

Avec les connexions non compressées, l'accélération ajoute des options à l'en-tête TCP du paquet, mais laisse la charge utile du paquet intacte. Ces options permettent aux périphériques Citrix SD-WAN WANOP à chaque extrémité de la connexion de communiquer entre eux. En outre, le numéro de séquence TCP est ajusté pour empêcher les problèmes de routage ou les défaillances de l'appliance de mélanger des paquets accélérés et des paquets non accélérés dans la même connexion.

Avec les connexions compressées, la charge utile est compressée et la sortie du compresseur est accumulée en paquets de taille réelle. Le résultat est que, par exemple, la compression 3:1 entraîne la transmission d'un tiers du nombre de paquets, plutôt que le même nombre de paquets, chacun étant réduit à un tiers de taille. La compression utilise également les options d'en-tête TCP de Citrix SD-WAN WANOP et l'ajustement du numéro de séquence.

Quelles sont les exigences de base de l'accélération ?

L'accélération nécessite un périphérique Citrix SD-WAN WANOP aux deux extrémités de la connexion, la connexion doit utiliser le protocole TCP et tous les paquets de la connexion doivent passer par les deux périphériques Citrix SD-WAN WANOP.

Plug-in Citrix SD-WAN WANOP

April 23, 2021

Quelles méthodes puis-je utiliser pour installer le plug-in Citrix SD-WAN WANOP sur mon ordinateur ?

Vous pouvez utiliser l'une des méthodes suivantes pour installer le plug-in Citrix SD-WAN WANOP sur votre ordinateur :

- Installation autonome : exécutez le fichier Microsoft Installer (msi).
- Installation silencieuse : exécutez la commande suivante :


```
*\> msiexec.exe /i path\\CitrixSD-WANWANOPPluginReleasex64-\<
Release\\_Nunmer\> /qn*
```

- Installation à distance : installez le plug-in Citrix SD-WAN WANOP à distance à partir de Citrix Receiver. Cette installation se fait à l'aide du serveur de merchandising.

Puis-je personnaliser le programme d'installation du plug-in Citrix SD-WAN WANOP ?

Oui. Vous pouvez personnaliser l'adresse IP de signalisation et la taille de compression basée sur disque (DBC) à l'aide du fichier msi pour le plug-in Citrix SD-WAN WANOP.

Quelle est la configuration matérielle minimale requise pour installer le plug-in Citrix SD-WAN WANOP ?

Pour le plug-in Citrix SD-WAN WANOP, votre ordinateur doit répondre aux exigences suivantes :

- CPU classe Pentium 4
- Minimum 4 Go de RAM
- Minimum 2 Go pour l'espace disque libre

Sur quels systèmes d'exploitation puis-je installer le plug-in Citrix SD-WAN WANOP ?

Vous pouvez installer le plug-in Citrix SD-WAN WANOP sur les systèmes d'exploitation suivants :

OS	Édition	Version
Windows XP	Accueil, Professionnel	32 bits
Windows Vista	Édition Familiale Basique, Édition Familiale Premium, Entreprise, Édition Intégrale	32 bits
Windows 7	Édition Familiale Basique, Édition Familiale Premium, Entreprise, Édition Intégrale	32 bits, 64 bits
Windows 8	Professionnel, Entreprise	32 bits, 64 bits
Windows 10	Professionnel, Entreprise	32 bits, 64 bits

Quelles précautions dois-je prendre avant d'installer le plug-in Citrix SD-WAN WANOP ?

Avant d'installer le plug-in Citrix SD-WAN WANOP sur votre ordinateur, prenez les précautions suivantes :

- En fonction de la version de votre système d'exploitation, téléchargez la version du programme d'installation Citrix SD-WAN WANOP 32 bits ou 64 bits.

- Vous ne pouvez pas installer le plug-in Citrix SD-WAN WANOP sur un lecteur ou un dossier compressé.
- Assurez-vous que l'ordinateur dispose d'un espace disque suffisant.
- Vous ne pouvez pas rétrograder la version du plug-in Citrix SD-WAN WANOP. Si vous souhaitez utiliser une version antérieure de Citrix SD-WAN WANOP, vous devez désinstaller la version actuelle, puis installer une version antérieure.

Quelles appliances Citrix SD-WAN WANOP prennent en charge le plug-in Citrix SD-WAN WANOP ?

Les appliances Citrix SD-WAN WANOP suivants prennent en charge le plug-in Citrix SD-WAN WANOP :

- SD-WAN WANOP 2000
- Appliance SD-WAN WANOP 2000 avec Windows Server
- SD-WAN WANOP 3000
- SD-WAN WANOP 4000
- SD-WAN WANOP 5000

Quelles appliances Citrix SD-WAN WANOP ne prennent pas en charge le plug-in Citrix SD-WAN WANOP ?

Les appliances Citrix SD-WAN WANOP suivantes ne prennent pas en charge le plug-in Citrix SD-WAN WANOP :

- SD-WAN WANOP 400
- SD-WAN WANOP 700
- SD-WAN WANOP 800
- SD-WAN WANOP 1000 avec Windows Server

Dois-je installer une licence Concurrent (CCU) sur les appliances Citrix SD-WAN WANOP 2000, 3000 et VPX pour utiliser le plug-in Citrix SD-WAN WANOP ?

Oui. Vous devez installer une licence CCU sur les appliances Citrix SD-WAN WANOP 2000, 3000 et VPX pour utiliser le plug-in Citrix SD-WAN WANOP.

Dois-je installer une licence CCU sur les appliances Citrix SD-WAN WANOP 4000 et 5000 pour utiliser le plug-in Citrix SD-WAN WANOP ?

Non. Vous n'avez pas besoin d'installer une licence CCU sur les appliances Citrix SD-WAN WANOP 4000 et 5000 pour utiliser le plug-in Citrix SD-WAN WANOP. La licence de base de l'appliance est suffisante pour que le plug-in Citrix SD-WAN WANOP puisse se connecter à ces appliances.

Quelles sont les recommandations Citrix pour accélérer les sous-réseaux ?

Citrix recommande ce qui suit pour accélérer les sous-réseaux :

- N'utilisez jamais ALL/ALL pour la configuration de l'accélération. Spécifiez les sous-réseaux en fonction des besoins.
- Ne configurez pas l'accélération pour l'adresse VIP Citrix Gateway.

Le plug-in Citrix SD-WAN WANOP est-il pris en charge sur les clients légers Windows ?

Non. Le plug-in Citrix SD-WAN WANOP n'est pas pris en charge sur les clients légers Windows.

Quelles versions Citrix Receiver et Citrix Gateway sont prises en charge avec le plug-in Citrix SD-WAN WANOP ?

Le plug-in Citrix SD-WAN WANOP prend en charge les versions Citrix Receiver 4.1 et Citrix Gateway 10.5.

Quelles fonctionnalités Citrix SD-WAN WANOP ne sont pas prises en charge avec le plug-in Citrix SD-WAN WANOP ?

Le plug-in SD-WAN WANOP Citrix ne prend pas en charge les fonctionnalités Citrix SD-WAN WANOP suivantes :

- Mise en cache de vidéo
- Traffic Shaping
- IPv6

Dois-je configurer des règles d'accélération sur une appliance Citrix SD-WAN WANOP 4000 ou 5000 pour que le plug-in Citrix SD-WAN WANOP puisse fonctionner avec elle ?

Oui. Vous devez configurer des règles d'accélération sur une appliance Citrix SD-WAN WANOP 4000 ou 5000 pour que le plug-in Citrix SD-WAN WANOP puisse fonctionner avec elle.

Quelle est la signification du filtrage des sources des canaux de signalisation ?

En utilisant le filtrage des sources des canaux de signalisation, vous pouvez autoriser ou refuser à un sous-réseau ou une adresse IP spécifique la possibilité de se connecter à l'appliance et de récupérer les règles d'accélération. Le sous-réseau source refusé ne peut pas établir de connexions de signalisation et accélérer le trafic.

Quelle est la signification de la détection LAN ?

Lorsque vous activez la détection du réseau local, cela empêche l'accélération du trafic lorsque le plug-in et l'appliance Citrix SD-WAN WANOP se trouvent sur le même réseau local. L'accélération locale n'est pas souhaitable, car l'application de la limite de bande passante de l'appliance à la connexion locale peut réduire la vitesse du trafic local.

Pour accélérer le trafic, quelle est la valeur RTT minimale recommandée entre le plug-in Citrix SD-WAN WANOP et l'appliance ?

Citrix vous recommande de configurer une valeur de RTT supérieure à n'importe quel RTT (temps ping) sur le LAN local, mais inférieure à la RTT pour tout utilisateur distant. La valeur par défaut de 20 millisecondes convient à la plupart des réseaux.

Quelles conditions dois-je prendre en compte lors de la définition des règles d'accélération pour le plug-in Citrix SD-WAN WANOP ?

Tenez compte des conditions suivantes lors de la définition des règles d'accélération pour le plug-in Citrix SD-WAN WANOP :

- Définissez des règles d'accélération pour tous les sous-réseaux locaux de l'appliance. Ces sous-réseaux sont les sous-réseaux LAN sur le site où l'appliance est installée.
- S'il existe des adresses IP de destination qui ne font pas partie du réseau local, ajoutez des règles d'exclusion pour ces adresses IP. Assurez-vous que les règles d'exclusion des adresses IP précèdent les règles d'accélération du trafic pour les sous-réseaux. Cela inclut les sous-réseaux sur des sites distants avec des adresses IP qui apparaissent locales.
- Si vous avez installé l'appliance en mode Inline avec un VPN et qu'elle fonctionne en mode transparent, vous pouvez configurer l'appliance pour accélérer tout le trafic d'entreprise, et pas seulement le trafic provenant ou destiné au site local. Dans ce cas, les seules connexions accélérées sont entre le plug-in Citrix SD-WAN WANOP et le VPN. L'accélération du trafic entre le plug-in Citrix SD-WAN WANOP et le VPN est optimale.

Où les fichiers de suivi et de plantage du plug-in SD-WAN WANOP de Citrix sont-ils stockés sur l'ordinateur ?

Les fichiers de plantage et de suivi du plug-in Citrix SD-WAN WANOP sont stockés dans les dossiers suivants :

- Fichiers de plantage : C:/ProgramFiles/Citrix/Citrix SD-WAN WANOP
- Fichiers de trace : C:/users/admin/appdata/local/temp

Comment le plug-in Citrix SD-WAN WANOP se connecte-t-il à une paire haute disponibilité ?

Le plug-in Citrix SD-WAN WANOP se connecte toujours à la même adresse IP de signalisation. L'adresse IP de signalisation est liée uniquement à l'appliance principale de la paire haute disponibilité, et non à l'appliance secondaire. Par conséquent, le plug-in Citrix SD-WAN WANOP se connecte toujours à l'appliance principale de la paire haute disponibilité.

Quels modes de déploiement le plug-in SD-WAN WANOP Citrix prend-il en charge ?

Le plug-in Citrix SD-WAN WANOP prend en charge les modes de déploiement suivants :

- En ligne.

- WCCP.
- Haute disponibilité.
- Plug-in Citrix SD-WAN WANOP avec déploiement NAT.
- Plug-in Citrix SD-WAN WANOP avec l'appliance Citrix SD-WAN WANOP en mode WCCP à l'aide d'un proxy ICA.
- Plug-in Citrix SD-WAN WANOP avec l'appliance Citrix SD-WAN WANOP 4000 ou 5000. Dans ce déploiement, le port de gestion (0/1) est connecté au réseau de gestion et l'adresse IP de signalisation se trouve sur un autre réseau.

Comment les paquets s'écoulent-ils en modes transparent et redirecteur ?

En mode transparent, l'appliance Citrix SD-WAN WANOP ne modifie pas l'adresse IP source du paquet. En mode redirecteur, l'appliance Citrix SD-WAN WANOP proxie les serveurs et modifie l'adresse IP des paquets.

> **Remarque**
>
> Citrix recommande le mode transparent pour le déploiement de production.

Comment puis-je établir un tunnel sécurisé entre le plug-in Citrix SD-WAN WANOP et l'appliance ?

Pour établir un tunnel sécurisé entre le plug-in SD-WAN WANOP Citrix et l'appliance, procédez comme suit :

1. Dans l'interface utilisateur du plug-in SD-WAN WANOP Citrix, ouvrez l'onglet **Certificats**.
2. Sélectionnez l'option **Certificat de l'autorité** de certification.
3. Cliquez sur **Importer** et téléchargez le certificat d'autorité de certification correspondant.
4. Sélectionnez un magasin de certificats dans lequel vous souhaitez stocker le certificat.
5. Sélectionnez l'option **Certificat client** .
6. Cliquez sur **Importer**.
7. Sélectionnez les formats de certificat appropriés et téléchargez les certificats pertinents.
8. Stockez les certificats dans un magasin de certificats.
9. Si la clé privée est protégée par mot de passe, saisissez le mot de passe pour déchiffrer la clé privée.
10. Vous devez charger le même certificat d'autorité de certification et la même paire de clés sur l'appliance pour établir un tunnel sécurisé.

Comment puis-je vérifier qu'un tunnel sécurisé est établi ?

Pour vérifier qu'un tunnel sécurisé est établi, procédez comme suit :

1. L'ordinateur sur lequel vous avez installé le plug-in Citrix SD-WAN WANOP, exécutez la commande suivante :

   \> telnet localhost 1362

2. Sur la console, exécutez la commande suivante :

   \> showtunnels

   Voici un exemple de sortie de la commande. Si la sortie inclut le texte sécurisé dans la section Connected Available, un tunnel sécurisé a été établi. Si un tunnel sécurisé n'est pas établi, le texte lit en *clair*.

   ```
   ```
   Tunnels d'exposition
   Tunnels de messages :
     Connected Available:
       172.16.9.100 auto,secure,client,initiator,configured
       CN: mike.199.130

   Connected Available : 1
   Clients: 1 peers: 0
   <!--NeedCopy--> ```
   ```

   Pour plus d'informations sur le plug-in WANOP Citrix SD-WAN, consultez [Citrix SD-WAN WANOP Plug-in] (/en-us/citrix-sd-wan-wanop/current-release/wanopt-plug-in.html).

## Traffic shaping

April 23, 2021

**Qu'est-ce que le traffic shaping Citrix SD-WAN WANOP** ?

Le traffic shaping Citrix SD-WAN WANOP utilise un groupe de stratégies pour définir la priorité du trafic de liaison différent et envoyer le trafic sur la liaison à un taux proche de la vitesse de liaison, mais pas supérieur à cette vitesse. Contrairement à l'accélération, qui s'applique uniquement au trafic TCP/IP, le régulateur de trafic gère tout le trafic sur la liaison.

**Quel est l'avantage du traffic shaping** ?

Le traffic shaping utilise des ressources de liaison réduites en fonction des stratégies que vous définissez, de sorte que le trafic connu pour être important recevra plus de bande passante que le trafic connu pour être sans importance.

 
   ```

Comment le shaper de trafic interagit-il avec le trafic Citrix Virtual Apps and Desktops ?

Le périphérique WANOP Citrix SD-WAN analyse le flux de données Applications/Virtual Desktops et est conscient des différents types de trafic et de ses priorités, favorisant le trafic hautement prioritaire. C'est le seul produit qui peut prioriser les flux ICA chiffrés et fournir un support natif pour MultiStream ICA, qui divise la session d'un utilisateur en quatre connexions avec des priorités différentes.

Qu'est-ce que la mise en file d'attente pondérée ?

Une appliance WANOP Citrix SD-WAN utilise une file d'attente équitable pondérée, qui fournit une file d'attente distincte pour chaque connexion. Avec une file d'attente équitable, une connexion trop rapide ne peut déborder que sa propre file d'attente. Il n'a aucun effet sur les autres connexions.

Quelle est la différence entre la mise en file d'attente pondérée et non pondérée ?

La mise en file d'attente pondérée inclut la possibilité de donner à certains trafic une priorité (poids) plus élevée que d'autres. Le trafic avec un poids de deux reçoit deux fois la bande passante du trafic avec un poids de un. Dans une configuration Citrix SD-WAN WANOP, les pondérations sont affectées dans les stratégies de traffic shaping.

Qu'est-ce qu'une définition de lien ?

Une définition de lien spécifie le trafic associé au lien défini, la bande passante maximale pour permettre le trafic reçu sur la liaison et la bande passante maximale pour le trafic envoyé sur la liaison. La définition identifie également le trafic comme trafic entrant ou sortant et comme trafic côté WAN ou côté LAN.

Quels sont les avantages de la définition de lien ?

Les définitions de liens permettent à l'appliance d'éviter la congestion et la perte de vos liaisons WAN et d'effectuer le traffic shaping. La définition identifie également le trafic comme trafic entrant ou sortant et comme trafic côté WAN ou côté LAN. Tout le trafic circulant à travers l'appliance est comparé à votre liste de définitions de lien, et la première définition correspondante identifie le lien auquel le trafic appartient.

Je n'ai configuré aucune classe de service avec la stratégie par défaut. Toutefois, les rapports de traffic shaping affichent une grande quantité de trafic représentée par la stratégie par défaut. Ai-je configuré quelque chose de mal ?

Non. Il n'y a aucun problème avec votre configuration. Le traffic shaping n'est applicable qu'à la liaison WAN. Le trafic sur le réseau local ou tout autre lien est représenté par la stratégie par défaut.

Par exemple, considérez une configuration dans laquelle vous créez une classe de services, telle que Management_Service_Class, qui a le sous-réseau de gestion comme adresse IP de destination et vous liez une stratégie de traffic shaping personnalisée à cette classe de services. Dans ce cas, lorsqu'il n'y a pas de trafic sur WAN, vous pouvez remarquer que le trafic de gestion est classé comme Management_Service_Class dans le rapport de classe de service. Toutefois, dans le rapport Stratégie de traffic

shaping, les entrées de stratégie par défaut existent toujours si bien que vous pouvez vous attendre à exister en tant que stratégie de traffic shaping personnalisée.

Dans le rapport Stratégie de traffic shaping, l'appliance n'utilise pas de stratégie de traffic shaping personnalisée pour la stratégie Management_Service_Class et applique la stratégie par défaut. Pour éviter cette confusion, vous pouvez désactiver l'option Tous les autres ou définir le lien de type LAN pour l'interface de gestion.

Processus de mise à niveau (OS)

April 23, 2021

La nouvelle mise à niveau du noyau OS WANOP est prise en charge à partir de quelle version SD-WAN ?

Citrix SD-WAN version 10.1 et ultérieure.

Le nouveau système d'exploitation est-il pris en charge sur toutes les plates-formes SD-WAN ?

Oui. La mise à niveau du système d'exploitation est prise en charge sur toutes les appliances SD-WAN WANOP (VPX, Physical, Cloud) et Premium/Enterprise.

Quels sont les profils WANOP VPX (RAM/disk/vCPU) pris en charge avec la version 10.1 ?

- 6 Go de RAM, disque 100 Go et 2 vCPU
- 6 Go de RAM, 250 Go de disque et 2 vCPU
- 8 Go de RAM, 500 Go de disque et 4 vCPU
- 16 Go de RAM, 500 Go de disque et 4 vCPU

Quelles sont les principales différences entre WANOP fonctionnant avec la version 10.0 ou inférieure par rapport à 10.1 ?

Fonctionnalité	10.0 ou plus tôt	10.1 ou version ultérieure	Commentaires
Prise en charge de la mise en cache vidéo sur WANOP	prise en charge	Non pris en charge	aucun
RAM minimale requise pour WANOP VPX	4 Go de RAM	6 Go de RAM	aucun
Assistant de déploiement WANOP VPX	prise en charge	Non pris en charge	aucun

Fonctionnalité	10.0 ou plus tôt	10.1 ou version ultérieure	Commentaires
Adresse IP principale de gestion de l'adaptateur apA pour WANOP VPX	DHCP est désactivé par défaut	DHCP est activé par défaut	aucun
Mise à niveau de la prise en charge sur WANOP VPX autonome existant sur Citrix Hypervisor	prise en charge	prise en charge. L'image SD-WAN 10.1 XVA fraîche doit être importée	aucun
Prise en charge de la mise à niveau sur la plate-forme WANOP physique disposant de la version hypervisor 6.0 de Citrix Hypervisor 6.0 (les plates-formes livrées avec la version 7.2.2 ou antérieure d'image de base d'usine auraient Citrix Hypervisor 6.0 version) version 10.1	prise en charge	Vous devez mettre à niveau Citrix Hypervisor vers la version 6.5 (à l'aide du bundle de mise à niveau WANOP Citrix Hypervisor 6.5), puis effectuer la mise à niveau de WANOP 10.1	En cliquant sur l'interface graphique « Configuration », afficherait la version de l'hyperviseur Citrix Hypervisor

La**mise à niveau de WANOP VPX s'exécutant sur Citrix Hypervisor autonome (avec WO build 10.0 ou version antérieure) vers la version 10.1 est-elle prise en charge, Si ce n'est pas le cas, pourquoi** ?

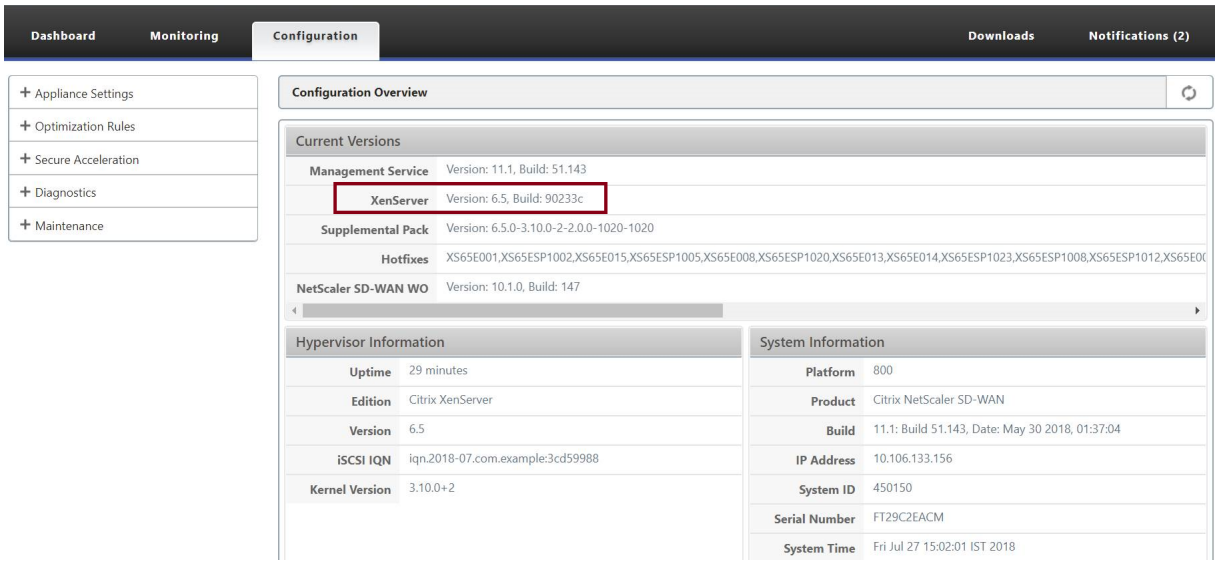
Cette mise à niveau n'est pas prise en charge en raison de la conversion PV vers HVM. Vous devez provisionner une nouvelle version SD-WAN sur 10.1 Citrix Hypervisor WANOP VPX à l'aide de l'image XVA.

Mise à niveau de WANOP VPX en cours d'exécution sur ESXi/Hyper-V autonome (avec WO build 10.0 ou version antérieure) vers la version 10.1 est celle prise en charge, sinon, pourquoi ?

Cette mise à niveau est prise en charge. Avant la mise à niveau, veuillez prendre connaissance des nouvelles modifications apportées aux exigences en matière de ressources RAM.

La**mise à niveau de WANOP sur l'appliance physique (avec WANOP build 10.0 ou version antérieure) vers la version 10.1 est-elle prise en charge, sinon, pourquoi** ?

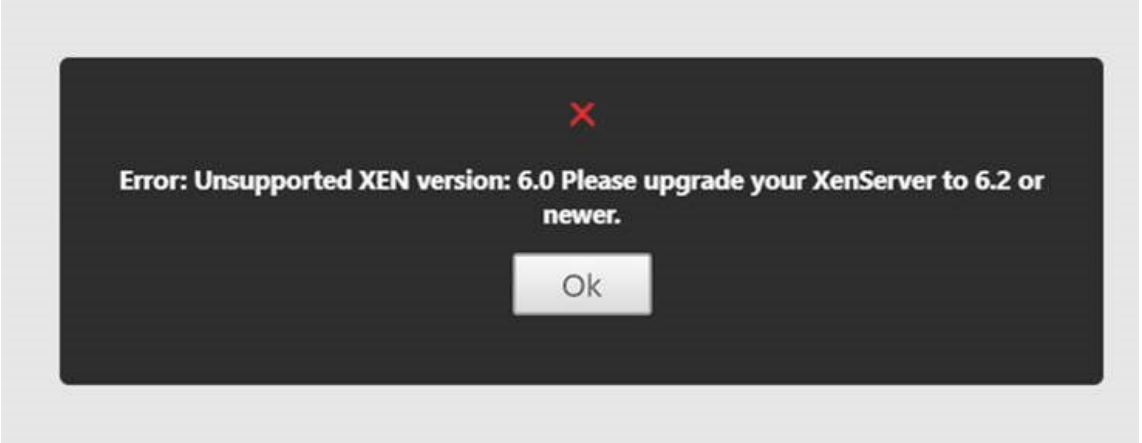
Cette mise à niveau est prise en charge. La condition préalable à cette mise à niveau est d'héberger Citrix Hypervisor Hypervisor (sur l'appliance SD-WAN physique) pour disposer de Citrix Hypervisor version 6.2/6.5 ou version ultérieure. Cela peut être vérifié à l'aide de l'onglet **Configuration**.



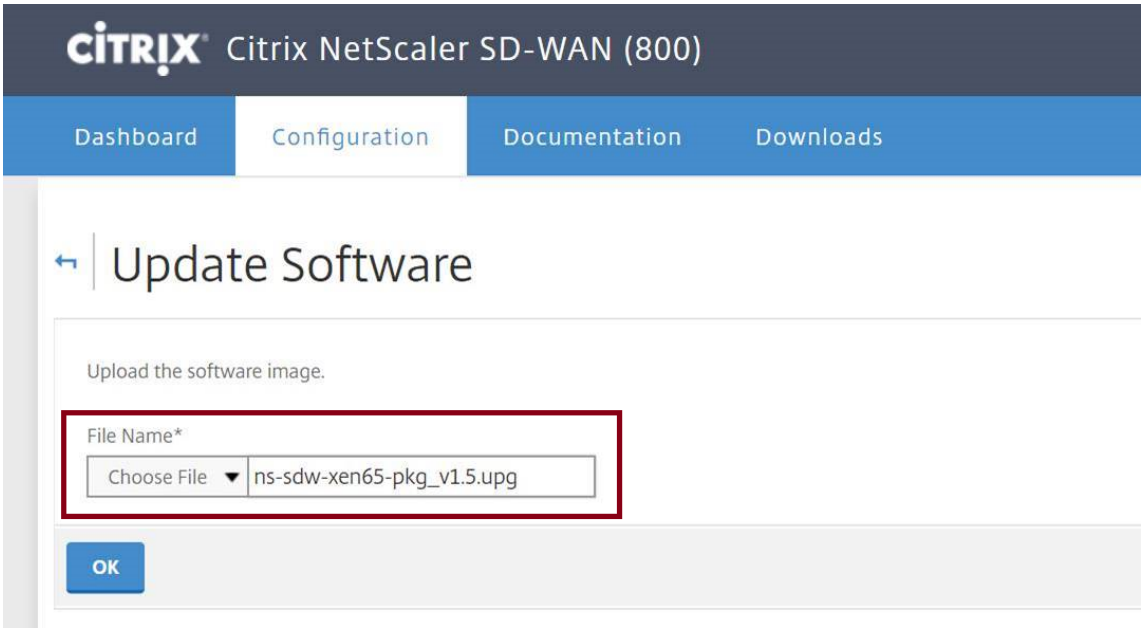
Si l'appliance WANOP physique ne s'exécute pas avec Citrix Hypervisor 6.2/6.5 ou version ultérieure, que doit effectuer l'utilisateur ?

Vous devez mettre à niveau Citrix Hypervisor, avant de mettre à niveau la version SD-WAN WO. Par exemple, dans ce cas d'utilisation ci-dessous, envisageons de mettre à niveau la plate-forme WANOP SD-WAN 800 exécutant avec 7.2.2 (qui a Citrix Hypervisor 6.0 version).

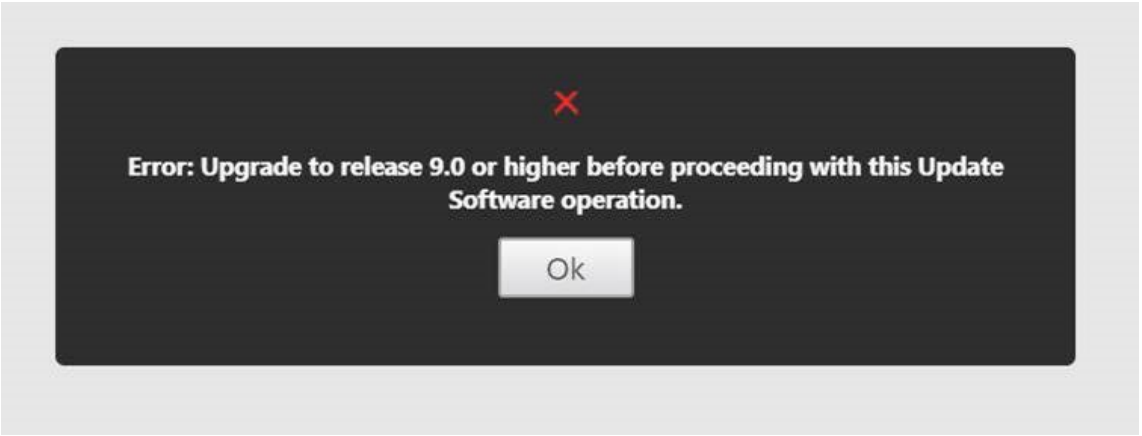
1. Lors de la mise à niveau de cette appliance vers la version SD-WAN 10.1, le message d'erreur suivant se produit.



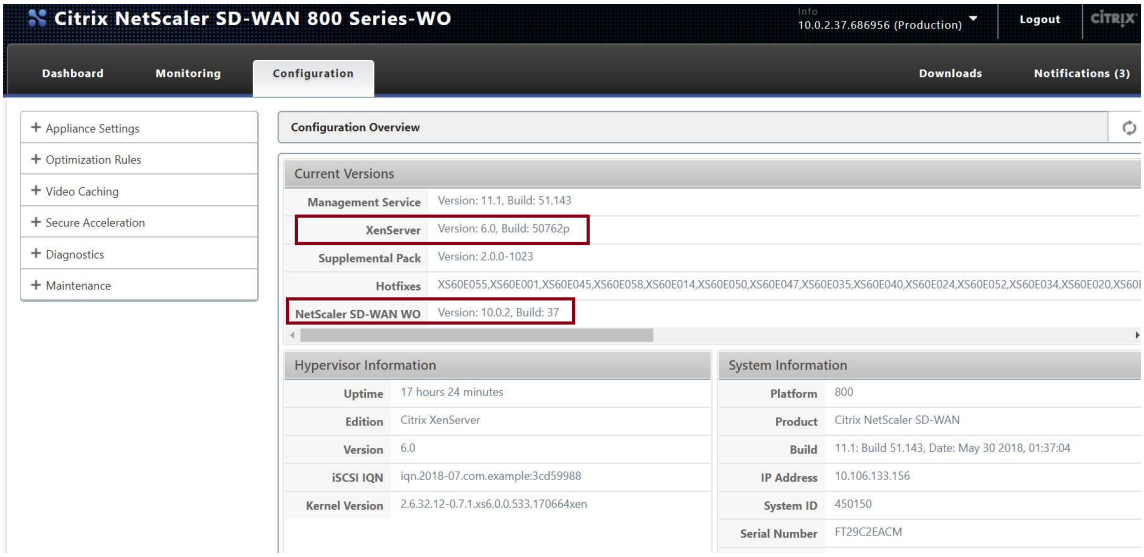
2. Mettez à niveau Citrix Hypervisor vers 6.5, en utilisant « ns-sdw-xen65-pkg_v1.5.upg » (cela peut être téléchargé à partir du site Web de téléchargement Citrix.



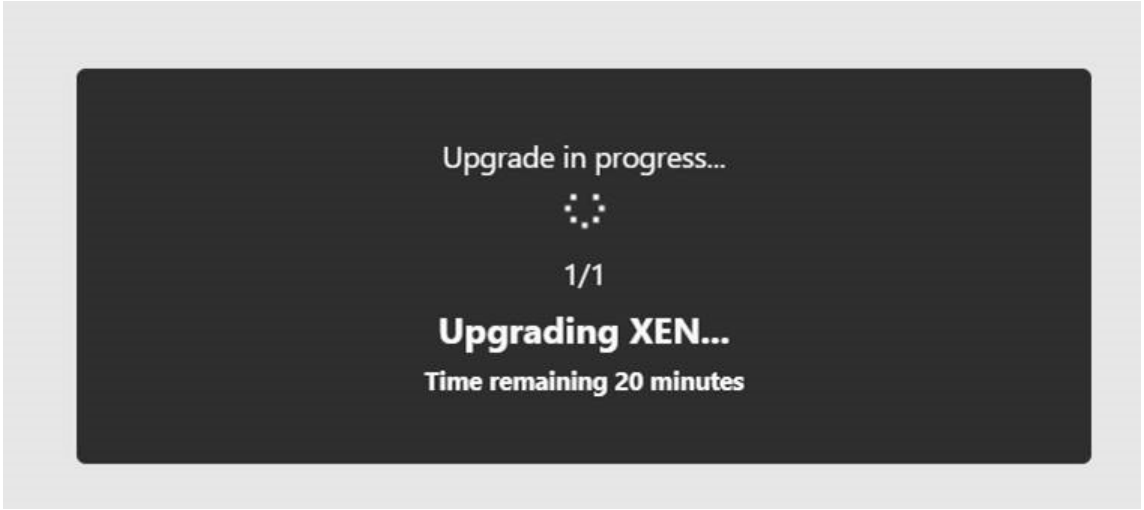
3. Si SD-WAN WO n'a pas la version 9.0 ou ultérieure, la mise à niveau vers Citrix Hypervisor 6.5 ne se produirait pas. Le message d'erreur ci-dessous s'afficherait.

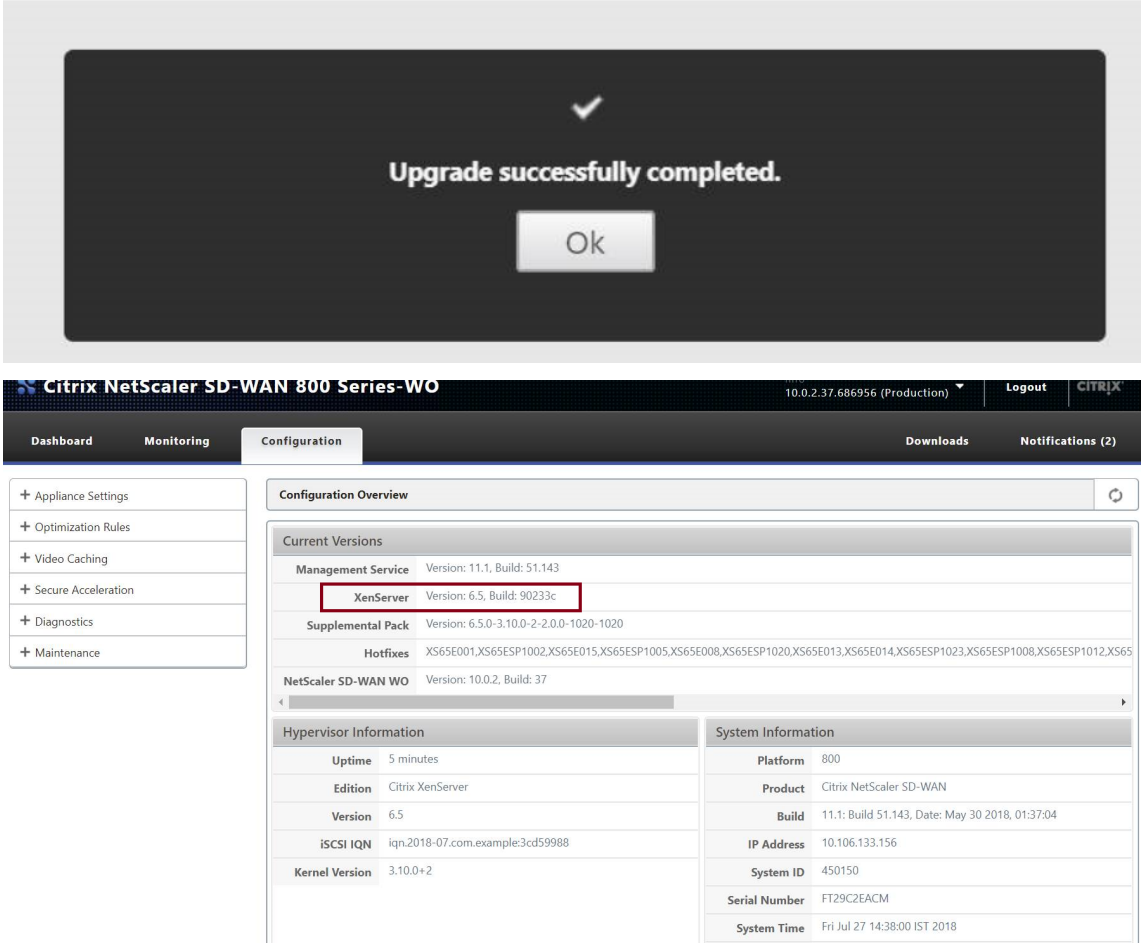


4. Supposons que l'utilisateur a mis à jour la version WO à 10.0.2 maintenant.

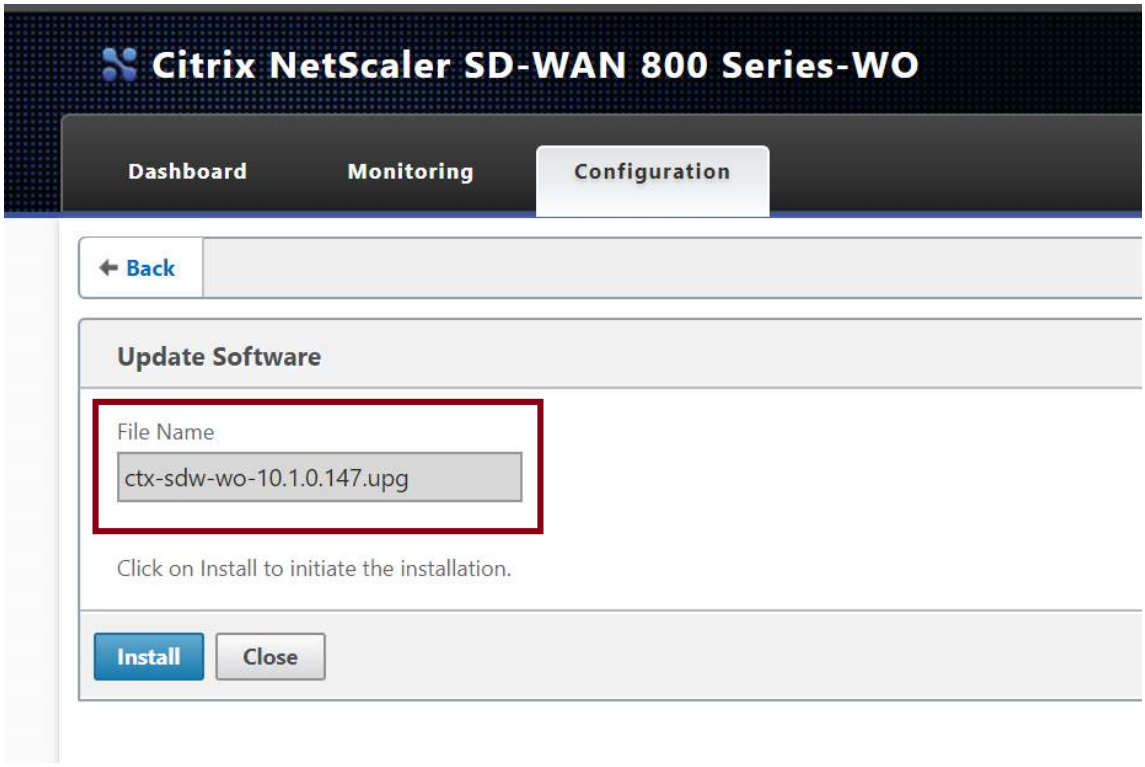


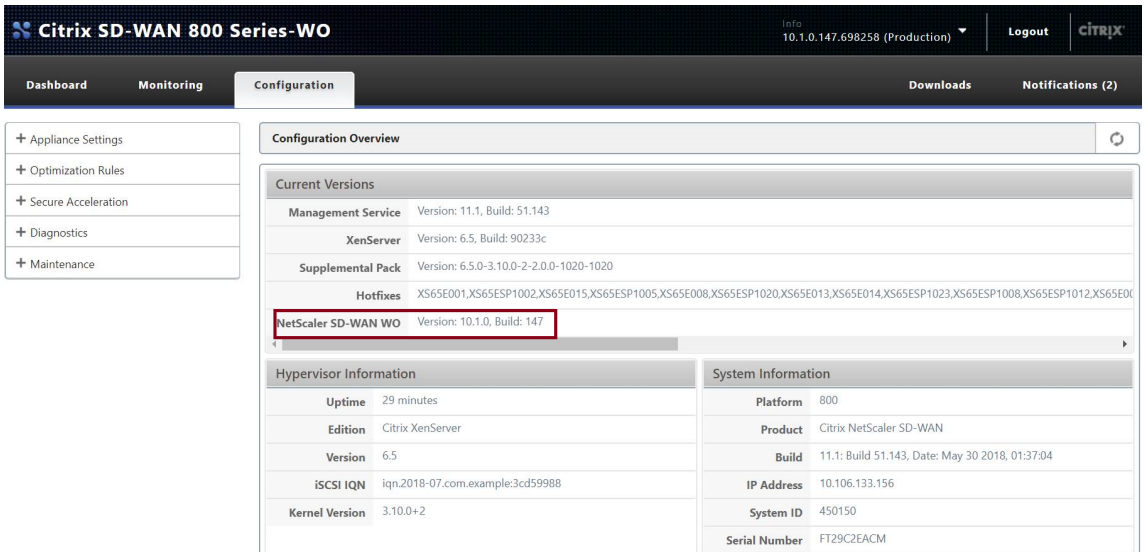
5. Maintenant, mettez à niveau Citrix Hypervisor vers 6.5, en utilisant « ns-sdw-xen65-pkg_v1.5.upg ».





6. Maintenant, mettez à niveau le SD-WAN vers la version 10.1.





Client to Server ICMP Ping fonctionne bien, mais le trafic TCP ne passe pas par l'appliance WANOP VPX (la désactivation du traitement du trafic WANOP fonctionne bien) ?

Vérifiez les paramètres du pare-feu sur le Client, le Serveur et le Routeur.
Lorsque WANOP VPX ou Client/Serveur sont hébergés en tant que VM, assurez-vous que la somme de contrôle est désactivée sur la machine virtuelle hôte final.

```
Exemples de commandes Linux :
    ethtool -K eth0 tx off
    ethtool -K eth0 rx off
```



```
    ethtool --offload eth0 tx off
    ethtool --offload eth0 rx off
```

Activez le paramètre « CheckSum.SendForceSW » sur les deux VPX WO (ON).

```
Exemple :
    Checksum.SendForceSW on
```

Y a-t-il des modifications au processus de mise à niveau de l'appliance SDWAN SE/EE/WO en raison du nouveau noyau WO OS ?

Non.

Mise en cache de vidéo

April 9, 2021

En quoi la mise en cache vidéo diffère-t-elle de la compression basée sur disque ?

Avec la mise en cache, une copie locale de l'objet mis en cache est desservie par l'appliance locale, sans le télécharger à nouveau depuis le serveur distant. La mise en cache ne nécessite pas de appliance aux deux extrémités de la liaison, uniquement à l'extrémité locale. Avec la compression, une copie distante de l'objet est desservie par le serveur distant. L'appliance distante (côté serveur) la compresse, ce qui réduit sa taille et, par conséquent, augmente sa vitesse de transmission, et l'appliance locale (côté client) la décompresse.

La compression fonctionne sur les objets modifiés et non modifiés. Si un fichier change de 1% sur le serveur, le transfert suivant atteint une compression allant jusqu'à 99:1.

La mise en cache ne fonctionne que sur les objets non modifiés. Si un fichier change de 1% sur le serveur, la nouvelle version doit être téléchargée dans son intégralité. La mise en cache et la compression sont des technologies complémentaires, car tout ce qui n'est pas mis en cache est comprimé, ce qui permet d'obtenir les avantages des deux.

Puis-je partitionner la mémoire totale de l'appliance entre le cache vidéo et d'autres fonctionnalités Citrix SD-WAN WANOP ?

Non. La partition de cache et la mémoire requise ne sont pas configurables.

Quels sont les formats de conteneur vidéo pris en charge ?

La mise en cache vidéo est indépendante du format codec et prend en charge tous les formats de conteneur majeurs.

Puis-je activer la mise en cache des vidéos d'entreprise internes et externes sur mes propres sites ?

Oui. Si l'accès à ces vidéos est via HTTP, vous pouvez configurer ces sites pour la mise en cache.

Puis-je configurer la taille maximale d'un objet mis en cache ?

Oui. Un objet supérieur à la limite que vous configurez n'est pas mis en cache. Pour définir cette limite, accédez à **Configuration** > **Règles d'optimisation** > **Mise en cache vidéo** et sélectionnez la valeur parmi les limites disponibles.

Comment la mise en cache vidéo améliore-t-elle l'expérience utilisateur ?

La mise en cache améliore l'expérience utilisateur pour les vidéos visualisées plus d'une fois, en particulier sur les liens plus lents. La première visionneuse d'un flux vidéo donné ne bénéficie pas de la fonctionnalité de mise en cache vidéo, mais les vues suivantes sont fournies à la vitesse LAN à partir de l'appliance Citrix SD-WAN WANOP, avec l'avantage supplémentaire d'une utilisation du réseau étendu réduite.

De plus, si un second utilisateur demande la même vidéo alors qu'elle est encore diffusée en continu pour le premier utilisateur, le second utilisateur recevra la copie mise en cache.

Contrairement à l'opération normale de Citrix SD-WAN WANOP TCP, où l'appliance conserve les adresses IP source et destination d'origine, l'appliance remplace l'adresse source du client par l'adresse IP attribuée au pont accéléré, de sorte que tout le trafic HTTP passant par l'appliance semble provenir de la l'appareil lui-même.

Quelles appliances Citrix SD-WAN WANOP prennent en charge la mise en cache vidéo ?

Les appliances suivantes prennent en charge la fonctionnalité de mise en cache vidéo :

- Appliance SD-WAN WANOP 800 avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 1000 avec Windows Server, avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 2000 avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 2000 avec Windows Server, avec tous les modèles de licence de bande passante.
- Appareil SD-WAN WANOP 3000 avec tous les modèles de licence de bande passante.

Pour la mise en cache vidéo, quels modes de déploiement sont pris en charge sur une appliance Citrix SD-WAN WANOP ?

- Déploiement pris en charge : Inline Virtual Inline, VLAN et WCCP
- Fonctionnalités non prises en charge - Citrix SD-WAN WANOP haute disponibilité, modes de groupe et chaînage en Daisy

Quelles extensions de fichiers sont prises en charge pour la mise en cache vidéo ?

Le nom du fichier vidéo doit avoir l'une des extensions suivantes : .3gp, .avi, .dat, .divx, .dvx, .dv-avi, .flv, .fmv, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e .m4v, .m75, .moov, .mov, .movie, .mp21, mp2v, .mp4, .mp4v, .mpe, .mpeg, mpeg4, mpg, mpg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd, .rms, rmvb, .rp, rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv, and .wtv.

Puis-je activer la fonctionnalité de mise en cache vidéo sur une plate-forme Citrix SD-WAN WANOP non prise en charge ?

Non. La fonctionnalité de mise en cache vidéo ne peut pas être utilisée sur les plates-formes non prises en charge.

Quelles sont la configuration minimale et les autres conditions préalables à l'activation de la fonction de mise en cache vidéo ?

Pour activer la fonctionnalité de mise en cache vidéo, vous devez :

- Attribuez une adresse IP et une Gateway valides à l'interface apA et, le cas échéant, à l'interface APB.
- Sur l'appliance, configurez un serveur DNS valide pouvant être résolu sur www.citrix.com.
- Avoir au moins une application dans la liste Applications de mise en cache vidéo sélectionnées.
- Vérifiez les alertes de l'interface graphique WANOP SD-WAN de Citrix et la notification des alertes de configuration existantes.

Le plug-in SD-WAN WANOP Citrix peut-il utiliser la fonctionnalité de mise en cache vidéo ?

Non. Vous ne pouvez pas utiliser la fonctionnalité de mise en cache vidéo avec le plug-in Citrix SD-WAN WANOP.

Quels sont les navigateurs et périphériques prisen charge ?

La mise en cache vidéo prend en charge les navigateurs Internet Explorer, Firefox et Chrome. Les vidéos peuvent être visualisées sur Windows 7 ou 8, iPad Apple et appareils Android iOS.

l'appliance Citrix SD-WAN WANOP prend-elle en charge la mise en cache vidéo pour tous les sites Web vidéo ?

Non. Le site Web de la vidéo est disponible et ajouté à partir de la liste des applications prises en charge de la page de configuration de la mise en cache vidéo. Par défaut, les applications prises en charge incluent YouTube, Vimeo, Youku, Dailymotion et Metacafe. Vous pouvez ajouter d'autres sites Web en spécifiant leurs adresses IP, s'ils n'utilisent pas de mécanismes d'évitement de mise en cache, tels que l'ajout de caractères aléatoires aux URL.

La surveillance SNMP est-elle prise en charge pour la mise en cache vidéo ?

Oui. Vous pouvez utiliser les MIB SNMP pour surveiller des tâches spécifiques de mise en cache vidéo.

La**mise en cache vidéo est-elle prise en charge pour le trafic non-HTTP** ?

Non. La mise en cache vidéo n'est pas prise en charge pour le trafic non HTTP, tel que HTTPS, RTSP et RTMP.

Puis-je utiliser la mise en cache vidéo avec le trafic HTTP envoyé à un port autre que le port 80 ?

Oui. Pour la mise en cache vidéo, vous pouvez ajouter des ports personnalisés à l'appliance. Pour ajouter des ports personnalisés pour la mise en cache vidéo, accédez à la page **Configuration** > **Règles d'optimisation** > **Mise en cache vidéo** et cliquez sur le lien **Paramètres globaux** dans l'onglet **Paramètres**.

La**compression Citrix SD-WAN WANOP (à l'aide d'une stratégie de classe de service HTTP) peut-elle être utilisée avec la mise en cache vidéo** ?

Oui. Lorsque les objets mis en cache sont présents à la fois dans l'historique de compression WANOP de Citrix SD-WAN et dans le cache vidéo, le contenu est servi à partir du cache lors d'un appel de cache, puis extrait du serveur (et compressé) sur une absence de cache.

Une application HTTP existante qui nécessite une configuration d'adresse IP lorsqu'il y a un proxy transparent nécessite-t-elle des modifications ?

Oui. Citrix SD-WAN WANOP effectue un proxy HTTP transparent, dans lequel il remplace l'adresse IP source du paquet. Par conséquent, si l'application HTTP existante a certaines stratégies (par exemple pour bloquer certaines adresses IP ou mécanismes proxy), ces stratégies doivent être modifiées.

Quelles sont les limites de mémoire système et de connexion pour la connexion proxy HTTP ?

Pour déterminer les limites, vérifiez les graphiques et les statistiques sur la page Débogage de la mise en cache vidéo (support.html). En outre, vérifiez que la commande Videocaching.cmd stats info affiche les informations suivantes.

	SD-WAN WANOP 800	SD-WAN 1000 avec serveur Widows	SD-WAN 2000 avec serveur Widows	SD-WAN 2000	SD-WAN 3000
Disque	25 Go	25 Go	50 Go	50 Go	99 Go
RAM	375 Mo	375 Mo	700 Mo	700 Mo	1 024 Mo
Nombre total de connexions HTTP	1 000	1 000	1500	1500	3000
Limite maximale d'écriture HTTP	200	200	300	300	600

Une fois que les limites de connexion HTTP ci-dessus sont atteintes, les nouvelles connexions sont contournées.

> **Remarque**
>
> Assurez-vous de ne pas modifier la configuration ci-dessus.

La page Surveillance de la mise en cache vidéo inclue-t-elle uniquement le trafic vidéo ?

Oui. Le trafic HTTP non vidéo (même s'il est intercepté par le proxy) n'est pas inclus dans les statistiques de l'interface graphique de mise en cache vidéo.

Dois-je configurer des interfaces apA et APB avec une adresse IP valide sur un dispositif Citrix SD-WAN WANOP ?

Non. Vous n'avez pas besoin d'attribuer une adresse IP valide aux deux interfaces. Les paquets HTTP reçus de l'interface apA sont transmis par proxy avec l'adresse IP apA, et les paquets HTTP reçus de l' interface APB sont transmis par proxy avec l'adresse IP APB.

Si vous ne configurez pas d'adresse IP pour une interface, les paquets HTTP reçus sur cette interface n'obtiennent pas l'avantage de mise en cache.

Quelle est la limite minimale et maximale pour la taille d'un fichier vidéo pouvant être mis en cache ?

- Minimum : 100 Ko
- Maximum : 300 Mo
- Par défaut : 100 Mo

Comment le disque de mise en cache vidéo est-il effacé ?

Les objets mis en cache sont effacés comme spécifié par l'algorithme le moins récemment utilisé.

Que se passe-t-il lorsque je mets à niveau l'appliance Citrix SD-WAN WANOP de la version 6.x vers la version 7.y et que la mise en cache vidéo est activée ?

L'historique de Citrix SD-WAN WANOP DBC existant est perdu et une partition séparée pour la mise en cache vidéo est créée.

Que se passe-t-il lorsque je rétrograde l'appliance Citrix SD-WAN WANOP de la version 7.y à la version 6.x et que la mise en cache vidéo est activée ?

L'historique de Citrix SD-WAN WANOP DBC et Video Caching est conservé. Toutefois, la fonctionnalité de mise en cache vidéo n'est pas disponible avec la version 6.x.

Que se passe-t-il lorsque je mets à niveau l'appliance Citrix SD-WAN WANOP de la version 7.x vers 7.y et que la mise en cache vidéo est activée ?

L'historique Citrix SD-WAN WANOP DBC et de la mise en cache vidéo est préservé.

J'ai un réseau unique en succursale qui partage une gestion ainsi que le trafic de données. Comment configurer la mise en cache vidéo dans ce réseau ?

Si vous disposez d'un réseau unique pour la gestion et le trafic de données, Citrix vous recommande d'ajouter l'adresse IP principale au côté LAN du port de pont accéléré.

Quel est le nombre maximal de tâches de préremplissage que je peux exécuter en même temps ?

Un. Si vous tentez de démarrer plusieurs tâches de préremplissage en même temps, l'appliance crée une file d'attente de tâches sur la base du premier, premier sorti.

Quel est le nombre maximal de sources de vidéos que je peux configurer sur l'appliance ?

100

Quel est le nombre maximal d'entrées préremplies que je peux ajouter à l'appliance ?

50

Quel est le nombre maximal de fichiers vidéo téléchargés et mis en cache à partir d'un dossier répertorié dans le répertoire ?

300

Le téléchargement vidéo et la mise en cache initiés par la fonctionnalité de préremplissage bénéficient-ils des avantages de la compression basée sur disque (DBC) ?

Oui. Étant donné que le fichier vidéo est mis en cache, la tentative d'accès à la vidéo est servie à partir du cache.

Accélération Office 365

April 23, 2021

1. Pourquoi analyser le SAN ?

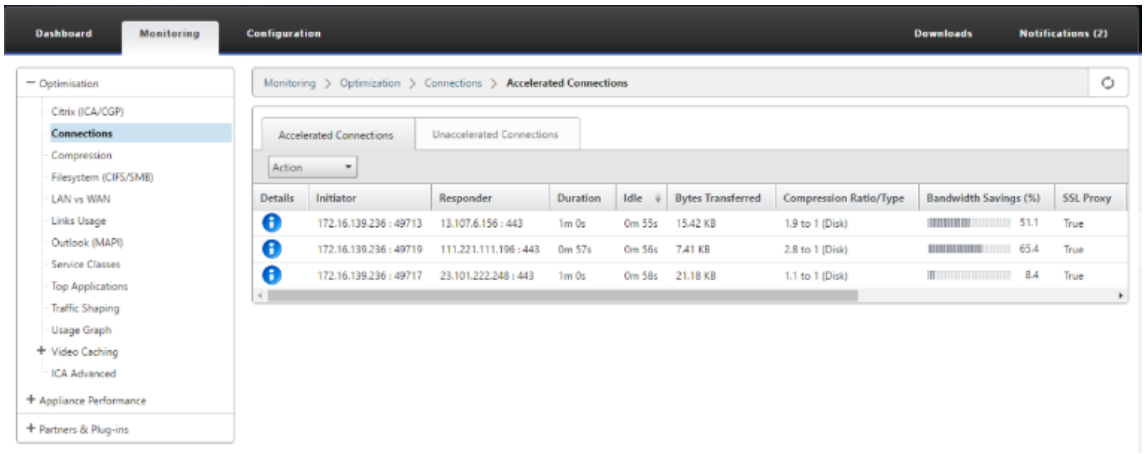
   Il est fastidieux de créer plusieurs profils pour FQDNS pour chacun des domaines, pour surmonter cela, nous analysons le SAN à partir des certificats.

2. Qu'est-ce qu'une liste d'exclusion ?

   Un message d'erreur ou d'avertissement s'affiche Si le navigateur ou l'application ne contient pas le certificat de l'autorité de certification, dans de tels cas, l'adresse IP du client sera ajoutée à une liste d'exclusion après quelques tentatives de connexion depuis le navigateur ou l'application (2-3 fois). Lors de la prochaine tentative, la connexion n'est pas proxy SSL et la page se charge sans erreur ni avertissement. L'adresse IP du client restera dans la liste d'exclusion pendant 48 heures. La liste d'exclusion est conservée uniquement pour le proxy fractionné.

3. Où vérifier les informations de connexion d'accélération Office 365 ?

   Accédez à **Surveillance** > **Connexions** > **Connexions accélérées**, vérifiez l'état du proxy SSL. Pour plus d'informations sur la connexion, cliquez sur l'icône Détails.



4. Que se passe-t-il si l'option de liste d'exclusion n'est pas activée par défaut dans le cadre de la configuration du profil SSL ?

   Si le navigateur ou l'application ne contient pas le certificat de l'autorité de certification, il affiche une erreur ou un avertissement et les connexions de ce client ou de cette application seront bloquées. Pour éviter de tels problèmes, sélectionnez l'option **Exclure la liste** dans le cadre de la configuration du profil SSL.

5. Que se passe-t-il si les SAN requis ne font pas partie du certificat proxy configuré/créé ?

   Les connexions ne seront pas transmises par proxy SSL et il n'y aura aucun avantage d'accélération pour les connexions SSL sans proxy.

6. Que se passe-t-il lorsque le client ne fait pas partie du domaine ou si le client ne possède pas le certificat racine du domaine ?

   Les connexions sont bloquées si la liste d'exclusion n'est pas activée.

7. Que se passe-t-il si le serveur Citrix SD-WAN WANOP côté datacenter n'a pas d'autorité de certification racine ou intermédiaire ?

   Les connexions sont bloquées ou les pages d'application Office 365 qui nécessitent l'autorité de certification racine ou intermédiaire manquante sont partiellement chargées. Pour débloquer les connexions ou pour que ces pages soient complètement chargées, ajoutez les certificats d'autorité de certification appropriés ou désactivez le profil SSL de l'accélération.

8. Comment savoir quels clients sont exclus de l'accélération ?

   Les informations sur les clients exclus peuvent être connues à partir des journaux ou à l'aide de la commande CLI *show ssl-exclude -list*.

9. Que faire lorsque les clients sont exclus ?

   Par défaut, les informations de liste d'exclusion de l'appliance sont effacées au bout de 48 heures. L'utilisateur peut effacer de force les informations de liste d'exclusion à l'aide des commandes CLI *`clear ssl-exclude-list -\<all\>/\<Client\\_IP\>`*.

10. Comment savoir quelles connexions SSL (SNI) ne sont pas proxy ?

    À partir des journaux ou en utilisant la commande CLI *show ssl-non-proxied-sni*, vous pouvez connaître la liste des SNI ne passant pas par un proxy.

11. Comment effacer les SNI n'utilisant pas un proxy ?

    Utilisation de la commande CLI *`clear ssl-non-proxied-sni -\<all\>/\<server name identifier\>`*.

12. Quelle est l'heure par défaut pour le client en état d'exclusion ?

    Le client reste à l'état exclu pendant 48 heures.

13. Peut-on appliquer plusieurs profils pour une classe de service particulière ?

    Oui, nous pouvons appliquer des classes de service avec plusieurs profils SSL.

    Pour ce faire, sur votre appliance Virtual WAN, accédez à **Configuration** > **Classe de service** > **Web (Sécurisé Internet)** > **Modifier> Modifier** (Application) et ajoutez les profils disponibles.

14. Comment vérifier pourquoi des connexions n'utilisent pas un proxy ?

    Vérifiez la page de connexion TCP, pour plus d'informations, consultez les journaux. Pour déboguer les problèmes de connexion n'utilisant pas un proxy, procédez comme suit.

    a) Si le journal n'affiche aucune configuration valide - Définissez la configuration valide. Pour plus d'informations sur la configuration de la fonctionnalité Office 365, reportez-vous à la section Accélération Office 365.

    b) Si le journal indique que la vérification de certification a échoué, ajoutez des certificats d'autorité de certification valides à l'appliance Citrix SD-WAN WANOP côté datacenter.

    c) si le journal affiche le client exclu : les informations sur les clients exclus peuvent être effacées de l'appliance à l'aide de la commande CLI *`clear ssl-exclude-list -\<all\>/\<Client\\_IP\>`*.

Notes supplémentaires

- La journalisation sur le client OneDrive affiche parfois un message d'avertissement « avertissement erroné », Ceci est un problème connu de Microsoft (https://support.microsoft.com/en-us/kb/3097938) et non spécifique à Citrix SD-WAN appliance WANOP.

- Pour que les pages redirigées Office 365 soient transmises par proxy, il est recommandé de créer un certificat proxy distinct contenant la liste SAN correspondant au certificat des pages redirigées. Créez un autre profil avec ce certificat proxy et appliquez-le à la classe de service. Ajoutez également l'autorité de certification pertinente dans l'appliance Citrix SD-WAN WANOP.
- Parfois, le navigateur n'affiche pas les certificats d'autorité de certification corrects, dans de tels cas, utilisez Wireshark ou OpenSSL pour obtenir les noms d'autorité de certification racine et intermédiaire et obtenir les certificats de source « authentique » (par exemple, Windows SSL store).
- Différence dans le comportement du navigateur peut être observée dans l'accès aux applications Office 365 à partir de différents navigateurs n'ayant pas de certificats requis et avec l'option de liste Exclure désactivée.
- Lorsque les connexions Office 365 sont proxy SSL (cela signifie que le proxy SSL est défini sur True) et que dans le navigateur Office 365 certificat est affiché à la place du certificat proxy, il est recommandé d'ouvrir le navigateur en mode cognitif et de vérifier le comportement ou effacer le cache, puis de vérifier à nouveau le comportement.
- Microsoft Office 365 comprend de nombreux composants et applications tels que OneDrive, Outlook, SharePoint, Word, PPT, Excel, OneNote. Toutes ces applications ont été testées et sont connues pour fonctionner sans aucun problème. D'autres applications sont également censées fonctionner sans aucun problème ; cependant, cet état peut changer au fil du temps et vous risquez de rencontrer des problèmes inconnus.

Compression

April 23, 2021

La compression Citrix SD-WAN WANOP utilise une technologie révolutionnaire pour fournir une compression multiniveaux transparente. C'est la vraie compression qui agit sur des flux d'octets arbitraires. Il ne prend pas en compte les applications, est indifférent aux limites de connexion et peut comprimer une chaîne de manière optimale la seconde fois qu'elle apparaît dans les données. La compression Citrix SD-WAN WANOP fonctionne à n'importe quelle vitesse de liaison.

Le moteur de compression est très rapide, ce qui permet au facteur d'accélération de la compression d'approcher le taux de compression. Par exemple, un transfert en masse monopolisant une liaison T1 de 1,5 Mbps et atteignant un taux de compression de 100:1 peut fournir un rapport d'accélération de près de 100x, ou 150 Mbps, à condition que la bande passante WAN soit le seul goulot d'étranglement dans le transfert.

Contrairement à la plupart des méthodes de compression, l'historique de compression Citrix SD-WAN WANOP est partagé entre toutes les connexions qui passent entre les deux mêmes appliances. Les données envoyées heures, jours ou même semaines plus tôt par connexion A peuvent être renvoyées plus tard par la connexion B, et bénéficier de l'avantage d'accélération complet de la compression. Les performances qui en résultent sont beaucoup plus élevées que celles qui peuvent être obtenues par les méthodes conventionnelles.

La compression peut utiliser le disque et la mémoire de l'appliance, fournissant jusqu'à téraoctets d'historique de compression.

Fonctionnement de la compression

Tous les algorithmes de compression analysent les données à compresser, en recherchant des chaînes de données correspondant aux chaînes qui ont déjà été envoyées. Si aucune correspondance de ce type n'est trouvée, les données littérales sont envoyées. Si une correspondance est trouvée, les données correspondantes sont remplacées par un pointeur sur l'occurrence précédente. Dans une très grande chaîne correspondante, des mégaoctets ou même des gigaoctets de données peuvent être représentés par un pointeur ne contenant que quelques octets, et seuls ces quelques octets doivent être envoyés sur le lien.

Les moteurs de compression sont limités par la taille de leur historique de compression. Les algorithmes de compression traditionnels, tels que LZS et ZLIB, utilisent des historiques de compression de 64 Ko ou moins. Les appliances Citrix SD-WAN WANOP conservent au moins 100 Go d'historique de compression. Avec plus d'un million de fois l'historique de compression des algorithmes traditionnels, l'algorithme Citrix SD-WAN WANOP trouve plus de correspondances et de correspondances plus longues, ce qui entraîne des ratios de compression supérieurs.

L'algorithme de compression Citrix SD-WAN WANOP est très rapide, de sorte que même les appliances d'entrée de gamme peuvent saturer un LAN de 100 Mbps avec la sortie du compresseur. Les modèles les plus performants peuvent fournir plus de 1 Gbit/s de débit.

Seules les données de charge utile sont compressées. Cependant, les en-têtes sont compressés indirectement. Par exemple, si une connexion atteint une compression de 4:1, un seul paquet de sortie grandeur nature est envoyé pour quatre paquets d'entrée grandeur nature. Ainsi, la quantité de données d'en-tête est également réduite de 4:1.

Compression en tant qu'optimisation générale :

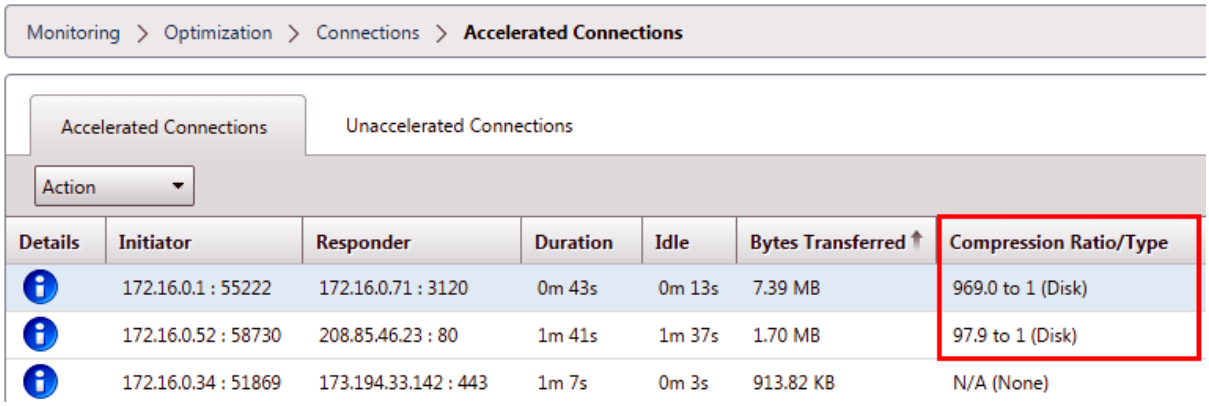
La compression Citrix SD-WAN WANOP est indépendante de l'application : elle peut compresser les données de n'importe quelle connexion TCP non chiffrée.

Contrairement à la mise en cache, les performances de compression sont robustes face à l'évolution des données. Avec la mise en cache, la modification d'un octet d'un fichier invalide la copie

entière dans le cache. Avec la compression, changer un seul octet au milieu d'un fichier crée simplement deux grandes correspondances séparées par un seul octet de données non concordantes, et le temps de transfert résultant n'est que légèrement supérieur à ce qu'avant. Par conséquent, le rapport de compression se dégrade gracieusement avec la quantité de changement. Si vous téléchargez un fichier, modifiez 1 % de celui-ci et rechargez-le, attendez-vous à un taux de compression de 99:1 sur le téléchargement.

Un autre avantage d'un historique de compression important est que les données précompressées se compriment facilement avec la technologie Citrix SD-WAN WANOP. Une image JPEG ou une vidéo YouTube, par exemple, est précompressée, laissant peu de possibilité de compression supplémentaire la première fois qu'elle est envoyée sur le lien. Mais chaque fois qu'il est envoyé à nouveau, le transfert entier est réduit à une poignée d'octets, même s'il est envoyé par différents utilisateurs ou avec différents protocoles, comme par FTP la première fois et HTTP la suivante.

En pratique, les performances de compression dépendent de la quantité de données traversant le lien identique à celle des données ayant précédemment traversé le lien. La quantité varie d'une application à l'autre, de jour en jour, et même d'un moment à l'autre. Lorsque vous examinez une liste de connexions accélérées actives, attendez-vous à voir des rapports entre 1:1 et 10 000:1.



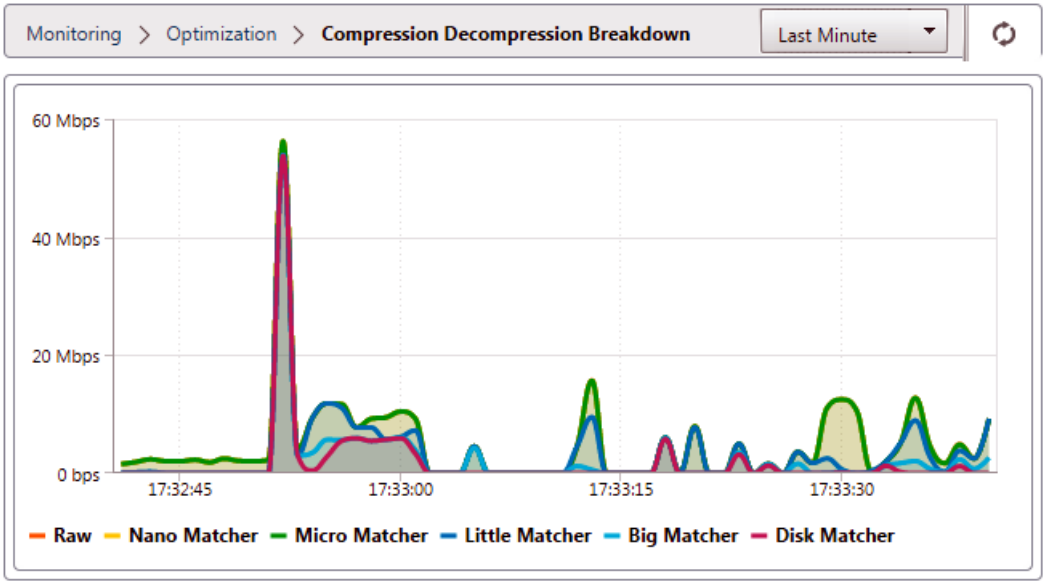
Compresser les protocoles chiffrés :

De nombreuses connexions présentant de faibles performances de compression le font parce qu'elles sont chiffrées. Le trafic chiffré est normalement incompressible, mais les appliances Citrix SD-WAN WANOP peuvent compresser les connexions chiffrées lorsque les appliances rejoignent l'infrastructure de sécurité. Les appliances WANOP Citrix SD-WAN rejoignent automatiquement l'infrastructure de sécurité avec Citrix Citrix Virtual Apps and Desktops et peuvent rejoindre l'infrastructure de sécurité des serveurs SSL, système de fichiers Windows (CIFS/SMB) et Outlook/Exchange (MAPI) avec configuration manuelle.

Fonctionnement adaptatif, sans configuration :

Pour répondre aux différents besoins de différents types de trafic, les appliances Citrix SD-WAN WANOP n'utilisent pas un, mais cinq moteurs de compression, de sorte que les besoins de tout, du

transfert en vrac le plus massif au trafic interactif le plus sensible à la latence peuvent être satisfaits avec facilité. Le moteur de compression est adapté dynamiquement aux besoins changeants des connexions individuelles, de sorte que la compression est automatiquement optimisée. Un avantage supplémentaire est que le moteur de compression ne nécessite aucune configuration.



Compression basée sur la mémoire

La plupart des moteurs de compression utilisent la RAM pour stocker leur historique de compression. C'est ce qu'on appelle la compression basée sur la mémoire. Certains appareils consacrent des gigaoctets de mémoire à ces moteurs de compression. La compression basée sur la mémoire a une faible latence et est souvent choisie automatiquement pour les tâches interactives telles que le trafic Application/Desktops virtuels.

Compression sur disque

Le moteur de compression sur disque utilise entre des dizaines de gigaoctets et téraoctets de mémoire pour stocker l'historique de compression, ce qui permet des correspondances de compression plus nombreuses et meilleures. Le moteur de compression basé sur disque est très rapide, mais a parfois une latence plus élevée que les moteurs basés sur la mémoire, et est souvent choisi automatiquement pour les transferts en masse.

Activer ou désactiver la compression

La compression est activée, par classe de service, sur la page Configuration : Classes de service. Cette page dispose d'un menu déroulant pour chaque classe de service, avec les options suivantes :

- **Disque**, ce qui signifie que la compression basée sur le disque et la compression basée sur la mémoire sont activées. Cette option doit être sélectionnée sauf si vous avez une raison spécifique pour la désactiver.
- **Mémoire**, ce qui signifie que la compression basée sur la mémoire est activée, mais pas la compression basée sur le disque. Ce paramètre est rarement utilisé, car l'appliance sélectionne automatiquement la mémoire ou le disque si les deux types de compression sont activés.
- **Contrôle du flux uniquement**, qui désactive la compression mais active l'accélération du contrôle du flux. Sélectionnez cette option pour les services toujours chiffrés et pour le canal de contrôle FTP.
- **Aucun**, ce qui signifie que la compression et le contrôle de flux sont tous les deux désactivés.

Pour de plus amples informations, consultez la section Classes de service.

Mesurer les performances de la compression sur disque

L'onglet État de la compression de la page
Rapports : Compression indique les performances de compression du système depuis le démarrage du système ou depuis que le bouton Effacer a été utilisé pour réinitialiser les statistiques. La compression pour les connexions individuelles est signalée dans les messages de fermeture de connexion dans le journal système.

Les performances de compression varient selon un certain nombre de facteurs, notamment la redondance dans le flux de données et, dans une moindre mesure, la structure du protocole de données.

Certaines applications, telles que FTP, envoient des flux de données purs ; la charge utile de la connexion TCP est toujours octet pour octet identique au fichier de données d'origine. D'autres, comme CIFS ou NFS, n'envoient pas de flux de données purs, mais mélangent des commandes, des métadonnées et des données dans le même flux. Le moteur de compression distingue les données du fichier en analysant la charge utile de connexion en temps réel. De tels flux de données peuvent facilement produire des rapports de compression entre 100:1 et 10000:1 sur la deuxième passe.

Les ratios de compression moyens pour le lien dépendent de la prévalence relative des correspondances longues, courtes et aucune correspondance. Ce ratio dépend du trafic et est difficile à prévoir dans la pratique.

Les résultats des tests montrent l'effet de la compression multi-niveaux dans son ensemble, avec la compression basée sur la mémoire et sur le disque faisant chacun sa contribution.

Les performances de compression maximales ne sont pas atteintes tant que l'espace de stockage disponible pour la compression sur disque n'est pas rempli, ce qui fournit une quantité maximale de données précédentes pour correspondre aux nouvelles données. Dans un monde parfait, les essais ne s'achèveraient pas tant que les disques de l'appareil n'avaient pas seulement été remplis, mais

remplis et écrasés au moins une fois, pour s'assurer que le fonctionnement en état permanent a été atteint. Cependant, peu d'administrateurs disposent de données aussi représentatives.

Une autre difficulté dans les tests de performance est que l'accélération expose souvent des liens faibles dans le réseau, généralement dans les performances du client, du serveur ou du réseau local, et que ces derniers sont parfois mal diagnostiqués comme des performances d'accélération décevantes.

Vous pouvez utiliser Iperf ou FTP pour les tests préliminaires et initiaux. Iperf est utile pour les tests préliminaires. Il est extrêmement compressible (même au premier passage) et utilise relativement peu de CPU et pas de ressources disque sur les deux systèmes de terminaison. Les performances compressées avec Iperf devraient envoyer plus de 200 Mbit/s sur une liaison T1 si les LAN des deux côtés utilisent Gigabit Ethernet, ou légèrement moins de 100 Mbit/s s'il y a un équipement Fast Ethernet dans les chemins LAN entre les terminaux et les appliances.

Iperf est préinstallé sur les appliances (sous le menu Diagnostics) et est disponible à partir dehttp://iperf.sourceforge.net/. Idéalement, il devrait être installé et exécuté à partir des systèmes de terminaison, de sorte que le réseau soit testé de bout en bout, et pas seulement d'une appliance à l'autre.

FTP est utile pour des tests plus réalistes que possible avec Iperf. FTP est simple et familier, et ses résultats sont faciles à interpréter. Les performances de seconde passe devraient être à peu près les mêmes qu'avec Iperf. Si ce n'est pas le cas, le facteur limitatif est probablement le sous-système de disque sur l'un des systèmes de terminaison.

Pour tester le système de compression sur disque :

1. Transférez un flux de données de plusieurs gigaoctets entre deux appliances avec la compression sur disque activée. Notez la compression obtenue lors de ce transfert. Selon la nature des données, une compression considérable peut être observée lors du premier passage.
2. Transférez le même flux de données une deuxième fois et notez l'effet sur la compression.

Rapports de compression en édition premium

Citrix SD-WAN Premium (Enterprise) Edition ne dispose pas d'une vue permettant d'afficher les rapports de compression sur une base par protocole ou application via les classes de service WANOP, qui ont le protocole ou l'association d'application. Si vous utilisez une appliance Edition Premium (Enterprise), le seul rapport disponible pour la compression est un rapport de compression au niveau de la connexion qui ne donne pas de visibilité sur la mesure dans laquelle un protocole a été optimisé ou compressé. Les rapports de compression sont disponibles dans l'interface graphique d'optimisation WAN qui affiche une répartition de tous les protocoles uniques et la façon dont les rapports ont été optimisés sur une période donnée.

Dans l'interface graphique de l'appliance Citrix SD-WAN Premium (Enterprise) Edition, pour l'optimisation WAN, les widgets suivants ont été ajoutés dans le tableau de bord d'optimisation WAN.

- Rapport de compression consolidé : tout le trafic passant par l'appliance WANOP et nombre total de connexions accélérées et non accélérées. Cela vous permet de surveiller le trafic total transmis du LAN au WAN.
- Taux de compression - 10 classes de service les plus importantes.
- Débit de liaison agrégé —LAN et WAN.

Taux de compression consolidé :

Ce rapport affiche le taux de compression consolidé pour tout le trafic transmis à WANOP et le nombre total de connexions accélérées et non accélérées. Il indique également le temps de disponibilité du service WANOP dans l'appliance.

Débit de liaison agrégé :

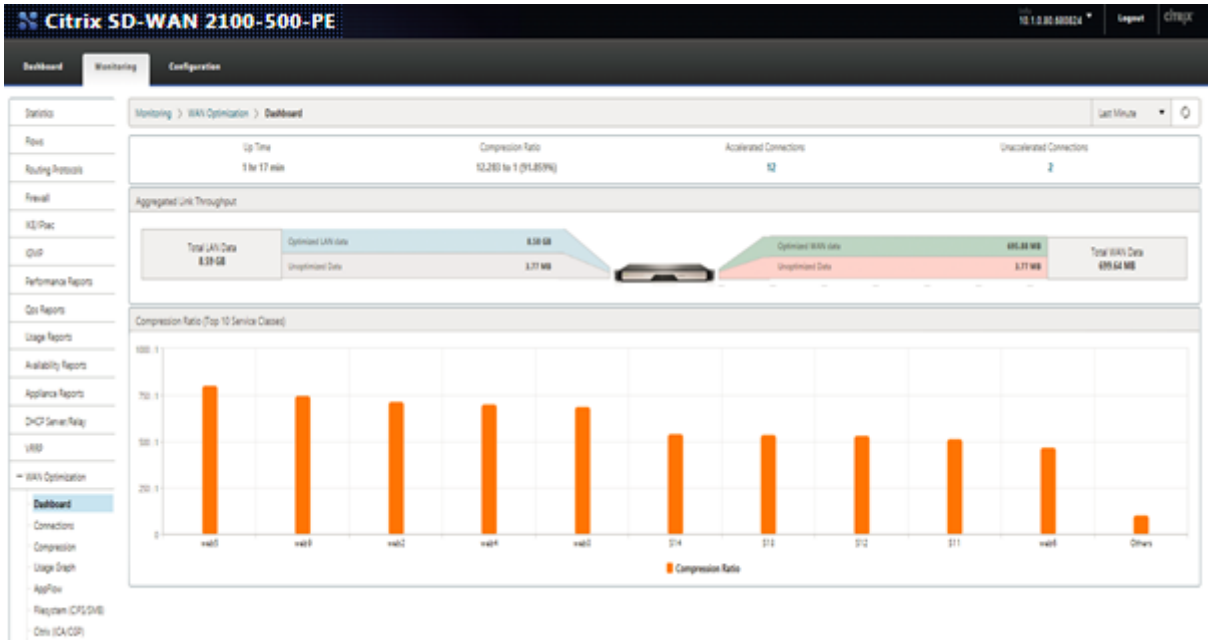
Ce rapport affiche le trafic total qui est transmis à WANOP et le trafic total qui transmet avec des ruptures dans les catégories de données optimisées et non optimisées aux deux extrémités.

Taux de compression (10 classes de service les plus importantes) :

Dans l'interface graphique du dispositif Citrix SD-WAN, vous pouvez vérifier les détails de la connexion et le taux de compression (par tableau de bord de classe de service) en accédant à **Surveillance** > **Optimisation du réseau étendu**. Cette option sélectionne automatiquement le nœud Tableau de bord et fournit une vue d'ensemble sous la forme de tableau de bord.

Le graphique affiche les 10 premières valeurs du taux de compression pour le trafic classé par classe de service.

Une barre supplémentaire « autres » s'affiche, qui indique le taux de compression pour toutes les autres connexions accélérées qui font partie du système, en plus des rapports de taux de compression Top 10 des classes de service.



Accélération HTTP

April 9, 2021

L'accélérateur Citrix SD-WAN WANOP utilise une variété d'optimisations sans configuration pour accélérer le trafic HTTP. Cela accélère à son tour les pages Web et toutes les autres applications utilisant le protocole HTTP (téléchargements de fichiers, streaming vidéo, mises à jour automatiques, etc.).

Les optimisations qui accélèrent HTTP incluent la compression, le traffic shaping, le contrôle de flux et la mise en cache.

Compression

HTTP est une application idéale pour la compression multi-niveaux Citrix SD-WAN WANOP.

Le contenu statique, y compris les pages HTML standard, les images, les vidéos et les fichiers binaires, reçoit des quantités variables de compression en premier passage, généralement 1:1 sur le contenu binaire pré-compressé et 2:1 ou plus sur le contenu textuel. À partir de la deuxième fois que l'objet est vu, les deux moteurs de compression les plus importants (compression basée sur la mémoire et compression sur disque) offrent des rapports de compression extrêmement élevés, avec des objets plus gros recevant des rapports de compression de 1 000:1 ou plus. Avec de tels taux de compression élevés, la liaison WAN cesse d'être le facteur limitatif, et le serveur, le client ou le LAN devient le goulot d'étranglement.

L'appliance bascule dynamiquement entre les compresseurs pour obtenir des performances maximales. Par exemple, l'appliance utilise un compresseur plus petit sur l'en-tête HTTP et un compresseur plus grand sur le corps HTTP.

Le contenu dynamique, y compris les en-têtes HTTP et les pages générées dynamiquement —pages qui ne sont jamais deux fois identiques mais qui présentent des similitudes les unes avec les autres —est compressé par les trois moteurs de compression qui traitent des correspondances plus petites. La première fois qu'une page est vue, la compression est bonne. Lorsqu'une variante sur une page précédente est visible, la compression est meilleure.

Traffic shaping

HTTP consiste en un mélange de trafic interactif et de trafic en vrac. Le trafic de chaque utilisateur est un mélange des deux, et parfois la même connexion contient un mélange des deux. Le régulateur du trafic assure de manière transparente et dynamique que chaque connexion HTTP obtient sa juste part de bande passante du lien, empêchant les transferts groupés de monopoliser le lien aux dépens des utilisateurs interactifs, tout en veillant à ce que les transferts groupés obtiennent toute bande passante que les connexions interactives n'utilisent pas.

Contrôle de débit

Les algorithmes de retransmission avancés et d'autres optimisations au niveau TCP conservent la réactivité et maintiennent les taux de transfert face à la latence et à la perte.

Mise en cache de vidéo

La mise en cache HTTP pour les fichiers vidéo a été introduite dans la version 7.0 La mise en cache implique d'enregistrer des objets HTTP dans le stockage local et de les servir aux clients locaux sans les recharger à partir du serveur.

Quelle est la différence entre la mise en cache et la compression ? Alors que la mise en cache fournit une accélération similaire à la compression, les deux méthodes sont différentes, ce qui les rend complémentaires.

- La compression accélère les transferts à partir du serveur distant, et ce débit de données plus élevé peut placer une charge plus élevée sur le serveur si la compression n'était pas présente. La mise en cache empêche les transferts à partir du serveur et réduit la charge sur le serveur.
- La compression fonctionne sur n'importe quel flux de données, ceci est similaire à un transfert précédent. Si vous changez le nom d'un fichier sur le serveur distant et le transférez à nouveau, la compression fonctionnera parfaitement. La mise en cache ne fonctionne que lorsque l'objet

demandé par le client et l'objet sur le disque sont connus pour être identiques. Si vous modifiez le nom d'un fichier sur le serveur distant et le transférez à nouveau, la copie mise en cache n'est pas utilisée.

- Les données compressées ne peuvent pas être livrées plus rapidement que le serveur ne peut les envoyer. Les données mises en cache dépendent uniquement de la vitesse de l'appliance côté client.
- La compression est intensive en CPU ; la mise en cache ne l'est pas.

Fonctionnement de HTML5

April 9, 2021

HTML5 utilise HTTP, qui est un protocole de requête/réponse pour la communication entre les clients et les serveurs. Un client initie une connexion TCP et l'utilise pour envoyer des requêtes HTTP au serveur. Le serveur répond à ces demandes en accordant des droits d'accès aux ressources disponibles. Une fois que le client et le serveur ont établi une connexion, les messages échangés entre eux contiennent uniquement des en-têtes WebSocket, et non des en-têtes HTTP.

L'infrastructure HTML5 est constituée de WebSockets, qui utilisent en outre l'infrastructure HTTP existante pour fournir un mécanisme léger de communication entre un client et un serveur Web. Vous implémentez généralement le protocole WebSocket dans un navigateur et des serveurs Web. Toutefois, vous pouvez utiliser ce protocole avec n'importe quelle application client ou serveur.

Lorsqu'un client tente d'établir une connexion à l'aide de WebSockets, les serveurs Web traitent la poignée de main WebSocket comme une demande de mise à niveau, et le serveur passe au protocole WebSocket. Le protocole WebSocket permet une interaction fréquente entre le navigateur et les serveurs Web. Par conséquent, vous pouvez utiliser ce protocole pour les mises à jour en direct, telles que les index boursiers et les cartes de score, et même les jeux en direct. Ceci est possible en raison d'un moyen standardisé pour le serveur d'envoyer des réponses non sollicitées au client tout en maintenant une connexion ouverte pour une communication continue bidirectionnelle entre le navigateur client et le serveur.

> **Remarque**
>
> Vous pouvez également obtenir cet effet, de manière non standardisée, en utilisant diverses autres technologies, telles que Comet. Pour plus d'informations sur Comet, reportez-vous à la section http://en.wikipedia.org/wiki/Comet_(programming).

Le protocole WebSocket communique via les ports TCP 80 et 443. Cela facilite la communication dans les environnements qui utilisent des pare-feu pour bloquer les connexions Internet non Web. En outre,

WebSocket a son propre mécanisme de fragmentation. Un message WebSocket peut être envoyé sous la forme de plusieurs trames WebSocket.

> **Remarque**
>
> Vous ne pouvez pas utiliser WebSocket si les applications Web sur les serveurs ne le supportent pas.

Comment HTML5 établit une session WebSocket

Un navigateur prenant en charge HTML5 utilise des API JavaScript pour effectuer les tâches suivantes :

- Ouvrez une connexion WebSocket.
- Communiquer via la connexion WebSocket.
- Fermez les connexions WebSocket.

Pour ouvrir une connexion WebSocket, le navigateur envoie un message de mise à niveau HTTP au serveur pour passer au protocole WebSocket. Le serveur accepte ou rejette cette demande. Voici des extraits d'un exemple de requête client et de réponse du serveur :

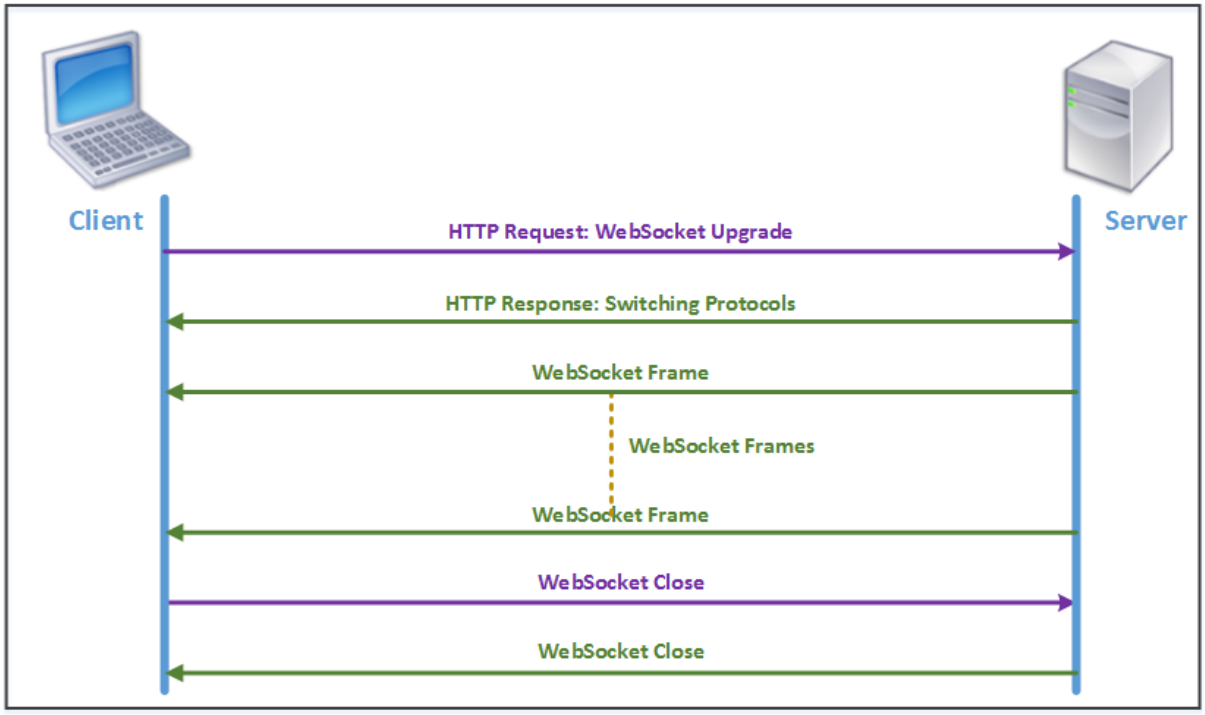
- Exemple de demande client

```
pre codeblock GET /HTTP/1.1 Upgrade: websocket Sec-websocket-
protocol: <List of protocols that the client supports over this
 websocket session, such as an application level protocol, for
 example ICA.> Sec-websocket-extensions: <List of extensions
client wants applied to this session, such as compression.> Sec-
Websocket-version: <Version of websocket protocol that the client
 intends to use.> <!--NeedCopy-->
```

- Exemple de réponse du serveur

```
pre codeblock HTTP/1.1 101 Switching Protocols Upgrade: websocket
 Connection: Upgrade Sec-Websocket-Protocol: <One from the list
of protocols in the client request.> Sec-Websocket-extensions:
<List of extensions server accepts for session.> Sec-Websocket-
version: <Version of websocket protocol that the server supports
.> <!--NeedCopy-->
```

La figure suivante montre la séquence des messages échangés entre un client et un serveur :



Au cours d'une connexion HTML5, les messages suivants sont échangés entre le client et le serveur :

- Le client envoie une requête HTTP pour mettre à niveau WebSocket.
- Le serveur répond à la demande du client et passe au protocole WebSocket.
- Le serveur envoie des trames WebSocket au client.
- Le client envoie une requête pour fermer le WebSocket.
- Le serveur ferme le WebSocket.

Accélération du protocole Internet version 6 (IPv6)

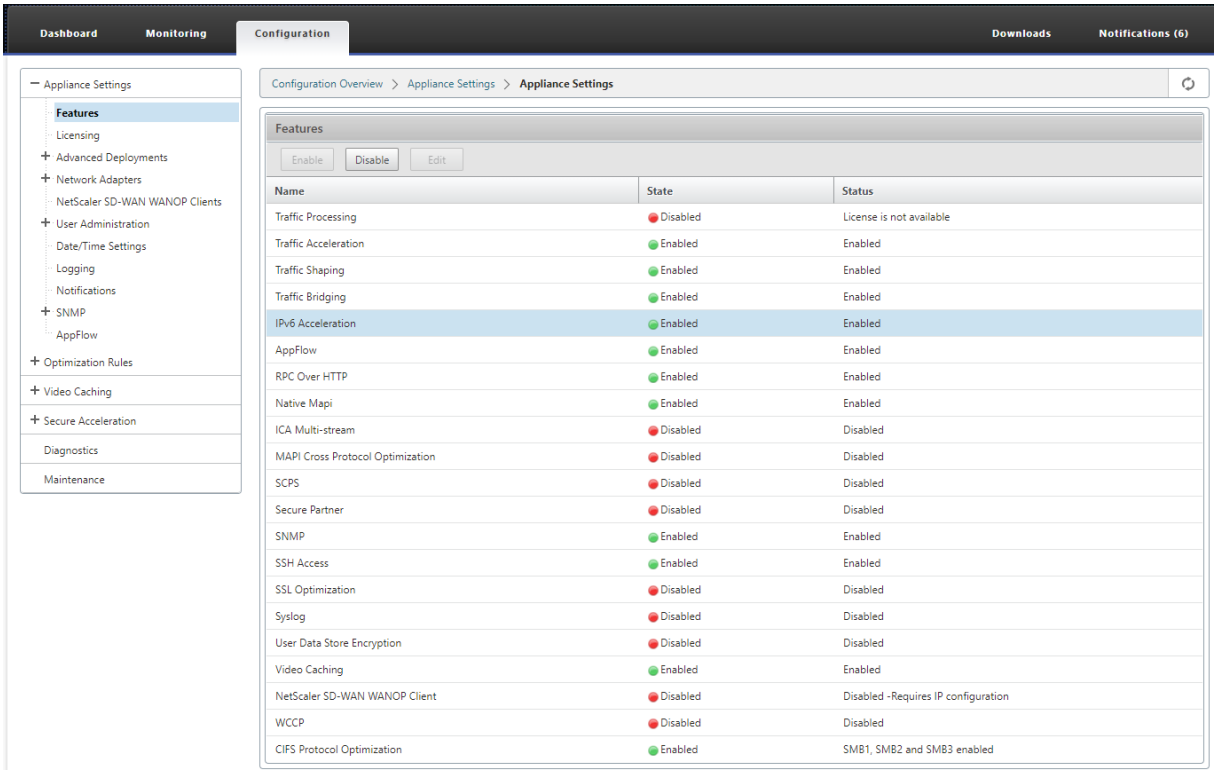
April 9, 2021

Lorsque vous vous connectez à Internet via un périphérique, une adresse IP lui est attribuée. L'adresse IP identifie l'appliance et indique son emplacement. Le nombre d'appareils se connectant à Internet augmente rapidement. En conséquence, il est difficile de gérer la demande d'adresses IP avec la version existante du protocole Internet (IP), IPv4, qui utilise des adresses 32 bits. En utilisant IPv4, environ 4,3 milliards d'adresses peuvent être attribuées aux appareils connectés à Internet.

IPv6 résout ce problème en utilisant des adresses 128 bits et une étiquette hexadécimale pour identifier les interfaces réseau des périphériques sur un réseau IPv6. Comme IPv6 prend en charge beaucoup plus d'adresses IP que IPv4, les organisations et les applications introduisent progressivement la prise en charge du protocole IPv6.

Les protocoles IPv4 et IPv6 ne sont pas interopérables, ce qui rend la transition difficile. Pour accélérer l'augmentation du trafic IPv6 provenant de diverses applications prises en charge par l'appliance Citrix SD-WAN WANOP, vous pouvez activer la fonctionnalité IPv6 Acceleration.

Par défaut, IPv6 est désactivé sur l'appliance. Pour activer l'accélération IPv6 sur un dispositif Citrix SD-WAN WANOP, accédez à la page **Configuration** > **Paramètres de l'appliance** > **Fonctionnalité** et activez la fonction d'**accélération IPv6**.

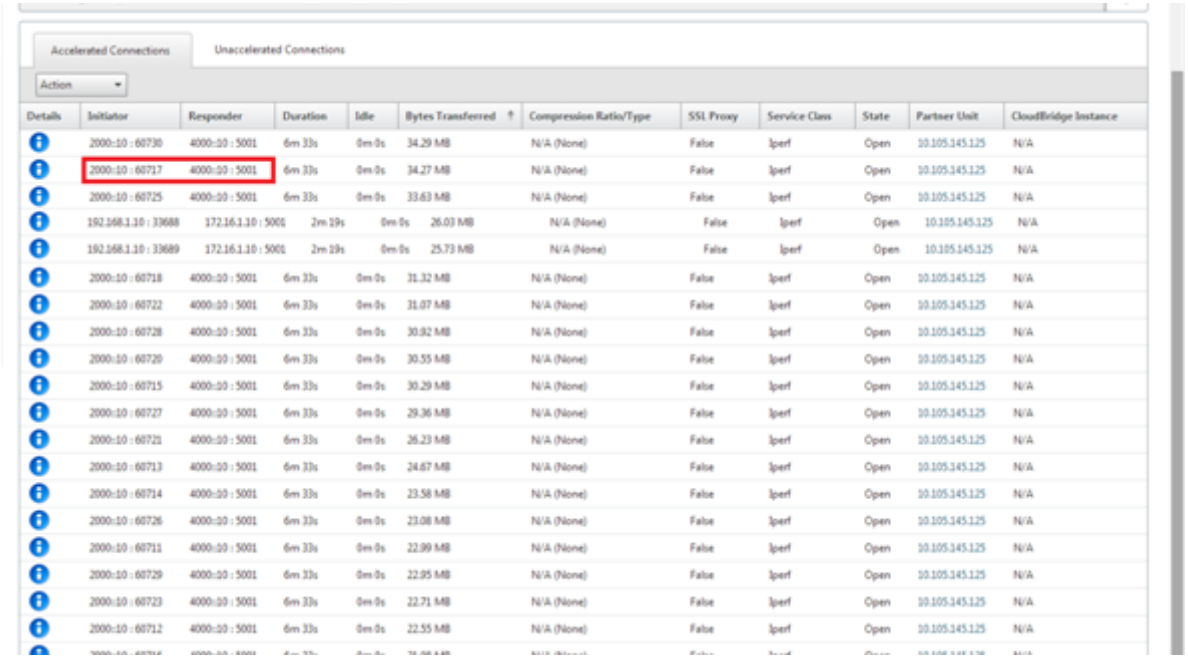


Vérifier les connexions IPv6

Après avoir activé l'accélération IPv6 sur l'appliance, l'appliance commence à accélérer le trafic des applications à l'aide du protocole IPv6. Pour vous assurer que l'appliance accélère le trafic IPv6, vous pouvez surveiller ces connexions sur l'appliance.

Pour surveiller les connexions IPv6, accédez à l'onglet Surveillance. La page **Connexions** de l'onglet **Surveillance** affiche les statistiques relatives au trafic des protocoles IPv6 :

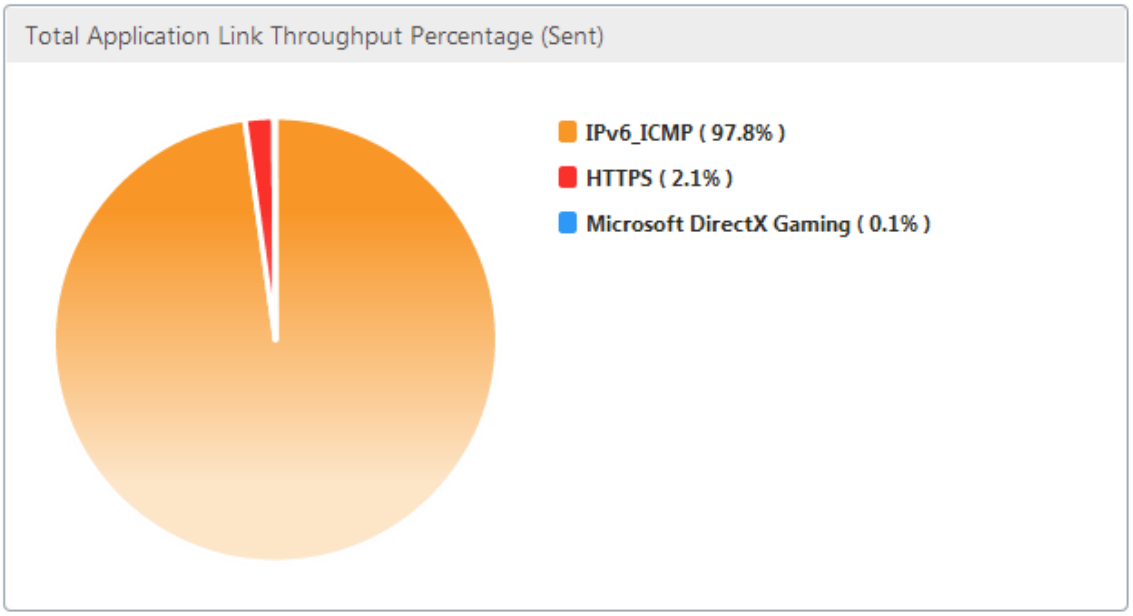
Connexions : la page Connexions répertorie les détails de toutes les connexions établies avec l'appliance. Cette page se compose de deux onglets, Connexions accélérées et Connexions non accélérées. L'onglet Connexions accélérées répertorie toutes les connexions que l'appliance accélère. Vous pouvez identifier le trafic IPv6 dans cet onglet en vous référant à la colonne Initiateur et Répondeur de chaque entrée. Si ces colonnes contiennent des valeurs d'adresse IP hexadécimales, l'entrée représente une connexion IPv6, comme indiqué dans la capture d'écran suivante.



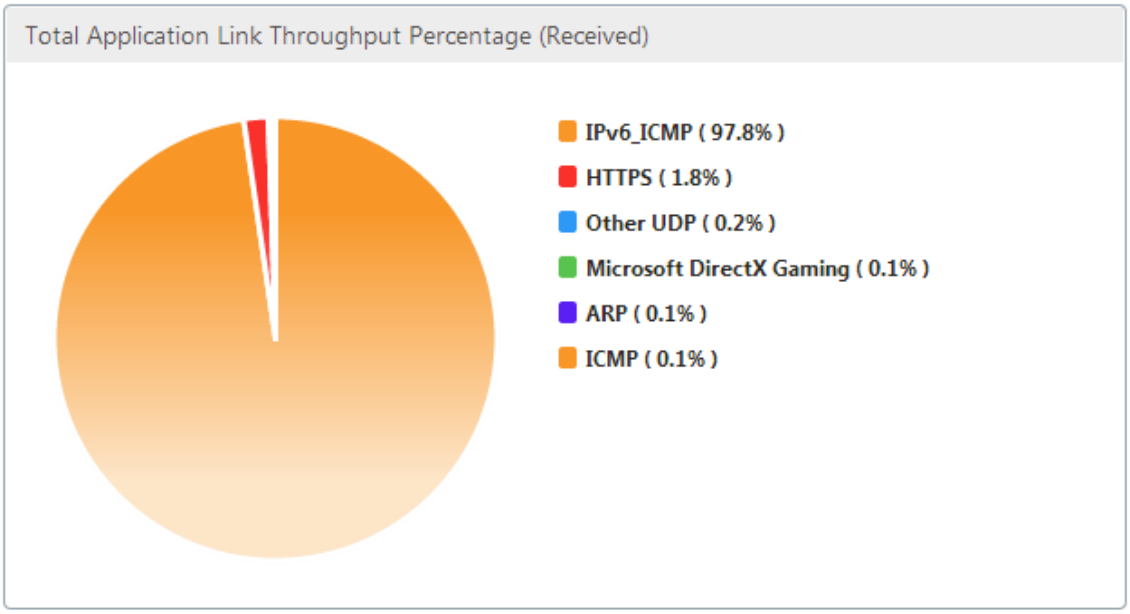
Les connexions IPv6 qui ne sont pas accélérées sont répertoriées sous l'onglet Connexions non accélérées. Si vous souhaitez accélérer ces connexions, vous devrez peut-être dépanner et affiner les paramètres de l'application sur l'appliance. Comme dans l'onglet **Connexions accélérées**, vous pouvez identifier les connexions IPv6 de cet onglet en vous référant aux colonnes **Initiateur** et **Répondeur** de chaque entrée.

Applications les pluspopulaires : la page Applications les plus importantes fournit une granularité dans la période que vous pouvez utiliser pour représenter graphiquement le débit de trafic de diverses applications desservies par l'appliance Citrix SD-WAN. Par défaut, le débit du trafic est affiché à la dernière minute. Toutefois, vous pouvez modifier la période en sélectionnant Dernière minute, Dernière heure, Dernier jour, Semaine dernière ou Mois dernier dans la liste disponible dans la barre de titre de la page. Cette page comporte trois onglets : **Graphiques d'applications principales**, **Depuis le dernier redémarrage**et **Applications actives (Depuis le dernier redémarrage)**. L'onglet Graphiques d'applications les plus importantes contient les statistiques suivantes :

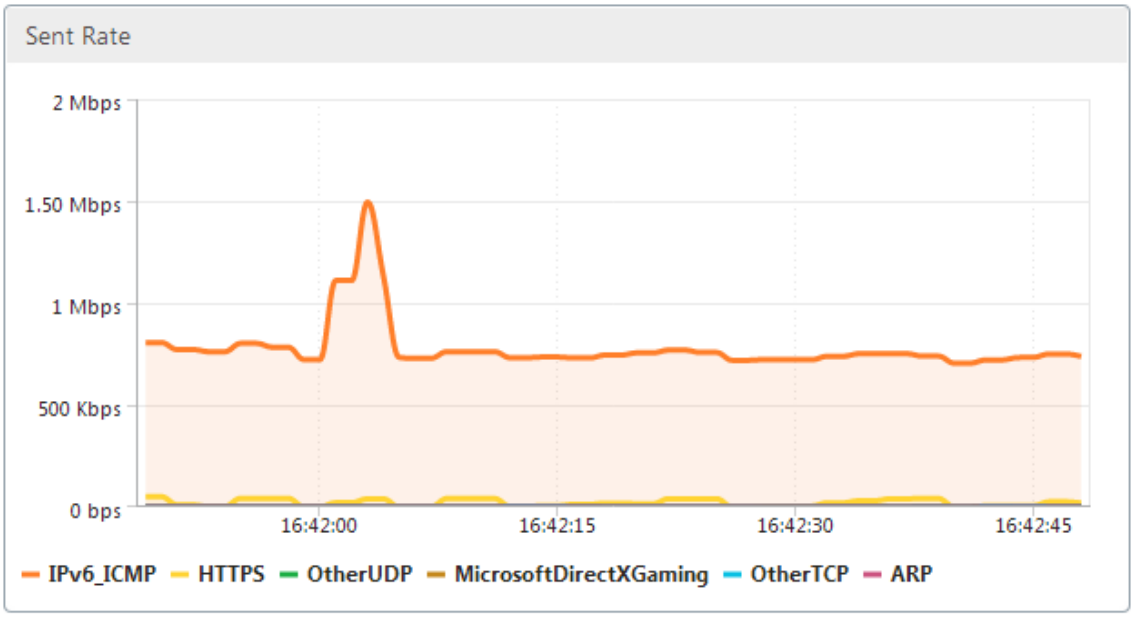
- **Pourcentage de débit total des liens d'application (envoyé)** : il s'agit d'un graphique circulaire représentant le pourcentage de trafic envoyé par l'appliance à chaque application. Si l'appliance a envoyé un pourcentage significatif de trafic pour une application utilisant le protocole IPv6, son pourcentage de trafic est représenté dans ce graphique.



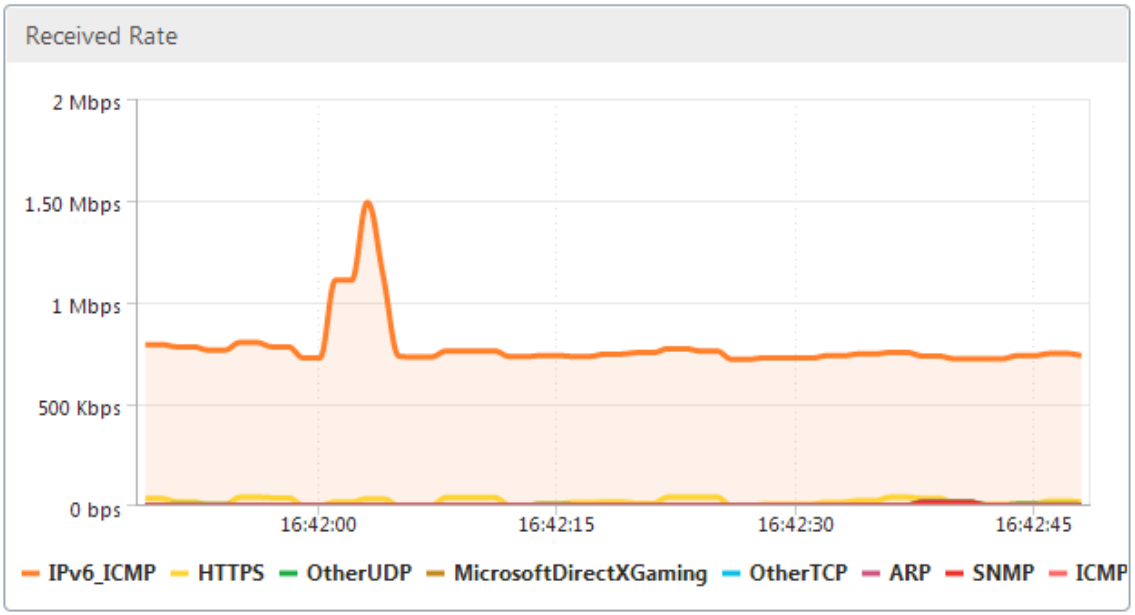
- **Pourcentage de débit total de la liaison d'application (reçu)** : il s'agit d'un graphique circulaire représentant le pourcentage de trafic reçu par l'appliance de chaque application. Si l'appliance a reçu un pourcentage significatif de trafic d'une application utilisant le protocole IPv6, le graphique affiche le pourcentage de trafic généré par l'application.



- **Taux d'envoi** : il s'agit d'un graphique empilé de séries de données représentant le taux, en bits par seconde, auquel l'appliance a envoyé du trafic à chaque application. Si l'appliance a envoyé des données à une application utilisant le protocole IPv6, une série représentant chaque application utilisant le protocole IPv6 est également tracée sur ce graphique.

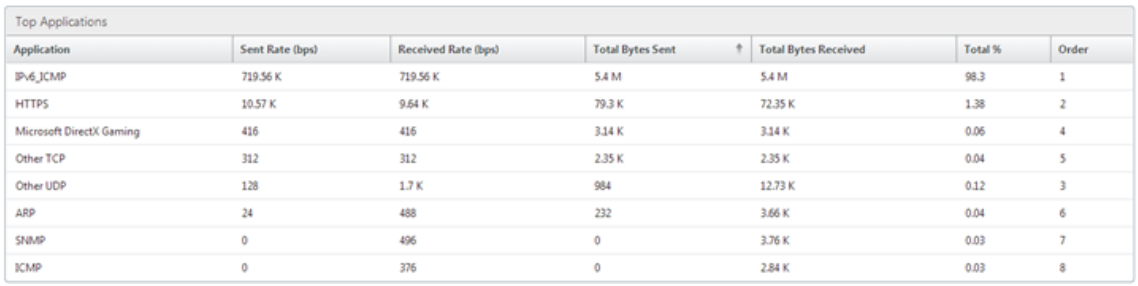


- **Taux de réception** : il s'agit d'un graphique empilé de séries de données représentant le débit, en bits par seconde, auquel l'appliance a reçu du trafic de chaque application. Si l'appliance a reçu des données d'une application utilisant le protocole IPv6, une série représentant chaque application utilisant le protocole IPv6 est également tracée sur ce graphique.



- **Tableau Applications les plus populaires** : Il s'agit d'un tableau de statistiques pour chaque application. Le tableau répertorie toutes les applications pour lesquelles l'appliance a servi le trafic, ainsi que les taux d'envoi et de réception en bits par seconde, le nombre total d'octets envoyés et reçus, le pourcentage du trafic de l'application et le taux auquel l'appliance a servi le trafic pour l'application. Si l'appliance a servi le trafic d'une application à l'aide du protocole

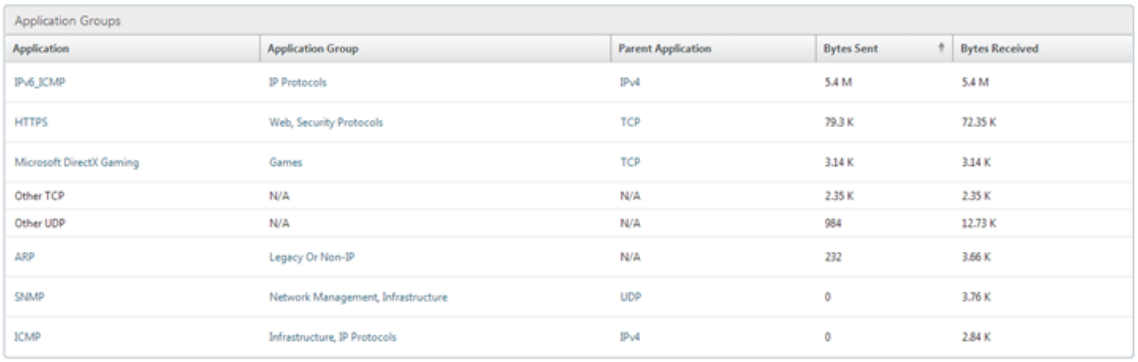
IPv6, l'application est répertoriée dans ce tableau, ainsi que ses statistiques.



Top Applications

Application	Sent Rate (bps)	Received Rate (bps)	Total Bytes Sent	Total Bytes Received	Total %	Order
IPv6_ICMP	719.56 K	719.56 K	5.4 M	5.4 M	98.3	1
HTTPS	10.57 K	9.64 K	79.3 K	72.35 K	1.38	2
Microsoft DirectX Gaming	416	416	3.14 K	3.14 K	0.06	4
Other TCP	312	312	2.35 K	2.35 K	0.04	5
Other UDP	128	1.7 K	984	12.73 K	0.12	3
ARP	24	488	232	3.66 K	0.04	6
SNMP	0	496	0	3.76 K	0.03	7
ICMP	0	376	0	2.84 K	0.03	8

- **Groupes d'applications** : il s'agit d'une table de statistiques pour chaque application, avec son groupe d'applications et l'application parent, le cas échéant. Le tableau répertorie les octets envoyés et reçus pour l'application. Chaque application, son groupe d'applications et son application parente sont affichés sous forme de liens hypertexte. Si vous cliquez sur le lien hypertexte, les détails granulaires des statistiques s'affichent pour le lien sur lequel vous avez cliqué. Si l'appliance a servi le trafic d'une application à l'aide du protocole IPv6, l'application est répertoriée dans ce tableau, ainsi que ses statistiques.



Application Groups

Application	Application Group	Parent Application	Bytes Sent	Bytes Received
IPv6_ICMP	IP Protocols	IPv4	5.4 M	5.4 M
HTTPS	Web, Security Protocols	TCP	79.3 K	72.35 K
Microsoft DirectX Gaming	Games	TCP	3.14 K	3.14 K
Other TCP	N/A	N/A	2.35 K	2.35 K
Other UDP	N/A	N/A	984	12.73 K
ARP	Legacy Or Non-IP	N/A	232	3.66 K
SNMP	Network Management, Infrastructure	UDP	0	3.76 K
ICMP	Infrastructure, IP Protocols	IPv4	0	2.84 K

L'onglet **Depuis le dernier redémarrage** contient des statistiques sur le trafic de l'application depuis le redémarrage de l'appliance. L'onglet contient les graphiques Pourcentage de débit total des liens d'application (envoyé) et Pourcentage de débit total des liens d'application (reçu), ainsi que les tableaux Applications et groupes d'applications les plus populaires, qui présentent des statistiques similaires à celles de l'onglet Graphiques d'applications les plus populaires, mais avec des données depuis le redémarrage de l'appliance. L'onglet Applications actives (depuis le dernier redémarrage) contient un tableau répertoriant toutes les applications actives depuis le redémarrage de l'appliance.** Ce tableau contient des détails sur le taux d'envoi et de réception, le nombre total d'octets envoyés et reçus et le nombre total de paquets envoyés et reçus pour les applications.

Définitions des liens

April 9, 2021

Les définitions de liens permettent à l'appliance d'éviter la congestion et la perte de vos liaisons WAN et d'effectuer le traffic shaping. Une définition de lien spécifie le trafic associé au lien défini, la bande passante maximale pour permettre le trafic reçu sur la liaison et la bande passante maximale pour le trafic envoyé sur la liaison. La définition identifie également le trafic comme trafic entrant ou sortant et comme trafic côté WAN ou côté LAN. Tout le trafic circulant à travers l'appliance est comparé à votre liste de définitions de lien, et la première définition correspondante identifie le lien auquel le trafic appartient.

En exécutant la procédure d'installation rapide, vous personnalisez les définitions de lien par défaut de l'appliance. Vous avez ensuite défini le lien de l'appliance au réseau étendu et sa liaison au réseau local. Pour un déploiement en ligne simple, aucune configuration supplémentaire des définitions de lien n'est nécessaire. D'autres types de déploiements nécessitent une configuration supplémentaire des définitions de liens.

Chaque liaison a deux limites de bande passante, représentant la vitesse d'envoi et la vitesse de réception. Ce n'est que lorsque la vitesse de liaison est connue que l'appliance peut injecter du trafic dans la liaison à la bonne vitesse, éliminant ainsi la congestion et la perte de paquets résultant d'une tentative d'envoi trop importante, ou la perte de performances résultant d'un envoi trop faible. Lorsqu'elle est placée entre un réseau local rapide et un WAN plus lent et agit comme *passerelle virtuelle,* l'appliance peut recevoir du trafic plus rapidement que le WAN ne peut l'accepter, ce qui crée un retard de trafic. L'existence de ce carnet de commandes permet à l'appliance de choisir le paquet à envoyer suivant, ce qui rend possible le traffic shaping. À moins qu'il y ait des paquets provenant de plusieurs flux à choisir, il n'y a pas de possibilité de privilégier un flux par rapport à l'autre. Le traffic shaping dépend donc de l'existence de la passerelle virtuelle et définit correctement les limites de bande passante.

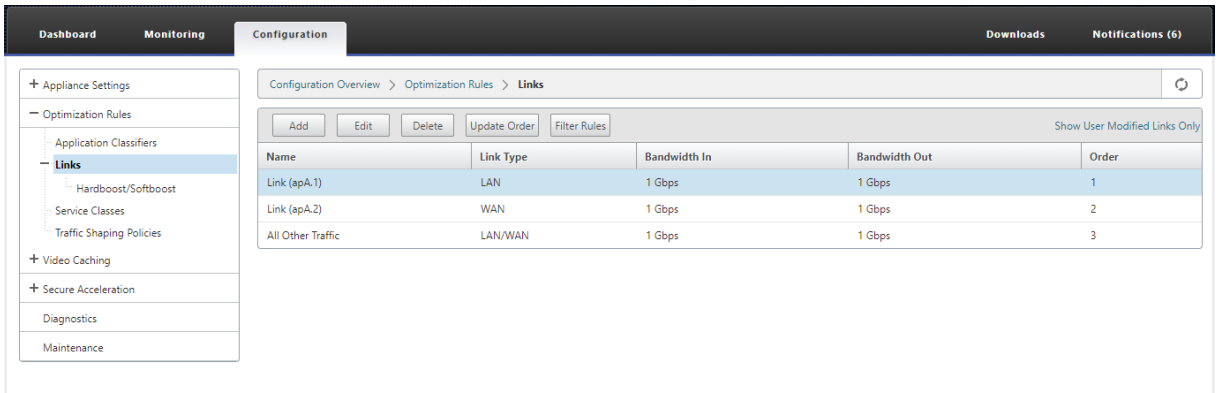
> **Remarque**
>
> Les définitions de lien s'appliquent normalement aux connexions à la paire accélérée de ports de pont. Les deux ports de carte mère, Primary et Aux1, peuvent également être définis comme des liens, mais cela sert rarement à quelque fin, car ils sont utilisés pour la gestion et comme un back-channel pour les modes haute disponibilité et groupe, et non pour le trafic WAN.
>
> **Important**
>
> Important : Pour des fins de définition de lien, un *lien* est un lien physique, avec sa propre capacité de bande passante. C'est généralement un câble qui quitte le bâtiment. Rappelez-vous les points suivants :
>
> - Un VLAN n'est pas un lien.
> - Un lien virtuel n'est pas un lien.
> - Un tunnel n'est pas un lien.

Définitions de liens par défaut

Accédez à **Configuration** > **Règles d'optimisation** > **Liens** pour afficher les liens actuellement définis. Les liens suivants sont définis par défaut.

1. **apA.1**, l'un des deux ports du pont accéléré.
2. **apA.2**, l'autre port sur le pont accéléré.
3. Si le système comporte des ponts à double accélération, APb.1 et APB.2 existent également.
4. Tout autre trafic, qui n'est pas un vrai lien, mais qui est un fourre-tout pour le trafic qui ne correspond à aucune définition de lien réelle.

L'ordre dans lequel les liens sont affichés sur cette page est significatif. Lorsque vous décidez du lien auquel appartient un paquet, l'appliance teste les liens dans l'ordre et le premier lien correspondant est sélectionné. Cela signifie que les définitions superposées sont autorisées et que la dernière définition du lien peut correspondre à tout le trafic, servant de lien par défaut. Pour modifier la commande, cliquez sur **Mettre à jour la commande**.



Gérer les définitions de liens dans le traffic shaping

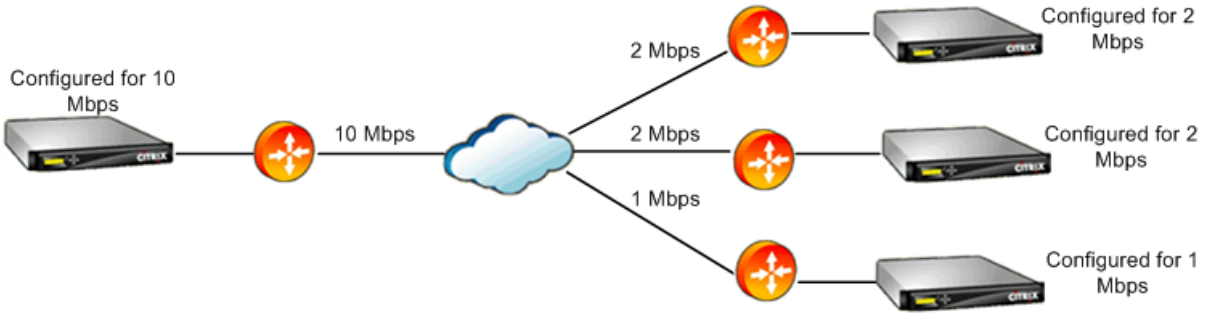
April 9, 2021

Pour gérer un lien, le régulateur du trafic a besoin des informations suivantes :

- La vitesse du lien dans les directions d'envoi et de réception.
- Indique si la liaison est une liaison WAN ou un réseau LAN.
- Un moyen de distinguer le trafic de liaison de l'autre trafic.
- La direction dans laquelle le trafic circule sur la liaison.

Vitesse de liaison : la *vitesse de liaison* fait toujours référence à la vitesse de la liaison physique. Dans le cas d'une liaison WAN, c'est la vitesse du segment WAN qui se termine dans le bâtiment avec l'appliance Citrix SD-WAN WANOP. La vitesse de l'autre extrémité du lien n'est pas prise en compte. Par exemple, la figure suivante montre un réseau de quatre appliances. Les bandes passantes entrantes et sortantes de chaque appliance sont définies à 95 % de la vitesse de son propre segment WAN local, sans tenir compte de la vitesse des points de terminaison distants.

Figure 1. Limites de bande passante locale pour suivre les vitesses de liaison locale



La raison pour laquelle les limites de bande passante sont fixées à 95 % de la vitesse de liaison au lieu de 100 % est de permettre la surcharge de liaison (peu de liaisons peuvent transporter des données à 100 % de leur vitesse publiée) et de s'assurer que l'appliance est légèrement plus lente que la liaison, de sorte qu'elle devient un léger goulot d'étranglement. Le traffic shaping n'est pas efficace sauf si le régulateur du trafic est le goulot d'étranglement dans la connexion.

Distinction de différents types de trafic : dans chaque définition de lien, vous devez indiquer si la définition s'applique à une liaison WAN ou à un réseau LAN.

Le régulateur du trafic doit savoir si un paquet se déplace sur le WAN et, le cas échéant, dans quelle direction. Pour fournir ces renseignements :

- Pour les déploiements en ligne simples, vous déclarez qu'un port du pont accéléré appartient à la liaison WAN et que l'autre port appartient au LAN.
- Dans d'autres modes de déploiement, l'appliance examine les adresses IP, les adresses MAC, les VLAN ou les groupes de services WCCP. (Notez que le test pour les groupes de services WCCP n'est pas encore pris en charge.)
- Si un site possède plusieurs WAN, les définitions de lien local doivent inclure des règles permettant à l'appliance de distinguer le trafic des différents WAN.

Configurer les définitions de liens

April 9, 2021

Les définitions de lien sont organisées dans une liste ordonnée, une entrée par lien, qui est testée de haut en bas pour chaque paquet entrant ou sortant de l'appliance. La première définition de correspondance détermine à quel lien appartient le paquet. Dans chaque définition de lien se trouve une liste ordonnée de règles, qui est également testée de haut en bas. Chaque paquet est comparé à ces règles, et s'il correspond à l'une d'entre elles, le paquet est considéré comme voyageant sur ce lien.

Dans une seule règle, les champs sont tous traités selon l'opérateur AND, de sorte que toutes les valeurs spécifiées doivent correspondre. Tous les champs ont la valeur par défaut Tout, une entrée générique qui correspond toujours. Lorsqu'un champ est constitué d'une liste, telle qu'une liste de sous-réseaux IP, les entrées de liste sont orées ensemble. Autrement dit, si un élément correspond, la liste dans son ensemble est considérée comme une correspondance.

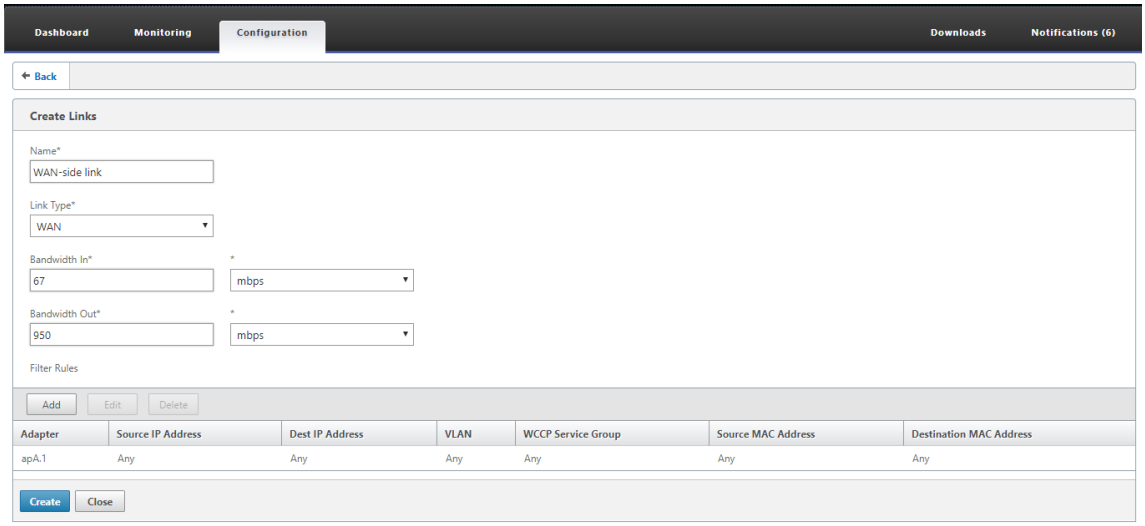
Les liens peuvent être basés sur l'adaptateur Ethernet associé au trafic, les adresses IP source et de destination, la balise VLAN, le groupe de services WCCP (pour WCCP-GRE uniquement) et l'adresse MAC Ethernet source et destination. Un déploiement en ligne simple peut identifier uniquement les ports de pont accéléré côté LAN et côté WAN (apA.1 et apA.2), tandis qu'un déploiement de centre de données complexe peut nécessiter l'utilisation de la plupart des options fournies pour désambiguïser le trafic.

La définition d'un lien en termes d'adresses IP est possible sauf lorsque des liens redondants sont utilisés. Étant donné qu'un paquet donné peut passer par un lien dans un déploiement active-standby ou active-active dual-link, une autre méthode doit être utilisée pour déterminer quel lien le paquet utilise. Si des ponts doubles sont utilisés, alors le trafic d'une liaison peut passer sur apA et l'autre sur APB, et les liens peuvent être définis en termes d'adaptateurs. Si les deux liens sont desservis par des routeurs différents, les adresses MAC des routeurs peuvent être utilisées pour distinguer le trafic. Lorsque tout le reste échoue, WCCP-GRE peut être utilisé, et le routeur peut utiliser un groupe de services différent pour chaque liaison WAN, permettant à l'unité Citrix SD-WAN WANOP de distinguer le trafic de liaison par groupe de services.

Citrix recommande des définitions de lien basées sur le port pour les déploiements en ligne simples, et des définitions de lien basées sur IP pour tous les autres déploiements.

Pour configurer les définitions de lien :

1. Accédez à **Configuration** > **Règles d'optimisation** > **Liens** et cliquez sur **Ajouter.**



2. Entrez des valeurs pour les paramètres suivants :

   - **Nom : Nom**descriptif du lien, qui peut également décrire s'il s'agit d'une liaison latérale LAN ou WAN.
   - **Type de lien** : Type de lien, LAN ou WAN.
   - **Bandwidth In** : limite de bande passante entrante.
   - **Sortie de bande passante** : limite de bande passante sortante.

3. Dans la section **Règles de filtrage**, cliquez sur **Ajouter** et entrez des valeurs pour les paramètres suivants :

   - **Adaptateur :** spécifie une liste d'adaptateurs (ports Ethernet). Lorsque les liens peuvent être identifiés par une carte Ethernet, cela simplifie la configuration.
   - **Adresse IP source :** Les règles IP source sont prises en compte pour les paquets entrant dans l'unité (les paquets sortant de l'unité sont ignorés). Sur ces paquets, les règles du champ IP Src sont comparées au champ Adresse source dans l'en-tête IP. La règle spécifie une liste d'adresses IP ou de sous-réseaux. Les correspondances négatives, telles que « Exclure 10.0.0.1 », sont également prises en charge.
   - **Adresse IP de destination :** Les règles IP de destination sont prises en compte pour les paquets sortant de l'unité (les paquets entrant dans l'unité sont ignorés). Sur ces paquets, les règles du champ IP Dst sont comparées au champ Adresse de destination dans l'en-tête IP. La règle spécifie une liste d'adresses IP ou de sous-réseaux. Les correspondances négatives, telles que « Exclure 10.0.0.1 », sont également prises en charge.
   - **VLAN :** les règles VLAN sont appliquées aux en-têtes VLAN des paquets entrant ou sortant de l'unité.

- Groupe de**services WCCP : Les règles Groupe** de services WCCP sont appliquées aux paquets WCCP encapsulés par GRE-encapsulés entrant ou sortant de l'unité. (Cela ne fonctionne pas avec L2 WCCP.)
- **Adresse MAC source :** L'adresse MAC source est utilisée comme critère de filtre.
- **Adresse MAC**de destination : adresse MAC de destination utilisée comme critère de dilter.

4. Cliquez sur **Créer**.

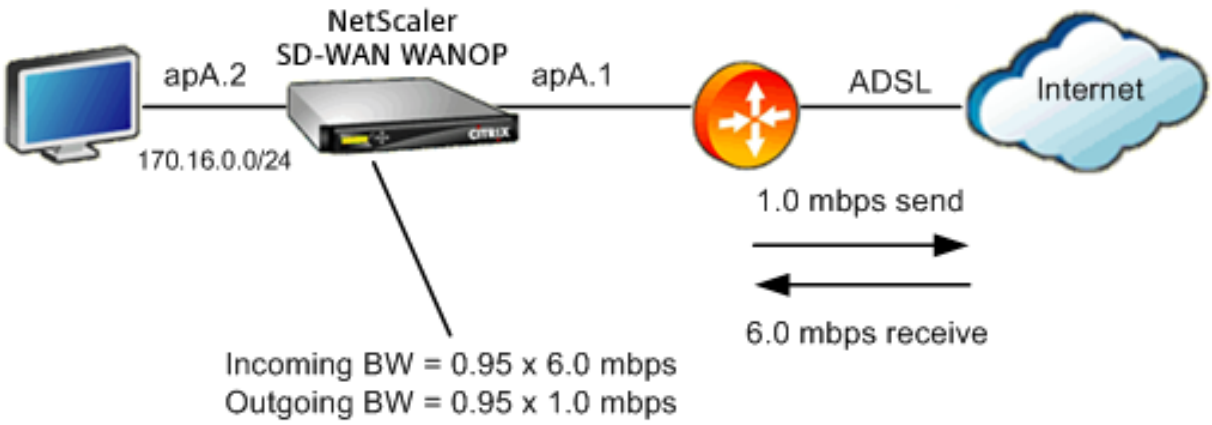
   Le classificateur de trafic utilise les champs Src IP et Dest IP de manière spécialisée (il en va de même pour Src MAC et Dst MAC) :

   - Le champ Src n'est examiné que sur les paquets entrant dans l'appliance.
   - Le Dst n'est examiné que sur les paquets sortant de l'appliance.

Liens en ligne

La plupart des appliances Citrix SD-WAN WANOP utilisent un déploiement en ligne simple, où chaque pont accéléré ne sert qu'une liaison WAN. C'est le mode le plus simple à configurer.

Lien en en ligne simple



Dans la figure ci-dessus, tout le trafic passant par le pont accéléré est supposé être du trafic WAN. La liaison est une liaison ADSL avec différentes vitesses d'envoi et de réception (6,0 Mbps vers le bas, 1,0 Mbps vers le haut). Le réseau étendu est connecté au port de pont accéléré apA.1, et le réseau local est connecté au port de pont accéléré apA.2.

Les tâches de définition de la liaison côté WAN (apA.1) sont les suivantes :

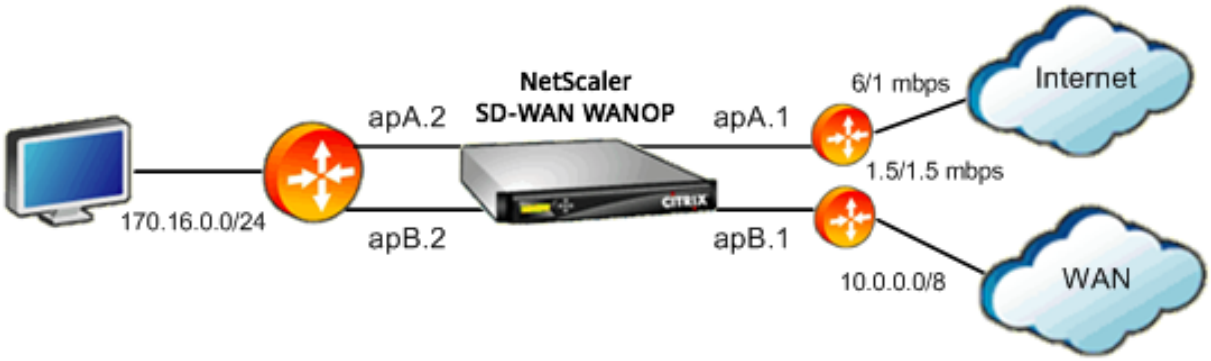
1. Donnez au WAN un nom descriptif, tel que « WAN to HQ (apA.1) ».
2. Définissez le type sur « WAN ».

3. Définissez les limites de bande passante entrante et sortante à 95 % de la vitesse de liaison nominale.
4. Vérifiez qu'une règle a été définie qui spécifie l'adaptateur Ethernet WAN, qui dans cet exemple est apA.
5. Cliquez sur Créer.

Les tâches pour le lien côté LAN (apA.2) sont similaires :

1. Donnez-lui un nom descriptif, tel que « Local LAN (apA.2) ».
2. Définissez le type sur « LAN ».
3. Définissez les limites de bande passante entrante et sortante à 95 % de la vitesse Ethernet nominale (95 Mbit/s ou 950 Mbit/s).
4. Vérifiez qu'il existe une règle spécifiant la carte Ethernet LAN, qui dans cet exemple est apA.2.
5. Cliquez sur Créer.

Déploiement en ligne avec deux ponts



La configuration est similaire à la configuration simple du lien en ligne, mais le site a un deuxième lien, un lien T1 vers le WAN de l'entreprise, en plus du lien Internet ADSL. L'appliance Citrix SD-WAN WANOP dispose de deux ponts accélérés, un pour chaque liaison WAN.

La configuration est presque aussi simple que le boîtier à pont unique, avec les étapes supplémentaires suivantes :

1. Modifiez une deuxième liaison WAN sur apB, qui dans ce cas est apB.1. Définissez le type sur « WAN ». Définissez la bande passante de la liaison sur 95 % de la vitesse T1 de 1,5 Mbit/s et donnez à la liaison un nouveau nom, tel que « WAN to HQ ».
2. Ajoutez une règle spécifiant APB.2 à la définition « LAN » et supprimez la définition de lien par défaut pour APB.2. (Vous pouvez également modifier la définition de lien par défaut pour APB.2 pour la spécifier en tant que lien LAN, comme cela a été fait pour apA.2.)

Liens non en ligne

Pour les déploiements en ligne autres que simples (qui ne servent qu'un seul réseau étendu par pont accéléré), utilisez des sous-réseaux IP au lieu des ports de pont pour distinguer le trafic LAN du trafic WAN. Cette approche est essentielle pour les déploiements à un bras, qui n'utilisent qu'un seul port de pont. Les sous-réseaux IP sont parfois utiles pour les déploiements en ligne, en particulier lorsque l'appliance dessert plusieurs réseaux WAN. Toutefois, pour les déploiements en ligne simples, les liens basés sur les ports sont plus faciles à définir.

Le classificateur de trafic applique une convention spécialisée lors de l'examen de l'IP Src et de l'IP Dst :

- Le champ IP Src n'est examiné que dans les paquets entrant dans l'appliance.
- Le champ IP Dst est examiné uniquement dans les paquets sortant de l'appliance.

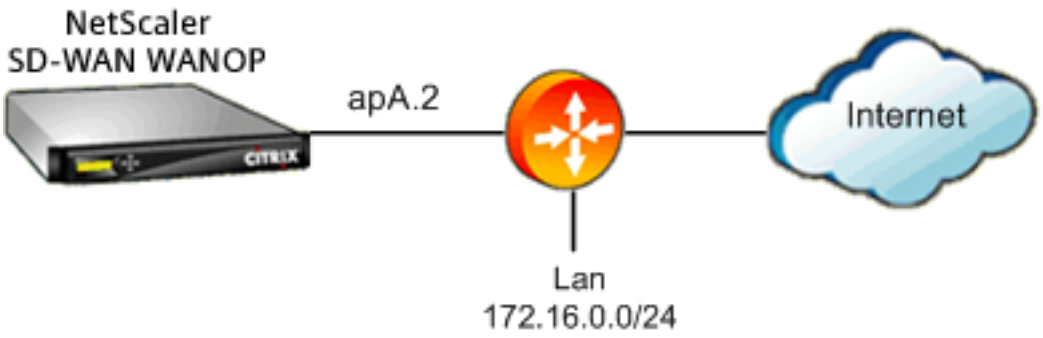
Cette convention peut parfois prêter à confusion, mais elle permet de considérer implicitement la direction du voyage par paquets comme faisant partie de la définition.

Utiliser l'adresse IP dans les définitions de lien

Pour configurer une définition LAN intégrée simple à l'aide de règles basées sur IP, vous pouvez définir les liaisons LAN et WAN sans spécifier les ports Ethernet, à l'aide du sous-réseau LAN à la place :

- Créez une règle pour la définition de lien LAN et spécifiez le sous-réseau LAN dans le champ IP Src.
- Créez une règle pour la définition de lien WAN et spécifiez le sous-réseau LAN (pas le sous-réseau WAN) dans le champ IP Dst.

Modes en ligne WCCP et Virtual



Configuration WCCP ou déploiement virtuel en ligne à l'aide de règles basées sur IP est identique à l'utilisation de l'adresse IP dans la définition de lien, car les sous-réseaux IP LAN et WAN sont identiques.

Lorsque WCCP-GRE est utilisé, les en-têtes GRE sont ignorés et les en-têtes IP dans les paquets de données encapsulés sont utilisés. Par conséquent, cette même définition de lien fonctionne pour les modes Inline WCCP-L2, WCCP-GRE, Inline et Virtual Inline.

(Les modes WCCP et virtuels en ligne nécessitent la configuration de votre routeur. WCCP nécessite également une configuration sur la page Configuration : Déploiements avancés.)

Gérer et surveiller à l'aide de Citrix Application Delivery Management

December 14, 2022

La prise en charge de Citrix SD-WAN WANOP AppFlow permet une surveillance flexible et personnalisée de vos appliances Citrix SD-WAN WANOP.

L'interface AppFlow fonctionne avec Citrix Application Delivery Management (ADM). Citrix ADM reçoit des informations détaillées de l'appliance, à l'aide de la norme ouverte AppFlow. Citrix ADM vous permet de surveiller, de gérer et d'afficher les analyses des appliances Citrix SD-WAN dans votre réseau.

Citrix ADM prend en charge un large éventail de périphériques et peut présenter une vue plus complète de votre réseau. L'appliance WANOP Citrix SD-WAN offre une vue étendue du trafic WAN, y compris des statistiques détaillées sur le trafic des Applications virtuelles/bureaux virtuels. Elle fournit des informations clés sur l'expérience utilisateur WAN.

Pour de plus amples informations, consultez la section Gestion des instances Citrix SD-WAN à l'aide de Citrix Application Delivery Management.

Exemple d'applications virtuelles/bureaux virtuels

Dans un environnement Citrix Virtual Apps and Desktops, si un utilisateur de branche rencontre de faibles performances, l'administrateur peut devoir surveiller le réseau, les utilisateurs et les applications hébergées sur des applications virtuelles ou des bureaux virtuels. Les administrateurs peuvent avoir besoin de poser les questions suivantes :

- Quelle partie du réseau cause une mauvaise expérience utilisateur ?
- Quel est un moyen facile d'identifier la lenteur dans les applications publiées ?
- Quels canaux virtuels consomment le plus de bande passante sur une période donnée ?
- Quels utilisateurs de bureaux virtuels ou d'applications virtuelles consomment le plus de bande passante sur une période donnée ?
- Pour un utilisateur de bureaux virtuels donné, quelle est la latence moyenne côté client et serveur, et la gigue moyenne ?
- Quelles sont les meilleures applications pour tous les utilisateurs d'applications virtuelles, par temps de disponibilité et nombre total de lancements sur une période donnée ?
- Qu'est-ce que la latence du centre de données ?

La prise en charge de Citrix SD-WAN WANOP AppFlow fournit des réponses à toutes les questions ci-dessus, permettant, par exemple, de distinguer une liaison WAN encombrée d'un serveur lent ou d'un client lent.

Citrix Cloud Connector

April 23, 2021

La fonction Citrix Cloud Connector de l'appliance Citrix SD-WAN WANOP connecte les centres de données d'entreprise aux clouds externes et aux environnements d'hébergement, ce qui fait du cloud une extension sécurisée de votre réseau d'entreprise. Les applications hébergées dans le cloud semblent s'exécuter sur un réseau d'entreprise contigu. Avec Citrix Cloud Connector, vous pouvez augmenter vos centres de données avec la capacité et l'efficacité disponibles auprès des fournisseurs de cloud.

Citrix Cloud Connector vous permet de déplacer vos applications vers le cloud afin de réduire les coûts et d'augmenter la fiabilité.

La fonctionnalité d'optimisation du réseau étendu de l'appliance Citrix SD-WAN WANOP accélère le trafic, offrant des performances de type LAN pour les applications exécutées sur les centres de données et les clouds d'entreprise.

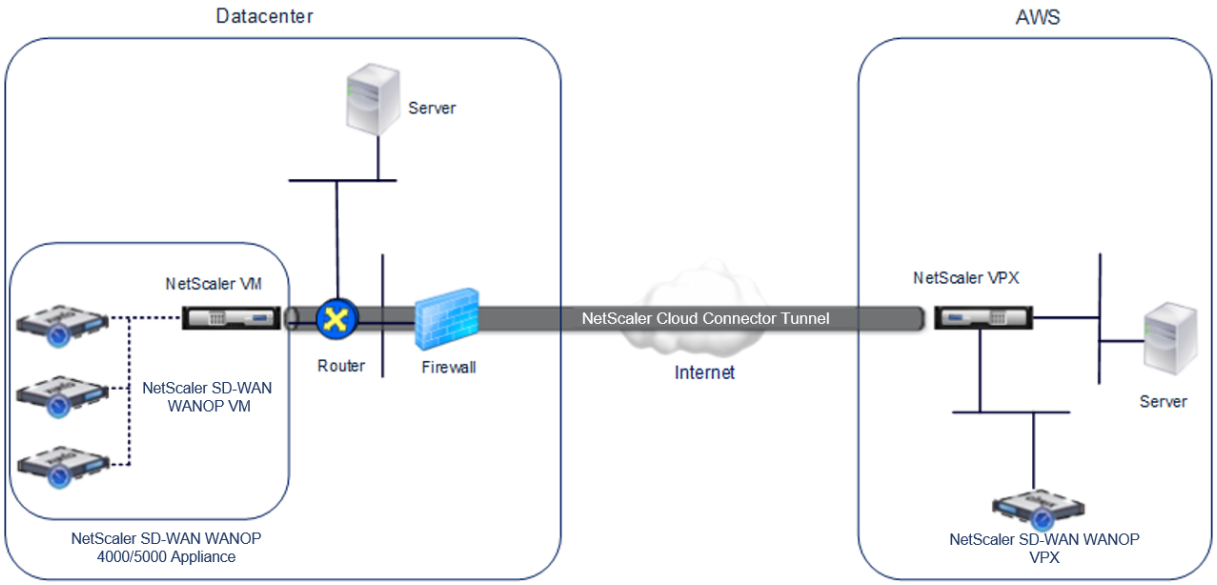
Outre l'utilisation de Citrix Cloud Connector entre un centre de données et un cloud, vous pouvez l'utiliser pour connecter deux centres de données pour une liaison sécurisée et accélérée haute capacité.

Pour implémenter la solution Citrix Cloud Connector, vous connectez un centre de données à un autre centre de données ou à un cloud externe en configurant un tunnel appelé Citrix Cloud Connector.

Pour connecter un centre de données à un autre centre de données, vous configurez un tunnel Citrix Cloud Connector entre deux appliances, une dans chaque centre de données.

Pour connecter un centre de données à un cloud externe (par exemple, le cloud Amazon AWS), vous configurez un tunnel Citrix Cloud Connector entre une appliance Citrix SD-WAN WANOP dans le centre de données et une appliance virtuelle (VPX) résidant dans le Cloud. Le point d'extrémité distant peut être un Citrix Cloud Connector ou un Citrix VPX avec licence platine.

L'illustration suivante montre un tunnel Citrix Cloud Connector configuré entre un centre de données et un cloud externe.



Les appliances entre lesquelles un tunnel Citrix Cloud Connector est configuré sont appelées *points d'extrémité* ou *homologues* du tunnel Citrix Cloud Connector.

Un tunnel Citrix Cloud Connector utilise les protocoles suivants :

- Protocole GRE (Generic Routing Encapsulation)
- Suite de protocole IPsec standard ouverte, en mode transport

Le protocole GRE fournit un mécanisme pour encapsuler les paquets, à partir d'une grande variété de protocoles réseau, à transférer sur un autre protocole. Le GRE est utilisé pour :

- Connectez des réseaux exécutant des protocoles non IP et non routables.

- Pont sur un réseau étendu (WAN).
- Créez un tunnel de transport pour tout type de trafic qui doit être envoyé inchangé sur un autre réseau.

Le protocole GRE encapsule les paquets en ajoutant un en-tête GRE et un en-tête GRE IP aux paquets.

La suite de protocoles IPSec (Internet Protocol security) sécurise la communication entre pairs dans le tunnel Citrix Cloud Connector.

Dans un tunnel Citrix Cloud Connector, IPsec garantit :

- Intégrité des données
- Authentification de l'origine des données
- Confidentialité des données (cryptage)
- Protection contre les attaques de relecture

IPSec utilise le mode de transport dans lequel le paquet encapsulé GRE est chiffré. Le chiffrement est effectué par le protocole ESP (Encapsulating Security Payload). Le protocole ESP assure l'intégrité du paquet à l'aide d'une fonction de hachage HMAC et assure la confidentialité à l'aide d'un algorithme de chiffrement. Une fois le paquet chiffré et le HMAC calculé, un en-tête ESP est généré. L'en-tête ESP est inséré après l'en-tête IP GRE et une remorque ESP est insérée à la fin de la charge utile chiffrée.

Les homologues du tunnel Citrix Cloud Connector utilisent le protocole IKE (Internet Key Exchange version) (partie de la suite de protocoles IPSec) pour négocier une communication sécurisée, comme suit :

- Les deux pairs s'authentifient mutuellement les uns avec les autres, en utilisant l'une des méthodes d'authentification suivantes :
  - **Authentification de clé pré-partagée**. Une chaîne de texte appelée clé pré-partagée est configurée manuellement sur chaque pair. Les clés pré-partagées des pairs sont comparées les unes aux autres pour l'authentification. Par conséquent, pour que l'authentification réussisse, vous devez configurer la même clé pré-partagée sur chacun des homologues.
  - **Authentification des certificats numériques**. L'homologue initiateur (expéditeur) signe les données d'échange de messages à l'aide de sa clé privée, et l'autre homologue récepteur utilise la clé publique de l'expéditeur pour vérifier la signature. Généralement, la clé publique est échangée dans des messages contenant un certificat X.509v3. Ce certificat fournit un niveau d'assurance que l'identité d'un pair représentée dans le certificat est associée à une clé publique particulière.
- Les pairs négocient ensuite pour parvenir à un accord sur :

- Un algorithme de chiffrement.
- Clés cryptographiques pour chiffrer les données dans un pair et déchiffrer les données dans l'autre.

Cet accord sur le protocole de sécurité, l'algorithme de chiffrement et les clés cryptographiques est appelé une association de sécurité (SA). Les SA sont unidirectionnelles (simplex). Par exemple, lorsque deux homologues, CB1 et CB2, communiquent via un tunnel Connector, CB1 a deux associations de sécurité. Une SA est utilisée pour le traitement des paquets sortants et l'autre SA pour le traitement des paquets entrants.

Les SA expirent après une durée spécifiée, appelée *durée de vie*. Les deux homologues utilisent le protocole IKE (Internet Key Exchange) (partie de la suite de protocoles IPSec) pour négocier de nouvelles clés cryptographiques et établir de nouvelles SA. Le but de la durée de vie limitée est d'empêcher les attaquants de craquer une clé.

En outre, les instances Citrix SD-WAN WANOP sur les points d'extrémité
du tunnel Citrix Cloud Connector offrent une optimisation WAN sur le tunnel.

Conditions préalables pour configurer le tunnel Citrix Cloud Connector

Avant de configurer un tunnel Citrix Cloud Connector entre AWS Cloud et un dispositif Citrix SD-WAN WANOP configuré pour le mode monobras dans le centre de données, vérifiez que les tâches suivantes ont été effectuées :

1. Assurez-vous que l'appliance Citrix SD-WAN WANOP dans le centre de données est correctement configurée. Pour plus d'informations sur le déploiement d'une appliance Citrix SD-WAN en mode monobras qui utilise le protocole WCCP/Virtual Inline, reportez-vous à la section Sites avec un routeur WAN.
2. Installez, configurez et lancez une appliance virtuelle Citrix (instance VPX) sur le cloud AWS. Pour de plus amples informations, consultez la section Installation de NetScaler VPX sur AWS.
3. Installez, configurez et lancez une instance de Citrix SD-WAN WANOP (VPX) sur le cloud AWS. Pour de plus amples informations, consultez la section Installation de l'AMI S SD-WAN VPX sur Amazon AWS.
4. Sur AWS, liez l'instance Citrix SD-WAN WANOP VPX sur AWS à un serveur virtuel d'équilibrage de charge dans l'instance Citrix VPX sur AWS. Cette liaison est requise pour l'envoi de trafic via les instances Citrix SD-WAN WANOP VPX, afin d'optimiser le réseau étendu via le tunnel Citrix Cloud Connector.

Pour créer un serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **enable ns mode** l2
- **add lb vserver** <cbvpxonaws_vs_name> ANY * * -**l2Conn** ON -**m** MAC

Pour ajouter l'instance Citrix SD-WAN WANOP VPX sur AWS en tant que service et la lier au serveur virtuel d'équilibrage de charge à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add service** < cbvpxonaws_service_name> <cbvpxonaws_IP> ANY * -**cltTimeout** 14400 -**svrTimeout** 14400
- **bind lb vserver** <cbvpxonaws_vs_name> <cbvpxonaws_service_name>

Configurer le tunnel du connecteur cloud

April 23, 2021

Pour configurer le tunnel Citrix Cloud Connector, utilisez l'utilitaire de configuration des deux appliances Citrix VPX pour effectuer les tâches suivantes :

- **Créer un profil IPSec** : une entité de profil IPSec spécifie les paramètres du protocole IPSec, tels que la version IKE, l'algorithme de chiffrement, l'algorithme de hachage et PSK, à utiliser par le protocole IPSec dans le tunnel Citrix Cloud Connector.
- **Créer un tunnel IP et associer le profil IPSec à celui-ci** : un tunnel IP spécifie l'adresse IP locale, l'adresse IP distante, le protocole utilisé pour configurer le tunnel Citrix Cloud Connector et une entité de profil IPSec. L'entité de tunnel IP créée est également appelée entité de tunnel Citrix Cloud Connector.
- **Créer une règle PBR et associer le tunnel IP à celle-ci** : une entité PBR spécifie un ensemble de conditions et une entité tunnel IP (tunnel Citrix Cloud Connector). La plage d'adresses IP source et la plage d'adresses IP de destination sont les conditions de l'entité PBR. Vous devez définir la plage d'adresses IP source et la plage d'adresses IP de destination pour spécifier le sous-réseau dont le trafic doit traverser le tunnel Citrix Cloud Connector. Par exemple, considérez un paquet de requête qui provient d'un client sur le sous-réseau du centre de données et qui est destiné à un serveur sur le sous-réseau dans le cloud AWS. Si ce paquet correspond à la plage d'adresses IP source et de destination de l'entité PBR sur l'appliance virtuelle Citrix sur l'appliance Citrix SD-WAN WANOP dans le centre de données, il est pris en compte pour le traitement Citrix SD-WAN WANOP, qui envoie le paquet à travers le tunnel Citrix Cloud Connector associé à l'entité PBR.

Pour créer un profil IPSEC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ipsec profile** \<ipsec_profile_name\> -**encAlgo** AES -**hashAlgo** HMAC_SHA1 -**lifetime** 500 -**psk** \<password\>

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add iptunnel** \<tunnel_name\> \<Remote CBC Public IP\> \<remote_cbs_Netmask\> \<lan_subnet_IP\> -**protocol** GRE -**ipsecProfileName** \<ipsec_profile\>

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'interface de ligne de commande :

À l'invite de commandes, tapez :

- **add ns pbr** \<pbr_name\> ALLOW -**srcIP** = \<local_lan_subnet\> -**destIP** = \<remote_lan_subnet\> -**ipTunnel** \<tunnel_name\>
- **apply ns pbrs**

Pour créer un profil IPSEC à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **Citrix Cloud Connector** > **Profil IPsec**.
2. Dans le volet d'informations, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un profil IPsec, définissez les paramètres suivants :
   - Nom
   - Algorithme de chiffrement
   - Algorithme de hachage
   - Version du protocole IKE (sélectionnez V2)
4. Utilisez l'une des méthodes d'authentification IPsec suivantes à utiliser par les deux homologues pour s'authentifier mutuellement.
   - Pour la méthode d'authentification de clé pré-partagée, définissez le paramètre Clé pré-partagée existe.
   - Pour la méthode d'authentification des certificats numériques, définissez les paramètres suivants :
     - Clé publique

- Clé privée
- Clé publique homologue

5. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer un tunnel IP et lier le profil IPSEC à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **Citrix Cloud Connector** > **Tunnels IP**.
2. Sous l'onglet Tunnels IPv4, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Ajouter un tunnel IP, définissez les paramètres suivants :
   - Nom
   - IP distante
   - Masque distant
   - Type IP local (dans la liste déroulante Type IP local, sélectionnez IP du sous-réseau).
   - IP locale (Toutes les adresses IP configurées du type d'IP sélectionné seront renseignées dans la liste déroulante IP locale. Sélectionnez l'adresse IP souhaitée dans la liste.)
   - Protocole
   - Profil IPsec
4. Cliquez sur **Créer**, puis sur **Fermer**.

Pour créer une règle PBR et y lier le tunnel IPSEC à l'aide de l'utilitaire de configuration :

1. Accédez à **Système** > **Réseau** > **PBR**.
2. Sous l'onglet PBR, cliquez sur **Ajouter**.
3. Dans la boîte de dialogue Créer PBR, définissez les paramètres suivants :
   - Nom
   - Action
   - Type de saut suivant (Select IP Tunnel)
   - Nom du tunnel IP
   - IP source Faible
   - IP source élevée
   - IP de destination faible
   - IP de destination élevée

4. Cliquez sur **Créer**, puis sur **Fermer**.

   La nouvelle configuration du tunnel Citrix Cloud Connector sur l'appliance Citrix SD-WAN WANOP dans le centre de données apparaît sous l'onglet Accueil de l'interface utilisateur du Service de gestion.

   La nouvelle configuration de tunnel Citrix Cloud Connector correspondante sur l'appliance Citrix VPX dans le cloud AWS apparaît dans l'utilitaire de configuration.

   L'état actuel du tunnel Citrix Cloud Connector est indiqué dans le volet Citrix SD-WAN WANOP configuré. Un point vert indique que le tunnel est actif. Un point rouge indique que le tunnel est arrêté.

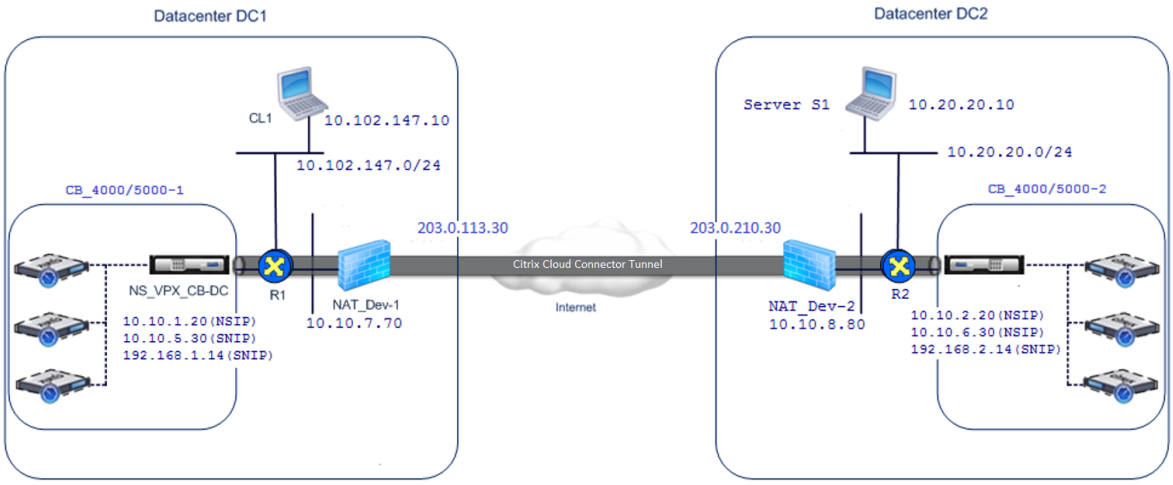
Configurer un tunnel de connecteur cloud entre deux centres de données

April 23, 2021

Vous pouvez configurer un tunnel Citrix Cloud Connector entre deux centres de données différents pour étendre votre réseau sans le reconfigurer et exploiter les capacités des deux centres de données. Un tunnel Citrix Cloud Connector entre les deux centres de données séparés géographiquement vous permet d'implémenter la redondance et de protéger votre installation contre les défaillances. Le tunnel Citrix Cloud Connector permet d'optimiser l'utilisation de l'infrastructure et des ressources entre deux centres de données. Les applications disponibles dans les deux centres de données apparaissent comme locales pour l'utilisateur.

Pour connecter un centre de données à un autre centre de données, vous configurez un tunnel Citrix Cloud
Connector entre une appliance SD-WAN WANOP 4000/5000 résidant dans un centre de données et une autre appliance SD-WAN WANOP 4000/5000 résidant dans l'autre centre de données.

Pour comprendre comment un tunnel Citrix Cloud Connector est configuré entre deux centres de données différents, considérez un exemple dans lequel un tunnel Cloud Connector est configuré entre l'appliance Citrix CB_4000/5000-1 dans le centre de données DC1 et l'appliance Citrix CB_4000/5000-2 dans le centre de données DC2.



CB_4000/5000-1 et CB_4000/5000-2 fonctionnent en mode un bras (WCCP/PBR). Ils permettent la communication entre les réseaux privés dans les centres de données DC1 et DC2. Par exemple, CB_4000/5000-1 et CB_4000/5000-2 permettent la communication entre le CL1 client dans le centre de données DC1 et le serveur S1 dans le centre de données DC2 via le tunnel Citrix Cloud Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Pour une communication correcte entre CL1 et S1, le mode L3 est activé sur NS_VPX_CB_4000/5000-1 et NS_VPX_CB_4000/5000-2, et les routes sont configurées comme suit :

- Le routeur R1 a une route pour atteindre S1 via NS_VPX_CB_ 4000/5000-1.
- NS_VPX_CB_4000/5000_1 a une route pour atteindre NS_VPX-CB_4000/5000-2 via R1.
- S1 devrait avoir un itinéraire atteignant CL1 via NS_VPX-CB_4000/5000-2.
- NS_VPX-CB_4000/5000-2 a une route pour atteindre NS_VPX_CB_4000/5000-1 à R2.

Le tableau suivant répertorie les paramètres de CB_4000/5000-1 dans le centre de données DC1.

Entité	Nom	Détails
Adresse IP du client CL1		10.102.147.10
Paramètres sur le périphérique NAT NAT-Dev-1		
Adresse IP NAT côté public		203.0.113.30*
Adresse IP NAT côté privé		10.10.7.70
Paramètres sur CB_4000/5000-1		
Adresse IP du service de gestion de CB_4000/5000-1		10.10.1.10

Entité	Nom	Détails
Paramètres sur NS_VPX_CB_4000/5000-1 en cours d'exécution sur CB_4000/5000-1		
Adresse NSIP		10.10.1.20
Adresse SNIP		10.10.5.30
Tunnel Cloud Connector	Cloud_Connector_DC1-DC2	Adresse IP du point de terminaison local du tunnel Citrix Cloud Connector = 10.10.5.30, Adresse IP du point de terminaison distant du tunnel Citrix Cloud Connector = 203.0.210.30* **Détails du tunnel GRE** Nom = Cloud_Connector_DC1-DC2 **Détails du profil IPsec** Nom = Cloud_Connector_DC1-DC2, Algorithme de chiffrement = AES, Algorithme de hachage = HMAC SHA1
Itinéraire basé sur des stratégies	CBC_DC1_DC2_PBR	Plage IP source = Sous-réseau dans datacenter1 = 10.102.147.0-10.102.147.255, Plage IP de destination = Sous-réseau dans datacenter2 = 10.20.20.0-10.20.20.255, Type de saut suivant = Tunnel IP, nom du tunnel IP = CBC_DC1_DC2

*Doivent être des adresses IP publiques.

Le tableau suivant répertorie les paramètres de CB-4000/5000-2 dans le centre de données DC2.

Entité	Nom	Détails
Adresse IP du serveur S1		10.20.20.10
Paramètres sur le périphérique NAT NAT-Dev-2		
Adresse IP NAT côté public		203.0.210.30*
Adresse IP NAT côté privé		10.10.8.80
Paramètres sur CB_4000/5000-2		
Adresse IP du service de gestion de CB_SDX-1		10.10.2.10
Paramètres sur NS_VPX_CB_4000/5000-2 en cours d'exécution sur CB_4000/5000-2		
Adresse NSIP		10.10.2.20
Adresse SNIP		10.10.6.30
Tunnel Citrix Cloud Connector	Cloud_Connector_DC1-DC2	Adresse IP du point de terminaison local du tunnel Citrix Cloud Connector = 10.10.6.30, Adresse IP du point de terminaison distant du tunnel Citrix Cloud Connector = 203.0.113.30* **Détails du tunnel GRE** Nom = Cloud_Connector_DC1-DC2 **Détails du profil IPsec** Nom = Cloud_Connector_DC1-DC2, Algorithme de chiffrement = AES, Algorithme de hachage = HMAC SHA1

Entité	Nom	Détails
Itinéraire basé sur des stratégies	CBC_DC1_DC2_PBR	Plage IP source = Sous-réseau dans datacenter2 = 10.20.20.0-10.20.20.255, Plage IP de destination = Sous-réseau dans datacenter1 = 10.102.147.0-10.102.147.255, Type de saut suivant = Tunnel IP, nom du tunnel IP = CBC_DC1_DC2

*Doivent être des adresses IP publiques.

Voici le flux de trafic dans le tunnel Citrix Cloud Connector :

1. Client CL1 envoie une requête au serveur S1.
2. La demande atteint l'appliance virtuelle Citrix NS_VPX_CB_4000/5000-1 qui s'exécute sur l'appliance Citrix SD-WAN WANOP CB_4000/5000-1.
3. NS_VPX_CB_4000/5000-1 transfère le paquet à l'une des instances WANOP SD-WAN exécutées sur l'appliance Citrix SD-WAN WANOP CB_4000/5000-1 pour l'optimisation WAN. Après le traitement du paquet, l'instance WANOP SD-WAN renvoie le paquet à NS_VPX_CB_4000/5000-1.
4. Le paquet de requête correspond à la condition spécifiée dans l'entité PBR CBC_DC1_DC2_PBR (configurée dans NS_VPX_CB_4000/5000-1), car l'adresse IP source et l'adresse IP de destination du paquet de requête appartiennent respectivement à la plage IP source et à la plage IP de destination définies dans CBC_DC1_DC2_PBR.
5. Étant donné que le tunnel CBC_DC1_DC2_PBR est lié à CBC_DC1_DC2_PBR, l'appliance prépare le paquet à envoyer à travers le tunnel Cloud_Connector_DC1-DC2.
6. NS_VPX_CB_4000/5000-1 utilise le protocole GRE pour encapsuler chacun des paquets de requête en ajoutant un en-tête GRE et un en-tête GRE IP au paquet. Dans l'en-tête IP GRE, l'adresse IP de destination est l'adresse du point d'extrémité du tunnel de connecteur de cloud (Cloud_Connector_DC1-DC2) dans le centre de données DC2.
7. Pour le tunnel Cloud Connector Cloud_Connector_DC1-DC2, NS_VPX_CB_4000/5000-1 vérifie les paramètres d'association de sécurité StoreDipsec (SA) pour le traitement des paquets sortants, comme convenu entre NS_VPX_CB_4000/5000-1 et NS_VPX_CB_4000/5000-2. Le protocole ESP (Encapsulating Security Payload) IPsec dans NS_VPX_CB_4000/5000-1 utilise ces paramètres SA pour les paquets sortants, pour chiffrer la charge utile du paquet encapsulé GRE.

8. Le protocole ESP assure l'intégrité et la confidentialité du paquet en utilisant la fonction de hachage HMAC et l'algorithme de chiffrement spécifié pour le tunnel Cloud_Connector_DC1-DC2 de Citrix Cloud Connector. Le protocole ESP, après avoir chiffré la charge utile GRE et calculé le HMAC, génère un en-tête ESP et un code de fin ESP et les insère avant et à la fin de la charge utile GRE cryptée, respectivement.
9. NS_VPX_CB_4000/5000-1 envoie le paquet résultant NS_VPX_CB_4000/5000-2.
10. NS_VPX_CB_4000/5000-2 vérifie les paramètres d'association de sécurité IPSec stockés pour le traitement des paquets entrants, comme convenu entre CB_DC-1 et NS_VPX-AWS pour le tunnel Cloud Connector Cloud_Connector_DC1-DC2. Le protocole IPsec ESP sur NS_VPX_CB_4000/5000-2 utilise ces paramètres SA pour les paquets entrants, et l'en-tête ESP du paquet de requête, pour déchiffrer le paquet.
11. NS_VPX_CB_4000/5000-2 puis décapsule le paquet en supprimant l'en-tête GRE.
12. NS_VPX_CB_4000/5000-2 transfère le paquet obtenu à CB_VPX_CB_4000/5000-2, qui applique le traitement lié à l'optimisation WAN au paquet. CB_VPX_CB_4000/5000-2 renvoie ensuite le paquet obtenu à NS_VPX_CB_4000/5000-2.
13. Le paquet résultant est le même que celui qui a été reçu par CB_VPX_CB_4000/5000-2 à l'étape 2. Ce paquet a l'adresse IP de destination définie sur l'adresse IP du serveur S1. NS_VPX_CB_4000/5000-2 transmet ce paquet au serveur S1.
14. S1 traite le paquet de requête et envoie un paquet de réponse. L'adresse IP de destination dans le paquet de réponse est l'adresse IP du client CL1 et l'adresse IP source est l'adresse IP du serveur S1.

Configurer un tunnel de connecteur cloud entre un centre de données et AWS/Azure

April 9, 2021

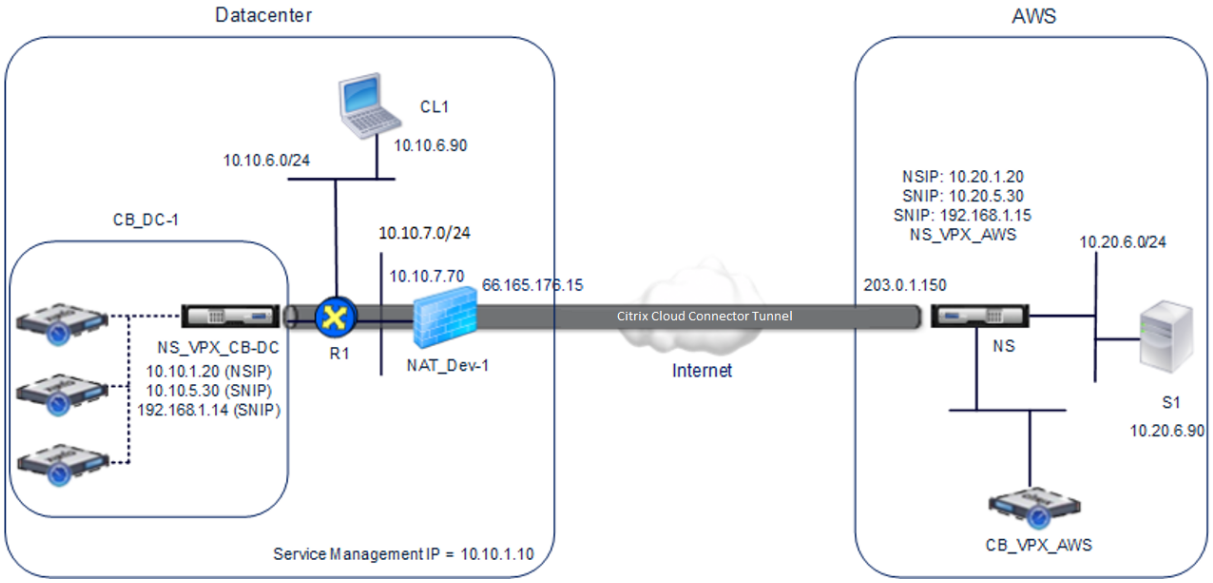
Vous pouvez configurer un tunnel de connecteur de cloud entre un centre de données et AWS, ou le cloud Azure.

Prenons un exemple dans lequel un tunnel Citrix Cloud Connector est configuré entre l'appliance Citrix SD-WAN WANOP CB_DC-1, déployée en mode monobras WCCP/PBR dans un centre de données, et le cloud AWS. CB_DC-1 est connecté au routeur R1. Un périphérique NAT est également connecté à R1 pour les connexions entre le centre de données et Internet.

Remarque : les paramètres de l'exemple fonctionnent également pour tout type de déploiement Citrix SD-WAN WANOP. Ce paramètre de cet exemple inclut des routes basées sur des stratégies au lieu

de Netbridge pour permettre au trafic du sous-réseau souhaité de passer par le tunnel Citrix Cloud Connector.

Comme illustré dans la figure suivante, le tunnel de connecteur Citrix Cloud est établi entre l'appliance virtuelle Citrix NS_VPX_CB-DC, s'exécutant sur l'appliance Citrix SD-WAN WANOP CB_DC-1, et l'appliance virtuelle Citrix NS_VPX-AWS exécutée sur le cloud AWS. Pour optimiser le flux de trafic via le tunnel Citrix Cloud Connector, NS_VPX_CB-DC est couplé aux instances Citrix SD-WAN WANOP exécutées sur CB_DC-1, et du côté AWS, l'appliance virtuelle Citrix SD-WAN WANOP CB_VPX-AWS exécutées sur AWS est jumelée à NS_VPX-AWS.



Le tableau suivant répertorie les paramètres du centre de données dans cet exemple.

Entité	Nom	Détails
Adresse IP du client CL1		10.10.6.90
Paramètres sur le périphérique NAT NAT-Dev-1		
Adresse IP NAT côté public		66.165.176.15 *
Adresse IP NAT côté privé		10.10.7.70
Paramètres sur CB_DC-1		
Adresse IP du service de gestion de CB_DC-1		10.10.1.10
Paramètres sur NS_VPX_CB-DC s'exécutant sur CB_DC-1		

Entité	Nom	Détails
Adresse NSIP		10.10.1.20
Adresse SNIP		10.10.5.30
Profil IPSec	CBC_DC_AWS_IPSEC_profile	Version IKE = v2, Algorithme de chiffrement = AES, Algorithme de hachage = HMAC SHA1
Tunnel Cloud Connector	CBC_DC_AWS	Adresse IP du point de terminaison local du tunnel Cloud Connector = 10.10.5.30, Adresse IP du point de terminaison distant du Cloud Connector = Adresse EIP publique mappée à l'adresse de point de terminaison Cloud Connector (SNIP) sur NS_VPX-AWS sur AWS = 203.0.1.150*, protocole de tunnel = GRE et IPSEC, nom du profil IPSec = CBC_DC_AWS_AWS_IPSEC_IPSEC_IPSEC_Pr
Itinéraire basé sur des règles	CBC_DC_AWS_PBR	Plage IP source = Sous-réseau dans le centre de données = 10.10.6.0-10.10.6.255, Plage IP de destination = Sous-réseau dans AWS = 10.20.6.0-10.20.6.255, Type de saut suivant = Tunnel IP, nom du tunnel IP = CBC_DC_AWS

*Doivent être des adresses IP publiques.

Le tableau suivant répertorie les paramètres du cloud AWS dans cet exemple.

Entité	Nom	Détails
——	—-	——-
Adresse IP du serveur S1		10.20.6.90
Paramètres sur NS_VPX-AWS
Adresse du NSIP		10.20.1.20
Adresse EIP publique mappée à l'adresse NSIP		203.0.1.120*

Adresse SNIP		10.20.5.30
Adresse EIP publique mappée à l'adresse SNIP		203.0.1.150*
IPSec profile	CBC_DC_AWS_IPSec_Profile
IKE version = v2, Encryption algorithm = AES, Hash algorithm = HMAC SHA1
Cloud Connector tunnel	CBC_DC_AWS	Local endpoint IP address of the Cloud Connector tunnel =10.20.5.30, Remote endpoint IP address of the Cloud Connector tunnel = Public NAT IP address of NAT device NAT-Dev-1 in the datacenter = 66.165.176.15*, Tunnel protocol = GRE and IPSEC, IPSec profile name = CBC_DC_AWS_IPSec_Profile
Policy based route	CBC_DC_AWS_PBR	Source IP range = Subnet in the AWS = 10.20.6.0-10.20.6.255, Destination IP range = Subnet in datacenter = 10.10.6.0-10.10.6.255, Next hop type = IP Tunnel, IP tunnel name = CBC_DC_AWS

*Doivent être des adresses IP publiques.

NS_VPX_CB-DC, sur CB_DC-1, et NS_VPX-AWS fonctionnent en mode L3. Ils permettent la communication entre les réseaux privés dans le centre de données et le cloud AWS. NS_VPX_CB-DC et NS_VPX-AWS permettent la communication entre le client CL1 dans le centre de données et le serveur S1 dans le cloud AWS via le tunnel Cloud Connector. Le client CL1 et le serveur S1 se trouvent sur différents réseaux privés.

Remarque : AWS ne prend pas en charge le mode L2. Par conséquent, il est nécessaire d'avoir uniquement le mode L3 activé sur les deux points de terminaison.

Pour une communication correcte entre CL1 et S1, le mode L3 est activé sur NS_VPX_CB-DC et NS_VPX-AWS, et les routes sont configurées comme suit :

- R1 a une route pour atteindre S1 via NS_VPX_CB-DC.
- NS_VPX_CB-DC a une route pour atteindre NS_VPX-AWS via R1.
- S1 doit avoir un itinéraire atteignant CL1 via NS_VPX-AWS.
- NS_VPX-AWS a une route pour atteindre NS_VPX_CB-DC via un routeur en amont.

Voici les routes configurées sur différents périphériques réseau dans le centre de données pour que le tunnel Cloud Connector fonctionne correctement :

Itinéraires	Réseau	Passerelle
Itinéraires sur le routeur R1		
Itinéraire pour atteindre le serveur S1	10.20.6.X/24	Adresse SNIP du point de terminaison du tunnel de NS_VPX_CB-DC = 10.10.5.30

Itinéraires	Réseau	Passerelle
Itinéraire pour atteindre le point d'extrémité distant du tunnel Cloud Connector	Adresse EIP mappée à l'adresse SNIP du Cloud Connector de NS_VPX-AWS = 203.0.1.50	Adresse IP privée du périphérique NAT = 10.10.7.70
Itinéraires sur NS_VPX_CB-DC		
Itinéraire pour atteindre NS_VPX-AWS	Adresse EIP mappée à l'adresse SNIP du Cloud Connector de NS_VPX-AWS = 203.0.1.50	Adresse IP de R1 = 10.10.5.1

Voici les itinéraires configurés sur divers périphériques réseau sur le cloud AWS pour que le tunnel Cloud Connector fonctionne correctement :

Itinéraires	Réseau	Passerelle
Routes sur le serveur S1		
Itinéraire pour atteindre le CL1 client	10.10.6.X/24	Adresse SNIP du point de terminaison du tunnel de NS_VPX-AWS = 10.10.6.1
Itinéraires sur l'appliance virtuelle Citrix NS_VPX-AWS		
Itinéraire pour atteindre NS_VPX_CB-DC	Adresse IP publique de Nat_dev-1 dans le datacenter = 66.165.176.15*	Adresse IP du routeur en amont sur AWS

Voici le flux de trafic d'un paquet de requête du client CL1 dans le tunnel Cloud Connector :

1. Client CL1 envoie une requête au serveur S1.
2. La demande atteint l'appliance virtuelle Citrix NS_VPX_CB-DC exécutée sur l'appliance Citrix SD-WAN WANOP CB_DC-1.
3. NS_VPX_CB-DC transfère le paquet à l'une des instances Citrix SD-WAN WANOP exécutées sur l'appliance Citrix SD-WAN WANOP CB_DC-1 pour l'optimisation WAN. Après le traitement du paquet, l'instance Citrix SD-WAN WANOP renvoie le paquet à NS_VPX_CB-DC.
4. Le paquet de requête correspond à la condition spécifiée dans l'entité PBR CBC_DC_AWS_PBR (configurée dans NS_VPX_CB-DC), car l'adresse IP source et l'adresse IP de destination du paquet de requête appartiennent respectivement à la plage IP source et à la plage IP de destination définies dans CBC_DC_AWS_PBR.

5. Étant donné que le tunnel de connecteur de cloud CBC_DC_AWS est lié à CBC_DC_AWS_PBR, l'appliance prépare le paquet à envoyer à travers le tunnel CBC_DC_AWS.
6. NS_VPX_CB-DC utilise le protocole GRE pour encapsuler chacun des paquets de requête en ajoutant un en-tête GRE et un en-tête IP GRE au paquet. L'en-tête IP GRE a l'adresse IP de destination définie sur l'adresse IP du point d'extrémité du tunnel de connecteur cloud (CBC_DC-AWS) côté AWS.
7. Pour le tunnel Cloud Connector CBC_DC-AWS, NS_VPX_CB-DC vérifie les paramètres d'association de sécurité IPSec (SA) stockés pour le traitement des paquets sortants, comme convenu entre NS_VPX_CB-DC et NS_VPX-AWS. Le protocole ESP (Encapsulating Security Payload) IPsec dans NS_VPX_CB-DC utilise ces paramètres SA pour les paquets sortants, pour chiffrer la charge utile du paquet encapsulé GRE.
8. Le protocole ESP assure l'intégrité et la confidentialité du paquet en utilisant la fonction de hachage HMAC et l'algorithme de chiffrement spécifié pour le tunnel Cloud Connector CBC_DC-AWS. Le protocole ESP, après avoir chiffré la charge utile GRE et calculé le HMAC, génère un en-tête ESP et un code de fin ESP et les insère avant et à la fin de la charge utile GRE cryptée, respectivement.
9. NS_VPX_CB-DC envoie le paquet résultant à NS_VPX-AWS.
10. NS_VPX-AWS vérifie les paramètres d'association de sécurité IPSec (SA) stockés pour le traitement des paquets entrants, comme convenu entre CB_DC-1 et NS_VPX-AWS pour le tunnel Cloud Connector CBC_DC-AWS. Le protocole IPsec ESP sur NS_VPX-AWS utilise ces paramètres SA pour les paquets entrants, et l'en-tête ESP du paquet de requête, pour déchiffrer le paquet.
11. NS_VPX-AWS décapsule ensuite le paquet en supprimant l'en-tête GRE.
12. NS_VPX-AWS transfère le paquet obtenu à CB_VPX-AWS, qui applique le traitement lié à l'optimisation WAN au paquet. CB_VPX-AWS renvoie ensuite le paquet obtenu à NS_VPX-AWS.
13. Le paquet résultant est le même que celui reçu par CB_DC-1 à l'étape 2. Ce paquet a l'adresse IP de destination définie sur l'adresse IP du serveur S1. NS_VPX-AWS transmet ce paquet au serveur S1.
14. S1 traite le paquet de requête et envoie un paquet de réponse. L'adresse IP de destination dans le paquet de réponse est l'adresse IP du client CL1 et l'adresse IP source est l'adresse IP du serveur S1.

Accélération d'Office 365

April 23, 2021

Citrix SD-WAN WANOP optimise le WAN pour offrir une expérience utilisateur cohérente pour les applications métier dans les succursales et les sites distants.

Microsoft Office 365 est une application SaaS (Software-as-a-Service) qui fournit la suite Microsoft Office d'applications de productivité de niveau entreprise. Cette application est hébergée sur le cloud et est livrée à la demande aux utilisateurs.

La fonctionnalité d'accélération Office 365 permet aux succursales d'obtenir les avantages d'optimisation que fournit Citrix SD-WAN WANOP pour l'application Microsoft Office 365.

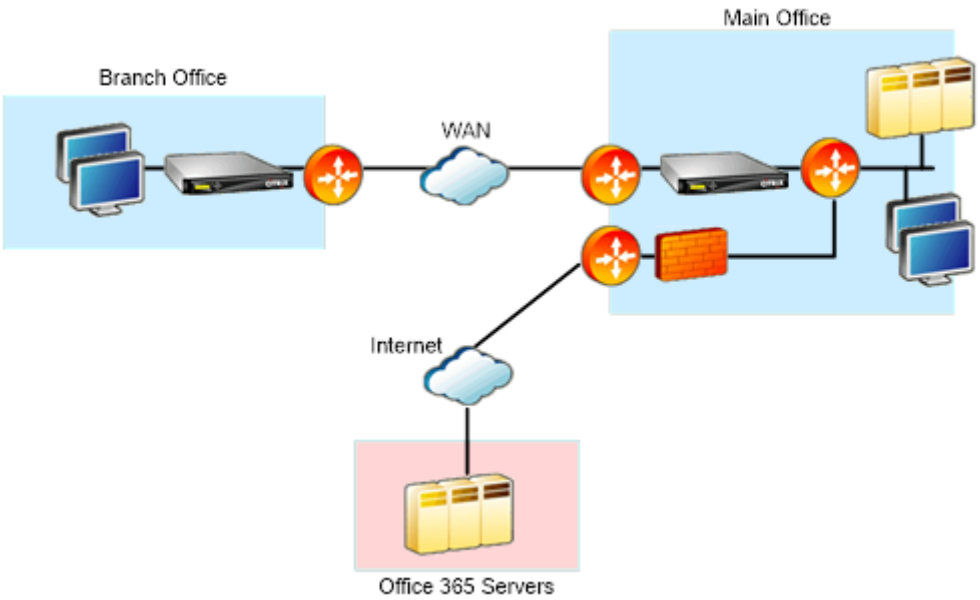
Cas d'utilisation

Lorsque le segment WAN est considérablement plus lent que le segment Internet, et les serveurs Office 365 de Microsoft sont plus proches du bureau plus grand que la succursale.

Topologie

Le trafic Office 365 de la succursale est envoyé via le réseau étendu vers le bureau principal, puis transféré vers les serveurs Office 365 via Internet. Le segment entre la succursale et le bureau principal est accéléré.

> **Remarque**
>
> Le segment entre le bureau principal et les serveurs Microsoft Office 365 n'est pas accéléré. Il est conseillé que le bureau principal se connecte au serveur Office 365 le plus proche.



Comment ça marche ?

L'accélération Citrix SD-WAN WANOP SSL peut déchiffrer et accélérer le trafic Office 365, fournissant une compression. En bref, l'accélération des succursales Office 365 peut être considérée comme un cas particulier d'accélération RPC sur HTTPS.

Procédure

1. Créez un appairage sécurisé entre les appliances Citrix SD-WAN WANOP de la succursale et du bureau principal.
2. Générer des certificats proxy/clé privée dans l'autorité de certification de domaine (CA).
3. Ajoutez toutes les CA requises dans Citrix SD-WAN WANOP.
    a) Autorité de certification, autorité de certification intermédiaire, autorité de certification racine des certificats Microsoft.
    b) Certificats de mandat/clés privées générés pour les URL Office 365.

    > **Remarque**
    >
    > Pour éviter les alertes de sécurité sur vos navigateurs, les certificats proxy doivent être signés par le serveur CA de votre domaine Windows, ce qui le rend acceptable pour tout utilisateur de domaine.

4. Créez un profil de proxy partagé SSL et liez le proxy divisé à la classe de service (web (internet-sécurisé)).
5. Lancez la connexion Office 365 et vérifiez les connexions accélérées.

    > **Avertissement**
    >
    > Les périphériques de succursale qui ne font pas partie du domaine afficheront des avertissements de sécurité, sauf si vous installez les certificats manuellement. Les utilisateurs de Firefox doivent également installer les certificats manuellement, car Firefox n'honore pas le magasin de certificats de l'appareil.

Configurer l'accélération d'Office 365

Pour configurer l'accélération Office 365 :

1. Configurer une relation d'appairage sécurisée entre les deux appliances WANOP Citrix SD-WAN, comme décrit dans *Secure Peering*
2. Créez un nouveau certificat.

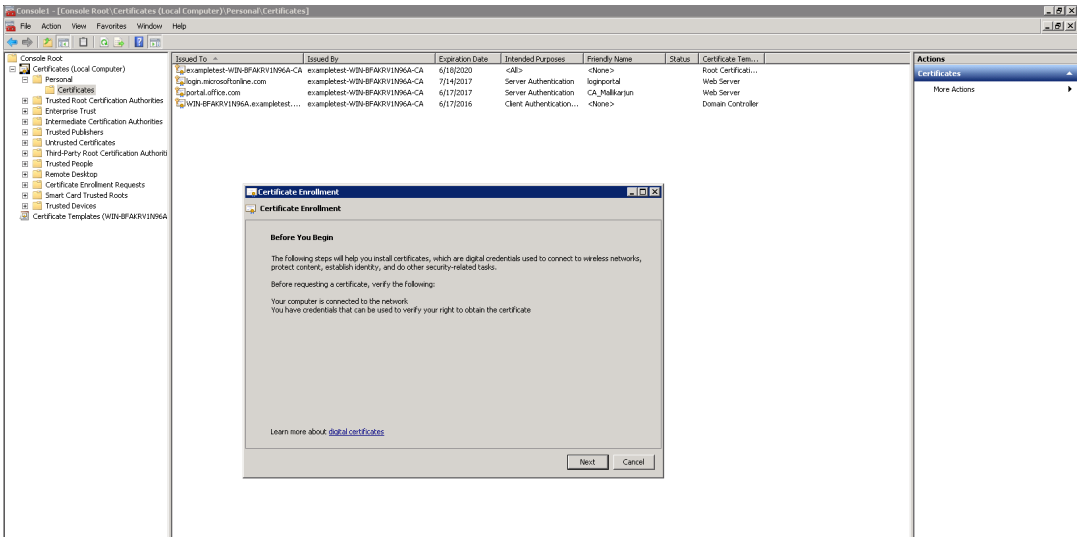
> **Remarque**
>
> L'appliance Citrix SD-WAN WANOP côté serveur sert d'intermédiaire entre Office 365 et les clients, de sorte que ces certificats seront signés par le contrôleur de domaine côté serveur, mais il fait référence aux domaines Office 356.

a) Ouvrez une session sur le **serveur d'autorité de certification** pour votre domaine Windows.

b) Si nécessaire, ajoutez les composants logiciels enfichables pour **l'autorité de certification**, le **modèle de certificat**et les **certificats**.

c) Accédez à **Modèles de certificats** > **Propriétés du serveur Web** > **Sécurité** et sélectionnez toutes les options.

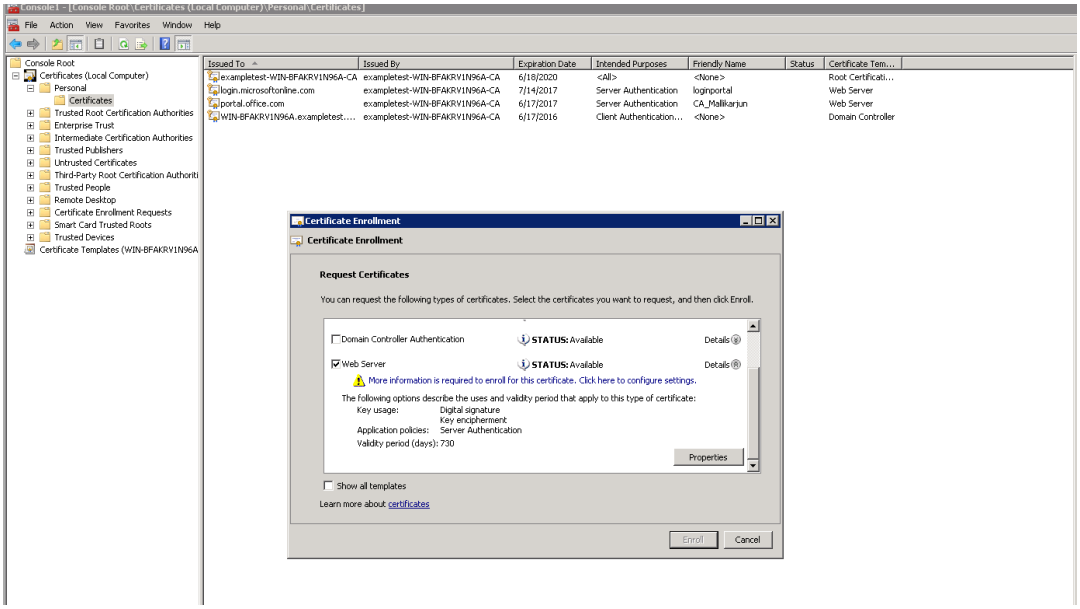
d) Accédez à **Certificats** > **Personnel** > **Certificats (Ordinateur)** > **Toutes les tâches** > **Demander un nouveau certificat**.



e) Dans la **fenêtre Inscription du certificat**, cliquez sur **Suivant**.

f) Dans la fenêtre **Sélectionner une stratégie d'inscription de certificat**, sélectionnez **Stratégie d'inscription Active Directory**.

g) Dans la fenêtre **Stratégie d'inscription Active Directory**, sélectionnez **Serveur Web** > **Détails** > **Propriétés**.



3. Copiez les informations des certificats Office365 dans vos nouveaux certificats. Vous vous retrouverez avec un seul certificat à partir de trois certificats Office365. Procédez comme suit :

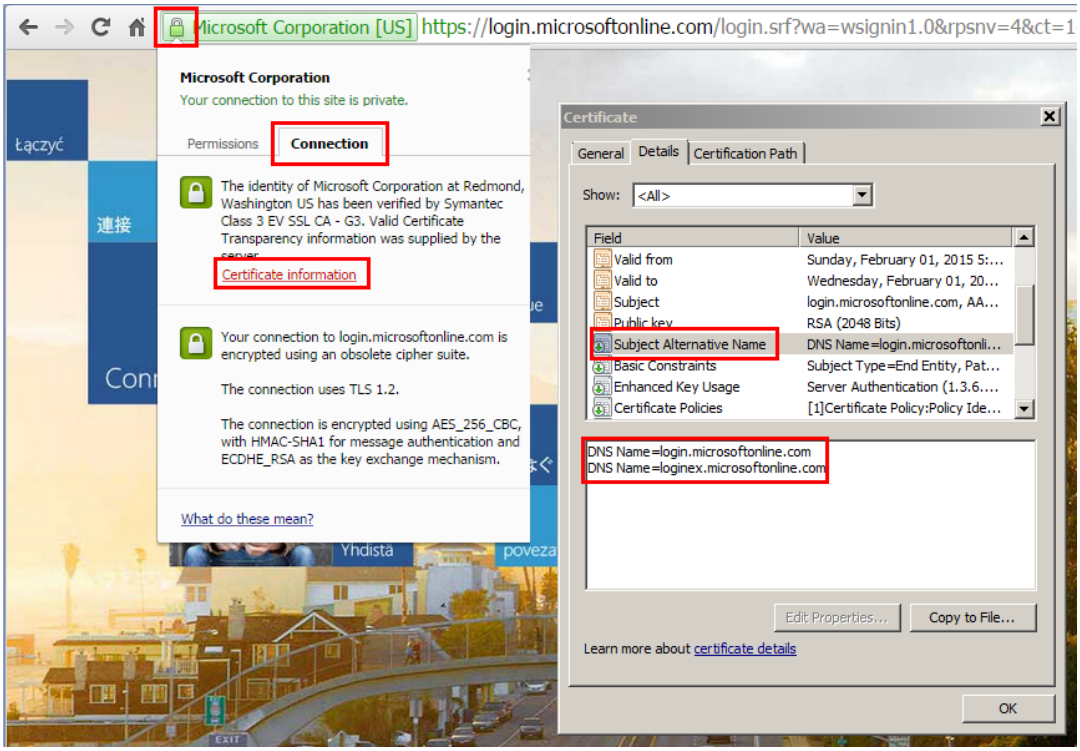
   a) Dans un navigateur, tel que Chrome, entrez l'url -https://login.microsoftonline.com.

   > **Remarque**
   >
   > Ne vous connectez pas.

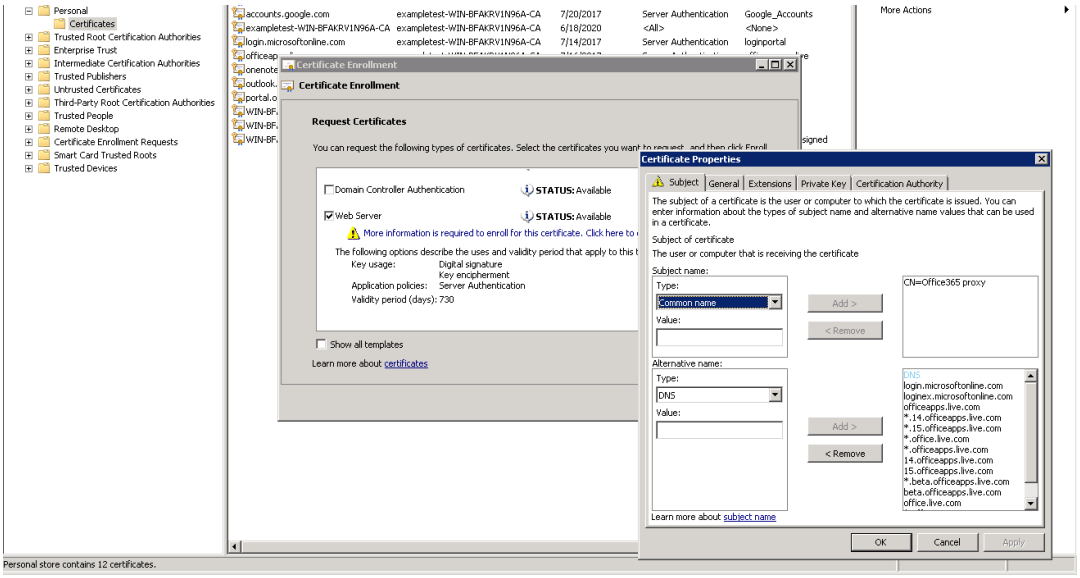
   b) Cliquez sur l'icône cadenas dans la barre d'URL et sélectionnez **Connexion** > **Informations sur le certificat** > **Détails**.

   > **Remarque**
   >
   > Ces instructions sont pour le navigateur Chrome ; la procédure est la même pour les autres navigateurs également.

   c) Cliquez sur **Subject Alternative Name**pour afficher une liste de noms DNS tels que « login.microsoftonline.com ». Copiez les informations dans la zone de texte située en dessous.



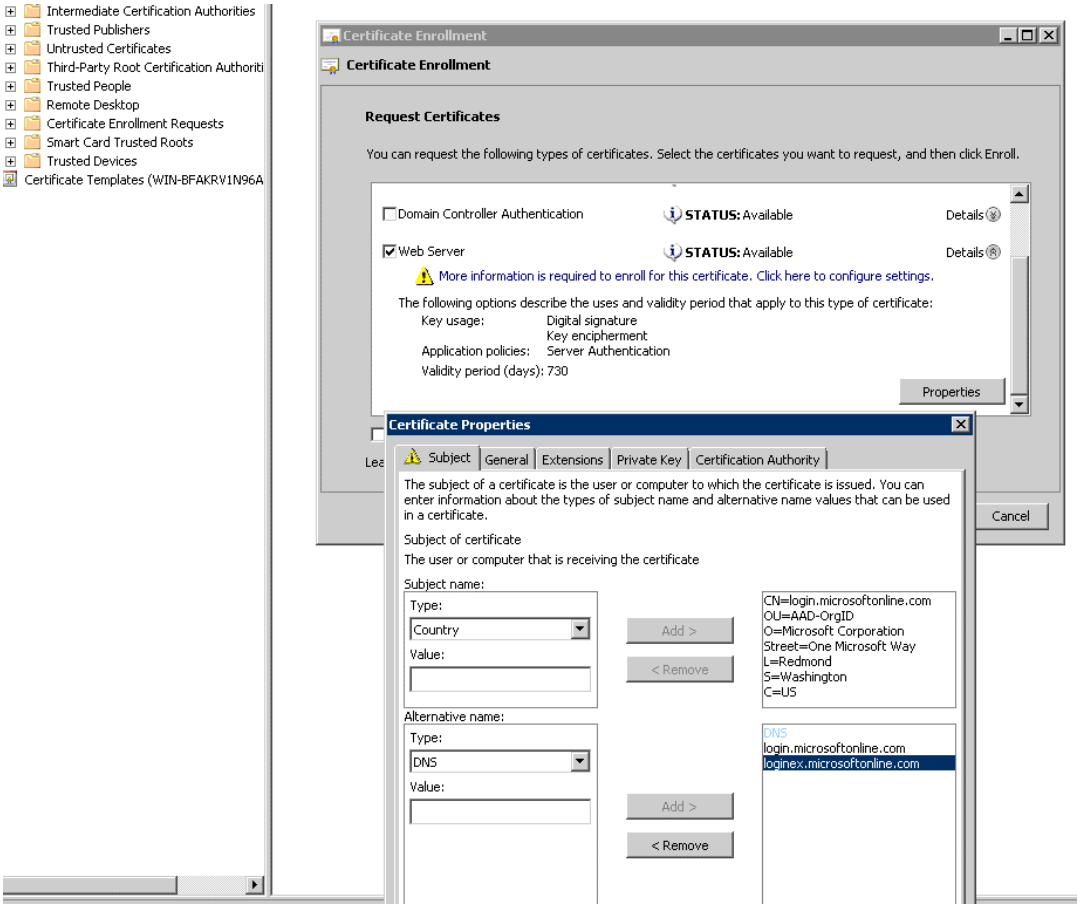
d) Revenez à la fenêtre **Propriétés des certificats** de votre nouveau certificat. Ajoutez les noms alternatifs dans le champ **Valeur** avec **Type** en tant que **DNS** pour correspondre à chaque autre nom dans le certificat Microsoft.



e) Répétez le processus de découverte des noms alternatifs de sujet et de les ajouter à votre certificat pour,https://outlook.office365.com,https://portal.office.com https://office.live.com et https://sharepoint.com (L'URL de SharePoint est spécifique au client).

f) Créez un nom commun pour votre nouveau certificat. L'exemple ci-dessus montre un nom

commun comme « proxy Office365 ».

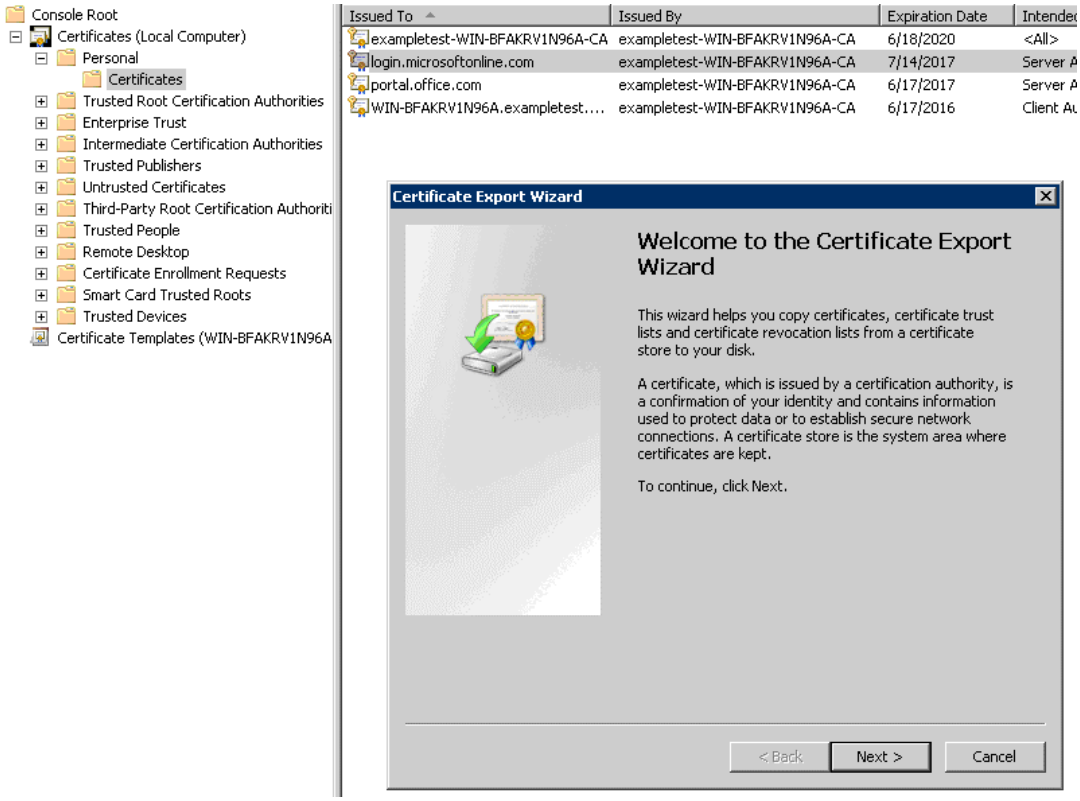


g) Dans l'onglet **Clé privée**, sélectionnez **Rendre la clé privée exportable**.

h) Cliquez sur **OK, Inscription** et **Terminer**.

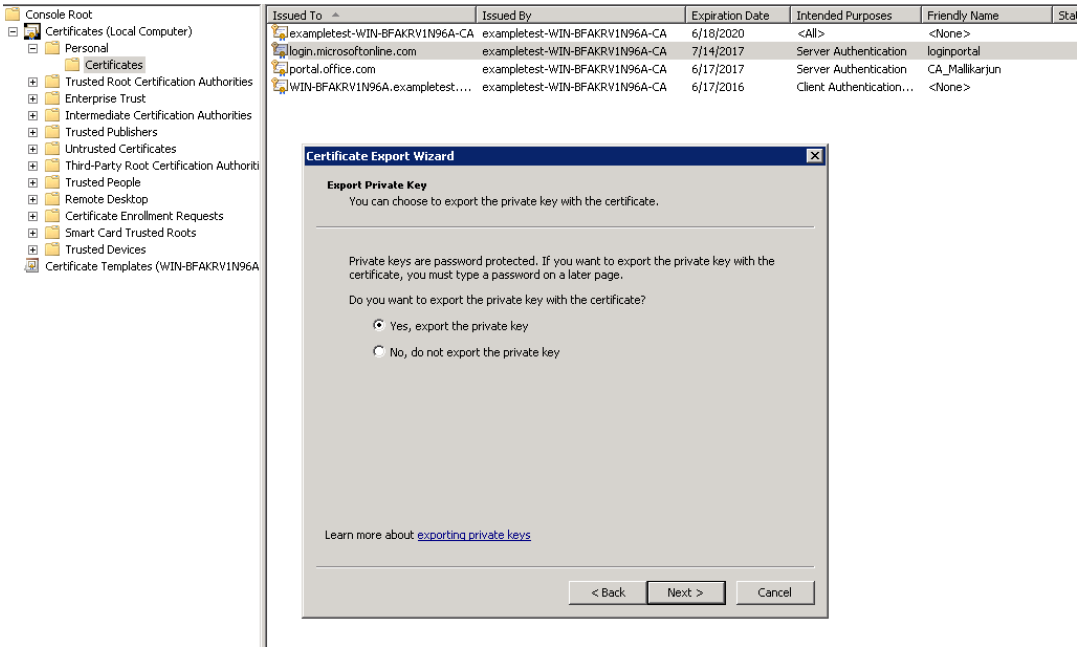
4. Exportez le certificat.

a) Sous **Certificats** > **Personnel** > **Certificats**, sélectionnez le certificat proxy créé ci-dessus, puis sélectionnez **Toutes les tâches** > **Exporter**.



b) L'**Assistant Exportation de certificat** s'affiche. Cliquez sur **Next**.

c) Dans **Exporter une clé privée**, sélectionnez l'option **Oui, exportez la clé privée**et cliquez sur **Suivant**.

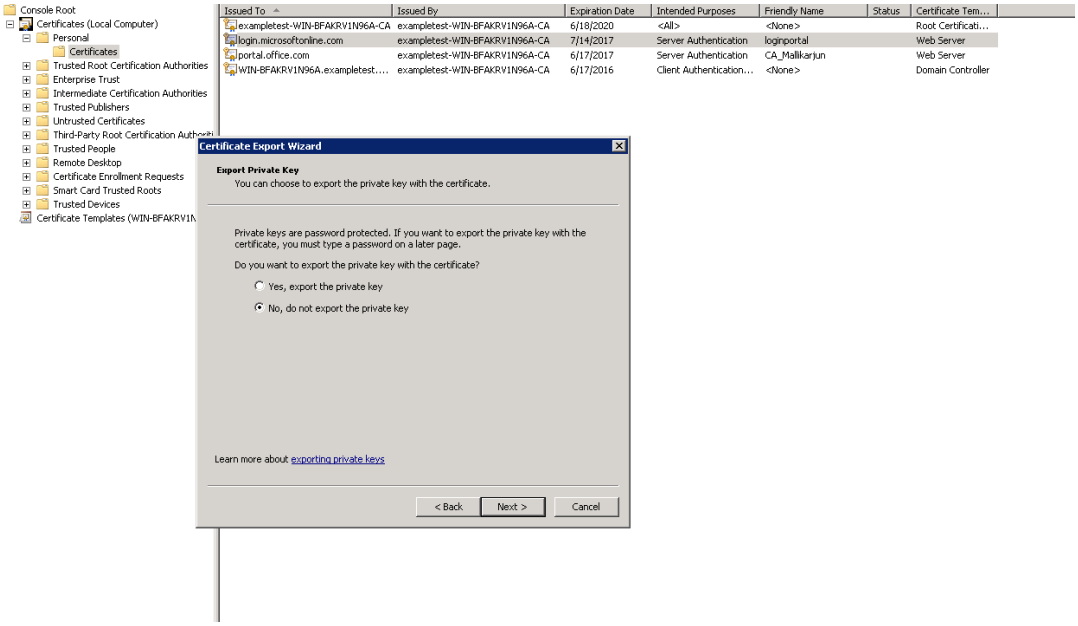


d) Conservez les valeurs par défaut du format de fichier d'exportation.

e) Saisissez et confirmez le mot de passe, exportez la clé privée et enregistrez le certificat en tant que *loginportal.pfx*.

5. Exportez vos certificats.

a) Dans l'**Assistant Exportation de certificat**, cliquez sur **Suivant**. Dans **Exporter la clé privée**, sélectionnez l'option **Non, n'exportez pas la clé privée**. Cliquez sur **Next**.



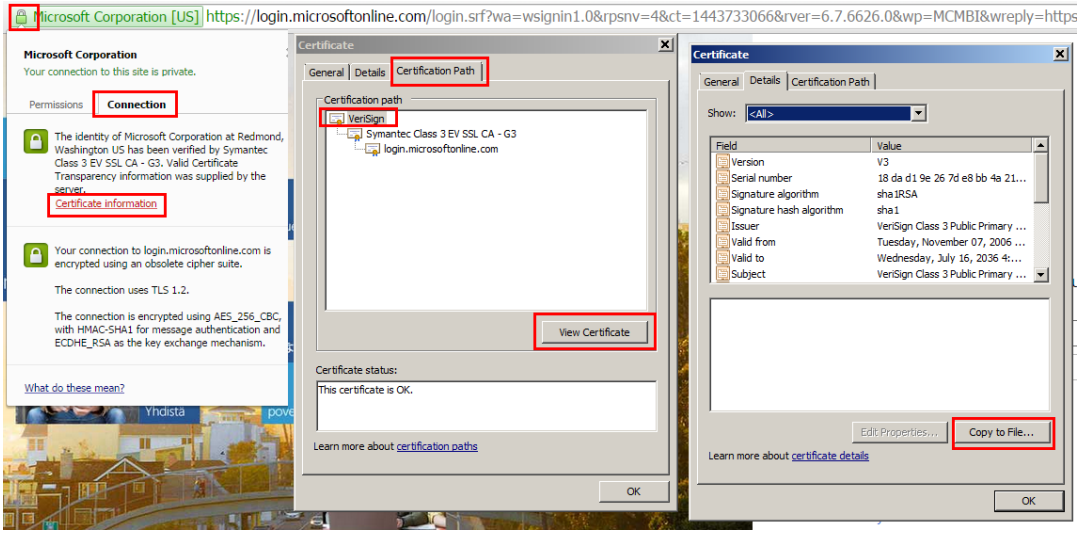
b) Conservez les valeurs par défaut du format de fichier d'exportation.

c) Tapez et confirmez le mot de passe, puis exportez la clé privée et le certificat, en enregistrant le fichier dans un fichier sous un nom de fichier tel que office365_keys.pfx.

6. Téléchargez les clés publiques de l'autorité de certification racine et des autorités de certification intermédiaires des certificats Microsoft.

a) À partir du navigateur, naviguez jusqu'àhttps://login.microsoftonline.com. Cliquez sur l'icône cadenas dans le navigateur. Accédez à **Connexion** > **Informations de certificat** > **Chemin de certification**.

b) Sélectionnez le certificat racine (celui situé en haut de la liste), puis cliquez sur **Afficher le certificat** > **Détails** > **Copier dans un fichier**. L'**Assistant Exportation de certificat** s'affiche. Cliquez sur **Next**.



c) Entrez le nom du fichier et enregistrez le fichier.

> **Remarque**
>
> Vous pouvez également utiliser Wireshark ou OpenSSL pour obtenir les noms d'autorité de certification racine et intermédiaire et obtenir les certificats à partir de la source « AUTHENTIC » (par exemple, le magasin SSL Windows).

d) Répétez l'étape 6 pour enregistrer les CA racine et intermédiaire des domaines suivants :

i. login.microsoftonline.com

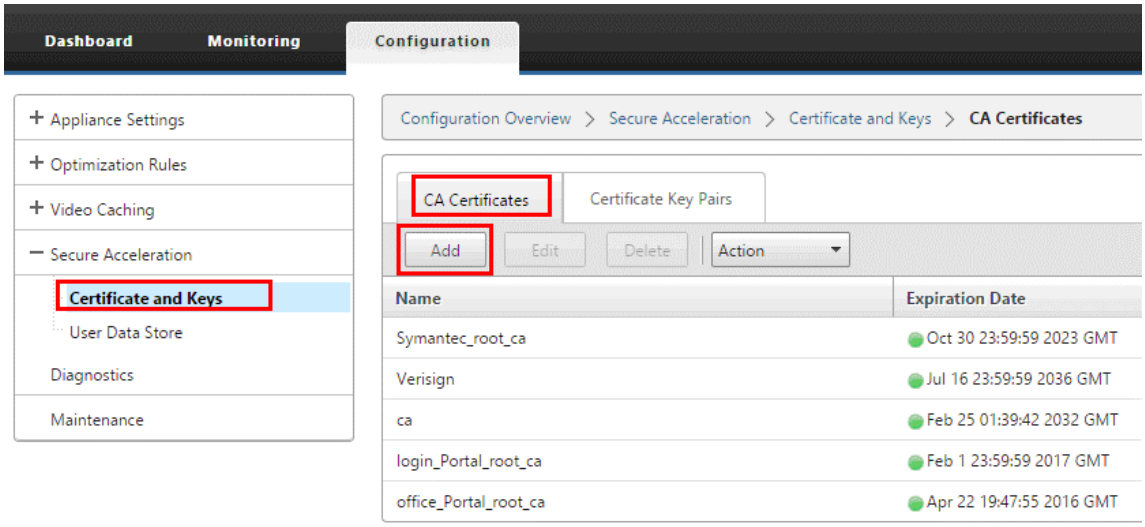
ii. portal.office.com

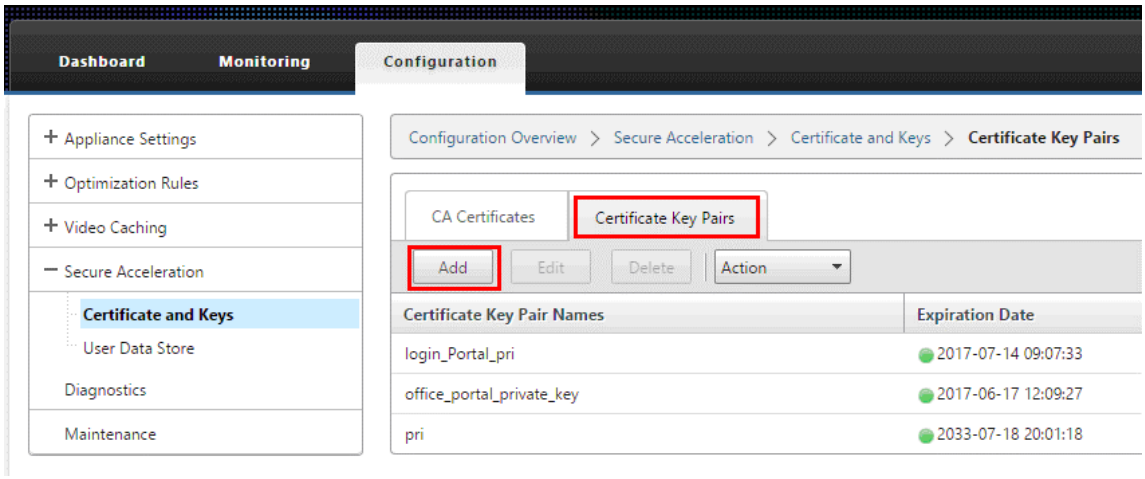
iii. outlook.office356.com

iv. *.sharepoint.com

v. office.live.com

7. Ajoutez toutes les CA de serveur Office 365, les paires de certificat/clé proxy et les clés privées à l'appliance Citrix SD-WAN WANOP côté serveur. Les autorités de certification sont ajoutées à l'aide de l'onglet **Certificats de l'autorité** de **certification de la page Certificats et clés**. Les certificats et les paires certificat/clé sont ajoutés dans l'onglet **Paires certificat/clé**.





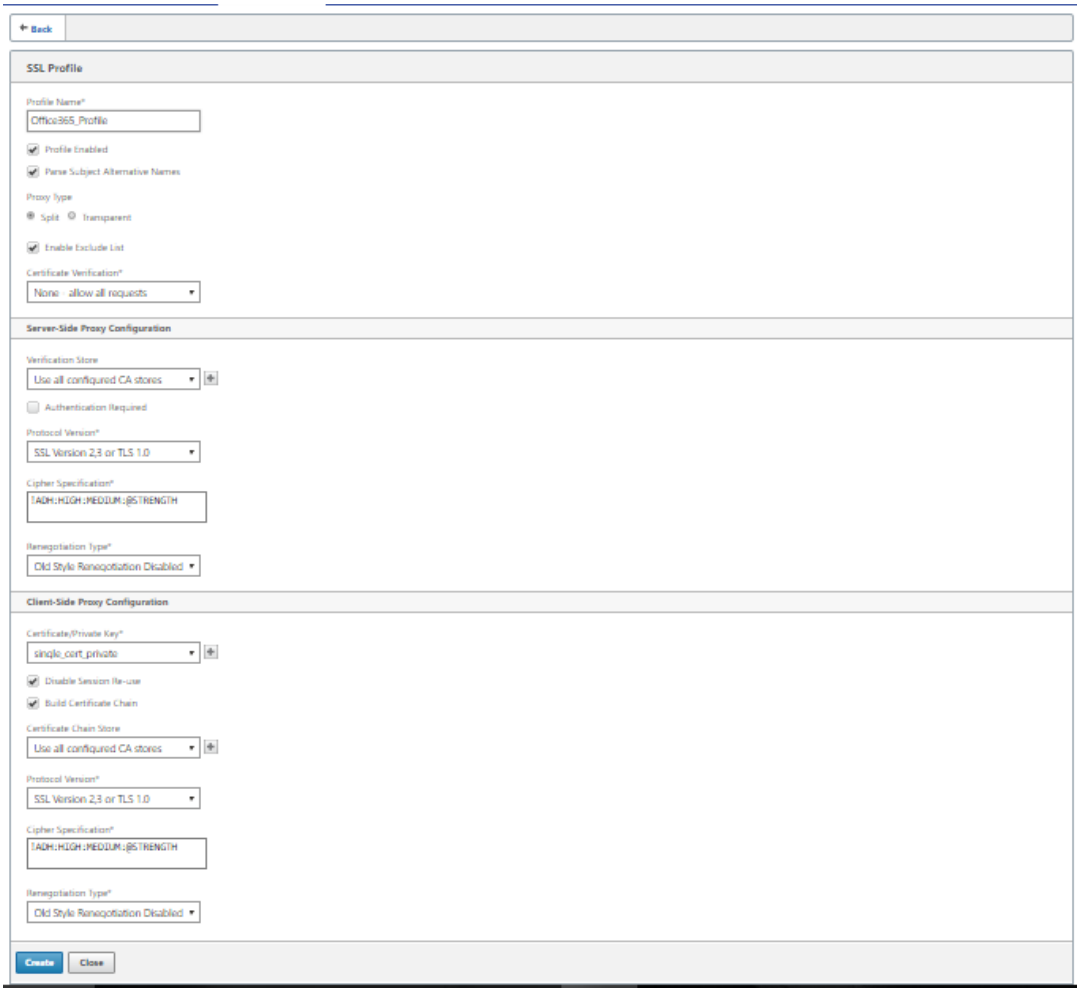
8. Créez un profil SSL split-proxy et liez le proxy split à la classe de service Web (Internet-Secure).

   a) Accédez à **Configuration** > **Accélération sécurisée** > **Profil SSL** > **Ajouter un profil**.

   b) Entrez le nom de profil de votre choix. Sélectionnez **Profile activé**, **Parse Subject Alternative Names**et **Split Proxy**.

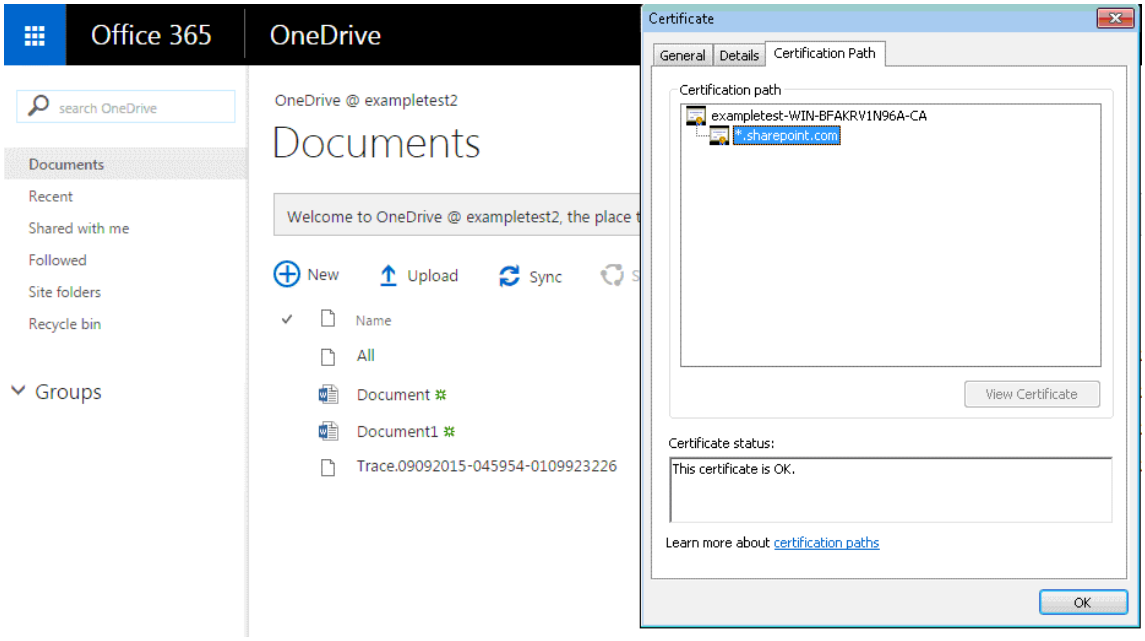
   c) Sous **Configuration du proxy côté serveur** > **Magasin de vérification**, sélectionnez **Utiliser tous les magasins d'autorité de certification configurés** .

   d) Sous **Configuration du proxy côté client** > **Certificate/clé privée**, sélectionnez la paire cert/clé privée que vous avez créée et exportée précédemment (celle illustrée dans l'exemple comme loginportal.pfx). Sélectionnez **Créer une chaîne de certificats**. Sélectionnez l'autorité de certification associée à la paire certificat/clé sous **Magasin de chaînes de certificats**.

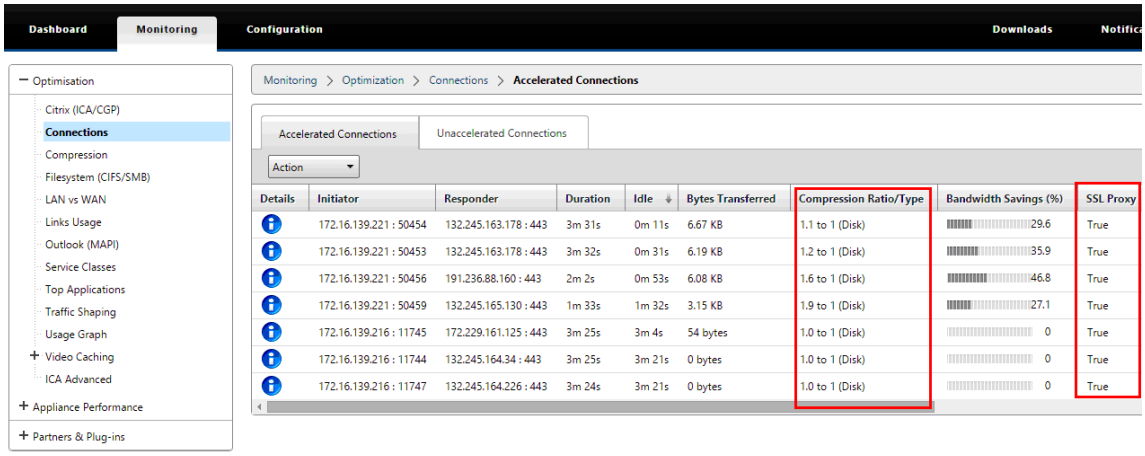


9. Liez le profil SSL créé à la classe de service Internet (Web-Secure). Accédez à **Configurer** > **Règles d'optimisation** > **Classes de service** et ajoutez le profil SSL à la liste des profils SSL.
10. Activez l'accélération et la compression sur disque pour la classe de service **Internet (Web-Secure)**.
11. Lancez une session Office 365 à partir de votre navigateur.

    La connexion est accélérée. Dans le navigateur, le certificat doit afficher votre autorité de certification racine, et non le certificat Office 365 réel, comme certificat d'autorité de certification de l'appliance côté serveur.



12. Sur la page Surveillance > Connexions de l'appliance, vérifiez que les connexions Office 365 sont compressées et reçoivent une accélération SSL.****

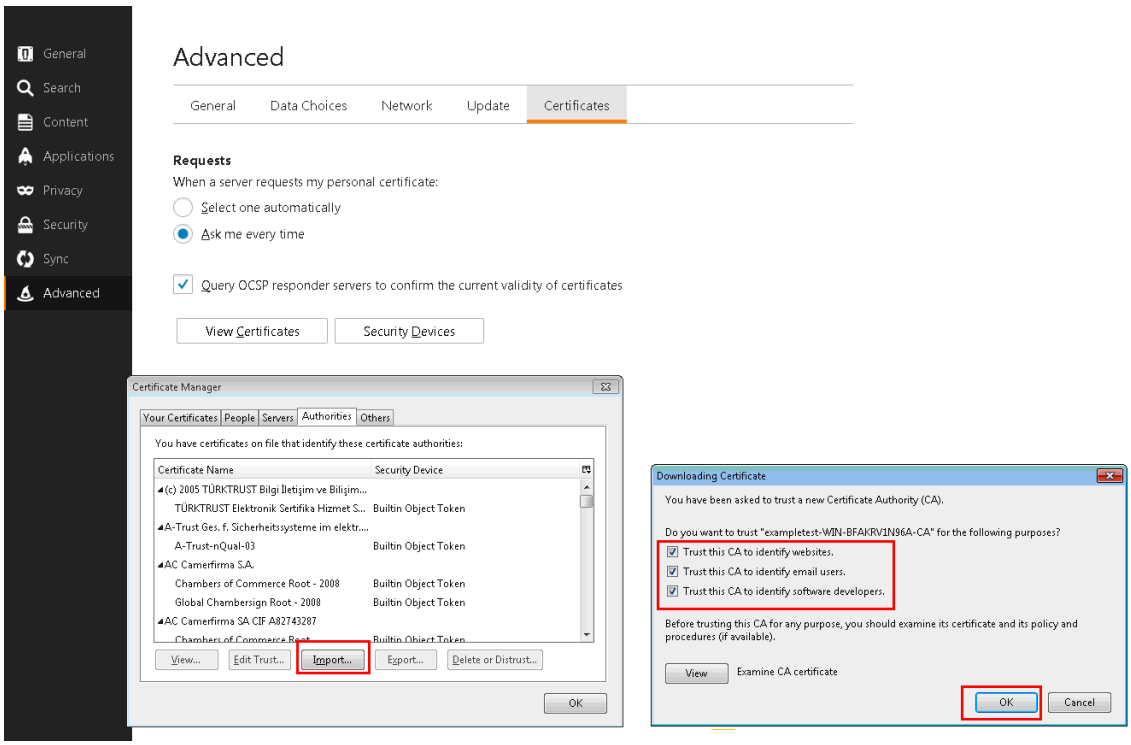


> **Remarque**
>
> Firefox n'accepte pas les certificats de l'appareil par défaut, mais possède son propre magasin de certificats. Par conséquent, les informations d'identification acceptées dans le comportement normal du domaine Windows par d'autres navigateurs, et par l'appareil dans son ensemble, doivent être installées manuellement dans Firefox. Pour installer des certificats dans Firefox, suivez la procédure décrite dans la section Installation des certificats dans Firefox.

Installer les certificats sur Firefox

Pour installer le certificat proxy de l'appliance côté serveur dans le magasin de certificats Firefox :

1. Dans le navigateur Firefox naviguant vers **Options** > **Avancé** > **Certificat** > **Afficher les certificats** > **Autorités** > **Importer**.
2. Téléchargez le certificat proxy de l'autorité de certification locale, sélectionnez toutes les options dans l'Assistant **Téléchargement de certificat**, puis cliquez sur **OK**.



Prise en charge de SCPS

April 9, 2021

Citrix SD-WAN WANOP prend en charge la variante TCP SCPS (Space Communications Protocol Standard). SCPS est largement utilisé pour les communications par satellite.

Pour plus d'informations générales sur SCPS, reportez-vous à la section http://www.scps.org.

SCPS est une variante TCP utilisée dans les communications par satellite et des applications similaires. L'appliance peut accélérer les connexions SCPS si l'option **SCPS** est sélectionnée sur la page Configuration : Réglage.

La principale différence pratique entre SCPS et le comportement de l'appliance par défaut est que les « accusés de réception négatifs sélectifs » (SNACK) de type SCPS sont utilisés à la place des accusés de réception sélective standard (SACK). Ces deux méthodes d'amélioration des retransmissions de données sont mutuellement exclusives. Par conséquent, si SCPS est activé à une extrémité de la connexion et que l'une ne l'est pas, les performances de retransmission en souffrent. Cette condition provoque également une alerte « Discordance du mode SCPS ».

Si vous devez mélanger des appliances compatibles SCPS avec des appliances non compatibles SCPS, déployez-les de manière à éviter les incohérences. Vous pouvez utiliser des règles de classe de service basées sur IP ou organiser le déploiement de sorte que chaque chemin d'accès ait des appliances correspondantes.

Accélération sécurisée du trafic

April 9, 2021

L'accelration sécurisée du trafic est obtenue par l'appairage sécurisé. Plusieurs fonctions avancées exigent que les appliances Citrix SD-WAN WANOP aux deux extrémités de la liaison établissent une *relation homologue sécurisée* entre elles, en installant un tunnel de signalisation SSL (également appelé *connexion de signalisation*). Ces fonctions sont la compression SSL, la prise en charge CIFS signée et la prise en charge MAPI chiffrée.

Lorsque l'appairage sécurisé est activé, la compression est automatiquement désactivée pour toutes les appliances partenaires (et les ordinateurs exécutant le plug-in Citrix SD-WAN WANOP) qui n'ont pas établi de relation homologue sécurisée avec l'appliance locale.

Pour établir une relation homologue sécurisée, vous devez générer des clés et des certificats de sécurité et configurer un tunnel de signalisation sécurisé entre les appliances. Avant de configurer le tunnel, commandez une licence crypto auprès de Citrix.

Peering sécurisé

April 23, 2021

Lorsqu'une appliance a activé le peering sécurisé, les connexions avec un partenaire pour lequel elle n'a pas de relation homologue sécurisée ne sont ni chiffrées ni compressées, bien que l'accélération du contrôle de flux TCP soit toujours disponible. La compression est désactivée pour garantir que les données stockées dans l'historique de compression des partenaires sécurisés ne peuvent pas être partagées avec des partenaires non sécurisés.

Lorsque l'appliance à une extrémité d'une connexion détecte que l'autre appliance a activé l'appairage sécurisé, elle tente d'ouvrir un tunnel de signalisation SSL. Si les deux appliances s'authentifient avec succès sur ce tunnel, elles disposent d'une relation d'appairage sécurisée. Toutes les connexions accélérées entre les deux appliances sont chiffrées et la compression est activée.

> **Remarque**
>
> Une appliance dont l'appairage sécurisé est activé ne compresse pas les connexions à des partenaires non sécurisés. L'utilisation réussie de la même appliance avec un mélange de partenaires sécurisés et non sécurisés est difficile. Gardez ce point à l'esprit lors de la conception de votre réseau accéléré.

Un mot de passe de keystore est requis pour accéder aux paramètres de sécurité. Ce mot de passe de la banque de clés est différent du mot de passe de l'administrateur, pour permettre à l'administration de la sécurité d'être séparée des autres tâches. Si le mot de passe du keystore est réinitialisé, toutes les données cryptées et les clés privées existantes sont perdues.

Pour protéger les données, même en cas de vol de l'appliance, le mot de passe du magasin de clés doit être réentré chaque fois que l'appliance est redémarrée. Jusqu'à ce que cela soit fait, le peering sécurisé et la compression sont désactivés.

Générer des clés de sécurité et des certificats

Les produits Citrix SD-WAN WANOP sont expédiés sans les clés et certificats requis pour le tunnel de signalisation SSL. Vous devez les générer vous-même. Vous pouvez générer des clés et des certificats via votre processus normal de génération d'informations d'identification, ou avec le paquet « openssl » à partir dehttp://www.openssl.org.

À des fins de test, vous pouvez générer et utiliser un certificat X509 auto-signé basé sur une clé privée (que vous générez également). En production, utilisez des certificats qui font référence à une autorité de certification approuvée. L'exemple suivant appelle openssl depuis la ligne de commande d'un PC pour générer une clé privée (
my.key) et un certificat auto-signé (
my.crt) :

```
pre codeblock
# Generate a 2048-bit private key
openssl genrsa -out my.key 2048
# Now create a Certificate Signing Request
openssl req -new -key my.key -out my.csr
# Finally, create a self-signed certificate with a 365-day expiration
openssl x509 -req -days 365 -in my.csr -signkey my.key -out my.crt
<!--NeedCopy-->
```

Pour une utilisation en production, consultez les stratégies de sécurité de votre organisation.

Configurer l'appairage sécurisé

Il existe deux façons d'établir un peering sécurisé :

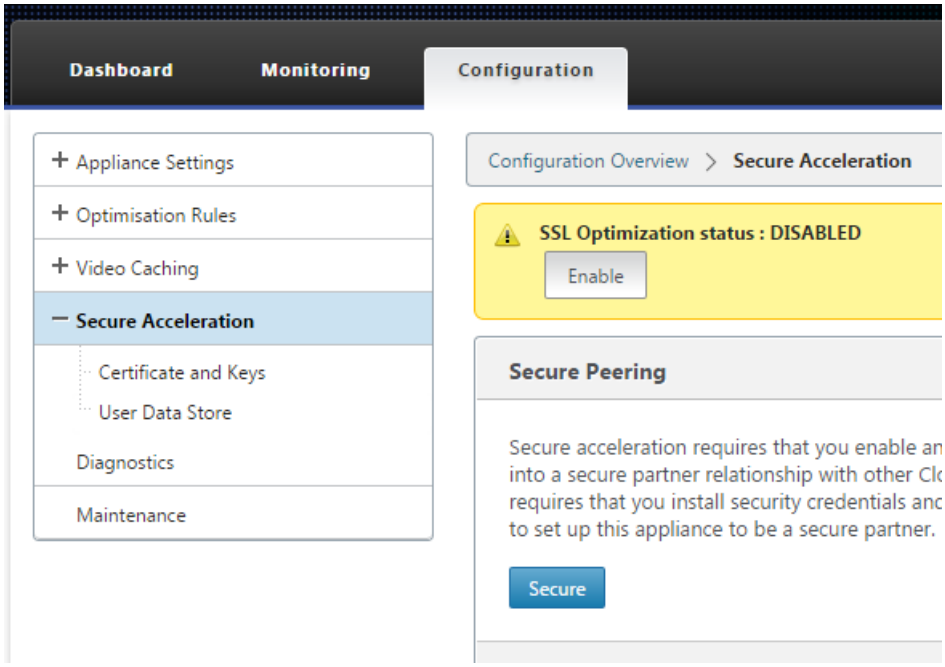
1. Utilisation des informations d'identification générées par les appliances.
2. En utilisant les informations d'identification que vous fournissez vous-même.

   Étant donné qu'une appliance dont l'appairage sécurisé est activé ne compresse que les connexions avec les appliances partenaires avec lesquelles elle a une relation d'appairage sécurisée, cette procédure doit être appliquée en même temps à toutes vos appliances.

Pour préparer les appareils pour un peering sécurisé :

Effectuez la procédure suivante sur chaque appliance de votre réseau.

1. Installez une licence de crypto sur l'appliance. Sans licence crypto, l'accélération sécurisée n'est pas disponible.
   a) Si vous ne l'avez pas déjà fait, achetez des licences crypto auprès de Citrix.
   b) Si vous utilisez un serveur de licences réseau, accédez à **Configuration** > **Paramètres de l'appliance** > **Licences.** Dans la section **Ajouter une licence**, cliquez sur **Modifier**, puis sélectionnez le serveur de licences distant et définissez Crypto License On.
   c) Si vous utilisez des licences locales, accédez à **Configuration** > **Paramètres de l'appliance** > **Licence.** Dans la page **Ajouter une licence**, cliquez sur l'option Serveur de licences local, puis cliquez sur **Ajouter** pour télécharger une licence de crypto locale.
   d) Vérifiez que l'installation de la licence est réussie sur la page **Configuration** > **Paramètres de l'appliance** > Licence. Sous Informations sur les licences, une licence crypto doit être affichée comme active et avec une date d'expiration dans le futur.
2. Accédez à la page **Configuration** > **Accélération sécurisée**. Si la page comporte un bouton nommé Sécurisé, cliquez dessus.



3. Si vous accédez automatiquement à l'écran Paramètres du magasin de clés, procédez comme suit :

   a) Entrez deux fois un mot de passe de keystore et cliquez sur Enregistrer.

   b) Lorsque l'écran est mis à jour pour afficher la section Certificats et clés d'appairage sécurisé, cliquez sur Activer l'appairage sécurisé et le certificat CA, puis cliquez sur Enregistrer.

   c) Passez à l'étape 6.

4. Si vous n'avez pas été dirigé automatiquement vers l'écran Paramètres du magasin de clés, cliquez sur l'icône du crayon sous **Secure Peering**, puis cliquez sur l'icône du crayon sous **Paramètres du magasin de clés.** Ouvrez dans le menu déroulant État de la banque de clés et entrez deux fois un mot de passe de la banque de clés. Cliquez sur **Enregistrer**.

5. Activez l'appairage sécurisé en accédant à la page **Configuration** > **Accélération sécurisée** et en cliquant sur le bouton **Activer**. Ignorer les avertissements à ce stade. Ce paramètre permet l'appairage sécurisé lorsque la configuration supplémentaire requise est terminée.

6. Activez le chiffrement de l'historique de compression en allant dans **Configuration** > **Stockage de données utilisateur d'accélération sécurisée** et en cliquant sur l'icône en forme de crayon. Cliquez sur **Activer le chiffrement du disque**, puis sur **Enregistrer**. Le chiffrement du stockage des données utilisateur empêche la lecture non autorisée de l'historique de compression sur disque, en cas de vol ou de retour à l'usine de l'appliance. La sécurité du chiffrement des données du disque repose sur le mot de passe du keystore. Cette fonctionnalité utilise le chiffrement AES-256. (Le chiffrement des données disque ne crypte pas l'ensemble du disque, juste l'historique de compression.)

7. Si vous utilisez des informations d'identification générées par l'appliance, passez à l'étape suivante. Si vous utilisez vos propres informations d'identification, procédez comme suit :

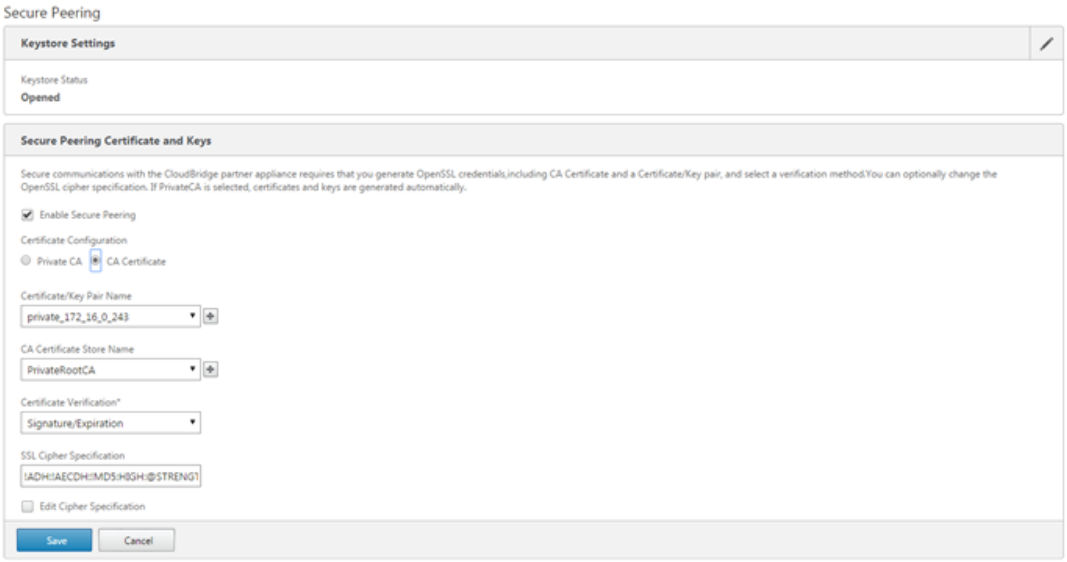
   a) Accédez à **Configuration** > **Accélération sécurisée**, puis cliquez sur l'icône représentant un crayon sous Secure Peering, puis cliquez sur l'icône représentant un crayon sous **Secure Peering Certificates and Keys**. Cliquez sur **Activer l'appairage sécurisé et la configuration des certificats > Certificat de** l'autorité de **certification**. Les champs de spécification des informations d'identification apparaissent.

   b) Sous **Nom de la paire de certificat/clé**, cliquez sur l'icône **+**et téléchargez ou collez la paire cert/clé de cette appliance. Si requis par les informations d'identification, entrez également le mot de passe de la clé ou le mot de passe du fichier. Cliquez sur **Créer**.

   c) Sous **Nom du magasin de certificats de l'autorité**de certification, cliquez sur l'icône **+**et téléchargez ou collez le certificat de l'autorité de certification pour cette appliance.

   d) Conservez les valeurs par défaut des champs Vérification de certificat et Spécification de chiffrement SSL, à moins que votre organisation n'en exige autrement.

   e) Cliquez sur **Enregistrer**.



8. Répétez l'opération pour le reste de vos appareils.
9. Si vous utilisez les informations d'identification que vous avez fournies vous-même, la configuration d'appairage sécurisé est terminée.
10. Si vous utilisez des informations d'identification générées par l'appliance, effectuez la procédure suivante.

Pour utiliser l'appairage sécurisé avec les informations d'identification générées par l'appliance :

1. Utilisez la procédure « Préparer les appareils pour sécuriser l'appairage » ci-dessus pour préparer vos appareils à cette procédure.
2. Sur une appliance de centre de données, accédez à **Configuration** > **Accélération sécurisée** et cliquez sur le bouton **Activer**, le cas échéant, pour activer l'appairage sécurisé.
3. Cliquez sur l'icône en forme de crayon sous Secure Peering. Le keystore devrait être ouvert. Si ce n'est pas le cas, ouvrez-le maintenant.
4. Cliquez sur l'icône en forme de crayon sous **Certificat et clés de peering sécurisé**. Cliquez sur les options **Activer le peering sécurisé et l'autorité de certification privée**, puis cliquez sur **Enregistrer**. Cela générera un certificat d'autorité de certification locale auto-signé et une paire de clés de certificat locale.
5. Cliquez sur **+** sous **Homologues connectés**. Entrez l'adresse IP, le nom d'utilisateur de l'administrateur et le mot de passe de l'administrateur pour l'une de vos appliances distantes, puis cliquez sur **Connexion**. Ceci émet un certificat d'autorité de certification et une paire de clés de certificat pour l'appliance distante et le copie sur l'appliance distante.

   > **Remarque**
   >
   > Pour les appliances WANOP SD-WAN, l'adresse IP peut être l'adresse IP de n'importe quelle interface où l'accès Web est activé. Pour les appliances SD-WAN PE, l'adresse IP est l'adresse IP de gestion.

6. Répétez cette procédure pour vos autres appliances distantes.
7. Sur l'appliance du centre de données, vérifiez la connectivité en accédant à **Surveillance** > **Partenaires et plug-ins** > **Partenaires sécurisés**. Pour chaque appliance distante, le contenu du champ Secure doit être True et l'état de la connexion doit être Connected Available.

CIFS, SMB2 et MAPI

April 9, 2021

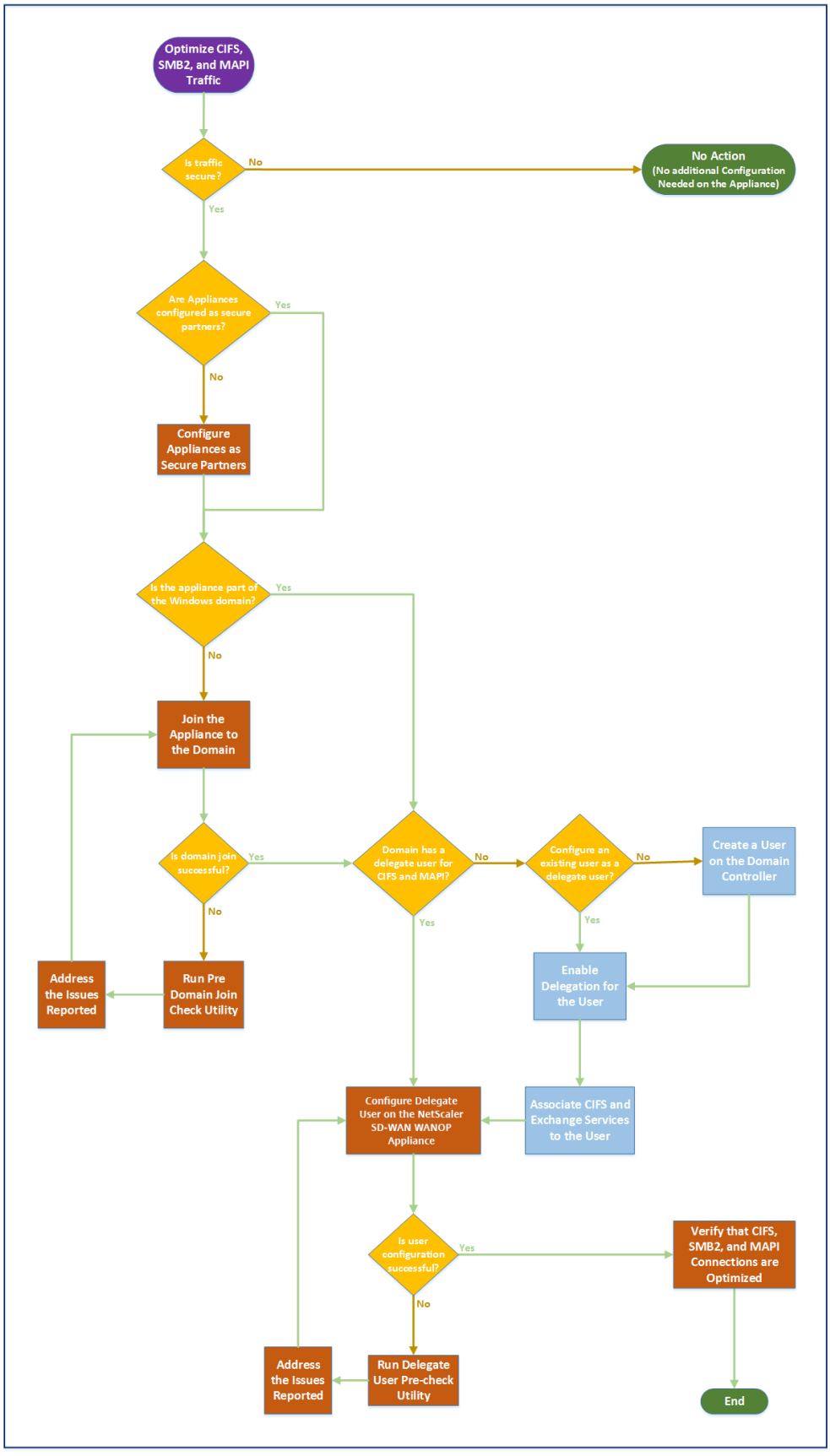
Windows est l'un des systèmes d'exploitation communs déployés sur le réseau. Le système d'exploitation Windows prend en charge les ressources distribuées partagées entre emplacements. Par exemple, vous pouvez rendre les ressources de votre centre de données accessibles à partir de diverses succursales. Pour l'accès via le réseau, Windows utilise le protocole CIFS (Common Internet File System) pour accéder aux fichiers partagés et les protocoles MAPI (Messaging Application Programming Interface) pour accéder au courrier électronique via Microsoft Outlook. Autrement dit, Windows utilise le protocole CIFS pour le transfert de fichiers CIFS (Windows et Samba) et la navigation dans les répertoires, et Microsoft Outlook utilise le protocole MAPI pour accéder aux données Outlook.

Vous pouvez utiliser une appliance Citrix SD-WAN WANOP pour optimiser les connexions CIFS, SMB2 (Server Message Block version 2) et MAPI sur le réseau.

En plus de prendre en charge le système d'exploitation Windows, les appliances Citrix SD-WAN WANOP prennent en charge CIFS et SMB2 sur les systèmes de stockage NetApp et Hitachi.

L'organigramme ci-dessous illustre la procédure complète de configuration d'une appliance Citrix SD-WAN WANOP pour optimiser le trafic CIFS, SMB2 et MAPI.

Configuration d'une appliance Citrix SD-WAN WANOP pour optimiser le trafic CIFS, SMB2 et MAPI



Configurer l'appliance Citrix SD-WAN WANOP pour optimiser la sécurité du trafic Windows

April 9, 2021

Vous devez ajouter l'appliance Citrix SD-WAN WANOP à l'infrastructure de sécurité Windows avant de pouvoir optimiser le système de fichiers Windows signé et le trafic MAPI Outlook/Exchange chiffré.

Grâce aux améliorations apportées au système de sécurité Windows dans les versions récentes de Windows, les clients et les serveurs sécurisent le trafic en authentifiant et en chiffrant les données. Cela nécessite que l'appliance Citrix SD-WAN WANOP soit un membre de confiance de l'infrastructure de sécurité Windows avant d'optimiser le système de fichiers Windows signé et le trafic MAPI Outlook/Exchange chiffré.

Après avoir ajouté l'appliance à l'infrastructure de sécurité Windows, elle dispose des fonctionnalités suivantes :

- Accélération du trafic des serveurs de fichiers pour les serveurs Microsoft Windows, NetApp et Hitachi HNAS à l'aide du protocole SMB signé et SMB2 signé.
- Accélération du trafic serveur Microsoft Exchange lorsqu'il est accessible par les clients Outlook à l'aide de MAPI chiffré ou RPC sur HTTPS.

Fonctionnement de l'appliance Citrix SD-WAN WANOP dans un système de sécurité Windows

La connexion de l'appliance à un domaine Windows nécessite des informations d'identification de l'administrateur. Lorsqu'elle rejoint le domaine Windows, l'appliance devient un membre approuvé du domaine. Cela permet à l'appliance d'être déclarée membre de l'infrastructure de sécurité du domaine.

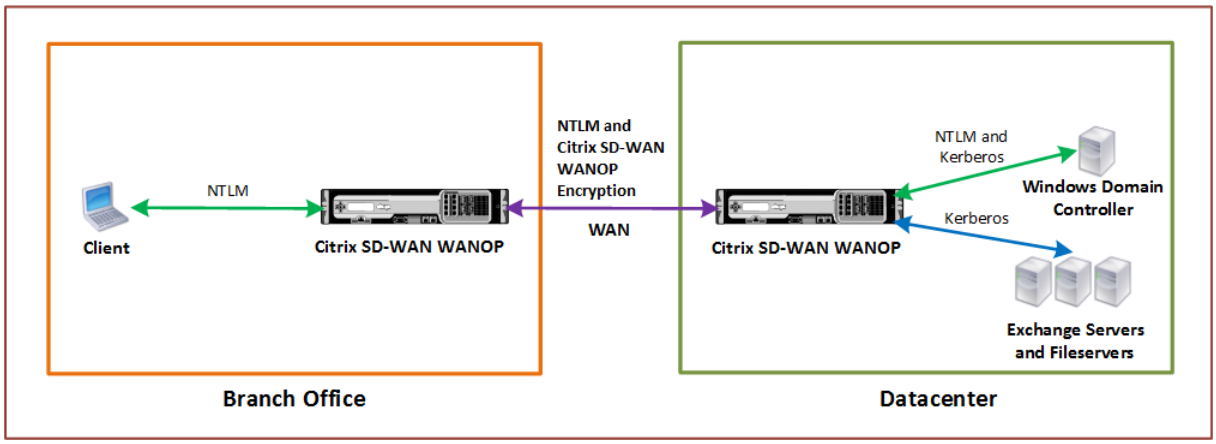
Une fois l'appliance intégrée à l'infrastructure de sécurité Windows, les utilisateurs doivent être authentifiés avant d'accéder aux ressources. Pour éviter la difficulté de configurer un grand nombre d'utilisateurs dans le domaine, vous pouvez déléguer la responsabilité d'authentification à un utilisateur délégué.

Vous créez un utilisateur délégué dans le répertoire actif. Cet utilisateur est similaire à un utilisateur normal, mais avec des privilèges spéciaux. Après avoir créé l'utilisateur délégué, vous devez configurer cet utilisateur sur l'appliance Citrix SD-WAN WANOP. L'appliance utilise l'utilisateur délégué pour s'authentifier au nom des utilisateurs lorsqu'ils accèdent à des flux de données authentifiés et chiffrés à l'aide de protocoles Windows, tels que CIFS et MAPI.

Pour accélérer le trafic CIFS et MAPI, le mécanisme de délégation Windows standard vous permet de limiter la délégation de sécurité aux services concernés. Cette délégation contrainte est disponible depuis la version de Windows Server 2003.

Après avoir fait partie du domaine, l'appliance accélère le trafic Windows sécurisé. Une appliance de centre de données qui rejoint un domaine Windows doit avoir une relation d'homologue sécurisée avec l'appliance distante ou le plug-in Citrix SD-WAN WANOP, mais seule l'appliance de centre de données rejoint le domaine Windows. Aux fins de l'accélération CIFS ou MAPI, l'appliance distante agit en tant qu'esclave de l'appliance du centre de données, étant contrôlée sur le tunnel SSL sécurisé entre les deux. Par conséquent, les informations d'identification de l'utilisateur délégué ne quittent pas le centre de données.

La figure suivante illustre un exemple de diagramme topologique pour cette configuration.



Dans la figure ci-dessus, un client de succursale accède aux ressources du centre de données. Le client de succursale, se trouvant dans un autre domaine, utilise l'authentification NTLM dans le cadre du système de sécurité Windows. Comme pour toutes les connexions accélérées entre deux appliances Citrix SD-WAN WANOP dans une relation homologue sécurisée, les connexions CIFS ou MAPI et les authentifications NTLM sur le WAN sont chiffrées. Selon la version du Controller de domaine Windows, la demande utilisateur du centre de données Citrix SD-WAN WANOP est authentifiée à l'aide du protocole d'authentification NTLM ou Kerberos. Une fois que le domaine authentifie l'utilisateur, les demandes d'accès ultérieures au serveur Exchange et aux serveurs de fichiers utilisent le protocole d'authentification Kerberos. L'appliance Citrix SD-WAN WANOP optimise ensuite les connexions établies entre le client et le serveur.

Si les appliances ne disposent pas d'une relation homologue sécurisée ou si l'appliance du centre de données n'a pas réussi à joindre le domaine, les connexions utilisent l'accélération du contrôle de flux TCP, qui n'effectue aucune opération de sécurité, compression ou transformation des données. Les connexions entre le client et le serveur sont établies comme si les appliances Citrix SD-WAN WANOP n'étaient pas là.

Vous pouvez configurer différents modes d'authentification client sur les systèmes d'exploitation Win-

dows. Les types de connexions optimisés par l'appliance Citrix SD-WAN WANOP dépendent du mode d'authentification client que vous configurez.

Le tableau suivant répertorie les modes d'authentification du client Windows sous Windows et les optimisations Citrix SD-WAN WANOP correspondantes.

Authentification et optimisation prises en charge pour le système d'exploitation Windows

Système d'exploitation client	Mode d'authentification du client	Optimisation	Commentaires
Windows XP/Windows Vista/Windows 7/Windows 8	Négocier l'authentification (SPNEGO)	Accélération de contrôle de débit TCP, Compression, accélération du protocole CIFS	Paramètre par défaut utilisé pour toutes les versions de Windows.
Windows XP/Windows Vista/Windows7/Windows 8	NTLM uniquement ou Kerberos uniquement	Accélération du contrôle de débit TCP uniquement	Modes d'authentification autres que par défaut

Remarque : Si vous utilisez les modes d'authentification client NTLM uniquement ou Kerberos uniquement, le trafic n'est pas accéléré s'il est chiffré.

Configuration requise pour ajouter un dispositif Citrix SD-WAN WANOP au système de sécurité Windows

Pour optimiser le trafic sécurisé pour le trafic SMB signé Windows et chiffré MAPI, votre déploiement Citrix SD-WAN WANOP doit répondre aux exigences suivantes avant d'ajouter l'appliance à l'infrastructure de sécurité Windows :

- Les appliances d'accélération côté client et côté serveur doivent avoir établi une relation homologue sécurisée.
- Les appliances doivent utiliser un serveur NTP étroitement synchronisé avec l'heure sur le serveur de domaine Windows. Idéalement, les appliances et le serveur de domaine Windows sont tous des clients du même serveur NTP.
- Outlook **ne doit pas** être configuré pour l'option **Kerberos uniquement** ou **NTLM uniquement**. L'option par défaut (négociée) est requise pour l'accélération.
- Le client et le serveur peuvent être membres de n'importe quel domaine bénéficiant d'une approbation bidirectionnelle avec le domaine de l'appliance côté serveur. L'approbation unidirectionnelle n'est pas prise en charge.

- Un utilisateur délégué Kerberos doit être configuré sur le Controller de domaine pour être utilisé par l'appliance participant à l'infrastructure de sécurité du domaine.
- Les adresses IP du serveur DNS pour le domaine doivent être configurées et accessibles sur l'appliance côté serveur.
- Les serveurs de domaine doivent être entièrement accessibles, avec des recherches avant et inversées pour toutes les adresses IP des contrôleurs de domaine configurés sur les serveurs DNS.
- Le nom d'hôte de l'appliance Citrix SD-WAN WANOP côté serveur doit être unique. L'utilisation du nom d'hôte par défaut de « hostname » est susceptible de causer des problèmes.

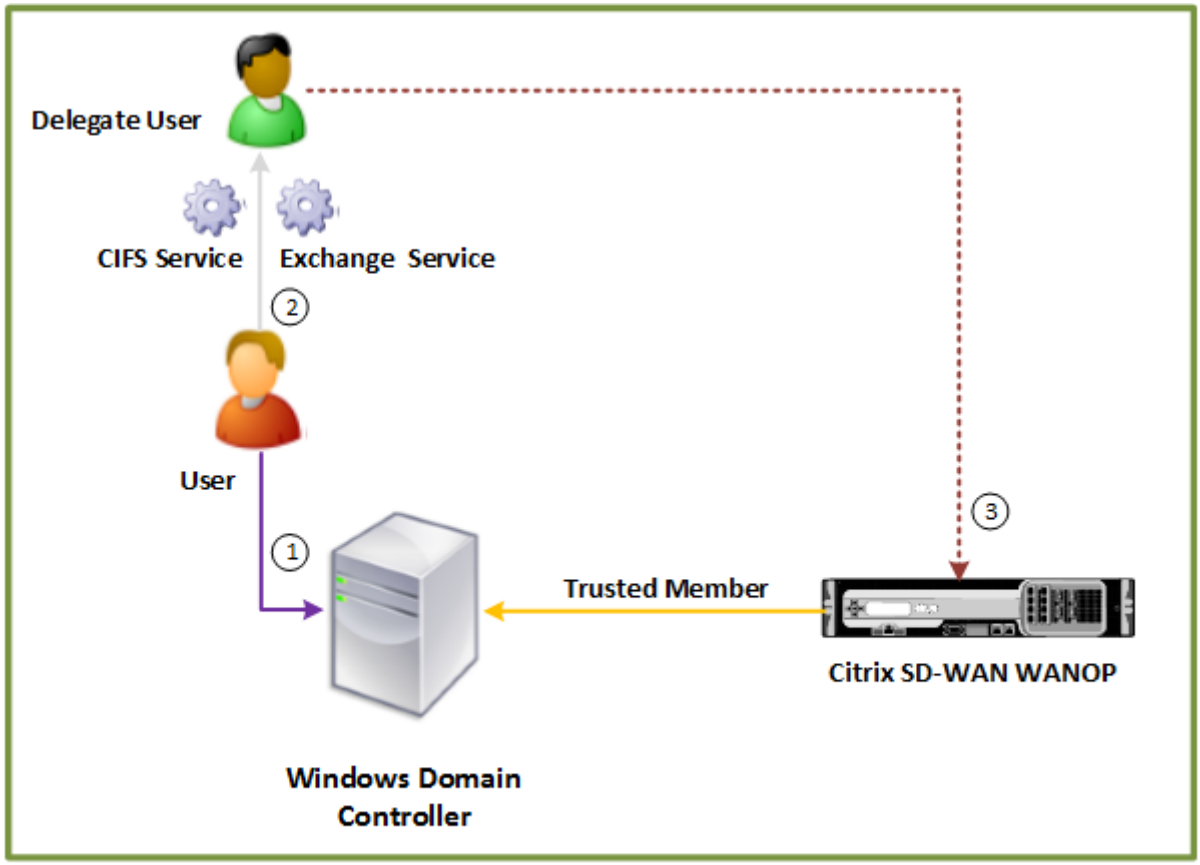
> **Remarque**
>
> Le client Outlook Macintosh n'utilise pas la norme MAPI (Outlook/Exchange) et n'est pas accéléré par cette fonctionnalité.

Ajouter un dispositif Citrix SD-WAN WANOP à l'infrastructure de sécurité Windows

Pour optimiser le trafic Windows sécurisé, l'appliance Citrix SD-WAN WANOP doit faire partie du système de sécurité Windows et doit s'authentifier auprès du système de sécurité ou du domaine. Comme indiqué dans la figure ci-dessous, pour faire de l'appliance une partie du système de sécurité Windows, vous devez faire en sorte que l'appliance joigne un domaine (à l'aide des informations d'identification administratives). En outre, vous devez configurer un utilisateur nouveau ou existant en tant qu'utilisateur délégué en associant les services CIFS et Exchange à cet utilisateur. Vous devez ensuite configurer cet utilisateur délégué sur l'appliance Citrix SD-WAN WANOP.

Vous pouvez utiliser l'utilitaire **Pre Domain Check** pour savoir s'il existe des problèmes liés à la connexion de l'appliance à un domaine.

> **Remarque**
>
> Le système de sécurité Windows utilise le service Exchange pour gérer les connexions MAPI. Configuration de la configuration pour optimiser le trafic Windows sécurisé



Joignez une appliance Citrix SD-WAN WANOP au domaine Windows :

Lorsque l'appliance rejoint le domaine, elle échange un secret partagé avec le contrôleur de domaine, ce qui lui permet de rester indéfiniment partie du domaine. Lorsque vous joignez une appliance à un domaine, assurez-vous que vous disposez des informations d'identification d'administrateur pour le Controller de domaine.

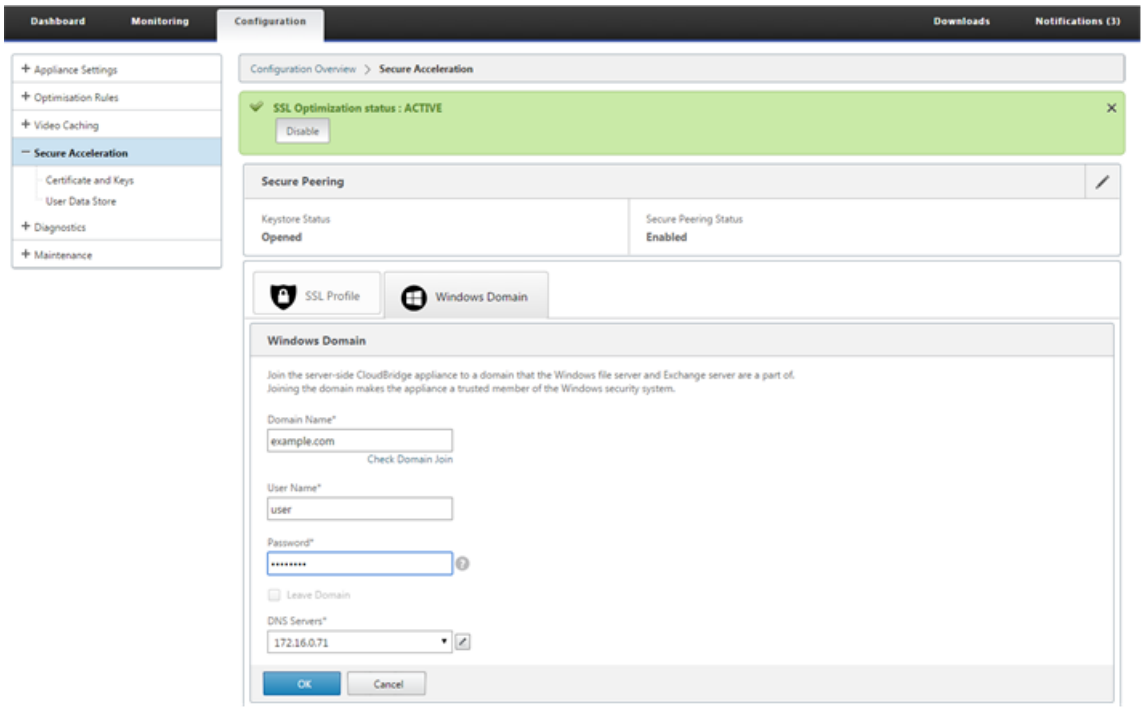
Pour vous assurer que l'appliance Citrix SD-WAN WANOP optimise le trafic CIFS et MAPI (y compris le trafic encapsulé en tant que RPC sur HTTPS), vous devez faire de l'appliance une partie du domaine dont font partie le serveur de fichiers Windows et le serveur Exchange. Vous devez joindre l'appliance côté serveur au domaine.

Remarque : les informations d'identification d'administration de domaine ne sont pas enregistrées sur l'appliance.

Pour joindre un dispositif Citrix SD-WAN WANOP à un domaine Windows :

1. Accédez à l'onglet **Configuration** > **Accélération sécurisée** > **Domaine Windows**.
2. Cliquez sur **Joindre le domaine Windows**.

3. Entrez le nom de domaine Windows dans le champ Nom de domaine.
4. Dans le champ Nom d'utilisateur, entrez le nom d'utilisateur de l'administrateur du Controller de domaine.
5. Dans le champ Mot de passe, spécifiez le mot de passe administrateur du Controller de domaine.
6. Si nécessaire, modifiez les serveurs DNS pour assurer la cohérence avec le domaine Windows.
7. Cliquez sur **OK**.
8. Dans la section Utilisateurs délégués, ajoutez un utilisateur délégué, comme décrit dans les procédures ci-dessous.



Configurer un utilisateur délégué :

Après avoir joint l'appliance à un domaine Windows, vous devez créer un utilisateur que l'appliance peut utiliser pour authentifier les utilisateurs avec le domaine. Cet utilisateur est connu sous le nom *d'utilisateur délégué*.

Remarque : Pour créer un compte d'utilisateur délégué, vous devez disposer d'un accès administrateur au Controller de domaine Windows et à l'appliance. Si vous n'avez pas accès administrateur au Controller de domaine Windows, assurez-vous qu'un administrateur autorisé effectue les tâches requises sur le Controller de domaine.

La configuration de l'authentification utilisateur à l'aide de la délégation Kerberos implique deux tâches : la configuration d'un utilisateur délégué sur le contrôleur de domaine, puis l'ajout de cet utilisateur à l'appliance Citrix SD-WAN WANOP.

Configurez un utilisateur délégué sur un Controller de domaine :

Avant de configurer un utilisateur délégué sur un dispositif Citrix SD-WAN WANOP, vous devez configurer un utilisateur délégué avec les propriétés requises sur le contrôleur de domaine. Vous pouvez créer un compte d'utilisateur délégué ou utiliser un compte d'utilisateur existant en tant que compte d'utilisateur délégué.

Après avoir créé un compte ou sélectionné un compte existant, activez la délégation pour cet utilisateur. Vous associez ensuite l'utilisateur délégué aux services CIFS et Exchange, afin que le trafic de ces services puisse être accéléré. Après avoir ajouté cet utilisateur à l'appliance Citrix SD-WAN WANOP, l'appliance présente des informations d'identification déléguées pour les services associés à ce compte.

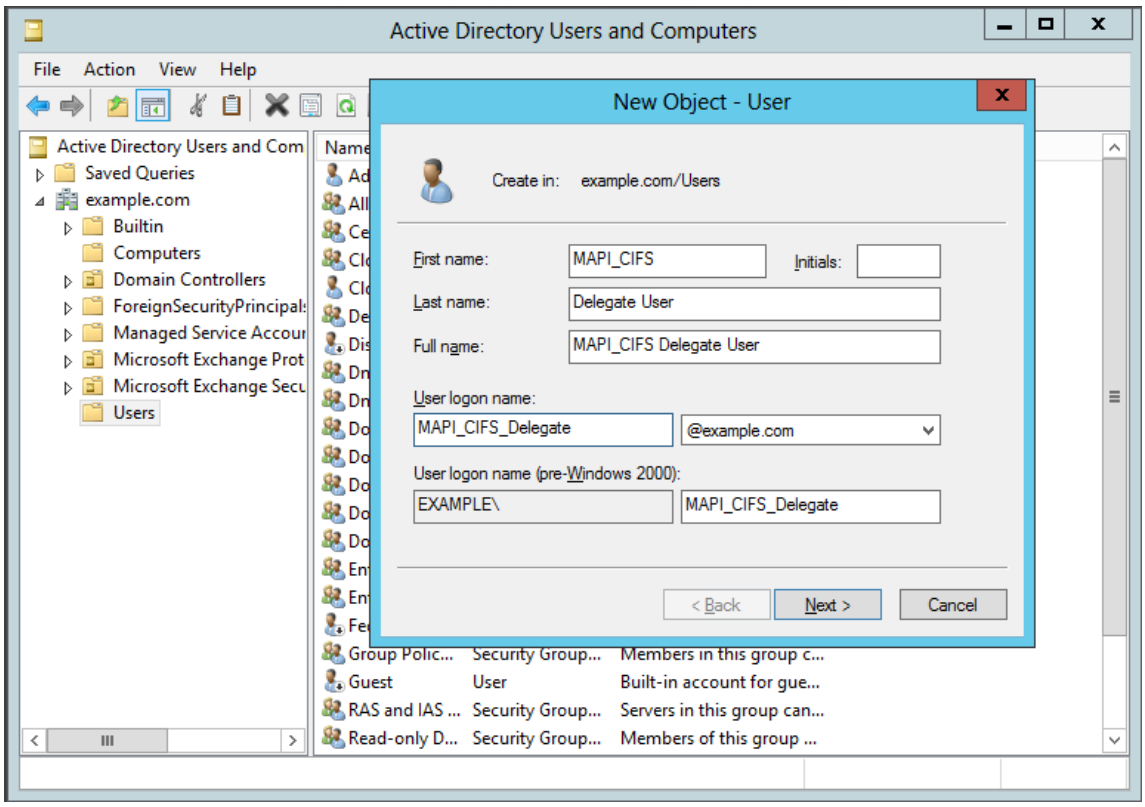
Créez un compte d'utilisateur délégué :

Créez un compte d'utilisateur délégué sur le contrôleur de domaine Windows afin que l'appliance Citrix SD-WAN WANOP puisse utiliser ce compte au nom des utilisateurs pour les authentifier auprès du contrôleur de domaine.

Remarque : si vous souhaitez configurer un utilisateur existant en tant qu'utilisateur délégué, ignorez cette procédure.

Pour créer un compte d'utilisateur délégué :

1. Ouvrez une session sur le Controller de domaine Windows en tant qu'administrateur. Assurez-vous que le serveur de fichiers ou le serveur Exchange est membre de ce domaine.
2. Dans le menu **Démarrer**, ouvrez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
3. Créez un utilisateur délégué, comme indiqué dans la capture d'écran suivante :

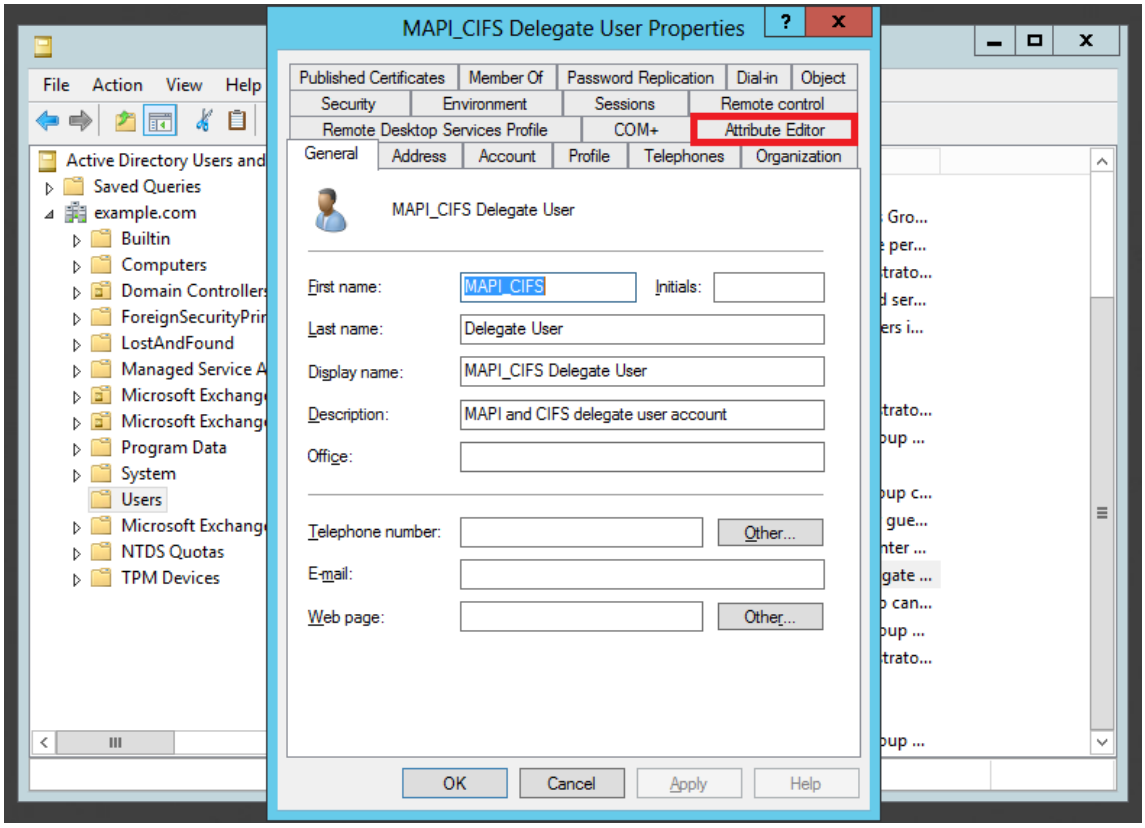


Activer la délégation pour un utilisateur :

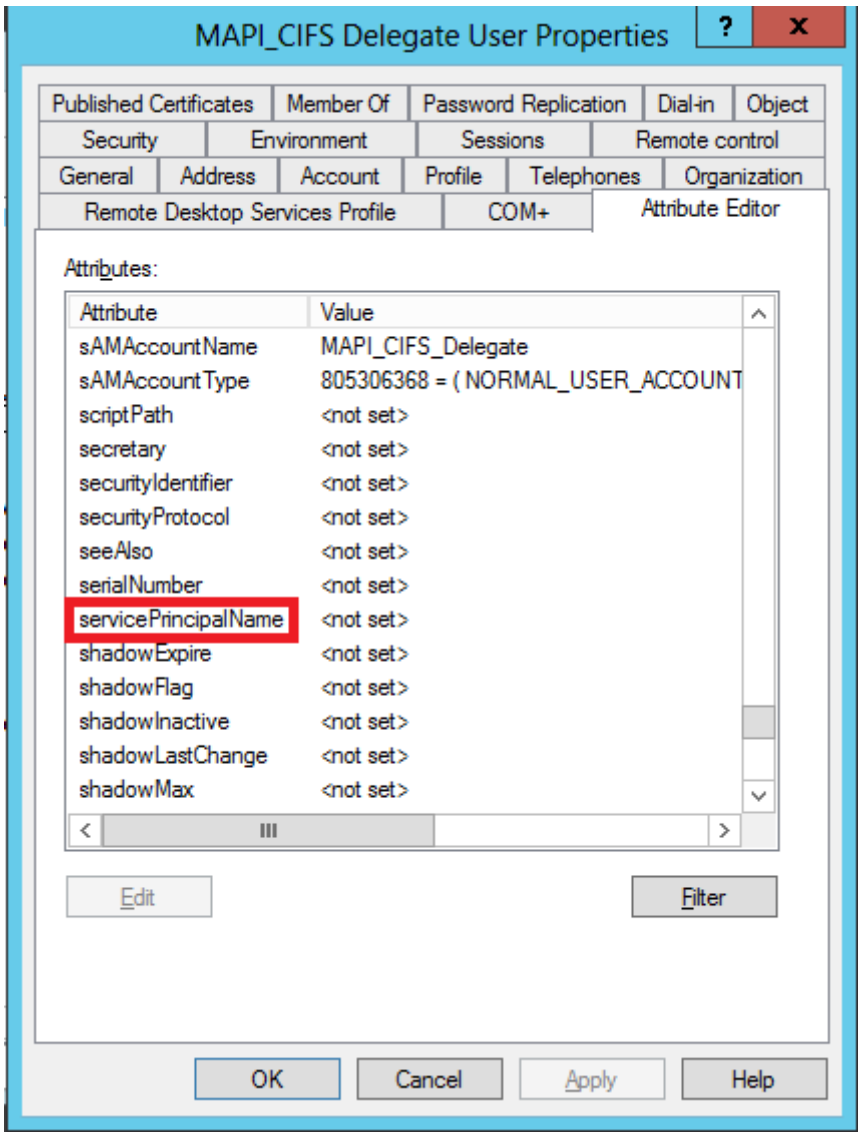
Jusqu'à présent, l'utilisateur que vous avez créé est similaire à n'importe quel utilisateur que vous créez sur le serveur Active Directory. Pour activer la délégation pour l'utilisateur, vous devez définir l'attribut Nom principal de service de l'utilisateur pour *déléguer* et associer l'utilisateur délégué aux services requis. Cela rend l'utilisateur à avoir des privilèges spéciaux attachés à lui et en faire un utilisateur délégué.

Pour activer la délégation pour l'utilisateur :

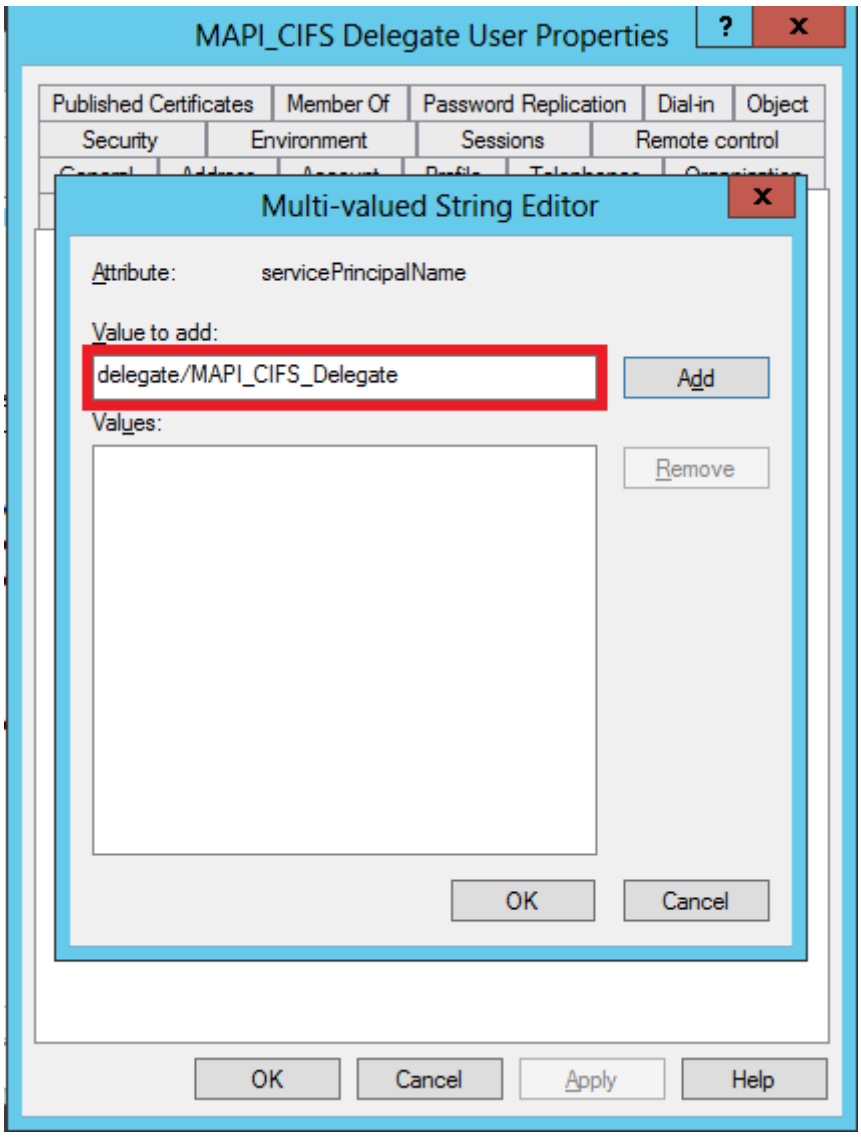
1. Dans le menu **Démarrer**, ouvrez la fenêtre **Utilisateurs et ordinateurs Active Directory**.
2. Dans le menu Affichage, sélectionnez **Fonctionnalités avancées**.
3. Sélectionnez le nœud **Utilisateur**.
4. Cliquez avec le bouton droit sur l'utilisateur que vous souhaitez créer un utilisateur délégué.
5. Dans le menu contextuel, sélectionnez **Propriétés** et accédez à l'onglet **Editeur d'attributs**, comme indiqué dans la capture d'écran suivante :



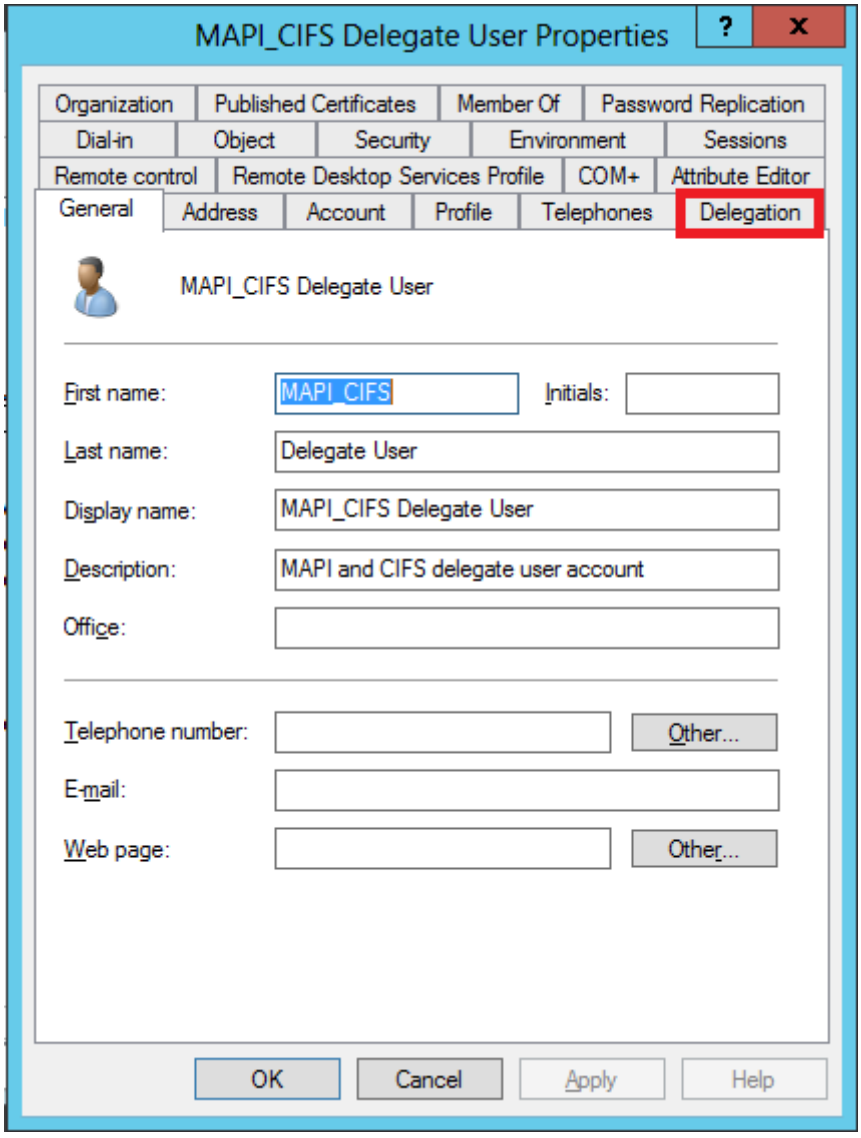
6. Dans la liste **Attributs**, sélectionnez **ServicePrincipalName**, comme indiqué dans la capture d'écran suivante :



7. Cliquez sur **Modifier**.
8. Dans la boîte de dialogue **Éditeur de chaîne à valeurs multiples**, dans le champ **Valeur à ajouter**, spécifiez **delegate/<*User_Name*>**, comme indiqué dans la capture d'écran suivante :



9. Cliquez sur **Ajouter**.
10. Cliquez sur **OK**.
11. Cliquez sur **Apply**.
12. Cliquez sur **OK**.
13. Ouvrez la boîte de dialogue **Propriétés de l'utilisateur délégué MAPI-CIFS** de l'utilisateur et vérifiez que l'onglet **Délégation** a été ajouté à la boîte de dialogue, comme indiqué dans la capture d'écran suivante :



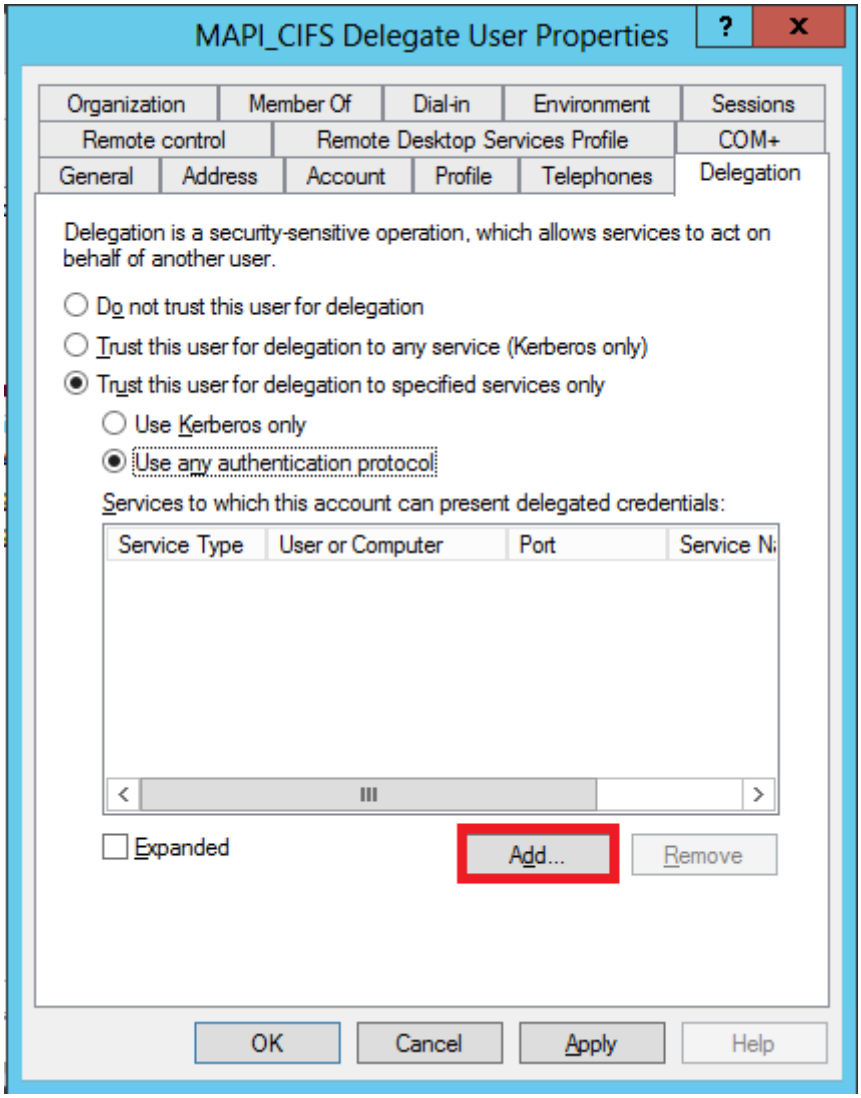
Associez l'utilisateur délégué à CIFS et Exchange Services :

Après avoir activé l'onglet Délégation pour l'utilisateur, vous pouvez l'associer à des services pour lesquels l'utilisateur peut présenter des informations d'identification déléguées. Lorsque vous ajoutez cet utilisateur à l'appliance Citrix SD-WAN WANOP, l'appliance présente des informations d'identification déléguées pour les services associés à ce compte.
Remarque : l'infrastructure de sécurité Windows utilise le service Exchange pour gérer le trafic MAPI.

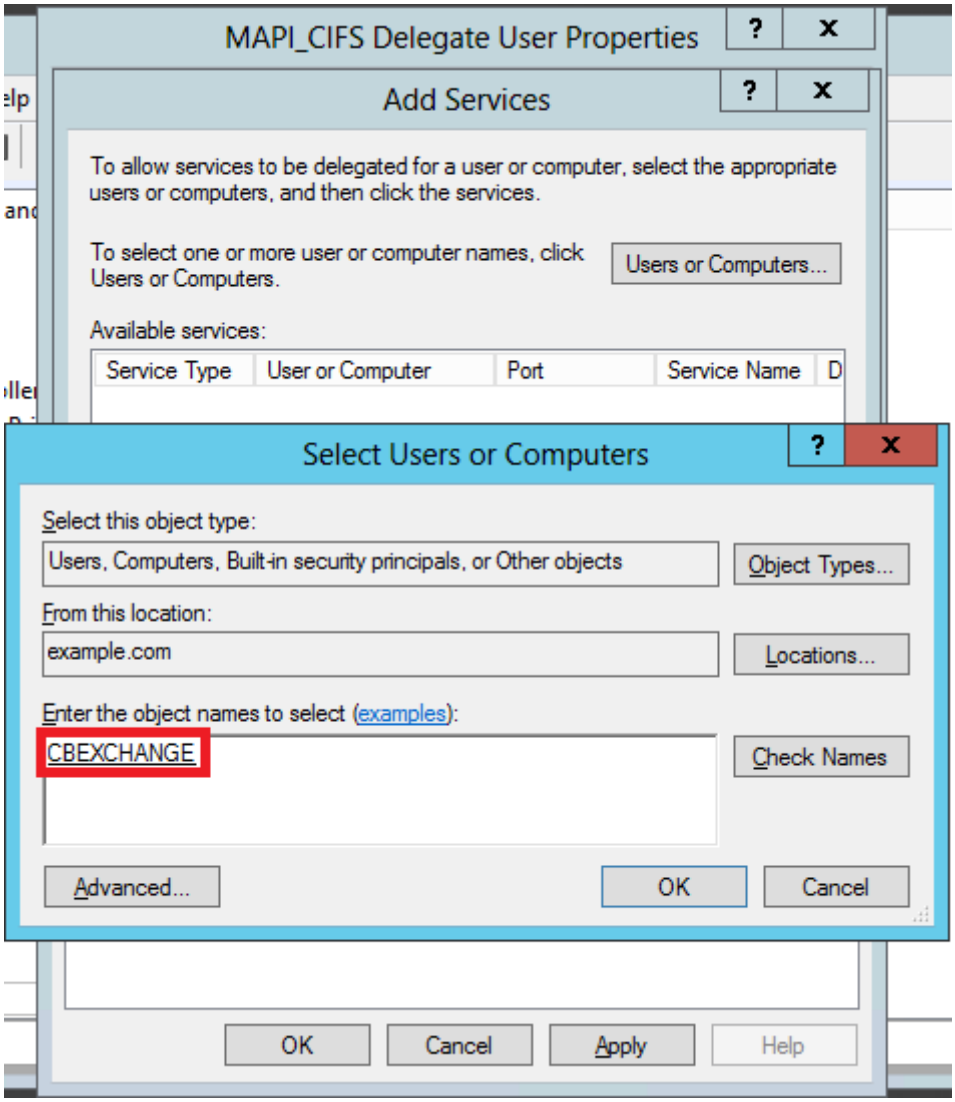
Pour associer l'utilisateur délégué aux services CIFS et Exchange :

1. Dans l'onglet Délégation, sélectionnez l'option **Approuver cet utilisateur pour la délégation à des services spécifiques uniquement**.
2. Sélectionnez l'option **Utiliser n'importe quel protocole d'authentification**.

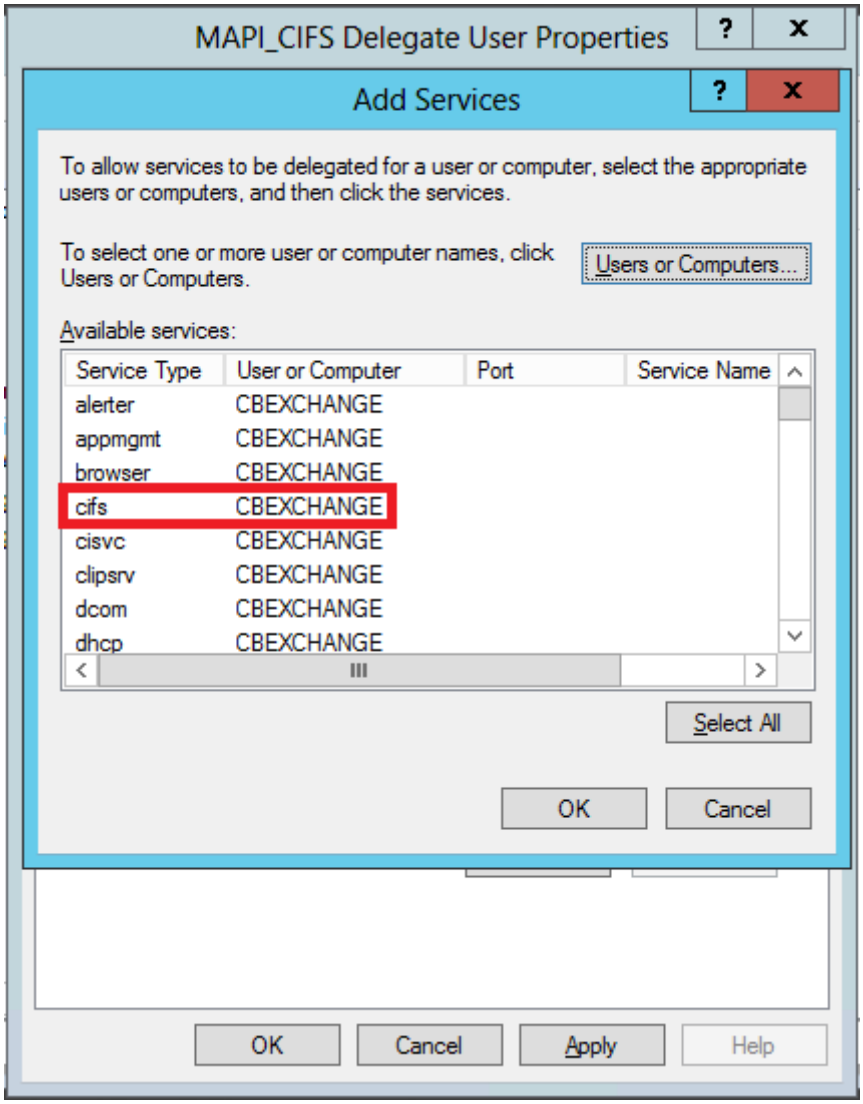
3. Cliquez sur **Ajouter**, comme indiqué dans la capture d'écran suivante :



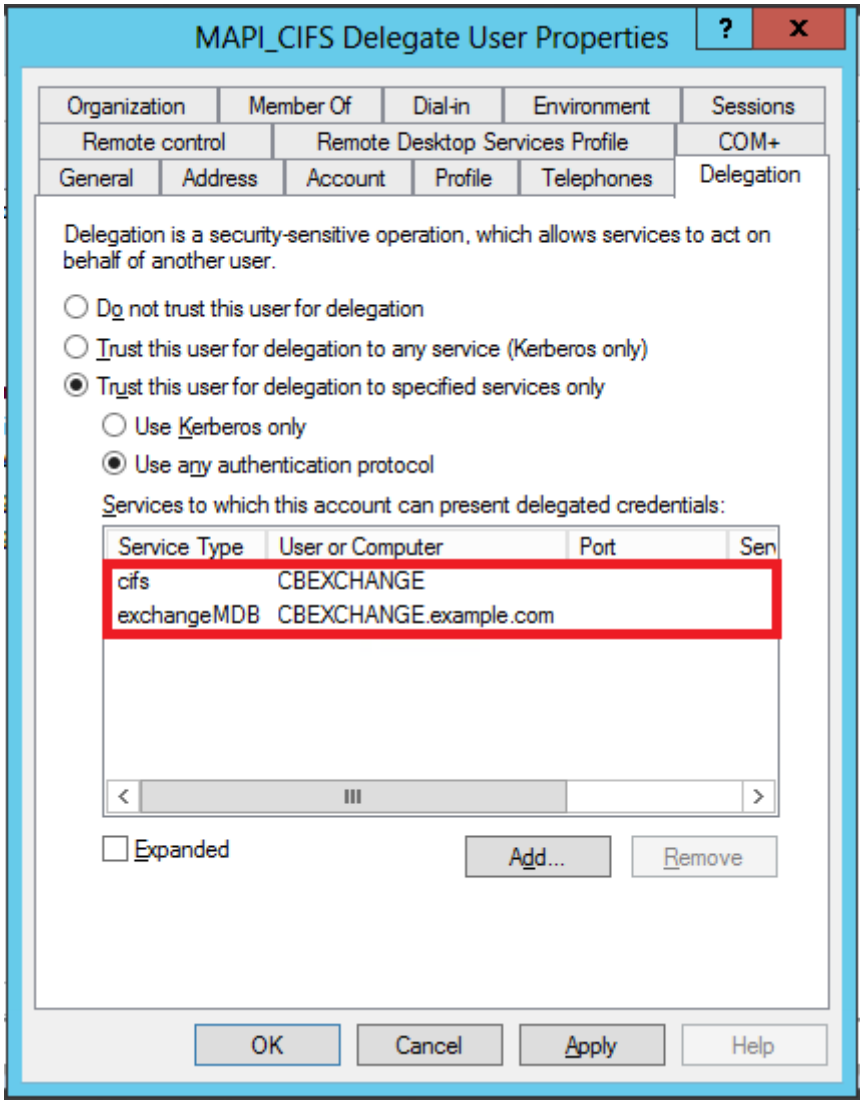
4. Dans la boîte **de dialogue Ajouter un service**, cliquez sur **Utilisateurs et ordinateurs**.
5. Dans la boîte de dialogue **Sélectionner les utilisateurs ou les ordinateurs**, ajoutez l'ordinateur local à sélectionner, comme indiqué dans la capture d'écran suivante :



6. Cliquez sur **OK**.
7. Dans la boîte de dialogue Ajouter des services, dans la liste **Services disponibles**, sélectionnez **cifs**, comme indiqué dans la capture d'écran suivante :



8. Si vous devez configurer l'accélération MAPI sur l'appliance Citrix SD-WAN WANOP, appuyez longuement sur la touche **Ctrl** et sélectionnez le service **ExchangeDB**.
9. Cliquez sur **OK**. Les services que vous avez sélectionnés sont ajoutés à la liste **Services auxquels ce compte peut présenter des informations d'identification déléguées**, comme indiqué dans la capture d'écran suivante :



10. Cliquez sur **OK**.
11. Fermez la fenêtre **Utilisateurs et ordinateurs Active Directory**.

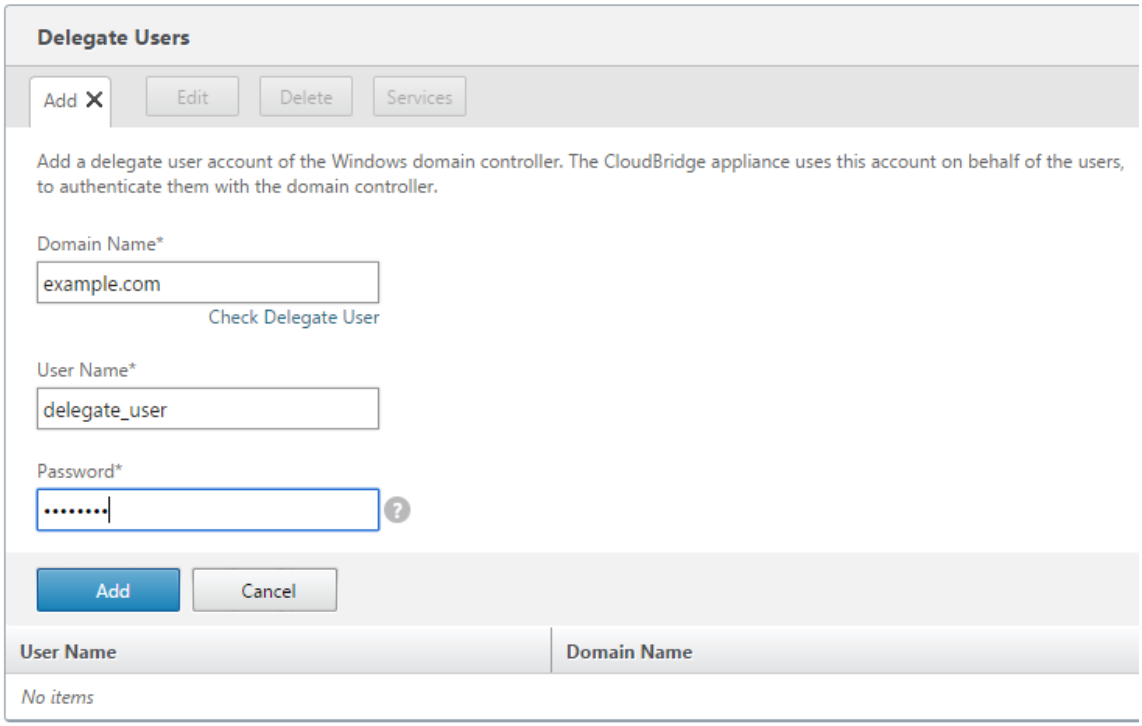
Configurez un utilisateur délégué sur une appliance Citrix SD-WAN WANOP :

Après avoir configuré l'utilisateur délégué sur le serveur Active Directory, vous devez configurer cet utilisateur sur l'appliance Citrix SD-WAN WANOP, afin que l'appliance puisse présenter les informations d'identification déléguées de cet utilisateur au domaine. Cela permet à l'appliance d'optimiser activement le trafic réseau pour les fonctionnalités d'accélération CIFS et MAPI avancées.

Pour ajouter l'utilisateur délégué à l'appliance côté serveur :

1. Accédez à l'onglet **Configuration** > **Accélération sécurisée** > **Domaine Windows**.
2. Cliquez sur le bouton **Joindre le domaine Windows**, le cas échéant.
3. Sous **Utilisateurs délégués**, cliquez sur **Ajouter**.

4. Dans le champ **Nom de domaine**, spécifiez le nom de domaine. Il s'agit généralement du domaine que vous avez spécifié dans la section **Domaine Windows**.
5. Dans le champ **Nom d'utilisateur**, entrez le nom d'utilisateur de l'utilisateur délégué.
6. Dans le champ **Mot de passe**, spécifiez le mot de passe de l'utilisateur délégué.
7. Cliquez sur **Ajouter**.



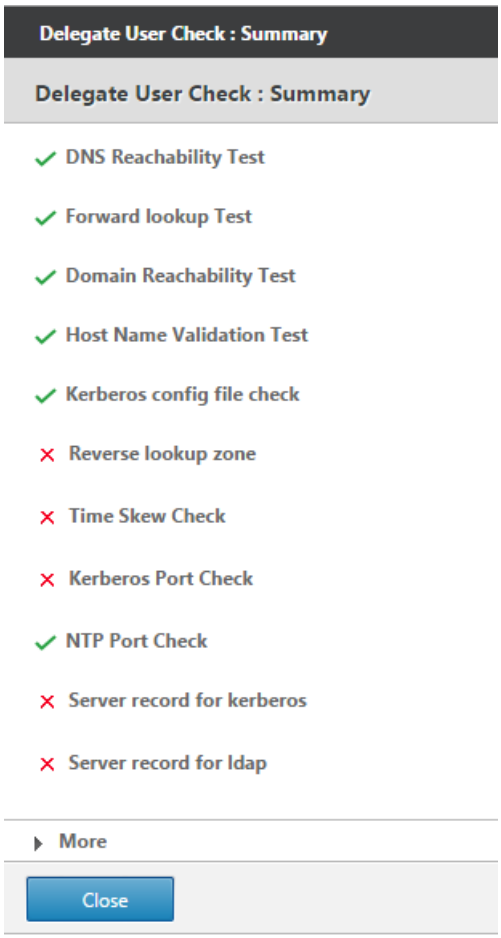
Vérifiez que l'appliance a rejoint le domaine

Si, après avoir ajouté l'appliance au domaine, vous remarquez qu'elle n'optimise pas le trafic Windows sécurisé, une erreur peut avoir empêché l'appliance de rejoindre le domaine. Vous pouvez utiliser l'utilitaire **Pre Domain Check** pour savoir s'il y a des problèmes avec la connexion du matériel au domaine. Vous pouvez même exécuter cet utilitaire pour identifier les problèmes éventuels avant de tenter de joindre l'appliance à un domaine.

Pour vérifier l'utilisateur délégué :

1. Connectez-vous à l'appliance Citrix SD-WAN WANOP côté serveur.
2. Accédez à **Configuration** > **Accélération sécurisée** > onglet **Windows**.
3. Cliquez sur le bouton **Joindre le domaine Windows**, le cas échéant.
4. Sélectionnez un utilisateur délégué et cliquez sur **Modifier**.
5. Cliquez sur **Vérifier l'utilisateur délégué**.

6. Attendez que la vérification du domaine utilisateur délégué se termine et examinez les résultats.



Configurer l'accélération CIFS et SMB2/SMB3

April 23, 2021

La fonction d'accélération CIFS fournit une suite d'améliorations des performances spécifiques au protocole pour le transfert de fichiers CIFS (Windows et Samba) et la navigation dans les répertoires, y compris des améliorations au transport CIFS et aux protocoles connexes tels que DCERPC.

L'accélération CIFS comporte trois parties :

- Accélération du contrôle de flux TCP : cette opération est effectuée sur toutes les connexions CIFS accélérées, quelle que soit la version du protocole (SMB1, SMB2 ou SMB3) ou le degré d'authentification et de chiffrement.
- Accélération du protocole CIFS : ces optimisations augmentent les performances CIFS en réduisant le nombre d'allers-retours nécessaires à l'exécution d'une commande CIFS. Ces optimi-

sations sont effectuées automatiquement sur les connexions CIFS SMB1 et SMB2 qui n'utilisent pas l'authentification par paquet CIFS (« signature »), ou lorsque la signature est utilisée et que les appliances ont rejoint le domaine Windows dans un rôle de « délégué de sécurité ».

- Compression CIFS : les connexions CIFS sont compressées automatiquement chaque fois qu'elles répondent aux exigences de l'accélération du protocole CIFS. En outre, les connexions SMB3 sont compressées lorsqu'elles sont non signées et non scellées.

Sur les réseaux sur lesquels la signature CIFS est activée, l'accélération et la compression du protocole CIFS exigent que vous désactiviez l'authentification par paquets CIFS (signature) ou que vos appliances de centre de données rejoignent le domaine Windows et créent une relation d'homologue sécurisée entre les appliances du centre de données et vos appliances distantes. et les plug-ins Citrix SD-WAN WANOP.

Tableau 1. Fonctionnalités d'accélération CIFS, selon la version du protocole SMB et si l'appliance a rejoint le domaine Windows.

Version SMB	Contrôle de débit TCP	Compression	Accélération du protocole
		Signature désactivée	
SMB 1.0	O	O	O
SMB 2.0	O	O	O
SMB 2.1	O	O	N
SMB 3.0	O	O	N
		*Signature activée, Citrix SD-WAN WANOP a rejoint le domaine ***	
SMB 1.0	O	O	O
SMB 2.0	O	O	O
SMB 2.1	O	O	O
SMB 3.0	O	O	Y *
		Signature activée, Citrix SD-WAN WANOP n'a pas rejoint le domaine	
SMB 1.0	O	N	N
SMB 2.0	O	N	N

Version SMB	Contrôle de débit TCP	Compression	Accélération du protocole
SMB 2.1	O	N	N
SMB 3.0	O	N	N

* SMB 3.0 Support a été ajouté dans la version 7.4.2.

** Citrix SD-WAN WANOP ne prend pas en charge l'authentification NTLMv2 (par défaut pour Windows 7) avec SMB 1/ SMB 2/ SMB 3 et avec le serveur NetApp. L'activation de l'authentification Kerberos permet l'accélération.

Tableau 2. Quelle version du protocole SMB est utilisée, par le système d'exploitation client et serveur.

Système d' exploitation client/serveur	Windows 8, Windows 10 ou Windows Server 2012	Windows 7 ou Windows Server 2008 R2	Windows Vista ou Windows Server 2008	Versions antérieures de Windows
Windows 8, Windows 10 ou Windows Server 2012	SMB 3.0	SMB 2.1	SMB 2.0	SMB 1.0
Windows 7 ou Windows Server 2008 R2	SMB 2.1	SMB 2.1	SMB 2.0	SMB 1.0
Windows Vista ou Windows Server 2008	SMB 2.0	SMB 2.0	SMB 2.0	SMB 1.0
Versions antérieures de Windows	SMB 1.0	SMB 1.0	SMB 1.0	SMB 1.0

Versions prises en charge de CIFS :

Toutes les implémentations CIFS n'utilisent pas les modèles de requête reconnus par l'appliance. Ces versions non prises en charge n'atteignent pas l'accélération dans toute la gamme des cas, comme indiqué dans le tableau suivant.

Tableau 3. Prise en charge de Citrix SD-WAN WANOP pour les serveurs et clients CIFS.

Produit	Serveur	Client
Windows Server 2003-2012	Oui*	Oui*
Windows XP, Vista, 7, 8, 2000	Oui*	Oui*
NetApp	Oui**	S.O.
Hitachi	Oui**	S.O.
Windows NT	Oui	Non
Windows ME et versions antérieures	Non	Non

> **Remarque** : la plupart des implémentations CIFS tierces émulent l'un des serveurs ou clients énumérés ci-dessus. Dans la mesure où l'émulation est réussie, le trafic est accéléré, ou non, comme indiqué dans le tableau ci-dessus. Si l'émulation se comporte différemment de ce que l'accélérateur CIFS attend, l'accélération CIFS est interrompue pour cette connexion.

Le comportement de l'accélération CIFS avec une implémentation CIFS donnée ne peut être connu avec certitude tant qu'il n'a pas été testé.

Les modes d'accélération CIFS sont :

- Lectures et écritures de fichiers volumineux
- Lectures et écritures de fichiers de petite taille
- Navigation dans le répertoire.

Lectures et écritures de fichiers volumineux : ces optimisations SMB1 sont destinées aux transferts de fichiers d'au moins 640 Ko. Des techniques sûres de lecture anticipée et d'écriture arrière sont utilisées pour diffuser les données sans pause pour chaque transfert (un transfert est de 64 Ko ou moins).

Ces optimisations ne sont activées que si le transfert a un verrou LOT ou EXCLUSIVE et est « simple. » Les copies de fichiers sont toujours simples. Les fichiers ouverts via les applications peuvent être ou non, selon la façon dont ils sont gérés au sein de l'application.

Des rapports de vitesse de 10x sont facilement accessibles avec l'accélération CIFS, à condition que votre liaison et vos disques soient suffisamment rapides pour accueillir dix fois vos vitesses de transfert actuelles. Une accélération de 50x peut être obtenue si nécessaire, mais n'est pas normalement activée, en raison de la consommation de mémoire. Contactez votre représentant Citrix si 10x n'est pas suffisant.

Lecture et écriture de petits fichiers : lesaméliorations de petits fichiers centrent davantage sur l'optimisation des métadonnées (répertoire) que sur la diffusion de données. CIFS natif ne combine pas

efficacement les demandes de métadonnées. L'accélération CIFS fait. Comme pour l'accélération de gros fichiers, ces optimisations ne sont pas effectuées à moins qu'elles ne soient sûres (par exemple, elles ne sont pas effectuées si le client CIFS n'a pas reçu de verrou exclusif sur le répertoire). Lorsque le protocole SMB2 est utilisé, les métadonnées de fichier sont mises en cache localement pour des améliorations encore plus importantes.

Navigation dans les répertoires : les clients CIFS standard effectuent la navigation dans les répertoires d'une manière extrêmement inefficace, nécessitant un grand nombre d'allers-retours pour ouvrir un dossier distant. L'accélération CIFS réduit le nombre de voyages aller-retour à 2 ou 3. Lorsque le protocole SMB2 est utilisé, les données de répertoire sont mises en cache localement pour des améliorations encore plus importantes.

Accélération du protocole CIFS

L'accélération CIFS est prise en charge sur tous les modèles. CIFS est un protocole basé sur TCP et bénéficie du contrôle de flux. Cependant, CIFS est mis en œuvre d'une manière très inefficace sur les réseaux longue distance, ce qui nécessite un nombre excessif d'allers-retours pour terminer une opération. Étant donné que le protocole est très sensible à la latence de liaison, l'accélération complète doit être sensible au protocole.

L'accélération CIFS réduit le nombre d'allers-retours grâce à une variété de techniques. Le modèle des requêtes du client est analysé et sa prochaine action est prédite. Dans de nombreux cas, il est sûr d'agir sur la prédiction même si elle est fausse, et ces opérations sûres sont à la base de nombreuses optimisations.

Par exemple, les clients SMB1 émettent des lectures de fichiers séquentielles sans chevauchement, en attendant que chaque lecture de 64 Ko se termine avant d'émettre la lecture suivante. En implémentant la lecture anticipée, l'appliance peut accélérer jusqu'à 10 fois en toute sécurité en récupérant les données anticipées à l'avance.

Des techniques supplémentaires accélèrent la navigation dans les répertoires et les opérations de petits fichiers. L'accélération est appliquée non seulement aux opérations CIFS, mais aussi aux opérations RPC connexes.

Conditions préalables

L'accélération CIFS est prise en charge sur tous les modèles. CIFS est un protocole basé sur TCP et bénéficie du contrôle de flux. Cependant, CIFS est mis en œuvre d'une manière très inefficace sur les réseaux longue distance, ce qui nécessite un nombre excessif d'allers-retours pour terminer une opération. Étant donné que le protocole est très sensible à la latence de liaison, l'accélération complète doit être sensible au protocole.

L'accélération CIFS réduit le nombre d'allers-retours grâce à une variété de techniques. Le modèle des requêtes du client est analysé et sa prochaine action est prédite. Dans de nombreux cas, il est sûr d'agir sur la prédiction même si elle est fausse, et ces opérations sûres sont à la base de nombreuses optimisations.

Par exemple, les clients SMB1 émettent des lectures de fichiers séquentielles sans chevauchement, en attendant que chaque lecture de 64 Ko se termine avant d'émettre la lecture suivante. En implémentant la lecture anticipée, l'appliance peut accélérer jusqu'à 10 fois en toute sécurité en récupérant les données anticipées à l'avance.

Des techniques supplémentaires accélèrent la navigation dans les répertoires et les opérations de petits fichiers. L'accélération est appliquée non seulement aux opérations CIFS, mais aussi aux opérations RPC connexes.

Si votre réseau utilise la signature CIFS, l'appliance doit être un membre approuvé du domaine. Pour faire de l'appliance un membre approuvé du domaine, reportez-vous à la section Ajout d'une appliance Citrix SD-WAN WANOP à l'infrastructure de sécurité Windows.

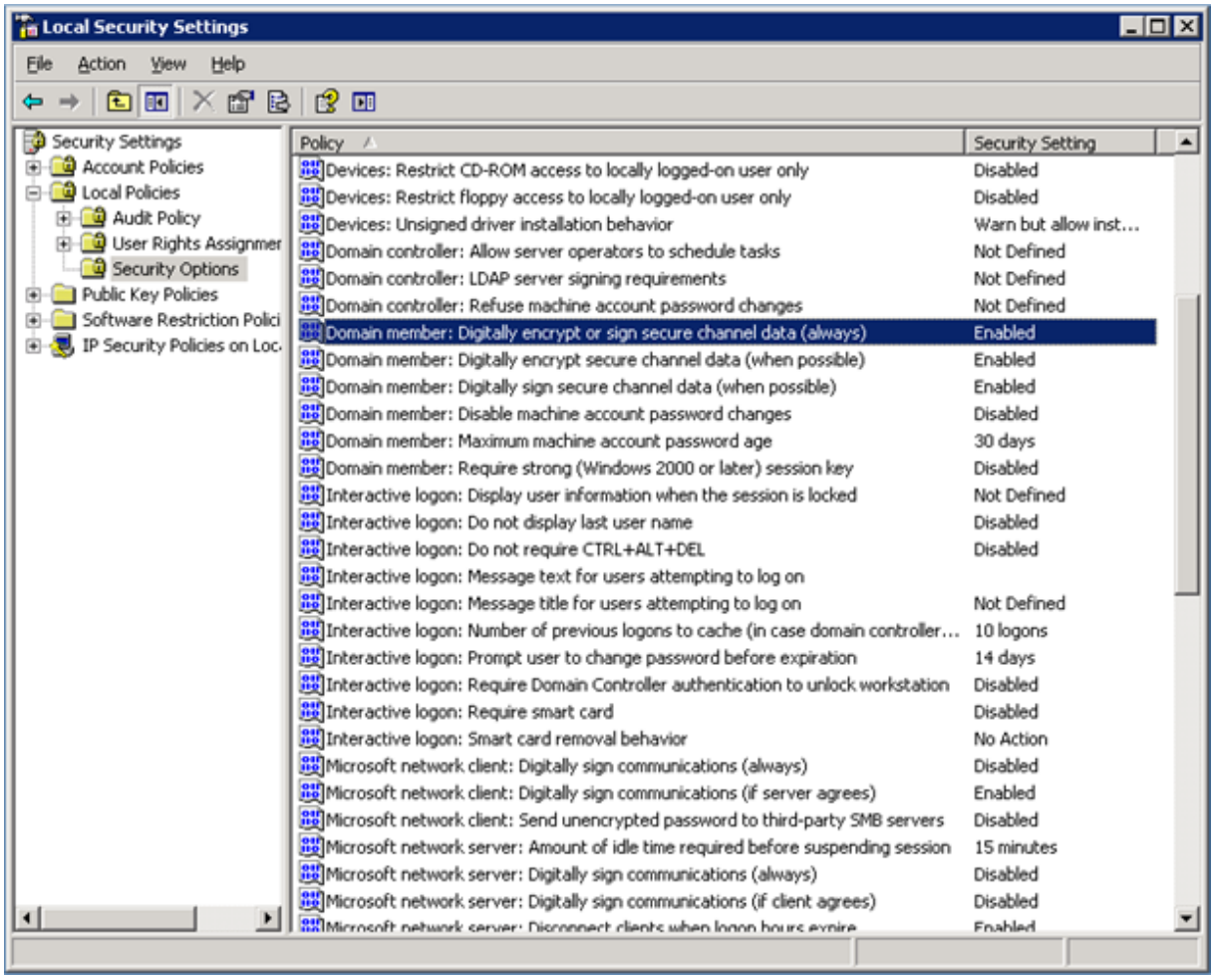
Configurer l'accélération du protocole CIFS

L'accélération CIFS est activée par défaut pour les connexions qui n'utilisent pas la signature CIFS. Si votre réseau utilise la signature, il peut être désactivé ou les appliances côté serveur peuvent le fairerejoignent le domaine Windows.

Désactiver la signature CIFS

En fonction de leurs paramètres de sécurité, les serveurs Windows ou les serveurs de domaine peuvent avoir besoin d'ajuster leurs paramètres de sécurité.

Figure 1. Options de sécurité Windows Server, Windows Server 2003 et Windows Server 2008.



Les serveurs de fichiers Windows ont deux modes de sécurité : « scellement » et « signature «.

L'étanchéité crypte le flux de données et empêche complètement l'accélération du protocole CIFS.

La signature ajoute des données d'authentification à chaque paquet de données, sans chiffrer le flux de données. Cela empêche l'accélération, sauf si vous avez implémenté les procédures décrites dansAjout d'une appliance Citrix SD-WAN WANOP à l'infrastructure de sécurité Windows. Lorsque cette exigence est satisfaite, la signature est accélérée automatiquement. Sinon, la signature doit être désactivée (si elle n'est pas déjà désactivée) pour que l'accélération du protocole ait lieu.

Par défaut, les serveurs de fichiers Windows proposent la signature mais ne l'exigent pas, sauf pour les serveurs de domaine, qui l'exigent par défaut.

Pour accélérer CIFS avec les systèmes qui nécessitent actuellement une signature, vous devez modifier les paramètres de sécurité du système pour désactiver cette exigence. Vous pouvez le faire dans les paramètres de sécurité locaux du serveur de fichiers ou dans les stratégies de groupe. Les exemples suivants, pour Windows Server 2003 et Windows Server 2008, montrent les paramètres locaux. Les changements de stratégie de groupe sont, bien sûr, presque identiques.

Citrix SD-WAN WANOP

Pour modifier le paramètre du serveur pour autoriser l'accélération CIFS

1. Accédez à la page Paramètres de sécurité locaux du système.
2. Définir un membre du domaine : chiffrer ou signer numériquement les données du canal sécurisé (toujours) sur Désactivé.
3. Définissez le client réseau Microsoft : Signer numériquement les communications (toujours) sur Désactivé.
4. Définissez le serveur réseau Microsoft : Signer numériquement les communications (toujours) sur Désactivé.

Interpréter les statistiques CIFS

La page Surveillance : système de fichiers (CIFS/SMB) affiche une liste de connexions CIFS accélérées. Ces connexions sont divisées en connexions « optimisées » et « non optimisées ». Comme toutes ces connexions sont accélérées (avec contrôle de débit et compression), les connexions « optimisées » ont des optimisations CIFS en plus du contrôle et de la compression, tandis que les connexions « non optimisées » ont uniquement le contrôle de débit et la compression.

Résumé de la gestion CIFS

- L'accélération CIFS apporte une amélioration significative même à des distances de liaison relativement courtes.
- L'accélération CIFS commence lorsqu'un système de fichiers est accessible pour la première fois par le client. Si l'accélération est activée avec le serveur de fichiers et le client déjà opérationnel, aucune accélération ne se produit pendant plusieurs minutes, jusqu'à ce que les connexions CIFS préexistantes soient complètement fermées. Les connexions CIFS sont très persistantes et durent longtemps avant de se fermer, même en cas d'inactivité. Ce comportement est ennuyeux pendant le test, mais a peu d'importance dans le déploiement normal.
- Le démontage et le remontage d'un système de fichiers dans Windows ne ferme pas les connexions CIFS, car Windows ne démonte pas vraiment le système de fichiers complètement. Le redémarrage du client ou du serveur fonctionne. Pour une mesure moins invasive, utilisez la commande NET USE devicename /DELETE de la ligne de commande Windows pour démonter complètement le volume. Sous Linux, smbmount et umount démontent complètement le volume.
- La désactivation, puis la réactivation des optimisations de lecture et d'écriture CIFS sur l'appliance soulève des problèmes similaires. Les connexions existantes ne sont pas accélérées

lorsque CIFS est activé et le nombre d'« erreurs de protocole détectées » sur la page Surveillance : système de fichiers (CIFS/SMB) augmente brièvement.

- Les statistiques CIFS peuvent prêter à confusion, car seule l'appliance la plus éloignée du serveur de fichiers signale une accélération CIFS avec des statistiques complètes. L'autre appliance le voit comme une accélération ordinaire.
- L'accélération CIFS n'est pas prise en charge en mode proxy.
- Si l'accélération CIFS n'a pas lieu avec un serveur Windows, vérifiez les paramètres de sécurité du serveur.

Configurer l'accélération MAPI

April 23, 2021

L'accélération de Microsoft Outlook améliore les performances du trafic entre les clients Microsoft Outlook et les serveurs Microsoft Exchange, augmentant ainsi le débit grâce à diverses optimisations, notamment la prérécupération et la compression des données.

Cette fonctionnalité est également appelée « accélération MAPI », après le protocole MAPI utilisé entre Outlook et Exchange Server.

Dans les réseaux où le flux de données Outlook est non chiffré (valeur par défaut avant Outlook 2007), cette fonctionnalité ne nécessite aucune configuration.

Dans les réseaux où les données Outlook sont chiffrées (valeur par défaut avec Outlook 2007 et versions ultérieures), l'accélération peut être obtenue de deux façons : en désactivant le chiffrement dans les clients Outlook ou en faisant en sorte que les appliances rejoignent le domaine Windows.

Versions et modes d'échange Outlook pris en charge

Les appliances Citrix SD-WAN WANOP fournissent une accélération MAPI pour Microsoft Outlook 2003-2016 et Exchange Server 2003-2010, dans les circonstances suivantes :

- Toute combinaison de clients et de serveurs pris en charge (à l'aide du protocole MAPI) est prise en charge.
- Si l'appliance côté serveur a rejoint un domaine Windows, les connexions avec le chiffrement MAPI sont accélérées. Sinon, ils ne le sont pas, et le chiffrement doit être désactivé dans les clients Outlook.

> **Remarque**
>
> Dans Exchange Server 2013, le protocole MAPI a changé en protocole RPC sur HTTP, ce protocole est pris en charge. Avec Exchange Server SP1, le protocole RPC sur HTTP a changé en protocole MAPI sur protocole HTTP, ce protocole n'est actuellement pas pris en charge.

Conditions préalables

Si votre réseau utilise des données Outlook chiffrées, qui est le paramètre par défaut dans Outlook 2007 et versions ultérieures, vous devez implémenter l'une des conditions préalables suivantes pour vous assurer que les connexions MAPI sont accélérées :

- Désactivez le chiffrement dans les clients Outlook.
- Effectuez les tâches décrites à la section Ajout d'une appliance Citrix SD-WAN WANOP à l'infrastructure de sécurité Windows.

Configuration

L'accélération Outlook est une fonctionnalité de configuration zéro activée par défaut. (Si ce n'est pas le cas, il peut être désactivé en désactivant l'accélération sur la classe de service MAPI sur la page **Configuration : Stratégie de classe de service**.) L'accélération Outlook a lieu automatiquement si les conditions suivantes sont remplies :

- Une appliance se trouve à l'extrémité Exchange Server du réseau étendu.
- Soit il y a une appliance à la fin Outlook du réseau étendu, soit le système exécutant Outlook exécute également le plug-in Citrix SD-WAN WANOP.
- Tout le trafic Outlook/Exchange passe par les appliances (ou l'appliance et le plug-in).
- Exchange Server ou Outlook est redémarré (l'accélération ne commence pas tant que les connexions MAPI existantes ne sont pas fermées).
- Soit le chiffrement est désactivé sur Outlook, soit l'appliance côté serveur appartient au domaine Windows et dispose d'une relation homologue sécurisée avec l'appliance côté client (ou le plug-in Citrix SD-WAN WANOP). Dans le cas où l'appliance a rejoint le domaine Windows, l'authentification sur le domaine doit être conservée au paramètre par défaut (négocier), pour que l'accélération fonctionne.

Désactiver le chiffrement sur Outlook 2007 ou Outlook 2010

Sauf si l'appliance côté serveur a rejoint le domaine Windows et a une relation homologue sécurisée avec l'appliance côté client (ou le plug-in Citrix SD-WAN WANOP), le chiffrement entre Outlook et Ex-

change Server doit être désactivé pour que l'accélération ait lieu.

Le chiffrement a été désactivé par défaut avant Outlook 2007. À partir d'Outlook 2007, le chiffrement est activé par défaut.

Note de performance

MAPI utilise un format de données différent des autres protocoles. Cette différence empêche une compression inter-protocole efficace. Autrement dit, un fichier qui a d'abord été transféré via FTP puis en tant que pièce jointe ne reçoit pas d'avantage de compression sur le second transfert. Si les mêmes données sont envoyées deux fois au format MAPI, le second transfert reçoit une compression complète.

Compression SSL

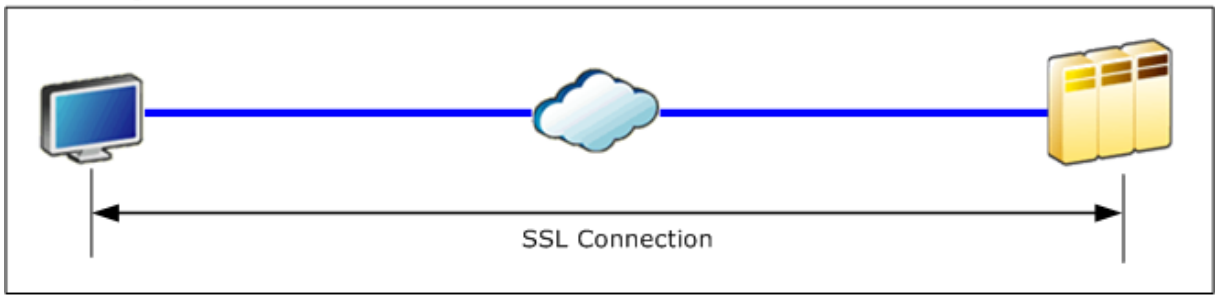
April 9, 2021

La compression SD-WAN WANOP SSL de Citrix applique la compression multisession aux connexions SSL (par exemple, trafic HTTPS), fournissant des rapports de compression allant jusqu'à 10 000:1.

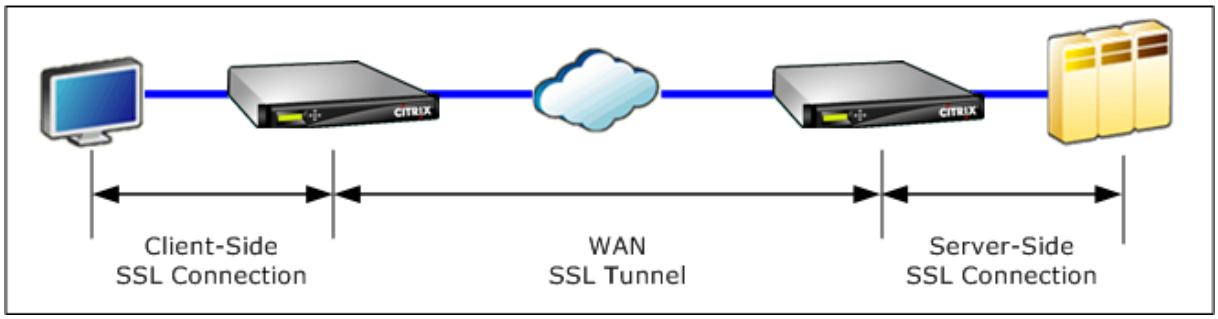
> **Remarque**
>
> La compression SSL nécessite une connexion sécurisée d'appairage (signalisation) entre les deux appliances aux extrémités de la liaison accélérée.

Le chiffrement est maintenu de bout en bout en divisant la connexion en trois segments chiffrés : l'appliance client à côté client, l'appliance côté client à côté serveur et l'appliance côté serveur à serveur.

Ordinary SSL Connection



Accelerated SSL Connection



Attention : La compression SSL déchiffre le flux de données chiffré et, à moins que l'option User Data Encryption soit utilisée, les historiques de compression des deux unités d'accélération conservent les enregistrements en texte clair des données déchiffrées. Vérifiez que votre déploiement et vos paramètres sont cohérents avec les stratégies de sécurité de votre organisation. Citrix vous recommande d'activer le chiffrement de l'historique de compression sur chaque unité lorsque vous configurez la connexion de signalisation d'appairage sécurisée requise pour l'accélération SSL.

> **Remarque**
>
> - Lorsque vous activez la compression SSL, l'appliance cesse de tenter de compression avec d'autres appliances avec lesquelles elle n'a pas de relation homologue sécurisée (qu'il s'agisse de Citrix SD-WAN WANOP ou de Citrix SD-WAN WANOP Plug-in). Cette fonctionnalité est donc la mieux adaptée aux réseaux où toutes les appliances sont configurées pour la compression SSL.
> - Lorsque la compression SSL est activée, vous devez saisir manuellement le mot de passe du magasin de clés chaque fois que l'appliance est redémarrée.

Fonctionnement de la compression SSL

April 9, 2021

La compression SSL a accès aux données en texte clair de la connexion, car l'appliance côté serveur agit en tant que *délégué de sécurité* des serveurs de point de terminaison. Ce comportement est possible car l'appliance côté serveur est configurée avec des copies des informations d'identification de sécurité des serveurs (clés privées et certificats), ce qui lui permet d'agir au nom des serveurs. Pour le client, ce comportement équivaut à communiquer directement avec le serveur de point de terminaison.

Étant donné que l'appliance fonctionne en tant que délégué de sécurité du serveur, la plupart des configurations se trouvent sur l'appliance côté serveur. L'appliance côté client (ou plug-in) agit comme un satellite de l'appliance côté serveur et ne nécessite pas de configuration par serveur.

Les appliances côté serveur et côté client partagent l'état de session via une *connexion de signalisation SSL.* Toutes les connexions accélérées entre les deux appliances sont envoyées via *des connexions de données SSL,* que les connexions d'origine aient été chiffrées ou non.

Remarque : la compression SSL ne crypte pas nécessairement tout le trafic de liaison. Le trafic initialement chiffré reste chiffré, mais le trafic non chiffré n'est pas toujours chiffré. Les appliances ne tentent pas de chiffrer le trafic non accéléré. Étant donné qu'il n'y a pas de garantie absolue que toute connexion donnée sera accélérée (divers événements empêchent l'accélération), il n'y a aucune garantie que les appliances chiffreront une connexion non chiffrée donnée.

La compression SSL fonctionne dans l'un des deux modes : proxy transparent ou proxy split. Ces deux modes prennent en charge des fonctionnalités SSL légèrement différentes. Vous sélectionnez le mode qui fournit les fonctionnalités requises par une application donnée.

Quel mode proxy SSL utiliser : utilisezle mode proxy transparent SSL *uniquement*si vous avez besoin d'une véritable authentification client (c'est-à-dire une authentification qui identifie correctement le client de point de terminaison individuel) *et*que vous n'avez pas besoin de tickets Diffie-Hellman, Temp RSA, TLS SSL version 2, ou renégociation de session. Utilisez SSL split proxy pour tous les autres déploiements.

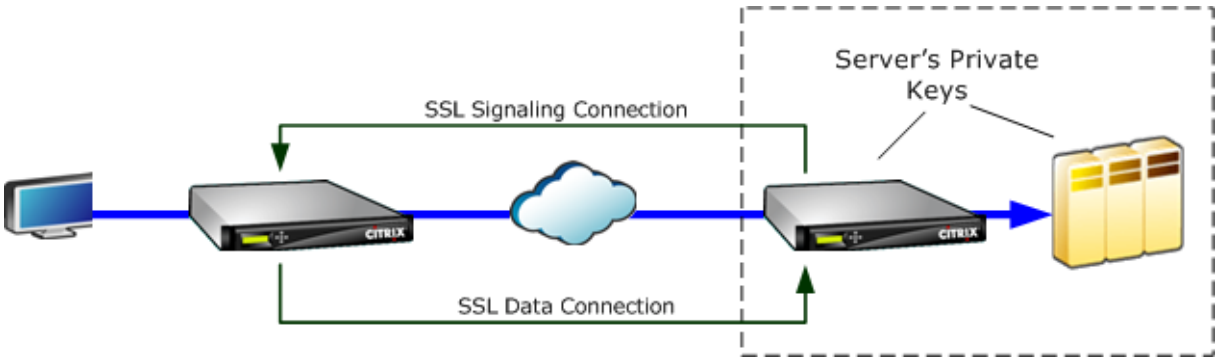
Proxy transparent SSL

En *mode proxy transparent SSL* (à ne pas confondre avec le mode transparent sur le plug-in Citrix SD-WAN WANOP), l'appliance côté serveur se fait passer pour le serveur. Les informations d'identification du serveur (paire de clés de certificat) sont installées sur l'appliance côté serveur afin qu'elle puisse agir au nom du serveur. L'appliance côté serveur configure ensuite l'appliance côté client pour qu'elle gère l'extrémité client de la connexion. Les informations d'identification du serveur ne sont pas installées sur l'appliance côté client.

L'authentification réelle du client est prise en charge dans ce mode, mais Temp RSA et Diffie-Hellman ne le sont pas. Le mode proxy transparent SSL est adapté aux applications nécessitant une authentification client, mais uniquement si aucune des fonctionnalités suivantes n'est requise : Diffie-Hellman,

Temp RSA, tickets de session TLS, SSL version 2. En outre, la renégociation de session ne doit pas être tentée, sinon la connexion se termine.

Aucune configuration n'est requise sur l'appliance côté client (autre que la configuration d'une relation d'appairage sécurisée avec l'appliance côté serveur) et aucune configuration n'est requise sur le client, ce qui traite la connexion exactement comme si elle communiquait directement avec le serveur.



Proxy de partage SSL

Le*mode proxy partagé SSL* est préféré dans la plupart des cas, car il prend en charge Temp RSA et Diffie-Hellman, ce dont de nombreuses applications ont besoin. En mode proxy partagé SSL, l'appliance côté serveur se cache comme un serveur sur le client et comme un client sur le serveur. Vous installez les informations d'identification du serveur (une paire de clés de certificat) sur l'appliance côté serveur pour lui permettre d'agir au nom du serveur.

Le mode proxy fractionné prend également en charge l'authentification client par proxy si vous installez des informations d'identification client facultatives, qui sont présentées à l'application du serveur de point de terminaison si elle demande l'authentification client. Ces informations d'identification du client seront présentées à la place des informations d'identification du client du point de terminaison réel. (Utilisez un proxy transparent si les informations d'identification du client de point de terminaison sont requises par l'application.)

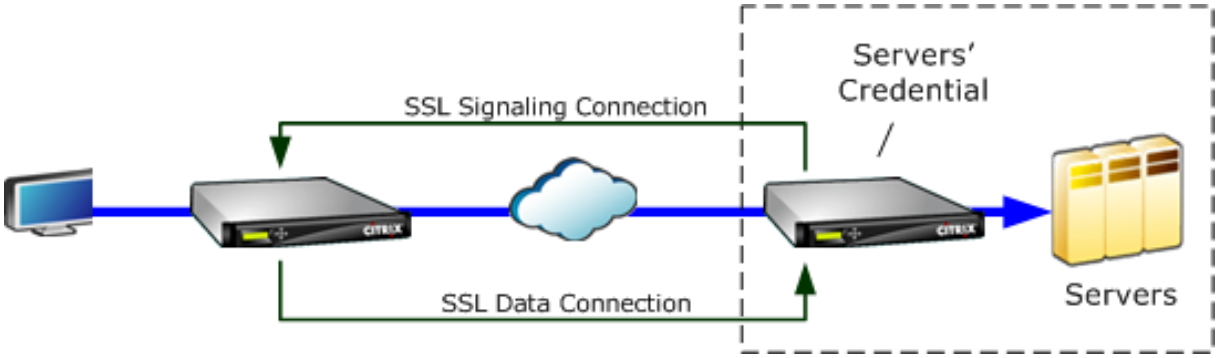
Étant donné que l'authentification vraie du client n'est pas prise en charge dans ce mode, le serveur ne peut pas authentifier le client de point de terminaison réel. Si l'appliance côté serveur n'est pas configurée avec des informations d'identification client, toutes les tentatives de l'application côté serveur lors de l'authentification client échouent. Si l'appliance côté serveur est configurée avec des informations d'identification client, toutes les demandes d'authentification client recevront ces informations d'identification, quelle que soit l'identité du client réel.

Aucune configuration n'est requise sur l'appliance côté client (autre que la configuration d'une relation d'appairage sécurisée avec l'appliance côté serveur) et aucune configuration n'est requise sur le client, ce qui traite la connexion comme si elle communiquait directement avec le serveur. Les infor-

mations d'identification du serveur sur l'appliance côté serveur ne sont pas installées sur l'appliance côté client.

Pour prendre en charge plusieurs serveurs, plusieurs paires de clés de certificat privées peuvent être installées sur l'appliance, une par profil SSL. Les règles SSL spéciales dans les définitions de classe de service correspondent aux serveurs aux profils SSL, et donc aux profils SSL aux informations d'identification.

En mode proxy partagé SSL, les certificats d'autorité de certification et les paires de clés de certificat et les certificats d'autorité de certification ne doivent pas correspondre à ceux des serveurs, bien qu'ils le puissent. En raison de la nature d'un proxy fractionné, l'appliance côté serveur peut utiliser des informations d'identification acceptables pour l'application cliente (informations d'identification valides délivrées par une autorité de confiance). Notez que, dans le cas des connexions HTTPS, les navigateurs Web émettent un avertissement si le nom commun ne correspond pas au nom de domaine dans l'URL. En général, l'utilisation de copies des informations d'identification du serveur est l'option la plus facile.



Configurer la compression SSL

April 23, 2021

La fonction de compression SD-WAN WO SSL de Citrix permet la compression multisession des connexions SSL (par exemple, trafic HTTPS), fournissant des rapports de compression allant jusqu'à 10 000:1. Pour de plus amples informations, consultez la section Compression SSL.

Pour que la compression SSL fonctionne, l'appliance Citrix SD-WAN WANOP a besoin de certificats provenant du serveur ou du client. Pour prendre en charge plusieurs serveurs, plusieurs clés privées peuvent être installées sur l'appliance, une par profil SSL. Les règles SSL spéciales dans les définitions de classe de service correspondent aux serveurs aux profils SSL, et donc aux profils SSL aux clés privées.

La compression SSL fonctionne en mode proxy divisé ou proxy transparent, vous pouvez choisir le

mode selon vos besoins. Pour de plus amples informations, consultez la section Fonctionnement de la compression SSL.

> **Remarque**
>
> Le mode proxy transparent n'est actuellement pas pris en charge.

Pour activer l'accès sécurisé avec le tunnel SSL, le dernier protocole SSL TLS 1.2 est utilisé dans le proxy SSL. Vous pouvez choisir d'utiliser le protocole TLS1.2 uniquement ou d'utiliser les protocoles TLS1.0, TLS1.1 et TLS1.2.

> **Remarque**
>
> Les protocoles SSL SSL v3 et SSL v2 ne sont plus pris en charge.

Pour configurer la compression SSL :

1. Acquérez des copies du certificat d'autorité de certification et de la paire de clés de certificat privées de votre serveur et installez-les sur l'appliance côté serveur. Ces informations d'identification sont susceptibles d'être spécifiques à l'application. Autrement dit, un serveur peut avoir des informations d'identification différentes pour un serveur Web Apache que pour un Exchange Server exécutant RPC sur HTTPS.
2. Vous pouvez choisir de créer un profil SSL proxy fractionné ou un profil SSL proxy transparent.

   Pour plus d'informations sur la configuration du profil SSL de proxy **partagé, consultez la section Configuration d'un profil SSL de proxy partagé** ci-dessous.

   Pour plus d'informations sur la configuration du profil SSL de proxy **transparent, consultez la section Configuration du profil SSL de proxy transparent** ci-dessous.

   > **Remarque**
   >
   > Le profil SSL proxy transparent n'est actuellement pas pris en charge.

3. Attachez le profil SSL à une classe de service sur l'appliance côté serveur. Cela peut être fait en créant une nouvelle classe de service basée sur l'adresse IP du serveur, ou en modifiant une classe de service existante.

   Pour plus d'informations, consultez la section **Création ou modification de la classe de service** ci-dessous.
4. Définissez des classes de service sur l'appliance côté client. Le trafic SSL n'est pas compressé à moins qu'il ne tombe dans une classe de service, sur l'appliance côté client, qui permet l'accélération et la compression. Il peut s'agir d'une règle de classe de service ordinaire, pas d'une règle SSL (seule l'appliance côté serveur a besoin de règles SSL), mais elle doit activer l'accélération et la compression. Le trafic appartient à une classe de service existante, telle

que « HTTPS » ou « Autre trafic TCP ». Si la stratégie de cette classe permet l'accélération et la compression, aucune configuration supplémentaire n'est nécessaire.

5. Vérifiez le fonctionnement de la règle. Envoyez du trafic qui devrait recevoir une accélération SSL via les appliances. Sur l'appliance côté serveur, sous l'onglet Surveillance : Optimisation : Connexions : Connexions accélérées, la colonne Classe de service doit correspondre à la classe de service que vous avez configurée pour l'accélération sécurisée, et la colonne Proxy SSL doit indiquer True pour les connexions appropriées.

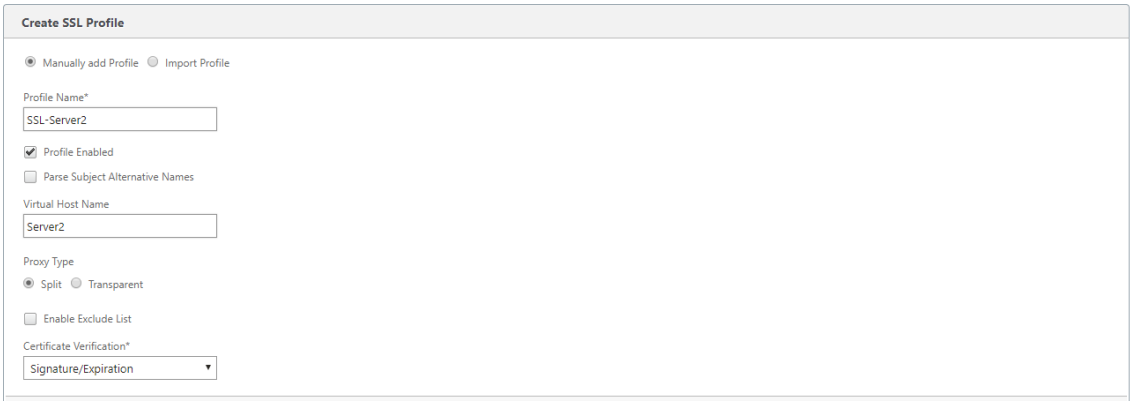
Configurer un profil SSL proxy fractionné

Pour configurer un profil SSL proxy fractionné :

1. Dans l'appliance Citrix SD-WAN WO côté serveur, accédez à **Configuration** > **Accélération sécurisée** > **Profil SSL**, puis cliquez sur **Ajouter un profil**.

   > **Remarque**
   >
   > Vous pouvez ajouter manuellement un profil SSL ou en importer un qui est stocké sur votre ordinateur local.

2. Dans le champ **Nom du profil**, entrez un nom pour le profil SSL et sélectionnez **Profil activé**.
3. Si votre serveur SSL utilise plusieurs noms d'hôte virtuel, entrez le **nom d'hôte virtuel** cible dans le champ Nom d'hôte virtuel. Il s'agit du nom d'hôte répertorié dans les informations d'identification du serveur.



   > **Remarque**
   >
   > Pour prendre en charge plusieurs hôtes virtuels, créez un profil SSL distinct pour chaque nom d'hôte.

4. Choisissez **Fractionner** le type de proxy.
5. Dans le champ **Vérification du certificat**, conservez la valeur par défaut (Signature/Expiration) à moins que vos stratégies n'en dictent autrement.

6. Effectuer la configuration du proxy côté serveur :

   Dans le champ **Magasin de vérification**, sélectionnez une autorité de certification de serveur existante ou cliquez sur **+** pour charger une autorité de certification de serveur.

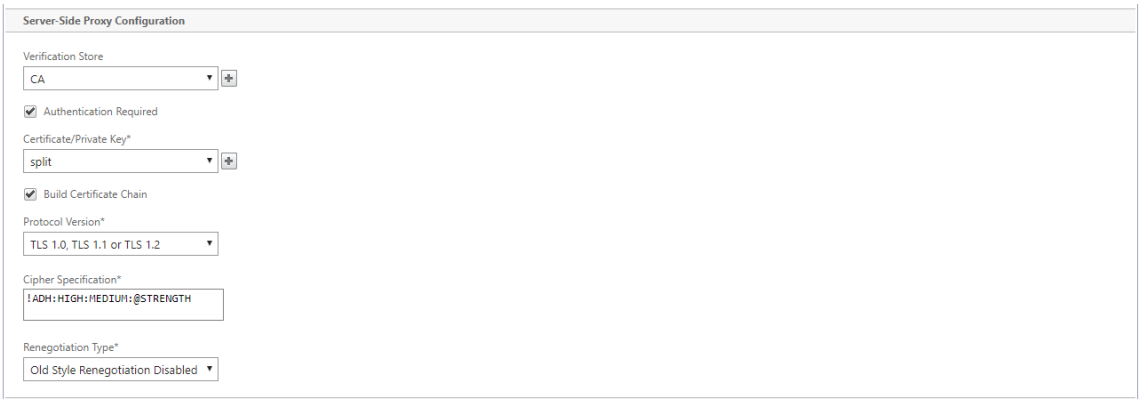
   Choisissez **Authentification requise** et, dans le champ **Certificat/clé privée**, sélectionnez une paire de clés de certificat, ou cliquez sur **+** pour télécharger une paire de clés de certificat.

   Dans le champ **Version du protocole**, sélectionnez les protocoles acceptés par votre serveur.

   > **Remarque**
   >
   > Citrix SD-WAN WO prend en charge une combinaison de **TLS1.0, TLS1.1 ou TLS1.2**ou **TLS1.2** uniquement**.** Les protocoles SSL SSLv3 et SSLv2 ne sont pas pris en charge.

   Si nécessaire, modifiez la chaîne de **spécification de chiffrement** en utilisant la syntaxe OpenSSL.

   Si nécessaire, sélectionnez le type de renégociation dans la liste déroulante **Type de renégociation** pour autoriser la renégociation de session SSL côté client.



7. Effectuer la configuration du proxy côté client :

   Dans le champ **Certificat/clé privée**, conservez la valeur par défaut.

   Choisissez **Construire une chaîne de certificats** pour permettre à l'appliance côté serveur de créer la chaîne de certificats SSL.

   Si nécessaire, sélectionnez ou téléchargez un magasin d'autorité de certification à utiliser comme magasin de chaînes de certificats.

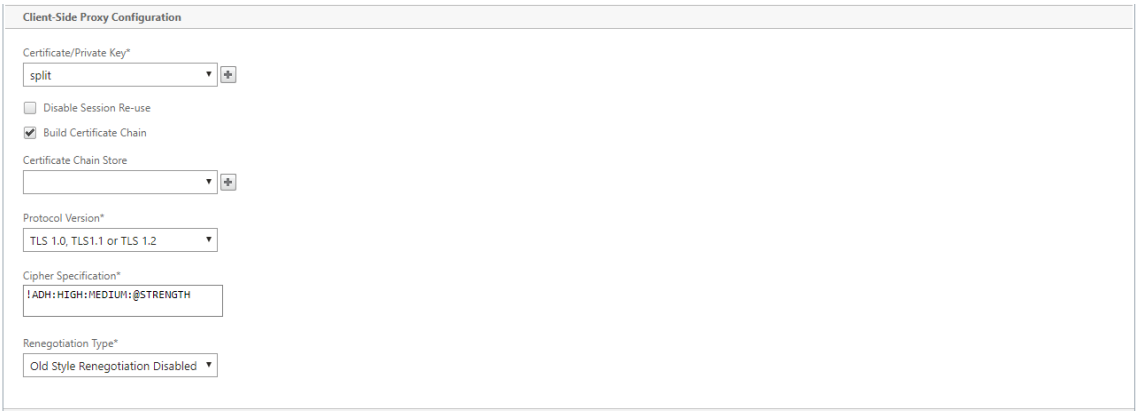
   Dans le champ **Version du protocole**, sélectionnez les versions de protocole que vous souhaitez prendre en charge du côté client.

   > **Remarque**

> Citrix SD-WAN WO prend en charge une combinaison de **TLS1.0, TLS1.1 ou TLS1.2**ou **TLS1.2** uniquement**.** Les protocoles SSL SSLv3 et SSLv2 ne sont pas pris en charge.

Si nécessaire, modifiez la spécification de chiffrement côté client.

Si nécessaire, sélectionnez le type de renégociation dans la liste déroulante **Type de renégociation** pour autoriser la renégociation de session SSL côté client.



8. Cliquez sur **Créer**.

Configurer le profil SSL proxy transparent

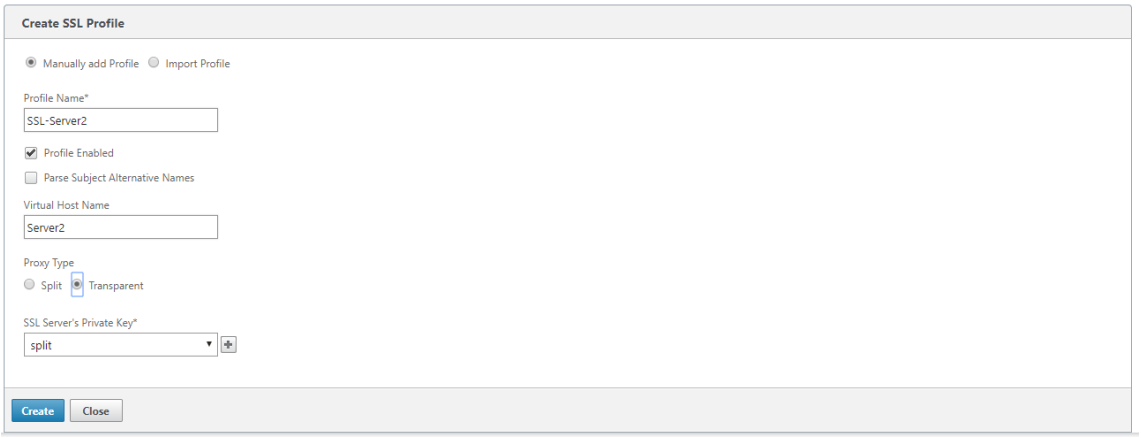
Pour configurer un profil SSL proxy transparent :

1. Dans l'appliance Citrix SD-WAN WO côté serveur, accédez à **Configuration** > **Accélération sécurisée** > **Profil SSL**, puis cliquez sur **Ajouter un profil**.

   > **Remarque**
   >
   > Vous pouvez ajouter manuellement un profil SSL ou en importer un qui est stocké sur votre ordinateur local.

2. Dans le champ **Nom du profil**, entrez un nom pour le profil SSL et sélectionnez **Profil activé**.
3. Si votre serveur SSL utilise plusieurs noms d'hôte virtuel, entrez le **nom d'hôte virtuel** cible dans le champ Nom d'hôte virtuel. Il s'agit du nom d'hôte répertorié dans les informations d'identification du serveur.

   > **Remarque**
   >
   > Pour prendre en charge plusieurs hôtes virtuels, créez un profil SSL distinct pour chaque nom d'hôte.



4. Choisissez Type de proxy **transparent**.
5. Dans le champ **Clé privée du serveur SSL**, sélectionnez la clé privée du serveur dans le menu déroulant ou cliquez sur **+** pour télécharger une nouvelle clé privée.
6. Cliquez sur **Créer**.

Créer ou modifier la classe de service

Pour créer ou modifier la classe de service et attacher le profil SSL :

1. Dans l'interface Web de l'appliance Citrix SD-WAN WO, accédez à **Configuration > Règles d'optimisation > Classes de service**, puis cliquez sur **Ajouter**. Pour modifier une classe de service existante, sélectionnez la classe de service appropriée et cliquez sur **Modifier**.
2. Dans le champ Nom, entrez un nom pour la nouvelle classe de service (par exemple, « HTTPS accéléré »).
3. Activez la compression en définissant la stratégie d'accélération **sur Disk**, **Memory**ou **Flow Control**.
4. Dans la section **Règles de filtrage**, cliquez sur **Ajouter**.
5. Dans le **champ Adresse IP de destination**, tapez l'adresse IP du serveur (par exemple, 172.16.0.1 ou, de manière équivalente, 172.16.0.1/32.
6. Dans le champ **Direction**, définissez la règle sur Unidirectional. Les profils SSL sont désactivés si Bidirectionnel est spécifié.
7. Dans la section **Profils SSL**, sélectionnez le profil SSL que vous avez créé et déplacez-le vers la section **Configuré**.
8. Cliquez sur **Créer** pour créer la règle.
9. Cliquez sur **Créer** pour créer la classe de service.

Commande CLI mise à jour

Citrix SD-WAN WO 9.3 prend en charge le dernier protocole SSL TLS1.2. Vous pouvez choisir d'utiliser le protocole TLS1.2 uniquement ou n'importe quelle version des protocoles TLS. Les protocoles SSL SSL v3 et SSL v2, et les profils SSL proxy transparents ne sont pas pris en charge. Les commandes **add ssl-profile** et **set ssl-profile** CLI sont mises à jour pour refléter ces modifications.

add ssl-profile:

```
*-name " profile-name " *

*\[-state {
 enable, disable }
 \]*

*-proxy-type split*

*\[-virtual-hostname " hostname " \]*

*-cert-key " cert-key-pair-name " *

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores, " store-name " }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*

*\[-verification-store {
 use-all-configured-CA-stores, " store-name " }
 \]*

*\[-server-side-protocol {
  TLS-1.2, TLS-version-any }
 \]*

*\[-server-side-ciphers " ciphers " \]*

*\[-server-side-authentication {
 enable, disable }
 \]*

*\[-server-side-cert-key " cert-key-pair-name " \]*

*\[-server-side-build-cert-chain {
```



```
 enable, disable }
 \]*

*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*

*\[-client-side-protocol-version {
  TLS-1.2, TLS-version-any }
 \]*

*\[-client-side-ciphers  " ciphers " \]*

*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*

*compatible }
 \]*
```

set ssl-profile:

```
*-name  " profile-name "  \[-state {
 enable, disable }
 \]*

*\[-proxy-type split\]*

*\[-virtual-hostname  " hostname " \]*

*\[-cert-key  " cert-key-pair-name " \]*

*\[-build-cert-chain {
 enable, disable }
 \]*

*\[-cert-chain-store {
 use-all-configured-CA-stores,  " store-name "  }
 \]*

*\[-cert-verification {
 none, Signature/Expiration, Signature/Expiration/*

*Common-Name-White-List, Signature/Expiration/Common-Name-Black-List }
 \]*

*\[-verification-store {
 use-all-configured-CA-stores,  " store-name "  }
 \]*

*\[-server-side-protocol {
 TLS-1.2, TLS-version-any }
```



```
 \]*
*\[-server-side-ciphers  " ciphers " \]*
*\[-server-side-authentication {
 enable, disable }
 \]*
*\[-server-side-cert-key  " cert-key-pair-name " \]*
*\[-server-side-build-cert-chain {
 enable, disable }
 \]*
*\[-server-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*
*compatible }
 \]*
*\[-client-side-protocol-version {
 TLS-1.2, TLS-version-any }
 \]*
*\[-client-side-ciphers  " ciphers " \]*
*\[-client-side-renegotiation {
 disable-old-style, enable-old-style, new-style,*
*compatible }
 \]*
```

Compression SSL avec le plug-in Citrix SD-WAN WANOP

April 9, 2021

Le plug-in Citrix SD-WAN WANOP est toujours utilisé comme unité côté client et ne nécessite donc aucune configuration SSL supplémentaire autre que l'installation des informations d'identification pour la connexion de signalisation SSL (appairage sécurisé). La principale différence entre la compression SSL sur le plug-in et l'appliance est que le plug-in n'est pas en mesure de chiffrer les données utilisateur dans l'historique de compression sur disque.

Attention : Étant donné que l'historique de compression sur disque du plug-in n'est pas chiffré, il conserve un enregistrement en texte clair des communications cryptées potentiellement sensibles et éphémères. Ce manque de chiffrement est potentiellement dangereux sur les ordinateurs pour lesquels l'accès physique n'est pas contrôlé. Par conséquent, Citrix recommande les meilleures pratiques suivantes :

- N'utilisez pas la **validation de certificat : aucune** sur vos appliances. (Notez que, dans ce cas, l'appliance refuse d'autoriser la compression avec des plug-ins qui ne disposent pas de certificats appropriés.)
- Installez les certificats uniquement sur les systèmes qui peuvent être vérifiés pour répondre aux exigences de votre organisation en matière de sécurité physique ou de sécurité des données (par exemple, les ordinateurs portables qui utilisent le chiffrement de disque intégral).

Le plug-in Citrix SD-WAN WANOP prend en charge le proxy séparé SSL et le proxy transparent SSL. Le plug-in est livré sans paires de clés de certificat pour la connexion de signalisation SSL. Si vous le souhaitez, les mêmes informations d'identification peuvent être utilisées par tous les plug-ins, ou chaque plug-in peut avoir ses propres informations d'identification.

Le plug-in ne tente pas de compression SSL sauf si les informations d'identification ont été installées.

Le plug-in hérite de sa licence de crypto de l'appliance.

RPC sur HTTP

April 23, 2021

Microsoft Exchange Server est l'un des serveurs de messagerie couramment utilisés dans les organisations. Grâce aux récentes améliorations apportées à Microsoft Exchange Server, vous pouvez vous y connecter en toute sécurité via Internet. Selon la bande passante disponible, vous pouvez rencontrer une latence dans le courrier électronique remis au client Outlook. Outre le protocole MAPI, l'appliance Citrix SD-WAN WANOP prend en charge l'appel de procédure distante sur HTTPS (RPC sur HTTPS) afin d'optimiser le trafic Microsoft Exchange. Cette fonctionnalité est également appelée Outlook Anywhere.

RPC sur HTTPS n'est pas un nouveau protocole, mais à partir de Microsoft Exchange 2013, il remplace MAPI comme protocole par défaut. Le principal avantage de RPC sur HTTPS est qu'il permet aux clients de se connecter en toute sécurité au serveur de messagerie via Internet.

Lorsque vous utilisez RPC sur HTTPS, le serveur Microsoft Exchange doit utiliser un certificat numérique et une clé privée pour s'authentifier auprès du client Outlook. La communication entre le client et le serveur utilise HTTPS comme protocole de transport.

Sur le dispositif Citrix SD-WAN WANOP, RPC sur HTTPS est pris en charge pour les versions suivantes de Microsoft Outlook et Exchange Server :

- Microsoft Outlook
  - Microsoft Outlook version 2007

  - Microsoft Outlook version 2010
  - Microsoft Outlook version 2013
- Microsoft Exchange Server
  - Microsoft Exchange Server version 2007
  - Microsoft Exchange Server version 2010
  - Microsoft Exchange Server version 2013

Parmi ceux-ci, toutes les versions à l'exception de Microsoft Exchange Server 2013 prennent en charge MAPI (sur TCP) ainsi que RPC sur HTTPS. Toutefois, Microsoft Exchange Server 2013 force les connexions à utiliser RPC sur HTTPS, quelle que soit la version de Microsoft Outlook que vous utilisez, pour se connecter au serveur Exchange.

Configurer RPC sur HTTPS

Par défaut, la fonctionnalité RPC sur HTTPS est activée sur l'appliance. Toutefois, pour configurer l'appliance de manière à accélérer RPC sur HTTPS, vous devez effectuer les tâches supplémentaires suivantes :

- Configurez MAPI chiffrée.
- Configurez un profil SSL avec un certificat de serveur.
- Créez une classe de service RPC sur HTTPS et liez le profil SSL à elle.

Configurer MAPI cryptée

> **Remarque**
>
> Ignorez cette section si vous avez déjà configuré l'accélération MAPI chiffrée sur l'appliance.

Microsoft Outlook utilise des connexions MAPI (Messaging Application Programming Interface) entre les clients Outlook et le serveur Microsoft Exchange. Les connexions MAPI utilisent des RPC, qui sont encapsulés par une connexion HTTP. Par conséquent, avant de configurer RPC sur HTTPS sur une appliance Citrix SD-WAN WANOP, vous devez configurer MAPI chiffrée sur l'appliance.

Prérequis :

Avant de configurer MAPI chiffrée, assurez-vous que les conditions préalables suivantes sont remplies :

- L'option Secure Peer doit être définie sur True sur le client ainsi que sur l'appliance côté serveur. Pour configurer un partenaire sécurisé, reportez-vous à la section Peering sécurisé.

- L'adresse IP DNS configurée sur l'appliance côté serveur doit être accessible.
- L'appliance côté centre de données doit joindre le domaine avec succès.
- Un utilisateur délégué doit être ajouté à l'appliance côté centre de données et son état doit être marqué comme « Succès ».

Pour de plus amples informations, consultez la section Configurer une appliance Citrix SD-WAN WANOP pour optimiser la sécurité du trafic Windows.

Configurer un profil SSL avec un certificat de serveur

La connexion HTTPS qui encapsule la connexion MAPI est sécurisée par SSL. Par conséquent, RPC sur HTTPS nécessite une connectivité via le port TCP 443. Ce port est affecté à HTTPS, que les administrateurs de serveurs Web gardent généralement ouverts dans l'application pare-feu. L'utilisation de la communication protégée par SSL aide RPC sur HTTPS à maintenir la sécurité de toutes les communications.

Pour activer l'accélération RPC sur HTTPS, vous devez installer un certificat de serveur sur l'appliance. À l'aide de ce certificat de serveur, vous pouvez configurer un profil SSL utilisé par RPC sur HTTPS pour une communication sécurisée. Pour configurer un profil SSL avec un certificat de serveur Exchange, reportez-vous à la section Installation de certificats de serveur et de client.

> **Remarque**
>
> Vous devez configurer un profil SSL uniquement sur l'appliance côté centre de données.

Créer une classe de service RPC sur HTTPS et lier le profil SSL à elle

Pour optimiser les connexions RPC sur HTTP, vous devez créer une classe de service qui répertorie HTTPS et toutes les applications MAPI. Vous devez fournir l'adresse IP du serveur Microsoft Exchange en tant qu'adresse IP de destination pour cette classe de services, puis lier le profil SSL que vous avez créé à cette classe de services. La liaison du profil à la classe de service garantit que la communication entre le client Outlook et le serveur Microsoft Exchange est sécurisée à l'aide de ce profil.

> **Remarque**
>
> Vous devez configurer et lier un profil SSL à la classe de service uniquement sur l'appliance côté centre de données.

Vérifier les connexions RPC accélérées sur HTTPS

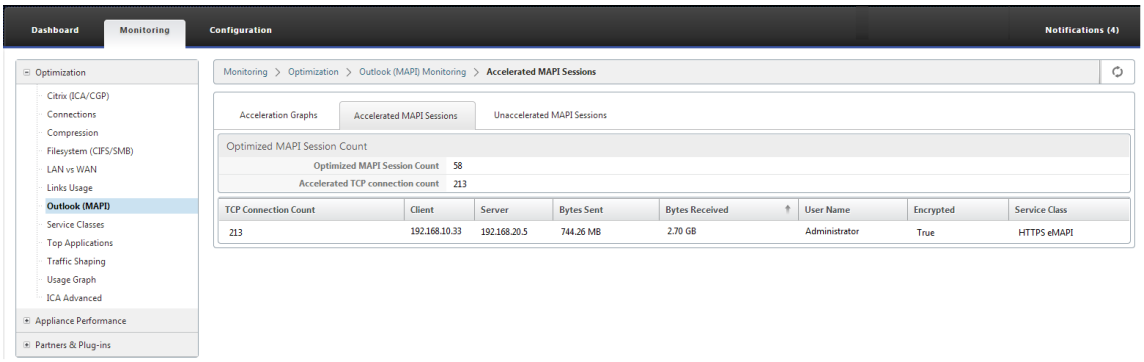
Une fois que vous avez configuré RPC sur HTTPS sur l'appliance, vous pouvez vérifier que l'appliance accélère la connexion RPC sur HTTPS sur la page Surveillance pour MAPI. Les connexions RPC

accélérées sur HTTPS sont répertoriées dans l'onglet Sessions MAPI accélérées.

> **Remarque**
>
> Vous devez configurer RPC sur HTTPS sur vos appliances côté client ainsi que vos appliances Citrix SD-WAN WANOP côté serveur pour accélérer les connexions RPC sur HTTPS.

Pour vérifier que les connexions RPC sur HTTPS sont accélérées

1. Accédez à **Surveillance** > **Optimisation** > **Outlook (MAPI)**.
2. Sous l'onglet **Sessions MAPI accélérées**, vérifiez que les connexions RPC sur HTTPS sont accélérées.



> **Remarque**
>
> L'application a des valeurs possibles de : HTTPS eMAPI, HTTP eMAPI, HTTPS MAPI et HTTP MAPI.

Accélération TCP Flow Control

April 9, 2021

Les réseaux WAN ordinaires ont une très faible réactivité à l'utilisation des liaisons élevées et à de longues distances. Une règle de base largement utilisée pour les liaisons WAN ordinaires non accélérées est : « une fois que l'utilisation des liaisons atteint 40%, il est temps d'ajouter plus de bande passante, car les performances et la fiabilité se sont dégradées au point où la liaison est largement inutilisable. » Les performances interactives en pâtissent, ce qui rend difficile l'exécution du travail et les connexions sont souvent interactives. Les liens accélérés n'ont pas ce problème. Un lien avec une utilisation de 95 % reste parfaitement utilisable.

Les appliances Citrix SD-WAN WANOP deviennent des passerelles virtuelles qui contrôlent le trafic TCP sur la liaison WAN. Le protocole TCP ordinaire est contrôlé par connexion par les périphériques de point de terminaison. Le contrôle optimal du trafic de liaison est difficile, car ni les terminaux ni

les connexions individuelles n'ont une connaissance de la vitesse de liaison ni de la quantité de trafic concurrent. Une Gateway, en revanche, est dans une position idéale pour surveiller et contrôler le trafic des liaisons. Les passerelles ordinaires gâchent cette opportunité parce qu'elles ne peuvent pas fournir le contrôle de flux qui manque à TCP. La technologie Citrix SD-WAN WANOP ajoute l'intelligence manquante dans l'équipement réseau et les connexions TCP. Il en résulte une amélioration considérable des performances WAN, même dans des conditions difficiles telles que des pertes élevées ou une distance extrême.

Le contrôle de flux Citrix SD-WAN WANOP est transparent et sans perte, et il implémente un large spectre d'optimisations de vitesse. Aucune configuration n'est requise en raison de la découverte automatique et de la configuration automatique. Vous devrez peut-être modifier vos pare-feu s'ils bloquent les options TCP utilisées par les algorithmes d'accélération.

Contrôle du flux transparent et sans perte

April 9, 2021

L'accélération fonctionne sur n'importe quelle connexion TCP passant par deux appliances (l'une sur le site d'envoi et l'autre sur le site de réception), ou une appliance Citrix SD-WAN WANOP et un plug-in Citrix SD-WAN WANOP. Bien que la figure ci-dessus montre un réseau de deux appliances, n'importe quelle appliance peut accélérer les connexions entre un nombre quelconque d'autres sites équipés d'appareils simultanément. Cela permet d'utiliser une appliance unique par site, plutôt que deux par lien.

Comme toute Gateway, l'appliance Citrix SD-WAN WANOP compte les paquets sur la liaison. Contrairement aux passerelles ordinaires, cependant, il impose un contrôle de flux transparent et sans perte sur chaque segment de liaison, y compris :

- Segment LAN entre l'expéditeur et l'appliance émettrice
- Segment WAN entre les appliances d'envoi et de réception
- Segment LAN entre l'appliance de réception et le récepteur

Le contrôle de débit peut être géré indépendamment pour chacun de ces trois segments. Les segments sont partiellement découplés, de sorte que chacun peut avoir sa vitesse contrôlée indépendamment. Ceci est important lorsque la vitesse d'une connexion doit être augmentée ou abaissée rapidement jusqu'à sa juste part de bande passante, et est également important pour prendre en charge les algorithmes WAN et la compression améliorés.

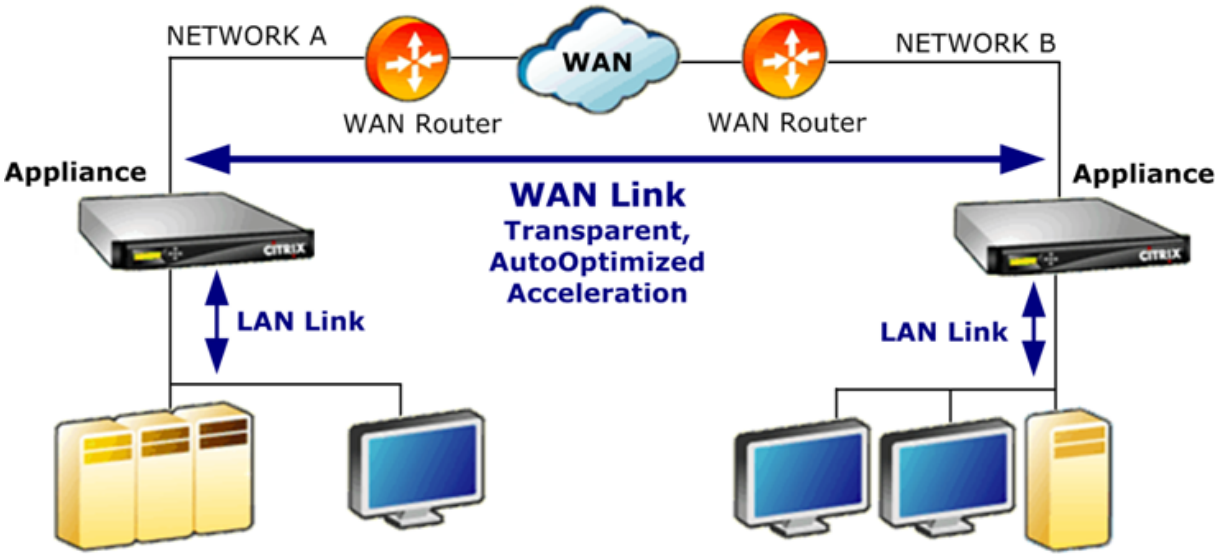
Le protocole TCP est conçu pour que chaque connexion TCP tente d'augmenter continuellement son utilisation de bande passante. Cependant, la bande passante du lien est limitée. Le résultat est que

les liens deviennent dépassés. Le contrôle de flux Citrix SD-WAN WANOP permet aux connexions TCP de circuler à la bonne vitesse. Le lien est rempli mais n'est jamais dépassé, de sorte que la latence de la file d'attente et les pertes de paquets sont minimisées, tandis que le débit est maximisé.

Avec TCP ordinaire, les connexions à long terme (qui ont eu le temps de saisir toute la bande passante) ont tendance à extraire les connexions à court terme. Ce problème, qui ruine la réactivité interactive, ne se produit pas avec le contrôle de flux.

Le contrôle de flux est une fonctionnalité standard sur toutes les appliances de la famille Citrix SD-WAN WANOP.

Figure 1. Accélération améliore les performances de manière transparente



Optimisation de la vitesse

April 9, 2021

La plupart des implémentations TCP ne fonctionnent pas bien sur les liaisons WAN. Pour ne nommer que deux problèmes, les algorithmes de retransmission TCP standard (Selective Accusés de réception et TCP Fast Recovery) sont inadéquats pour les liaisons avec des taux de perte élevés et ne tiennent pas compte des besoins des connexions transactionnelles de courte durée.

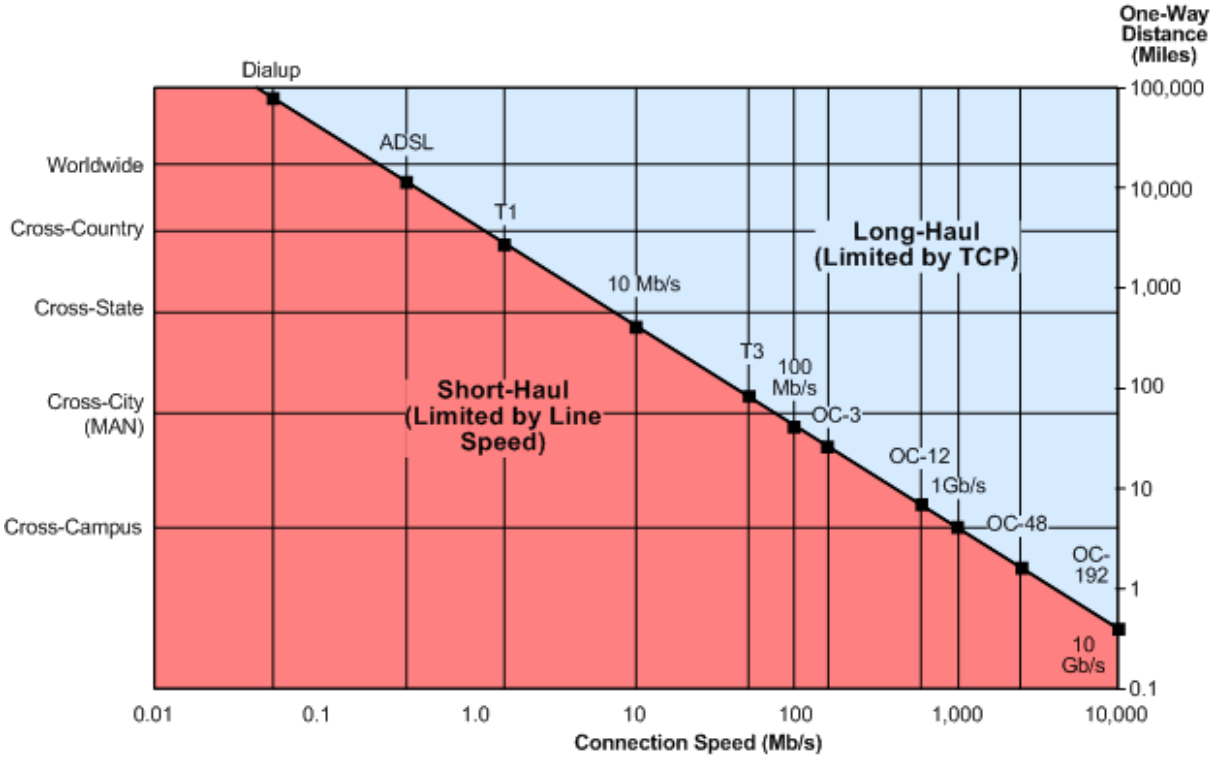
Citrix SD-WAN WANOP implémente un large éventail d'optimisations WAN pour garder les données circulant dans toutes sortes de conditions défavorables. Ces optimisations fonctionnent de manière transparente pour garantir que les données arrivent à leur destination le plus rapidement possible.

L'optimisation WAN fonctionne de manière transparente et ne nécessite aucune configuration.

L'optimisation WAN est une fonctionnalité standard sur toutes les appliances Citrix SD-WAN WANOP.

La figure ci-dessous montre les vitesses de transfert possibles à différentes distances, sans accélération, lorsque les terminaux utilisent TCP standard (TCP Reno). Par exemple, les débits gigabits sont possibles sans accélération dans un rayon de quelques miles, 100 Mbit/s est atteignable à moins de 100 miles et le débit sur une connexion mondiale est limité à moins de 1 Mbit/s, quelle que soit la vitesse réelle de la liaison. Avec l'accélération, cependant, les vitesses au-dessus de la ligne diagonale deviennent disponibles pour les applications. La distance n'est plus un facteur limitatif.

Figure 1. Les performances TCP non accélérées chutent avec la distance



> **Remarque**
>
> Sans l'accélération Citrix, le débit TCP est inversement proportionnel à la distance, ce qui rend impossible l'extraction de la bande passante complète des liaisons longue distance et haute vitesse. Avec l'accélération, le facteur de distance disparaît, et la pleine vitesse d'une liaison peut être utilisée à n'importe quelle distance. (Graphique basé sur le modèle de Mathis, *et coll.,* Pittsburgh Supercomputer Center.)

Les performances de transfert accélérées sont approximativement égales à la bande passante de la liaison. La vitesse de transfert est non seulement supérieure à celle d'un TCP non accéléré, mais elle est également beaucoup plus constante face à l'évolution des conditions du réseau. L'effet est de faire en sorte que les connexions distantes se comportent comme si elles étaient locales. La réactivité

perçue par l'utilisateur reste constante, quelle que soit l'utilisation des liens. Contrairement à TCP normal, avec lequel un WAN fonctionnant à 90 % d'utilisation est inutile pour les tâches interactives, une liaison accélérée a la même réactivité à 90 % d'utilisation de la liaison qu'à 10 %.

Avec les connexions court-courrier (celles qui tombent en dessous de la ligne diagonale dans la figure ci-dessus), peu ou pas d'accélération se produit dans de bonnes conditions de réseau, mais si le réseau se détériore, les performances diminuent beaucoup plus lentement qu'avec le TCP ordinaire.

Le trafic non-TCP, tel que UDP, n'est pas accéléré. Cependant, il est toujours géré par le régulateur du trafic.

Exemple

Un exemple d'optimisation TCP avancée est une optimisation de retransmission appelée *mode transactionnel*. Une particularité de TCP est que, si le dernier paquet d'une transaction est abandonné, sa perte n'a pas été remarquée par l'expéditeur jusqu'à ce qu'un délai d'expiration du récepteur (RTO) soit écoulé. Ce retard, qui est toujours d'au moins une seconde, et souvent plus long, est la cause des retards de plusieurs secondes observés sur les liens-retards qui rendent les sessions interactives désagréables ou impossibles.

Le mode transactionnel résout ce problème en retransmettant automatiquement le paquet final d'une transaction après un bref délai. Par conséquent, un RTO ne se produit que si les deux copies sont supprimées, ce qui est peu probable.

Un transfert en masse est essentiellement une seule transaction énorme, de sorte que la bande passante supplémentaire utilisée par le mode transactionnel pour un transfert en masse peut être aussi peu qu'un paquet par fichier. Cependant, le trafic interactif, comme les presses de touches ou les mouvements de souris, a de petites transactions. Une transaction peut consister en un seul paquet sous-dimensionné. L'envoi de ces paquets deux fois a un besoin de bande passante modeste. En effet, le mode transactionnel fournit une correction d'erreur directe (FEC) sur le trafic interactif et offre une protection RTO de fin de transaction à d'autres trafic.

Détection automatique et configuration automatique

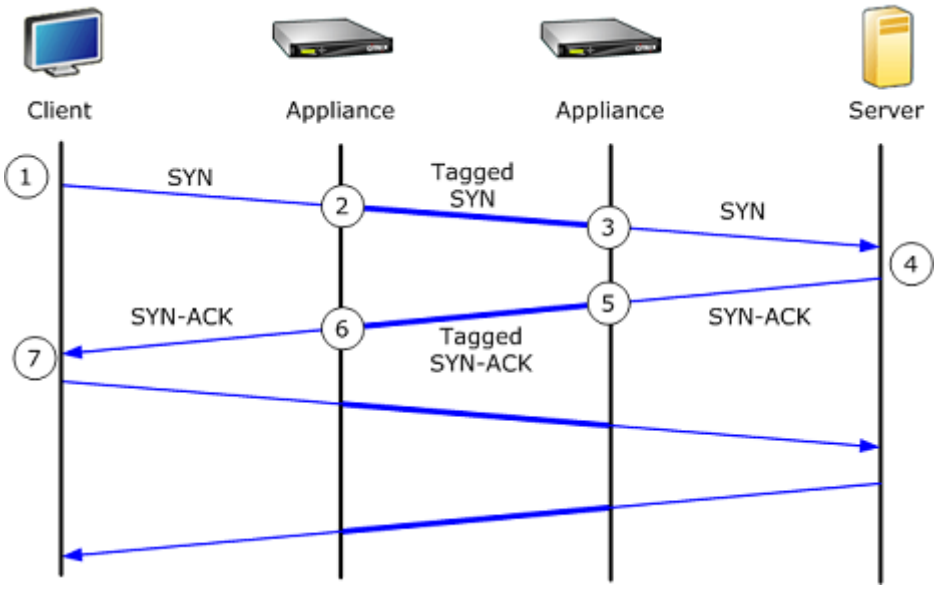
April 9, 2021

Dans le processus appelé autodiscovery, les unités Citrix SD-WAN WANOP détectent automatiquement la présence de l'autre. Les appliances attachent les options d'en-tête TCP aux premiers paquets de chaque connexion : le paquet SYN (envoyé par le client au serveur pour ouvrir la connexion) et le paquet SYN-ACK (envoyé par le serveur au client pour indiquer que la connexion a été acceptée). En

taggant les paquets SYN et en écoutant les paquets SYN et SYN-ACK taggés, les appliances peuvent détecter la présence réciproque en temps réel, connexion par connexion.

Le principal avantage de la découverte automatique est que vous n'avez pas à reconfigurer toutes vos appliances chaque fois que vous en ajoutez une nouvelle à votre réseau. Ils se retrouvent automatiquement. En outre, le même processus permet la configuration automatique. Les deux appliances utilisent les options d'en-tête TCP pour échanger des paramètres de fonctionnement, y compris les limites de bande passante (dans les directions d'envoi et de réception), le mode d'accélération de base (hardboost ou softboost) et les modes de compression acceptables (disque, mémoire ou aucun). Toutes les informations dont chaque appliance a besoin sur son partenaire sont échangées avec chaque connexion, ce qui permet des variations par connexion (par exemple, des variations par classe de service dans les types de compression autorisés).

Figure 1. Fonctionnement de la découverte automatique



Le processus de découverte automatique fonctionne comme suit :

1. Le client ouvre une connexion TCP au serveur, comme d'habitude, en lui envoyant un paquet TCP SYN.
2. La première appliance transmet le paquet SYN après avoir attaché un ensemble d'options d'en-tête TCP propres à l'appliance et ajusté la taille de la fenêtre.
3. La deuxième appliance lit les options TCP, les supprime du paquet et les transfère au serveur.
4. Le serveur accepte la connexion en répondant comme d'habitude avec un paquet TCP SYN-ACK.
5. La deuxième appliance se souvient que cette connexion peut être accélérée et attache ses propres options d'accélération à l'en-tête SYN-ACK.
6. La première appliance lit les options ajoutées par la seconde appliance, les supprime de l'en-tête du paquet et transfère le paquet au client. La connexion est maintenant accélérée. Les

deux appliances ont échangé les paramètres nécessaires à travers les valeurs d'option, et ils les stockent en mémoire pendant toute la durée de la connexion.

La connexion est accélérée et l'accélération est transparente pour le client, le serveur, les routeurs et les pare-feu.

Modes de contrôle de flux TCP

April 9, 2021

Le contrôle de flux TCP a deux modes : softboost et hardboost.

Softboost utilise un expéditeur basé sur le taux qui envoie un trafic accéléré à des vitesses allant jusqu'à la limite de bande passante de la liaison. Si la limite de bande passante est définie légèrement inférieure à la vitesse de liaison, la perte de paquets et la latence sont minimisées, tandis que l'utilisation des liens est maximisée. Les applications interactives voient des temps de réponse rapides tandis que les applications de transfert en masse voient une bande passante élevée. Softboost partage le réseau avec d'autres applications dans n'importe quelle topologie, et il interagit avec des systèmes QoS tiers.

Hardboost est plus agressif que softboost. En ignorant les pertes de paquets et d'autres soi-disant « signaux de congestion », il fonctionne très bien sur les liaisons en proie à de lourdes pertes non liées à la congestion, telles que les liaisons satellites. Il est également excellent sur les liaisons long-courriers de faible qualité avec une perte de paquets de fond élevée, comme de nombreux liens outremer. Hardboost est recommandé uniquement pour les liaisons point à point qui n'atteignent pas les performances adéquates avec softboost.

Softboost est le mode par défaut et est recommandé dans la plupart des cas.

> **Remarque**
>
> - Hardboost ne doit être utilisé que sur les liaisons point à point à vitesse fixe ou les déploiements en étoile où la bande passante du concentrateur est au moins égale à la somme des largeurs de bande en rayon accélérées.
> - Softboost et hardboost sont mutuellement exclusifs, ce qui signifie que tous les appareils qui doivent communiquer les uns avec les autres doivent être réglés de la même manière. Si une unité est définie sur hardboost et l'autre sur softboost, aucune accélération n'a lieu.

Pour sélectionner le mode softboost :

Softboost est le mode par défaut et est recommandé dans la plupart des cas.

1. Accédez à **Configuration** > **Liens** > **Hardboost/Softboost** et cliquez sur Modifier.

2. Sélectionnez **Softboost** comme **mode WAN Boost**.

3. Cliquez sur **Enregistrer**

Pour sélectionner le mode Boost :

Sélectionnez le mode Boost uniquement sur les liaisons point à point à vitesse fixe ou les liaisons en étoile où la bande passante du concentrateur est supérieure ou égale à celle des liaisons en étoile accélérées.

1. Accédez à **Configuration** > **Liens** > **Hardboost/Softboost** et cliquez sur Modifier.
2. Sélectionnez **Hardboost** comme **mode WAN Boost**.
3. Définissez la **limite de réception de bande passante WAN** à 95 % de la vitesse de liaison.
4. Cliquez sur **Enregistrer**.

Considérations sur les pare-feux

April 9, 2021

L'utilisation des options TCP par l'appliance Citrix SD-WAN WANOP met en danger le trafic accéléré provenant de pare-feu qui ont des règles agressives sur le refus de service aux connexions utilisant des options TCP moins courantes.

Certains pare-feu suppriment les options « inconnues », puis transmettent le paquet. Cette action empêche l'accélération mais n'altère pas la connectivité.

D'autres pare-feu refusent le service aux connexions avec des options inconnues. Autrement dit, les paquets SYN avec les options Citrix SD-WAN WANOP sont supprimés par le pare-feu. Lorsque l'appliance détecte des échecs répétés de tentatives de connexion, elle tente de nouveau sans les options. Cela restaure la connectivité après un retard de longueur variable, généralement dans la plage de 20-60 secondes, mais sans accélération.

Tout pare-feu qui ne transmet pas les options Citrix SD-WAN WANOP via non modifié doit être reconfiguré pour accepter les options TCP comprises entre 24 et 31 (décimal).

La plupart des pare-feu ne bloquent pas ces options. Cependant, les pare-feu Cisco ASA et PIX (et peut-être d'autres) avec le firmware de la version 7.x peuvent le faire par défaut.

Les pare-feu aux deux extrémités de la liaison doivent être examinés, car l'une ou l'autre peut autoriser des options sur les connexions sortantes mais les bloquer sur les connexions entrantes.

L'exemple suivant devrait fonctionner avec les pare-feu Cisco ASA 55x0 utilisant un firmware 7.x. Comme il autorise globalement des options dans la plage de 24-31, il n'y a pas de configuration personnalisée par interface ou par unité :

```
 ================================================================
 CONFIGURATION FOR CISCO ASA 55X0 WITH 7.X CODE TO ALLOW TCP OPTIONS
 ================================================================
 hostname(config)# tcp-map WSOptions
 hostname(config-tcp-map)# tcp-options range 24 31 allow
 hostname(config-tcp-map)# class-map WSOptions-class
 hostname(config-cmap)# match any
 hostname(config-cmap)# policy-map WSOptions
 hostname(config-pmap)# class WSOptions-Class
 hostname(config-pmap-c)# set connection advanced-options WSOptions
 hostname(config-pmap-c)# service-policy WSOptions global
<!--NeedCopy-->
```

La configuration d'un pare-feu PIX est similaire :

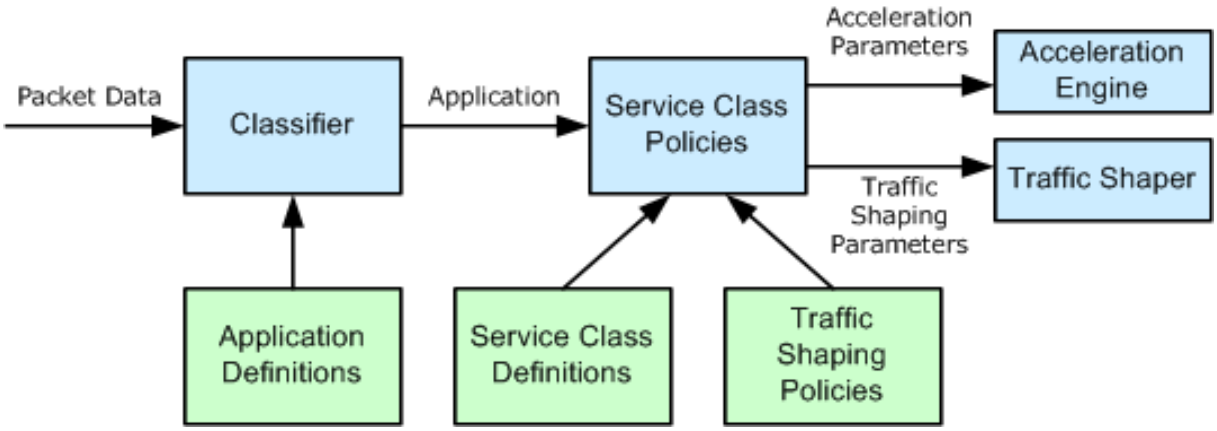
```
 ====================================================
 POLICY MAP TO ALLOW APPLIANCE TCP OPTIONS TO PASS (PIX 7.x)
 ====================================================
 pixfirewall(config)#access-list tcpmap extended permit tcp any any
 pixfirewall(config)# tcp-map tcpmap
 pixfirewall(config-tcp-map)# tcp-opt range 24 31 allow
 pixfirewall(config-tcp-map)# exit
 pixfirewall(config)# class-map tcpmap
 pixfirewall(config-cmap)# match access-list tcpmap
 pixfirewall(config-cmap)# exit
 pixfirewall(config)# policy-map global_policy
 pixfirewall(config-pmap)# class tcpmap
 pixfirewall(config-pmap-c)# set connection advanced-options tcpmap
<!--NeedCopy-->
```

Classification du trafic

April 9, 2021

Les deux principales fonctions d'une appliance Citrix SD-WAN WANOP sont le traffic shaping, qui maximise l'utilisation des liaisons pour tous les types de trafic, et l'accélération, qui applique la compression et diverses optimisations pour accélérer le trafic TCP. Deux composants de base du traffic shaping

et de l'accélération du trafic sont le mécanisme de classificateur d'applications et le mécanisme de classe de service. Le premier identifie le type de trafic, de sorte que le second peut affecter le trafic à une classe de service. Chaque classe de service a une politique de traffic shaping et une stratégie d'accélération.



Classificateur d'applications

April 9, 2021

Le classificateur d'application utilise les définitions d'application pour classer le trafic par protocole et application. Ces informations sont utilisées pour créer des rapports, et par le mécanisme de classe de service. De nombreuses applications sont déjà définies, et vous pouvez en définir plus au besoin.

Spécifications de protocole et de port dans les définitions d'application

Le classificateur d'applications utilise le protocole officiel et les spécifications de port de l'Internet Assigned Numbers Authority (IANA), http://www.iana.org. Parfois, des applications autres que les applications officielles utilisent un port. Le classificateur ne peut généralement pas détecter une telle utilisation. Si votre réseau utilise de telles applications, vous pouvez généralement résoudre ce problème en renommant l'application, dans le classificateur d'applications, pour indiquer l'application qui utilise ce port sur votre réseau. Par exemple, si vous utilisez le port 3128 non pas pour son utilisation standard pour un cache Web Squid, mais pour un proxy SOCKS, vous pouvez renommer l'application Squid (TCP) en SOCKS (Port 3128) pour plus de clarté.

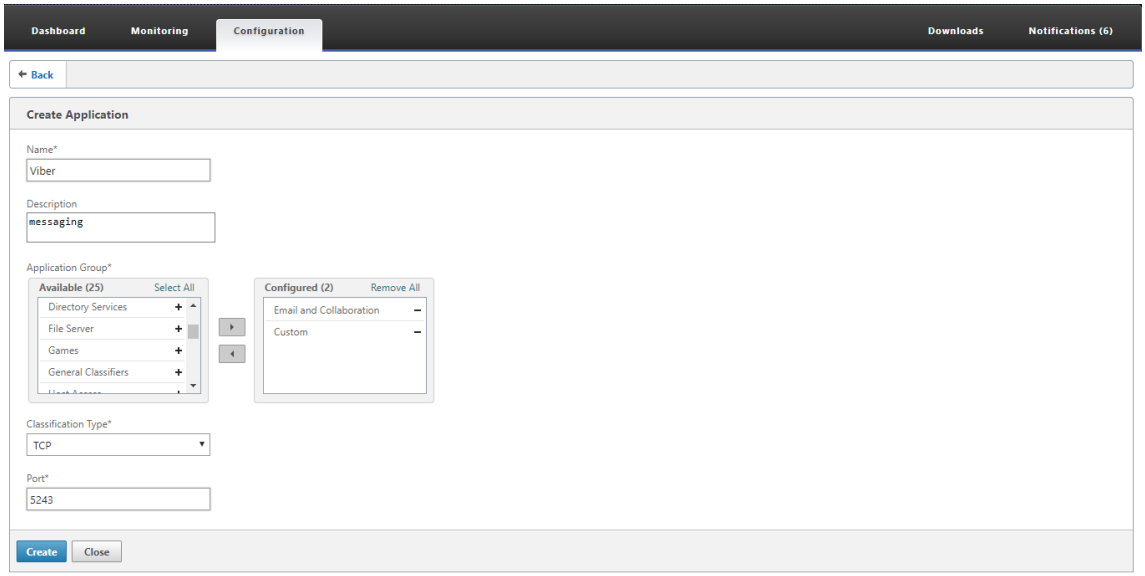
Les applications ne doivent pas avoir de définitions qui se chevauchent. Par exemple, si une application sur votre réseau utilise les ports TCP 3120 et 3128 et qu'une autre application utilise le port 3120, une seule définition d'application Citrix SD-WAN WANOP peut inclure le port 3120.

Configurer les définitions d'application

- TCP dynamique, pour les applications utilisant des allocations de port dynamiques
- Type d'éther, pour les types de paquets Ethernet
- Application publiée par l'ICA, pour applications virtuels/bureaux virtuels
- IP, pour les protocoles IP tels que ICMP ou GRE
- TCP, pour les applications TCP
- UDP, pour les applications UDP
- Adresse Web, pour des sites Web ou des domaines spécifiques.

Pour configurer la défense de l'application :

1. Accédez à **Configuration** > **Règles d'optimisation**> **Classificateurs d'applications**, puis cliquez sur **Ajouter**.



2. Dans la page **Créer une application**, définissez les paramètres suivants :

   - **Nom** - Nom du classificateur d'application. Doit commencer par un caractère alphanumérique ASCII ou un trait de soulignement (_), et ne doit contenir que des caractères alphanumériques ASCII, un trait de soulignement, un hachage (#), un point (.), deux points (:), à (@), égal à (=) et un trait d'union (-). Longueur maximale : 31 caractères.
   - **Description** - Description du classificateur d'application.
   - **Groupe d'applications** - Le classificateur d'applications appartient à ce groupe d'applications. Les groupes d'applications sont un ensemble de groupes d'applications prédéfinis qui sont classés en fonction de leurs fonctionnalités.

- **Type de classification** : classification de haut niveau que vous souhaitez utiliser pour ce classificateur d'application. La classification de haut niveau se fait principalement sur la base du port utilisé par une application.
- **Port** —Numéro de port à utiliser. Vous pouvez entrer une plage, une liste ou un nombre compris entre 0 et 65535.

3. Cliquez sur **Créer**.

   La page **Classificateurs d'applications** répertorie toutes les applications reconnues par le classificateur WANOP SD-WAN.

La page **Classificateurs d'applications** répertorie toutes les applications reconnues par le classificateur WANOP SD-WAN.

> **Conseil**
>
> Cliquez sur **Découverte automatique** pour permettre à toutes les applications publiées Citrix vues dans le flux de données d'être ajoutées automatiquement à la liste des applications. Une fois découverts, ils apparaîtront dans les rapports et peuvent être utilisés pour des politiques de traffic shaping.

Classes de service

April 9, 2021

Les classes de service sont affectées à des stratégies de traffic shaping et à des stratégies d'accélération à utiliser pour toutes les connexions qui correspondent à la définition de classe de service. Les classes de service peuvent être basées sur les paramètres suivants :

- Applications
- Adresses IP ou VLAN
- Bits DSCP
- Profils SSL

Les définitions de classe de service par défaut sont recommandées comme point de départ. Modifiez-les s'ils s'avèrent inadéquats pour vos liens.

Les classes de service sont définies dans une liste ordonnée. La première définition qui correspond au trafic traité devient la classe de service pour le trafic.

Différences entre les décisions d'accélération et les politiques de traffic shaping

Pour prendre une décision d'accélération, l'appliance Citrix SD-WAN WANOP examine le paquet SYN initial de chaque connexion TCP pour déterminer si la connexion est susceptible d'être accélérée. Le paquet SYN ne contient aucune charge utile, uniquement des en-têtes. La décision d'accélération doit donc être basée sur le contenu des en-têtes du paquet SYN, tel que le port de destination ou l'adresse IP de destination de la connexion. L'accélération, une fois appliquée, dure toute la durée de la connexion.

Contrairement aux décisions d'accélération, les politiques de traffic shaping peuvent être basées sur le contenu du flux de données de la connexion. En fonction du temps nécessaire au classificateur d'application pour recevoir suffisamment de données pour une classification finale, une connexion peut être reclassée pendant sa durée de vie.

Par exemple, le premier paquet d'une connexion HTTP à`http://www.example.com` est un paquet SYN qui contient un en-tête mais aucune charge utile. L'en-tête a un port de destination IP de 80, qui correspond à la définition de classe de service HTTP : Internet, de sorte que le moteur d'accélération fonde sa décision d'accélération, dans ce cas, aucune (aucune accélération) sur cette classe de service.

Le régulateur du trafic utilise la stratégie de traffic shaping de la classe de service HTTP : Internet, mais cette décision est temporaire. Le premier paquet de charge utile contient la chaîne GET`http://www.example.com`, qui correspond à l'exemple de définition d'application dans le classificateur d'application. La classe de service qui inclut l'exemple d'application est sélectionnée par le régulateur du trafic, à la place la classe de service qui inclut HTTP : Internet, et le régulateur du trafic utilise la stratégie de classe de service nommée dans cette définition de classe de service.

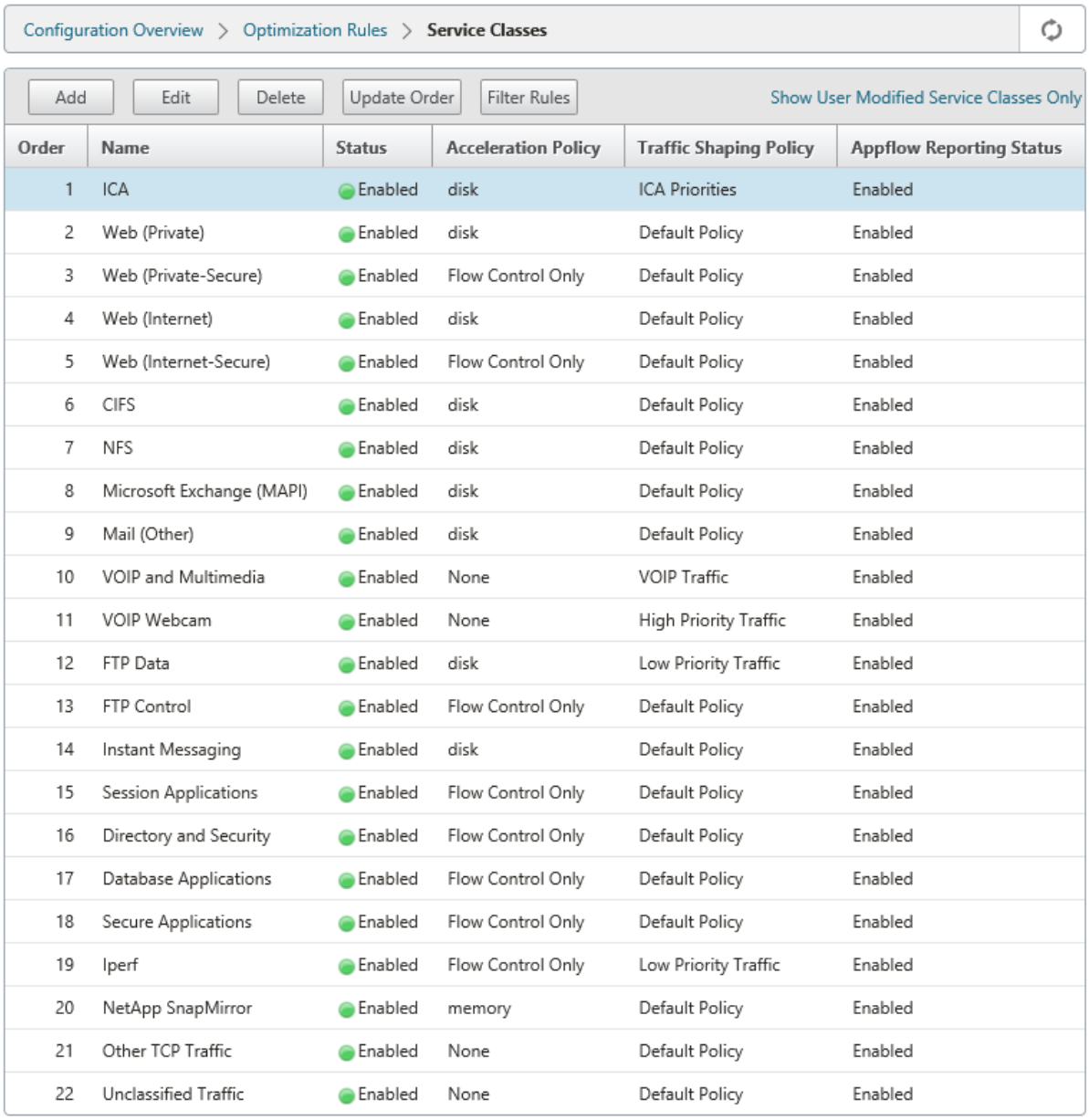
> **Remarque**
>
> Quelle que soit la stratégie de classe de service, la fonction de génération de rapports suit l'utilisation de l'exemple d'application.
>
> **Important**
>
> Tout le trafic est associé à une application et à une classe de service, et toutes les classes de service ont une stratégie de traffic shaping, mais seules les connexions TCP ont une stratégie d'accélération autre qu'aucune.

Configurer les définitions de classe de service

Étant donné que les définitions de classe de service sont une liste ordonnée, une définition qui fait exception à un cas général doit précéder la définition plus générale de la page Classe de service. La première définition dont la règle correspond au trafic est celle qui est appliquée. Par exemple :

- Les classes de service basées sur des URL doivent précéder les classes de service HTTP dans la liste des classes de service, car toute règle basée sur une URL correspond également à la classe de service HTTP. Par conséquent, placer la classe de service HTTP en premier empêcherait l'utilisation des règles basées sur l'URL ou des règles basées sur les applications publiées.
- De même, les classes de service basées sur les applications publiées ICA (Virtual Apps/Virtual Desktops) doivent précéder la classe de service Citrix.

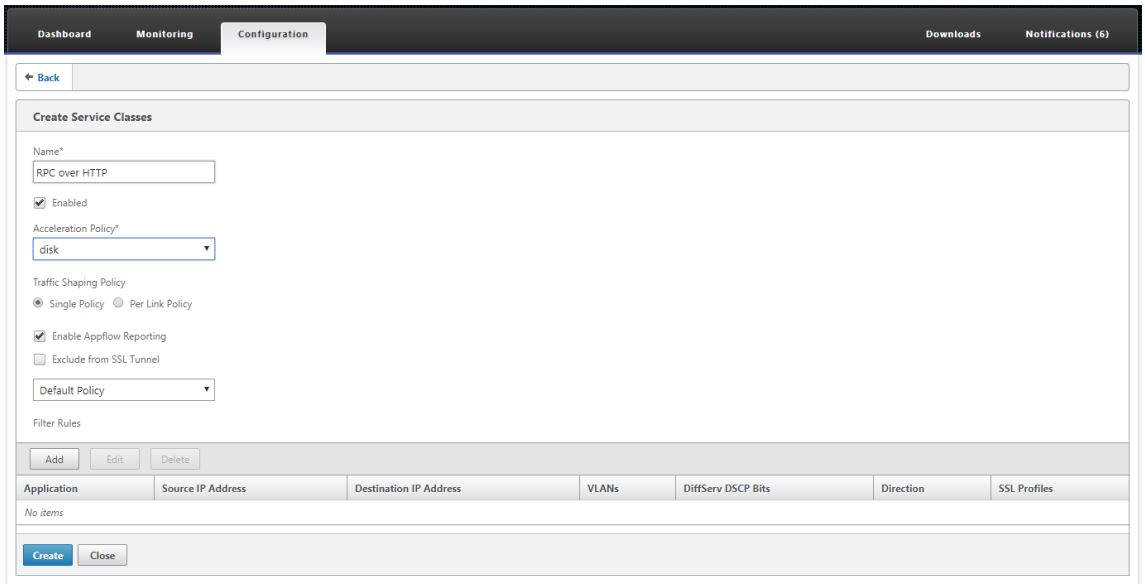
Comme toutes les règles basées sur l'URL correspondent à la classe de service HTTP, placer la classe de service HTTP au-dessus d'elles entraînerait l'utilisation des règles basées sur l'URL ou des règles basées sur l'application publiées.



Order	Name	Status	Acceleration Policy	Traffic Shaping Policy	Appflow Reporting Status
1	ICA	Enabled	disk	ICA Priorities	Enabled
2	Web (Private)	Enabled	disk	Default Policy	Enabled
3	Web (Private-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
4	Web (Internet)	Enabled	disk	Default Policy	Enabled
5	Web (Internet-Secure)	Enabled	Flow Control Only	Default Policy	Enabled
6	CIFS	Enabled	disk	Default Policy	Enabled
7	NFS	Enabled	disk	Default Policy	Enabled
8	Microsoft Exchange (MAPI)	Enabled	disk	Default Policy	Enabled
9	Mail (Other)	Enabled	disk	Default Policy	Enabled
10	VOIP and Multimedia	Enabled	None	VOIP Traffic	Enabled
11	VOIP Webcam	Enabled	None	High Priority Traffic	Enabled
12	FTP Data	Enabled	disk	Low Priority Traffic	Enabled
13	FTP Control	Enabled	Flow Control Only	Default Policy	Enabled
14	Instant Messaging	Enabled	disk	Default Policy	Enabled
15	Session Applications	Enabled	Flow Control Only	Default Policy	Enabled
16	Directory and Security	Enabled	Flow Control Only	Default Policy	Enabled
17	Database Applications	Enabled	Flow Control Only	Default Policy	Enabled
18	Secure Applications	Enabled	Flow Control Only	Default Policy	Enabled
19	Iperf	Enabled	Flow Control Only	Low Priority Traffic	Enabled
20	NetApp SnapMirror	Enabled	memory	Default Policy	Enabled
21	Other TCP Traffic	Enabled	None	Default Policy	Enabled
22	Unclassified Traffic	Enabled	None	Default Policy	Enabled

Pour créer une classe de service RPC sur HTTP et y lier le profil SSL :

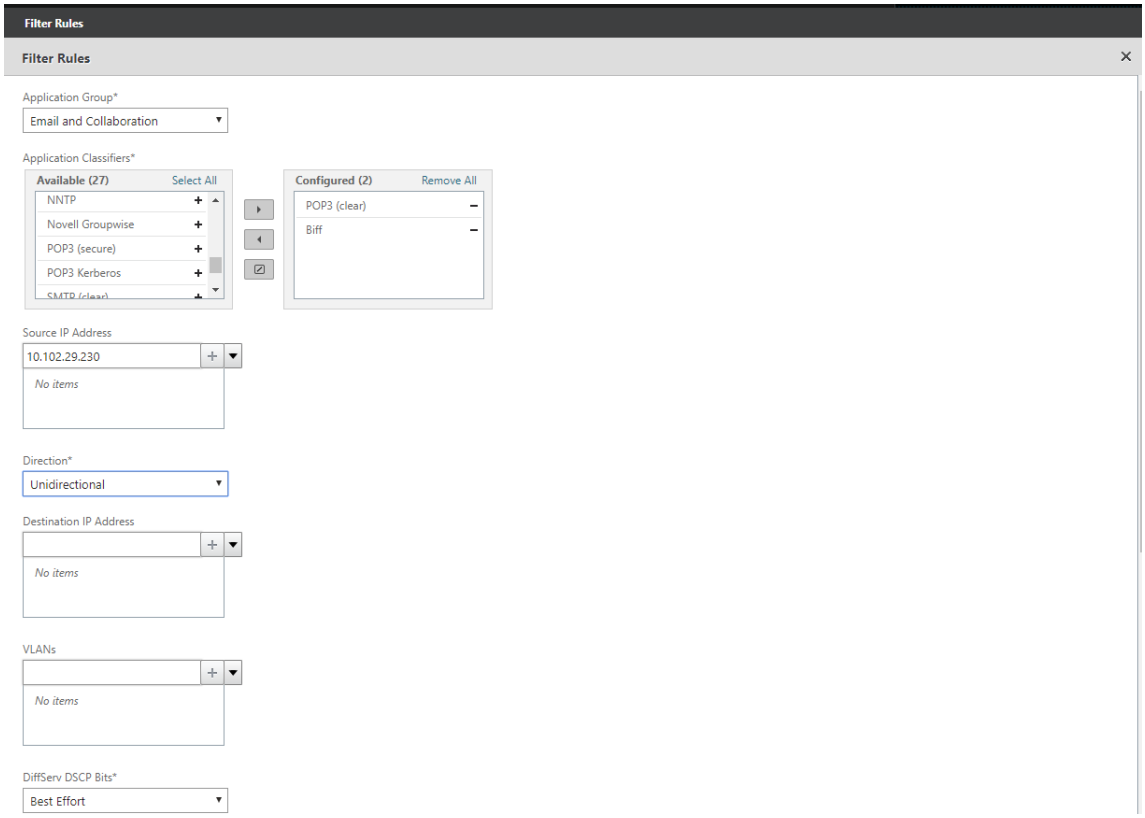
1. Accédez à **Configuration** > **Règles d'optimisation** > **Classes de service** , puis cliquez sur **Ajouter**.



2. Dans le champ **Nom**, entrez un nom pour la classe de service.
3. Assurez-vous que l'option **Activé** est sélectionnée.
4. Dans la liste **Stratégie d'accélération**, sélectionnez une stratégie d'accélération. **Mémoire** et **disque** spécifient où stocker l'historique du trafic utilisé pour la compression. Le**disque** est généralement le meilleur choix, car l'appliance sélectionne automatiquement le disque ou la mémoire, en fonction de celui qui convient le mieux au trafic. **La mémoire** spécifie uniquement la mémoire. Sélectionnez**Contrôle du flux uniquement** pour désactiver la compression mais activer l'accélération du contrôle du flux. Sélectionnez cette option pour les services toujours chiffrés et pour le canal de contrôle FTP. **Aucun n'** est utilisé uniquement pour le trafic chiffré non compressible et la vidéo en temps réel.
5. Sélectionnez **Activer AppFlow Reporting** pour activer les rapports AppFlow pour cette classe de service. Les informations de cette classe de service sont incluses dans tous les rapports AppFlow. AppFlow est une norme de l'industrie pour le déverrouillage des données transactionnelles d'application traitées par l'infrastructure réseau. L'interface AppFlow d'optimisation WAN fonctionne avec n'importe quel collecteur AppFlow pour générer des rapports. Le collecteur reçoit des informations détaillées de l'appliance, à l'aide de la norme ouverte AppFlow.
6. Sélectionnez **Exclure du tunnel SSL** pour exclure le trafic associé à la classe de service du tunnel SSL.
7. Dans la liste des stratégies de traffic shaping, assurez-vous que l'option **Stratégie par défaut** est sélectionnée. Les stratégies de traffic shaping ont une priorité pondérée et d'autres attributs qui déterminent la manière dont le trafic correspondant sera traité, par rapport à un autre trafic. La plupart des classes de service sont définies sur Stratégie par défaut, mais une stratégie de

traffic shaping de priorité supérieure peut être affectée au trafic de priorité supérieure et une stratégie de priorité inférieure peut être affectée au trafic de priorité inférieure.

8. Dans la section Règles de filtrage, cliquez sur **Ajouter** pour créer une règle de filtre dont la valeur par défaut n'importe quel pour tous les paramètres. Si une règle est évaluée comme TRUE pour une connexion donnée, la connexion est affectée à cette classe de service. Les règles de filtrage pour la plupart des classes de service consistent uniquement en une liste d'applications, mais les règles peuvent également inclure des adresses IP, des balises VLAN, des valeurs DSCP et des noms de profils SSL. Tous les champs d'une règle sont par défaut « Tout » (un caractère générique). Les champs d'une règle sont traités selon l'opérateur AND.
9. Cliquez sur **Ajouter** pour ajouter des règles de filtre.



10. Dans la liste **Groupe d'applications**, sélectionnez **E-mail et collaboration**.
11. Dans la liste **Disponible**, sélectionnez les applications requises.
12. Déplacez les applications sélectionnées vers la liste **Configuré**.
13. Dans le champ **Adresses IP source**, ajoutez les adresses IP client.
14. Dans la liste **Direction**, sélectionnez la direction du trafic.
15. Dans la liste **Profils SSL** , sélectionnez le profil SSL que vous avez créé.
16. Cliquez sur **Créer**.

> **Remarque**
>
> - Vous devez configurer et lier un profil SSL à la classe de service uniquement sur l'appliance côté centre de données.
> - Seules les classes de service dont la direction des règles de filtre est définie sur unidirectionnel peuvent être associées à des profils SSL.

Traffic shaping

April 23, 2021

18 avr. 2018

Le traffic shaping vous permet de réguler le flux de trafic réseau pour assurer un certain niveau de qualité de service (QoS). Vous pouvez réguler le flux de paquets dans un réseau (limitation de la bande passante) ou hors d'un réseau (limitation de débit).

En utilisant des stratégies de traffic shaping, vous pouvez définir la priorité d'un trafic de liaison différent et envoyer du trafic sur la liaison à une vitesse proche de la vitesse de liaison, mais pas supérieure à cette vitesse. Contrairement à l'accélération, qui s'applique uniquement au trafic TCP/IP, le régulateur de trafic gère tout le trafic sur la liaison.

Vous pouvez définir une bande passante élevée pour les flux de trafic considérés comme plus importants que le reste des flux de trafic, ce qui vous permet d'utiliser de manière optimale les ressources de liaison rares.

Le traffic shaping est basé sur une file d'attente pondérée, ce qui donne à chaque classe de service sa juste part de la bande passante de liaison. Si le lien est inactif, toute connexion (dans n'importe quelle classe de service) peut utiliser le lien entier. Lorsque plusieurs connexions sont en concurrence pour la bande passante de liaison, le régulateur du trafic applique des stratégies de traffic shaping pour déterminer la bonne combinaison de trafic.

Pour plus d'informations sur la mise en file d'attente pondérée, reportez-vous à la section Queuing équitable pondérée.

Pour configurer le traffic shaping :

1. Configurez la définition de lien.

   La définition de lien est utilisée par le régulateur du trafic pour déterminer la vitesse du lien d'envoi et de réception et d'autres informations liées au lien. Pour plus d'informations sur la façon dont Traffic shaper utilise la définition de lien et comment configurer les définitions de lien, reportez-vous à la section Définitions des liens.

2. Configurez la définition de l'application.

   Le trafic qui traverse le lien est examiné par le classificateur d'applications pour déterminer à quelle application il appartient, puis l'application est recherchée dans la liste des classes de services pour déterminer à quelle classe de service elle appartient. Pour plus d'informations sur la classification des applications et la configuration de la définition des applications, reportez-vous à la section Classification du trafic.

3. Créez une stratégie de traffic shaping.

   Vous pouvez utiliser les stratégies de traffic shaping par défaut ou créer une nouvelle stratégie pour définir la priorité pondérée et d'autres paramètres en fonction des besoins de votre réseau. Pour plus d'informations sur la création d'une stratégie de traffic shaping, reportez-vous à la section Stratégies de traffic shaping.

4. Configurez une définition de classe de service et associez la stratégie de traffic shaping à la classe de service.

   Pour plus d'informations sur la configuration de la définition de classe de service, reportez-vous à la section Classes de service.

Quelques points sur le régulateur du trafic :

- Tout le trafic WAN est soumis au traffic shaping : connexions accélérées, connexions non accélérées et trafic non-TCP comme les flux UDP et GRE.
- L'algorithme est pondérée juste file d'attente, dans laquelle l'administrateur attribue une priorité à chaque classe de service. Chaque classe de service représente un pool de bande passante, ayant droit à une fraction minimale de la vitesse de liaison, égale à (my_priority/sum_of_all_priorities). Une classe de service avec une priorité pondérée de 100 obtient deux fois plus de bande passante qu'une classe de service avec une priorité pondérée de 50. Vous pouvez affecter des pondérations de 1 à 256.
- Chaque connexion au sein d'une classe de service obtient une part égale de la bande passante allouée à cette classe de service.
- Chaque connexion obtient sa juste part de la bande passante du lien, car les priorités sont appliquées aux données WAN réelles transférées, après compression. Par exemple, si vous avez deux flux de données avec la même priorité, l'un avec une compression 10:1 et l'autre avec une compression 2:1, les utilisateurs voient une différence de débit de 5:1, même si l'utilisation de la liaison WAN des deux connexions est identique. En pratique, cette disparité est souhaitable, car la bande passante WAN, et non la bande passante des applications, est la ressource rare qui doit être gérée.
- Les politiques de traffic shaping s'appliquent également au trafic accéléré et non accéléré. Par exemple, une connexion accélérée aux applications virtuelles et une connexion d'applications

virtuelles non accélérées reçoivent toutes deux une mise en forme du trafic, de sorte que les deux peuvent avoir une priorité élevée par rapport au trafic en masse. Autre exemple, le trafic non TCP sensible au temps, tel que VoIP (qui utilise le protocole UDP) peut être accéléré.

- Le traffic shaping est appliqué à la liaison WAN dans les directions d'envoi et de réception, à la fois au trafic accéléré et non accéléré. Cette fonctionnalité empêche la congestion et l'augmentation de la latence même lorsque l'autre côté de la liaison n'est pas équipé d'une appliance Citrix SD-WAN WANOP. Par exemple, les téléchargements Internet peuvent être priorisés et gérés.
- La stratégie de traffic shaping pour une classe de services peut être spécifiée par liaison si vous le souhaitez.
- En plus de façonner le trafic directement, le régulateur du trafic peut l'affecter indirectement en définissant le champ DSCP (Differentiated Services Code Point) pour informer les routeurs en aval du type de formage du trafic requis par chaque paquet.

Mise en file d'attente pondérée (WFQ)

April 9, 2021

Dans n'importe quel lien, la Gateway goulot d'étranglement détermine la discipline de mise en file d'attente, car les données des passerelles sans goulot d'étranglement ne sont pas de sauvegarde. Sans données en attente dans les files d'attente, le protocole de mise en file d'attente n'est pas pertinent.

La plupart des réseaux IP utilisent des files d'attente FIFO profondes. Si le trafic arrive plus vite que la vitesse du goulot d'étranglement, les files d'attente se remplissent et tous les paquets subissent des temps de file d'attente plus élevés. Parfois, le trafic est divisé en quelques classes différentes avec des FIFO distincts, mais le problème reste. Une connexion unique qui envoie trop de données peut entraîner des retards importants, des pertes de paquets ou les deux pour toutes les autres connexions de sa classe.

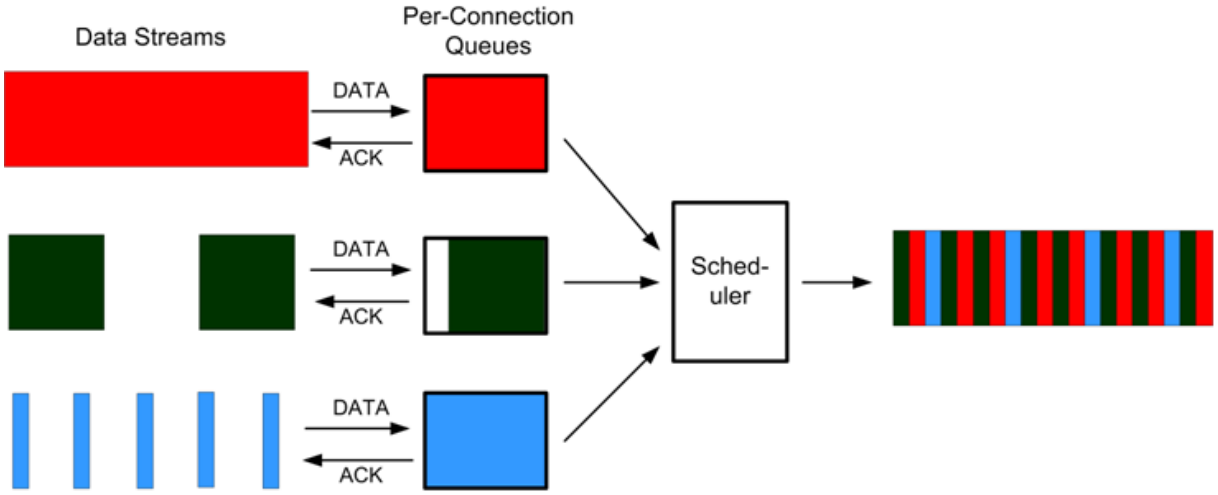
Une appliance WANOP Citrix SD-WAN utilise une file d'*attente équitable pondérée,* qui fournit une file d'attente distincte pour chaque connexion. Avec une file d'attente équitable, une connexion trop rapide ne peut déborder que sa propre file d'attente. Il n'a aucun effet sur les autres connexions. Mais à cause du contrôle de flux sans perte, il n'y a pas de connexion trop rapide, et les files d'attente ne débordent pas.

Le résultat est que chaque connexion a son trafic mesuré dans la liaison d'une manière équitable, et que la liaison dans son ensemble a une bande passante et un profil de latence optimaux.

La figure suivante montre l'effet de la file d'attente équitable. Une connexion qui nécessite moins que sa juste part de bande passante (la connexion inférieure) obtient autant de bande passante qu'

elle tente d'utiliser. En outre, il a très peu de latence de mise en file d'attente. Les connexions qui tentent d'utiliser plus que leur juste part obtiennent leur juste part, ainsi que toute bande passante restante provenant des connexions qui utilisent moins que leur juste part.

Figure 1. Queuing équitable en action



Le profil de latence optimal offre aux utilisateurs d'applications interactives et transactionnelles des performances idéales, même lorsqu'ils partagent la liaison avec plusieurs transferts groupés. La combinaison d'un contrôle de flux transparent sans perte et d'une file d'attente équitable vous permet de combiner tous les types de trafic sur la même liaison en toute sécurité et en toute transparence.

La différence entre la juste file d'attente pondérée et la juste file d'attente non pondérée est que la juste file d'attente pondérée inclut la possibilité de donner à certains trafic une priorité (poids) plus élevée que d'autres. Le trafic avec un poids de deux reçoit deux fois la bande passante du trafic avec un poids de un. Dans une configuration Citrix SD-WAN WANOP, les pondérations sont affectées dans les stratégies de traffic shaping.

Stratégies de traffic shaping

April 23, 2021

Chaque définition de classe de service est associée à une stratégie de traffic shaping, qui définit les paramètres du trafic de la classe de service associée. Vous pouvez créer et configurer des stratégies de traffic shaping pour les sites ayant des besoins particuliers, mais les paramètres de stratégie par défaut fonctionnent correctement pour la plupart des installations, offrant les avantages suivants :

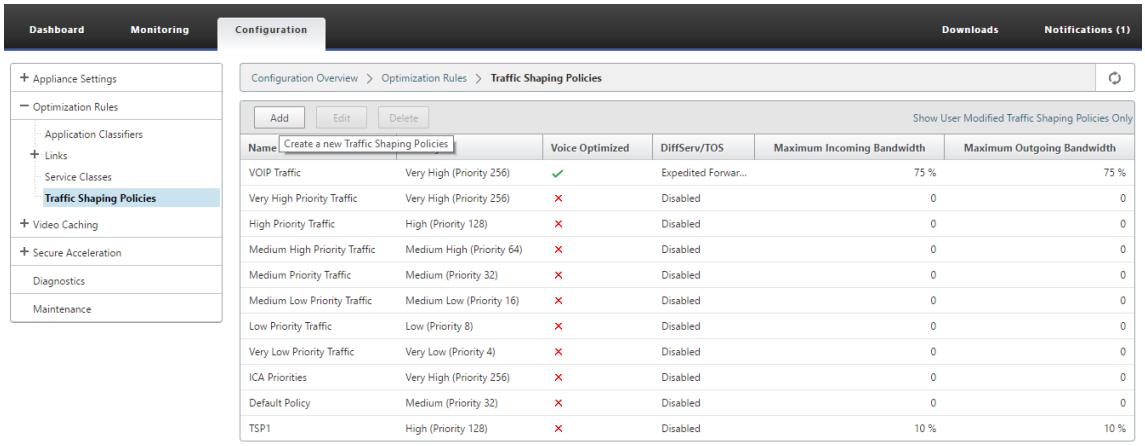
- Réactivité accrue pour le trafic interactif tel que Citrix Virtual Apps and Desktops.
- Protection du trafic VoIP sensible à la latence et à l'instabilité.

- Pas de « frapper le mur » pendant les périodes de pointe. Vous obtenez des performances utilisables même sous une charge extrême.
- Amélioration de l'utilisation de la bande passante en permettant aux transferts groupés de remplir le lien avec la bande passante restante des tâches interactives.
- Extension des avantages d'une file d'attente équitable à tout le trafic

Une appliance Citrix SD-WAN WANOP est livrée avec des stratégies de traffic shaping par défaut qui couvrent un large éventail de priorités. Ces stratégies sont répertoriées dans la page **Stratégies de traffic shaping**. En dehors de la **stratégie par défaut**, les autres stratégies par défaut d'usine ne peuvent pas être modifiées ou supprimées. La raison est de s'assurer qu'ils ont la même signification sur tous les appareils. Pour apporter des modifications, créez une nouvelle stratégie de traffic shaping avec les nouveaux paramètres et modifiez les définitions de classe de service appropriées pour faire référence à la nouvelle stratégie de traffic shaping.

Pour créer une stratégie de traffic shaping :

1. Dans l'interface utilisateur de gestion WANOP SD-WAN, accédez à **Configuration** > **Règles d'optimisation** > **Stratégies de traffic shaping**, puis cliquez sur **Ajouter**.

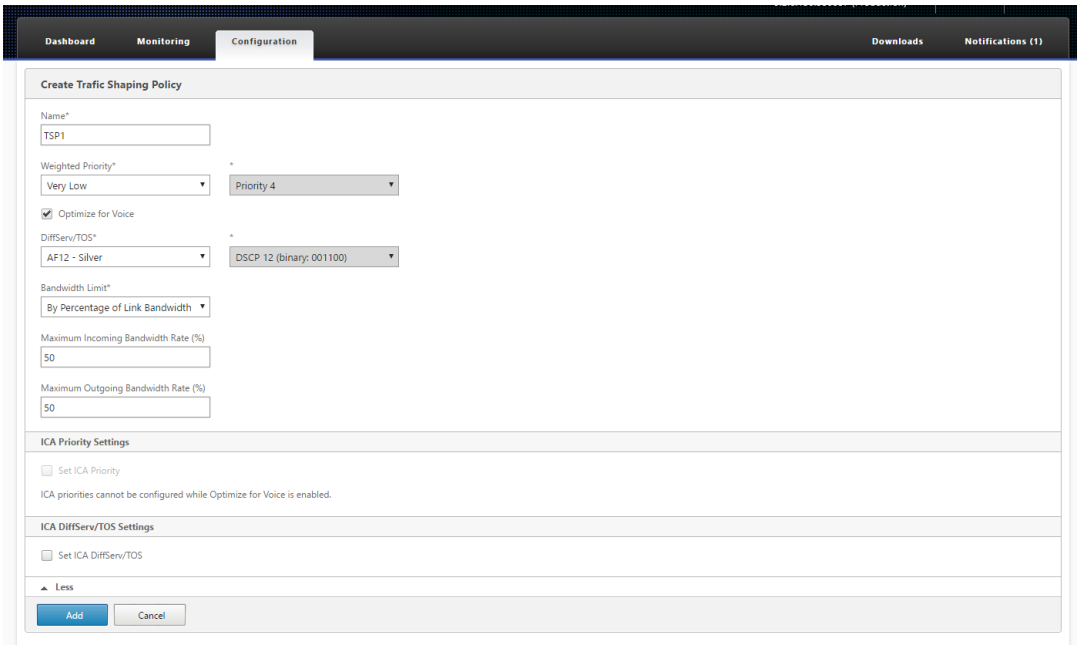


2. Dans la page **Créer une stratégie de traffic shaping**, entrez des valeurs pour les paramètres suivants :

   - **Nom** : nom de la nouvelle stratégie. Doit être unique.
   - **Priorité pondérée** : vous pouvez sélectionner une valeur de priorité existante ou sélectionner une valeur personnalisée comprise entre 1 et 256. Une connexion avec une priorité de 256 obtient 256 fois la part de bande passante en tant que connexion avec une priorité de 1.
   - **Optimiser pour la voix** : si elle est sélectionnée, cette stratégie aura effectivement une priorité infinie. Ceci est hautement indésirable pour la plupart du trafic, car cela empêchera un traffic shaping significatif et entraînera une privation de données pour les autres trafic

s'il y a suffisamment de trafic « optimisé pour la voix » pour remplir le lien. Utilisez uniquement pour VoIP et utilisez toujours en conjonction avec une limite de bande passante sur la stratégie (par exemple, 50 % de la vitesse de liaison)

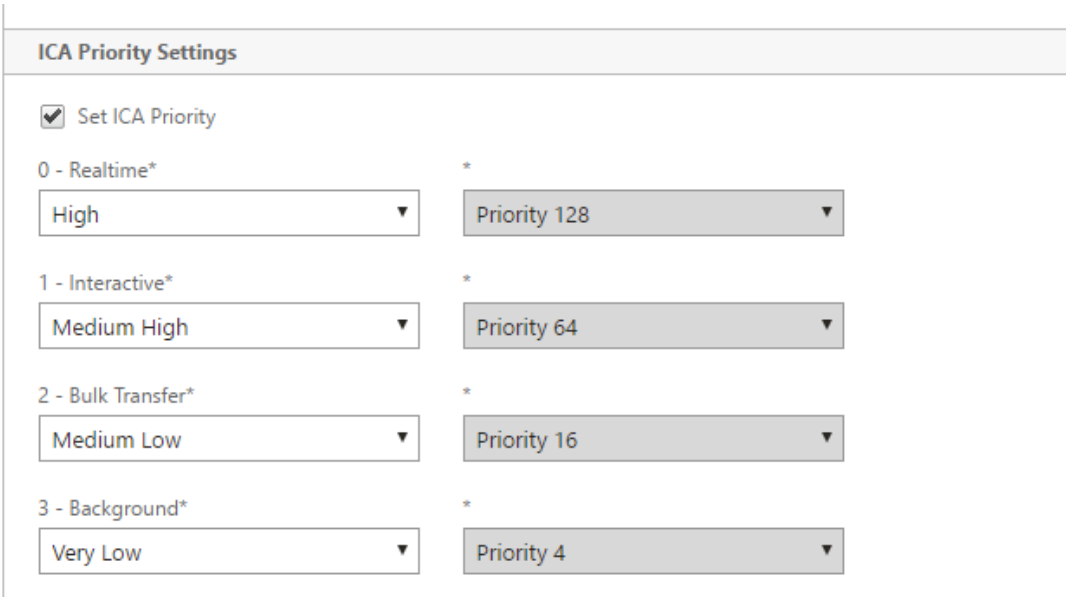
> **Remarque**
>
> L'optimisation vocale ne peut pas être configurée tant que les priorités ICA sont définies.



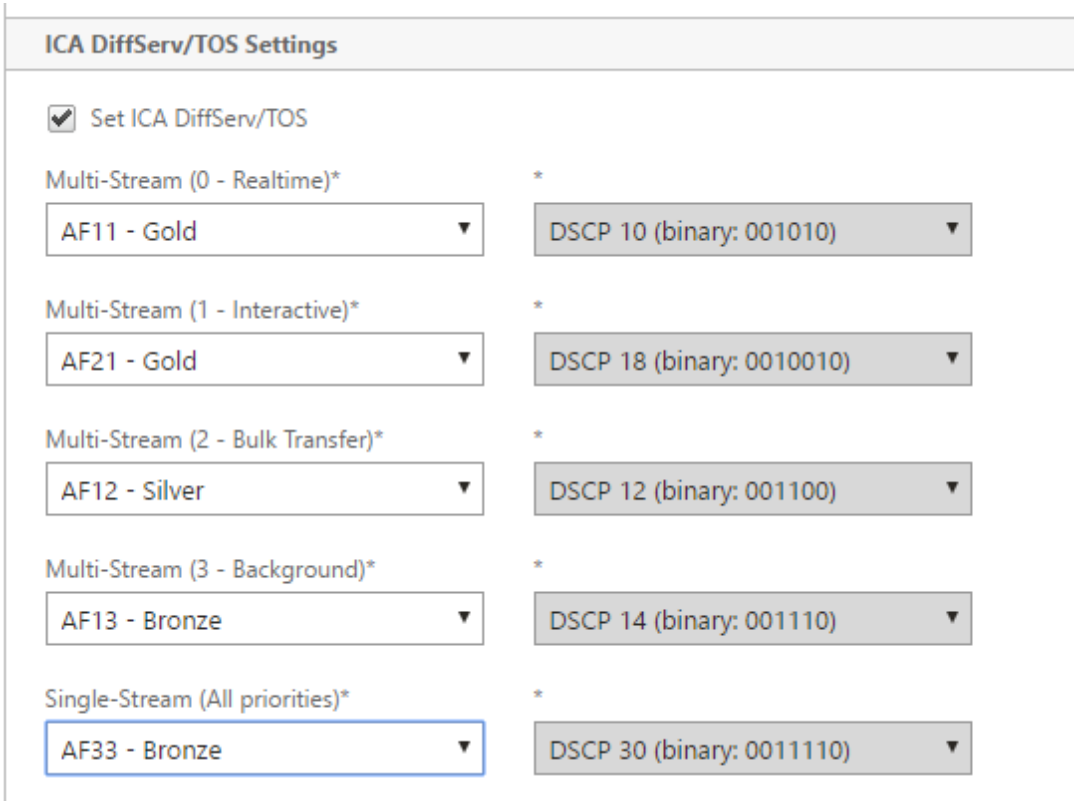
- **DiffServ/TOS**—Définit les bits DSCP des paquets de sortie sur la valeur sélectionnée. Utilisé pour contrôler les routeurs en aval.
- **Limite de bande passante** : empêche le trafic utilisant cette stratégie de dépasser la bande passante spécifiée, exprimée soit en pourcentage de la vitesse de liaison, soit en valeur absolue. Citrix recommande de spécifier un pourcentage, afin que la même définition puisse s'appliquer aux liaisons de vitesses différentes. Cette fonctionnalité peut laisser la bande passante inutilisée. Par exemple, une stratégie définie sur 50 % de la vitesse de liaison ne permet pas au trafic affecté d'utiliser plus de 50 % de la liaison, même si la liaison est autrement inactive. La limitation du trafic de cette manière n'est pas cohérente avec les performances maximales, de sorte que cette fonctionnalité est rarement utilisée, sauf avec le trafic VoIP avec le paramètre Optimiser pour la voix.

  > **Remarque**
  >
  > La configuration de la **limite de bande passante** est applicable uniquement pour Citrix SD-WAN édition WANOP. Pour Citrix SD-WAN PE édition, le paramètre **Limite de bande passante** est désactivé par défaut.

- **Définir les priorités ICA**—Si cette stratégie est utilisée pour le trafic Citrix Virtual Apps/Virtual Desktops, la priorité interne du trafic en temps réel, interactif, transfert en bloc et en arrière-plan est remplacée par la priorité définie ici.



- **Définir ICA Diffserv/TOS** : pour le trafic ICA (Virtual Apps/Virtual Desktops), chacune des quatre valeurs de priorité ICA peut être balisée avec une valeur DSCP différente. Cette fonctionnalité est particulièrement utile avec la nouvelle fonctionnalité ICA Multistream, dans laquelle le client Virtual Apps ou Virtual Desktops utilise différentes connexions pour différents niveaux de priorité.



3. Cliquez sur **Ajouter**. La nouvelle stratégie de traffic shaping créée est répertoriée dans la liste Stratégies de traffic shaping.

   Vous pouvez désormais associer la stratégie de traffic shaping à une classe de service. Pour plus d'informations, reportez-vous à la section Classes de service.

Mise en cache de vidéo

April 9, 2021

De nombreuses organisations utilisent la vidéo pour les communications qui ne sont pas sensibles au temps (par exemple, les sessions de formation et les messages pré-enregistrés destinés aux employés). Communiquer des messages par le biais de vidéos est non seulement rentable, mais aussi pratique lorsque le public est réparti entre les fuseaux horaires. Cependant, les vidéos consomment beaucoup de bande passante lorsqu'elles sont lues sur Internet. Une bande passante insuffisante provoque une latence, ce qui affecte l'expérience utilisateur et dégrade l'impact de la communication vidéo.

La mise en cache vidéo améliore l'expérience de visualisation des flux vidéo HTTP, en particulier sur les liens plus lents. Le cache vidéo est géré sur l'appliance Citrix SD-WAN WANOP local. Lorsqu'un utilisateur local affiche une vidéo déjà mise en cache, l'appliance peut remettre la copie mise en cache à pleine vitesse du réseau local.

Après avoir configuré l'appliance pour mettre en cache les vidéos, elle met en cache les vidéos affichées par vos utilisateurs. Vous pouvez également utiliser l'option de pré-peuplement pour récupérer les vidéos sélectionnées à partir du serveur vidéo local en prévision d'une utilisation ultérieure.

La fonctionnalité de mise en cache vidéo utilise un cache proxy d'interception pour examiner toutes les requêtes HTTP. Les demandes qui répondent aux exigences énumérées ci-dessous sont mises en cache. Les vidéos ne sont pas diffusées à partir du cache sauf si elles sont évaluées comme neuves par le moteur de cache. Sinon, ils sont récupérés à nouveau pour la visionneuse, et la version précédemment mise en cache est écrasée.

Contenu le plus récent garanti. Chaque fois qu'une vidéo est affichée, le cache vérifie le serveur d'origine et si la vidéo a changé, le contenu mis en cache est ignoré et le nouveau contenu est téléchargé.

> **Remarque**
>
> La mise en cache est désormais transparente. Autrement dit, l'adresse IP du client et du serveur sont maintenues de bout en bout. Dans les versions antérieures, l'adresse IP de l'appliance Citrix SD-WAN WANOP était affichée en tant qu'adresse source.

Une vidéo est mise en cache lorsque tous les critères suivants sont remplis :

- Le protocole utilisé pour diffuser la vidéo est HTTP. Par défaut, le port 80 est configuré pour la mise en cache vidéo. Toutefois, si vous avez configuré un autre port, tel que 8080 pour un serveur Web, vous devez spécifier ce port pour la mise en cache des vidéos.
- Vous avez ajouté des sources vidéo à partir desquelles vous souhaitez mettre en cache les vidéos. Par défaut, les sources vidéo YouTube, Vimeo, Youku, Dailymotion et Metacafe sont ajoutées à l'appliance, mais seuls YouTube et Vimeo sont activés. Si vous souhaitez mettre en cache des vidéos provenant de l'une des autres sources par défaut, vous devez les activer. Lorsque vous ajoutez de nouvelles sources vidéo, vous pouvez les activer à mesure que vous les ajoutez.
- Outre YouTube, Vimeo, Metacafe, Dailymotion et Youku, vous pouvez spécifier d'autres sites Web, adresses IP ou sous-réseaux comme sources vidéo. Notez que ces sites Web ne doivent pas avoir de mécanismes d'évitement, tels que l'ajout de caractères aléatoires à une URL.
- La vidéo doit être dans l'un des formats vidéo reconnus et avoir l'une des extensions de fichier suivantes : .3gp, .avi, .dat, .divx, .dvx, .dv-avi, .flv, .fmv, .h264, .hdmov, .m15, .m1v, .m21, .m2a, .m2v, .m4e .m4v, .m75, .moov, .mov, .movie, .mp21, mp2v, .mp4, .mp4v, .mpe, .mpeg, mpeg4, mpg, mpg2, .mpv, .mts, .ogg, .ogv, .qt, .qtm, .ra, .rm, .ram, .rmd, .rms, rmvb, .rp, rv, .swf, .ts, .vfw, .vob, .webm, .wm, .wma, .wmv, and .wtv.

Plates-formes prises en charge

La fonctionnalité de mise en cache vidéo est prise en charge par les appliances suivantes :

- Appareil SD-WAN WANOP 600 avec des modèles de licence de bande passante de 1 Mbps et 2 Mbps.
- Appliance SD-WAN WANOP 800 avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 1000 avec Windows Server, avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 2000 avec tous les modèles de licence de bande passante.
- Appliance SD-WAN WANOP 2000 avec Windows Server, avec tous les modèles de licence de bande passante.
- Appareil SD-WAN WANOP 3000 avec tous les modèles de licence de bande passante.
- SD-WAN WANOP VPX et SD-WAN WANOP VPX pour Amazon

Serveur vidéo pris en charge

La fonctionnalité de mise en cache vidéo est prise en charge sur Adobe Flash Media Server 4.5 ou version ultérieure. En outre, tout serveur vidéo qui sert des vidéos sur HTTP en tant que liens statiques est pris en charge pour la mise en cache vidéo.

Modes de déploiement pris en charge

La mise en cache vidéo est prise en charge en mode Inline, Inline dans les ports de jonction VLAN, Virtual Inline et WCCP.

Considérations relatives à l'utilisation de la fonction de mise en cache vidéo

Voici quelques points à prendre en compte lors de l'utilisation de la fonctionnalité de mise en cache vidéo.

- Si l'un des sites Web pris en charge modifie la façon dont il présente le contenu, l'avantage de mise en cache vidéo pour ces sites peut ne pas être atteint tant que le fichier de stratégie de mise en cache vidéo n'est pas mis à jour. Pour de telles modifications occasionnelles, Citrix fournit un fichier de stratégie de mise en cache vidéo mis à jour. Pour l'utiliser, reportez-vous à la section Mise à niveau du fichier de stratégie de mise en cache vidéo.

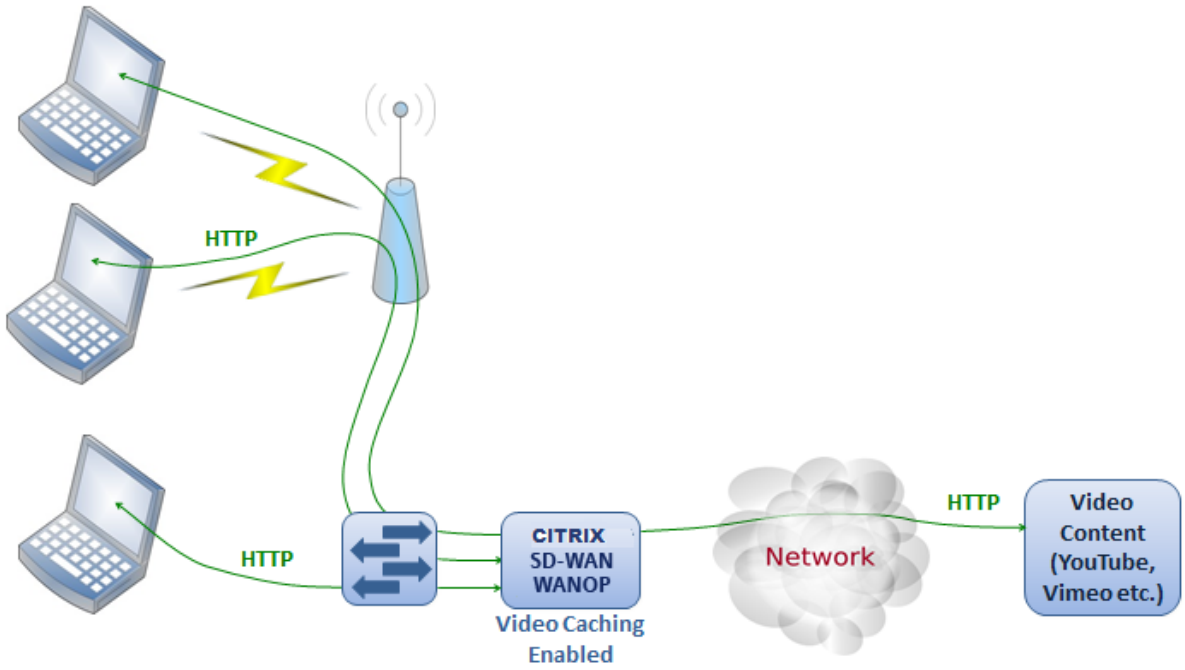
- Certains sites Web vidéo peuvent utiliser différents formats de fichier pour la même vidéo, selon le système d'exploitation ou le navigateur utilisé pour accéder à la vidéo. Cela peut entraîner une absence de cache.
- Certains sites vidéo, tels que YouTube, s'adaptent aux conditions du réseau. La qualité d'une vidéo peut donc dépendre des conditions du réseau au moment où elle est mise en cache.

Scénarios de mise en cache de vidéo

April 9, 2021

Vous pouvez déployer la mise en cache vidéo sur l'appliance Citrix SD-WAN WANOP dans les scénarios suivants :

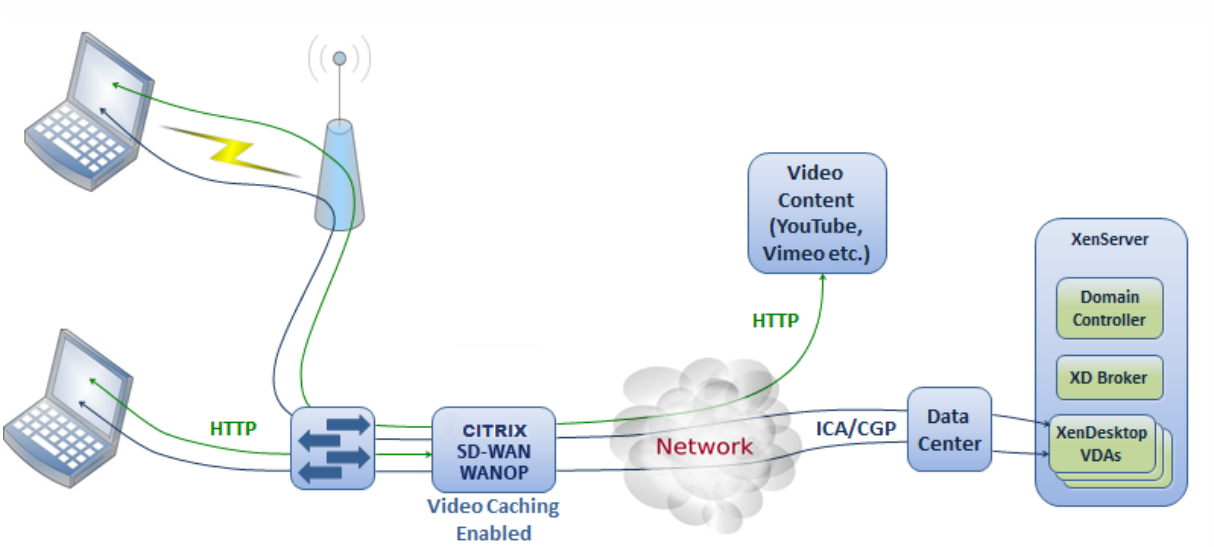
Accès aux succursales



Dans ce cas d'utilisation, les utilisateurs accèdent à Internet via les navigateurs Web sur leurs ordinateurs. Les demandes qui impliquent du contenu vidéo provenant d'un site activé, tel que Vimeo, sont mises en cache sur l'appliance Citrix SD-WAN WANOP local. Tout accès ultérieur à la même vidéo entraîne des accès au cache sur l'appliance locale, ce qui permet à la vidéo d'être livrée à la vitesse du réseau local et sans attendre le serveur distant.

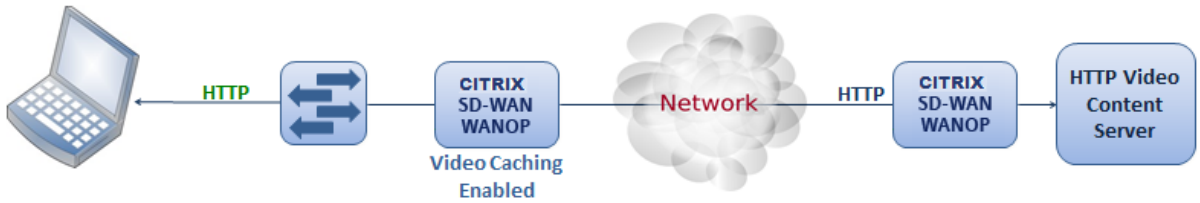
Contrairement aux autres fonctionnalités Citrix SD-WAN WANOP, qui accélèrent le trafic entre les périphériques jumelés, cette fonctionnalité est une opération à extrémité unique qui nécessite uniquement l'appliance locale, avec accès au site Web vidéo.

Filiale avec les utilisateurs Citrix Virtual Apps and Desktops utilisant la redirection Flash HDX MediaStream



La redirection flash HDX est une fonctionnalité de Citrix Virtual Apps and Desktops. Au lieu de rendre la vidéo sur l'affichage des bureaux virtuels distants à l'aide de l'Internet côté serveur ou du centre de données, les vidéos flash sont tunnelées vers le système local via cette fonctionnalité. La vidéo est diffusée en continu sur l'ordinateur client réel et est rendue sur le client réel, à l'aide de la succursale Internet. L'activation de la fonctionnalité de mise en cache vidéo sur l'appliance Citrix SD-WAN WANOP côté succursale peut offrir aux utilisateurs une expérience de visionnage considérablement améliorée. En outre, l'activation de la fonctionnalité réduit la bande passante requise pour les vidéos en streaming.

Serveur Web vidéo HTTP d'entreprise



Dans ce cas d'utilisation, les utilisateurs accèdent aux serveurs Web vidéo à partir du centre de données. Lorsque vous activez la fonctionnalité de mise en cache vidéo sur l'appliance Citrix SD-WAN

WANOP côté succursale, la demande utilisateur est envoyée à partir du cache de l'appliance Citrix SD-WAN côté succursale. Cela permet de réduire le trafic réseau vers l'appliance Citrix SD-WAN WANOP du centre de données. Par conséquent, la bande passante de l'appliance Citrix SD-WAN WANOP du centre de données peut être utilisée pour servir le trafic d'autres succursales.

Configurer la mise en cache de vidéo

April 23, 2021

Vous pouvez configurer la fonctionnalité de mise en cache vidéo via l'interface utilisateur graphique Citrix SD-WAN WANOP ou l'interface de ligne de commande. Par défaut, l'appliance est configurée pour mettre en cache les vidéos de YouTube et Vimeo. Youku, Metacafe et Dailymotion sont également configurés sur l'appliance par défaut. Tout ce que vous avez à faire est de les activer. Vous pouvez ajouter des sites Web vidéo, comme un site Web interne proposant des didacticiels vidéo ou d'autres informations.

> **Remarque**
>
> Mise en cache vidéo une fonctionnalité facultative qui n'est pas activée par défaut. Vous n'avez pas besoin de l'activer sauf si vous avez un volume important de trafic vidéo HTTP.

Conditions préalables

Pour configurer la mise en cache vidéo sur l'appliance, assurez-vous que les conditions préalables suivantes sont remplies :

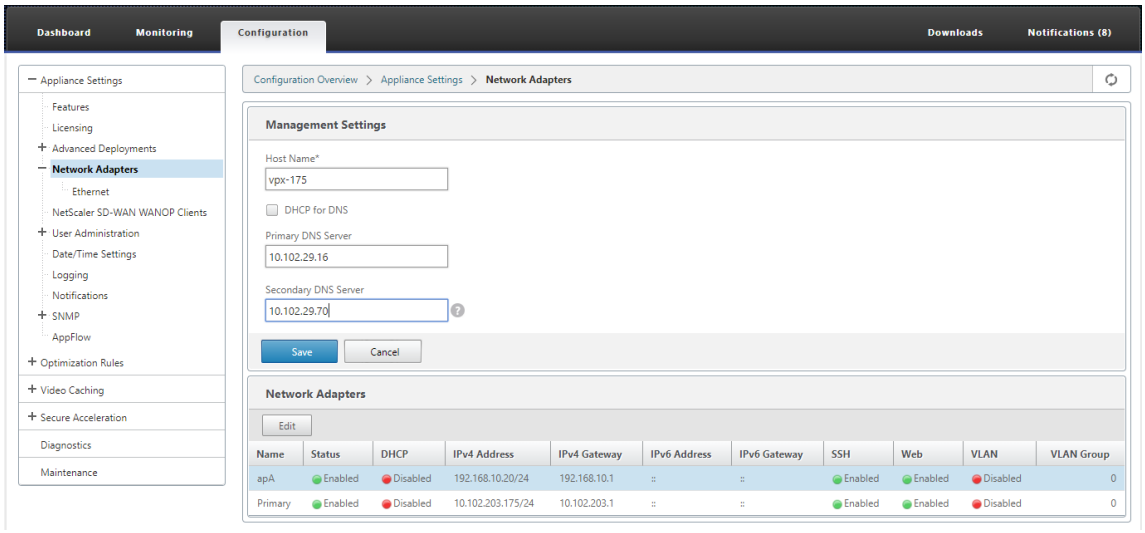
- Vous avez configuré l'adresse IP appropriée pour le port de pont accéléré que vous prévoyez d'utiliser pour la mise en cache vidéo.
- Vous pouvez effectuer un ping sur la passerelle apA/apB à partir de l'appliance.
- Les détails du serveur DNS sont exacts.
- L'appliance peut résoudre le nom DNS www.Citrix.com.
- L'adresse IP Citrix SD-WAN WANOP APX dispose d'un accès HTTP dans votre réseau d'entreprise.
- Si l'appliance est déployée entre les ports de jonction de deux périphériques réseau, vous devez spécifier l'ID VLAN avec l'adresse IP que l'appliance doit utiliser pour envoyer des requêtes HTTP sur la page Configuration réseau.
- Pour les **classes de service**Web (Internet)**et Web (privé)**, le paramètre **Stratégie d'accélération**ne doit pas être défini sur **Aucun**.

Activer la fonctionnalité de mise en cache vidéo

Avant de pouvoir commencer à utiliser la fonction de mise en cache vidéo, vous devez l'activer.

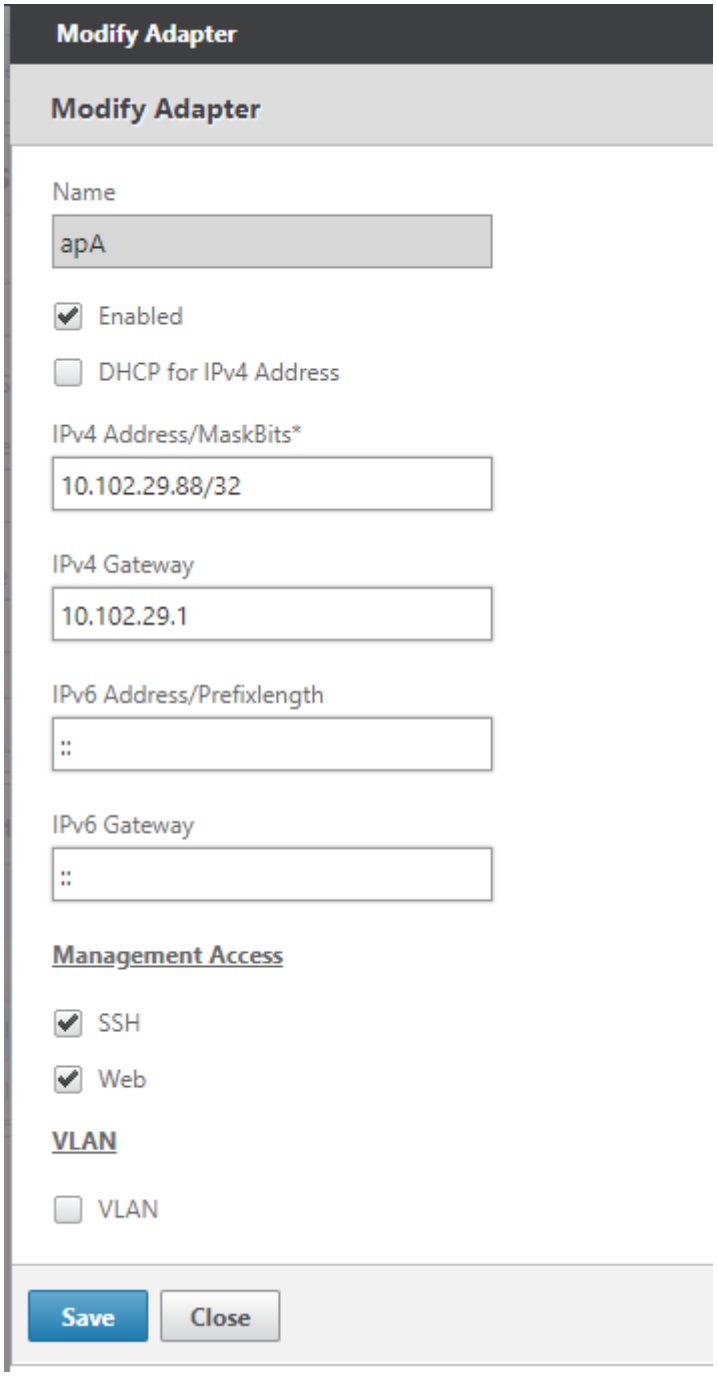
Pour activer la mise en cache vidéo :

1. Accédez à **Configuration** > **Paramètres de l'appliance** > **Cartes réseau**, sous la section **Paramètres de gestion**, vérifiez et vérifiez que les détails du serveur DNS principal sont exacts et que l'appliance est en mesure de résoudre le nom DNS. www.Citrix.com. Cliquez sur l'icône Modifier pour modifier les paramètres.



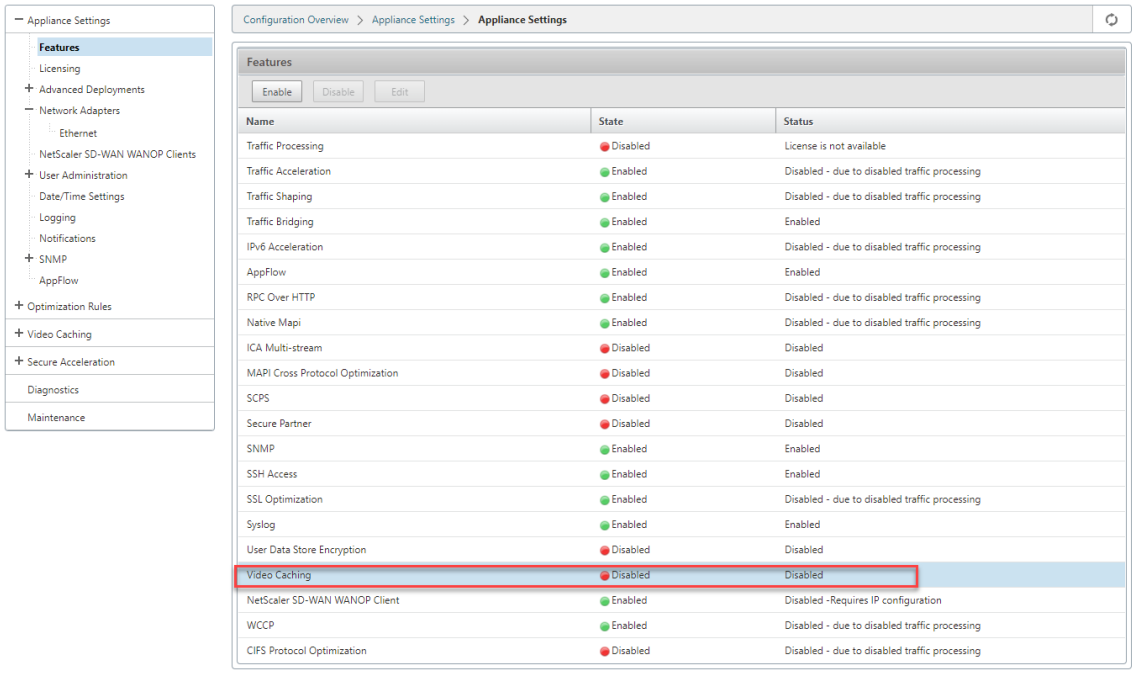
2. Accédez à **Configuration** > **Paramètres de l'appliance** > **Cartes réseau**. Dans la section **Cartes réseau**, sélectionnez une paire d'accélération (par exemple ApA) et clik **Edit**.

   Assurez-vous que les adresses IP, le masque réseau et les adresses IP de Gateway par défaut spécifiées pour la paire accélérée sont exactes.



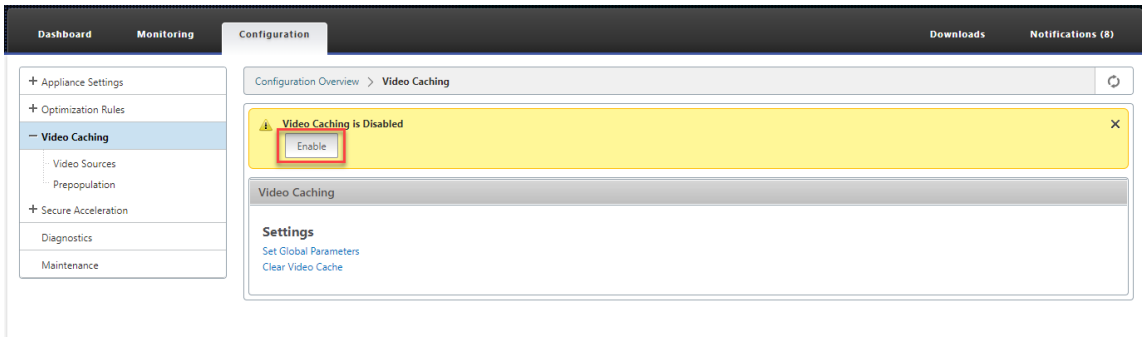
3. Accédez à la page **Configuration** > **Paramètres de l'appliance** > **Fonctionnalités** et activez la fonction de **mise en cache vidéo**.

   Une boîte de dialogue de confirmation apparaît, cliquez sur **Oui**.



> **Remarque**
>
> Le service redémarre et une nouvelle partition de mise en cache est créée. Si vous activez la fonctionnalité pour la première fois sur l'appliance, une nouvelle partition est créée en réduisant l'espace disque alloué à une autre compression basée sur le disque. L'historique de compression basé sur le disque est réinitialisé et les connexions existantes sont interrompues.

4. Vous pouvez également accéder à **Configuration** > **Règles d'optimisation** > Mise en **cache vidéo** et cliquer sur **Activer**.



Ajouter des sites vidéo

L'appliance est configurée pour mettre en cache les vidéos de YouTube et Vimeo et est partiellement configurée pour mettre en cache les vidéos de Youku, Metacafe et Dailymotion. Pour mettre en cache des vidéos de l'un des trois derniers sites, vous devez activer le site. Une vidéo d'un site Web activé

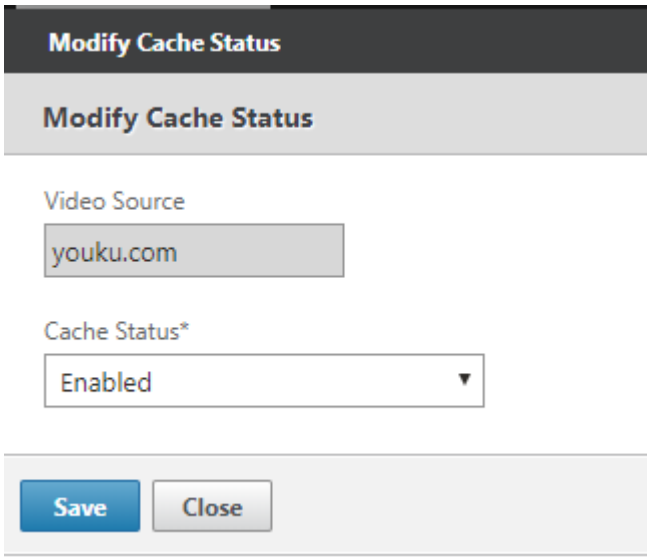
est mise en cache dès qu'un utilisateur y accède. Vous pouvez configurer des sites Web vidéo supplémentaires qui ne nécessitent pas de réécriture d'URL en ajoutant leurs noms d'hôte ou adresses IP à la liste Source vidéo de l'appliance. Vous pouvez également inclure des sites personnalisés qui ne disposent pas de mécanismes d'évitement de cache.

Vous devez activer ces sources vidéo avant que l'appliance puisse mettre en cache les vidéos de ces sources.

La fonctionnalité de mise en cache vidéo utilise des sources vidéo pour le flux de travail de configuration. Si vous configurez l'une des sources vidéo avec un nom d'hôte ou un site Web/nom d'hôte, l'appliance proxie tout le trafic HTTP qui circule via l'appliance. Toutefois, si vous configurez toutes les sources vidéo avec des adresses IP uniquement, l'appliance proxie et met en cache uniquement ces adresses IP. Que vous utilisiez des noms d'hôte ou des adresses IP, si votre organisation n'autorise pas l'accès aux sites Web YouTube, Vimeo, Dailymotion, Metacafe et Youku, assurez-vous de désactiver ces sources vidéo.

Pour activer une source vidéo :

1. Accédez à **Configuration** > **Règles d'optimisation** > **Mise en cache vidéo** > **Sources vidéo.**
2. Sélectionnez une source vidéo dans la liste, cliquez sur **Modifier**.

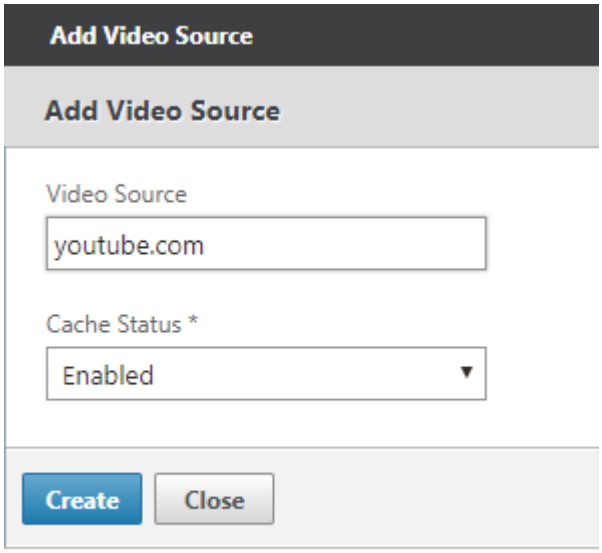


3. Dans la liste déroulante **État du cache**, sélectionnez **Activer** et cliquez sur **Enregistrer**.

Pour ajouter une source vidéo :

1. Accédez à **Configuration** > **Règles d'optimisation** > **Mise en cache vidéo** > **Sources vidéo**, cliquez sur **Ajouter.**
2. Dans le champ **Source vidéo**, tapez le nom du site Web ou l'adresse IP du serveur Web que vous souhaitez ajouter à la liste des sources vidéo.

3. Dans la liste **État du cache**, vérifiez que **Activé** est sélectionné. Vous pouvez sélectionner **Désactivé** dans cette liste si vous souhaitez activer la mise en cache vidéo pour ce site ultérieurement.



4. Cliquez sur **Créer**.

   Pour supprimer une source vidéo, sélectionnez-la dans la liste **Sources vidéo** et cliquez sur **Supprimer**.

Préremplissage de vidéo

April 9, 2021

Une appliance Citrix SD-WAN WANOP peut télécharger et mettre en cache des vidéos à partir de votre serveur vidéo interne avant que quiconque ne les voit. Cette fonctionnalité est utile lorsque vous voulez vous assurer que tous les utilisateurs bénéficient des mêmes avantages (par exemple lors de la lecture d'une vidéo d'auto-formation programmée à un moment précis). Vous pouvez planifier des URL statiques à partir desquelles vous souhaitez récupérer des vidéos.

Les vidéos récupérées sont stockées dans le cache vidéo. Dès qu'un utilisateur envoie une requête pour l'URL, la vidéo est servie à partir du cache, même pour le premier accès à la vidéo.

Pour récupérer des vidéos à l'avance, vous pouvez effectuer les tâches suivantes :

- Spécifiez une URL à partir de laquelle vous souhaitez mettre en cache les vidéos à l'avance.
- Programmer la date et l'heure auxquelles mettre en cache les vidéos.

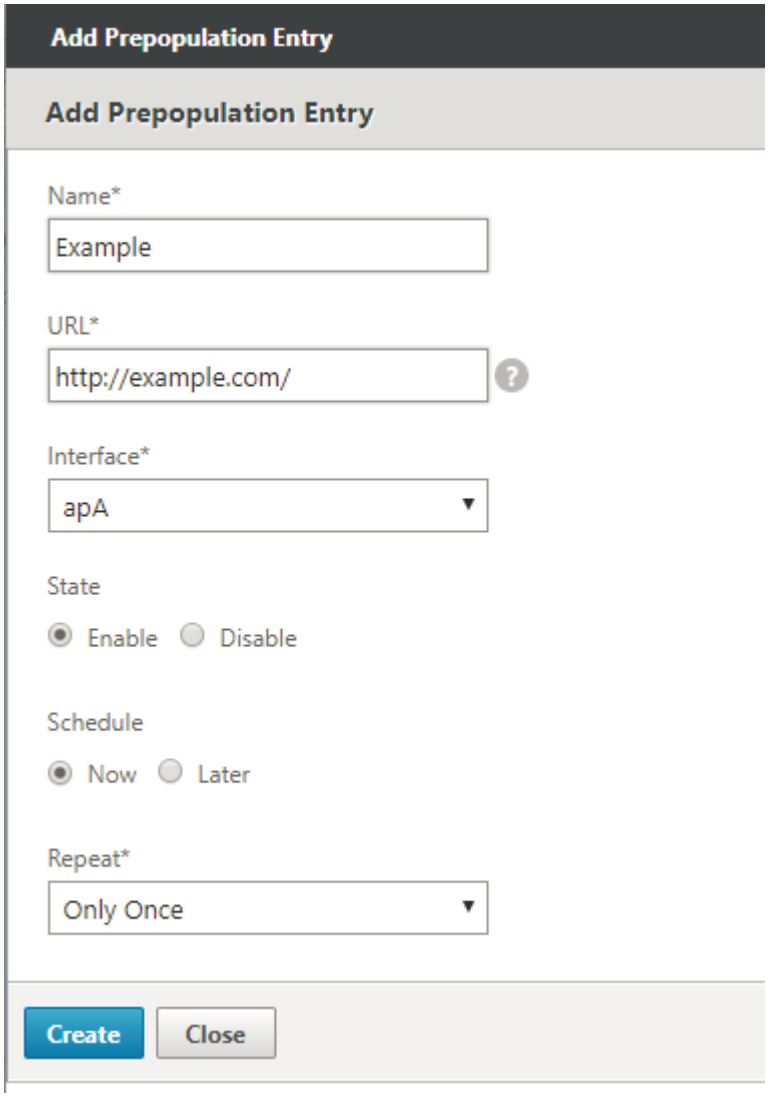
- Planifiez un intervalle auquel vous souhaitez mettre en cache les vidéos.
- Gérer les entrées que vous avez ajoutées à la liste.

Pour télécharger et mettre en cache une vidéo à l'avance, vous devez spécifier le chemin absolu de l'URL d'une vidéo spécifique ou d'un dossier vidéo sur lequel l'indexation de répertoires est activée.

> **Remarque**
>
> Si vous ajoutez simplement une entrée aux tâches de préremplissage vidéo, la vidéo associée est téléchargée et mise en cache. Cependant, lorsqu'un client accède à la vidéo, il est servi à partir du serveur vidéo et ne bénéficie pas d'avantages de mise en cache. Pour vous assurer que le client bénéficie des avantages de la mise en cache, vous devez ajouter le serveur vidéo ou l'adresse IP utilisée dans la tâche de préremplissage à la liste des sources vidéo.

Pour ajouter à l'avance une URL à la mise en cache des vidéos :

1. Accédez à **Configuration** > **Mise en cache vidéo** > **Préremplissage**, puis cliquez sur **Ajouter**.



2. Dans le champ **Nom**, spécifiez un nom que vous pouvez utiliser pour identifier l'entrée de préremplissage.
3. Dans le champ **URL**, spécifiez l'URL à partir de laquelle vous souhaitez mettre en cache une ou plusieurs vidéos. L'URL peut être pour une vidéo spécifique ou un serveur vidéo. Assurez-vous de spécifier une URL complète ou un dossier vidéo.
4. Dans le champ **Interface**, sélectionnez le port de pont accéléré pour télécharger des vidéos à partir de l'URL.
5. Définissez **Étatsur Activer** pour recevoir des informations d'état. Les différents états et leur description sont prouvés dans le tableau ci-dessous.
6. Vous pouvez démarrer immédiatement le téléchargement et la mise en cache des vidéos à partir de l'URL vers l'appliance, ou les télécharger à une heure planifiée.
7. Cliquez sur **Créer**.

Le tableau suivant décrit les messages d'état :

État	Description
Configuré	Récupère la vidéo pour la mise en cache avant que la première vue ne soit configurée pour l'URL et qu'une nouvelle tâche soit ajoutée.
Erreur de délai d'expiration de connexion	La connexion au serveur a expiré et il n'y a pas de réponse du serveur.
Erreur 301 - Déplacé de façon permanente	La vidéo à télécharger et à mettre en cache a été déplacée de façon permanente vers un autre emplacement.
Erreur 403 - Interdit	L'accès à la vidéo à télécharger et à mettre en cache est refusé.
Erreur 404 - introuvable	La vidéo à télécharger et à mettre en cache n'est pas disponible sur le lien fourni.
Erreur 504 : Serveur inaccessible	L'URL que vous avez spécifiée n'est pas accessible.
Fichier (s) « x » téléchargé (s) avec succès	Téléchargement réussi pour l'URL, et le nombre « x » de fichiers multimédias sont téléchargés dans le cache.
Impossible de télécharger « x » depuis les fichiers « y »	Le téléchargement de certains fichiers multimédias à partir de l'URL a échoué.
Impossible de télécharger x fichiers	Impossible de télécharger un fichier multimédia à partir de l'URL.
Téléchargement terminé	Le traitement de toutes les URL de cette entrée est terminé.
Téléchargement en cours	Le téléchargement est en cours.
Début	L'appliance a commencé à télécharger des fichiers multimédias à partir de l'URL.
Suppression de cette entrée	L'entrée est supprimée de la liste des URL.
Échec de l'obtention de la liste du répertoire	Impossible d'obtenir la liste à partir du répertoire distant que vous avez spécifié.
Entrée supprimée par opération de vidage du cache	L'entrée a été purgée par l'opération d'effacement du cache.
Mise à jour de l'état	L'appliance met à jour l'état de l'entrée.
Temps de planification écoulé	L'heure planifiée du téléchargement de l'objet distant est passée.

État	Description
Fichiers « x » /"y » dans le cache	Lors de l'actualisation de l'état d'une entrée, l'appliance a constaté que le nombre « x » de fichiers par rapport au nombre « y » de fichiers existe dans le cache.
Interface ap"X"désactivée pour la mise en cache vidéo	L'interface de pont ap"X"n'est pas activée pour la mise en cache vidéo.
Actualisation de l'état	Le statut de l'entrée est en cours d'actualisation.
Erreur 0	Une erreur inconnue s'est produite lors du téléchargement des vidéos. Contactez l'équipe du support technique Citrix pour résoudre le problème.

Gérer le préremplissage de la mise en cache vidéo

Vous pouvez gérer le préremplissage de mise en cache vidéo pour contrôler la façon dont vous souhaitez télécharger et mettre en cache les vidéos à partir des URL. Vous pouvez effectuer les tâches suivantes pour gérer le préremplissage de mise en cache vidéo :

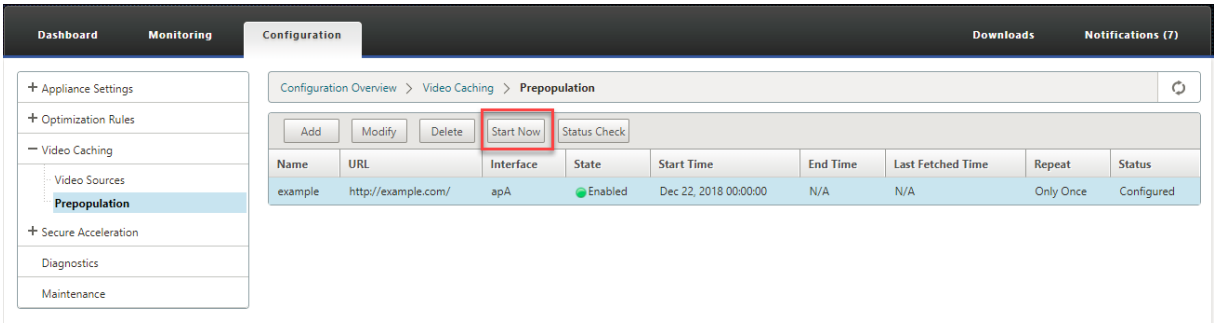
- Commencez à télécharger des vidéos avant ou après la date et l'heure prévues.
- Mettre à jour l'URL d'une entrée.
- Désactiver la mise en cache des vidéos à partir d'une entrée d'URL.
- Planifier la mise en cache des vidéos à partir d'une entrée d'URL.
- Mettre à jour une interface pour une entrée d'URL.
- Actualisez l'état d'une entrée d'URL.
- Supprimer une entrée d'URL.

L'organigramme suivant montre le contrôle du flux des processus suivis lors de la gestion des diverses activités de la fonction de prépopulation vidéo.

Télécharger des vidéos

Si des problèmes techniques avec un site Web ou l'URL que vous avez ajoutée interfèrent avec le téléchargement et la mise en cache planifiés, vous pouvez commencer le téléchargement et la mise en cache des vidéos si nécessaire à tout moment.

Pour télécharger et mettre en cache immédiatement une vidéo, accédez à **Configuration** > **Mise en cache vidéo** > **Prépopulation**, sélectionnez l'entrée de la vidéo à mettre en cache, puis cliquez sur **Démarrer maintenant**. La mise à jour de l'état de la vidéo prend environ une minute.



Après avoir cliqué sur Démarrer maintenant, la colonne Statut affiche l'état des téléchargements vidéo à partir de l'URL.

Mettre à jour l'URL d'une entrée de prépopulation

Après avoir ajouté une URL à partir de laquelle télécharger et mettre en cache la vidéo à l'avance, vous pouvez affiner l'URL pour obtenir des résultats optimaux, par exemple en reconfigurant l'URL lorsque l'emplacement des vidéos change ou le nom du fichier multimédia est modifié dans la source.

Pour mettre à jour une URL :

1. Accédez à la page **Configuration** > **Mise en cache vidéo** > **Prépopulation**.
2. Sélectionnez l'entrée à mettre à jour et cliquez sur **Modifier**.
3. Dans le champ URL, spécifiez la nouvelle URL.
4. Cliquez sur **OK**.

Désactiver la mise en cache des vidéos à partir d'une URL dans une entrée de prépopulation

Si vous souhaitez préremplir périodiquement le cache avec des vidéos à partir d'une URL donnée, vous n'avez pas besoin de supprimer l'entrée. Vous pouvez le désactiver, puis l'activer si nécessaire.

Pour désactiver une entrée :

1. Accédez à **la page Configuration** > **Mise en cache vidéo** > **Prépopulation**.
2. Sélectionnez l'entrée à mettre à jour et cliquez sur **Modifier**.
3. Dans État, sélectionnez l'option **Désactiver**.
4. Cliquez sur **OK**.

Planifier la mise en cache des vidéos à partir d'une URL dans une entrée de prépopulation

Vous pouvez planifier la date et l'heure auxquelles vous souhaitez commencer le téléchargement et la mise en cache des vidéos depuis l'URL vers l'appliance. Par exemple, vous pouvez chercher des vidéos juste avant de vous attendre à ce que les utilisateurs commencent à y accéder. Cela permet non seulement d'économiser de l'espace disque, mais aussi de mettre les dernières versions des vidéos dans le cache.

Pour planifier la mise en cache à partir d'une URL :

1. Accédez à **la page Configuration** > **Mise en cache vidéo** > **Prépopulation**.
2. Sélectionnez l'entrée à mettre à jour et cliquez sur **Modifier**.
3. Dans **Planifier**, sélectionnez l'option **Plus tard**.
4. Dans le champ **Début**, spécifiez la date et l'heure auxquelles vous souhaitez télécharger des vidéos à partir de l'URL. Le format de la date et de l'heure est AAAA-MM-JJ HH:MM:SS.
5. Dans la liste **Répéter**, sélectionnez la fréquence de téléchargement et de mise en cache des vidéos. Les options disponibles sont :
    - **Only Once** : téléchargez les vidéos à partir de l'URL une seule fois, à la date et à l'heure prévues.
    - **Tous les jours** : téléchargez des vidéos depuis l'URL tous les jours, en commençant par la date et l'heure prévues. Le téléchargement commence tous les jours à l'heure de début que vous spécifiez.
    - **Hebdomadaire** : téléchargez des vidéos à partir de l'URL une fois par semaine, en commençant par la date et l'heure prévues. Le téléchargement commence chaque semaine le jour et l'heure que vous spécifiez.
    - **Mensuel** : Téléchargez des vidéos à partir de l'URL une fois par mois, en commençant par la date et l'heure prévues. Le téléchargement commence tous les mois le jour et l'heure que vous spécifiez.
6. Cliquez sur **OK**.

Mettre à jour une interface dans une entrée d'URL

Si vous avez configuré plusieurs liens sur le réseau, vous pouvez utiliser un lien particulier pour télécharger des vidéos, en raison d'une meilleure connectivité réseau. Pour configurer plusieurs liens, vous utilisez les ports de pont disponibles, tels que les ports pontés ApA et apB. Vous pouvez utiliser ces ports pour télécharger des vidéos pour une entrée d'URL.

Pour mettre à jour une interface pour une entrée d'URL :

1. Accédez à **Configuration** > **Mise en cache vidéo** > **Prépopulation**.
2. Sélectionnez l'entrée à mettre à jour. puis cliquez sur **Modifier**.
3. Dans la liste **Interface**, sélectionnez l'interface que vous souhaitez utiliser pour l'entrée URL. La liste affiche les interfaces disponibles et configurées sur l'appliance.
4. Cliquez sur **OK**.

Actualiser l'état d'une entrée d'URL

Au fil du temps, l'état des vidéos mises en cache peut changer. La vérification périodique de l'état de l'entrée permet de s'assurer que les utilisateurs n'obtiennent pas de résultats inattendus lors de l'accès aux vidéos.

Pour vérifier le dernier état des vidéos mises en cache à partir d'une URL :

1. Accédez à **Configuration** > **Mise en cache vidéo** > **Prépopulation**.
2. Sélectionnez l'entrée pour laquelle vous souhaitez actualiser l'état des vidéos mises en cache.
3. Cliquez sur **Vérification de l'état**.

Supprimer une entrée d'URL

Si vous n'avez pas besoin d'une entrée d'URL, vous pouvez supprimer si de la liste. Pour supprimer une entrée URL, sélectionnez-la et cliquez sur **Supprimer**.

> **Remarque**
>
> Lorsque vous supprimez une tâche de préremplissage vidéo de la liste, elle supprime également les objets vidéo associés du cache.

Vérifier la mise en cache de vidéo

April 9, 2021

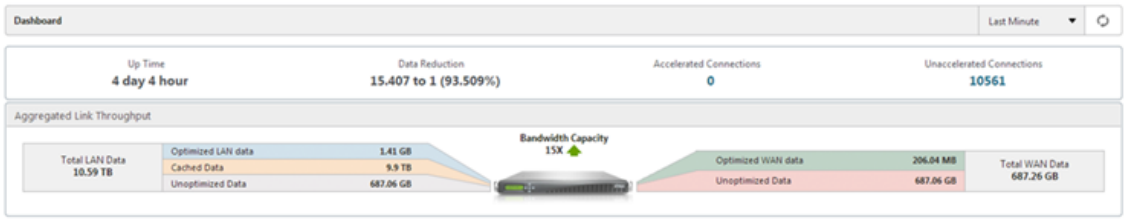
Les graphiques et les données de la page Surveillance, de la page Tableau de bord et de la page Utilisation vous aident à évaluer les avantages de votre configuration de mise en cache vidéo. Le ratio de réduction des données résultant de la mise en cache vidéo (similaire au taux de compression global) est affiché sur le Tableau de bord, sur la page de surveillance de la mise en cache vidéo et sur la page

Graphique Utilisation. En outre, le survol du ratio de réduction des données sur la page Tableau de bord affiche le pourcentage d'avantages de mise en cache ainsi que le pourcentage d'avantages de compression sur les plates-formes prises en charge.

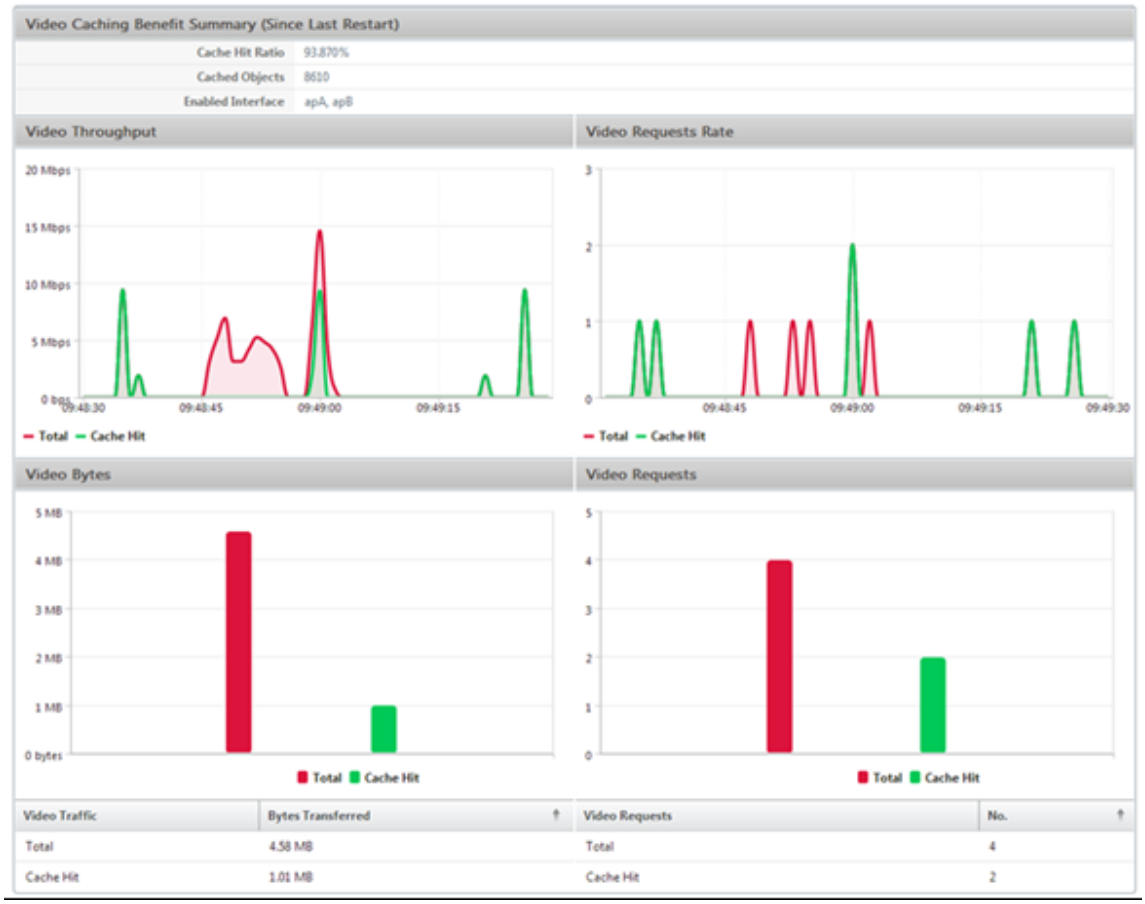
Le but de la mise en cache n'est pas seulement d'économiser la bande passante, mais aussi d'augmenter les performances, de réduire la charge sur les serveurs vidéo et de réduire l'impact de la congestion réseau.

Les économies estimées de bande passante WAN résultant de la mise en cache vidéo sont affichées comme suit :

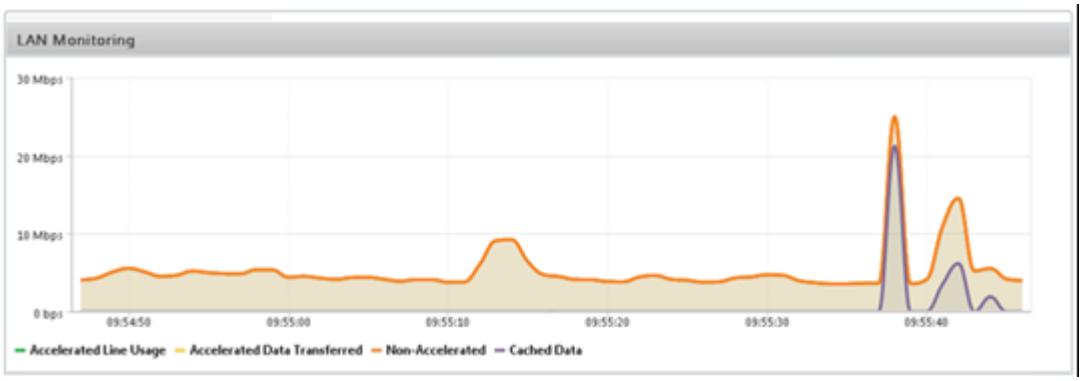
- Sur la page Tableau de bord, vous pouvez afficher l'avantage de mise en cache, sous forme de pourcentage, en plaçant le curseur sur le champ Réduction des données du Tableau de bord. Vous pouvez également afficher les octets servis à partir du cache (données mises en cache) sous Débit de lien agrégé.



- Sur la page **Surveillance** > **Mise en cache vidéo**, vous pouvez afficher le nombre d'objets mis en cache et le ratio d'accès au cache (en pourcentage). La barre et les graphiques temporelles affichent le nombre de requêtes et d'octets servis à partir du cache sur 1 minute, 1 heure, 1 jour, 1 semaine et 1 mois. Ces données sont également affichées sous forme de tableau sous le graphique.

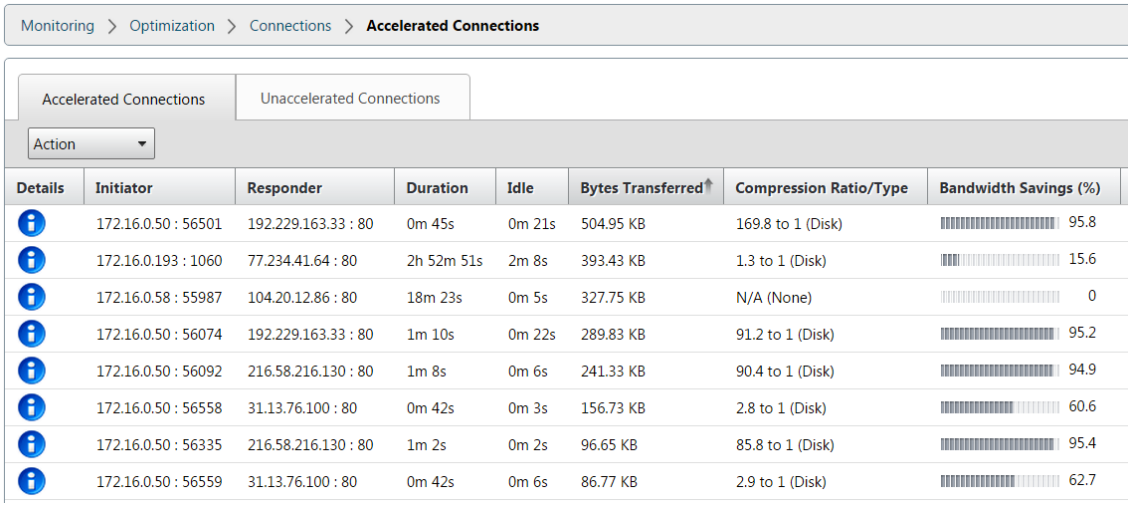


- Sur la page **Surveillance** > **Optimisation** > **Graphique d'utilisation**, vous pouvez afficher les données mises en cache dans le graphique Surveillance du réseau local.



- Sur la page **Surveillance** > **Mise en cache vidéo** > **Liste desétats HTTP**, vous pouvez surveiller le comportement amélioré du cache. Cette page indique l'état des connexions HTTP par rapport à la mise en cache vidéo.
- Sur la page **Surveillance** > **Optimisation** > **Connexions**, vous pouvez afficher les connexions mises en cache sous l'onglet Connexions accélérées. Les appels de cache et les échecs de cache sont affichés ici. Les connexions de cache sont affichées ici même si elles ne sont pas accélérées.

Autrement dit, les connexions mises en cache sont affichées ici même si un partenaire Citrix SD-WAN WANOP n'est pas impliqué dans la connexion. La colonne**Économies de bande passante** (%) affiche un graphique à barres indiquant la quantité de bande passante WAN enregistrée par la transaction, que ce soit par mise en cache ou compression. Alors que le but de la mise en cache et de la compression est d'augmenter la vitesse et la facilité d'utilisation et non de réduire l'utilisation de la bande passante, les augmentations de la vitesse et de la facilité d'utilisation sont souvent liées à la réduction de la bande passante. Autrement dit, une économie de bande passante de 90% implique une augmentation de vitesse 10x.



Details	Initiator	Responder	Duration	Idle	Bytes Transferred	Compression Ratio/Type	Bandwidth Savings (%)
	172.16.0.50 : 56501	192.229.163.33 : 80	0m 45s	0m 21s	504.95 KB	169.8 to 1 (Disk)	95.8
	172.16.0.193 : 1060	77.234.41.64 : 80	2h 52m 51s	2m 8s	393.43 KB	1.3 to 1 (Disk)	15.6
	172.16.0.58 : 55987	104.20.12.86 : 80	18m 23s	0m 5s	327.75 KB	N/A (None)	0
	172.16.0.50 : 56074	192.229.163.33 : 80	1m 10s	0m 22s	289.83 KB	91.2 to 1 (Disk)	95.2
	172.16.0.50 : 56092	216.58.216.130 : 80	1m 8s	0m 6s	241.33 KB	90.4 to 1 (Disk)	94.9
	172.16.0.50 : 56558	31.13.76.100 : 80	0m 42s	0m 3s	156.73 KB	2.8 to 1 (Disk)	60.6
	172.16.0.50 : 56335	216.58.216.130 : 80	1m 2s	0m 2s	96.65 KB	85.8 to 1 (Disk)	95.4
	172.16.0.50 : 56559	31.13.76.100 : 80	0m 42s	0m 6s	86.77 KB	2.9 to 1 (Disk)	62.7

Gérer les sources de mise en cache vidéo

April 9, 2021

Vous pouvez gérer vos sources vidéo soit globalement, en configurant des paramètres globaux, soit individuellement, en modifiant l'état d'une source vidéo.

Configurer les paramètres globaux

Les paramètres globaux vous permettent de configurer la fonctionnalité au niveau de l'appliance. Indépendamment des sources vidéo que vous avez ajoutées, ces paramètres s'appliquent à l'ensemble de la fonction de mise en cache vidéo de l'appliance. Vous pouvez :

- Configurer la taille maximale des objets mis en cache
- Configurer un suffixe DNS
- Configurer les ports de mise en cache

- Mettre à jour le fichier de stratégie de mise en cache vidéo

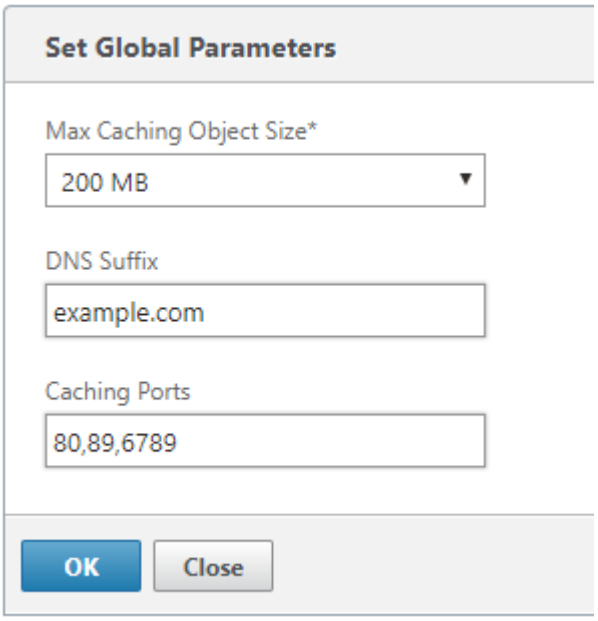
Vous pouvez configurer une taille maximale pour les objets mis en cache. Un objet supérieur à cette limite n'est pas mis en cache. Par défaut, la taille maximale de l'objet de mise en cache est de 100 Mo.

Pour les URL qui ne contiennent pas de noms de domaine complets et qui nécessitent l'ajout de suffixes de nom de domaine au nom d'hôte du serveur vidéo, l'ajout d'un nom de domaine par défaut est nécessaire pour obtenir une réponse du serveur. Par exemple, lorsque vous accédez à la vidéo `http://training/CitrixSD-WANWANOP\\_VideoCaching.mp4`, l'appliance doit traduire l'URL vers `http://training.example.com/CitrixSD-WANWANOP\\_VideoCaching.mp4`. Dans ce cas, vous devez spécifier example.com comme suffixe de nom de domaine.

La fonction de mise en cache vidéo nécessite un numéro de port pour le serveur vidéo HTTP. La valeur par défaut est le port 80. Si votre serveur vidéo HTTP utilise un port autre que ce port HTTP bien connu, vous devez ajouter le numéro de port à la liste des ports de mise en cache.

Pour configurer les paramètres globaux pour la mise en cache vidéo :

1. Accédez à **Configuration** > **Mise en cache vidéo** > **Définir les paramètres globaux.**



2. Dans le champ **MaxCaching Object Size**, définissez la taille maximale des objets mis en cache.

   Sélectionnez une valeur parmi les limites disponibles. Un objet supérieur à cette limite n'est pas mis en cache.

3. Dans le champ **Suffixe DNS**, entrez un nom de domaine à ajouter aux URL qui ne contiennent pas de noms de domaine complets et qui nécessitent l'ajout de suffixes de nom de domaine au nom d'hôte du serveur vidéo.

4. Dans le champ **Ports de mise en cache**, tapez le port du serveur vidéo HTTP pour l'ajouter à la liste des ports de mise en cache. Vous pouvez également ajouter plusieurs numéros de port séparés par des virgules.
5. Cliquez sur **OK**.

L'appliance utilise 10 % de l'espace disque alloué à des fins de gestion. Lorsque l'utilisation du disque atteint 90 % de l'espace disque alloué, cela indique que le disque est plein. Pour mettre en cache davantage d'objets vidéo, l'appliance supprime les objets les moins utilisés du cache vidéo. Vous n'avez pas besoin d'effacer le cache sauf si le cache sert des objets vidéo obsolètes.

Pour effacer le cache vidéo, accédez à **Configuration** > Mise en **cache vidéo**, puis cliquez sur **Effacer le cache vidéo**.

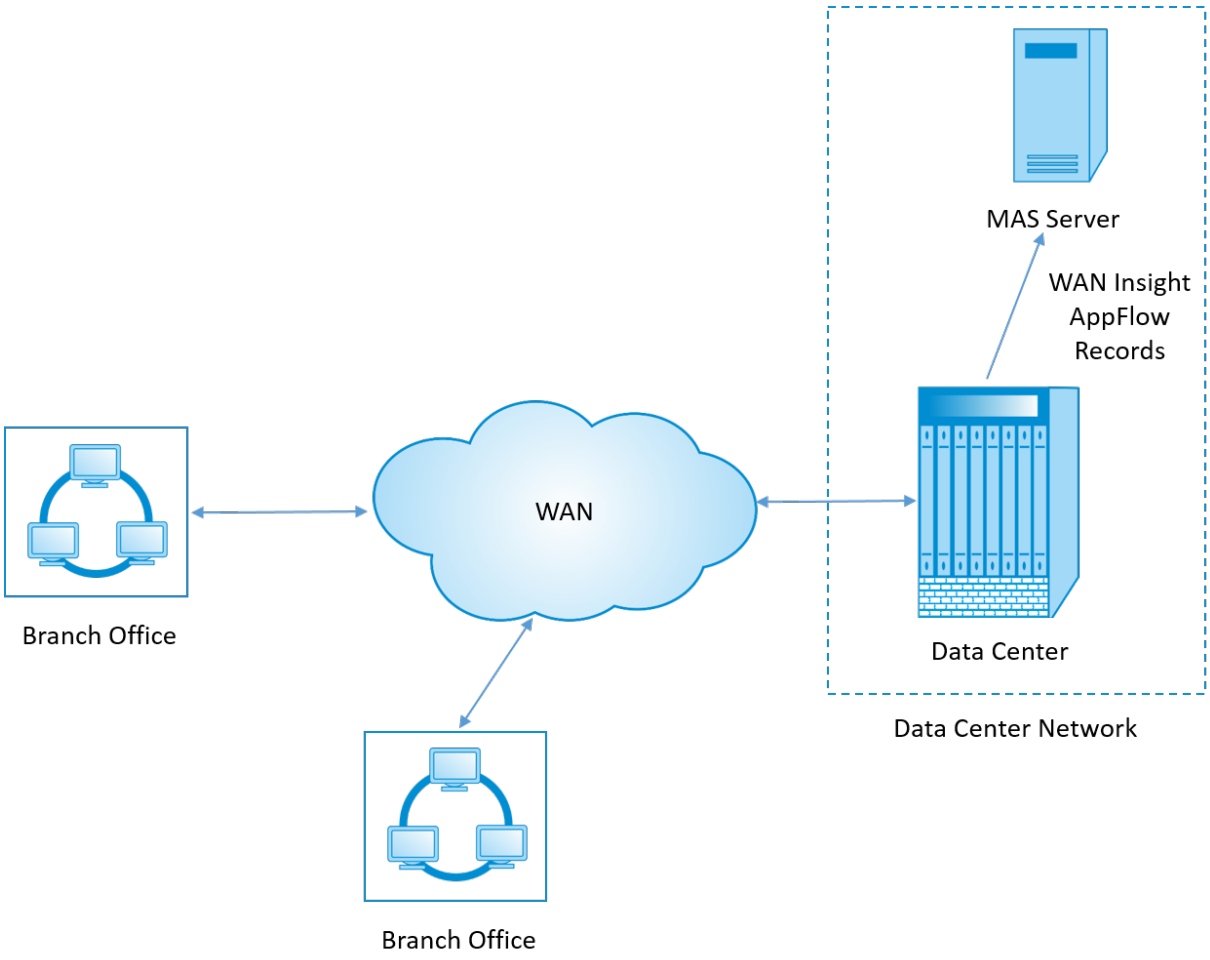
WAN Insight

December 14, 2022

Les appliances Citrix SD-WAN WANOP optimisent la fourniture d'un grand nombre d'applications via le WAN, en améliorant l'efficacité du flux de données sur le réseau entre le centre de données et les sites de succursale. L'analyse WAN Insight permet aux administrateurs de surveiller facilement le trafic WAN accéléré et non accéléré qui circule entre le centre de données et les appliances d'optimisation WAN des succursales. WAN Insight fournit une visibilité sur les clients, les applications et les succursales sur le réseau, pour aider à résoudre efficacement les problèmes réseau. Les rapports actifs et historiques vous permettent de résoudre les problèmes de manière proactive, le cas échéant.

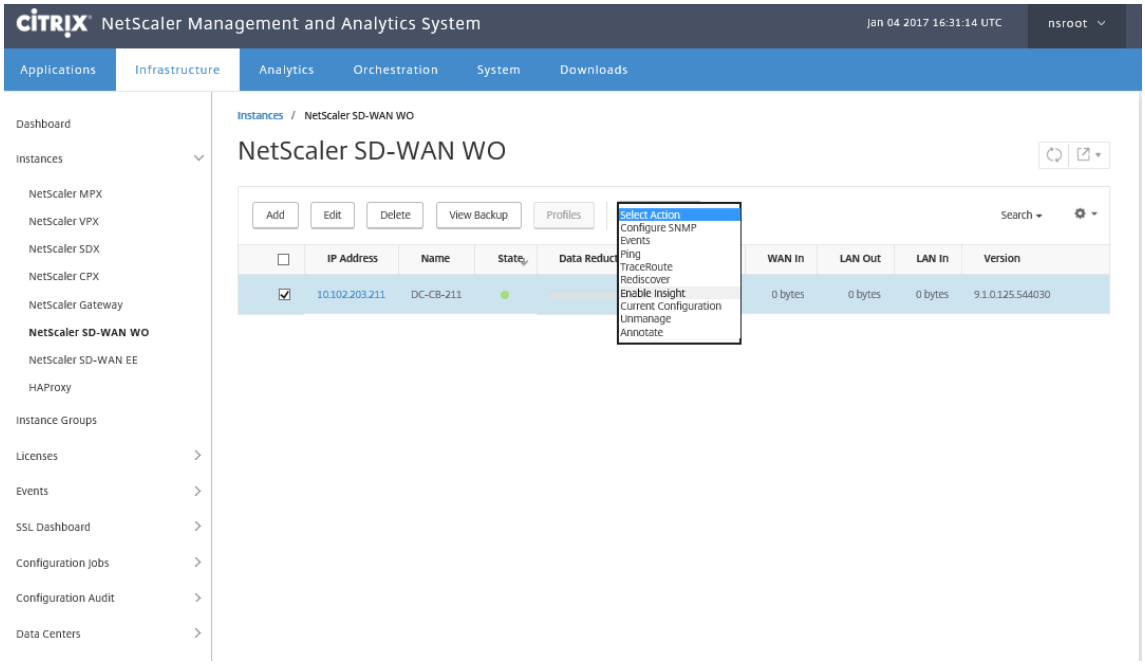
L'activation de l'analyse sur l'appliance d'optimisation du réseau étendu du centre de données permet à Citrix Application Delivery Management (ADM) de collecter des données et de fournir des rapports et des statistiques pour le centre de données et les appliances d'optimisation du réseau étendu des succursales.

> **Remarque**
>
> Pour plus d'informations sur l'ajout d'une instance, reportez-vous à la section Ajouter des instances à Citrix ADM.



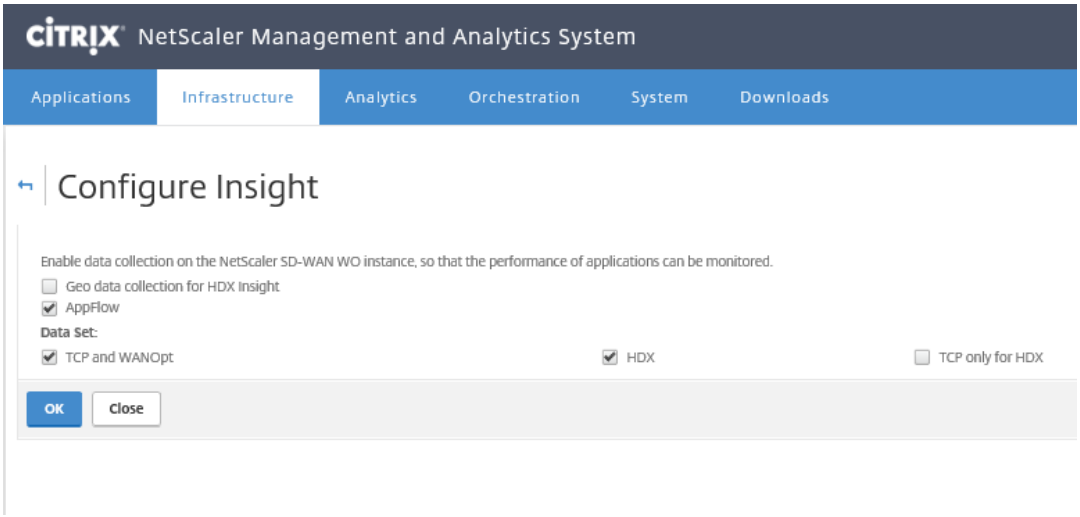
Pour activer l'analyse sur l'appliance d'optimisation WAN :

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM (par exemple, http://192.168.100.1).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à**Infrastructure** > **Instances** > **Citrix SD-WAN WO**, puis sélectionnez l'appliance d'optimisation WAN du centre de données.



4. Dans la liste déroulante **Action**, sélectionnez **Activer Insight**.
5. Sélectionnez les paramètres suivants selon les besoins :

   - **Collecte de données géographiques pour HDX Insight** : partage l'adresse IP du client avec l'API Google Geo.
   - **AppFlow** : Commence à collecter des données à partir d'instances d'optimisation WAN.
   - **TCP et WanOpt** : fournit des rapports TCP et WanOpt Insight.
   - **HDX** : fournit des rapports HDX Insight.
   - **TCP uniquement pour HDX** : fournit TCP uniquement pour les rapports HDX Insight.



6. Cliquez sur **OK**.

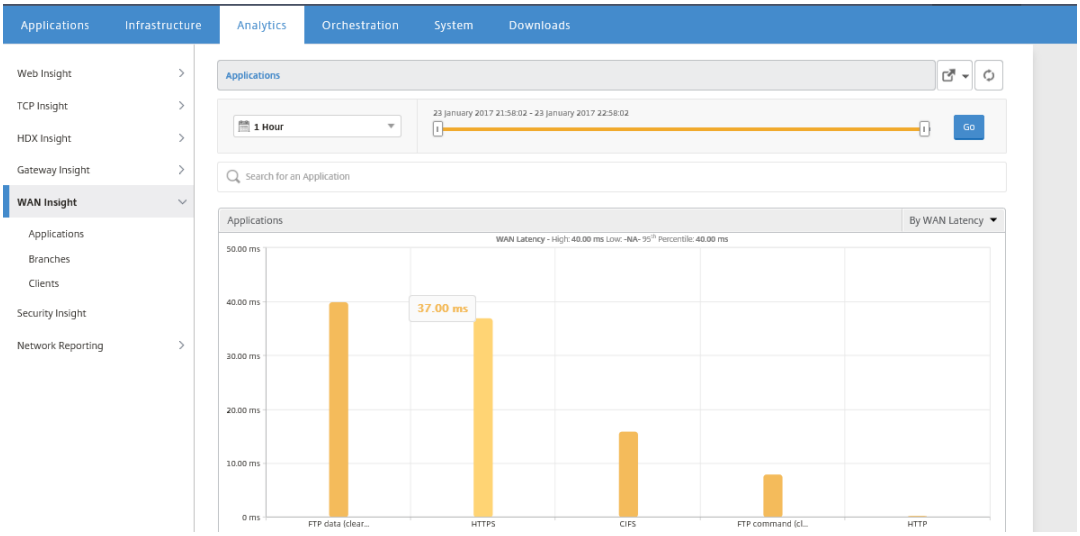
Pour afficher les rapports WAN Insight :

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM (par exemple, http://192.168.100.1).
2. Dans les champs **Nom d'utilisateur** et **Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Accédez à **Analytics** > **WAN Insight**.

> **Remarque**
>
> L'option WAN Insight n'est visible qu'après l'ajout d'une instance WO SD-WAN à Citrix ADM.

Vous pouvez consulter les rapports suivants :

- **Applications** : affiche les statistiques d'utilisation et de performances de toutes les applications pour la durée sélectionnée.
- **Branches** : affiche les statistiques d'utilisation et de performances de toutes les appliances de branche d'optimisation WAN.
- **Clients :** affiche les statistiques d'utilisation et de performances de tous les clients accédant aux appliances d'optimisation WAN, dans chaque branche.



Les mesures suivantes sont affichées :
Mesure	**Description**
———-	———–
Connexions accélérées actives	Nombre de connexions WAN actives qui sont accélérées.
Connexions actives non accélérées	Nombre de connexions WAN actives qui ne sont pas accélérées.
Latence WAN	Délai, en millisecondes, que l'utilisateur rencontre lors de l'interaction

avec une application. |
Taux de compression	Rapport de compression des données entre la succursale et les appliances de centre de données pour la durée sélectionnée.
Paquets envoyés	Nombre de paquets envoyés par l'appliance d'optimisation WAN sur le réseau pendant la durée sélectionnée.
Paquets reçus	Nombre de paquets reçus du réseau par l'appliance d'optimisation WAN pendant la durée sélectionnée.
Octets envoyés sur le WAN	Nombre d'octets envoyés par l'appliance d'optimisation WAN Citrix sur le WAN pendant la durée sélectionnée.
Octets reçus sur le WAN	Nombre d'octets que l'appliance d'optimisation WAN a reçus du WAN pendant la durée sélectionnée.
RTO LAN	Nombre de fois que l'appliance d'optimisation WAN a expiré la retransmission vers le réseau local pendant la durée sélectionnée.
RTO WAN	Nombre de fois que l'appliance d'optimisation WAN a expiré la retransmission vers le WAN pendant la durée sélectionnée.
Retransmission de paquets (LAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau LAN pendant la durée sélectionnée.
Retransmission de paquets (WAN)	Nombre de paquets que l'appliance d'optimisation WAN a retransmis au réseau WAN pendant la durée sélectionnée.

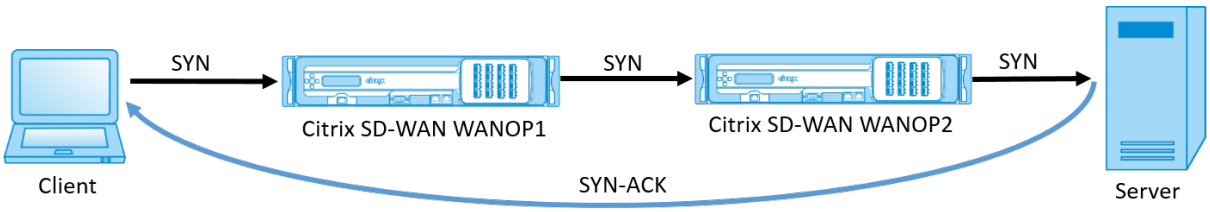
Routage asymétrique

April 9, 2021

Dans le réseau Citrix SD-WAN WANOP, le routage asymétrique se produit lorsque les paquets circulant d'un client à un serveur ou d'un serveur à un client pour la même connexion TCP ne passent pas par l'une ou les deux appliances WANOP côté client et côté serveur. Les cas d'asymétrie suivants sont observés.

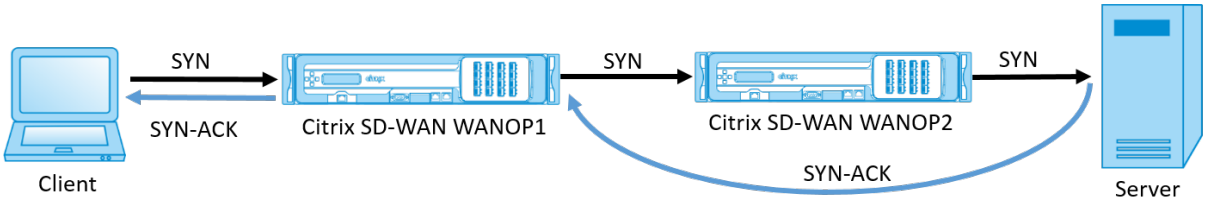
Asymétrie complète :

Une asymétrie complète se produit lorsque les paquets circulent d'un client vers le serveur via les appliances Citrix SD-WAN WANOP côté client et côté serveur. Toutefois, sur le chemin de retour du serveur au client, les paquets prennent une route différente en contournant les appliances Citrix SD-WAN WANOP.



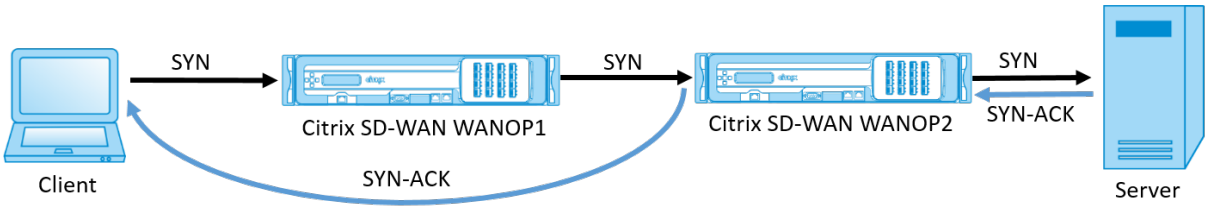
Asymétrie côté serveur :

L'asymétrie côté serveur se produit lorsque les paquets circulent d'un client vers le serveur via les appliances Citrix SD-WAN WANOP côté client et côté serveur. Toutefois, sur le chemin de retour, les paquets contournent l'appliance Citrix SD-WAN WANOP côté serveur, mais traversent l'appliance Citrix SD-WAN côté client.



Asymétrie côté client :

L'asymétrie côté client se produit lorsque les paquets circulent d'un client vers le serveur via les appliances Citrix SD-WAN WANOP côté client et côté serveur. Toutefois, sur le chemin de retour, les paquets traversent l'appliance Citrix SD-WAN WANOP côté serveur mais contournent l'appliance Citrix SD-WAN côté client.



Gestion de l'asymétrie dans le réseau Citrix SD-WAN WANOP

Dans le réseau Citrix SD-WAN WANOP, lorsque l'asymétrie complète se produit, la connexion TCP est réinitialisée. Pour éviter la rupture de connexion TCP et continuer à envoyer du trafic non accéléré, une liste de connexions asymétriques est introduite dans SD-WAN WANOP 10.1. Cette fonctionnalité est désactivée par défaut ; vous pouvez l'activer sur les appliances WANOP SD-WAN côté client et côté serveur.

Lors de la détection d'une connexion asymétrique pour la première fois, la connexion TCP entre le client et le serveur est réinitialisée et une entrée du tuple est effectuée dans la liste des connexions asymétriques. Le tuple se compose de l'adresse IP du client et de l'adresse IP du serveur. Les connexions ultérieures du tuple passent par non accéléré. Le tuple de connexion reste dans la liste des

connexions asymétriques pendant une période d'attente par défaut de quatre heures ou jusqu'à ce que la symétrie soit détectée. La transmission non accélérée est effective jusqu'à ce que le délai d'expiration se produise ou jusqu'à ce que l'appliance détecte dynamiquement que l'asymétrie n'est plus présente.

Lorsque l'asymétrie côté client ou l'asymétrie côté serveur est détectée, la connexion TCP est conservée et les paquets passent par l'appliance Citrix SD-WAN WANOP sans accélération, par défaut.

Pour activer la liste des connexions asymétriques sur les appliances Citrix SD-WAN WANOP :

1. Accédez à l'invite de commande WANOP CLI (WANOP Accelerator/Broker IP).
2. Connectez-vous avec les informations d'identification suivantes :

```
**Connectez-vous en tant que :** *cli*****

**Connexion** : **** *admin*****

**Mot de passe** : **** *nsroot*****
```

> **Remarque**
>
> Le mot de passe par défaut pour admin est *nsroot*. Si vous avez changé le mot de passe, utilisez le bon.

3. Tapez la commande suivante et appuyez sur Entrée.

```
*Set parameter AssymetricConnectionList.Enable on*
```

> **Remarque**
>
> Vous pouvez configurer le délai d'attente conformément à votre besoin réseau, à l'aide de la commande *AssyMetricConnectionList.AutoflushDuration*.

Il existe plusieurs paramètres disponibles avec une liste d'asymétrie qui peuvent être affinés, à la demande, en fonction de votre environnement réseau. Pour plus d'informations, contactez le support clientèle Citrix.

Plug-in client Citrix SD-WAN WANOP

April 9, 2021

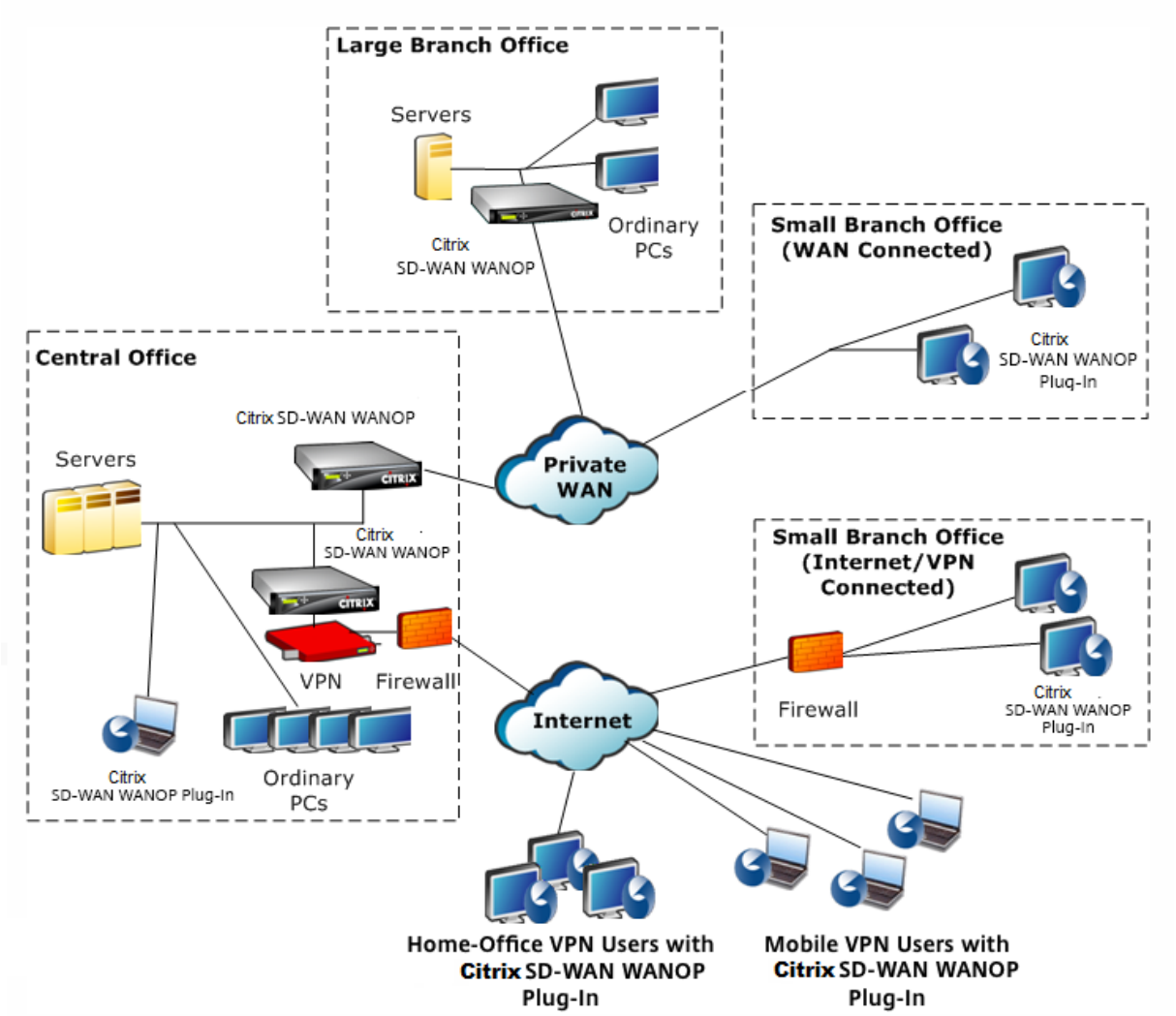
Le plug-in client WANOP Citrix est un accélérateur de réseau basé sur un logiciel qui s'exécute sur des ordinateurs portables et des stations de travail Windows, offrant une accélération partout, pas

seulement dans les bureaux avec les appliances WANOP Client Plug-in. Il se connecte à une appliance Citrix WANOP à l'autre extrémité de la liaison.

Les principes de fonctionnement du plug-in client WANOP sont généralement les mêmes que ceux d'un plug-in client WANOP. Pour les rubriques qui ne sont pas incluses dans la documentation du plug-in, reportez-vous à l'ensemble de documentation plus volumineux.

Le plug-in est distribué sous la forme d'un fichier d'installation Microsoft standard (MSI). Le déploiement du plug-in nécessite une configuration spécifique du plug-in des appliances WANOP aux autres extrémités des liens. Si vous personnalisez le fichier MSI avec les adresses DNS ou IP des appliances WANOP et quelques autres paramètres, vos utilisateurs n'ont pas à saisir d'informations de configuration lors de l'installation du plug-in sur leurs ordinateurs Windows.

Figure 1. Réseau de plug-in client WANOP typique Affichage du plug-in client WANOP



> **Remarque**
>
> Le plug-in est pris en charge par Citrix Receiver 1.2 ou version ultérieure et peut être distribué et géré par Citrix Receiver.

Configuration matérielle et logicielle requise

April 9, 2021

Du côté client de la liaison accélérée, le plug-in client
WANOP est pris en charge sur les ordinateurs de bureau et portables Windows, mais pas sur les netbooks ou les clients légers. Citrix recommande les spécifications matérielles minimales suivantes pour l'ordinateur exécutant le plug-in client
WANOP :

- Processeur classe Pentium 4
- 2 Go de RAM
- 2 Go d'espace disque libre

Le plug-in client WANOP est pris en charge sur la plate-forme Windows 10 et nécessite la configuration système suivante :

- 4 Go de RAM
- 10 Go d'espace disque libre

Le plug-in client WANOP est pris en charge sur les systèmes d'exploitation suivants :

- Windows XP Édition Familiale
- Windows XP Professionnel
- Windows Vista (toutes les versions 32 bits de Familiale Basique, Familiale Premium, Professionnel, Entreprise et Intégrale)
- Windows 7 (toutes les versions 32 bits et 64 bits de Familiale Basique, Familiale Premium, Professionnel, Entreprise et Intégrale)
- Windows 8 (versions 32 bits et 64 bits d'Enterprise Edition)
- Windows 10 (versions 32 bits et 64 bits d'Enterprise Edition)

Côté serveur, les appliances suivantes prennent actuellement en charge les déploiements de plug-in client
WANOP :

- Plug-in client WANOP VPX
- Plug-in client WANOP 2000
- Plug-in client WANOP 3000
- Plug-in client WANOP 4000
- Plug-in client WANOP 5000

Fonctionnement du plug-in WANOP

April 9, 2021

Les produits WANOP Client Plug-in utilisent votre infrastructure WAN/VPN existante. Un ordinateur sur lequel le plug-in est installé continue d'accéder au LAN, au WAN et à Internet comme il l'a fait avant l'installation du plug-in. Aucune modification n'est requise pour vos tables de routage, paramètres réseau, applications clientes ou applications serveur.

Les VPN Citrix Access Gateway nécessitent une petite quantité de configuration spécifique au plug-in client WANOP.

Il existe deux variations dans la façon dont les connexions sont gérées par le plug-in et l'appliance : le *mode transparent* et le *mode redirecteur.* Le redirecteur est un mode hérité qui n'est pas recommandé pour les nouveaux déploiements.

- Le **mode transparent** pour l'accélération plug-in-appliance est très similaire à l'accélération appliance-appliance. L'appliance WANOP Client Plug-in doit se trouver dans le chemin emprunté par les paquets lorsqu'ils se déplacent entre le plug-in et le serveur. Comme pour l'accélération appliance-appliance, le mode transparent fonctionne comme un proxy transparent, préservant l'adresse IP source et de destination et les numéros de port d'une extrémité de la connexion à l'autre.
- **Le mode redirecteur** (non recommandé) utilise un proxy explicite. Le plug-in adresse à nouveau les paquets sortants à l'adresse IP du redirecteur de l'appliance. L'appliance réachemine les paquets au serveur, tout en changeant l'adresse de retour pour qu'elle pointe vers elle-même au lieu du plug-in. Dans ce mode, l'appliance n'a pas besoin d'être physiquement intégrée au chemin entre l'interface WAN et le serveur (bien qu'il s'agisse du déploiement idéal).

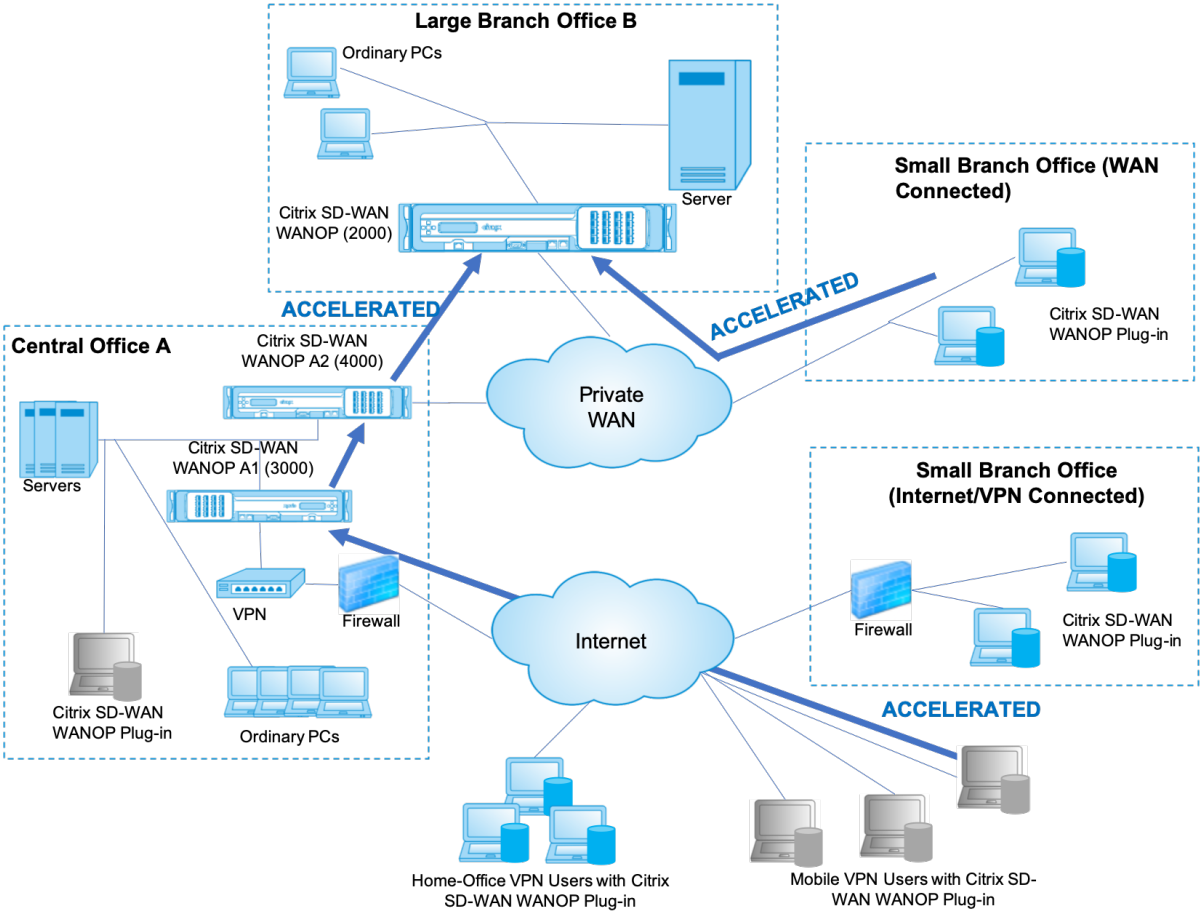
  Meilleure pratique : utilisez le mode transparent lorsque vous le pouvez, et le mode redirecteur lorsque vous le devez.

Mode transparent

En mode transparent, les paquets pour les connexions accélérées doivent passer par l'appliance cible, tout comme ils le font pour l'accélération appliance-appliance.

Le plug-in est configuré avec une liste des appliances disponibles pour l'accélération. Il tente de contacter chaque appliance, ouvrant une connexion de signalisation. Si la connexion de signalisation réussit, le plug-in télécharge les règles d'accélération à partir de l'appliance, qui envoie les adresses de destination pour les connexions que l'appliance peut accélérer.

Figure 1. Mode transparent, mise en évidence de trois trajectoires d'accélération



Remarque

- Flux de trafic : le mode transparent accélère les connexions entre un plug-in client Citrix WANOP et une appliance compatible plug-in.
- Licence : les appliances ont besoin d'une licence pour prendre en charge le nombre de plug-ins souhaité. Dans le diagramme, Citrix SD-WAN WANOP A2 n'a pas besoin d'être sous licence pour l'accélération du plug-in, car Citrix SD-WAN WANOP A1 fournit l'accélération du plug-in pour le site A.

> - daisy-chaining : si la connexion passe par plusieurs appliances en cours de route vers l'appliance cible, l'option « daisy-chaining » doit être activée pour les appliances du milieu, sinon l'accélération est bloquée. Dans le diagramme, le trafic provenant des utilisateurs VPN de bureau à domicile et mobiles destinés aux grandes succursales B est accéléré par Citrix SD-WAN WANOP B. Pour que cela fonctionne, Citrix SD-WAN WANOP A1 et A2 doit avoir activé le chaînage en marguerite.

Chaque fois que le plug-in ouvre une nouvelle connexion, il consulte les règles d'accélération. Si l'adresse de destination correspond à l'une des règles, le plug-in tente d'accélérer la connexion en attachant des options d'accélération au paquet initial de la connexion (le paquet SYN). Si une appliance connue du plug-in attache des options d'accélération au paquet de réponse SYN-ACK, une connexion accélérée est établie avec cette appliance.

L'application et le serveur ne savent pas que la connexion accélérée a été établie. Seuls le logiciel plug-in et l'appliance savent que l'accélération est en cours.

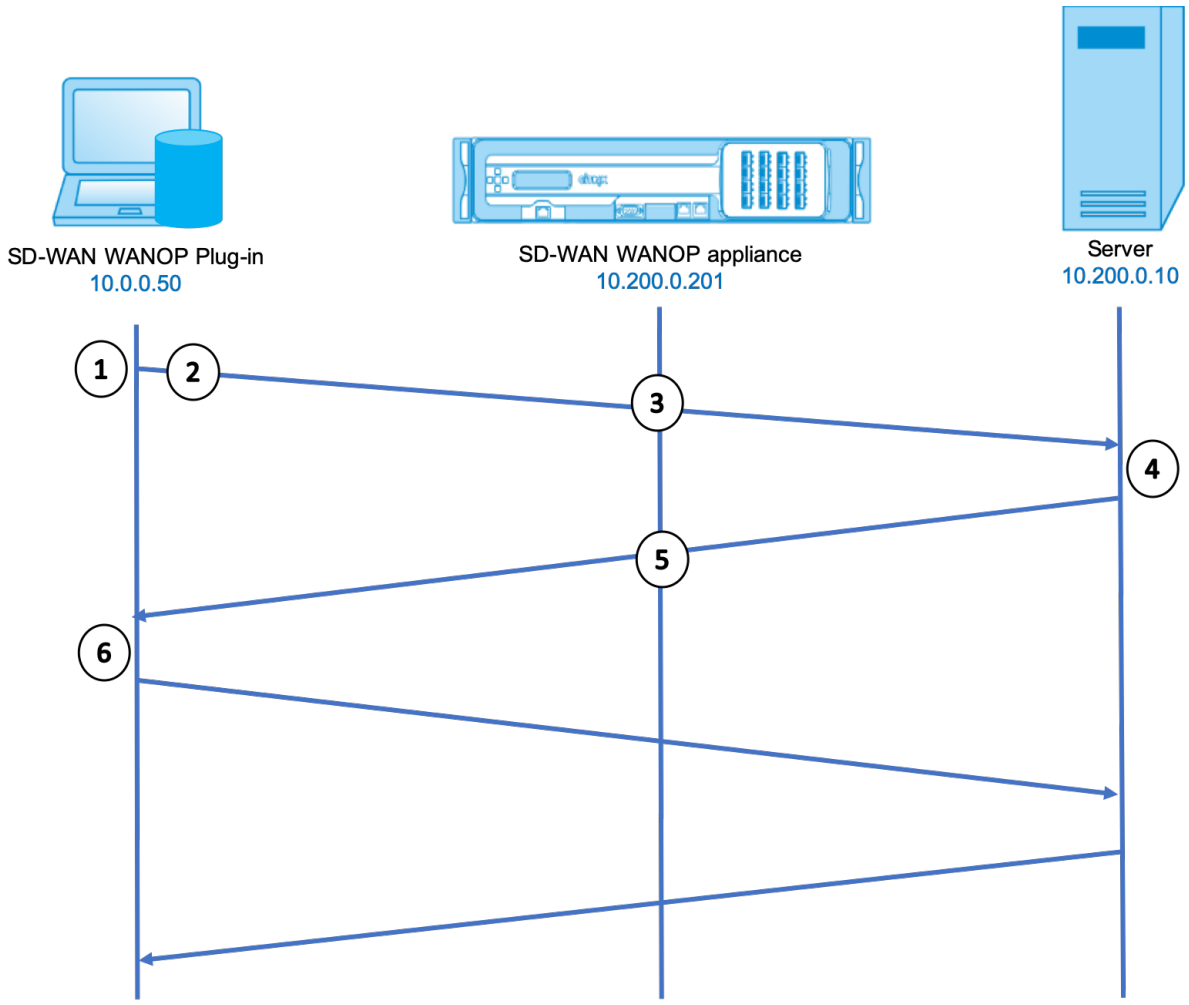
Le mode transparent ressemble à l'accélération appliance-appliance, mais n'est pas identique à celui-ci. Les différences sont les suivantes :

- Connexions initiées par le client uniquement : le mode transparent accepte uniquement les connexions initiées par le système équipé d'un plug-in. Si vous utilisez un système équipé d'un plug-in en tant que serveur, les connexions au serveur ne sont pas accélérées. D'autre part, l'accélération appliance-appliance fonctionne indépendamment du côté du client et du serveur. (Le FTP en mode actif est traité comme un cas particulier, car la connexion initiant le transfert de données demandé par le plug-in est ouverte par le serveur.)
- Connexion de signalisation : le mode transparent utilise une connexion de signalisation entre le plug-in et l'appliance pour la transmission des informations d'état. l'accélération appliance-appliance ne nécessite pas de connexion de signalisation, à l'exception des relations homologues sécurisées, qui sont désactivées par défaut. Si le plug-in ne peut pas ouvrir une connexion de signalisation, il ne tente pas d'accélérer les connexions via l'appliance.
- Chaîne en marguerite : pour une appliance située dans le chemin d'accès entre un plug-in et son matériel cible sélectionné, vous devez activer le chaînage en marguerite dans le menu **Configuration : Réglage**.

Le mode transparent est souvent utilisé avec les VPN. Le plug-in client WANOP est compatible avec la plupart des VPN IPsec et PPTP, ainsi qu'avec les VPN Citrix Access Gateway.

La figure suivante montre le flux de paquets en mode transparent. Ce flux de paquets est presque identique à l'accélération appliance-appliance, sauf que la décision de tenter ou non d'accélérer la connexion repose sur des règles d'accélération téléchargées sur la connexion de signalisation.

Figure 2. Flux de paquets en mode transparent



1. L'application de l'utilisateur ouvre une connexion TCP au serveur, en envoyant un paquet TCP SYN.

   Src : 10.0.0.50, heure d'été : 10.200.0.10

2. Le plug-in WANOP recherche l'adresse de destination et voit qu'elle correspond à un sous-réseau accéléré par l'appliance. Il attache les options WANOP à l'en-tête TCP du paquet SYN. Aucune adresse n'est modifiée.

   Src : 10.0.0.50, heure d'été : 10.200.0.10

3. L'appliance prend note des options SYN et reconnaît qu'il s'agit d'une connexion accélérée. Il supprime les options du paquet et lui permet de passer au serveur. Aucune adresse n'est modifiée.

   Src : 10.0.0.50, heure d'été : 10.200.0.10

4. Le serveur accepte la connexion et répond avec un paquet TCP SYN-ACK.

   Src : 10.200.0.10, heure d'été : 10.0.0.50

5. L'appliance marque le paquet SYN-ACK avec une option d'en-tête TCP qui indique que l'accélération aura lieu.

   Src : 10.200.0.10, heure d'été : 10.0.0.50

6. Le plug-in WANOP reçoit le paquet SYN-ACK. Les options des en-têtes de paquets indiquent que la connexion est accélérée. Le plug-in supprime les options et transmet le paquet SYN-ACK à l'application. La connexion est maintenant entièrement ouverte et accélérée.

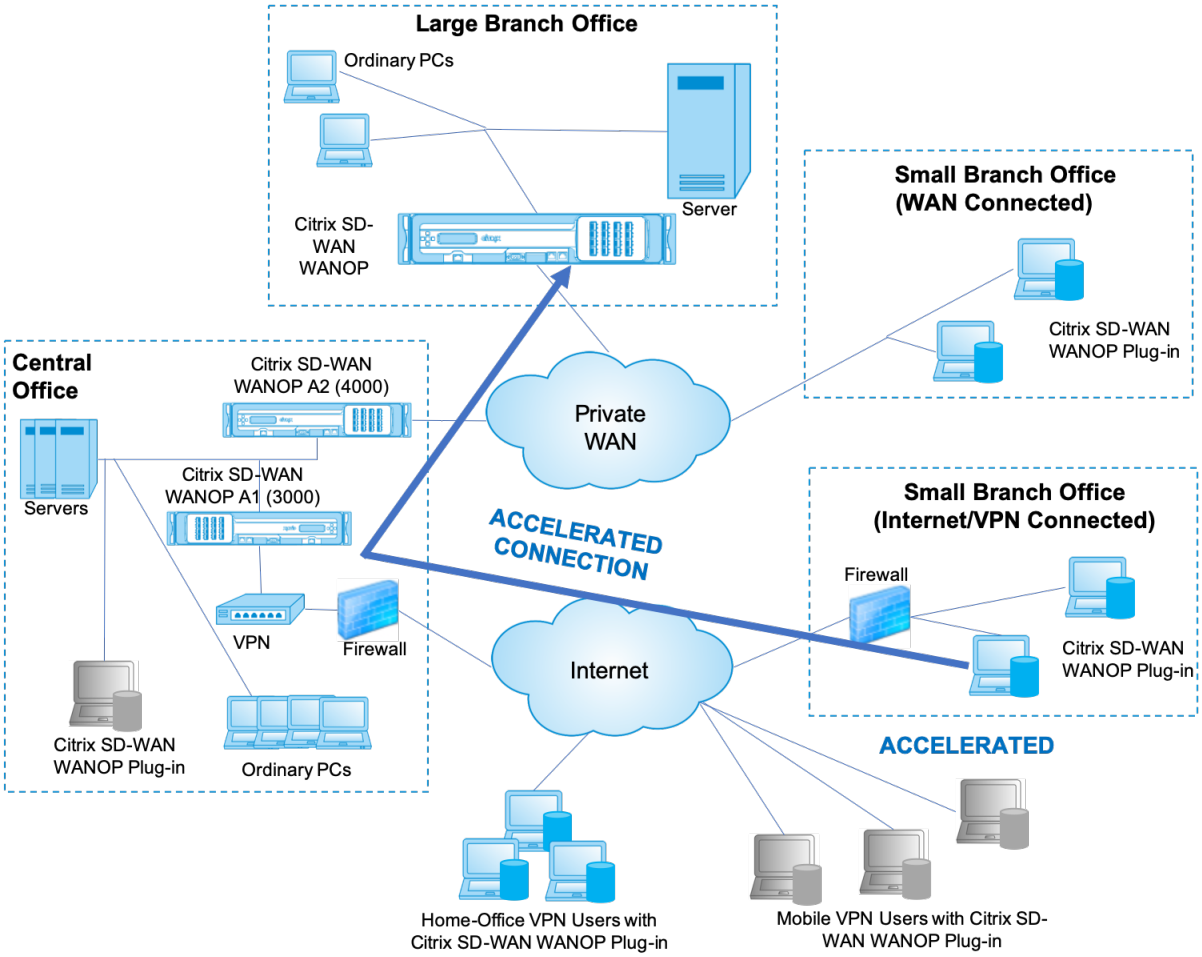
Mode redirecteur

Le mode redirecteur fonctionne différemment du mode transparent de la manière suivante :

- Le plug-in client WANOP redirige les paquets en les adressant explicitement à l'appliance.
- Par conséquent, l'appliance en mode redirecteur n'a pas à intercepter tout le trafic WAN Link. Comme les connexions accélérées lui sont adressées directement, il peut être placé n'importe où, tant qu'il peut être atteint à la fois par le plug-in et le serveur.
- L'appliance effectue ses optimisations, puis redirige les paquets de sortie vers le serveur, en remplaçant l'adresse IP source des paquets par sa propre adresse. Du point de vue du serveur, la connexion provient de l'appliance.
- Le trafic de retour du serveur est adressé à l'appliance, qui effectue des optimisations dans le sens de retour et transfère les paquets de sortie au plug-in.
- Les numéros de port de destination ne sont pas modifiés, de sorte que les applications de surveillance réseau peuvent toujours classer le trafic.

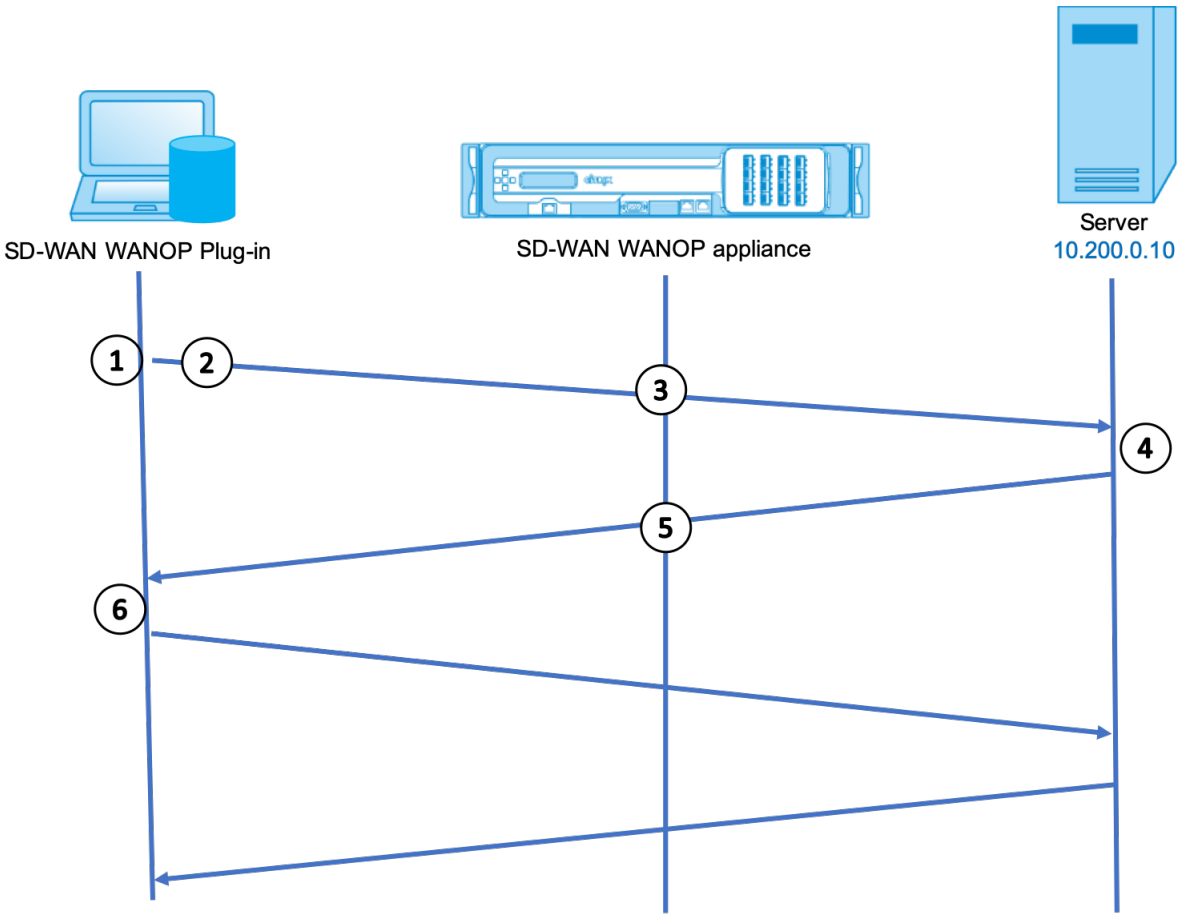
La figure ci-dessous montre comment fonctionne le mode Redirecteur.

Figure 1. Mode redirecteur



La figure ci-dessous montre le flux de paquets et le mappage d'adresses en *mode redirecteur*.

Figure 2. Flux de paquets en mode redirecteur



1. L'application de l'utilisateur ouvre une connexion TCP au serveur, en envoyant un paquet TCP SYN.

   Src : 10.0.0.50, heure d'été : 10.200.0.10

2. Le plug-in WANOP SD-WAN Citrix recherche l'adresse de destination et décide de rediriger la connexion vers l'appliance à l'adresse 10.200.0.201.

   Src : 10.0.0.50, heure d'été : 10.200.0.201

   (10.200.0.10 est conservé dans un champ d'option TCP. Les options 24-31 sont utilisées pour divers paramètres.)

3. L'appliance accepte la connexion et transmet le paquet au serveur (en utilisant l'adresse de destination du champ d'options TCP), et se donne comme source.

   Src : 10.200.0.201, heure d'été : 10.200.0.10

4. Le serveur accepte la connexion et répond avec un paquet TCP SYN-ACK.

   Src : 10.200.0.10, heure d'été : 10.200.0.201

5. L'appliance réécrit les adresses et transfère le paquet au plug-in (Placement de l'adresse du serveur dans un champ d'option).

Src : 10.200.0.201, heure d'été : 10.0.0.50

6. La connexion est maintenant entièrement ouverte. Le client et le serveur envoient des paquets par l'intermédiaire de l'appliance.

   Alors que les adresses sont modifiées en mode Redirecteur, les numéros de port de destination ne le sont pas (bien que le numéro de port éphémère puisse être). Les données ne sont pas encapsulées. Le mode redirecteur est un proxy, pas un tunnel.

   Il n'y a pas de relation 1:1 entre les paquets (bien qu'à la fin, les données reçues soient toujours identiques aux données envoyées). La compression peut réduire de nombreux paquets d'entrée en un seul paquet. L'accéralation CIFS effectuera des opérations de lecture anticipée et de blanchiment d'or spéculatives. En outre, si des paquets sont déposés entre l'appliance et le plug-in Reperter, la retransmission est gérée par l'appliance, et non le serveur, à l'aide d'algorithmes de récupération avancés.

Mode de sélection d'une appliance par le plug-in

Chaque plug-in est configuré avec une liste des appliances qu'il peut contacter pour demander une connexion accélérée.

Les appliances disposent chacune d'une liste de règles d'accélération, qui est une liste d'adresses ou de ports cibles auxquels l'appliance peut établir des connexions accélérées.** Le plug-in télécharge ces règles à partir des appliances et correspond à l'adresse et au port de destination de chaque connexion avec l'ensemble de règles de chaque appliance. Si un seul appareil propose d'accélérer une connexion donnée, la sélection est facile. Si plusieurs appliances proposent d'accélérer la connexion, le plug-in doit choisir l'une des appliances.

Les règles de sélection de l'appliance sont les suivantes :

- Si toutes les appliances proposant d'accélérer la connexion sont des appliances en mode redirecteur, l'appliance la plus à gauche dans la liste des appliances du plug-in est sélectionnée. (Si les appliances ont été spécifiées en tant qu'adresses DNS et que l'enregistrement DNS comporte plusieurs adresses IP, celles-ci sont également analysées de gauche à droite.)
- Si certaines des appliances proposant d'accélérer la connexion utilisent le mode redirecteur et d'autres le mode transparent, les appliances en mode transparent sont ignorées et la sélection est effectuée à partir des appliances en mode redirecteur.
- Si toutes les appliances proposant d'accélérer la connexion utilisent le mode transparent, le plug-in ne sélectionne pas un appareil spécifique. Il initie la connexion avec les options SYN du plug-in client WANOP, et quelle que soit l'appliance candidate attache les options appropriées au paquet SYN-ACK de retour utilisé. Cela permet à l'appliance qui est en ligne avec le trafic de s'identifier au plug-in. Toutefois, le plug-in doit avoir une connexion de signalisation ouverte avec l'appliance répondant, sinon l'accélération n'a pas lieu.

- Certaines informations de configuration sont considérées comme globales. Ces informations de configuration proviennent de l'appliance la plus à gauche de la liste pour laquelle une connexion de signalisation peut être ouverte.

Déployer des appliances pour une utilisation avec des plug-ins

April 23, 2021

L'accélération du client nécessite une configuration spéciale sur l'appliance WANOP Client Plug-in. Parmi les autres considérations, mentionnons le placement de l'appliance. Les plug-ins sont généralement déployés pour les connexions VPN.

Utiliser une appliance dédiée si possible

Il est souvent difficile d'utiliser la même appliance pour l'accélération de plug-in et l'accélération de liaison, car les deux utilisations exigent parfois que l'appliance se trouve à des points différents du centre de données, et les deux utilisations peuvent appeler à des règles de classe de service différentes.

En outre, une appliance peut servir de point de terminaison pour l'accélération de plug-in ou de point de terminaison pour l'accélération de site à site, mais elle ne peut pas servir les deux objectifs pour la même connexion en même temps. Par conséquent, lorsque vous utilisez une appliance pour l'accélération de plug-in pour votre VPN et pour l'accélération de site à site vers un datacenter distant, les utilisateurs de plug-in ne reçoivent pas d'accélération de site à site. La gravité de ce problème dépend de la quantité de données utilisées par les utilisateurs de plug-in provient de sites distants.

Enfin, étant donné que les ressources d'une appliance dédiée ne sont pas réparties entre les demandes de plug-in et de site à site, elles fournissent davantage de ressources et donc des performances supérieures à chaque utilisateur de plug-in.

Utiliser le mode en ligne lorsque cela est possible

Une appliance doit être déployée sur le même site que l'unité VPN qu'elle prend en charge. Typiquement, les deux unités sont alignées les unes avec les autres. Un déploiement en ligne offre la configuration la plus simple, le plus grand nombre de fonctionnalités et les performances les plus élevées. Pour de meilleurs résultats, l'appliance doit être directement en ligne avec l'unité VPN.

Toutefois, les appliances peuvent utiliser n'importe quel mode de déploiement, à l'exception du mode groupe ou du mode haute disponibilité. Ces modes conviennent à l'accélération appliance-

appliance et client-à-matériel. Ils peuvent être utilisés seuls (*mode transparent*) ou en combinaison avec le mode redirecteur.

Placez les appliances dans une partie sécurisée de votre réseau

Une appliance dépend de votre infrastructure de sécurité existante de la même manière que vos serveurs. Il doit être placé du même côté du pare-feu (et de l'unité VPN, le cas échéant) que les serveurs.

Éviter les problèmes NAT

La traduction d'adresses réseau (NAT) côté plug-in est gérée de manière transparente et n'est pas un problème. Du côté de l'appliance, la NAT peut être gênante. Appliquez les instructions suivantes pour assurer un déploiement sans heurts :

- Placez l'appliance dans le même espace d'adressage que les serveurs, de sorte que les modifications d'adresse utilisées pour atteindre les serveurs soient également appliquées à l'appliance.
- N'accédez jamais à l'appliance à l'aide d'une adresse qu'elle n'associe pas elle-même.
- L'appliance doit pouvoir accéder aux serveurs à l'aide des mêmes adresses IP auxquelles les utilisateurs du plug-in accèdent aux mêmes serveurs.
- En résumé, n'appliquez pas NAT aux adresses des serveurs ou des appliances.

Sélectionner le mode softboost

Sur la page Configurer les paramètres : Gestion de la bande passante, sélectionnez Mode Softboost. Softboost est le seul type d'accélération pris en charge avec le plug-in client WANOP.

Définir les règles d'accélération du plug-in

L'appliance gère une liste de règles d'accélération indiquant aux clients le trafic à accélérer. Chaque règle spécifie une adresse ou un sous-réseau et une plage de ports que l'appliance peut accélérer.

Ce qu'il faut accélérer - Le choix du trafic à accélérer dépend de l'utilisation de l'appliance :

- Accélérateur VPN : si l'appliance est utilisée comme accélérateur VPN, avec tout le trafic VPN passant par l'appliance, tout le trafic TCP doit être accéléré, quelle que soit la destination.
- Mode redirecteur : contrairement au mode transparent, une appliance en mode redirecteur est un proxy explicite, ce qui fait que le plug-in transfère son trafic à l'appliance en mode redirecteur

même si cela n'est pas souhaitable. L'accélération peut être contre-productive si le client transfère le trafic vers une appliance éloignée du serveur, en particulier si cette « route triangulaire » introduit une liaison lente ou peu fiable. Par conséquent, Citrix recommande que les règles d'accélération soient configurées pour permettre à une appliance donnée d'accélérer son propre site uniquement.

- Autres utilisations - Lorsque le plug-in n'est utilisé ni comme accélérateur VPN ni en mode redirecteur, les règles d'accélération doivent inclure des adresses distantes aux utilisateurs et locales aux centres de données.

Définition des règles - Définissez des règles d'accélération sur l'appliance, sous l'onglet **Configuration : WANOP Client Plug-in : Acceleration Rules**.

Les règles sont évaluées dans l'ordre et l'action (Accélérer ou Exclure) est effectuée à partir de la première règle de correspondance. Pour qu'une connexion soit accélérée, elle doit correspondre à une règle Accélération.

L'action par défaut consiste à ne pas accélérer.

1. Dans l'onglet Configuration : WANOP Plug-in : Règles d'accélération :
    - Ajoutez une règle Accelerated pour chaque sous-réseau LAN local auquel l'appliance peut accéder. Autrement dit, cliquez sur **Ajouter**, sélectionnez **Accélérer**et tapez l'adresse IP du sous-réseau et le masque.
    - Répétez la procédure pour chaque sous-réseau local de l'appliance.
2. Si vous devez exclure une partie de la plage incluse, ajoutez une règle Exclure et déplacez-la au-dessus de la règle plus générale. Par exemple, 10.217.1.99 ressemble à une adresse locale. S'il s'agit vraiment du point de terminaison local d'une unité VPN, créez une règle Exclure pour elle sur une ligne au-dessus de la règle Accélération pour 10.217.1.0/24.
3. Si vous souhaitez utiliser l'accélération pour un seul port (non recommandé), tel que le port 80 pour HTTP, remplacez le caractère générique dans le champ Ports par le numéro de port spécifique. Vous pouvez prendre en charge des ports supplémentaires en ajoutant des règles supplémentaires, une par port.
4. En général, lister les règles étroites (généralement des exceptions) avant les règles générales.
5. Cliquez sur **Apply**. Les modifications ne sont pas enregistrées si vous quittez cette page avant de les appliquer.

Utilisation du port IP

Utilisez les instructions suivantes pour l'utilisation du port IP :

- **Ports utilisés pour la communication avec le plug-in client WANOP** : le plug-in maintient une boîte de dialogue avec l'appliance via une connexion de signalisation, qui est par défaut sur le port 443 (HTTPS), qui est autorisé par la plupart des pare-feu.
- **Ports utilisés pour la communication avec les serveurs** : la communication entre le plug-in client WANOP et l'appliance utilise les mêmes ports que le client utiliserait pour la communication avec le serveur si le plug-in et l'appliance n'étaient pas présents. Autrement dit, lorsqu'un client ouvre une connexion HTTP sur le port 80, il se connecte à l'appliance sur le port 80. L'appliance contacte le serveur sur le port 80.

  En mode redirecteur, seul le port connu (c'est-à-dire le port de destination sur le paquet TCP SYN) est conservé. Le port éphémère n'est pas conservé. En mode transparent, les deux ports sont conservés.

  L'appliance suppose qu'elle peut communiquer avec le serveur sur n'importe quel port demandé par le client et qu'elle peut communiquer avec l'appliance sur n'importe quel port souhaité. Cela fonctionne bien si l'appliance est soumise aux mêmes règles de pare-feu que les serveurs. Dans ce cas, toute connexion qui réussirait dans une connexion directe réussirait dans une connexion accélérée.

Utilisation de l'option TCP et pare-feu

Les paramètres du plug-in client WANOP sont envoyés dans les options TCP. Les options TCP peuvent se produire dans n'importe quel paquet et sont garanties d'être présentes dans les paquets SYN et SYN-ACK qui établissent la connexion.

Votre pare-feu ne doit pas bloquer les options TCP dans la plage de 24-31 (décimale), sinon l'accélération ne peut pas avoir lieu. La plupart des pare-feu ne bloquent pas ces options. Cependant, un pare-feu Cisco PIX ou ASA avec le firmware de la version 7.x peut le faire par défaut, et par conséquent vous devrez peut-être ajuster sa configuration.

Personnaliser le fichier MSI du plug-in

April 9, 2021

Vous pouvez modifier les paramètres dans le fichier de distribution du plug-in client WANOP, qui est au format Microsoft Installer (MSI) standard. La personnalisation nécessite l'utilisation d'un éditeur MSI.

> **Remarque**
>
> Les paramètres modifiés dans votre édition. Le fichier MSI s'applique uniquement aux nouvelles installations. Lorsque des utilisateurs de plug-in existants sont mis à jour vers une nouvelle version, leurs paramètres existants sont conservés. Par conséquent, après avoir modifié les paramètres, vous devriez conseiller à vos utilisateurs de désinstaller l'ancienne version avant d'installer la nouvelle.

Pratiques exemplaires :

Créez une entrée DNS qui se résout à l'appliance plug-in la plus proche. Par exemple, définissez « Repeater.myCompany.com » et faites en sorte qu'il soit résolu en fonction de votre appliance, si vous n'avez qu'un seul appareil. Ou, si vous avez, disons, cinq appareils, ont Repeater.mycompany.com résoudre à l'un de vos cinq appareils, avec l'appareil sélectionné sur la base de la proximité avec le client ou l'unité VPN. Par exemple, un client utilisant une adresse associée à un VPN particulier doit voir Repeater.mycompany.com résoudre l'adresse IP du plug-in client WANOP connecté à ce VPN. Construisez cette adresse dans votre binaire de plug-in avec un éditeur MSI, tel que Orca. Lorsque vous ajoutez, déplacez ou supprimez des appliances, la modification de cette définition DNS unique sur votre serveur DNS met automatiquement à jour la liste des appliances de vos plug-ins.

L'entrée DNS peut également être résolue sur plusieurs appliances, mais cela n'est pas souhaitable, sauf si toutes les appliances sont configurées de manière identique, car le plug-in prend certaines caractéristiques de l'appliance la plus à gauche de la liste et les applique globalement (y compris les caractéristiques de compression SSL). Cela peut conduire à des résultats indésirables et déroutants, en particulier si le serveur DNS fait pivoter l'ordre des adresses IP pour chaque requête.

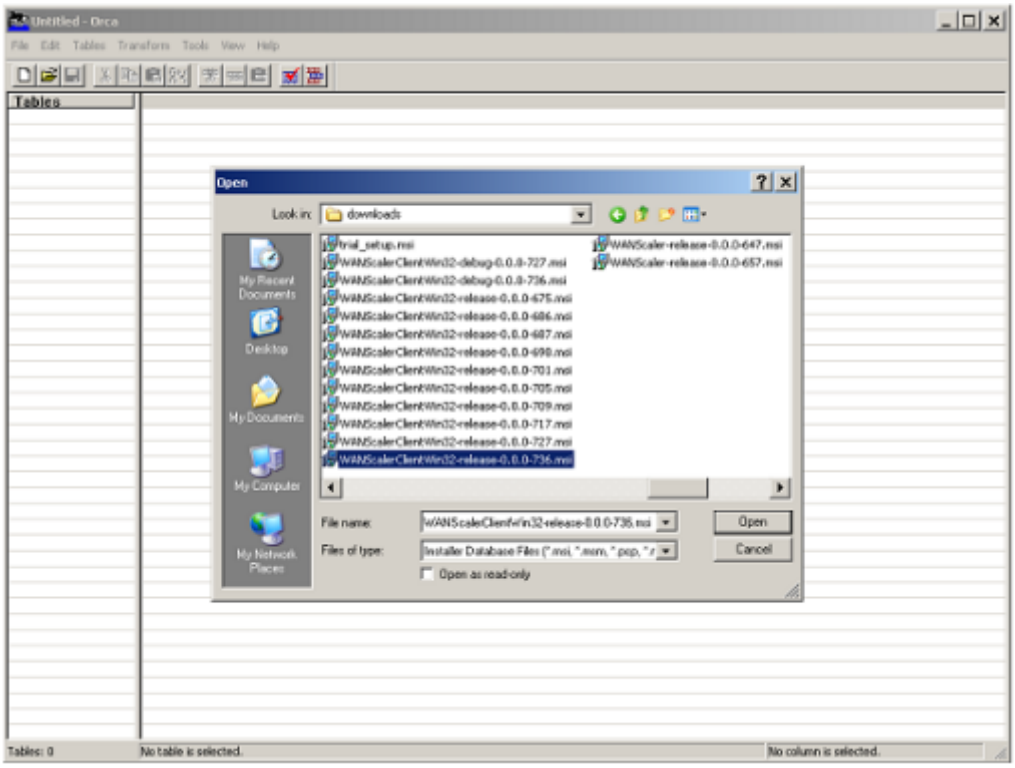
Installez l'éditeur Orca MSI :

Il existe de nombreux éditeurs MSI, y compris Orca, qui fait partie du SDK gratuit de plate-forme de Microsoft et peut être téléchargé à partir de Microsoft.

Pour installer l'éditeur Orca MSI :

1. Téléchargez la version PSDK-x86.exe du SDK et exécutez-la. Suivez les instructions d'installation.
2. Une fois le SDK installé, l'éditeur Orca doit être installé. Il sera sous Microsoft Platform SDK\Bin\Orca.Msi. Lancez Orca.msi pour installer l'éditeur Orca (orca.exe).
3. **Running Orca**—Microsoft fournit sa documentation Orca en ligne. Les informations suivantes décrivent comment modifier les paramètres de plug-in client WANOP les plus importants.
4. Lancez Orca avec **Démarrer > Tous les programmes > Orca.** Lorsqu'une fenêtre Orca vide apparaît, ouvrez le fichier MSI Plug-in Client WANOP Plug-in avec **Fichier > Ouvrir**.

   Figure 1. Utilisation d'Orca



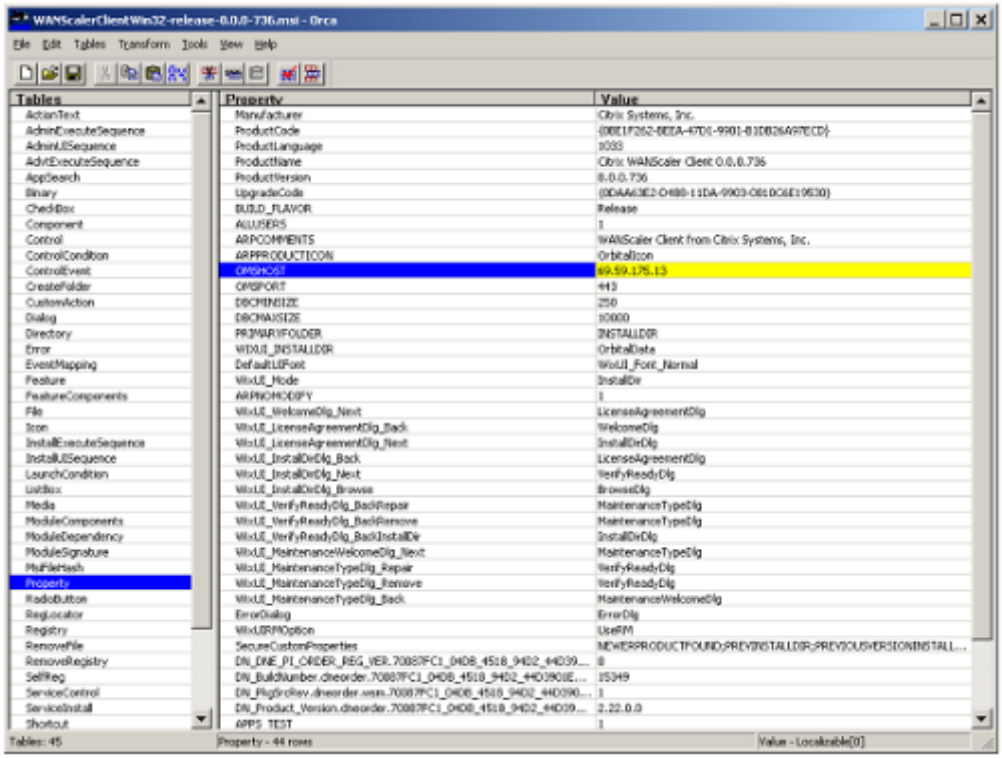
5. **Dans le menu Tables**, cliquez sur **Propriété**. Une liste de toutes les propriétés modifiables du fichier .MSI s'affiche. Modifiez les paramètres affichés dans le tableau suivant. Pour modifier un paramètre, double-cliquez sur sa valeur, tapez la nouvelle valeur et appuyez sur **Entrée**.

   Pour plus d'informations, veuillez consulter le tableau.

   a) Dans le menu Tables, cliquez sur Propriété. Une liste de toutes les propriétés modifiables du fichier .MSI s'affiche. Modifiez les paramètres affichés dans le tableau suivant. Pour modifier un paramètre, double-cliquez sur sa valeur, tapez la nouvelle valeur et appuyez sur **Entrée**.

      Pour plus d'informations, veuillez consulter le tableau.

      Figure 2 : Modification des paramètres dans Orca :



6. Lorsque vous avez terminé, utilisez la commande **Fichier : Enregistrer sous** pour enregistrer votre fichier modifié avec un nouveau nom de fichier ; par exemple, test.msi.

Votre logiciel de plug-in a maintenant été personnalisé.

> **Remarque**
>
> Certains utilisateurs ont vu un bug dans orca qui l'entraîne à tronquer les fichiers à 1 Mo. Vérifiez la taille du fichier enregistré. S'il a été tronqué, faites une copie du fichier d'origine et utilisez la commande Enregistrer pour remplacer l'original.

Une fois que vous avez personnalisé la liste des appliances avec Orca et distribué le fichier MSI personnalisé à vos utilisateurs, l'utilisateur n'a pas besoin de saisir les informations de configuration lors de l'installation du logiciel.

Déployer des plug-ins sous Windows

April 23, 2021

Le plug-in client WANOP est un fichier exécutable Microsoft Installer (MSI) que vous téléchargez et installez comme avec tout autre programme distribué sur le Web. Obtenez ce fichier à partir de la section MyCitrix du site Web Citrix.com.

> **Remarque**
>
> L'interface utilisateur WANOP Client Plug-in se réfère à elle-même comme « Citrix Acceleration Plug-in Manager. »

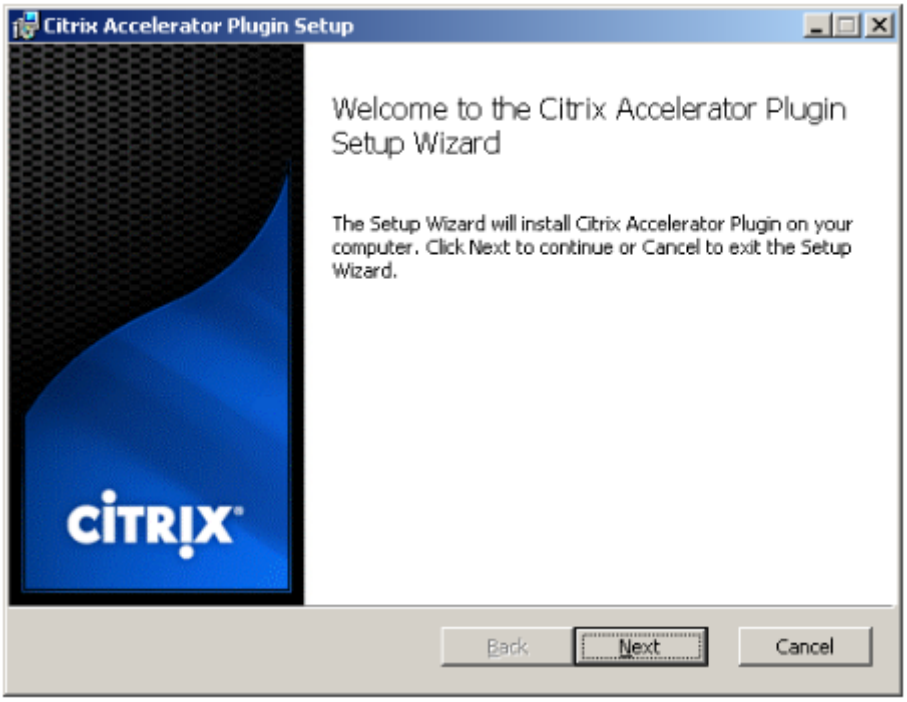
La seule configuration utilisateur requise par le plug-in est la liste des adresses de matériel. Cette liste peut consister en une liste d'adresses IP ou DNS séparées par des virgules. Les deux formes peuvent être mélangées. Vous pouvez personnaliser le fichier de distribution de sorte que la liste pointe vers votre appliance par défaut. Une fois installé, le fonctionnement est transparent. Le trafic vers les sous-réseaux accélérés est envoyé via une appliance appropriée, et tout autre trafic est envoyé directement au serveur. L'application utilisateur ne sait pas que tout cela se produit.

Installation

Pour installer WANOP Client Plug-in Accelerator sur le système Windows :

1. Le fichier Repeater*.msi est un fichier d'installation. Fermez toutes les applications et toutes les fenêtres qui pourraient être ouvertes, puis lancez le programme d'installation de la manière habituelle (double-cliquez sur dans une fenêtre de fichier, ou utilisez la commande run).

   Figure 1. Écran d'installation initiale :

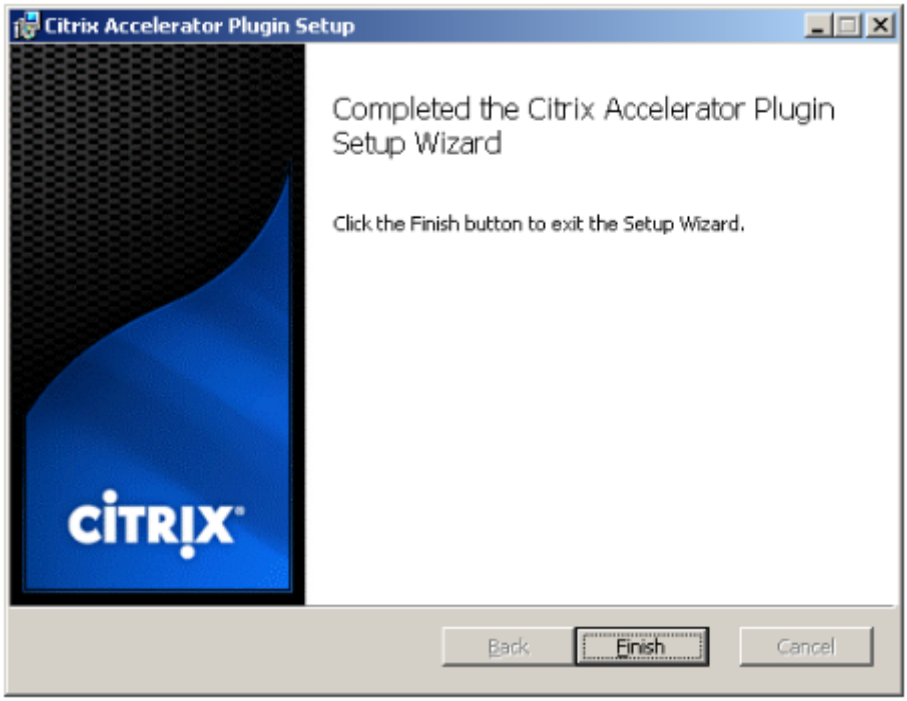
   

   Les étapes ci-dessous sont pour une installation interactive. Une installation silencieuse peut être effectuée avec la commande :

   msiexec /i client_msi_file /qn

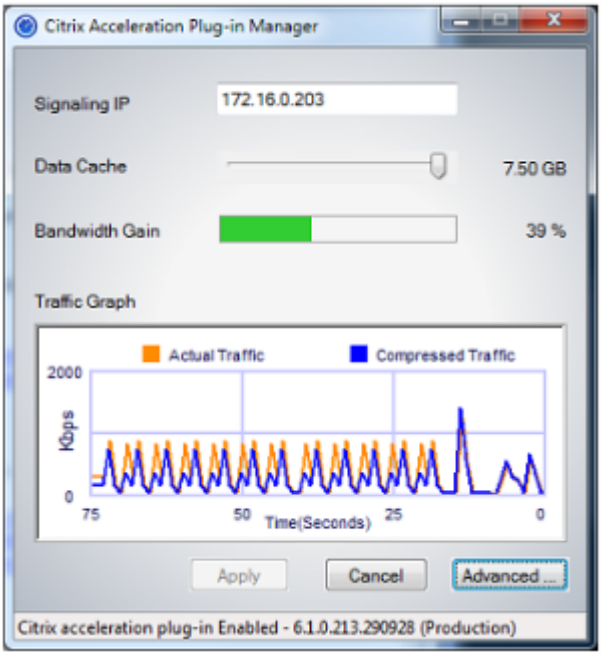
2. Le programme d'installation vous invite à indiquer l'emplacement où installer le logiciel. Le répertoire que vous spécifiez est utilisé à la fois pour le logiciel client et pour l'historique de compression sur disque. Ensemble, ils nécessitent un minimum de 500 Mo d'espace disque.
3. Une fois le programme d'installation terminé, il peut vous demander de redémarrer le système. Après un redémarrage, le plug-in client WANOP démarre automatiquement.

Figure 2. Écran d'installation finale :



4. Cliquez avec le bouton droit sur l'icône Accelerator dans la barre des tâches et sélectionnez **Gérer l'accélération** pour lancer Citrix Plug-in Accelerator Manager.

Figure 3. Gestionnaire de prise Citrix Accelerator, affichage initial (de base) :



5. Si le fichier .MSI n'a pas été personnalisé pour vos utilisateurs, spécifiez l'adresse de signalisation et la quantité d'espace disque à utiliser pour la compression :

   - Dans le champ Appliances : Adresses de signalisation, tapez l'adresse IP de signalisation de votre appliance. Si vous disposez de plusieurs appliances Plug-in, listez-les tous, séparés par des virgules. Les adresses IP ou DNS sont acceptables.
   - À l'aide du curseur Data Cache, sélectionnez la quantité d'espace disque à utiliser pour la compression. Plus il y en a, mieux c'est. 7,5 Go n'est pas trop, si vous avez autant d'espace disque disponible.
   - Appuyez sur Appliquer.

   L'accélérateur WANOP Client Plug-in est en cours d'exécution. Toutes les futures connexions aux sous-réseaux accélérés seront accélérées

   Dans l'onglet Règles avancées du plug-in, la liste Règles d'accélération doit afficher chaque appliance comme Connecté et les sous-réseaux accélérés de chaque appliance comme Accéléré. Si ce n'est pas le cas, vérifiez le champ IP Adresses de signalisation et votre connectivité réseau en général.

Dépannage des plug-ins

L'installation du plug-in se déroule généralement sans problème. Si ce n'est pas le cas, vérifiez les problèmes suivants :

Problèmes courants :

- Si vous ne redémarrez pas le système, le plug-in client WANOP ne s'exécute pas correctement.
- Un disque très fragmenté peut entraîner de mauvaises performances de compression.
- Une défaillance de l'accélération (aucune connexion accélérée répertoriée dans l'onglet **Diagnostics**) indique généralement que quelque chose empêche la communication avec l'appliance. Vérifiez la liste **Configuration : Règles d'accélération** du plug-in pour vous assurer que l'appliance est correctement contactée et que l'adresse cible est incluse dans l'une des règles d'accélération. Les causes typiques des échecs de connexion sont :
  - L'appliance n'est pas en cours d'exécution ou l'accélération a été désactivée.
  - Un pare-feu dépouille les options TCP du plug-in client WANOP à un moment donné entre le plug-in et l'appliance.
  - Le plug-in utilise un VPN non pris en charge.

Erreur de verrouillage de l'activateur de réseau déterministe

Dans de rares cas, après avoir installé le plug-in et redémarré votre ordinateur, le message d'erreur suivant s'affiche deux fois :

L'installation de l'Enhancer de réseau déterministe nécessite d'abord un redémarrage, pour libérer les ressources verrouillées. Veuillez réexécuter cette installation après avoir redémarré l'ordinateur.

Si cela se produit, procédez comme suit :

1. Accédez à **Ajout/Suppression de programmes** et supprimez le plug-in client WANOP, le cas échéant.
2. Accédez au **Panneau de configuration** > **Cartes réseau** > **Connexion au réseau local** > **Propriétés**, recherchez l'entrée pour l'Enhancer de réseau déterministe, désactivez la case à cocher et cliquez sur **OK**. (Votre carte réseau peut être appelée par un nom autre que « Connexion au réseau local ».)
3. Ouvrez une fenêtre de commande et allez dans c:windowsinf (ou dans le répertoire équivalent si vous avez installé Windows dans un emplacement non standard).
4. Exécutez la commande suivante :

   trouver « dne2000.cat » oem*.inf
5. Recherchez le fichier oem*.inf le plus grand numéro qui a renvoyé une ligne correspondante (la ligne correspondante est CatalogFile= dne2000.cat) et modifiez-la. Par exemple :

   notepad oem13.inf

6. Supprimez tout sauf les trois lignes en haut qui commencent par des points-virgules, puis enregistrez le fichier. Cela effacera les paramètres inappropriés ou obsolètes et la prochaine installation utilisera les valeurs par défaut.
7. Réessayez l'installation.

Autres problèmes d'installation

Tout problème lié à l'installation du plug-in client WANOP est généralement dû à l'interférence du réseau, du pare-feu ou du logiciel antivirus existant dans l'installation. Habituellement, une fois l'installation terminée, il n'y a pas d'autres problèmes.

Si l'installation échoue, procédez comme suit :

1. Assurez-vous que le fichier d'installation du plug-in a été copié sur votre système local.
2. Déconnectez tous les clients VPN/réseau distant actifs.
3. Désactivez temporairement tout pare-feu et logiciel antivirus.
4. Si cela est difficile, faites ce que vous pouvez.
5. Réinstallez le plug-in client WANOP.
6. Si cela ne fonctionne pas, redémarrez le système et réessayez.

Interface graphique du plug-in Citrix SD-WAN WANOP

April 9, 2021

L'interface graphique du plug-in client WANOP apparaît lorsque vous cliquez avec le bouton droit de la souris sur l'icône **Plug-in Citrix Accelerator** et sélectionnez **Gérer l'accélération**. L'affichage de base de l'interface graphique apparaît en premier. Il y a aussi un affichage avancé qui peut être utilisé si vous le souhaitez.

Affichage de base

Sur la page de base, vous pouvez définir deux paramètres :

- Le champ Adresses de signalisation spécifie l'adresse IP de chaque appliance à laquelle le plug-in peut se connecter. Citrix recommande de n'afficher qu'une seule appliance, mais vous pouvez créer une liste séparée par des virgules. Il s'agit d'une liste ordonnée, les appliances les plus à gauche ayant priorité sur les autres. L'accélération est tentée avec l'appareil le plus à gauche

pour lequel une connexion de signalisation peut être établie. Vous pouvez utiliser à la fois des adresses DNS et des adresses IP.

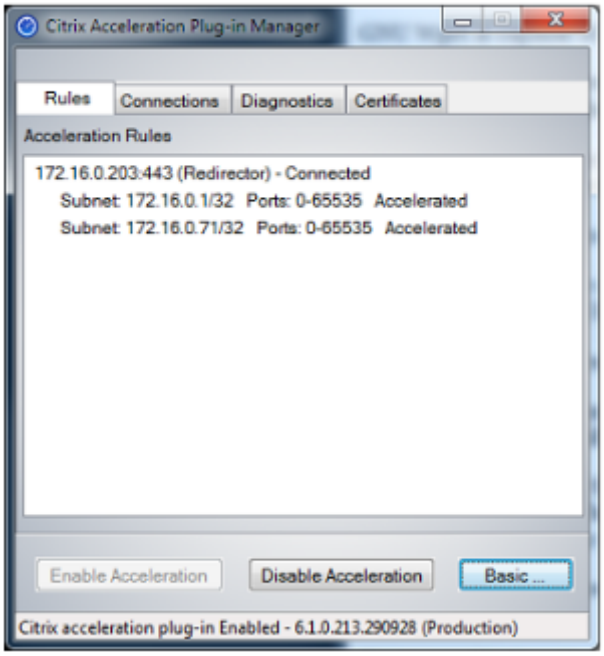
Exemples : 10.200.33.200, ws.mycompany.com, ws2.mycompany.com

- Le curseur Data Cache ajuste la quantité d'espace disque allouée à l'historique de compression sur disque du plug-in. Plus il y en a, mieux c'est.

En outre, il y a un bouton pour passer à l'affichage Avancé.

Affichage avancé

La page Avancé contient quatre onglets : Règles, Connexions, Diagnostics et Certificats.



Au bas de l'écran se trouvent des boutons pour activer l'accélération, désactiver l'accélération et revenir à la page de base.

Onglet Règles

L'onglet Règles affiche une liste abrégée des règles d'accélération téléchargées depuis les appliances. Chaque élément de liste affiche l'adresse et le port de signalisation de l'appliance, le mode d'accélération (redirecteur ou transparent) et l'état de connexion, suivi d'un résumé des règles de l'appliance.

Onglet Connexions

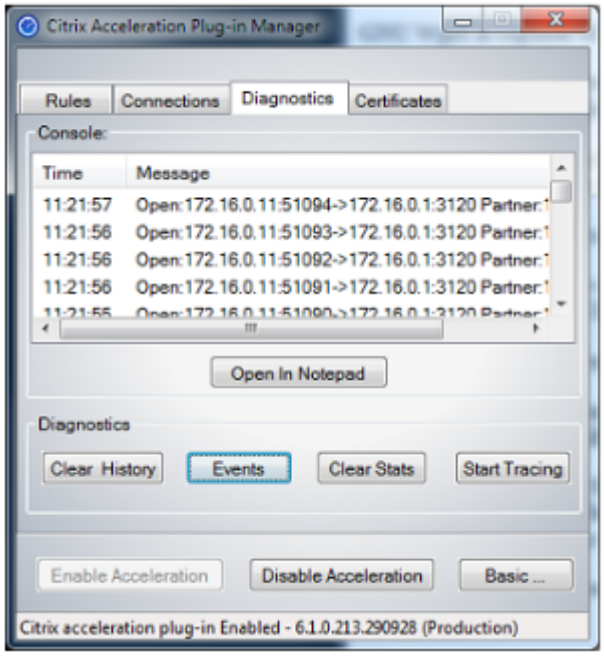
L'onglet **Connexions** répertorie le nombre de connexions ouvertes de différents types :

- **Connexions accélérées** : nombre de connexions ouvertes entre le plug-in client WANOP et les appliances. Ce numéro inclut une connexion de signalisation par appliance, mais n'inclut pas les connexions CIFS accélérées. Cliquez sur Plus pour ouvrir une fenêtre avec un bref résumé de chaque connexion. (Tous les boutons Plus vous permettent de copier les informations de la fenêtre dans le Presse-papiers, si vous souhaitez les partager avec le Support.)
- **Connexions CIFS accélérées** : nombre de connexions ouvertes et accélérées avec des serveurs CIFS (système de fichiers Windows). Ceci est généralement le même que le nombre de systèmes de fichiers réseau montés. Cliquez sur Plus pour afficher les mêmes informations que pour les connexions accélérées, ainsi qu'un champ d'état indiquant Actif si la connexion CIFS est en cours d'exécution avec les optimisations CIFS spéciales du plug-in client WANOP.
- **Connexions MAPI accélérées** : nombre de connexions Outlook/Exchange ouvertes et accélérées.
- **Connexions ICA accélérées : nombre de connexions**Citrix Virtual Apps and Desktops ouvertes et accélérées à l'aide des protocoles ICA ou CGP.
- **Connexions non accélérées** : ouvre les connexions qui ne sont pas accélérées. Vous pouvez cliquer sur Plus pour afficher une brève description des raisons pour lesquelles la connexion n'a pas été accélérée. En général, la raison en est qu'aucune appliance n'accélère l'adresse de destination, qui est signalée comme règle de stratégie de service.
- **Ouvrir/fermer les connexions** : connexions qui ne sont pas entièrement ouvertes, mais qui sont en cours d'ouverture ou de fermeture (connexions TCP « semi-ouvertes » ou « demi-fermées »). Le bouton Plus affiche des informations supplémentaires sur ces connexions.

Onglet Diagnostics

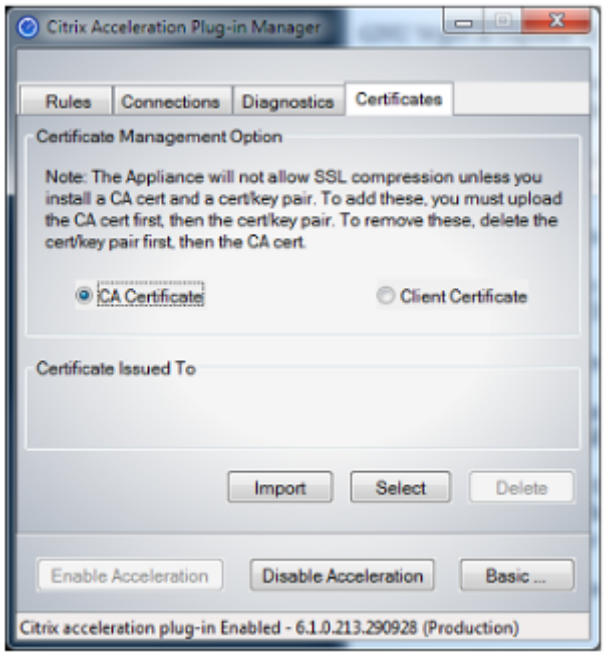
La page Diagnostics indique le nombre de connexions dans différentes catégories et d'autres informations utiles.

- **Démarrer le traçage/Arrêter le traçage** : si vous signalez un problème, votre représentant Citrix peut vous demander d'effectuer un suivi de connexion pour identifier les problèmes. Ce bouton démarre et arrête la trace. Lorsque vous arrêtez le suivi, une fenêtre contextuelle affiche les fichiers de suivi. Envoyez-les à votre représentant Citrix par les moyens qu'il recommande.
- **Effacer l'historique**—Cette fonctionnalité ne doit pas être utilisée.
- **Effacer les statistiques** : en appuyant sur ce bouton, les statistiques sont effacées dans l'onglet Performances.
- **Console** : fenêtre déroulante avec des messages d'état récents, principalement des messages d'ouverture de connexion et de fermeture de connexion, mais aussi des messages d'erreur et d'état divers.



Onglet Certificats

Sous l'onglet Certificats, vous pouvez installer des informations d'identification de sécurité pour la fonctionnalité d'appairage sécurisé facultative. Ces informations d'identification de sécurité ont pour but de permettre à l'appliance de vérifier si le plug-in est un client approuvé ou non.



Pour télécharger le certificat de l'autorité de certification et la paire de clés de certificat :

1. Sélectionnez **Gestion des certificats**de l'autorité de certification.
2. Cliquez sur **Importer**.
3. Chargez un certificat d'autorité de certification. Le fichier de certificat doit utiliser l'un des types de fichiers pris en charge (.pem, .crt., .cer ou .spc). Une boîte de dialogue peut s'afficher, vous demandant de sélectionner le magasin de certificats que vous souhaitez utiliser et de vous présenter une liste de mots-clés. Sélectionnez le premier mot clé dans la liste.
4. Sélectionnez **Gestion des certificats client**.
5. Cliquez sur **Importer**.
6. Sélectionnez le format de la paire de clés de certificat (PKCS12 ou PEM/DER).
7. Cliquez sur **Soumettre**.

> **Remarque**
>
> Dans le cas de PEM/DER, il existe des cases de téléchargement distinctes pour le certificat et la clé. Si votre paire de clés de certificat est combinée dans un seul fichier, spécifiez le fichier deux fois, une fois pour chaque case.

Mise à jour du plug-in Citrix SD-WAN WANOP

April 9, 2021

Pour installer une version plus récente du plug-in client WANOP, suivez la procédure que vous avez utilisée lors de l'installation du plug-in pour la première fois.

Désinstaller le plug-in client WANOP

Pour désinstaller le plug-in du client WANOP, utilisez l'utilitaire **Ajout/Suppression de programmes** Windows. Le plug-in client WANOP est répertorié comme **plug-in Citrix Acceleration** dans la liste des programmes actuellement installés. Sélectionnez-le et cliquez sur **Supprimer**.

Redémarrez le système pour terminer la désinstallation du client.

Accélération Citrix Virtual Apps and Desktops

April 9, 2021

> **Remarque**
>
> Dans cette discussion, *Virtual Apps* fait référence aux flux de protocole ICA et CGP. Par conséquent, ce qui est dit à propos des applications virtuelles s'applique également aux bureaux virtuels.

L'accélération des applications virtuelles/bureaux virtuels (ICA/CGP) comporte trois composantes :

- **Compression** : l'appliance coopère avec les clients et les serveurs Virtual Apps pour compresser les flux de données Virtual Apps pour les données interactives (clavier/souris/affichage/audio) et les données par lots (impression et transfert de fichiers). Cette interaction se déroule de manière transparente et ne nécessite aucune configuration de l'appliance. Une petite quantité de configuration, décrite ci-dessous, est requise sur les anciens serveurs Virtual Apps (version 4.x).
- **ICA multistream**—Outre la compression, les appliances Citrix SD-WAN WANOP prennent en charge le nouveau protocole ICA multistream, dans lequel jusqu'à quatre connexions sont utilisées pour les différentes priorités ICA, au lieu de multiplexer toutes les priorités sur la même connexion. Cette approche permet d'améliorer la réactivité des tâches interactives, en particulier lorsqu'elle est associée au traffic shaping de l'appliance.
- **Régulateur du trafic** : le régulateur du trafic Citrix SD-WAN WANOP utilise les bits de priorité dans les protocoles de données de Virtual Apps pour moduler la priorité de la connexion en temps réel, en faisant correspondre la part de bande passante de chaque connexion à ce que la connexion transmet en ce moment.

  > **Remarque**
  >
  > L'ICA multiflux est désactivée par défaut. Il peut être activé sur la page Fonctionnalités. Multi-Stream ICA et AutoQoS nécessitent l'activation de la fiabilité de session.

Pour optimiser les connexions ICA pour Citrix Virtual Apps and Desktops versions 7.0 et ultérieures, l'appliance Citrix SD-WAN WANOP prend en charge Citrix Receiver pour Chrome versions 1.4 et ultérieures, et Citrix Receiver pour HTML5 versions 1.4 et ultérieures.

Protocole de transport HDX de UDP/EDT à TCP —Dans certaines conditions réseau, UDP/EDT ne peut pas être utilisé comme protocole optimisé pour livrer le trafic HDX. Vous pouvez changer le protocole en TCP afin que WANOP puisse fournir :

- Avantages de compression/DDUP
- Visibilité (rapports locaux et HDX Insight)

WANOP peut bloquer le trafic EDT et forcer la session à TCP. Pendant l'initiation de la session, Citrix Receiver démarre la session sur TCP et EDT. Si la session EDT n'est pas établie, la session TCP est utilisée. L'interface graphique WANOP fournit une option pour forcer la session sur le protocole TCP sur la page des fonctionnalités.

Configurer l'accélération des applications virtuelles

April 9, 2021

L'accélération des applications virtuelles s'applique aux protocoles ICA et CGP dans les applications virtuelles. Les appliances WANOP Citrix SD-WAN, les serveurs d'applications virtuelles et les clients Virtual Apps fournissent une accélération coopérative des connexions Virtual Apps, offrant une accélération substantielle par rapport aux applications virtuelles seules. Cette coopération nécessite des versions à jour des trois composantes.

La compression des applications virtuelles bascule dynamiquement entre la compression basée sur la mémoire pour les canaux interactifs (tels que la souris, le clavier et les données d'écran) et la compression sur disque pour les tâches en bloc (telles que les transferts de fichiers et les tâches d'impression). Les ratios de compression augmentent à mesure que l'historique de compression se remplit, ce qui augmente la quantité de données pouvant être mises en correspondance avec les nouvelles données. La compression des applications virtuelles permet de réduire plusieurs fois plus de données que les applications virtuelles non assistées, dépassant souvent 50:1 sur les transferts groupés répétitifs tels que l'impression ou l'enregistrement de versions successives d'un même document.

La compression des applications virtuelles permet une utilisation élevée des liens sans encombrement, en empêchant les utilisateurs de s'interférer les uns avec les autres.

Pour activer l'accélération des applications virtuelles

1. Vérifiez la politique de classe de service ICA. Sur la page Configuration : Classes de service, la classe de service ICA doit afficher le disque dans la colonne Accélération et les priorités ICA dans la colonne Traffic Shaping. Sinon, modifiez la définition de la classe de service.
2. Mettez à jour les serveurs et les clients Virtual Apps 4.x. (Non nécessaire sur Virtual Apps 5.0 ou version ultérieure). Utilisez Presentation Server 4.5 avec correctif cumulatif PSE450W2K3R03 (bêta) ou version ultérieure. Cette version inclut les logiciels serveur et client suivants, qui doivent tous deux être installés pour la compression Virtual Apps :
    a) Package serveur PSE450R03W2K3ws.msp ou version ultérieure.
    b) Version client 11.0.0.5357 ou ultérieure.
3. Mettez à jour les serveurs et les clients Virtual Desktops vers la version 4.0 ou ultérieure.
4. Vérifiez les paramètres du registre du serveur Virtual Apps. (Non nécessaire sur Virtual Apps 5.0 ou version ultérieure.) Sur les serveurs Virtual Apps, vérifiez les paramètres suivants et corrigez-les ou créez-les si nécessaire :


```
pre codeblock HKLM\System\CurrentControlSet\Control\Citrix\
WanScaler\EnableForSecureIca = 1 HKLM\System\CurrentControlSet
\Control\Citrix\WanScaler\EnableWanScalerOptimization = 1 HKLM\
System\CurrentControlSet\Control\Citrix\WanScaler\UchBehavior = 2
 <!--NeedCopy-->
```

Ce sont toutes des valeurs DWORD.

5. Ouvrez et utilisez des connexions Virtual Apps, entre les clients et serveurs Virtual Apps mis à jour, qui passent par le WANOP Citrix SD-WAN mis à jour. Par défaut, ces sessions utilisent CGP. Pour ICA, sur le client, sous Citrix Program Neighborhood, désactivez la case à cocher Connexions ICA personnalisées. Ensuite, cliquez avec le bouton droit sur une icône de connexion, accédez à **Propriétés** > **Options**, puis cliquez sur **Activer la fiabilité de la session** case à cocher. Multi-Stream ICA et AutoQoS nécessitent l'activation de la fiabilité de session.
6. Vérifiez l'accélération.

   Après avoir démarré les sessions Virtual Apps via le lien accéléré, les connexions ICA accélérées doivent apparaître sur la page Surveillance : Connexions de l'appliance. Un rapport de compression supérieur à 1:1 indique que la compression a lieu.

Optimiser Citrix Receiver pour HTML5

April 23, 2021

Application qui doit servir le contenu dynamique fonctionne sur HTML5 WebSockets. Citrix Receiver pour Chrome et Citrix Receiver pour HTML5 sont des applications qui prennent en charge HTML5 WebSockets. Ces applications ont un accès simplifié aux bureaux virtuels car ils peuvent être intégrés aux navigateurs Web les plus récents prenant en charge HTML5 WebSockets.

> **Remarque**
>
> Vous n'avez pas besoin d'apporter des modifications à la configuration de l'appliance pour utiliser cette fonctionnalité.

Comment un dispositif Citrix SD-WAN WANOP optimise Citrix Receiver pour HTML5

Dans une installation standard de succursale et d'un centre de données, des ressources partagées telles que Virtual Desktop Agent (VDA) sont installées sur un serveur Citrix Hypervisor dans le centre de données. Les clients des succursales accèdent à ces ressources partagées via le réseau à l'aide de Citrix Receiver.

Dans une installation standard de succursale et d'un centre de données, des ressources partagées telles que Virtual Desktop Agent (VDA) sont installées sur un serveur Citrix Hypervisor dans le centre de données. Les clients des succursales accèdent à ces ressources partagées via le réseau à l'aide de Citrix Receiver.

Étant compatible HTML, VDA utilise un écouteur WebSocket qui s'exécute sur le port 8008. Lors de l'accès à une application, le client initie une connexion TCP au port 8008 et l'utilise pour envoyer une requête HTTP au serveur pour mettre à niveau la connexion et utiliser le protocole WebSocket. Après que le client négocie la connexion WebSocket avec VDA, les négociations ICA (Independent Computing Architecture) commencent et le client et le serveur utilisent ICA sur HTML5 pour échanger des données. Pour plus d'informations sur la séquence des messages échangés entre le client et le serveur, voir Messages échangés entre le client et le serveur.

Une fois les connexions établies entre les clients et le serveur, l'appliance Citrix SD-WAN WANOP commence à optimiser les connexions en accélérant le trafic sur le réseau et en accélérant la page Web et d'autres applications à l'aide de Citrix Receiver pour HTML5. La fonctionnalité d'optimisation des connexions Citrix Receiver pour HTML5 est similaire à HTTP Acceleration.

> **Remarque**
>
> - Pour plus d'informations sur HTML5, reportez-vous à la section Fonctionnement de HTML5.
> - Pour plus d'informations sur Citrix Receiver pour HTML5, reportez-vous à la section Receiver pour HTML5.
> - Pour plus d'informations sur la configuration système requise de Receiver pour HTML5, reportez-vous à la section Configuration système requise.

Configurer une appliance Citrix SD-WAN WANOP pour optimiser Citrix Receiver pour HTML5

L'optimisation des connexions Citrix Receiver pour HTML5 est une fonctionnalité de configuration zéro. Il n'est pas nécessaire de modifier la configuration de l'appliance. La mise à niveau du logiciel Citrix SD-WAN WANOP vers la version CB 7.3.1 ou ultérieure crée le classificateur d'applications alt-http sur l'appliance et mappe ce classificateur d'applications au port 8008, qui est la valeur par défaut pour Virtual Desktops. Dès que vous mettez à niveau le logiciel de l'appliance, il est prêt à optimiser les connexions Chrome natives qui utilisent Citrix Receiver pour HTML5.

Si vous utilisez le chiffrement SSL pour les connexions via Citrix Receiver pour HTML5, les connexions utilisent ICA sur SSL. Pour activer l'accélération ICA sur SSL avec Citrix Receiver pour HTML5, vous devez configurer l'accélération SSL standard, qui inclut l'adresse IP de destination appropriée dans la classe de service et le mappage de profil SSL. Si vous prévoyez de déployer l'appliance en mode proxy ICA, vous devez mapper l'adresse VIP StoreFront aux certificats StoreFront. De même, si vous prévoyez de déployer l'appliance dans un mode de déploiement de chiffrement SSL de bout en bout,

vous devez mapper l'adresse IP du VDA aux certificats VDA.

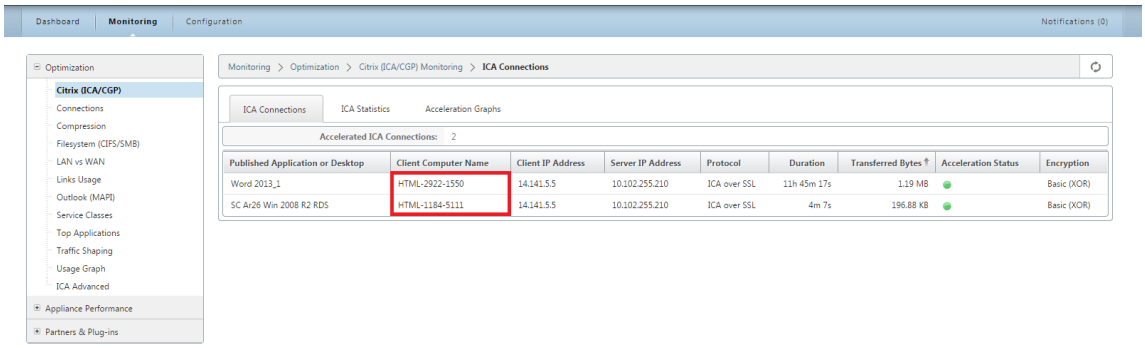
> **Avertissement**
>
> Assurez-vous que vous ne modifiez pas le numéro de port de l'application alt-http par un autre numéro de port. Si vous supprimez ce classificateur d'application ou que vous devez y apporter des modifications, vous devez ajouter le port 8008 au classificateur d'application HTTP.

Vérifier les connexions HTML5 de Citrix Receiver

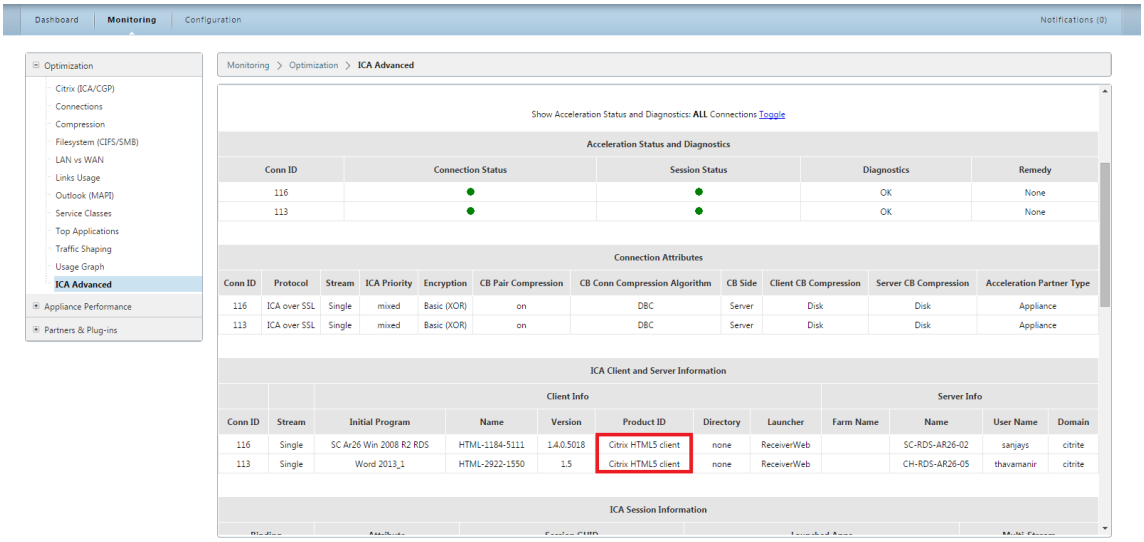
Pour vérifier que l'appliance optimise les connexions Citrix Receiver pour HTML5, vous pouvez vérifier si les connexions sont répertoriées dans les pages de surveillance Citrix (ICA/CGP) et ICA Advanced. L'existence de connexions HTML5 dans les pages de surveillance indique que l'appliance optimise les connexions Citrix Receiver pour HTML5.

Pour vérifier la connexion Citrix Receiver HTML5 sur un dispositif Citrix SD-WAN WANOP :

1. Accédez à la page **Surveillance** > **Optimisation** > **Citrix (ICA/CGP)**.
2. Sous l'onglet Connexions ICA, vérifiez que les connexions HTML5 sont répertoriées.** Une connexion HTML5 est affichée avec HTML comme préfixe dans la colonne Nom de l'ordinateur client, comme indiqué dans la capture d'écran suivante :



3. Accédez à la page **Surveillance > Optimisation > ICA Avancé**.
4. Dans l'onglet **Informations conn**, faites défiler jusqu'à la section Informations sur le client ICA et le serveur. Les entrées pour les connexions HTML5 ont le client Citrix HTML5 dans la colonne ID produit, comme illustré dans la capture d'écran suivante :

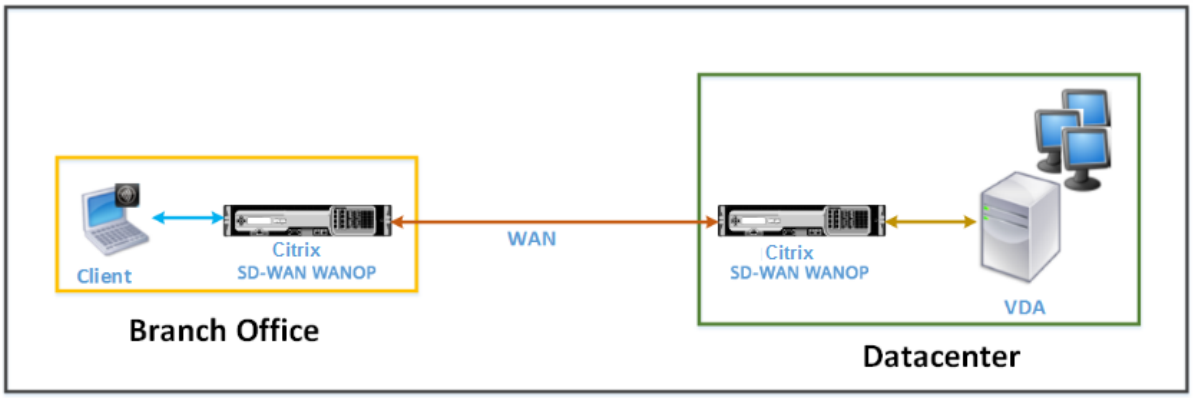


Modes de déploiement

April 23, 2021

Dans un déploiement WANOP SD-WAN typique de Citrix, les appliances Citrix SD-WAN WANOP sont jumelées entre les succursales et les centres de données. Vous installez des ressources partagées, telles que VDA, dans le centre de données. Les clients de diverses succursales accèdent aux ressources du centre de données à l'aide de Citrix Receiver, comme illustré dans la figure suivante.

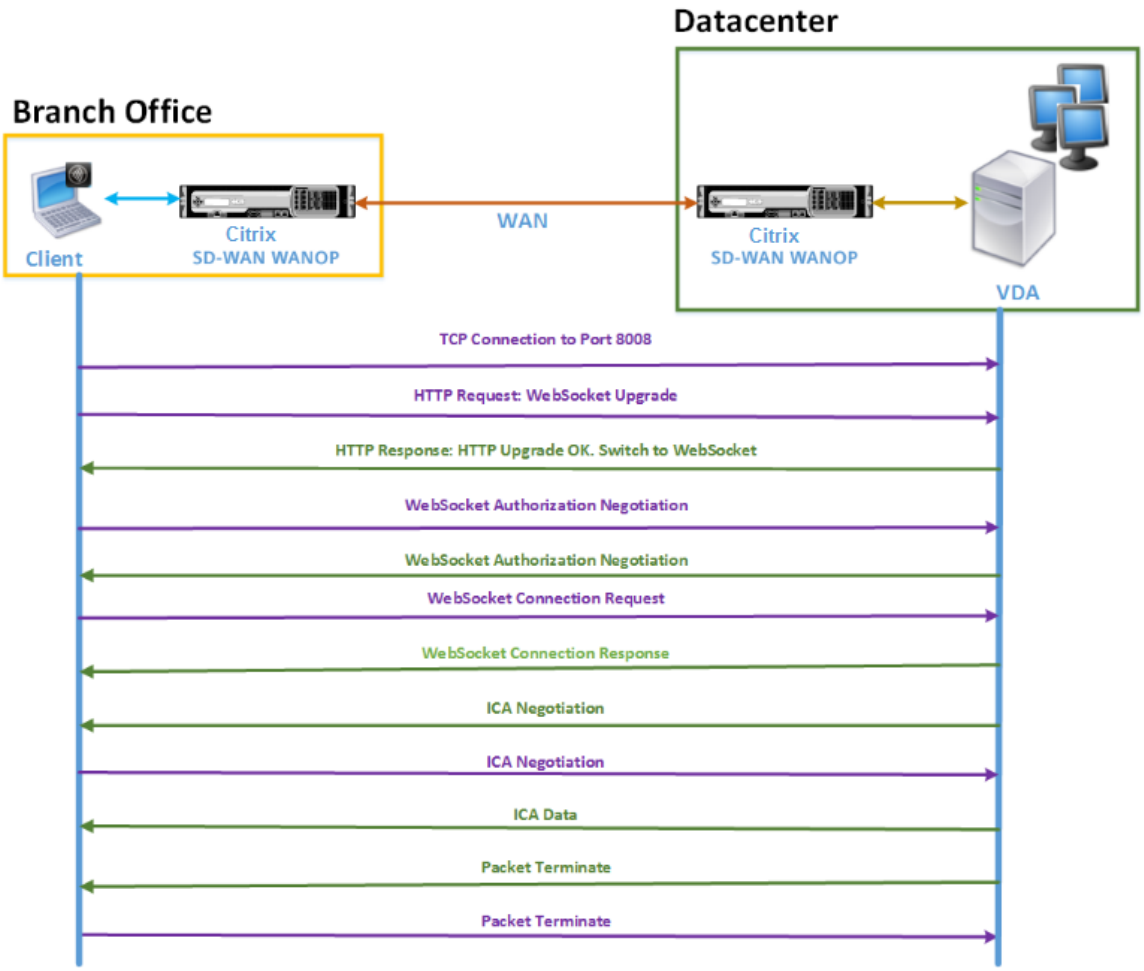
Topologie de déploiement WANOP SD-WAN typique de Citrix



Les clients installent un produit logiciel Citrix Receiver, tel que Citrix Receiver pour HTML5, sur leurs ordinateurs locaux et l'utilisent pour accéder aux ressources du centre de données. Les connexions via la paire d'appliances Citrix SD-WAN WANOP sont optimisées.

Comprendre les messages échangés entre le client et le serveur

Comme pour tout type de connexion réseau, un client utilisant Citrix Receiver pour HTML5 échange divers messages avec le serveur. La figure suivante montre un flux typique de messages entre le client et le serveur lorsqu'une connexion est établie entre eux.



Comme le montre la figure ci-dessus, la séquence de messages suivante est échangée entre le client et le serveur lorsqu'un client d'une succursale souhaite accéder aux ressources du serveur de centre de données :

1. Le client utilise Citrix Receiver pour HTML5 pour envoyer une demande de connexion TCP au VDA sur le port 8008.
2. Après avoir établi la connexion TCP, le client envoie une demande de mise à niveau WebSocket au VDA.
3. VDA répond à la demande de mise à niveau et passe au protocole WebSocket.
4. Le client et le VDA négocient l'autorisation WebSocket.
5. Le client envoie une demande de connexion WebSocket au VDA.

6. VDA répond à la demande de connexion WebSocket.
7. VDA lance la négociation ICA avec le client.
8. Après la négociation ICA, VDA commence à transmettre des données ICA.
9. Le VDA envoie un message de terminaison de paquets.
10. Le client répond avec le message de fin de paquet.

> **Remarque**
>
> L'exemple ci-dessus répertorie les exemples de messages échangés contre ICA sur WebSocket. Si vous utilisez ICA sur le protocole CGP (Common Gateway Protocol), le client et le serveur négocient CGP au lieu de WebSocket. Toutefois, pour ICA sur TCP, le client et le serveur négocient ICA.

Selon les composants que vous avez déployés sur le réseau, la connexion est interrompue à différents points. La figure précédente représente une topologie qui n'a pas de composants supplémentaires déployés sur le réseau. Par conséquent, le client communique directement avec le VDA au port 8008. Toutefois, si vous avez installé une Gateway, telle que Citrix Gateway, au centre de données, la connexion est établie avec la passerelle et elle proxie VDA. Jusqu'à ce que la passerelle négocie l'autorisation WebSocket, il n'y a aucune communication avec le VDA. Une fois que la passerelle a négocié l'autorisation WebSocket, elle ouvre une connexion avec VDA. Par la suite, la Gateway agit comme un intermédiaire et transmet les messages du client au VDA et vice versa.

De même, si un tunnel VPN est créé entre un plug-in de Gateway Citrix installé sur le client et Citrix Gateway installé sur le centre de données, la passerelle transmet de manière transparente tous les messages du client, dès l'établissement d'une connexion TCP, au VDA, et vice versa.

> **Remarque**
>
> Pour optimiser une connexion nécessitant un chiffrement SSL de bout en bout, une connexion TCP est établie sur le port 443 du VDA.

Modes de déploiement pris en charge

Lors de la configuration d'une appliance Citrix SD-WAN WANOP pour optimiser Citrix Receiver pour HTML5, vous pouvez prendre en compte l'un des modes de déploiement suivants, en fonction de vos besoins réseau. Pour optimiser les connexions Citrix Receiver pour HTML5, les appliances Citrix SD-WAN WANOP prennent en charge les modes de déploiement suivants :

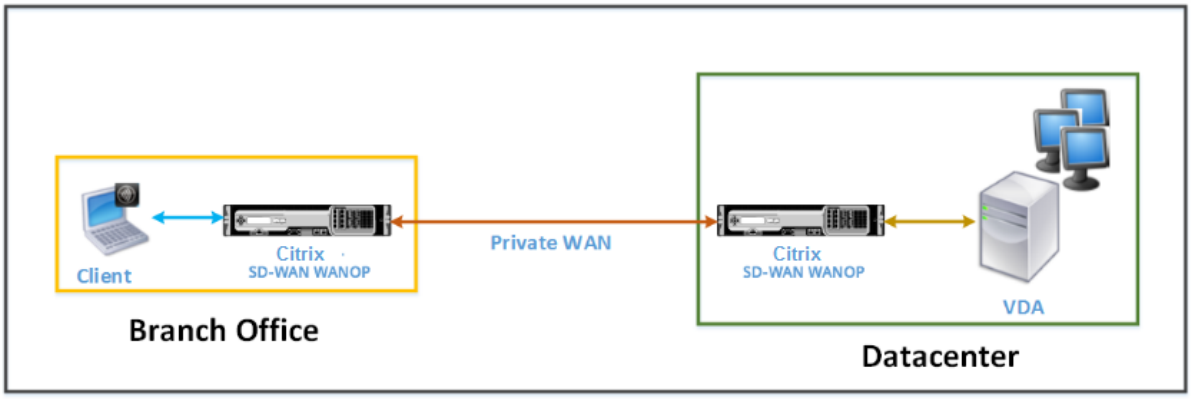
- Accès direct
- Accès direct avec chiffrement SSL de bout en bout
- Mode proxy ICA

- Mode proxy ICA avec chiffrement SSL de bout en bout
- Mode Réseau privé virtuel complet (VPN)
- Mode réseau privé virtuel (VPN) complet avec chiffrement SSL de bout en bout

Accès direct :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installée sur le client en mode d'accès direct.

Appliances Citrix SD-WAN WANOP déployées en mode accès direct



En mode accès direct, une paire d'appliances Citrix SD-WAN WANOP est installée sur une succursale et le centre de données en mode Inline. Un client accède aux ressources VDA via Citrix Receiver pour HTML5 sur le WAN privé. Les connexions entre le client et les ressources VDA sont sécurisées à l'aide du chiffrement au niveau ICA. Les messages échangés entre le client et le VDA sont expliqués dans la section Présentation des messages échangés entre le client et le serveur.

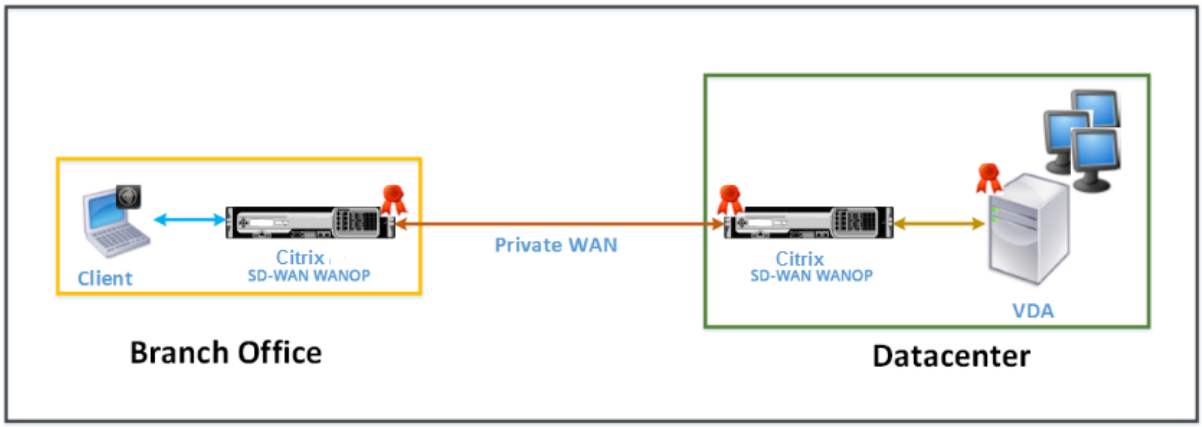
Les appliances Citrix SD-WAN WANOP installés entre le client et le centre de données VDA optimisent les connexions Citrix Receiver pour HTML5 établies entre eux.

Un déploiement d'accès direct convient à un intranet d'entreprise sur lequel les clients se connectent sans utiliser Citrix Gateway ou tout autre pare-feu. Vous déployez une configuration avec accès direct lorsque les appliances Citrix SD-WAN WANOP sont déployées en mode inline et qu'un client à partir d'un WAN privé se connecte aux ressources VDA.

Accès direct avec chiffrement SSL de bouten bout :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installée sur le client en mode d'accès direct sécurisé avec le chiffrement SSL de bout en bout.

Appliances Citrix SD-WAN WANOP déployées en mode d'accès direct sécurisées avec chiffrement SSL de bout en bout



L'accès direct avec le mode de chiffrement SSL de bout en bout est similaire au mode Accès direct, à la différence que la connexion entre le client et les ressources VDA est sécurisée par le cryptage SSL et utilise le port 443 au lieu du port 8008 pour la connexion.

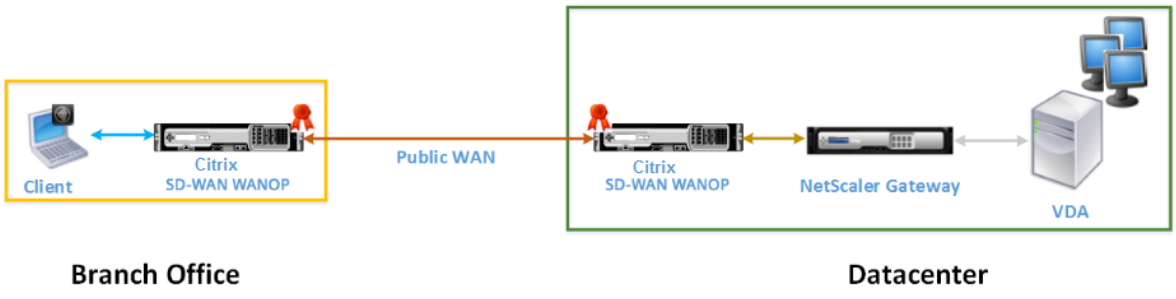
Dans ce déploiement, la communication entre une paire d'appliances Citrix SD-WAN WANOP est sécurisée en faisant en sorte que les deux partenaires soient sécurisés. Ce déploiement convient à un réseau d'entreprise où les connexions entre le client et les ressources VDA sont sécurisées par cryptage SSL.

> **Remarque**
>
> Vous devez configurer les certificats appropriés sur les appliances pour créer des partenaires sécurisés. Pour plus d'informations sur le partenariat sécurisé, reportez-vous à Peering sécurisé.

Mode proxy ICA :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installé sur le client en mode proxy ICA.

Appliances Citrix SD-WAN WANOP déployées en mode proxy ICA



En mode proxy ICA, une paire d'appliances Citrix SD-WAN WANOP est installée sur toute la succursale et un centre de données en mode inline. En outre, vous installez Citrix Gateway, qui proxie VDA, au

centre de données. Un client accède aux ressources VDA via Citrix Receiver pour HTML5 sur le WAN public. Étant donné que la passerelle proxie le VDA, deux connexions sont établies : une connexion SSL entre le client et Citrix Gateway et une connexion sécurisée ICA entre Citrix Gateway et VDA. Citrix Gateway établit une connexion avec les ressources VDA pour le compte du client. Les connexions entre la Gateway et les ressources VDA sont sécurisées par chiffrement au niveau ICA.

Les messages échangés entre le client et le VDA sont expliqués dans la section Présentation des messages échangés entre le client et le serveur. Toutefois, dans ce cas, la connexion est interrompue à Citrix Gateway. La passerelle proxie le VDA et ouvre une connexion au VDA uniquement après que la passerelle a négocié l'autorisation WebSocket. La Gateway transmet ensuite de manière transparente les messages du client au VDA et vice versa.

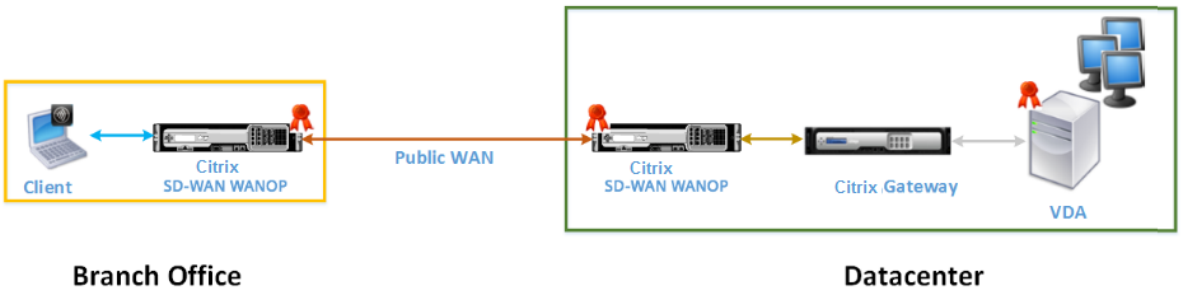
Si vous attendez des utilisateurs à accéder aux ressources VDA à partir d'un réseau étendu public, vous pouvez envisager de déployer le mode proxy ICA configuré.

> **Remarque**
>
> Vous devez configurer les certificats appropriés sur les appliances pour créer des partenaires sécurisés. Pour plus d'informations sur le partenariat sécurisé, reportez-vous à Peering sécurisé.

Mode proxy ICA avec chiffrement SSL de bouten bout :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installé sur le client en mode proxy ICA sécurisé avec un chiffrement SSL de bout en bout.

Appliances Citrix SD-WAN WANOP déployées en mode proxy ICA sécurisées avec chiffrement SSL de bout en bout



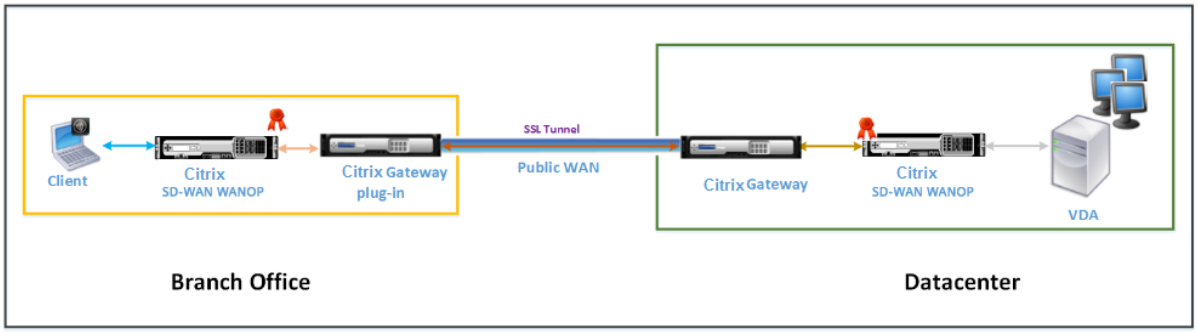
Le mode Proxy ICA avec le mode de chiffrement SSL de bout en bout est similaire au mode Proxy ICA ordinaire, à la différence que la connexion entre Citrix Gateway et VDA est sécurisée par le cryptage SSL au lieu d'utiliser une connexion sécurisée ICA. Dans ce scénario, vous devez installer les certificats appropriés sur le dispositif Citrix SD-WAN WANOP et le VDA. La connexion entre Citrix Gateway et le VDA utilise le port 443 au lieu du port 8008, comme dans le cas du mode proxy ICA ordinaire.

Ce déploiement convient à un réseau dans lequel vous devez sécuriser la communication de bout en bout entre les clients et le VDA, y compris la connexion entre Citrix Gateway et le VDA.

Mode réseau privé virtuel complet (VPN) :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installée sur le client en mode VPN (Virtual Private Network) complet.

Appliances Citrix SD-WAN WANOP déployées en mode VPN



En mode VPN complet, une paire d'appliances Citrix SD-WAN WANOP est installée sur une succursale et le centre de données en mode inline. En plus de Citrix Receiver pour HTML5, vous installez le plug-in Citrix Gateway sur le client et le réseau externe d'interface Citrix Gateway au niveau du centre de données. Le plug-in Citrix Gateway sur le client et Citrix Gateway sur le centre de données créent un tunnel SSL ou un VPN sur le réseau lorsqu'ils établissent une connexion. Par conséquent, le client dispose d'un accès sécurisé direct aux ressources VDA, avec une connexion transparente via l'appliance Citrix SD-WAN WANOP. Lorsque la connexion client est terminée sur Citrix Gateway, la Gateway ouvre une connexion transparente au port 8008 sur le VDA.

Les messages échangés entre le client et le VDA sont expliqués dans la section Présentation des messages échangés entre le client et le serveur. Toutefois, dans ce cas, la connexion est interrompue à Citrix Gateway. La Gateway proxie le VDA et ouvre une connexion transparente au VDA au port 8008, et transmet de manière transparente tous les messages du client au VDA et vice versa.

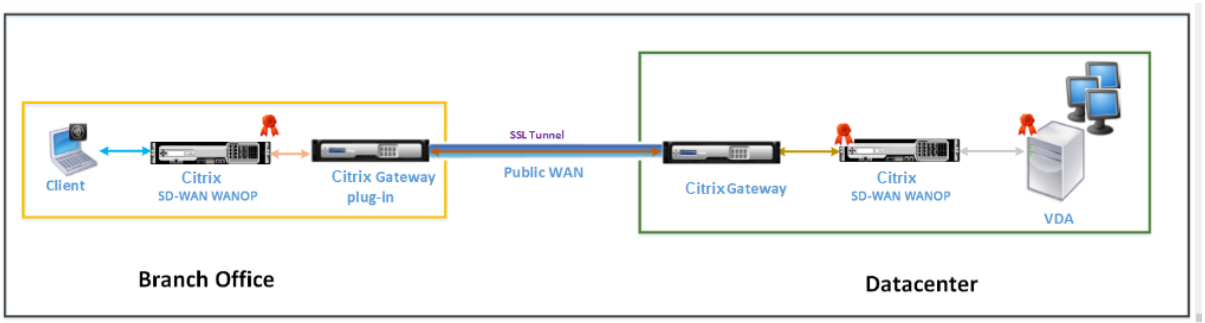
Le plug-in Citrix SD-WAN WANOP permet au client d'accéder aux ressources quel que soit l'emplacement du client. Lorsque vous vous attendez à ce que les clients aient besoin d'accéder aux ressources VDA à partir d'emplacements autres que leurs bureaux, vous pouvez déployer l'installation en mode VPN (Virtual Private Network) complet.

Ce déploiement convient aux organisations qui attendent de leurs employés qu'ils accèdent aux ressources lorsqu'ils se déplacent.

Mode réseau privé virtuel (VPN) complet avec chiffrement SSL de bouten bout :

La figure suivante illustre la topologie de déploiement de Citrix Receiver pour HTML5 installée sur le client en mode VPN complet sécurisé avec un chiffrement SSL de bout en bout.

Appliances Citrix SD-WAN WANOP déployées en mode VPN sécurisées avec chiffrement SSL de bout en bout



Le mode VPN (Virtual Private Network) complet avec déploiement de chiffrement SSL de bout en bout est similaire au mode VPN complet ordinaire, à la différence que la communication entre Citrix Gateway et VDA est sécurisée par le cryptage SSL et utilise le port 443 au lieu du port 8008.

Ce déploiement convient aux organisations qui ont besoin d'un chiffrement SSL de bout en bout pour les ressources accessibles par les employés en déplacement.

Interopérabilité du transport adaptatif

April 9, 2021

Le transport adaptatif est un mécanisme de transport de données pour Citrix Virtual Apps and Desktops. Plus rapide et évolutif, il améliore l'interactivité avec les applications et il est plus adapté aux connexions WAN et Internet longue distance difficiles. Le transport adaptatif assure une capacité à monter en charge élevée du serveur et une utilisation efficace de la bande passante. Le transport adaptatif permet aux canaux virtuels ICA de répondre automatiquement aux conditions changeantes du réseau. Les canaux basculent intelligemment entre le protocole Citrix appelé Enlightened Data Transport (EDT) et TCP afin d'offrir des performances optimales. Par défaut, le transport adaptatif est activé et l'EDT est utilisé lorsque cela est possible, avec repli à TCP.

Citrix SD-WAN WANOP offre une compression par jetons intersessions (déduplication des données), y compris la mise en cache vidéo basée sur l'URL. Il permet une réduction significative de la bande passante si deux personnes ou plus au bureau regardent la même vidéo récupérée par le client, ou transfèrent ou impriment des portions importantes du même fichier ou document. En outre, en exécutant les processus de réduction des données ICA et de compression des travaux d'impression au niveau de l'appliance de la succursale, WANOP décharge l'UC du serveur VDA et permet une plus grande capacité à monter en charge des serveurs Citrix Virtual Apps and Desktops.

Lorsque TCP est utilisé comme protocole de transport de données, Citrix SD-WAN WANOP prend en charge l'optimisation décrite ci-dessus. Lorsque vous utilisez Citrix SD-WAN WANOP sur des connexions réseau, choisissez TCP et désactivez EDT. En utilisant le contrôle de flux TCP et le contrôle de la

congestion, Citrix SD-WAN WANOP assure l'interactivité équivalente à l'EDT à une latence élevée et à une perte modérée de paquets.

Pour plus d'informations sur la configuration du transport adaptatif sur Citrix Virtual Apps and Desktops, reportez-vous à la section Transport adaptatif.

Mise à niveau Citrix Hypervisor 6.5

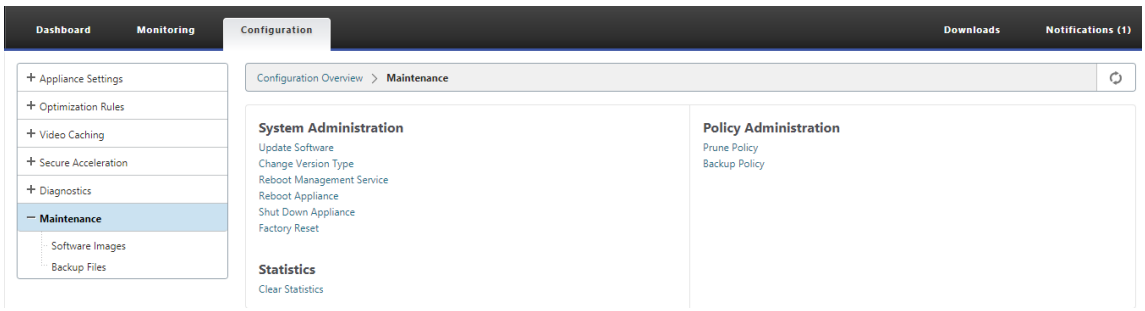
April 9, 2021

> **Important**
>
> **Pour effectuer une mise à niveau vers Citrix Hypervisor version 6.5, les appliances doivent exécuter le logiciel Citrix SD-WAN WANOP version 9.0.x ou ultérieure.**
>
> **Remarque**
>
> N'essayez pas de mettre à niveau lorsque l'appliance est exécutée sur une version inférieure à la version 9.0.x pour éviter les problèmes de mise à niveau.

Procédure de mise à niveau vers Citrix Citrix Hypervisor 6.5

Pour effectuer une mise à niveau vers Citrix Hypervisor 6.5 sur les appliances WANOP SD-WAN, assurez-vous que l'appliance exécute la version 9.0.x ou ultérieure. Si les appliances exécutent une version plus ancienne, effectuez la mise à niveau vers la dernière version du logiciel.

1. Dans l'interface graphique Citrix SD-WAN WANOP, accédez à **Configuration** > **Maintenance** > **Mise à jour du logiciel**. Téléchargez le fichier *ns-sdw-wo-<Build_No>.upg* pour mettre à niveau l'appliance.



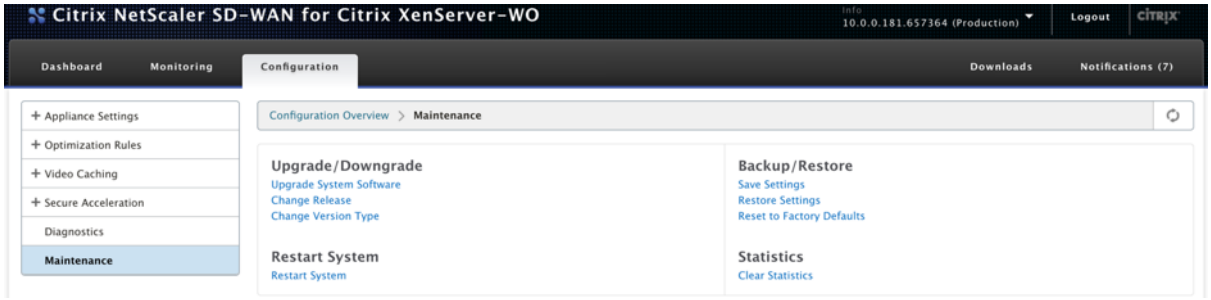
2. Après la mise à niveau vers la dernière version logicielle du logiciel WANOP, accédez à **Configuration > Maintenance > Mettre à jour le logiciel** dans l'interface graphique. Téléchargez le fichier *ns-sdw-xen65-pkg_v1.5.upg*.

3. Attendez environ 20 minutes avant la fin de la mise à niveau. L'appliance redémarre une fois la mise à niveau terminée.

Maintenance

April 23, 2021

Utilisez la page **Maintenance** pour effectuer des activités de maintenance telles que la mise à niveau du logiciel système, la sauvegarde et la restauration des configurations et l'effacement des statistiques.



Mise à niveau/rétrogradation

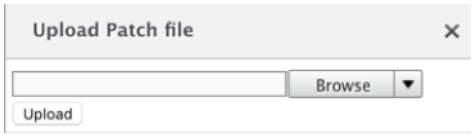
Mise à niveau du logiciel système

Il existe un package logiciel Citrix SD-WAN différent pour chaque modèle d'appliance. Vous devez télécharger le package logiciel SD-WAN WANOP approprié pour une appliance que vous souhaitez inclure dans un réseau et l'enregistrer sur votre disque local.

Le logiciel de l'appliance est mis à niveau à l'aide de fichiers correctifs que vous obtenez auprès de Citrix.

> **NOTE** :
>
> Si les appliances exécutent une version plus ancienne, vous devez d'abord effectuer une mise à niveau vers la dernière version du logiciel.

Pour mettre à niveau le logiciel système, accédez à **Configuration > Maintenance**. Sélectionnez **Mettre à niveau le logiciel système** sous **Mise à niveau et rétrogradation**. Sélectionnez le fichier de correctif et téléchargez-le sur l'appliance.



Le fichier de correctifs sera examiné par l'appliance. Seul un fichier de correctifs valide peut mettre à niveau le système vers une version différente de celle actuellement utilisée.

Une mise à niveau préserve les fichiers de licence et les paramètres système. L'unité mise à niveau ne nécessite aucune reconfiguration, sauf pour les nouvelles fonctionnalités qui ont été ajoutées avec la nouvelle version.

Modifier la version

La page de version des modifications affiche la version actuellement installée. Si vous souhaitez modifier la version de la version, cliquez sur l'option **Modifier la version**, sélectionnez la version dans la liste déroulante, puis cliquez sur **Modifier**.

Modifier le type de version

L'option **Modifier le type de version** vous permet de sélectionner une version de débogage de la version. Vous pouvez sélectionner le type de version dans la liste déroulante **Type** et cliquer sur **Modifier**. Voici les versions de débogage possibles :

- Valeur par défaut
- Niveau 1
- Niveau 2
- MC par défaut
- Niveau 1 MC
- Niveau 2 MC

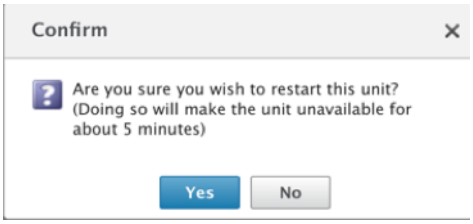
Vous devez effectuer cette action conformément aux instructions de l'équipe de support.

Redémarrer le système

Une fois qu'un correctif est installé, un message contextuel vous demandera si l'appliance peut être redémarrée. Le correctif ne sera pas appliqué tant que l'appliance n'a pas été redémarrée. Si vous

choisissez de ne pas redémarrer le système immédiatement, un rappel sera placé en haut de chaque page.

Cliquez sur **Redémarrer le système** pour redémarrer l'appliance WANOP SD-WAN. Ce processus prend plusieurs minutes.



Paramètres de sauvegarde

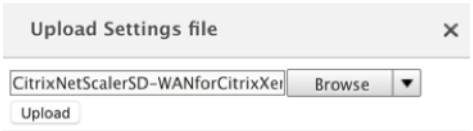
Vous pouvez sauvegarder la configuration de l'appliance en l'enregistrant sous forme de fichier texte.

Cliquez sur **Enregistrer les paramètres**, un fichier texte est téléchargé sur votre disque local. Les fichiers de licence, les paramètres SSH et les adresses IP de la page Gestion IP ne peuvent pas être enregistrés. Le fichier est un fichier texte ordinaire, mais ne doit pas être modifié manuellement.

Restaurer les paramètres

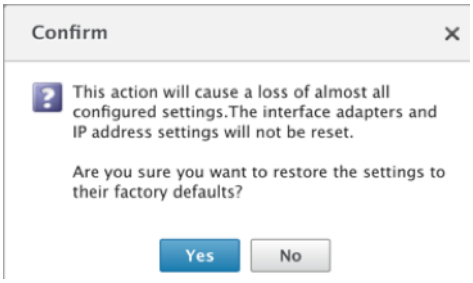
Une fois le fichier enregistré, il peut être restauré dans le même dispositif SD-WAN WANOP.

L'appliance conserve des copies d'anciennes versions. L'option**Restaurer les paramètres** permet de restaurer les paramètres configurés. Les fichiers de licences, les paramètres SSH et les adresses IP de la page Gestion IP ne sont pas copiés de la version la plus récente vers l'ancienne. Au lieu de cela, l'appliance rétablit les paramètres en vigueur au moment de la mise à niveau de l'ancienne version.



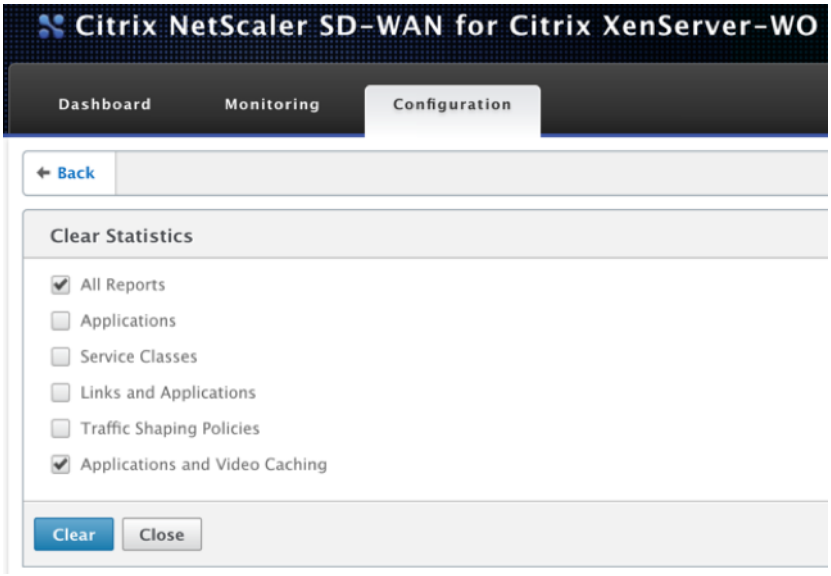
Réinitialiser les paramètres d'usine par défaut

L'option**Réinitialiser les paramètres par défaut d'usine** permet de réinitialiser les paramètres. Il définit tous les paramètres à l'exception des adresses IP, des paramètres de bande passante et des licences à leurs paramètres d'usine. Cliquez sur **Réinitialiser les valeurs par défaut d'usine**, un message de confirmation s'affiche. Cliquez sur **Oui** si vous souhaitez restaurer les paramètres par défaut.



Statistiques claires

La page**Effacer les statistiques** permet de réinitialiser les statistiques de l'appliance WANOP SD-WAN. Il permet également de créer des rapports qui commencent au début de la fenêtre d'échantillonnage souhaitée. Sélectionnez les options statistiques à effacer de l'appliance, puis cliquez sur Effacer.**



Diagnostics

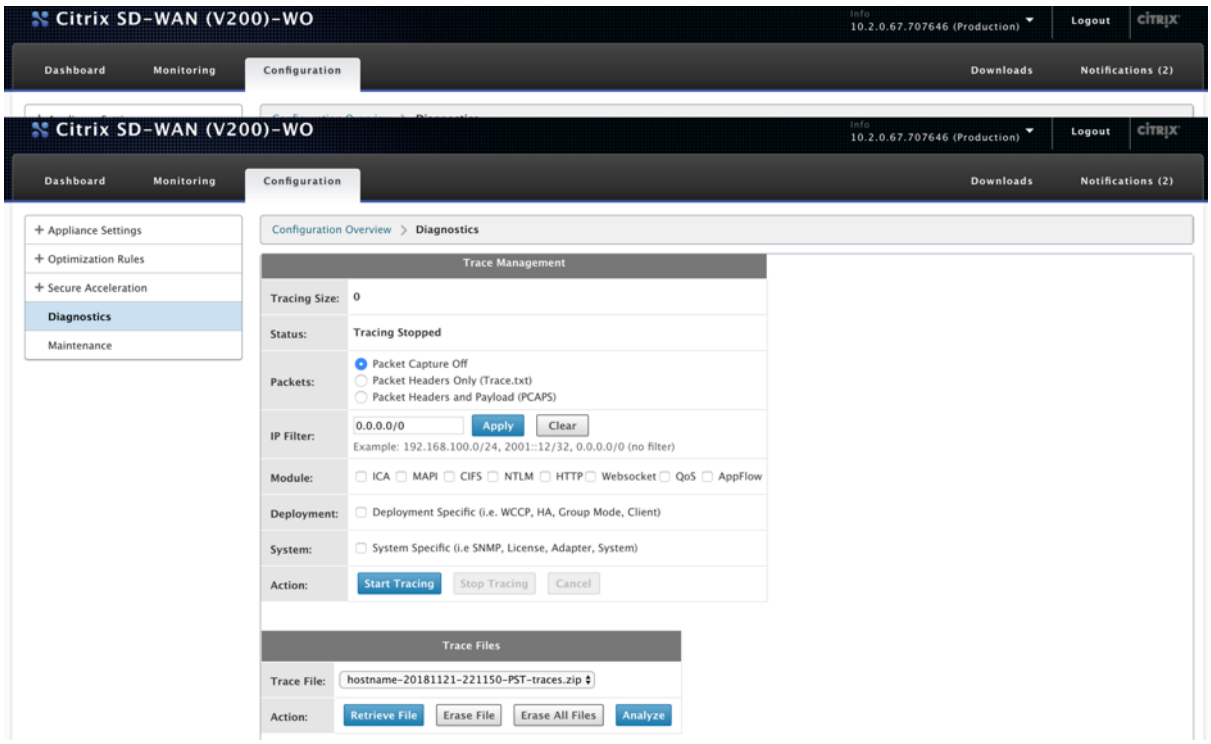
April 9, 2021

Cette section fournit des outils de diagnostic pour identifier les problèmes de réseau dans votre réseau WANOP SD-WAN et les résoudre. Vous pouvez également obtenir des fichiers journaux système, des informations système et d'autres informations nécessaires pour aider l'équipe de support Citrix SD-WAN à diagnostiquer et résoudre les problèmes réseau.

Voici l'outil de diagnostic disponible dans SD-WAN WANOP :

- Traçage

- Analyseur de paquets
- Test de carte de contournement
- Récupérer le cours
- Testeur de ligne
- Ping
- Traceroute
- Infos système
- Données de diagnostic



Traçage

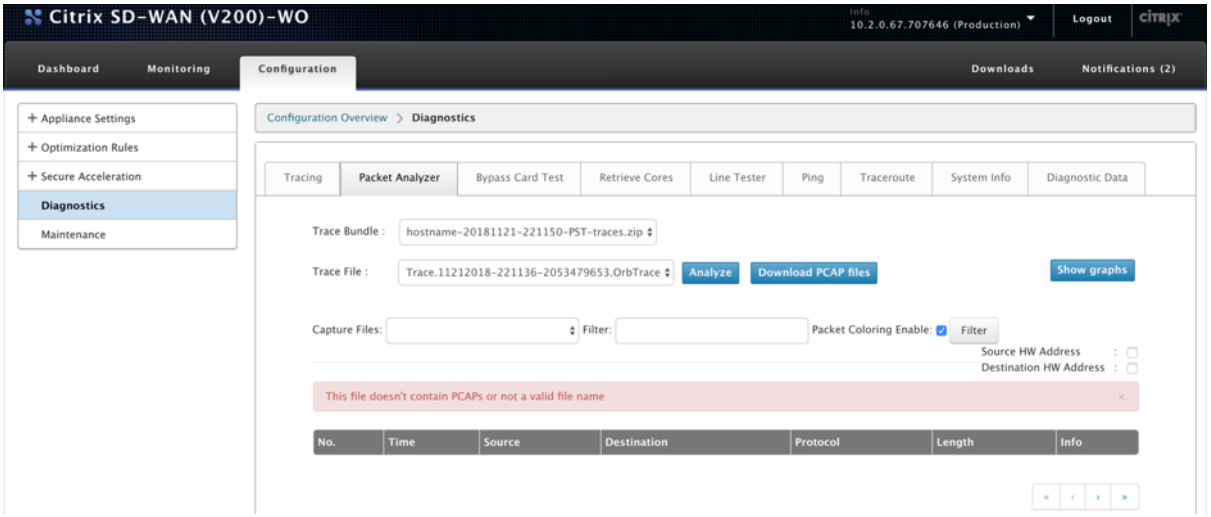
L'outil **de suivi** est utilisé pour surveiller les paquets circulant sur le réseau WANOP SD-WAN. Il peut ouvrir chaque paquet et identifier le protocole utilisé, l'adresse IP de la source et de la destination, ainsi que d'autres informations de charge utile. Ces informations sont utilisées par l'équipe de support Citrix pour trouver la cause première des problèmes réseau.

Vous pouvez choisir de suivre **les en-têtes de paquet uniquement** ou les **en-têtes de paquet et la charge utile**. Vous pouvez choisir le module à suivre et spécifier si le suivi doit être spécifique au déploiement ou au système.

Cliquez sur Démarrer le suivi, l'appliance commence à suivre les paquets.** **Les résultats sont empaquetés**
dans une archive ZIP lorsque vous cliquez sur **Arrêter le suivi. Cette archive peut être

téléchargée sur votre
ordinateur à l'aide de l'option **Récupérer le fichier**. Vous pouvez ensuite transférer ces fichiers à l'équipe de support. Les fichiers de suivi fournissent également des données d'analyse de plantage.

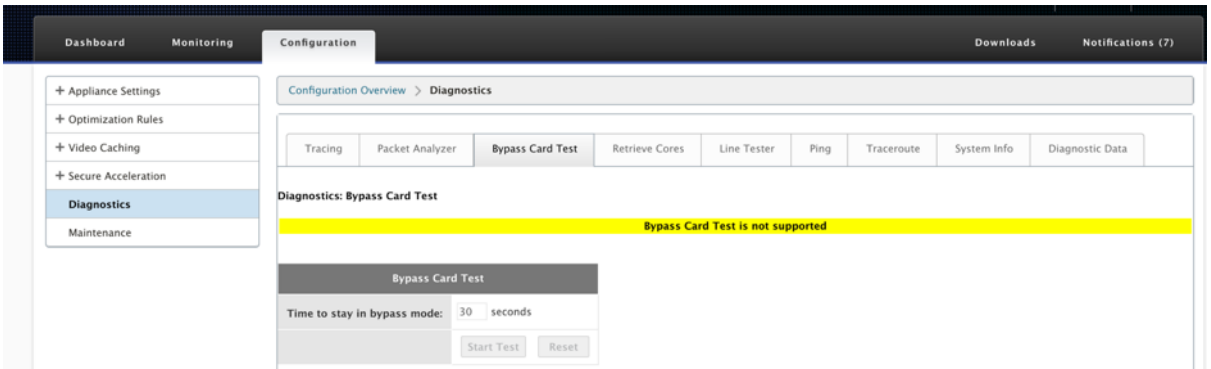
Cliquez sur **Analyser** pour afficher plus d'informations sur les **paquets dans l'onglet Analyseur** de paquets.



Vous pouvez afficher l'heure, l'adresse source, l'adresse de destination, le protocole, la longueur et les informations de charge utile.

Test de carte de contournement

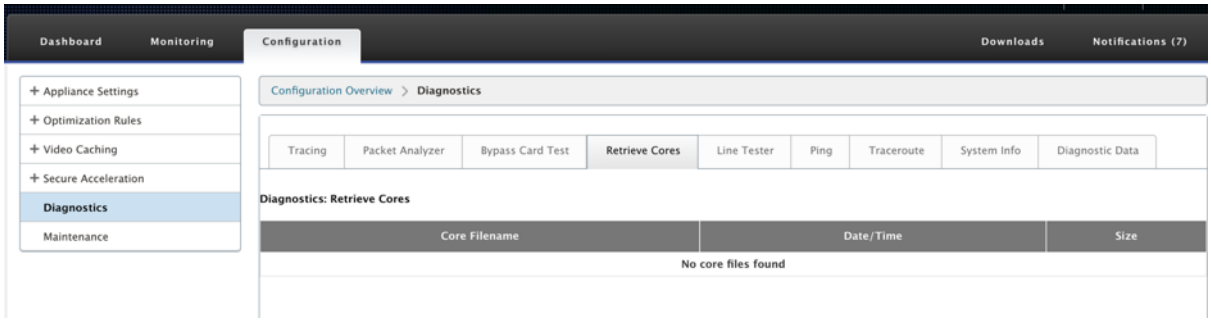
Vous pouvez tester la fonctionnalité de faille à fil de l'interface Ethernet pour un déploiement de matériel en mode Inline (Fail-to-Wire). Entrez le nombre de secondes pendant lesquelles l'appliance doit rester en mode de contournement, puis cliquez sur Démarrer le test.** Pendant cette période, l'appliance est contournée. Le fonctionnement normal reprendra après cela.



Récupérer les cœurs

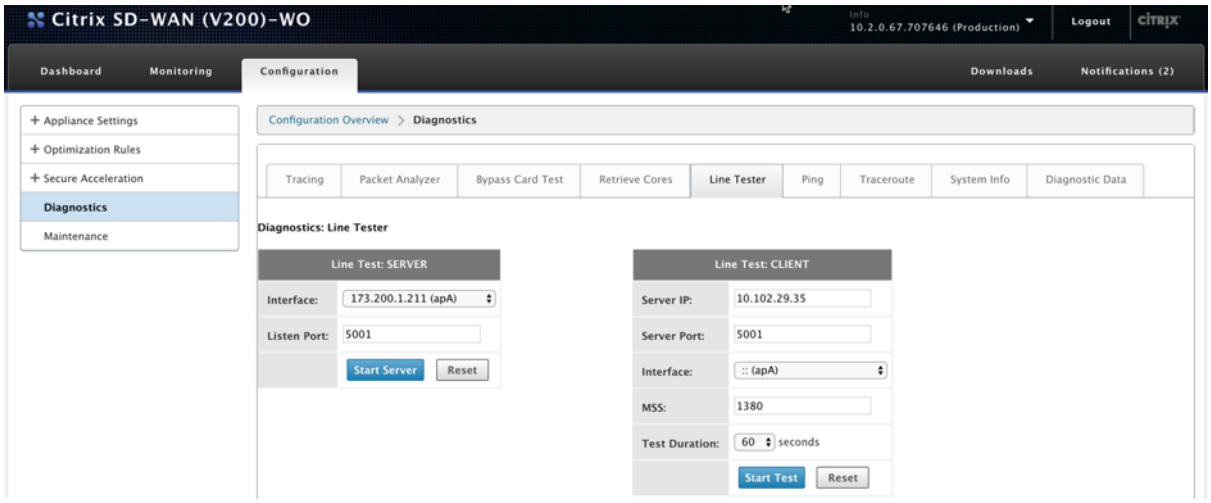
Les fichiers de**base** sont créés lorsque l'appliance WANOP SD-WAN se ferme anormalement ou se bloque. L'appliance redémarre automatiquement après un plantage. En cas de plantages persistants, l'accélération est désactivée mais l'interface de gestion reste active.

Vous pouvez sélectionner et récupérer les fichiers principaux requis qui ont été créés pendant le plantage de l'appliance ou lorsque l'appliance s'est comportée analement. Les fichiers récupérés sont enregistrés dans une archive ZIP. Vous pouvez le partager avec l'équipe de support pour une analyse plus approfondie.

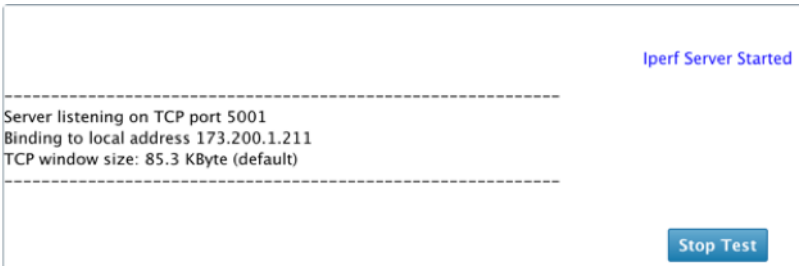


Testeur de ligne

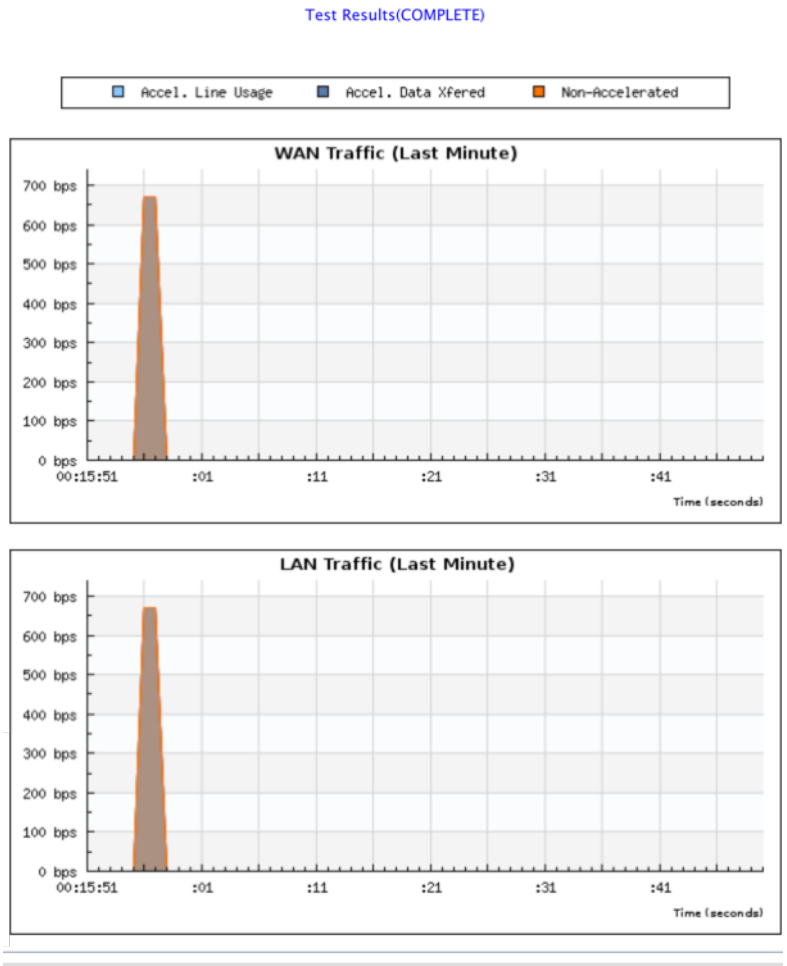
La fonction **Test de ligne : SERVER** démarre un serveur iperf sur l'appliance, s'exécutant en mode TCP. Cette option peut être utilisée pour vérifier la connectivité entre les appliances WANOP et le dépannage du trafic réseau. Pour exécuter les tests iperf, un système (une appliance ou un autre hôte) doit exécuter iperf en tant que serveur, et un autre doit s'y connecter en tant que client.



Vous pouvez utiliser l'interface et le numéro de port **du serveur Line Tester** par défaut. Cliquez sur **Démarrer le serveur** pour démarrer un serveur iperf sur l'appliance.

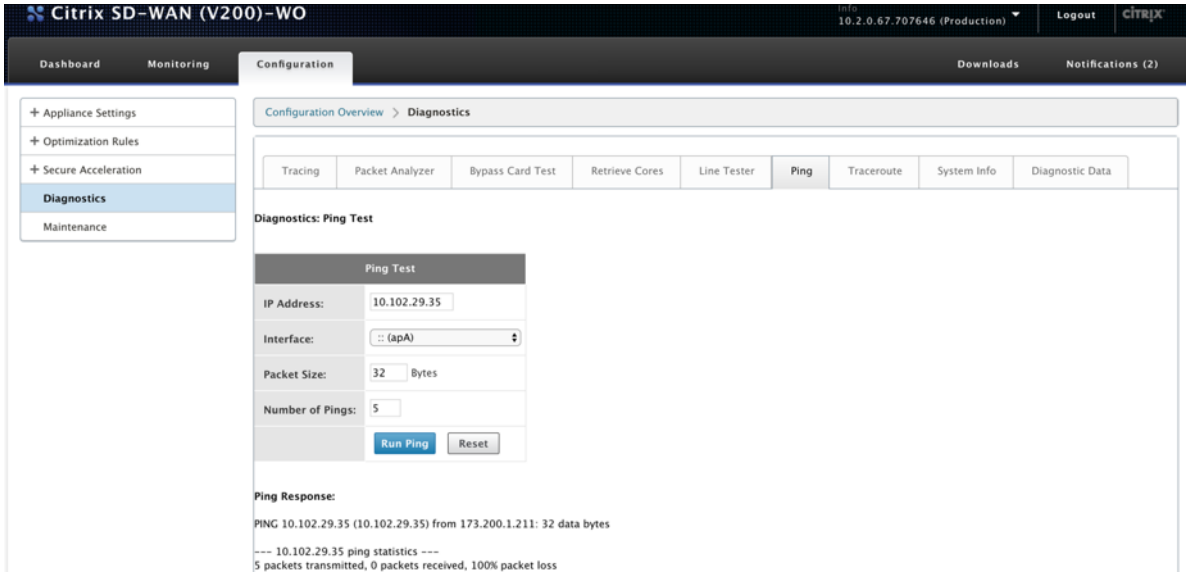


La fonction **Test de ligne : CLIENT** démarre un client iperf sur l'unité, s'exécutant en mode TCP. Vous pouvez également spécifier le numéro de port du serveur iperf et la longueur du test. Lorsque l'essai est terminé, la vitesse de connexion est indiquée. Cliquez sur **Démarrer le test** pour afficher le résultat du trafic WAN et LAN.



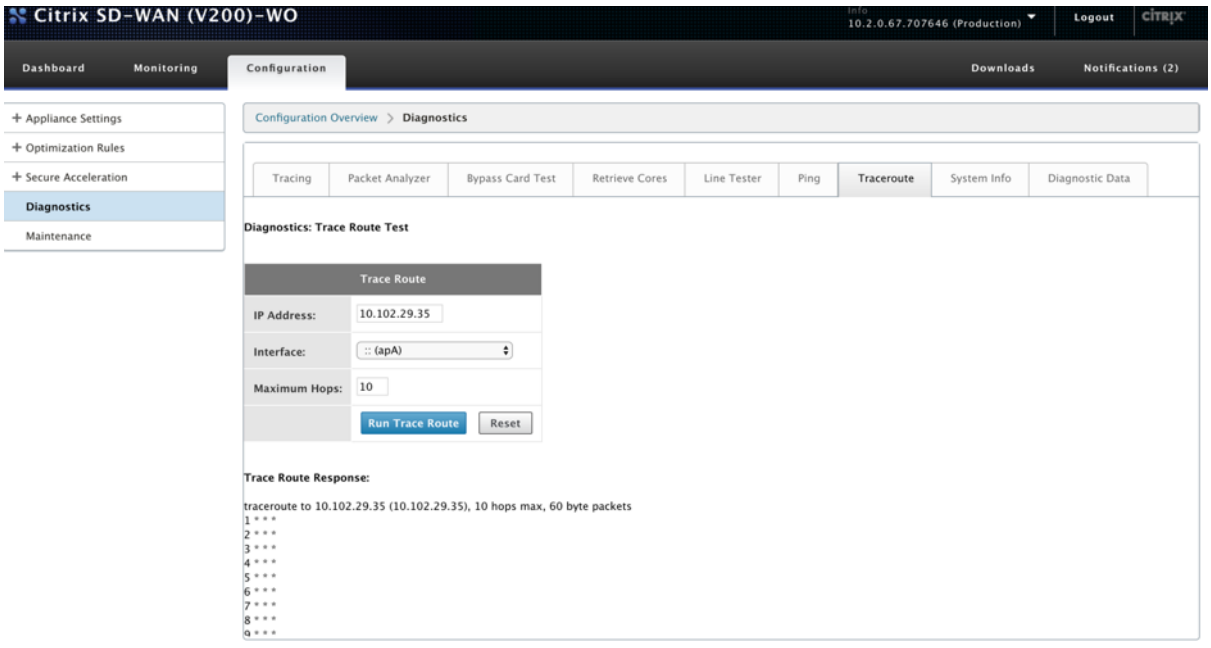
Ping

Ping vous permet de vérifier la connectivité des éléments réseau de votre réseau SD-WAN. Entrez l'adresse IP de l'élément réseau et cliquez sur **Exécuter Ping** pour afficher le résultat.



Traceroute

Traceroute vous permet d'enregistrer l'itinéraire entre votre appliance SD-WAN et tout autre élément réseau de votre réseau SD-WAN ou sur Internet. Il calcule et affiche la durée de chaque saut.

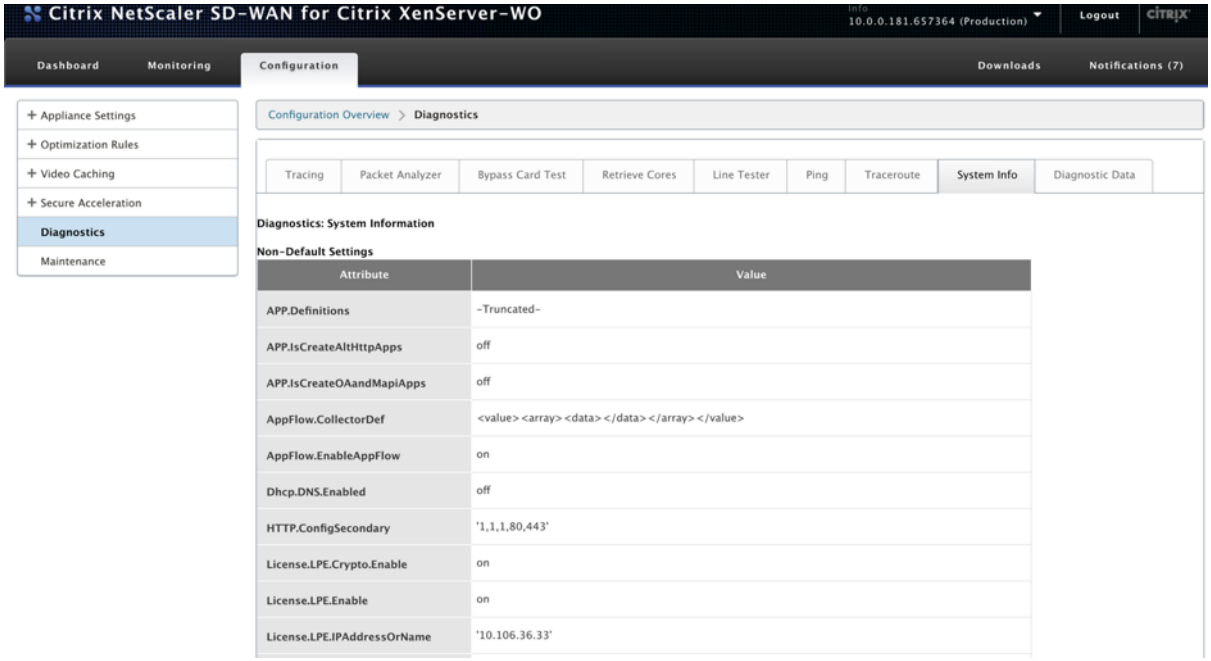


Infos système

Les **informations système** répertorient tous les paramètres qui ne sont pas définis sur leurs valeurs par défaut. Ces informations sont en lecture seule. Il est utilisé par le support lorsqu'une erreur de

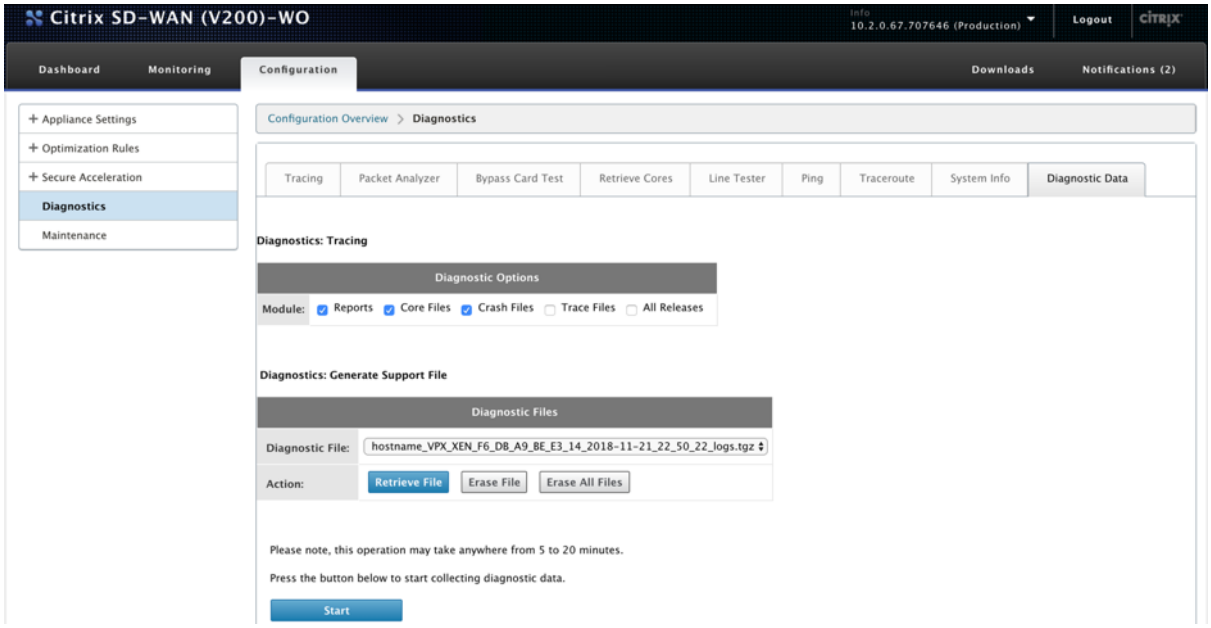
configuration est suspectée. Lorsque vous signalez un problème, vous pouvez être invité à vérifier une ou plusieurs valeurs sur cette page.

Il fournit des **paramètres autres que par défaut, des informations détaillées pour l'adaptateur principal, des informations détaillées pour l'adaptateur apA.2**et **des informations détaillées pour l'adaptateur apA.1**.



Données de diagnostic

Les données de diagnostic vous permettent de mettre en package des données de diagnostic pour analyse par l'équipe de support Citrix. Sélectionnez les fichiers de diagnostic requis et cliquez sur **Démarrer**. Vous pouvez ensuite cliquer sur **Récupérer le fichier** pour télécharger l'archive zip et la partager avec Citrix Support.



Résolution des problèmes

April 23, 2021

Les rubriques suivantes fournissent une liste des problèmes, la cause du problème et les étapes de résolution de certaines fonctionnalités Citrix SD-WAN WANOP.

CIFS et MAPI

Plug-in Citrix SD-WAN WANOP

RPC sur HTTPS

Mise en cache de vidéo

Accélération Citrix Virtual Apps and Desktops

CIFS et MAPI

April 9, 2021

- **Problème** : Un Controller de domaine est supprimé du réseau. Toutefois, l'appliance Citrix SD-WAN WANOP ne peut pas quitter le domaine.

  Cause : il s'agit d'un problème connu avec l'appliance.

Solution : à partir de la page Domaine Windows, modifiez le DNS en celui par lequel vous pouvez résoudre le domaine prévu. Ensuite, utilisez l'option
Rejoin Domain pour que l'appliance Citrix SD-WAN WANOP rejoigne ce domaine. Maintenant, essayez de quitter le domaine.

- **Problème** : les connexions MAPI ne sont pas optimisées et le message d'erreur suivant s'affiche :

  paramètre non par défaut dans Outlook n'est pas pris en charge

  Cause : Il s'agit d'un problème connu avec la version 6.2.3 et les versions antérieures.

  Résolution : mettez à niveau l'appliance vers la dernière version.

- **Problème** : l'appliance a optimisé les connexions MAPI. Toutefois, les pages de surveillance affichent le nombre d'octets envoyés et reçus comme zéro.

  Cause : il s'agit d'un problème connu avec l'appliance.

  Résolution : il s'agit d'un problème bénin qui n'affecte pas les fonctionnalités de l'appliance. Vous pouvez l'ignorer.

- **Problème** : impossible d'établir un appairage sécurisé entre les appliances Citrix SD-WAN WANOP.

  Cause : L'appairage sécurisé avec l'appliance partenaire n'est pas correctement configuré.

  Résolution : procédez comme suit :

  1. Vérifiez que vous avez téléchargé la combinaison appropriée de certificats d'autorité de certification et de serveur vers l'appliance.
  2. Accédez à la page **Citrix SD-WAN WANOP** > **Configuration** > **Paramètres SSL** > **Partenaires sécurisés**.
  3. Dans la section **Sécurité des partenaires**, sous **Vérification des certificats**, sélectionnez **Aucun - autoriser toutes les demandes** pour vous assurer que le certificat n'expire jamais.
  4. Vérifiez que l'appliance peut établir un appairage sécurisé avec l'appliance partenaire.
  5. Vérifiez que la section **Écouter sur** contient une entrée pour l'adresse IP de l'appliance Citrix SD-WAN WANOP prévue.

- **Problème** : Lors de la connexion à un cluster Exchange, les utilisateurs Outlook avec des connexions optimisées sont parfois contourné ou invité à entrer des informations d'identification d'ouverture de session.

  Cause : L'optimisation MAPI nécessite que chaque nœud du cluster Exchange soit associé au nom principal de service (SPN) ExchangeMDB. Au fil du temps, comme vous avez besoin de

plus de capacité, vous ajoutez des nœuds supplémentaires au cluster. Cependant, parfois, la tâche de configuration peut ne pas être terminée, laissant certains nœuds dans le cluster sans paramètres SPN. Ce problème est le plus répandu dans les clusters Exchange avec Exchange Server 2003 ou Exchange Server 2007.

Résolution : effectuez les opérations suivantes sur chaque serveur Exchange de la configuration :

1. Accédez au Controller de domaine.
2. Ouvrez l'invite de commandes.
3. Exécutez les commandes suivantes :

```
pre codeblock setspn -A exchangeMDB/Exchange1 Exchange1
setspn -A exchangeMDB/Exchange1.example.com Exchange1 <!--
NeedCopy-->
```

- **Problème** : lors de la tentative de connexion à Outlook, le message Essayer de connexion s'affiche, puis la connexion est interrompue.

  Cause : l'appliance Citrix SD-WAN WANOP côté client comporte des entrées de liste noire qui n'existent pas sur l'appliance côté serveur.

  Résolution : supprimez les entrées de liste noire des deux appliances ou mettez (recommandé) à niveau le logiciel des appliances vers la version 6.2.5 ou ultérieure.

- **Problème** : l'appliance ne parvient pas à joindre le domaine même après avoir passé les vérifications préalables au domaine.

  Cause : Il s'agit d'un problème connu.

  Résolution : procédez comme suit :

  1. Accédez à l'appliance à l'aide d'un utilitaire SSH.
  2. Connectez-vous à l'appliance à l'aide des informations d'identification racine.
  3. Exécutez la commande suivante :

     ```
     /opt/likewise/bin/domainjoin-cli join \<Domain\\_Name\>
     administrator
     ```

- **Problème** : le message d'erreur LdapError s'affiche lorsque vous ajoutez un utilisateur délégué à l'appliance Citrix SD-WAN WANOP.

  Résolution : effectuez l'une des opérations suivantes :

  - Sur le serveur DNS de l'appliance Citrix SD-WAN WANOP, vérifiez qu'une zone de recherche inversée est configurée pour chaque adresse IP de contrôleur de domaine.

  - Vérifiez que l'horloge système de l'ordinateur client est synchronisée avec l'horloge système du serveur Active Directory. Lors de l'utilisation de Kerberos, ces horloges doivent être synchronisées.
  - Mettez à jour l'utilisateur délégué sur la page Domaine Windows en fournissant à nouveau le mot de passe de l'utilisateur délégué.

- **Problème** : le message d'erreur de décalage temporel s'affiche lorsque vous ajoutez un utilisateur délégué à l'appliance Citrix SD-WAN WANOP.

  Résolution : vérifiez que l'appliance est jointe au domaine. Si ce n'est pas le cas, joignez l'appliance au domaine. Cette opération synchronise l'heure de l'appliance avec l'heure du serveur de domaine-domaine et résout le problème.

- **Problème** : le client est temporairement exclu pour l'accélération. Le message d'erreur Dernière erreur (erreur Kerberos.) s'affiche lorsque vous ajoutez un utilisateur délégué à l'appliance Citrix SD-WAN WANOP.

  Cause : l'utilisateur délégué est configuré pour l'authentification **Utiliser Kerberos uniquement**.

  Résolution : Vérifiez que, sur le Controller de domaine, le paramètre d'authentification de l'utilisateur délégué est **Utiliser n'importe quel protocole d'authentification**.

- **Problème** : le message d'erreur utilisateur délégué non prêt s'affiche lorsque vous ajoutez un utilisateur délégué à l'appliance Citrix SD-WAN WANOP.

  Résolution : si le message apparaît uniquement sur l'appliance côté client, ignorez-le. Toutefois, si le message s'affiche sur l'appliance côté serveur, exécutez l'outil de prévérification utilisateur délégué, disponible sur la page **Domaine Windows**, puis configurez l'utilisateur délégué sur l'appliance côté serveur.

- **Problème** : Dernière erreur (le serveur n'est pas délégué pour l'authentification Kerberos. Veuillez ajouter un utilisateur délégué, une liste de contrôle pour les services et le serveur autorisé pour la délégation.) UR:4 message d'erreur s'affiche lorsque vous ajoutez un utilisateur délégué à l'appliance Citrix SD-WAN WANOP.

  Résolution : vérifiez que l'utilisateur délégué est correctement configuré sur le Controller de domaine et que vous avez ajouté les services appropriés au Controller de domaine.

- **Problème** : l'appliance n'est pas en mesure de rejoindre le domaine.

  Résolution : exécutez l'outil de prévérification du domaine, disponible sur la page Domaine Windows, et résolvez les problèmes, le cas échéant. Si l'outil de prévérification de domaine ne signale aucun problème, contactez le support technique Citrix pour obtenir de l'aide supplémentaire pour résoudre le problème.

Plug-in Citrix SD-WAN WANOP

April 9, 2021

- **Problème** : Je suis confronté à des problèmes de connectivité des canaux de signalisation. Comment puis-je résoudre ces problèmes ?

  Résolution : pour résoudre les problèmes de connectivité des canaux de signalisation, effectuez les étapes de dépannage suivantes :

  - Vérifiez que vous avez correctement configuré l'adresse IP de signalisation. Vous pouvez le faire en envoyant un ping à l'adresse IP de signalisation et en vérifiant la réponse.
  - Vérifiez que l'état de la signalisation est activé sur l'appliance WANOP.
  - Vérifiez que le pare-feu installé sur le réseau ne supprime pas les options TCP WANOP.
  - Vérifiez qu'une licence de plug-in WANOP valide est installée sur l'appliance WANOP.
  - Vérifiez que la configuration de filtrage des sources du canal de signalisation ne bloque pas l'adresse IP de la source du client.
  - Si vous avez activé la détection de réseau local, vérifiez que le temps d'aller-retour entre le plug-in WANOP et l'appliance WANOP est une valeur acceptable.

- **Problème** : sur une appliance WANOP 4000, je ne suis pas en mesure de désactiver le plug-in WANOP.

  Cause : Il s'agit d'un problème connu.

  Résolution : Néant. Vous ne pouvez pas désactiver le plug-in WANOP sur une appliance WANOP 4000.

- **Problème** : lors de la connexion à l'appliance WANOP à l'aide du plug-in WANOP, l'entrée de message d'erreur suivante est enregistrée sous l'onglet Alertes :

  Plus de plug-ins WANOP que la limite actuelle de <Number> ont tenté de se connecter à cette appliance.

  Cause : le nombre de connexions à l'appliance WANOP a dépassé la limite d'utilisateurs sous licence.

  Résolution : attendez qu'un utilisateur se déconnecte ou terminez une connexion.

- **Problème** : Une adresse IP de signalisation incorrecte est configurée sur une appliance WANOP 4000 ou 5000.

  Résolution : Pour mettre à jour l'adresse IP de signalisation sur une appliance WANOP 4000 ou 5000, procédez comme suit :

1. Ouvrez une session sur l'instance Citrix de l'appliance WANOP.
2. Accédez à la page **Gestion du trafic** > **Équilibrage de charge** > **Serveurs virtuels** > BR_LB_VIP_SIG.
3. Mettez à jour l'adresse IP de signalisation.
4. Enregistrez la configuration.

- **Problème** : le trafic CIFS et ICA ne s'accélère pas.

  Résolution : Pour résoudre ce problème, effectuez les étapes de dépannage suivantes :

  – Vérifiez que les règles d'accélération pour les adresses IP et les numéros de port sont correctement définies pour le plug-in WANOP.

  – Vérifiez que les connexions CIFS ou ICA sont établies une fois la connexion de signalisation réussie.

  – Vérifiez la stratégie d'accélération de la classe de service utilisée.

RPC sur HTTPS

April 9, 2021

- **Problème** : après la mise à niveau du logiciel de l'appliance vers la version 7.3, les rapports de surveillance n'ont pas de catégorie spéciale pour les connexions RPC sur HTTPS.

  Cause : lorsque vous mettez à niveau l'appliance vers la version 7.3, les applications RPC sur HTTPS n'appartiennent pas à leur propre classe de service. Par conséquent, toutes les connexions RPC sur HTTPS sont répertoriées en tant que connexions TCP Other dans les rapports.

  Résolution : pour classer ces connexions en tant que connexions RPC sur HTTPS, créez une classe de service pour ces applications.

- **Problème** : Après avoir créé une classe de service pour RPC sur HTTPS, tout le trafic HTTP et HTTPS est classé comme RPC sur HTTP.

  Cause : Vous n'avez pas ajouté l'adresse IP de destination à la classe de service que vous avez créée pour les applications RPC sur HTTPS.

  Résolution : modifiez la classe de service que vous avez créée pour les applications RPC sur HTTPS, en ajoutant les adresses IP de destination de vos serveurs.

Mise en cache de vidéo

April 9, 2021

- **Problème** : après avoir ajouté une entrée à la liste des tâches de préremplissage, l'entrée est toujours dans l'état Configuré.

  Cause : une tâche de préremplissage prend environ une minute pour passer à l'état Téléchargement.

  Résolution : Vérifiez l'état de l'entrée après une minute ou actualisez la page pour vérifier que le statut passe à Téléchargement.

- **Problème** : après avoir ajouté une entrée à la liste des tâches de préremplissage, l'état de l'entrée affiche ERREUR 403. Cependant, le site Web fonctionne bien dans un navigateur Web.

  Cause : L'adresse IP de l'apA Citrix SD-WAN WANOP n'a pas accès au serveur vidéo.

  Résolution : Pour résoudre ce problème, vérifiez et mettez à jour les éléments suivants :

  - Règles d'accès à travers les pare-feu
  - Limitations basées sur l'adresse IP source dans le fichier httpd.conf du serveur vidéo

  Cause : Le serveur vidéo ne prend pas en charge la méthode HEAD.

  Résolution : le serveur vidéo doit autoriser l'adresse IP Citrix SD-WAN WANOP pour cette méthode.

  Cause : la liste des répertoires pour les dossiers n'est pas activée sur le serveur vidéo.

  Résolution : le serveur vidéo doit activer la liste des répertoires pour les dossiers.

- **Problème** : après avoir créé des entrées pour les tâches de préremplissage, vous ne pouvez pas modifier ou supprimer des entrées.

  Cause : Vous avez peut-être cliqué sur **Démarrer maintenant**pour l'entrée.

  Résolution : Ceci est par conception. Vous ne pouvez pas modifier ou supprimer une entrée après avoir cliqué sur **Démarrer maintenant** pour l'entrée et que l'entrée est en file d'attente, en démarrage ou en téléchargement. Vous ne pouvez supprimer l'entrée qu'une fois le téléchargement terminé.

- **Problème** : Après avoir créé des entrées pour les tâches de préremplissage, la vidéo n'est pas téléchargée et mise en cache. L'état de l'entrée affiche Échec du téléchargement.

  Cause : l'entrée de préremplissage n'a pas d'URL absolue pour la vidéo.

  Résolution : Pour résoudre ce problème, procédez comme suit :

1. Vérifiez que l'entrée de préremplissage contient l'URL réelle de la vidéo, telle que`http:` `//10.102.29.16/Citrix SD-WAN WANOP\\_demo.mp4`, et non un fichier HTML. L'appliance Citrix SD-WAN WANOP ne peut pas rechercher le contenu du fichier HTML pour trouver le lien vidéo.
2. Vérifiez que le protocole HTTP est utilisé pour servir la vidéo. Vous pouvez vérifier cela en utilisant l'option Afficher la source du navigateur Web.
3. Vous pouvez obtenir l'URL absolue de la vidéo en utilisant l'option Outils de développement du navigateur Web.

Accélération Citrix Virtual Apps and Desktops

April 9, 2021

- **Problème** : après la mise à niveau d'une appliance vers la version 7.3.1, les connexions ICA ne sont pas classées en tant que connexions Citrix Receiver pour HTML5 dans les pages de surveillance ICA.

  Cause : La classe de service définie sur l'appliance est **HTTP (Privé)**au lieu de Web (Privé). Lorsque vous mettez à niveau une appliance vers la version 7.3.1, l'application **ALTHTTP** n'est pas ajoutée à cette classe de service. Par conséquent, même si les connexions ICA via Citrix Receiver pour HTML5 sont optimisées, elles ne sont pas classées en tant que connexions Citrix Receiver pour HTML5 dans les pages de surveillance ICA.

  Résolution : Pour classer les connexions ICA sur Citrix Receiver pour HTML5, procédez comme suit :

  1. Accédez à la page **Configuration** > **Règles d'optimisation** > **Classes de service**.
  2. Modifiez la classe de service **HTTP (Private)**.
  3. Cliquez sur **Ajouter une règle**.
  4. Dans Règles de filtrage, sous Applications, cliquez sur **Toutes**.
  5. Dans la liste Applications, sélectionnez **ALTHTTP**.
  6. Cliquez sur **Ajouter**.
  7. Cliquez sur **Enregistrer**.
  8. Apportez d'autres modifications à la règle de filtre, selon les besoins.
  9. Cliquez sur **Enregistrer**.