NetScaler Intelligent Traffic Management

Machine translated content

Disclaimer

Contents

Nouveautés

April 29, 2022

Nouvelle fonctionnalité/Amélioration	Version
Alertes - Cette fonction surveille les problèmes de performances ou les anomalies de vos plateformes configurées à partir d'un réseau d'utilisateurs finaux dans le monde entier.	2022.02.15
Persistance locale - Cette fonctionnalité offre la capacité d'adhérence des décisions lorsqu'elle est activée. Les demandes sont identifiées à l'aide du masque de sous-réseau IP, dont la longueur est configurable. Par exemple, lorsqu'un client répète une demande à la même application dans un certain délai (Persistence TTL), la décision initiale est renvoyée.	2021.12.09
Connecteur AWS ELB : ce nouveau connecteur extrait `HealthyHostCount` `UnHealthyHostCount` les `Load Balancer Capacity Units` (`LCUs`) métriques d'AWS ELB via Fusion. Il offre aux clients une expérience intégrée d'équilibrage de charge et une visibilité sur les métriques Fusion disponibles dans leurs applications Openmix.	2019.08.16
Changer le type de plateforme (privée en communauté) : cette nouvelle fonctionnalité permet aux clients de modifier les paramètres actuels de leur plateforme privée ou GSLB pour référencer la plateforme communautaire à la place. Cette fonctionnalité est utile pour les clients dont les plateformes privées sont hébergées dans un centre de données public ou une région cloud.	2019.07.03

Nouvelle fonctionnalité/Amélioration	Version
Nouveau tableau de bord - Le nouveau tableau de bord ITM est désormais opérationnel, riche en informations, personnalisable et globalement plus utile que la version précédente. Dans le nouveau tableau de bord, vous pouvez afficher les graphiques des sessions radar, des performances radar, des décisions de gestion du trafic Openmix et des graphiques d'état de surveillance du sonar. Vous pouvez créer plusieurs tableaux de bord, chacun adapté à une vue qui vous intéresse. Vous pouvez également choisir de faire du Visualizer ITM ou du Tableau de bord votre page de destination par défaut.	2019.06.27
Quarantaine Fusion : cette fonctionnalité met en quarantainela source de données Fusion défaillante d'un client, si celle-ci échoue ou s'exécute à un intervalle d'interrogation inférieur à 24 heures. Fusion applique la logique de quarantaine pour empêcher l'exécution de ces flux défaillants afin d'économiser des ressources (CPU/mémoire) et d'éviter tout impact sur d'autres sources de données Fusion valides ou valides.	2019.06.19
Activer/Désactiver les plateformes pour Openmix - Une plate-forme peut désormais être activée ou désactivée pour Openmix en activant ou en désactivant le bouton **Openmix Enabled** dans les paramètres de la plateforme. Si une plateforme particulière est désactivée pour Openmix, elle n'est pas prise en compte dans les décisions Openmix.	2019.04.09

Nouvelle fonctionnalité/Amélioration	Version
Géolocalisation de la plateforme : cette fonctionnalité permet aux clients d'afficher et de gérer la géolocalisation attribuée à une plateforme. Par défaut, aucun emplacement **géographique** n'est attribué aux plates-formes privées. Lorsqu'un utilisateur crée une plate-forme privée et configure une sonde Radar, nous utilisons l'URL de la sonde pour localiser la plate-forme. Alternativement, l'utilisateur peut assigner un Géo manuellement sans compter sur le chemin d'URL Radar. Pour les importations de configuration GSLB et F5, nous géo localisons l'IP publique et l'utilisons comme **géo** de la plate-forme. Les plates-formes communautaires héritent par défaut de l'emplacement d'origine de la plate-forme.	2019.04.09
Visualiseur : analyse descendante au niveau de l'état : alertes actives contenant des informations sur les performances et la disponibilité des Clouds, des centres de données, des CDN et d'autres services. Ces alertes sont mesurées et visualisées au niveau de l'État aux États-Unis.	2019.04.01
Visualiseur : Importations F5 et GSLB - Importations F5 et GSLB : Vous pouvez désormais importer une plateforme via une configuration GSLB ou F5. Les informations de base du site (IP et nom) sont importées sous forme de plateformes ITM. ITM géolocalise le site et permet à la plateforme d'être affichée sur le visualiseur pour l'analyse des performances.	2019.03.29
Adaptateur depurge G-Core - L'adaptateur de purge CDN G-Core est maintenant ajouté à la liste des adaptateurs pris en charge par ITM pour exécuter des purges.	2019.03.29

Nouvelle fonctionnalité/Amélioration	Version
Radar DSA 3 pour tous les fournisseurs de la communauté —Afin d'améliorer continuellement la communauté Radar et la précision de nos benchmarks, nous avons récemment publié un nouveau Dynamic Content Benchmark. Ce nouveau benchmark a une page HTML dynamique et une signature avec laquelle la mesure peut être vérifiée.	2019.03.21
Visualiseur —Le visualiseur ITM est un outil intuitif et intelligent qui vous permet de surveiller et d'analyser les performances globales des FAI et des services. L'interface utilisateur ITM Visualizer fournit des alertes actives contenant des informations sur les performances et la disponibilité des Clouds, des centres de données, des CDN et d'autres services. La communauté ITM mesure ces alertes dans le monde entier. ITM Radar collecte des milliards de mesures auprès d'utilisateurs réels du monde entier via la communauté Radar. Il utilise un modèle de crowdsourcing pour mesurer ces alertes.	2019.03.08
Des visites guidées (visites guidées) pour Visualizer et Openmix sont maintenant disponibles sur le **portail de démonstration ITM**. Le portail de démonstration est accessible via l'icône d'aide du portail ITM. Dans le coin inférieur droit du **portail de démonstration**, vous voyez une icône qui lance les visites guidées.	2019.03.08

Avis de tiers

September 13, 2023

Notifications tierces relatives à la gestion intelligente du trafic NetScaler (PDF)

Glossaire

September 13, 2023

Terme	Description
Application	Une application Openmix est une spécification de logique d'équilibrage de charge qui peut être configurée dans le portail. La demande sera traitée pour chaque demande faite à Openmix et une décision de routage sera prise en fonction de la logique spécifiée. Les applications peuvent être utilisées pour un ou plusieurs types de contenu. Un client peut avoir une application pour un type de contenu à forte valeur commerciale et une autre application pour un contenu de moindre valeur qui doit être acheminé différemment. Par exemple, le client peut disposer d'une seule application pour afficher le contenu à tous les utilisateurs, qui met l'accent sur le routage vers le fournisseur le plus rapide, quel que soit le coût. Le client peut également disposer d'une autre application pour le contenu rarement diffusé qui met l' accent sur l'optimisation des coûts entre les fournisseurs pour le contenu de moindre valeur. Dans le scénario ci-dessus, le client disposerait de deux applications Openmix.

Terme	Description
Mesures communautaires	Les mesures communautaires sont obtenues par le biais d'un modèle de crowdsourcing fournissant au client une vue de la performance et de la disponibilité d'un fournisseur à un niveau géographique et logique à l'échelle mondiale. Les mesures communautaires sont disponibles gratuitement pour les membres de la communauté participants (l'installation de la balise JavaScript est requise). L'accès aux données communautaires pour les organisations non contributrices (c'est-à-dire n' intégrant pas JS) est un élément facturé.
Décision	Une décision Openmix est spécifiée sous la forme d'une demande unique adressée à l'un des équilibreurs de charge de NetScaler. Pour le DNS, il s'agit d'une requête DNS unique adressée aux équilibreurs de charge DNS. Pour le protocole HTTP, il s'agit d'une requête GET ou HEAD envoyée au point de terminaison HTTP Openmix.
Mesure	Une mesure concerne le radar et la collecte de données auprès des utilisateurs finaux sur les performances d'une application de service. Pour les mesures communautaires, voir Mesures communautaires.
Plateforme	Une plate-forme est un CDN, un cloud, un centre de données ou un autre point de terminaison que le client souhaite surveiller dans Radar ou utiliser dans l'application Openmix.

Terme	Description
Mesure privée	Les mesures privées par radar permettent de transmettre des données de mesure ou de télémétrie (dans le cas du streaming) à propos de l'expérience des utilisateurs finaux qui ne sont pas partagées avec la communauté. Cela peut s'appliquer lorsqu'un client cherche à mesurer : + Sa propre architecture de centre de données + Utilisation de son propre objet ou page de test + Utilisation de son propre contrat avec un fournisseur + Qualité d'expérience audio/vidéo pour l'utilisateur final

Définitions des données radar

June 4, 2021

Les partenaires de référence et les membres de la communauté Radar qui ont déployé l'étiquette Radar peuvent éventuellement avoir accès à leurs mesures Radar. Dans le cas des partenaires de référence, nous partageons les mesures prises sur ce partenaire, quelle que soit la page sur laquelle l'étiquette Radar a été déployée ou le moment où la mesure a été prise. Les membres de la communauté peuvent voir toutes les mesures prises par leurs internautes, quel que soit le partenaire de référence mesuré.

Partage de données radar client

Les systèmes de déploiement de balises Radar peuvent éventuellement accéder à un sous-ensemble des champs que nous recevons du client Radar lorsqu'une mesure Radar est effectuée sur leur site Web. Les adresses IP de l'utilisateur sont anonymisées avant que les rapports ne soient générés. Pour les descriptions des journaux, reportez-vous à la documentation de Netscope (NEM).

Mesures radars brutes

Les mesures radar brutes contiennent un sous-ensemble des champs que nous recevons du client Radar lorsqu'une mesure radar est effectuée. Les adresses IP de l'utilisateur sont anonymisées avant que les rapports ne soient générés.

Les rapports peuvent être mis à disposition quotidiennement ou en temps réel qui fournissent des données de mesure en moins de 5 minutes.

Les fichiers peuvent être délimités par des TAB, CSV ou JSON. Pour les descriptions de journaux et les rapports, reportez-vous à la documentation Netscope.

Numéros de système autonome

https://s3-eu-west-1.amazonaws.com/community-radar/ref/asns.json.gz

Identifiants de fournisseur (public) de la communauté

https://s3-eu-west-1.amazonaws.com/community-radar/ref/providers.json.gz

Types de sonde (Types de mesure)

https://s3-eu-west-1.amazonaws.com/community-radar/ref/probetypes.json.gz

---

Codes de réponse

Code	Module	Description	Valeur
0	Tous	Succès	Valeur de mesure
1	Sondage à distance	Délai d'expiration de la requête HTTP	0
2	Sondage à distance	Échec de la connexion RTMP	0
3	Sondage à distance	Flux RTMP introuvable	0
4	Sondage à distance	Fichier HTTP non valide	0
5	Chronométrage de navigation	API de synchronisation de navigation non prise en charge	0

Codes du marché

Code	Nom	Abréviation ISO
0	Inconnu	XX
1	Amérique du Nord	SO
2	Océanie	O.C
3	Europe	UE
4	Asie	COMME
5	Afrique	AF
6	Amérique du Sud	SA

Codes de pays

Basé surISO 3166 -1 Alpha 2

https://s3-eu-west-1.amazonaws.com/community-radar/ref/countries.json.gz

Codes de région

Il n'existe pas de normes ISO pour les régions que nous connaissons. De plus, notre fournisseur GEO fournit des régions pour un petit sous-ensemble de pays. Selon leurs documents, l'objectif des « régions » est de subdiviser certains pays en zones plus grandes que les États. Par exemple « US - Southwest »

Pour commencer, nous fournissons nos propres « ID de région » numériques et une cartographie :https://s3-eu-west-1.amazonaws.com/community-radar/ref/regions.json.gz

> **NOTE :** Nous nous réservons le droit de modifier le format de ce fichier. Tout code créé pour charger dans ces mappages doit être créé dans cet esprit. À long terme, il y aura un appel d'API pour télécharger ces mappages.

Codes d'État

Il existe une norme ISO pour les états 3166-2. Nous évaluons si cette norme répond à nos besoins. Alors commencez, nous utilisons nos propres mappages numériques à chaînes. Semblable à la région, le format peut changerhttps://s3-eu-west-1.amazonaws.com/community-radar/ref/states.json.gz

Codes de Ville

Nous utilisons nos propres mappages numériques à chaînes. Similaire à la région, le format peut changer et nous pouvons éventuellement fournir ces mappages en tant qu'appel d'API. https://s3-eu-west-1.amazonaws.com/community-radar/ref/cities.json.gz

Visualiseur

September 13, 2023

Introduction

Le visualiseur ITM est un outil intuitif et intelligent qui vous permet de surveiller et d'analyser les performances globales des FAI et des services. L'interface utilisateur ITM Visualizer fournit des alertes actives contenant des informations sur les performances et la disponibilité des Clouds, des centres de données, des CDN et d'autres services. La communauté ITM mesure ces alertes dans le monde entier. ITM Radar collecte des milliards de mesures auprès d'utilisateurs réels du monde entier via la communauté Radar. Il utilise un modèle de crowdsourcing pour mesurer ces alertes.

Pour un nouvel utilisateur, la page du visualiseur s'ouvre avec toutes les alertes de communauté disponibles sur la carte. ITM Radar mesure les anomalies de performance et génère des alertes sur presque tous les réseaux et partout dans le monde.

Les quatre tuiles situées au-dessus de la carte du visualiseur présentent les données suivantes.

Alertes radar actives

Les alertes radar actives sont à jour et en cours.

Alertes radar

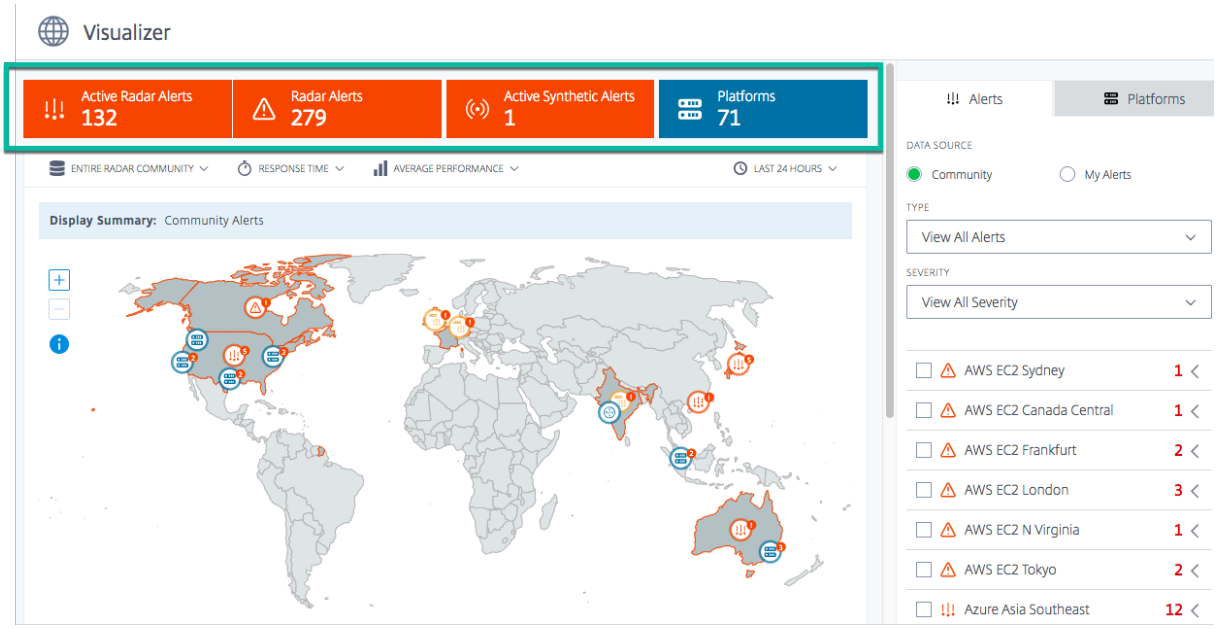
Les alertes radar actives sont à jour et en cours. Par défaut, cette vignette affiche toutes les alertes des dernières 24 heures, mais elle change en fonction de la période sélectionnée par l'utilisateur.

Alertes synthétiques actives

Ces alertes sont déclenchées en temps réel. Sonar, notre système de surveillance synthétique qui mesure la disponibilité globale d'un service ou d'un centre de données, génère ces alertes.

Plates-formes

Le nombre de plateformes configurées dans le compte client.



Options d'affichage

Vous pouvez afficher les alertes et les plateformes sur la carte selon les critères suivants :

Toute la communauté Radar ou uniquement vos visiteurs

Choisissez **Radar Community** pour voir les performances des plateformes de la communauté Radar. Ou bien, pour afficher les performances de vos visiteurs uniquement via vos plateformes privées, choisissez **Only Your Visitors**.

Temps de réponse ou disponibilité

Cliquez sur n'importe quelle plateforme sur la carte ou dans la liste pour afficher ses performances en fonction de **la disponibilité** ou du **temps de réponse**.

Meilleure performance ou performance moyenne

Sélectionnez **Performances moyennes** ou Meilleures performances pour afficher les performances moyennes/meilleures que vous pourriez obtenir pour vos plateformes.

Les**performances moyennes** sont similaires à celles d'un round robin entre vos plateformes, et les **meilleures performances** sont les performances que nous obtenons en utilisant l'ITM.

Lorsque vous choisissez **Best Performance**, vous voyez les performances sur la carte en fonction de la plateforme la plus performante. Par exemple, si vous examinez les performances d'un pays spécifique et que vous avez sélectionné deux plateformes, **Best Performance** colore la carte du pays en fonction de la plate-forme présentant les meilleures performances entre les deux (disponibilité la plus élevée ou temps de réponse le plus faible) pour ce pays.

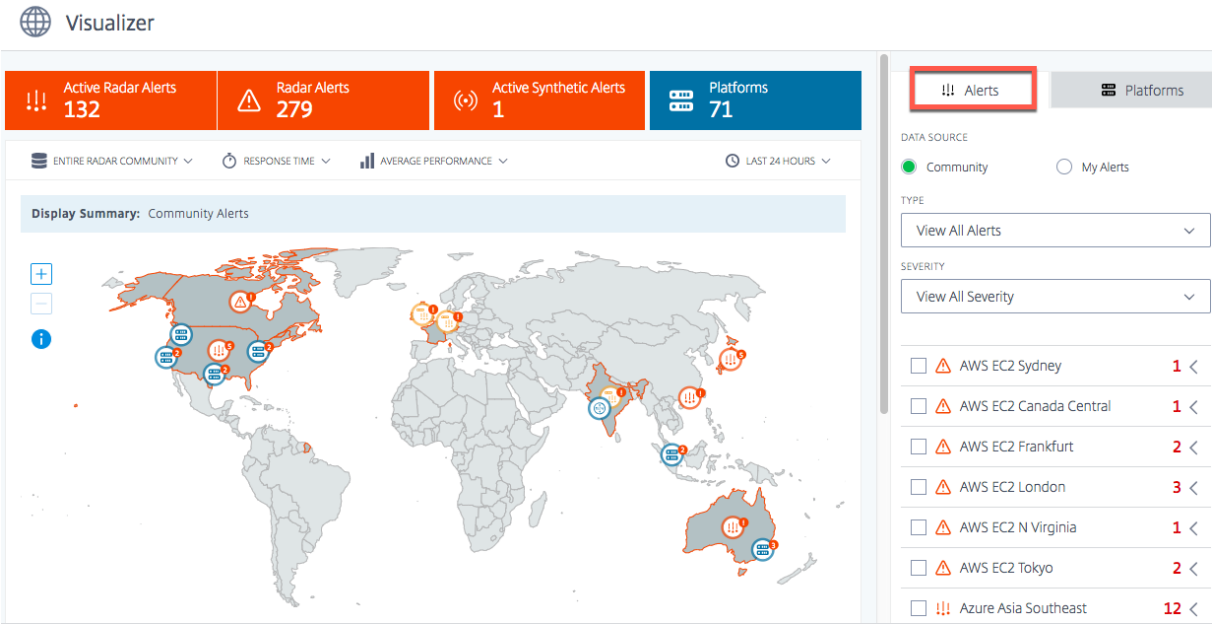
Sinon, si vous choisissez **Performances moyennes**, vous voyez les performances sur la carte en fonction de la moyenne de toutes les plates-formes sélectionnées. Il colore la carte du pays avec la disponibilité moyenne (ou le temps de réponse) des deux plateformes.

Période

Les alertes sur la carte peuvent être générées avec une période comprise entre les **60 dernières minutes, les 24 dernières heures, les 48 dernières heures, les 7 derniers jours, les 30 derniers jours ou une plage personnalisée**. La vue par défaut est la dernière 24 heures. Chaque fois que vous modifiez la période, les données de la carte sont actualisées et vous indiquent les alertes déclenchées pour cette période.

Alertes

L'onglet **Alertes** est l'onglet par défaut affiché lorsque vous arrivez sur la page du visualiseur. La source de données par défaut affichée pour un nouvel utilisateur n'ayant aucune alerte est **Community.** Cela signifie que toutes les alertes que vous visualisez sur la carte en tant que nouvel utilisateur sont des alertes communautaires. Même si vous avez configuré des alertes, mais que vous n'avez pas d'alertes actives ou en cours, votre vue est par défaut des alertes de communauté. Toutefois, si vous avez configuré vos alertes et que vous avez des alertes continues actives, votre vue par défaut est celle de vos propres alertes. Pour plus d'informations sur les alertes, voir Alertes.



Communauté

Les alertes de la communauté sont des problèmes de performance ou des anomalies comme le montre ITM Radar qui se produisent dans toute la communauté ITM. Ces alertes sont mesurées via les réseaux d'utilisateurs finaux du monde entier. Lorsque vous ouvrez le **Visualizer** pour la première fois en tant que nouvel utilisateur, toutes les alertes de communauté s'affichent sur la carte. Une fois que vous avez configuré vos propres alertes, celles-ci s'affichent à la place des alertes communautaires.

Toutefois, si vous avez configuré des plateformes privées et que des alertes sont configurées, vous pouvez voir vos propres alertes sous la forme **Mes alertes**, la vue par défaut.

Mes alertes

Ces alertes sont des problèmes de performance ou des anomalies de vos plateformes privées. Il utilise les réseaux d'utilisateurs finaux du monde entier pour mesurer ces alertes.

En tant que nouvel utilisateur, si vous ne voyez aucune alerte, cela signifie que vous n'avez aucune alerte configurée. Vous pouvez accéder à la page **Alertes** à partir de la barre latérale gauche pour configurer des alertes pour les performances de vos plates-formes. Mais vous devez d'abord configurer vos plateformes privées. Pour configurer des plates-formes, vous pouvez soit accéder à la page **Plateformes** à partir de la barre latérale gauche, soit le faire à la volée via l'onglet **Plateformes** .

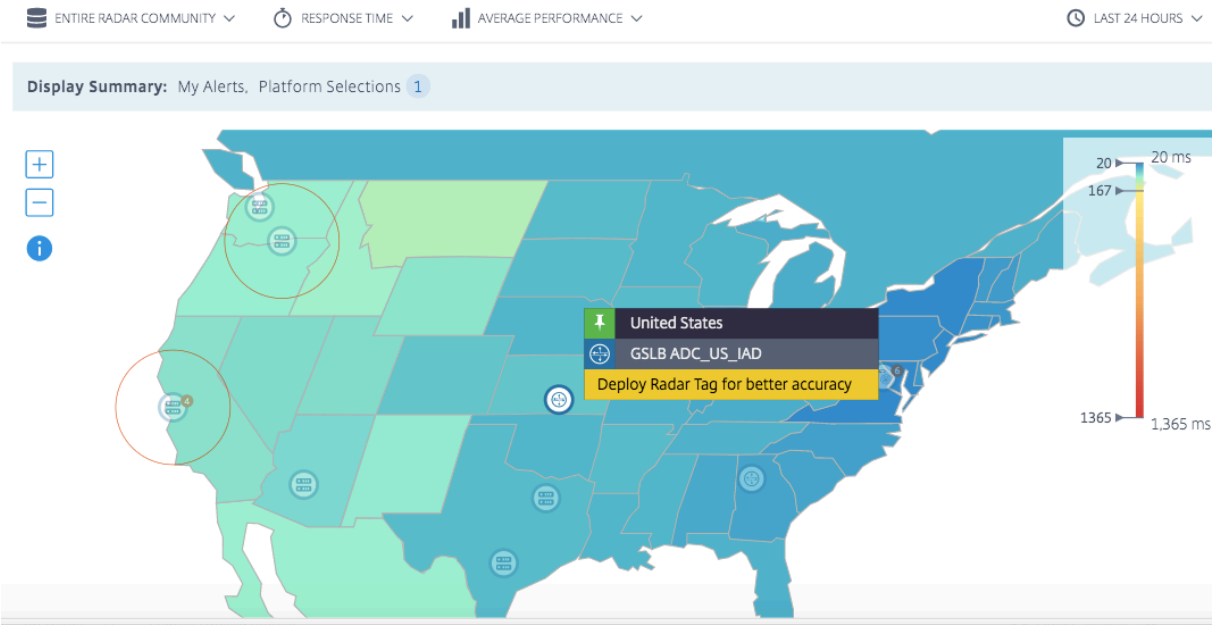
Détails de l'alerte

Vous pouvez survoler l'alerte sur la carte pour voir le pays et les services pour lesquels les alertes sont déclenchées. Pour plus de détails sur une alerte spécifique,

1. Cliquez sur l'icône d'alerte sur la carte pour cocher la case du service déclenche l'alerte et la met en surbrillance dans la liste.
2. Cliquez sur la flèche située à droite de la plateforme ou du service sélectionné pour afficher les détails de l'alerte, notamment :

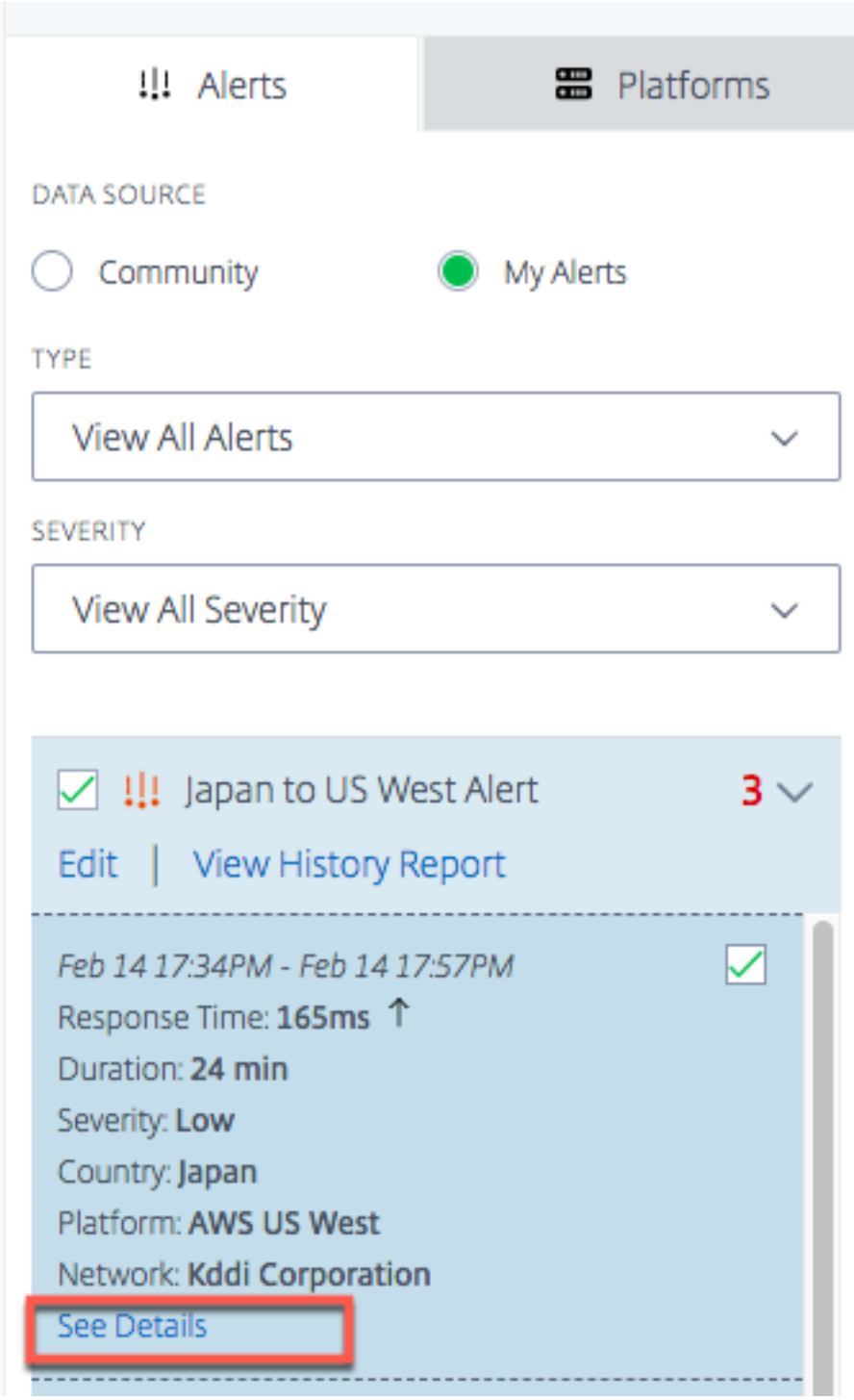
   a) **Disponibilité** ou **temps de réponse** de la source de données
   b) **Durée** de l'alerte
   c) **Gravité** de l'alerte
   d) **Pays** du réseau à partir duquel les problèmes sont mesurés
   e) Nom de la **plateforme** pour laquelle l'alerte est déclenchée.
   f) Nom du **réseau** à partir duquel les problèmes sont mesurés.

Alertes au niveau de l'état : alertes actives contenant des informations sur les performances et la disponibilité des Clouds, des centres de données, des CDN et d'autres services. Ces alertes sont mesurées et visualisées au niveau de l'État aux États-Unis.



Pour en savoir plus sur l'alerte, cliquez sur **Afficher les détails** pour accéder à la page **des alertes** .

> **REMARQUE :** Vous ne pouvez afficher le lien **Voir les détails** que pour vos propres alertes.

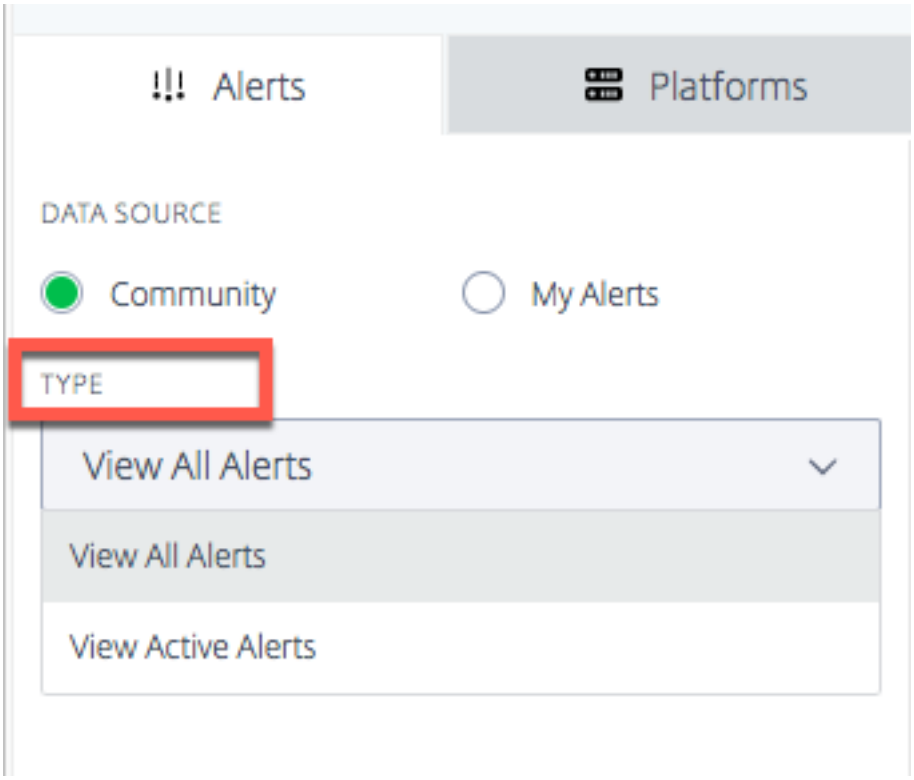


Type d'alerte

Le menu **Type** vous permet de visualiser les types d'alertes suivants.

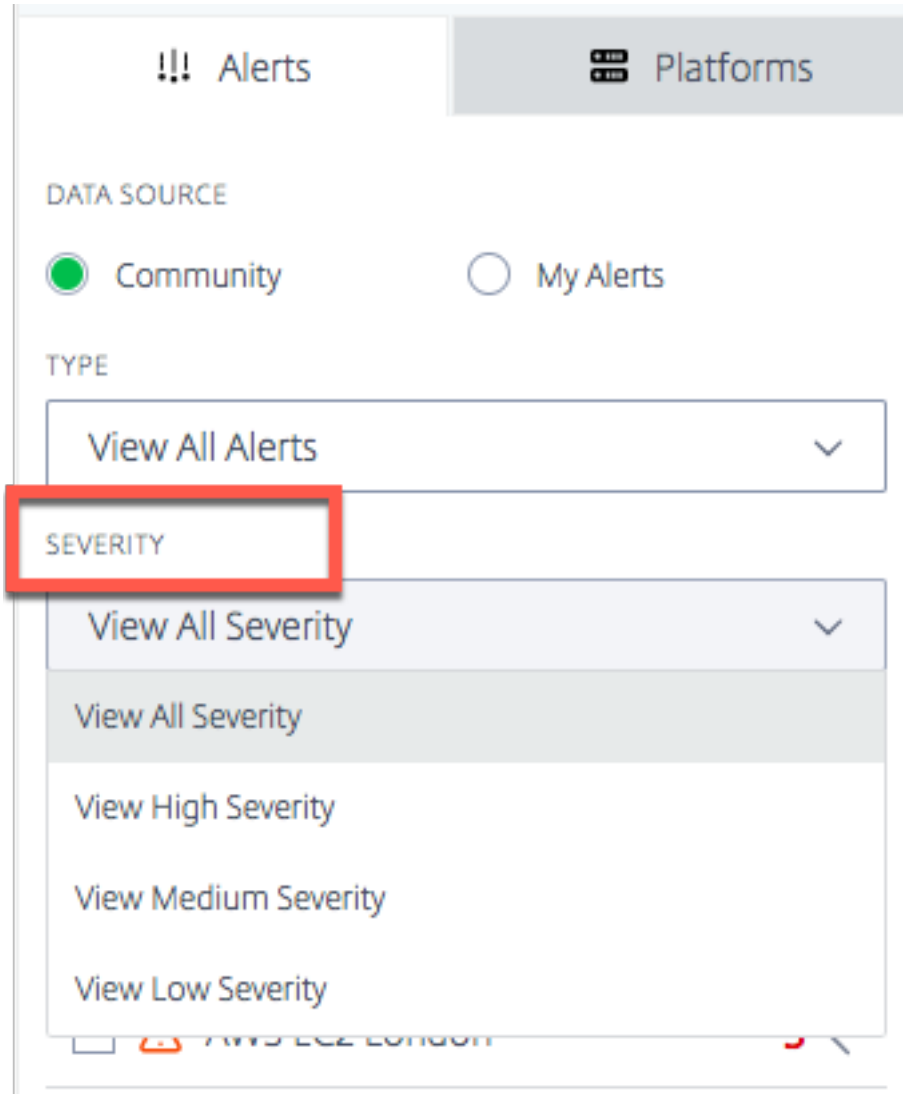
Toutes les alertes Toutes les alertes incluent des alertes actives et historiques. Les alertes historiques sont des alertes qui ont été émises plus tard dans la période sélectionnée.

Alertes actives Les alertes actives incluent les alertes en cours. Ils sont valides et à jour pour la période spécifiée par l'utilisateur.



Gravité des alertes

Les alertes peuvent être filtrées en fonction de leur gravité **élevée, moyenne**et **faible** . **All Gravity** est l'affichage par défaut.



Logique de gravité Pour connaître la disponibilité :

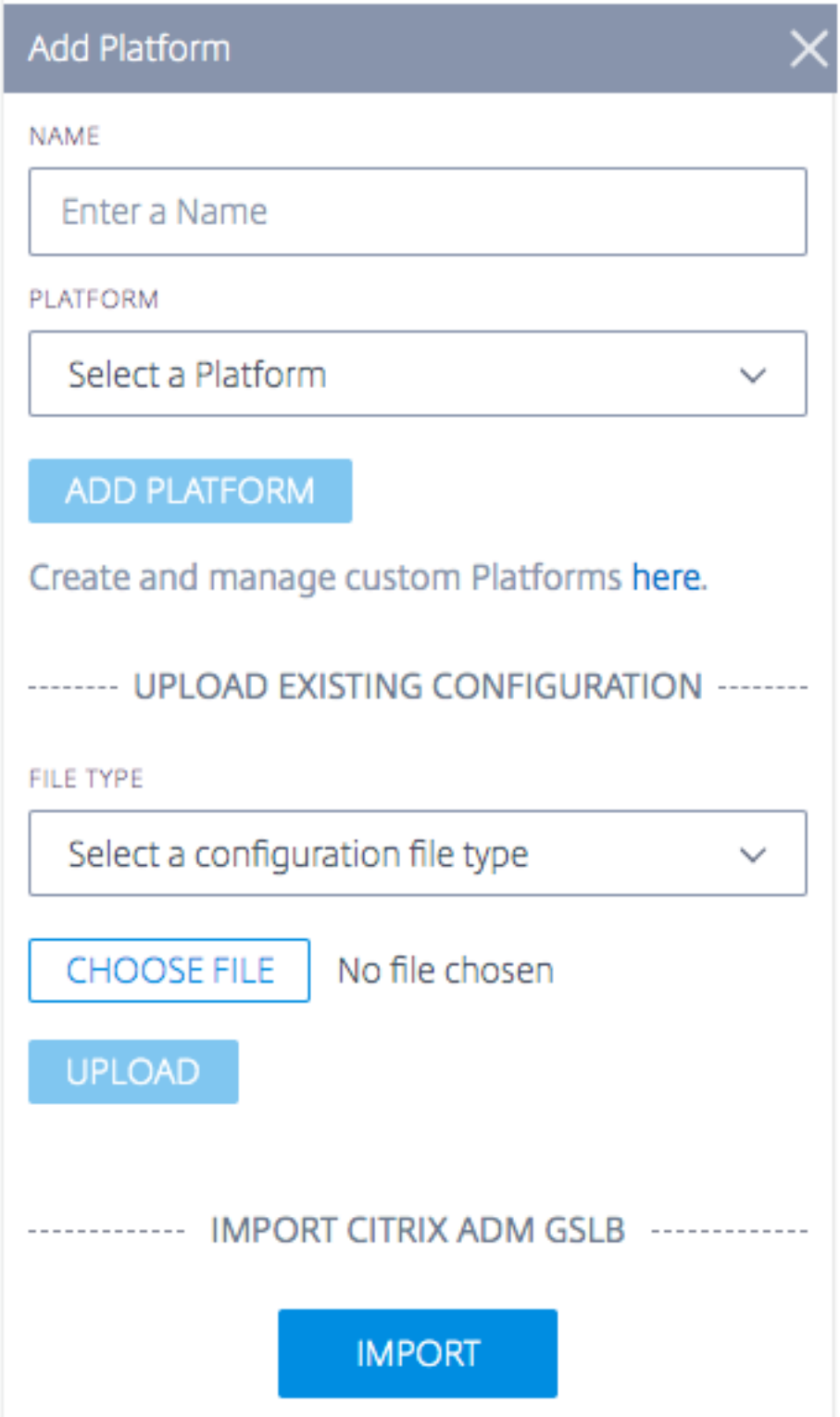
- Si plus de 50 % en dessous du seuil -> La gravité est **élevée**
- Si plus de 25 % mais moins de 50 % en dessous du seuil -> La gravité est **moyenne**
- Si le seuil est inférieur à 25 % -> La gravité est **faible**

Pour le temps de réponse :

- **Si le seuil est dépassé de plus de 200 % -> La gravité est élevée**
- **Si le seuil est supérieur à 100 % mais inférieur à 200 % -> La gravité est moyenne**
- Si le seuil est dépassé de moins de 100 % -> La gravité est **faible**

Plates-formes

Lorsque vous sélectionnez l'onglet **Plateformes**, la liste des plateformes que vous avez ajoutées s' affiche. Toutefois, si vous êtes un nouvel utilisateur et que vous n'avez pas encore configuré de plateforme, vous pouvez soit ajouter une plateforme communautaire ici à la volée, soit configurer une plateforme privée en cliquant sur le lien **Créer et gérer des plateformes personnalisées ici** .



Ajouter une plateforme communautaire

1. Pour ajouter une plateforme communautaire, cliquez sur l'icône + à côté de la barre **Ajouter une plateforme** .
2. Donnez un nom à la plateforme et sélectionnez-la dans la liste des plateformes communautaires du menu **Plateforme** .
3. Cliquez sur **Ajouter une plateforme**.

Ajouter une plateforme personnalisée/privée

1. Pour ajouter une plate-forme privée, cliquez sur l'icône + en regard de la barre **Ajouter une plate-forme** .
2. Cliquez sur le lien **Créer et gérer des plateformes personnalisées ici** qui vous amène à la page **Plateformes**, où vous pouvez ajouter une nouvelle plateforme privée. Vous pouvez également accéder à la page **Plates-formes** à partir de la barre latérale gauche.

Télécharger la configuration existante : NetScaler et F5 BIG-IP DNS

Cette option vous permet de choisir un fichier de configuration DNS NetScaler ou F5 BIG-IP et d'importer directement la configuration (de vos plateformes existantes). Il crée automatiquement des plateformes privées pour votre configuration DNS NetScaler ou F5 BIG-IP.

Importer Citrix GSLB à partir du service ADM

Cette option vous permet d'importer directement tous vos GSLB configurés dans le service ADM.

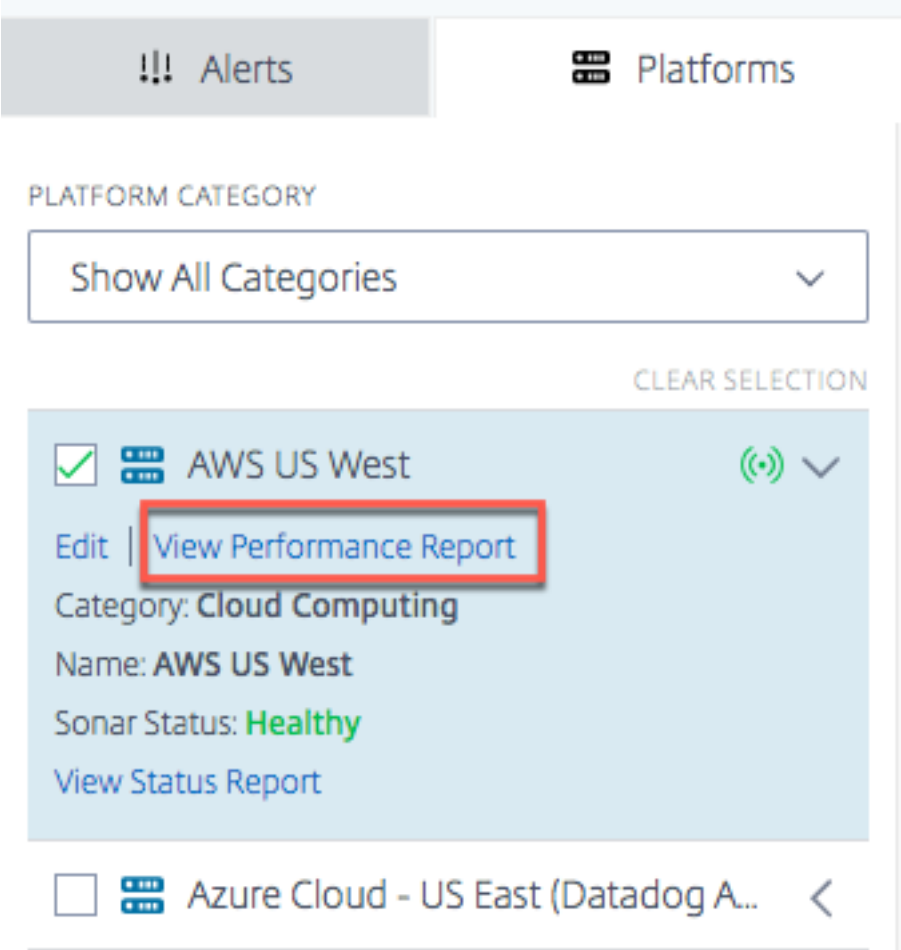
Si vous utilisez Citrix Cloud ADM Service, vous pouvez importer les GSLB configurées là. Les informations de base du site - IP et nom sont importées en tant que plateformes ITM. ITM géolocalise le site et permet à la plateforme d'être affichée sur le visualiseur pour l'analyse des performances.

Rapport sur le rendement

Le rapport de performance radar fournit des détails sur les plateformes spécifiques, les alertes déclenchées et chaque réseau à partir duquel elles ont été mesurées. Le rapport affiche les mesures de temps de réponse ou de disponibilité et la période pour le problème qui a été mesuré. Il inclut tous les filtres qui ont été appliqués dans le **visualiseur**.

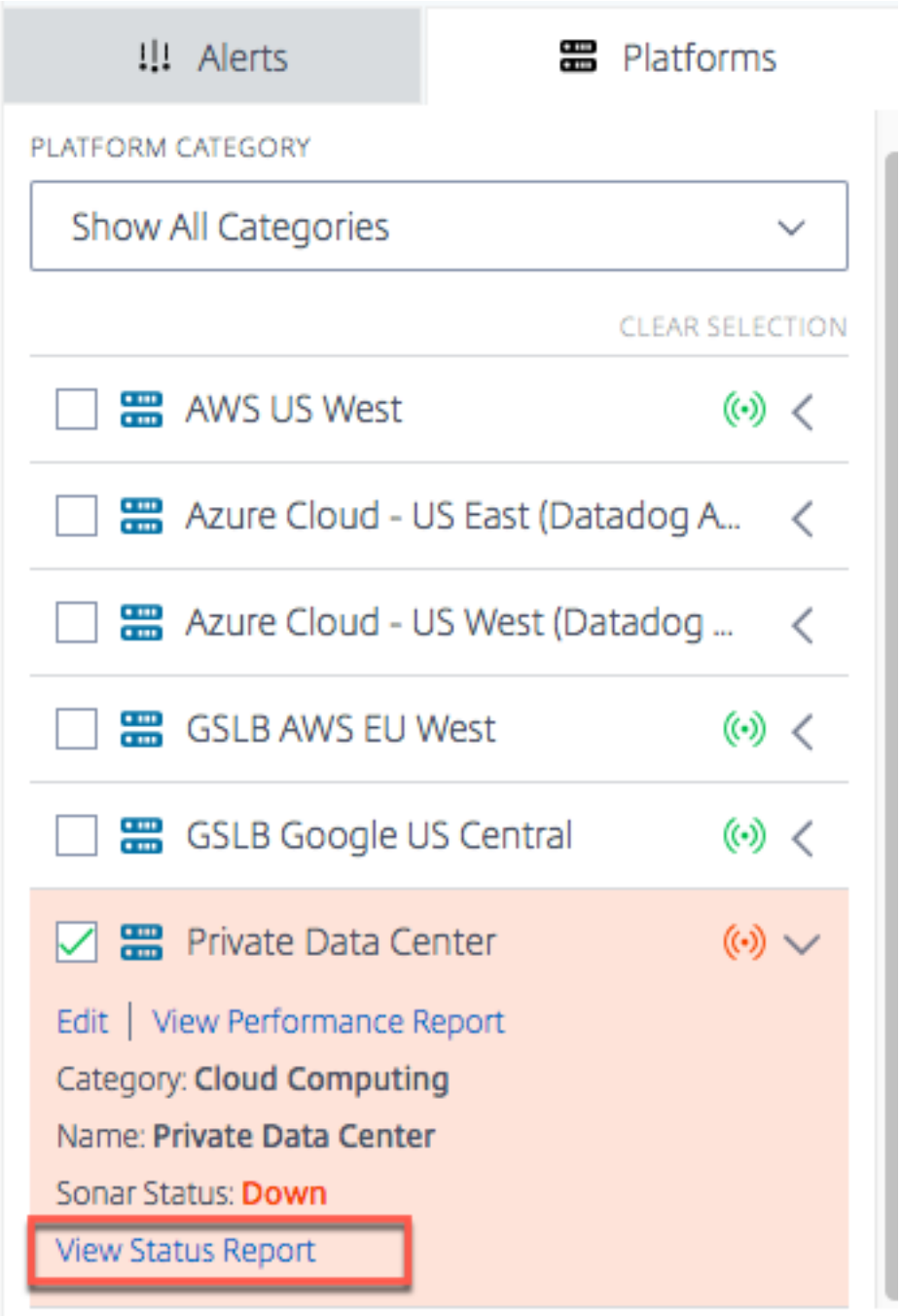
Pour afficher les détails des performances d'une plate-forme spécifique pour laquelle l'alerte a été déclenchée, procédez comme suit.

1. Cliquez sur l'icône de la plate-forme ou sur l'icône d'alerte sur la carte pour la mettre en surbrillance et cochez la case dans la liste de droite.
2. Cliquez sur la flèche en regard de la plate-forme ou de l'alerte pour la développer.
3. Cliquez sur le lien **Afficher le rapport de performances** pour accéder à la page **Rapport de performances** radar.

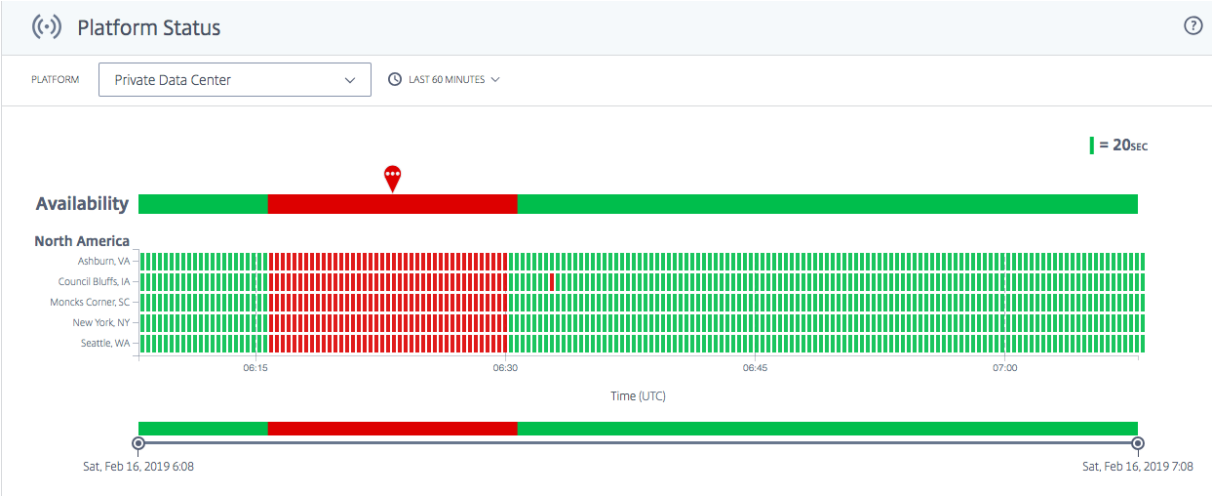


Rapport d'état

Pour les alertes de surveillance synthétiques, vous pouvez consulter les détails des alertes en développant la plateforme pour afficher les détails, puis en cliquant sur **Afficher le rapport d'état**.



Le lien **Afficher le rapport d'état** vous amène à la page d'**état de la plateforme** Sonar et vous donne des détails sur l'état de santé de votre plate-forme sur la base de contrôles de surveillance synthétiques en temps réel.



Radar

September 13, 2023

Vue d'ensemble

Le radar constitue l'épine dorsale de la méthodologie de collecte de données. Radar utilise un script JavaScript intégré à une page de contenu ou aux pages d'un fournisseur d'applications pour collecter des informations sur les performances et la disponibilité d'un centre de données ou d'une plateforme de diffusion.

Le client Radar est une application JavaScript qui s'exécute sur les pages Web des clients et dans les applications mobiles. Son objectif principal est de recueillir les données de performance du réseau utilisées pour prendre des décisions de routage intelligentes via Openmix, et de fournir des plug-ins optionnels pour activer d'autres services de gestion intelligente du trafic NetScaler, tels que le temps de chargement des pages, le chronométrage des ressources de page et les mesures de lecture vidéo.

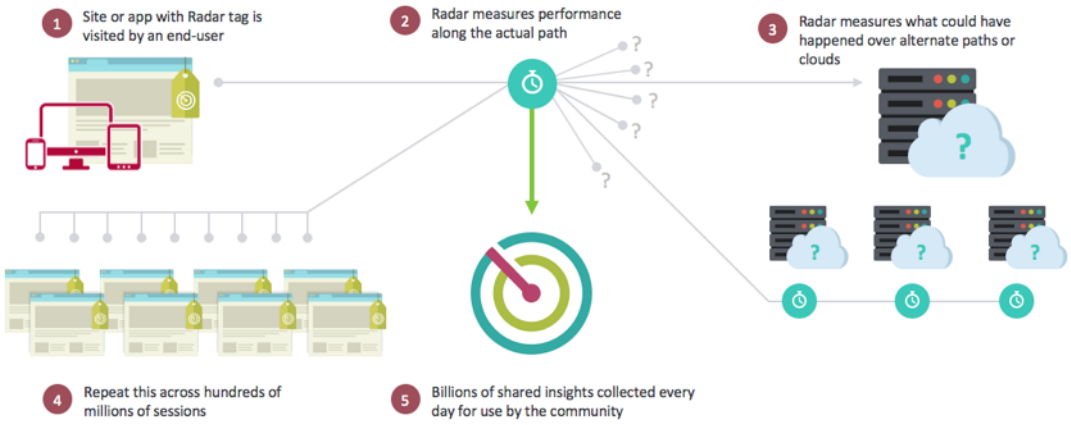
Le client Radar est complet, léger et discret. Le client attend que la plupart des ressources de la page soient téléchargées avant d'effectuer l'essentiel de son travail, et toutes les communications réseau sont effectuées de manière asynchrone dans la mesure du possible. Ces instructions indiquent la plateforme à mesurer ensuite au cours de la session, choisie parmi les plateformes communautaires et toutes les plateformes privées spécifiques à ce membre de la communauté. Ils indiquent également les types de mesures à effectuer, qui peuvent inclure la disponibilité, le temps d'aller-retour, le débit ou d'autres collectes métriques.

Pour le rendre aussi petit que possible, le JavaScript est compilé avec des optimisations avancées à l'aide du compilateur Google Closure. Les fonctionnalités optionnelles avancées sont fournies sous

forme de plug-ins aux clients qui choisissent de les utiliser.

Communauté Radar

Grâce à une approche communautaire unique, Radar apporte une transparence inégalée aux performances et à la disponibilité mondiales des plus grandes infrastructures publiques du monde, du cloud computing au stockage en passant par les réseaux de diffusion de contenu et d'applications. Grâce à Radar, les clients peuvent rapidement trouver les plateformes les plus performantes et les moins performantes pour chacun de leurs visiteurs.



Radar est la première coopérative de surveillance du cloud sur Internet. Devenir membre de la communauté signifie un accès illimité à notre base de données de rapports historiques, y compris une segmentation détaillée par fournisseur, pays et réseau.

Être membre de la communauté Radar fournit également un ensemble complet d'outils permettant de saisir les niveaux de service fournis par les infrastructures de diffusion de contenu internes et externes. La particularité de Radar est la capacité d'utiliser les visiteurs de votre site Web pour mesurer l'expérience qu'ils recevraient de plateformes non utilisées actuellement par une entreprise. La même méthodologie permet des évaluations objectives des plateformes cloud tout au long de leur cycle de vie, y compris une évaluation continue des performances par rapport aux SLA.

En ajoutant une simple balise JavaScript à votre page Web ou un SDK aux applications mobiles, les clients peuvent transformer chacun de leurs visiteurs en un « agent de test » virtuel. Le radar déclenche des mesures basées sur les appareils en téléchargeant des objets de référence et en comparant les infrastructures internes et externes, les centres de données, les réseaux de distribution et les plateformes cloud tels que vus par les utilisateurs finaux réels des sites ou des applications Web.

Principaux avantages de la participation

Radar répond à de nombreux défis liés à la diffusion Web grâce à son approche de surveillance et de collecte de données. Les principaux avantages de la participation à la communauté Radar sont les suivants :

- Environnement de test massif, avec des utilisateurs finaux sur tous les réseaux et sur tous les sites (plus de 42 000 réseaux reconnus à ce jour).
- Obtenez des informations importantes sur les fournisseurs de services avant de les tester afin de prendre une décision plus éclairée.
- Transparence des performances des fournisseurs actuels et de leur comportement dans les zones géographiques où vous avez ou n'avez pas d'utilisateurs.
- Concentrez-vous sur les indicateurs qui font une réelle différence pour les utilisateurs du Web et des appareils mobiles (performance, disponibilité et qualité de service).
- Vue globale (plus de 190 pays) des informations illimitées au niveau du pays, du réseau, de la région et de l'État.
- Des données réelles et impartiales provenant des utilisateurs finaux Les données radar sont des informations du « monde réel » plutôt qu'un test synthétique ou une meilleure estimation.
- Tous les utilisateurs ne sont pas les mêmes : comprenez les différentes machines, connexions et appareils.
- Visibilité sur les performances des pages réelles.

Points de référence

ITM Radar fournit 3 points de référence principaux :

- Analyse comparative communautaire
- Benchmarking privé
- Analyse comparative du chargement des pages

Analyse comparative communautaire du CDN, du cloud et des centres de données

Les mesures communautaires sont obtenues par le biais d'un modèle de crowdsourcing fournissant au client une vue des performances et de la disponibilité d'un fournisseur à un niveau géographique et logique à l'échelle mondiale. Les mesures communautaires permettent de comparer la qualité d'expérience d'un fournisseur telle qu'elle est perçue par l'utilisateur final et d'effectuer une analyse « hypothétique » lors de l'évaluation des fournisseurs et des fournisseurs pour la distribution de contenu et d'applications. En utilisant un modèle de crowdsourcing, les clients d'ITM bénéficient d'un meilleur niveau de granularité et de qualité des données lors de l'évaluation et du suivi des performances des fournisseurs, même dans les endroits où le client n'a pas une forte densité d'utilisateurs, voire aucun utilisateur du tout.

Les mesures elles-mêmes utilisent un ensemble standard d'objets situés dans les différents fournisseurs de cloud et de CDN que les utilisateurs finaux téléchargent lorsqu'ils exécutent le client JavaScript Radar, ou la logique du SDK mobile, sur le site ou l'application d'un propriétaire de contenu.

Les métriques suivantes sont ensuite transmises à l'ITM et présentées dans les interfaces de reporting du portail ou de l'API :

- Disponibilité : que l'objet soit chargé ou non.
- Temps de réponse : temps nécessaire au serveur pour répondre à une demande ultérieure, une fois que tout le bruit lié à l'établissement d'une connexion est terminé. Il s'agit d'une approximation relativement proche du temps d'aller-retour TCP (RTT) entre le navigateur et le fournisseur.
- Débit : débit de données de la connexion, en kilobits par seconde, tel que mesuré à partir de la récupération d'un objet de 100 Ko.

Benchmarking privé

Dans le cadre du déploiement de Radar Tag, ITM permet au client de créer ses propres tests « de référence » qui sont mesurés par les visiteurs du client. Cela peut être pour les centres de données ou pour leurs propres contrats CDN et cloud. Comme pour les mesures de référence de la communauté, les mêmes indicateurs sont fournis : disponibilité, temps de réponse et débit, ce qui permet au client d'évaluer efficacement une stratégie de diffusion de contenu existante.

Ces informations privées ne sont accessibles qu'au client et ne sont pas partagées.
Les exemples d'utilisation incluent :

- Leur propre architecture de centre de données
- En utilisant leur propre objet de test ou leur propre page
- En utilisant leur propre contrat et compte avec un fournisseur ou un ensemble de fournisseurs spécifiques

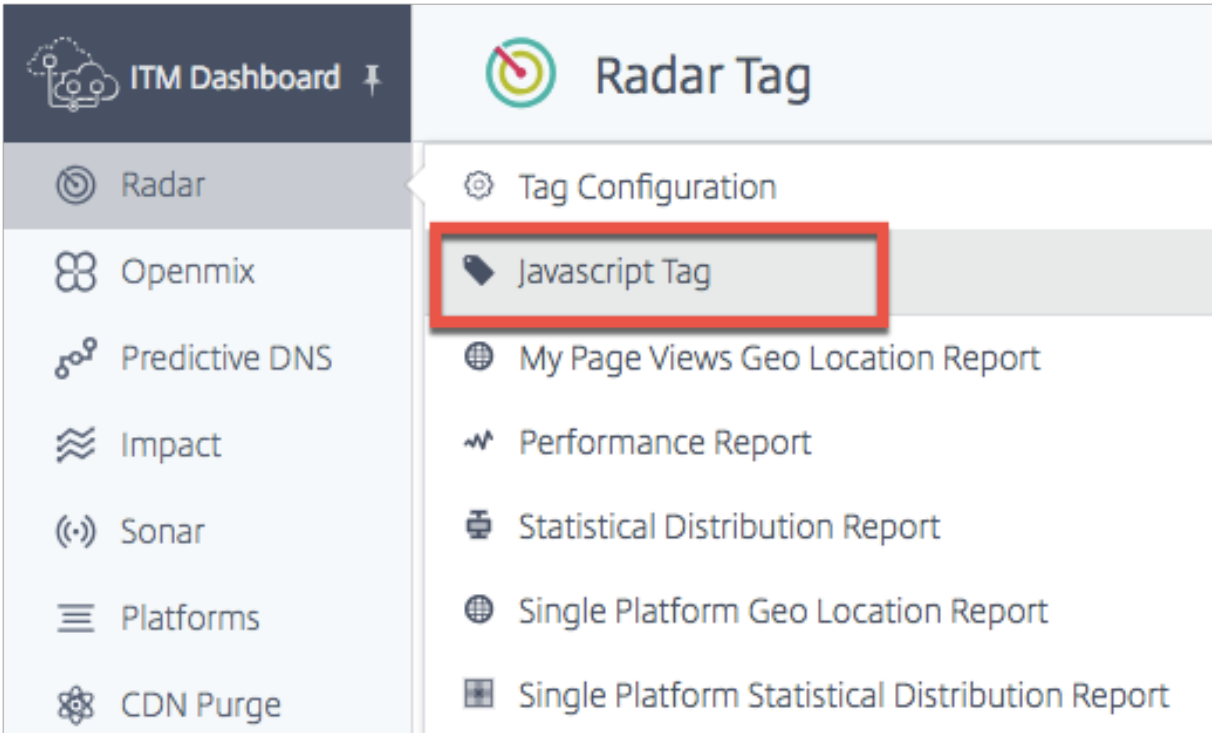
Analyse comparative du chargement des pages Radar

Dans Radar, ITM permet au client de voir des informations détaillées sur la manière dont les pages sur lesquelles le tag est implémenté sont téléchargées. L'ITM fournit des informations qui vous permettent de voir les performances réelles des utilisateurs finaux lorsqu'ils interagissent avec vos pages Web. Les données sont fournies par le biais de l'API Navigation Timing prise en charge par de nombreux navigateurs de nouvelle version.

Balise radar

La balise Radar peut être intégrée à l'aide d'un extrait de code JavaScript. Pour accéder à la page **Radar Tag**, procédez comme suit :

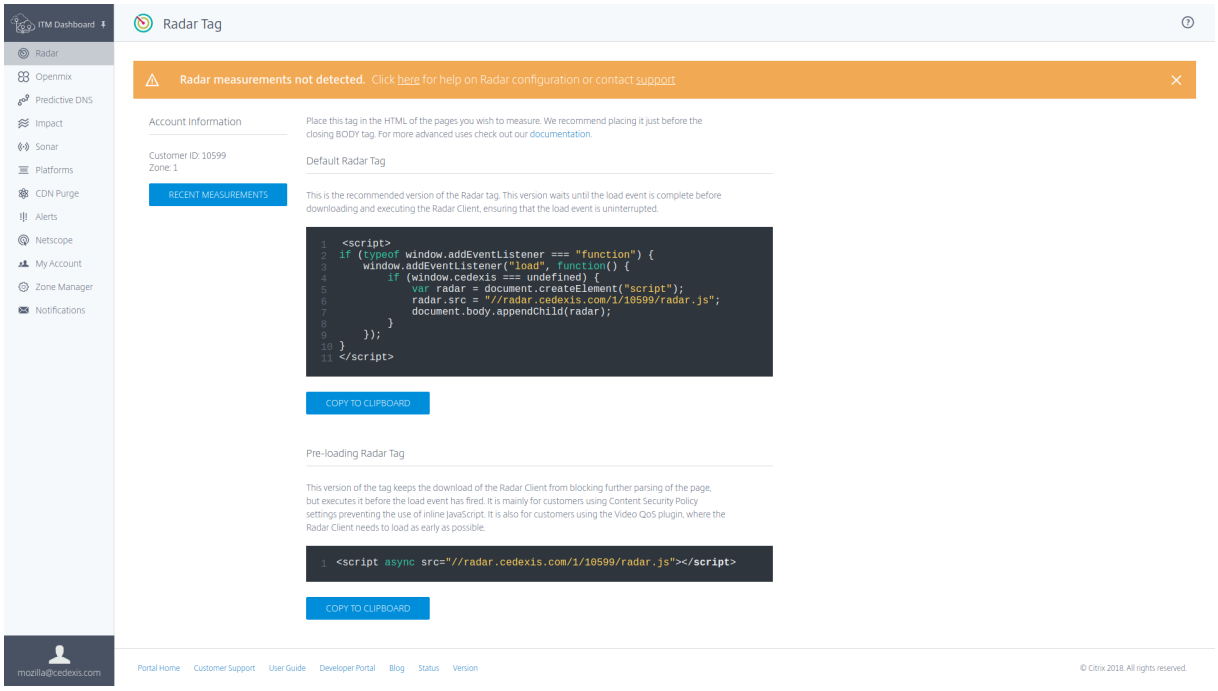
1. Connectez-vous au portail de gestion intelligente du trafic NetScaler.
2. Dans le menu de navigation de gauche, sélectionnez **Radar > Tag Javascript**.



La page **Radar Tag** s'ouvre.

Si vous n'avez pas encore configuré le tag Radar, une barre horizontale orange apparaît en haut de l'écran pour vous indiquer que les mesures radar n'ont pas été détectées.

Cette barre orange apparaîtra également si le tag n'a pas été configuré correctement.



Sinon, si le Radar Tag fonctionne comme prévu, une barre horizontale verte s'affiche pour vous indiquer que les mesures radar ont été obtenues avec succès.

Sur cette page, vous pouvez sélectionner la version de balise applicable à votre utilisation et la copier dans le presse-papiers.

Remarque : Il est important de ne pas modifier cet extrait de code JavaScript. Le code contient des informations importantes qui, si elles sont modifiées, peuvent créer un comportement inattendu ou peu fiable.

Intégration du Radar Tag

L'intégration du tag Radar est relativement simple. Il vous suffit d'ajouter l'un des extraits de code JavaScript ci-dessous au balisage de votre site. Placez-le dans le code HTML des pages que vous souhaitez mesurer. Nous vous recommandons de le placer en bas de page avant la balise body de fermeture `</body>`.

Tag radar par défaut

Il s'agit de la version recommandée de la balise Radar. Cette version attend que l'événement de chargement soit terminé avant de télécharger et d'exécuter le client Radar, ce qui garantit que l'événement de chargement est ininterrompu.

```
1  <script>
2  if (typeof window.addEventListener === "function") {
```



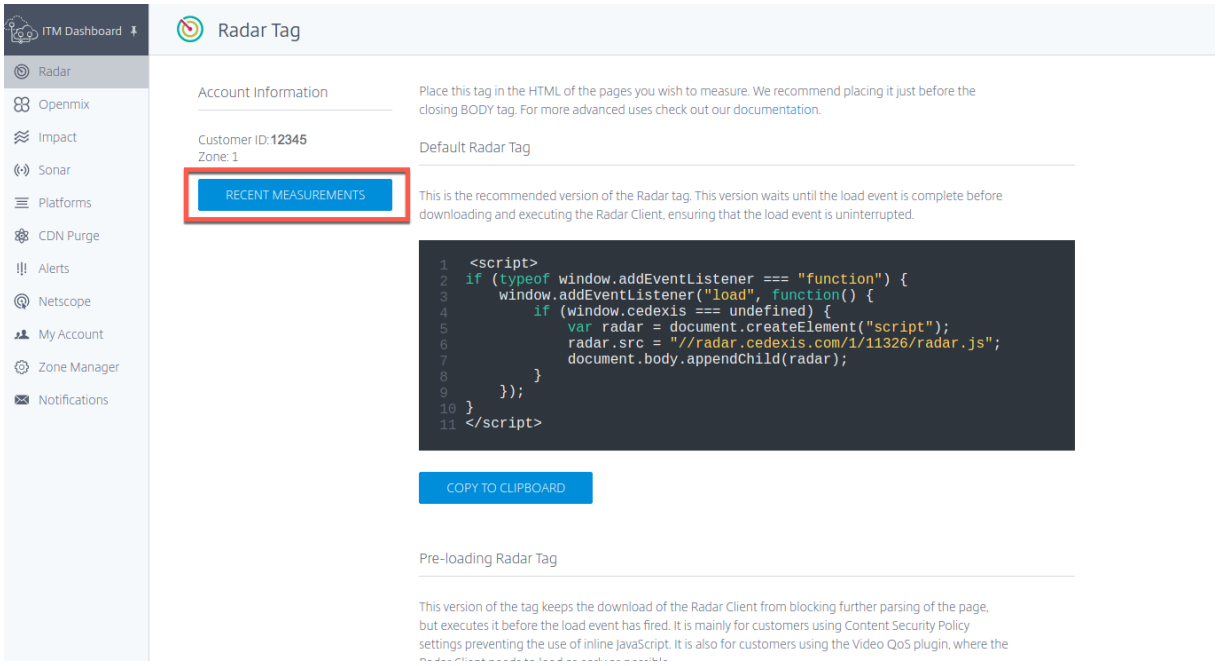
```
3
4       window.addEventListener("load", function() {
5
6           if (window.cedexis === undefined) {
7
8               var radar = document.createElement("script");
9               radar.src = "//radar.cedexis.com/1/54621/radar.js"; //
                    replace with user specific value
10              document.body.appendChild(radar);
11           }
12
13       }
14   );
15   }
16
17 </script>
18 <!--NeedCopy-->
```

Cette version de la balise empêche le téléchargement du client Radar de bloquer l'analyse ultérieure de la page, mais l'exécute avant le déclenchement de l'événement de chargement. Il s'adresse principalement aux clients utilisant des paramètres de politique de sécurité du contenu empêchant l'utilisation de JavaScript en ligne. Il est également destiné aux clients utilisant le plug-in Video QoS, où le client Radar doit être chargé le plus tôt possible.

```
1 <script src="//radar.cedexis.com/1/54621/radar.js" async></script>
2 <!--NeedCopy-->
```

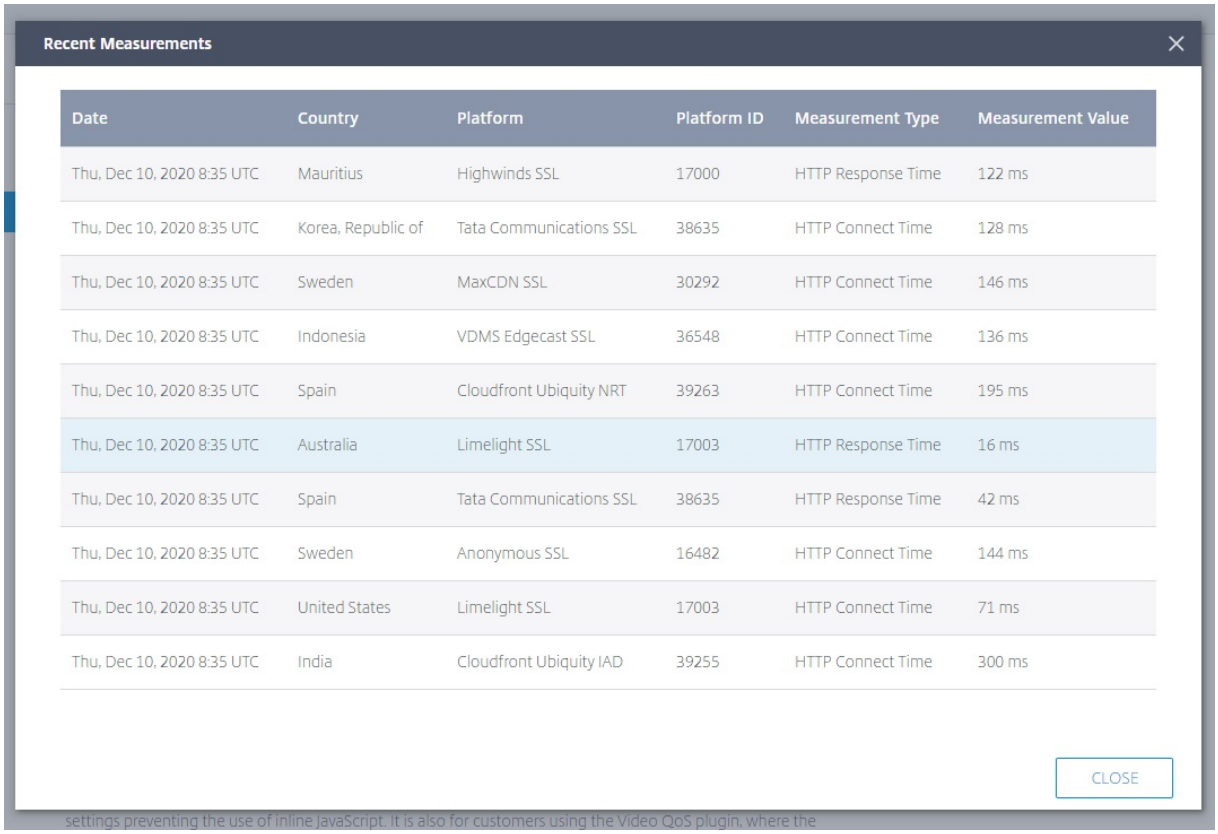
Mesures récentes

Le tableau **des mesures récentes** vous permet de visualiser les dernières mesures prises à l'aide du radar.



Cliquez sur le bouton **Mesures récentes** . Il vous donne les informations suivantes :

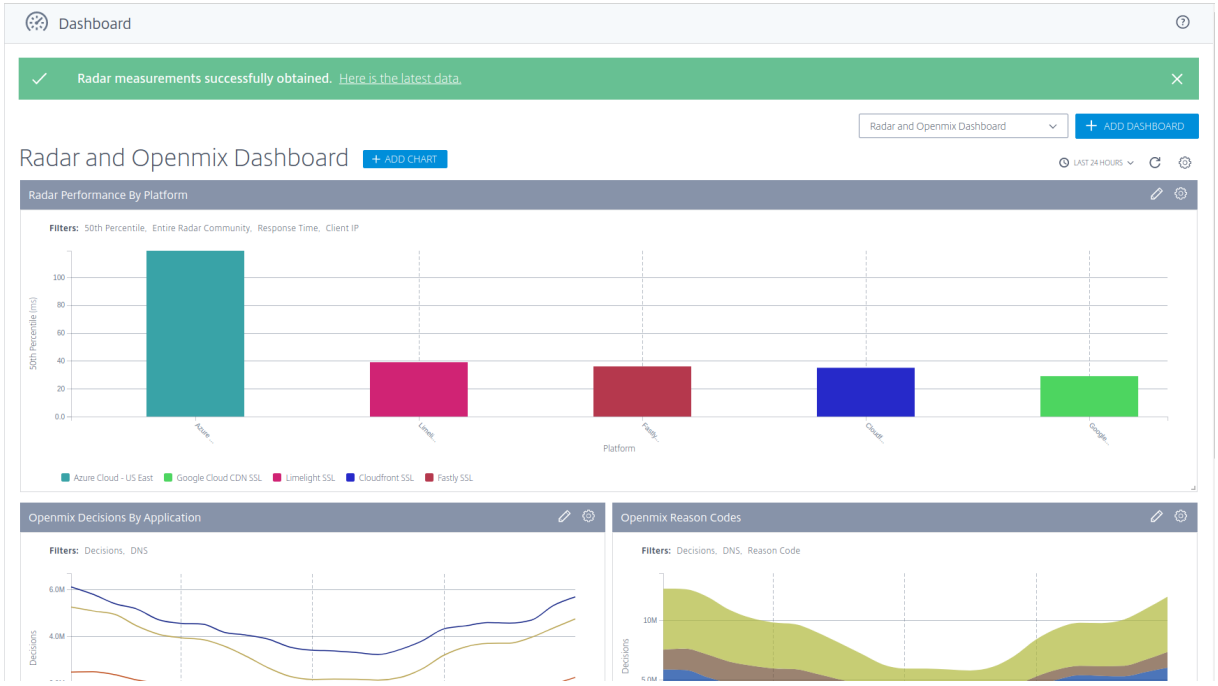
- Date et heure auxquelles la mesure a été prise en UTC.
- Pays dans lequel la mesure a été prise.
- La plateforme qui a été utilisée pour effectuer la mesure.
- L'ID de la plateforme.
- Type de mesure prise, à savoir le temps de connexion (en millisecondes), le temps de réponse (en millisecondes) ou le débit (en kilobits par seconde)
- La valeur réelle de la mesure en millisecondes (pour le temps de connexion et le temps de réponse) ou en kilobits par seconde (pour le débit).



Date	Country	Platform	Platform ID	Measurement Type	Measurement Value
Thu, Dec 10, 2020 8:35 UTC	Mauritius	Highwinds SSL	17000	HTTP Response Time	122 ms
Thu, Dec 10, 2020 8:35 UTC	Korea, Republic of	Tata Communications SSL	38635	HTTP Connect Time	128 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	MaxCDN SSL	30292	HTTP Connect Time	146 ms
Thu, Dec 10, 2020 8:35 UTC	Indonesia	VDMS Edgecast SSL	36548	HTTP Connect Time	136 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Cloudfront Ubiquity NRT	39263	HTTP Connect Time	195 ms
Thu, Dec 10, 2020 8:35 UTC	Australia	Limelight SSL	17003	HTTP Response Time	16 ms
Thu, Dec 10, 2020 8:35 UTC	Spain	Tata Communications SSL	38635	HTTP Response Time	42 ms
Thu, Dec 10, 2020 8:35 UTC	Sweden	Anonymous SSL	16482	HTTP Connect Time	144 ms
Thu, Dec 10, 2020 8:35 UTC	United States	Limelight SSL	17003	HTTP Connect Time	71 ms
Thu, Dec 10, 2020 8:35 UTC	India	Cloudfront Ubiquity IAD	39255	HTTP Connect Time	300 ms

settings preventing the use of inline JavaScript. It is also for customers using the Video QoS plugin, where the

La barre de mesures radar apparaîtra également sur la page du tableau de **bord** radar lorsque vous vous connecterez pour la première fois au portail ITM.



Intégration aux applications mobiles

L'intégration aux applications mobiles s'effectue via des wrappers entourant des vues Web masquées qui exécutent le client JavaScript. Cela garantit la cohérence des données collectées dans les navigateurs et les applications mobiles.

Instructions pour intégrer Radar à l'application iOS
Ce référentiel GitHub suivant contient le code wrapper et les instructions étape par étape pour intégrer Radar à l'application iOS :

Radar Runner pour iOS

Instructions pour intégrer Radar à Android
Android Radar est une bibliothèque cliente qui facilite l'intégration de Radar dans les applications Android. Vous pouvez le trouver ici :

Bibliothèque AndroidRadar

Intégration à NetScaler

La balise Radar est importante car elle fournit à Openmix des mesures qui permettent à Openmix de prendre de meilleures décisions en matière de routage. Plus le nombre de pages Web utilisant la balise est élevé, meilleures sont les décisions de routage.

Les méthodes suivantes vous permettent de placer la balise JavaScript Radar sur votre page Web à l'aide de NetScaler. Vous pouvez utiliser la ligne de commande ou l'utilitaire de configuration NetScaler.

Ces méthodes vous permettent d'injecter le tag Radar dans vos réponses. Pour injecter la balise Radar, vous devez utiliser des réécritures. Les réécritures se décomposent en trois étapes : créer des actions, configurer des politiques et lier des politiques.

Configuration en ligne de commande

Ligne de commande Configuration de l'action de réécriture Modèle :

```
add rewrite action <name> <type> <target> [<stringBuilderExpr>] [-pattern <expression> | -search <expression>] [-refineSearch <string>] [-comment <string>]
<!--NeedCopy-->
```

Exemple :

```
add rewrite action radar_tag action insert_after HTTP.RES.BODY(HTTP.RES.CONTENT_LENGTH).BEFORE_STR("</body>") '"<script async src=\\"//radar.cedexis.com/1/<customer_id>/radar.js\\"></script>"'
```



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

Remarque : insérez votre propre numéro de client là où il est écrit `<customer_id>`

Configuration de la politique de réécriture par la ligne de commande Modèle :

```
add rewrite policy <name> <rule> <action> [<undefAction>] [-comment <
    string>] [-logAction <string>]
<!--NeedCopy-->
```

Exemple :

```
add rewrite policy radar_tag_policy HTTP.RES.HEADER("Content-Type").
    TO_LOWER.CONTAINS("text/html") radar_tag_action
<!--NeedCopy-->
```

Politique de réécriture liée à la ligne de commande Modèle 1 :

```
bind vpn vserver <name> [-policy <string> [-priority <positive_integer
    >] [-secondary] [-groupExtraction] [-gotoPriorityExpression <
    expression>] [-type <type>]] [-intranetApplication <string>] [-
    nextHopServer <string>] [-urlName <string>] [-intranetIP <ip_addr> <
    netmask> ] [-staServer <URL> [-staAddressType ( IPV4 | IPV6 )]] [-
    appController <URL>] [-sharefile <string>]
<!--NeedCopy-->
```

Exemple 1 :

```
bind vpn vserver <name_of_vserver> -policy radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Modèle 2 :

```
bind cs vserver <name> (-lbvserver <string> | -vServer <string> | (-
    policyName <string> [-targetLBVserver <string>] [-priority <
    positive_integer>] [-gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] ) | (-
    domainName <string> [-TTL <secs>] [-backupIP <ip_addr|ipv6_addr|*>]
    [-cookieDomain <string>] [-cookieTimeout <mins>] [-sitedomainTTL <
    secs>]))
<!--NeedCopy-->
```

Exemple 2 :

```
bind cs vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Modèle 3 :


```
bind lb vserver <name>@ (<serviceName>@ [- weight <positive_integer>])
    | <serviceGroupName>@ | (- policyName <string>@ [-priority <
    positive_integer>] [- gotoPriorityExpression <expression>] [-type (
    REQUEST | RESPONSE )] [-invoke (<labelType> <labelName>) ] )
<!--NeedCopy-->
```

Exemple 3 :

```
bind lb vserver <name_of_vserver> -policyName radar_tag_policy -type
    RESPONSE -priority 10
<!--NeedCopy-->
```

Modèle 4 :

```
bind rewrite global <policyName> <priority> [<gotoPriorityExpression>]
    [-type <type>] [-invoke (<labelType> <labelName>) ]
<!--NeedCopy-->
```

Exemple 4 :

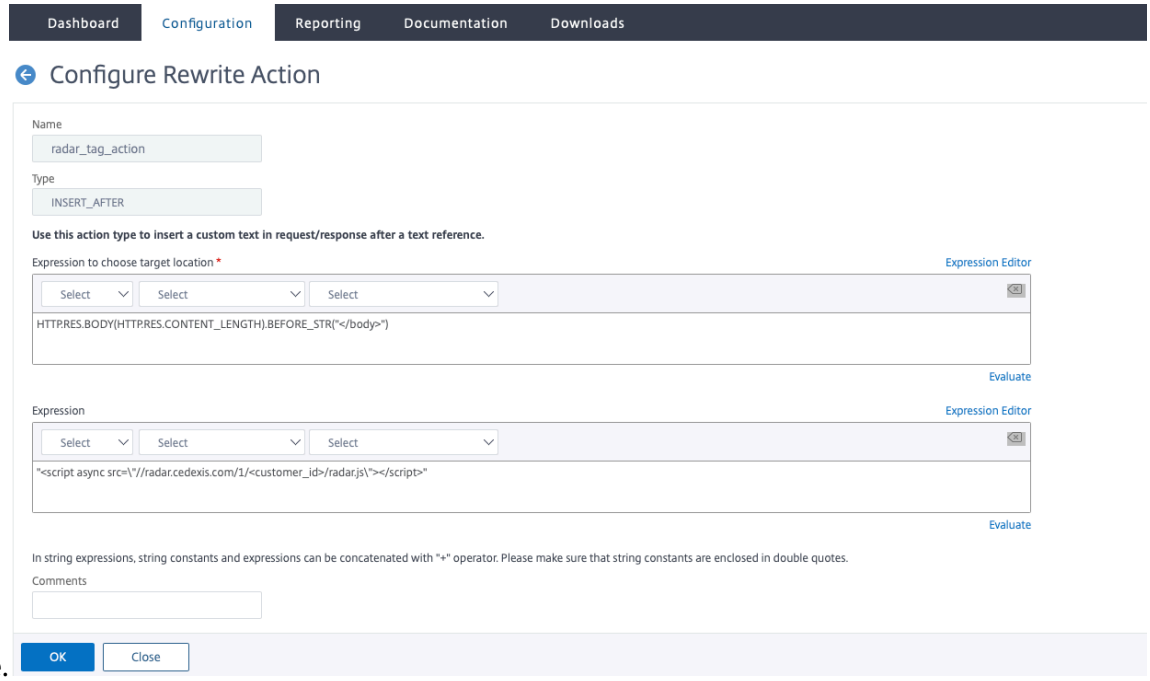
```
bind rewrite global radar_tag_policy 100 -type RES_DEFAULT
<!--NeedCopy-->
```

Configuration de l'utilitaire GUI

Action de réécriture de l'interface graphique

1. ****Dans le menu de navigation de gauche de la page de configuration de **NetScaler**, accédez à **AppExpert** -> Rewrite -> Rewrite Actions**
2. Sélectionnez le bouton **Ajouter** .
3. Dans la page **Configurer l'action de réécriture**, saisissez l'expression comme indiqué dans l'

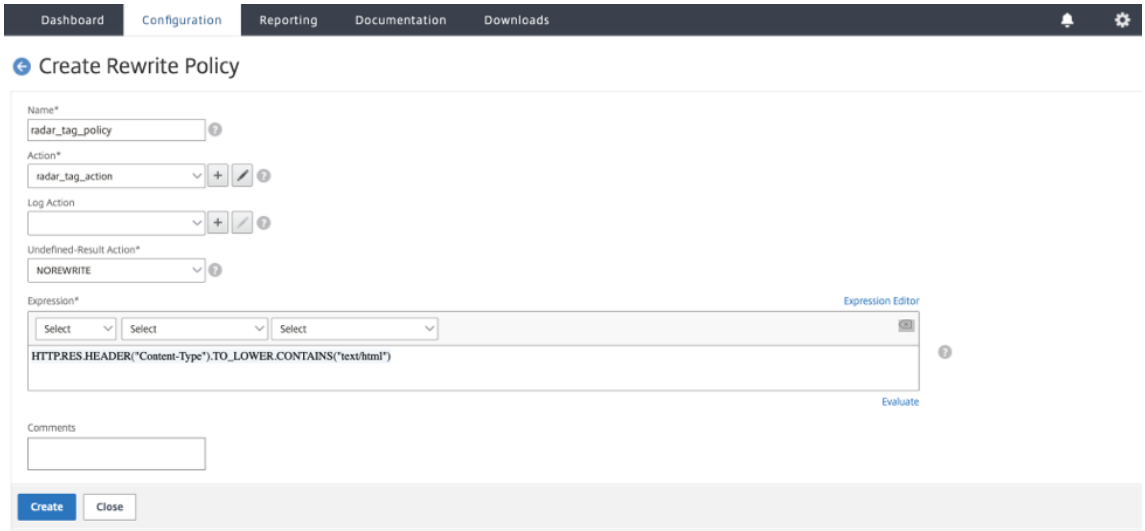
exemple.



4. Dans le script Radar, entrez votre numéro de client dans l'espace marqué `<customer_id>`.
5. Sélectionnez **OK**. Vous avez terminé de créer votre action de réécriture.

Politique de réécriture de l'interface graphique

1. ****Dans le menu de navigation de gauche de la page de configuration de **NetScaler**, accédez à **AppExpert -> Réécriture -> Politiques** de réécriture**
2. Sélectionnez le bouton **Ajouter** .
3. Sur la page **Configurer la politique de réécriture**, saisissez l'expression comme indiqué dans l'exemple.

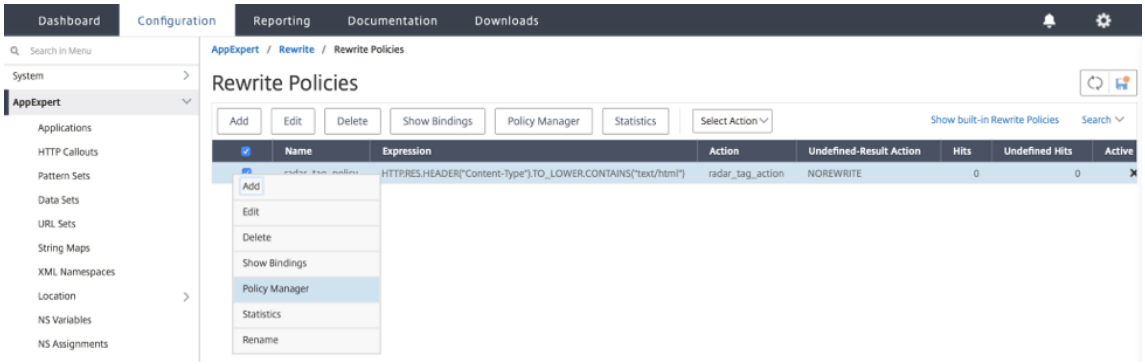


4. Cliquez sur **Create**.

Vous avez terminé la configuration de la politique de réécriture.

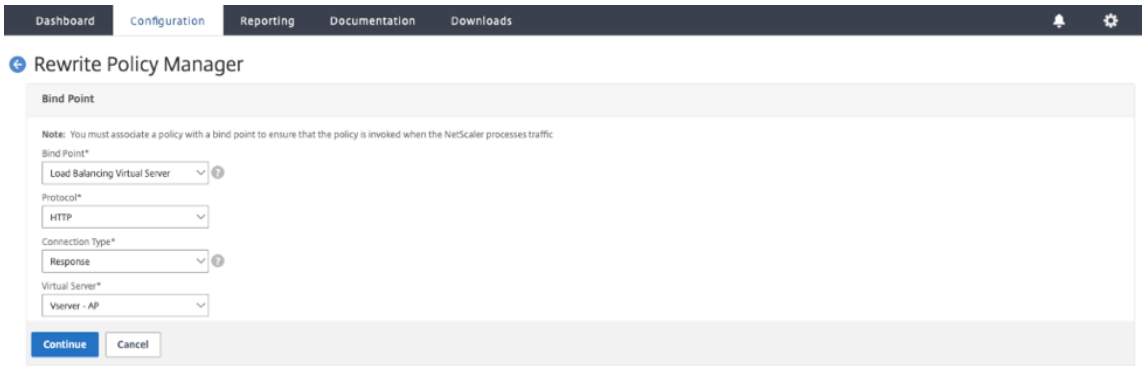
Politique de réécriture des liaisons de l'interface graphique Une fois que vous avez terminé de configurer votre politique, la dernière étape consiste à lier la politique à l'aide du **Policy Manager**.

1. Accédez à la page des **politiques de réécriture** .
2. Sélectionnez la politique de réécriture que vous avez créée pour le Radar Tag.
3. Accédez au **Gestionnaire de politiques**.



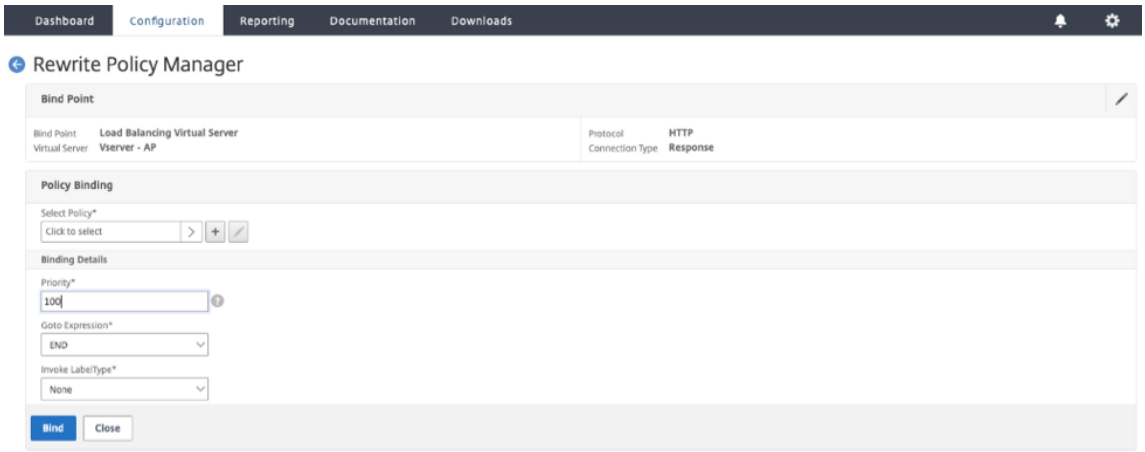
4. Dans la page **Gestionnaire de politiques**, vous pouvez lier la politique en procédant comme suit.

   - Pour **Bind Point**, vous avez la possibilité de sélectionner **Override Global**, **Serveur virtuel VPN, Serveur virtuel**de **commutation de contenu ou Serveur virtuel**d' **équilibrage de charge**.
   - Pour **Protocole**, sélectionnez **HTTP**.
   - Pour **Type de connexion**, sélectionnez **Réponse**.
   - Pour **Virtual Server**, utilisez votre propre nom de serveur virtuel.



   - Cliquez sur **Continuer**.
   - Sur la page suivante, sélectionnez la **politique de réécriture** que vous avez créée précédemment.

- Ajoutez les **détails de la reliure**.
- Cliquez sur **Bind**.

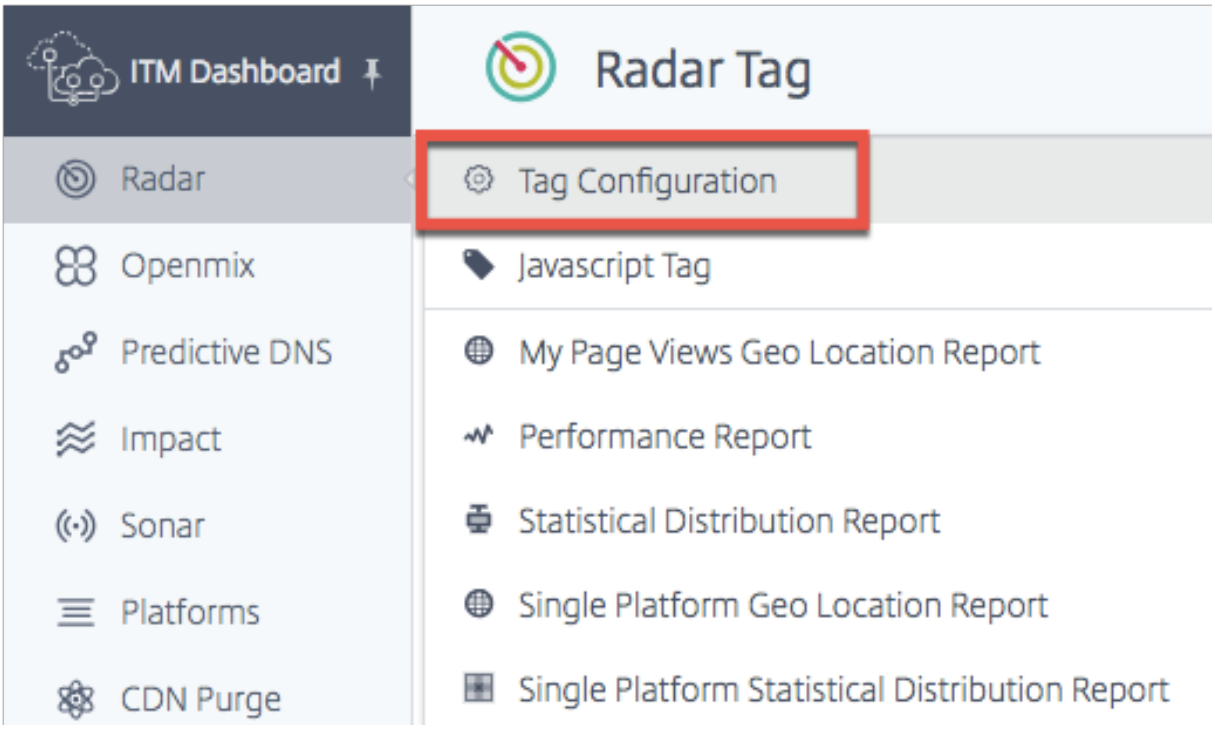


Avec les méthodes ci-dessus, vous pouvez insérer la balise Radar dans vos pages Web. Cependant, il convient de noter qu'il s'agit d'une implémentation de base. Un filtrage supplémentaire peut être effectué pour mieux contrôler les pages sur lesquelles la balise est implémentée.

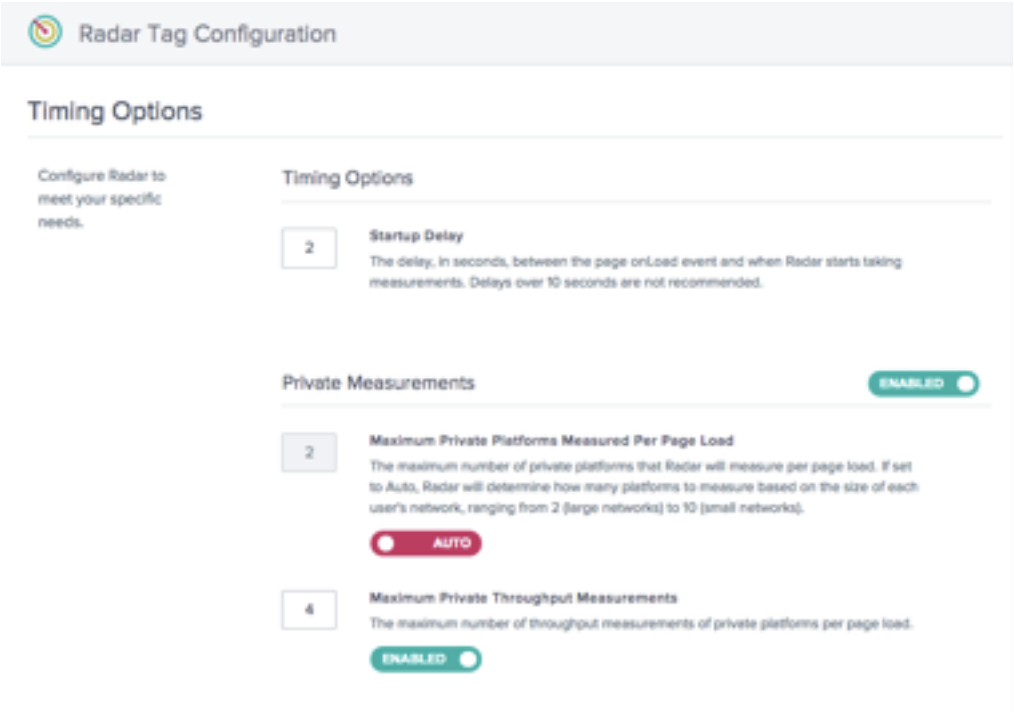
Configuration des balises radar

Vous pouvez configurer le radar sur la page de **configuration des balises radar** .

1. Connectez-vous au portail de gestion intelligente du trafic NetScaler.
2. Dans le menu de navigation de gauche, sélectionnez **Radar > Configuration des balises**.



La page de configuration des balises radar s'ouvre. Ici, vous pouvez définir différentes options pour personnaliser les mesures radar. Le JavaScript Radar comporte des paramètres que vous pouvez personnaliser pour ajuster les éléments de temporisation et de délai, le nombre de tests effectués par les utilisateurs finaux pour des mesures communautaires et privées, et les valeurs de délai pour mesurer la disponibilité, etc.



Le tableau suivant fournit des informations sur les options de configuration et les paramètres par défaut de chacune d'entre elles. Lorsque vous apportez des modifications, assurez-vous de cliquer sur **Mettre à jour les paramètres du radar** en bas de l'écran pour appliquer les modifications.

Fonction	Paramètre	Description	Paramètre par défaut
Options de chronométrage	Retard de démarrage	Délai, en secondes, entre l'événement OnLoad de la page et le moment où Radar enregistre le temps de navigation.	2 secondes
	Retard de répétition	Le délai, en minutes, entre les sessions de mesure. Si la valeur est supérieure ou égale à 5, le tag Radar prendra davantage de mesures après chaque intervalle de retard de répétition. Si la valeur est 0, le Radar Tag ne prendra aucune mesure supplémentaire.	5 minutes
Options de protocole	Autoriser toujours les mesures HTTPS privées	Permet au client Radar de prendre des mesures HTTPS même à partir d'un site Web HTTP.	Prend des mesures sur les plateformes dont les protocoles URL correspondent à la page sur laquelle le client Radar est exécuté.
	Autorisez les mesures HTTP privées sur les connexions HTTPS.	Permet au client Radar de prendre des mesures HTTP à partir d'un site Web HTTPS.	Prend des mesures sur les plateformes dont les protocoles URL correspondent à la page sur laquelle le client Radar est exécuté.

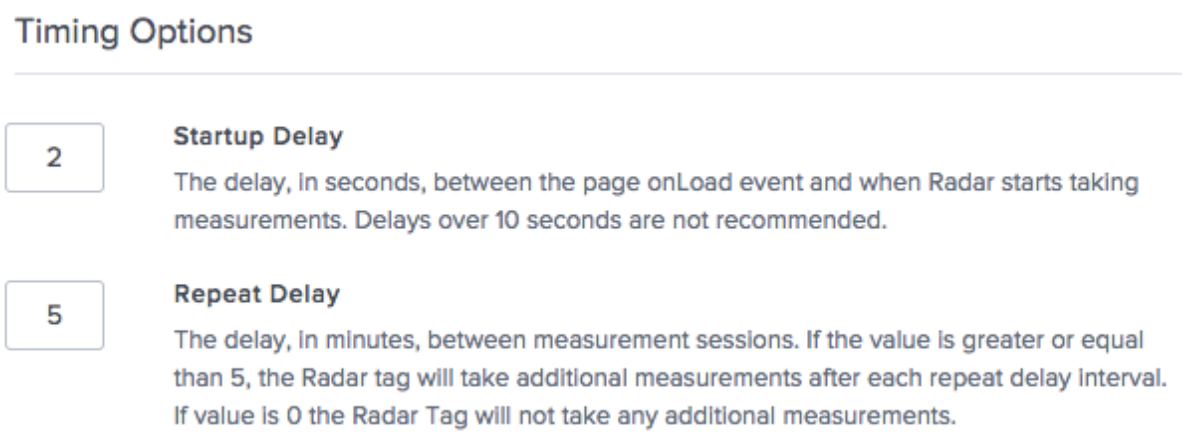
Fonction	Paramètre	Description	Paramètre par défaut
Fréquence d' échantillonnage	Fréquence d' échantillonnage du radar	Pourcentage de pages où la balise Radar est activée pour prendre des mesures.	Désactivé
Mesures privées	Nombre maximal de mesures privées par chargement de page	Le nombre maximum de plateformes privées que Radar mesurera par chargement de page.**	Auto*
	Mesures du débit privé maximal	Le nombre maximal de mesures de débit des plateformes privées par chargement de page.**	4
Mesures communautaires	Nombre maximal de mesures communautaires par chargement de page	Le nombre maximum de plateformes communautaires que Radar mesurera par chargement de page.**	Auto*
	Mesures du débit maximal de la communauté	Le nombre maximal de mesures de débit des plateformes communautaires par chargement de page.**	4

*Auto signifie que NetScaler Intelligent Traffic Management détermine le nombre de plateformes à mesurer pour une session donnée, en fonction de l'emplacement de l'utilisateur final. Nous essayons de mesurer un plus grand nombre de plateformes par session pour les petits réseaux, où les données sont rares, plutôt que pour les grands réseaux, où elles sont denses.

**Il s'agit du nombre maximum de mesures tentées par session. Par exemple, Radar peut mesurer 4 plateformes privées par session, toutes configurées pour mesurer à la fois le RTT et le débit. Mais si les mesures de débit privé maximum sont définies sur 2, le client cessera d'inclure les mesures de débit après avoir mesuré les 2 premières plateformes privées. Pour les deux dernières plateformes, il ne mesurera que le RTT.

Les options de chronométrage vous permettent de définir la durée pendant laquelle le radar doit attendre avant de commencer à prendre des mesures.

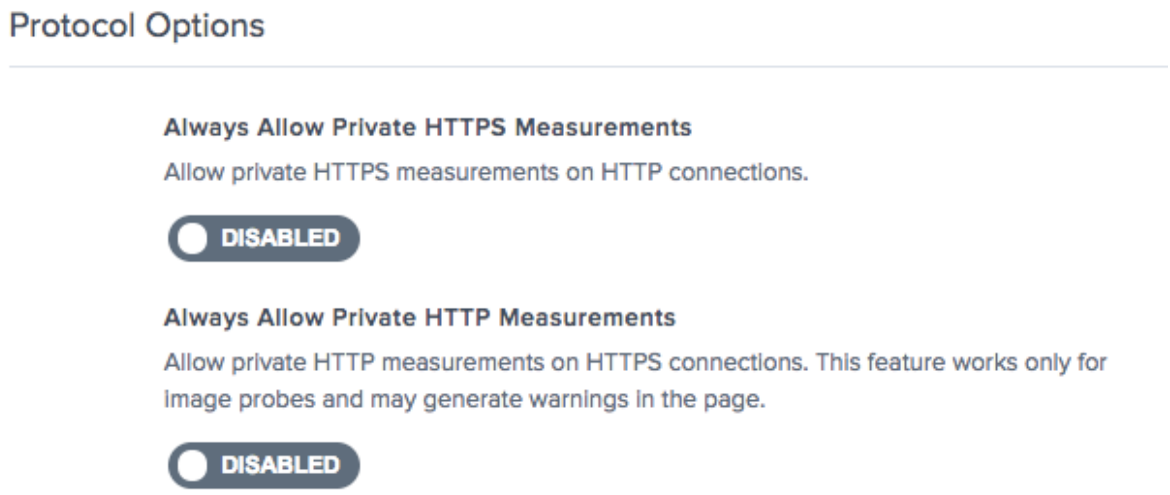
Remarque : le délai de démarrage est exprimé en secondes, tandis que le **délai de répétition** est exprimé en minutes.



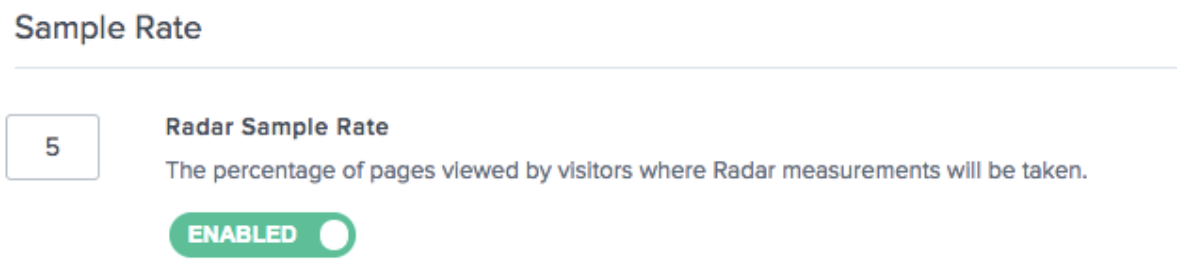
Options de protocole

Normalement, le client Radar mesure uniquement les plateformes avec des URL dont les protocoles correspondent à ceux de la page sur laquelle il s'exécute. Ces options vous permettent de modifier ce comportement pour les plateformes privées. Par exemple, l'activation de « Toujours autoriser les mesures HTTPS privées » permet au client `https://myprovider.com/r20.png` de mesurer à partir de `http://example.com`, tandis que « Toujours autoriser les mesures HTTP privées » permet au client `http://myprovider.com/r20.png` de mesurer à partir de `https://example.com`.

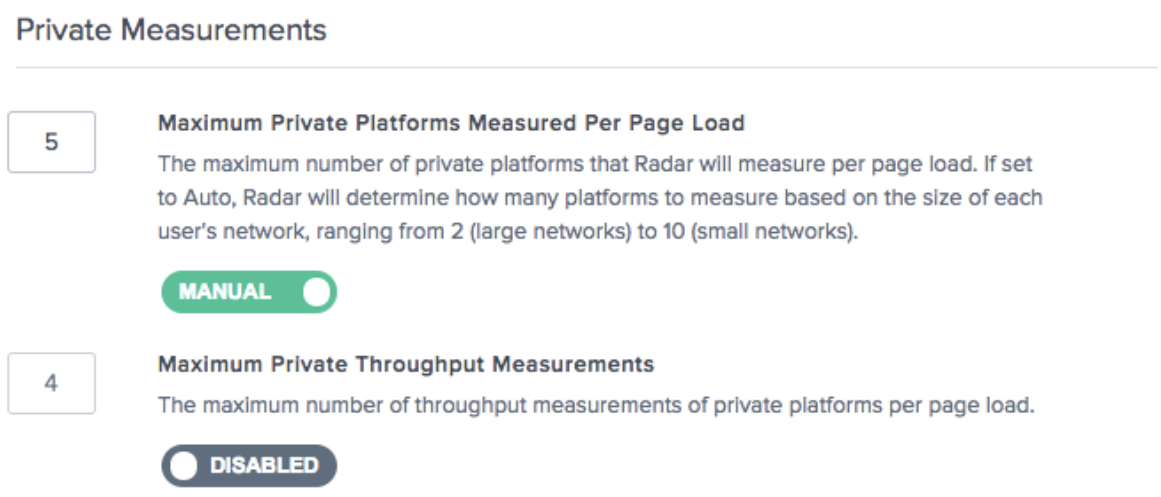
Ces options doivent généralement être évitées, sauf dans les cas d'utilisation extrêmes. Le meilleur moyen de garantir une densité de mesures privées adéquate est de configurer vos plateformes pour mesurer les plateformes et les protocoles que vous utilisez réellement en production (et pas plus), et de déployer la balise Radar sur autant de pages de production que possible. Nous appelons parfois cela « Mettre le radar là où c'est nécessaire ». «



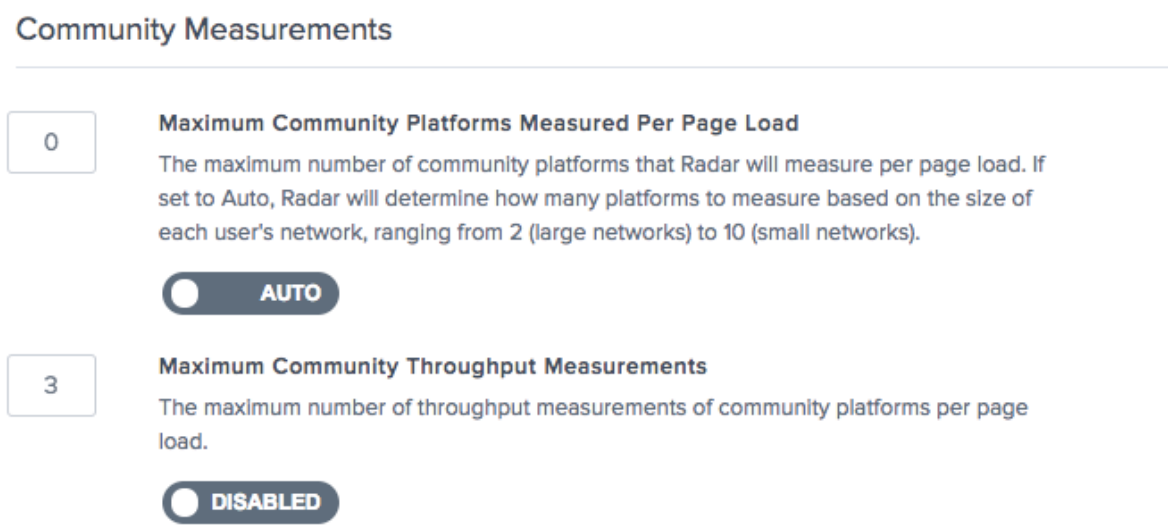
Le taux d'échantillonnage vous permet de définir un pourcentage de pages Web (consultées par les utilisateurs) à partir desquelles des mesures seront collectées. Par exemple, si votre site Web enregistre 100 000 pages vues par jour et que vous définissez un taux d'échantillonnage de 5 %, Radar ne collectera des mesures qu'à partir de 5 % des 100 000 pages vues.



Mesures privées Ces paramètres s'appliquent aux mesures de vos plateformes privées. Les plateformes privées sont celles que vous configurez dans la section **Plateformes** pour mesurer des CDN spécifiques, des fournisseurs de cloud et d'autres parties de votre infrastructure. Consultez la section Plateformes pour plus d'informations.



Cette option vous permet de configurer le comportement de Radar lorsque vous renvoyez des informations à la communauté.



Désactiver les tests radar

S'il est nécessaire de désactiver rapidement les mesures radar en cas d'imprévu, vous pouvez le faire depuis le portail pour éviter de modifier le code d'urgence de votre site.

Sur la page de configuration des balises radar, désactivez les mesures privées, les mesures communautaires ou les deux en cliquant sur le bouton **Activé** pour désactiver.

Cliquez sur **Enregistrer la configuration du radar** pour confirmer les modifications. Les modifications peuvent prendre une minute ou deux pour se propager, après quoi les mesures radar s'arrêtent.

mesures communautaires

Méthodologie du client Radar

La **session**est une dimension fondamentale du comportement du client. Toutes les données envoyées par le client sont associées à une session. Les sessions sont créées en effectuant un appel aux serveurs NetScaler ITM, appelé demande d'initialisation. Les sessions expirent assez rapidement, ce qui permet de garantir que seules les données radar valides sont acceptées. Grâce à cette fonctionnalité, les mesures radar sont toujours fournies par lots associés à leur identifiant de transaction de session, et nous faisons souvent référence à une « session radar » pour décrire les mesures qui y sont associées.

Séance radar

Une session Radar est la principale unité de travail effectuée par le client. Il consiste en une demande adressée aux serveurs NetScaler ITM pour obtenir la configuration du client et un ensemble de plateformes à mesurer, suivie de demandes visant à mesurer ces plateformes et à communiquer les résultats. Elles se déroulent de manière asynchrone et sérialisée, de sorte qu'une seule demande a lieu à la fois. Une session typique se termine en moins de 10 secondes.

Types de sondes

Chaque rapport envoyé par le client est associé à un type de sonde, qui indique au système de quel type de mesure il s'agit et comment le traiter. Il indique également les types de mesures à effectuer, qui peuvent inclure la disponibilité, le temps de trajet aller-retour, le débit ou toute autre collecte métrique. »

Il existe une relation importante entre la disponibilité et l'analyse des performances (comme le temps de trajet aller-retour et le débit). La disponibilité d'une ressource particulière est toujours mesurée en premier lors d'une session de mesure particulière. Ce n'est que si la mesure de disponibilité réussit que des mesures de performance supplémentaires de la même ressource peuvent être prises au cours de cette même session. «

Si un réseau particulièrement lent subit une panne de disponibilité, cela peut entraîner une amélioration effective des performances agrégées des rapports incluant ce réseau. Il ne s'agit que d'un artefact

lié au reporting, car NetScaler Intelligent Traffic Management utilise toujours les données de performance les plus détaillées et spécifiques au réseau pour prendre des décisions en temps réel.

Disponibilité La disponibilité, également connue sous le nom de sondes de démarrage à froid, est destinée à permettre aux services de réchauffer leurs caches. Bien qu'une valeur de mesure soit associée à cette sonde. Nous utilisons la sonde de disponibilité pour déterminer si le fournisseur est disponible.

Si une plate-forme n'est pas configurée pour effectuer une sonde de démarrage à froid, nous utilisons les résultats de la sonde RTT au lieu d'un rapport de démarrage à froid pour fournir des mesures de disponibilité.

De même, pour les objets dynamiques qui mesurent les services d'accélération du site, le client télécharge le petit objet de test une seule fois et indique la valeur de mesure pour le démarrage à froid et le temps de réponse.

Objet de test	Définition
Standard	Utilisation des horodatages temporels des ressources : ResponseStart - RequestStart
Méthode dynamique	Utilisation des horodatages temporels des ressources : ResponseEnd - DomainLookupStart

RTT

Objet de test	Intervalle	API	Description
Standard	ResponseStart - RequestStart	Calendrier des ressources	Durée pendant laquelle un seul paquet doit être renvoyé en réponse à une requête HTTP.
Méthode dynamique	ResponseEnd - DomainLookupStart	Calendrier des ressources	Le délai de traitement d'une demande, y compris le temps de recherche DNS, le temps de connexion et le temps de réponse.

Débit

Objet de test	Intervalle	API	Description
Standard	Taille du fichier (kilo-octets) * 8/(ResponseEnd - RequestStart)	Calendrier des ressources	Débit mesuré (kilobits par seconde) pour l'ensemble d'une demande et d'une réponse basées sur le téléchargement d'un objet de test volumineux.
Méthode dynamique	Taille du fichier (kilo-octets) * 8/(ResponseEnd - DomainLookupStart)	Calendrier des ressources	Débit mesuré (kilobits par seconde) pour l'ensemble d'une demande et d'une réponse basées sur le téléchargement d'un objet de test volumineux. Cela n'inclut généralement pas le temps de connexion ou le temps de recherche DNS au cas où un objet de test RTT aurait déjà été téléchargé.

Objets de test

Les objets de test sont des fichiers hébergés sur des plateformes et téléchargés par le client pour générer des mesures. Cette section décrit les différents types d'objets de test pris en charge par le client. Tous les types d'objets ne s'appliquent pas à toutes les plateformes.

En-tête obligatoire :

L'en-tête de réponse Timing-Allow-Origin est requis pour permettre à JavaScript d'accéder aux données de chronométrage de bas niveau fournies par l'API Resource Timing. Le paramètre recommandé est `Timing-Allow-Origin: *`, ce qui indique que l'autorisation d'accéder aux données temporelles de la ressource doit être accordée à JavaScript exécuté sur n'importe quel domaine.

Standard Les objets de test standard sont des médias que le client télécharge en définissant l'`src` attribut sur un objet Image. Une fois le téléchargement terminé, le client utilise l'API Resource Timing pour recueillir des données de performance.
Ces objets de test doivent être servis avec l'en-tête de réponse Timing-Allow-Origin. Consultez la section **Timing-Allow-Origin Header** pour plus d'informations.

Standard : petit Le petit objet de test standard est un fichier image d'un pixel, utilisé lorsque le client doit effectuer une demande réseau légère.

Le petit objet de test standard est utilisé dans les cas d'utilisation suivants :

- Sondes de démarrage à froid non dynamiques
- Sondes temporelles aller-retour non dynamiques

Grand standard L'objet de test standard de grande taille est un fichier image de 100 Ko utilisé pour mesurer le débit d'une plate-forme.

Dénomination des objets volumineux : pour calculer le débit, le client doit connaître la taille de l'objet de test. Le client détermine le nom du fichier en recherchant KB quelque part dans le nom du fichier `r20-100KB.png`, par exemple. Les clients peuvent mesurer des fichiers image de différentes tailles à condition que le nom indique la taille du fichier de la même manière, par exemple `myimage-2048kb.jpg`.

Méthode dynamique Les objets de test dynamiques sont utilisés pour mesurer les performances associées aux services d'accélération de site.
Chacun est un fichier HTML contenant du code JavaScript capable de collecter des horodatages à partir de l'API de synchronisation de navigation et de les publier sur la page parent. Le client télécharge l'objet de test à l'aide d'un iframe et obtient ces horodatages, qu'il utilise pour calculer les mesures.

Sécurité et validation L'objet de test est un objet de 40 Ko. Une nouvelle fonctionnalité de l'objet de test est un code HMAC (code d'authentification des messages basé sur le hachage) qu'il fournit en fonction des paramètres de requête et d'une clé secrète à laquelle le serveur a accès. Ce HMAC est renvoyé avec notre mesure, ce qui nous permet de valider que le client radar a pu accéder à l'objet de test et que rien n'a été mis en cache.

Différence entre les objets de test dynamiques et standard :

Pour les mesures radar standard, nous essayons d'isoler uniquement l'activité de demande principale associée au téléchargement d'objets de test, tandis que pour les services d'accélération de site, notre objectif est de mesurer davantage cette activité. Par conséquent, la recherche DNS et le temps de connexion sont également inclus.

En outre, les mesures dynamiques visent à mesurer les performances des demandes lorsqu'elles atteignent l'origine du service, et pas seulement un cache périphérique.

Dans le portail, vous pouvez choisir cette méthodologie en procédant comme suit :

- Dans le menu de navigation de gauche, accédez à **Plateformes**.
- Cliquez sur l'icône **Ajouter une plateforme** en haut à droite de la page.
- Accédez à **Plateforme privée > Catégorie > Contenu dynamique**.
- Dans la boîte de dialogue **Objets de test radar**, cochez la case **Personnaliser les sondes** .
- Entrez l'URL du **temps de réponse** et choisissez **Webpage Dynamic** dans la liste déroulante **Type d'objet** .

Le petit objet de test dynamique est utilisé pour mesurer la disponibilité et le temps de trajet aller-retour à l'aide de la même sonde pour les services d'accélération du site.

en AV L'objet de test iNav est un fichier HTML statique contenant du code JavaScript capable d' effectuer un certain nombre de tâches. Le client indique la tâche qu'il souhaite effectuer en incluant des paramètres de chaîne de requête dans l'URL qui charge le fichier HTML dans un iframe.
L'objet de test iNav prend en charge les cas d'utilisation suivants : démarrage à froid
iNav, temps
aller-retour

IU L'objet de test IUNI est utilisé pour détecter la valeur UNI associée à un ensemble de mesures radar pour une plate-forme (l'autre méthode étant CORS AJAX qui ne nécessite pas d'objet de test distinct).

AJAX GET **La méthodologie AJAX GET peut généralement être utilisée avec n'importe quelle URL que le client souhaite mesurer, à condition qu'elle soit servie avec l'en-tête**Timing-Allow-Origin et un en-tête Access-Control-Allow-Origin approprié**.**
Dans le portail, vous pouvez choisir cette méthodologie en procédant comme suit :

- Dans le menu de navigation de gauche, accédez à **Plateformes**.
- Cliquez sur l'icône **Ajouter une plateforme** en haut à droite de la page.
- Accédez à **Plateforme privée > Catégorie > Contenu dynamique**.
- Dans la boîte de dialogue **Objets de test radar**, cochez la case **Personnaliser les sondes** .
- Entrez le **temps de réponse** et choisissez **AJAX (GET)** dans la liste déroulante **Type d'objet** .

En-tête Timing-Allow-Origin L'en-tête de réponse Timing-Allow-Origin est requis afin de permettre à JavaScript d'accéder aux données de chronométrage de bas niveau fournies par l'API Resource Timing.

Le paramètre recommandé est `Timing-Allow-Origin: *`, ce qui indique que l'autorisation d'accéder aux données temporelles de la ressource doit être accordée à JavaScript exécuté sur n'importe quel domaine.

API radar

Radar fournit des API pour les fonctions opérationnelles et de récupération de données.

- API d'opérations —Ajouter/modifier/supprimer des comptes Radar et les mécanismes de contrôle pour gérer votre compte via une API
- API de données radar —L'API de données radar ITM fournit des agrégats de données de mesure publiques et privées provenant de la communauté radar. Les données sont mises à jour en continu et mises en lots environ toutes les 60 secondes pour être récupérées par l'API. L'API de données est fournie pour permettre aux clients d'intégrer les données Radar dans leurs propres rapports et tableaux de bord. Un seul appel à l'API peut fournir des moyennes de mesures par quartiles ou moyennes de radar pour tous les pays et jusqu'à 30 ASN présentant un intérêt, pour chaque plateforme.

Rapports radar

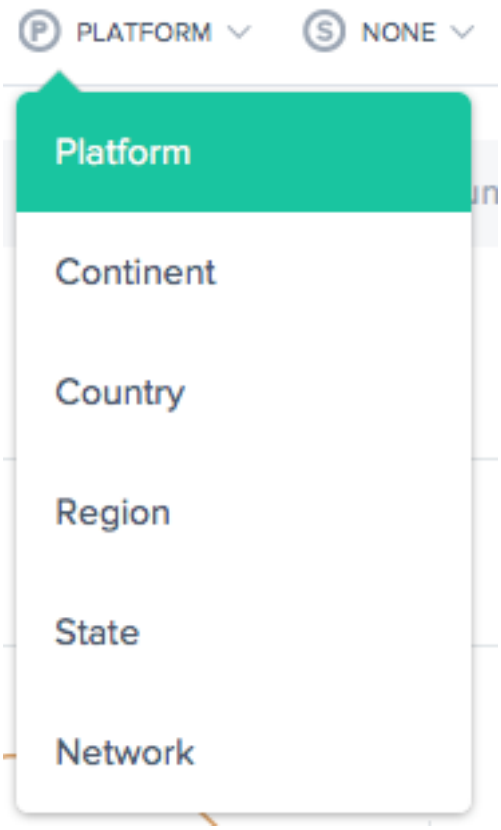
Les rapports radar fournissent une visibilité puissante sur les données dynamiques collectées par le biais du Radar Tag.

Les membres de Radar ont accès à un riche ensemble de données présenté sous forme de graphiques interactifs intuitifs. L'ensemble de données collecté intègre à la fois l'ensemble de données publiques complet de milliards de mesures et le contexte des données privées collectées à partir du tag Radar ou du déploiement du SDK mobile d'un client. Les informations relatives au temps de chargement des pages sont capturées à l'aide du propre tag du client, ce qui permet de mieux comprendre les performances réelles des utilisateurs finaux de votre site Web et de votre application mobile.

Outre les indicateurs de performance, les rapports Radar fournissent des informations sur de nombreuses facettes de votre public d'utilisateurs finaux, notamment : les volumes, les zones géographiques, les agents utilisateurs, les types de systèmes d'exploitation et le calendrier d'utilisation de votre site Web ou de votre application mobile.

Chaque rapport est défini ci-dessous, mais voici les aspects importants de tous les rapports :

Dimensions principales et secondaires

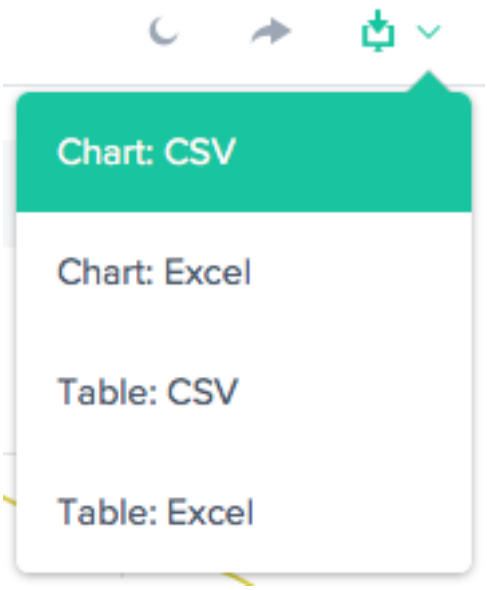


La dimension principale du graphique est sélectionnée via une liste de sélection située au-dessus du graphique. Utilisez-le comme un puissant pivot du rapport. Une dimension secondaire peut également être choisie pour affiner davantage le rapport.

Contexte de visualisation Basculer

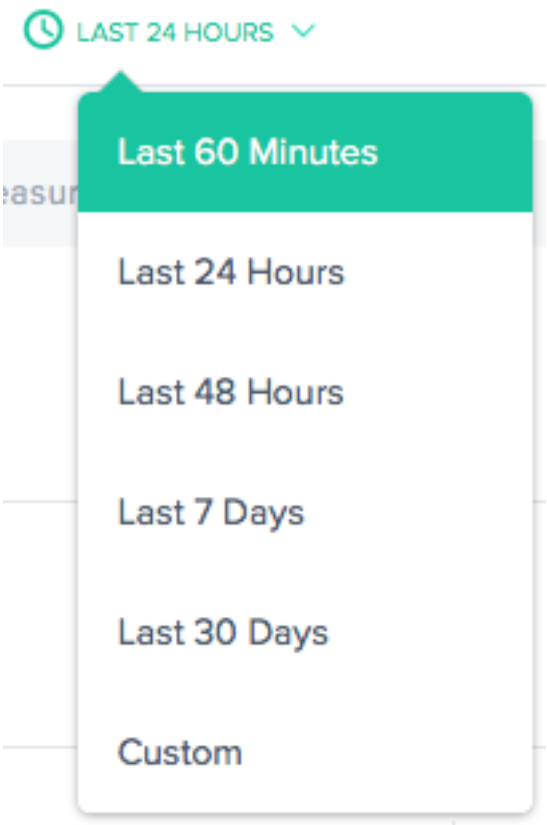
Par défaut, les graphiques sont définis sur un fond blanc. Basculez l'arrière-plan sur une couleur foncée pour les moniteurs à contraste élevé à l'aide de la bascule d'arrière-plan.

Export de données



En outre, l'utilisateur final peut télécharger les données du graphique et du tableau via le lien de téléchargement en haut du rapport.

Filtre : Période du rapport



Les rapports Radar peuvent être générés avec une plage de temps comprise entre les 60 dernières minutes, les 24 dernières heures, les 48 dernières heures, les 7 derniers jours, les 30 derniers jours ou une plage personnalisée. La vue par défaut est la dernière 24 heures.

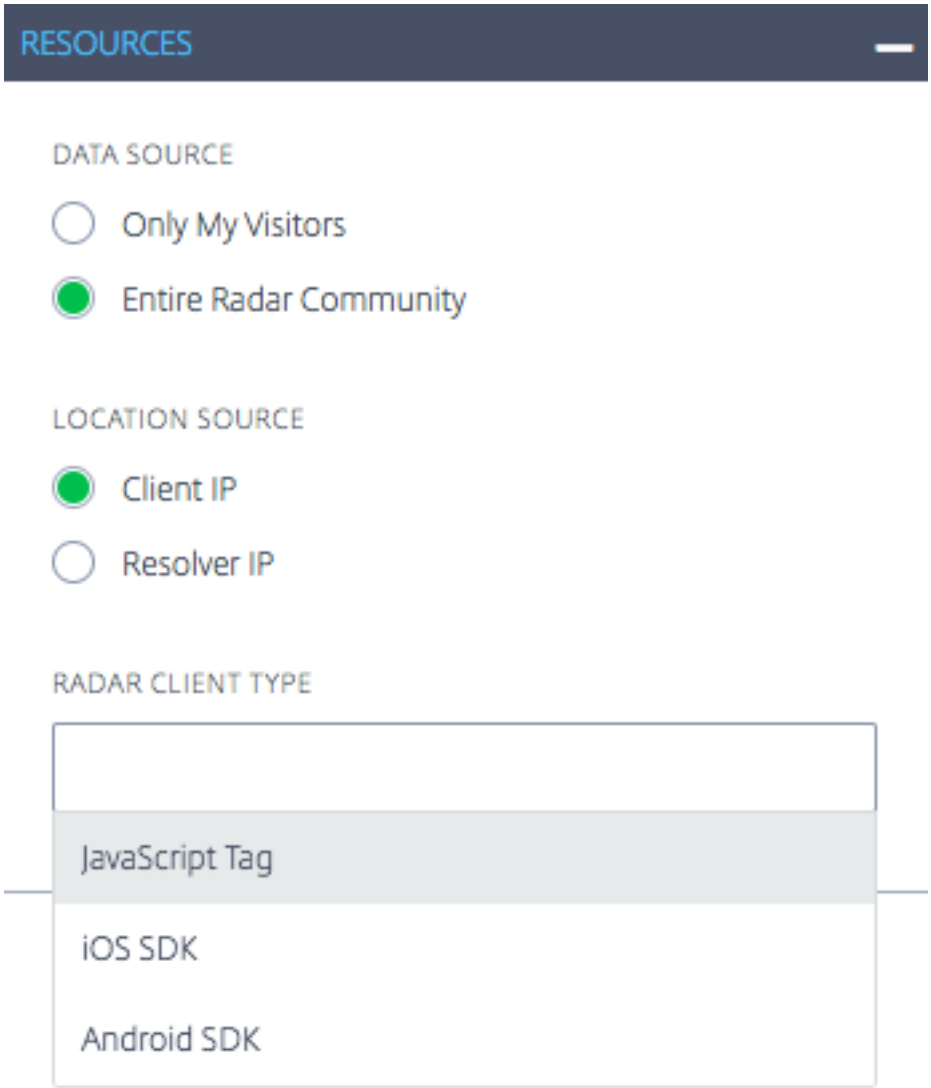
Filtre : Plateforme et emplacement

Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les plus courantes sont les suivantes :

- **Plateforme** : sélectionnez une ou plusieurs plateformes (fournisseur) à inclure.
- **Continent** : sélectionnez un ou plusieurs continents à inclure.
- **Pays** : sélectionnez un ou plusieurs pays à inclure.
- **Région** : sélectionnez une ou plusieurs régions géographiques (le cas échéant) à inclure.
- **État** : sélectionnez un ou plusieurs états géographiques (le cas échéant) à inclure.
- **Réseau** : sélectionnez un ou plusieurs réseaux (ASN) à inclure.

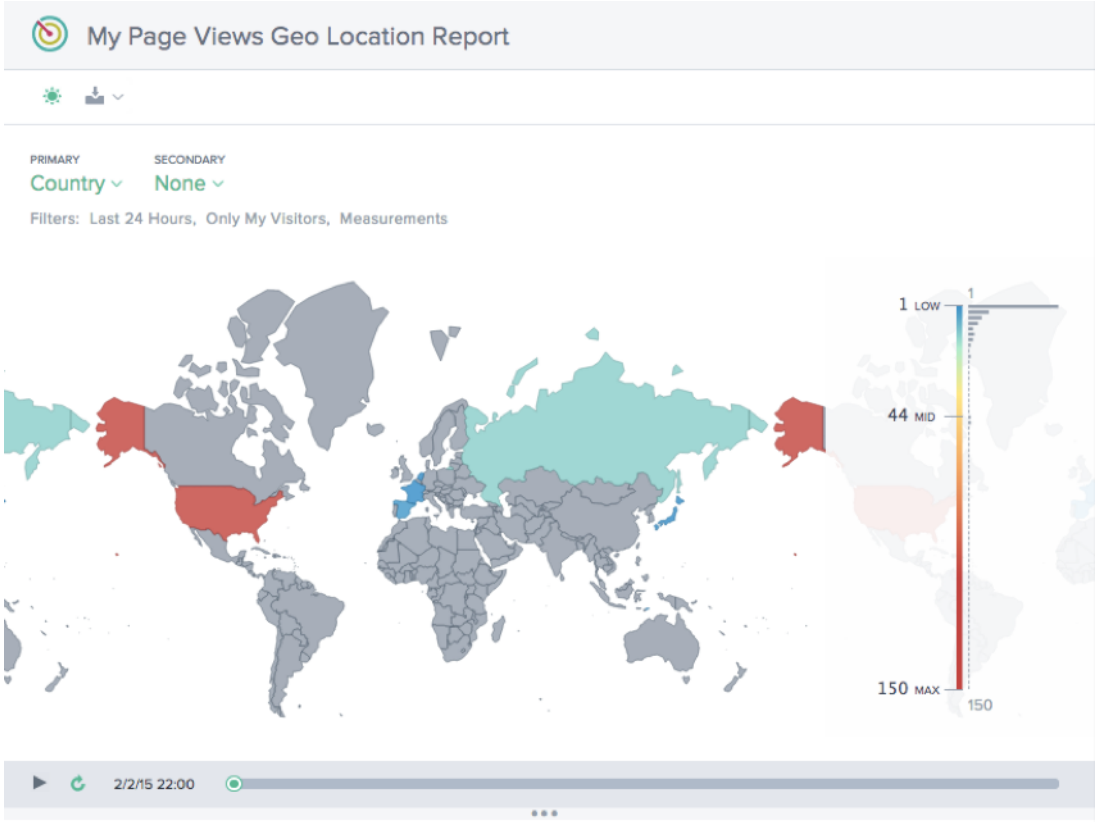
Filtre : Ressources

- **Source de données** - Incluez des données provenant de l'ensemble de la communauté Radar ou uniquement des visiteurs de votre site.
- **Source de localisation** - Sélectionnez l'adresse IP du client ou l'adresse IP du résolveur comme source de localisation.
- **Type de client Radar** : sélectionnez le type de client Radar sous la forme d'une balise JavaScript, d'un SDK iOS ou d'un SDK Android.



Rapport de géolocalisation de mes pages vues

Ce rapport indique le nombre de pages vues pour chaque pays. Cette vue cartographique peut être visualisée au fil du temps (en fonction de la plage de temps choisie pour le rapport) en sélectionnant le bouton « **Play** » en bas du graphique.



Rapport sur le rendement

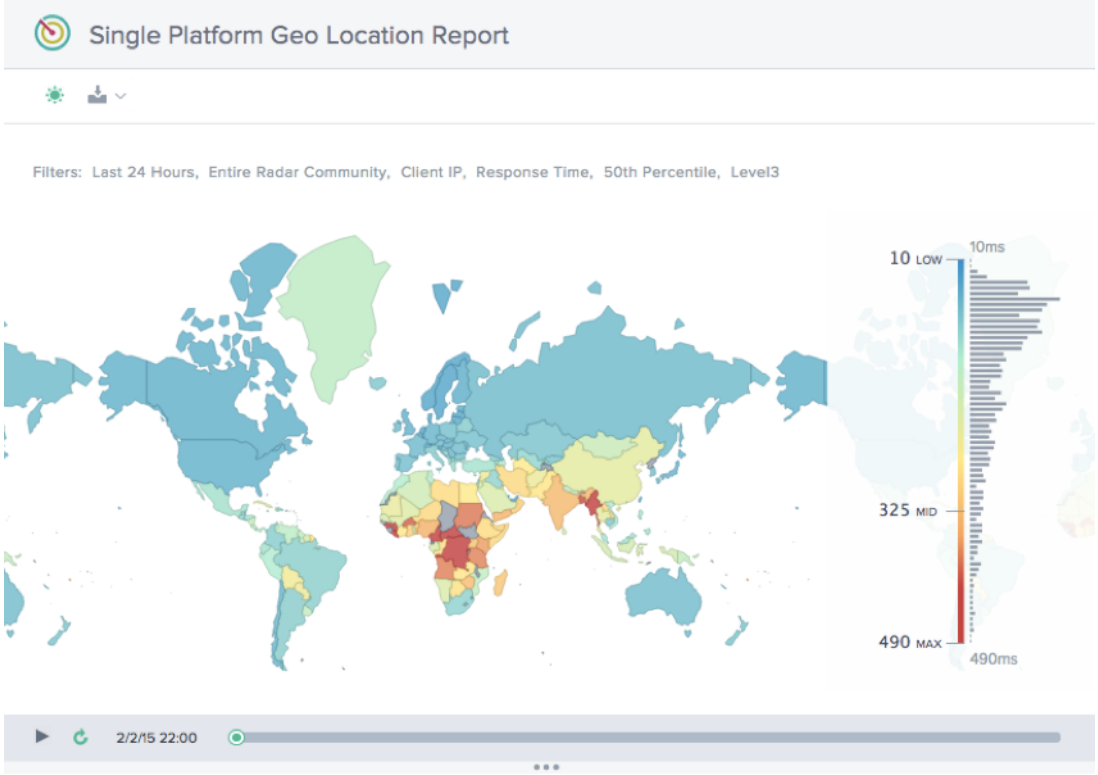
Ce rapport montre l'évolution des performances pour chacune des plateformes définies.

Rapport de distribution statistique

Ce rapport présente la ventilation statistique pour chacune des plateformes définies pour le compte.

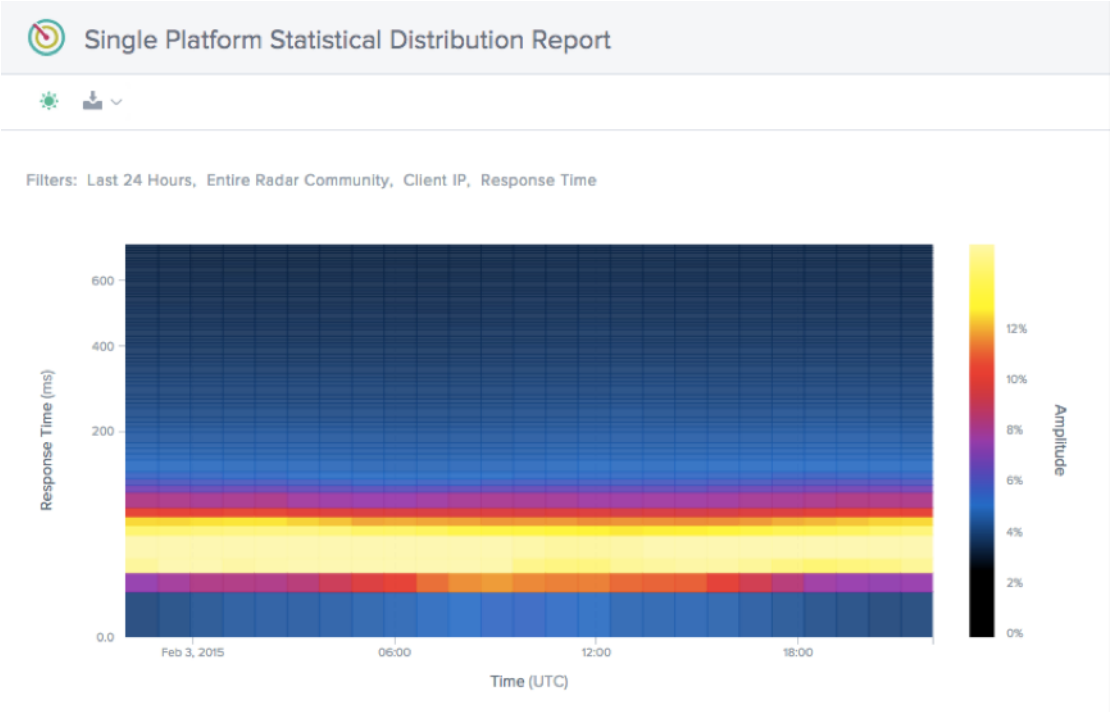
Rapport de géolocalisation sur une plateforme unique

Ce rapport montre la distribution du trafic radar par pays au fil du temps pour une seule plateforme à la fois.



Rapport sur la distribution statistique d'une plate-forme unique

Ce rapport montre la distribution du trafic radar dans le temps par temps de réponse.

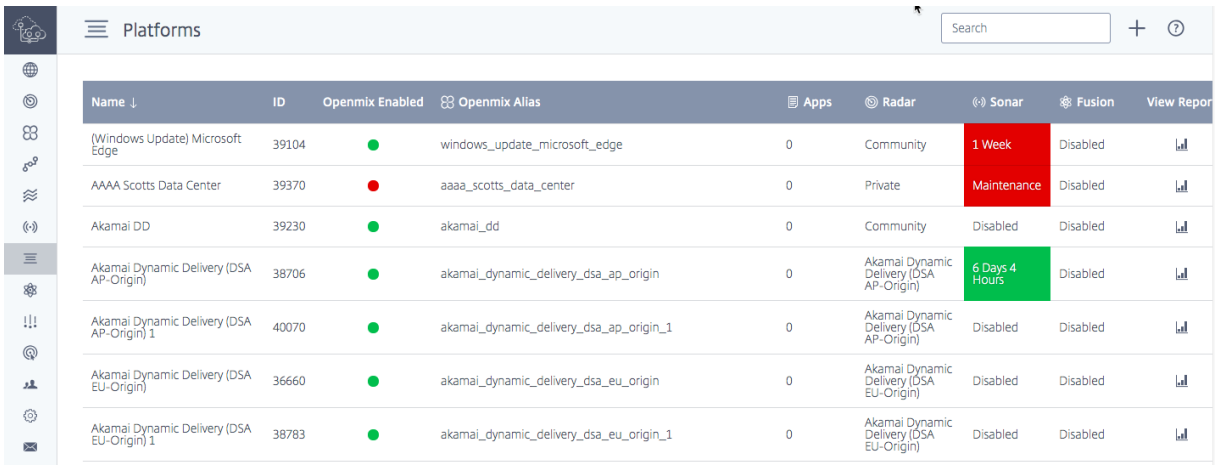


Plates-formes

June 4, 2021

La page **Plates-formes** est l'endroit où le client spécifie les CDN, les clouds, les centres de données ou d'autres points de terminaison qui doivent être surveillés et utilisés avec Openmix. Une plate-forme doit être configurée pour chaque point de terminaison de routage sur lequel vous souhaitez établir un rapport. Le plus souvent, une plate-forme représente un CDN, une région cloud ou une instance individuelle, si elle utilise Openmix pour GSLB.

En cliquant sur cet élément de menu, le client est présenté avec l'écran suivant.



Cet écran affiche une liste complète de toutes les plates-formes configurées pour les rapports, les mesures radar ou les services Sonar et Fusion.

Le tableau indique :

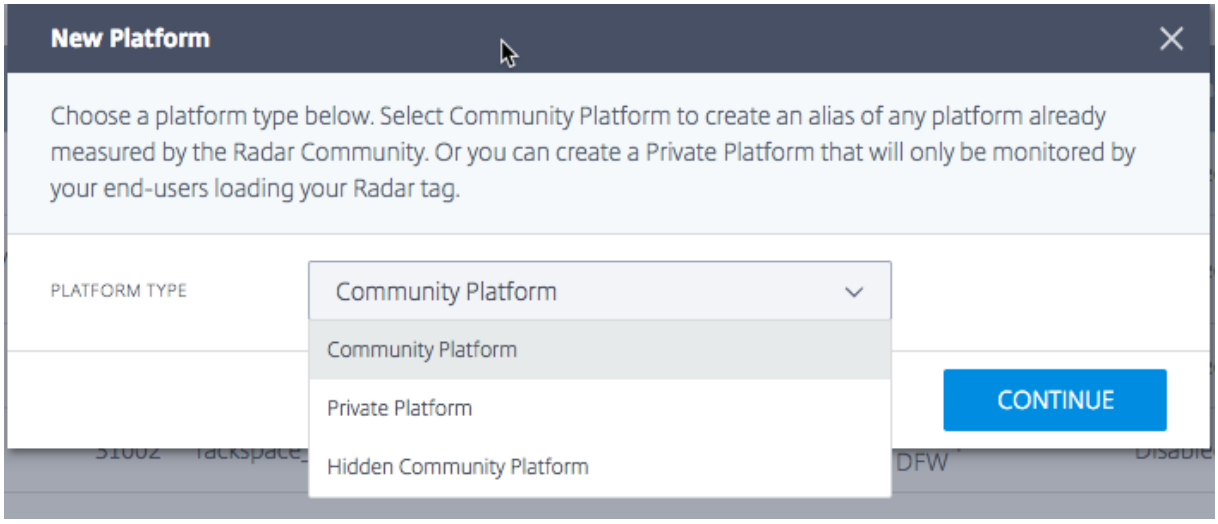
En-tête	Description
Nom	Nom défini par l'utilisateur de la plate-forme.
ID	ID généré pour la plate-forme, utile pour l'accès aux API et le reporting.
Alias Openmix	Alias avec lequel faire référence à la plate-forme à partir des applications Openmix.
Applications	Le nombre d'applications Openmix utilisant la plate-forme.
Radar	Indique si la plate-forme est configurée pour utiliser des mesures Radar communautaires ou privées.
Sonar	Indique si le Sonar est activé sur cette plateforme.
Fusion	Indique si Fusion est activée sur cette plateforme.

Création d'une plateforme

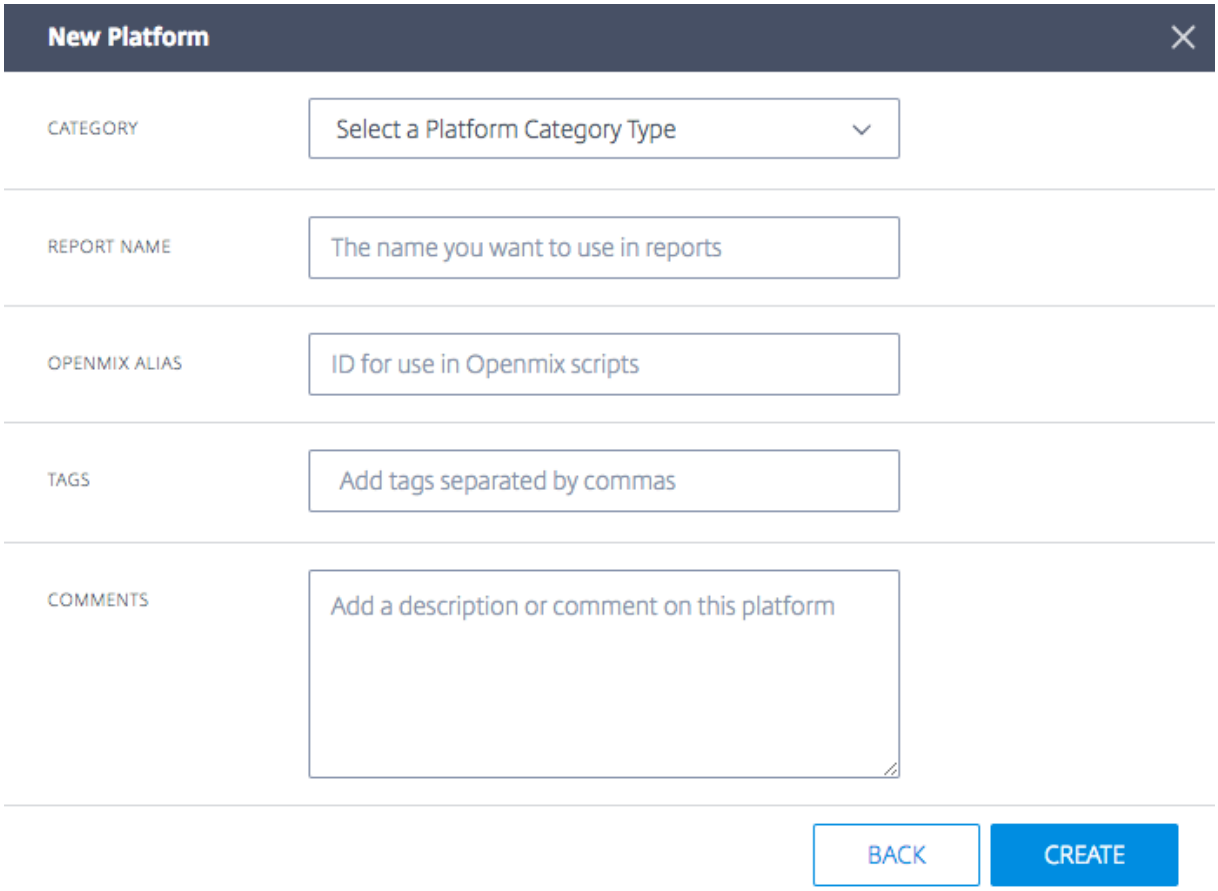
Pour ajouter une plateforme, cliquez sur le **bouton+** en haut de la page Plateformes.

Nouvelles plates-formes

Une fois que vous avez cliqué sur **Ajouter des plates-formes**, vous voyez la page suivante où vous pouvez sélectionner le type de plate-forme que vous souhaitez configurer.



Une fois que vous avez sélectionné le **type de plate-forme**, vous pouvez fournir un nom à la plate-forme qui sera utilisé pour afficher des informations et utilisé dans d'autres services fournis par ITM, tels que Openmix.



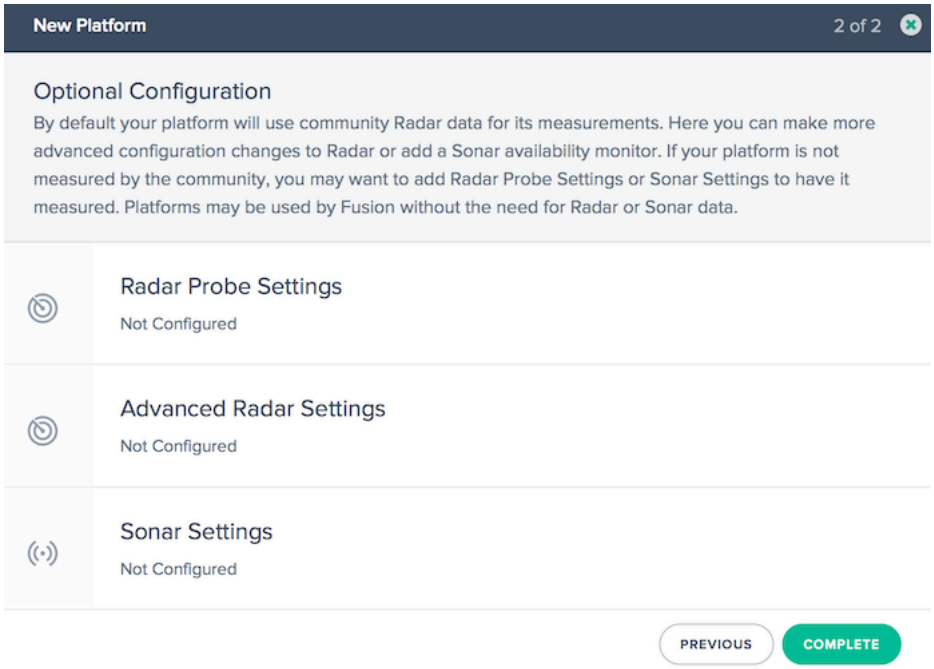
Dans **Paramètres de la plate-forme**, entrez les informations suivantes :

Élément de saisie	Description
Catégorie	Type de service que représente la plate-forme. Les plates-formes sont gérées différemment dans Radar et Openmix, selon le type. Les catégories de plateformes disponibles sont : Cloud Computing, Dynamic Content, Delivery Networks, Cloud Storage, Secure Object Delivery et Managed DNS. Pour les plates-formes **privées**, une autre catégorie disponible est **Data Center** . Remarque : Toutes les GSLB importées sont créées en tant que centres de données.
Plate-forme	Sélectionnez la plate-forme que vous souhaitez tester, par exemple Akamai, Amazon, Azure, etc.
Nom du rapport	Nom de la plate-forme utilisée dans l'affichage et le reporting.

Élément de saisie	Description
Alias Openmix	L'alias utilisé par les applications Openmix pour identifier la plate-forme.
Balises	Les balises peuvent être assignées aux plates-formes afin qu'elles puissent être organisées selon les besoins.

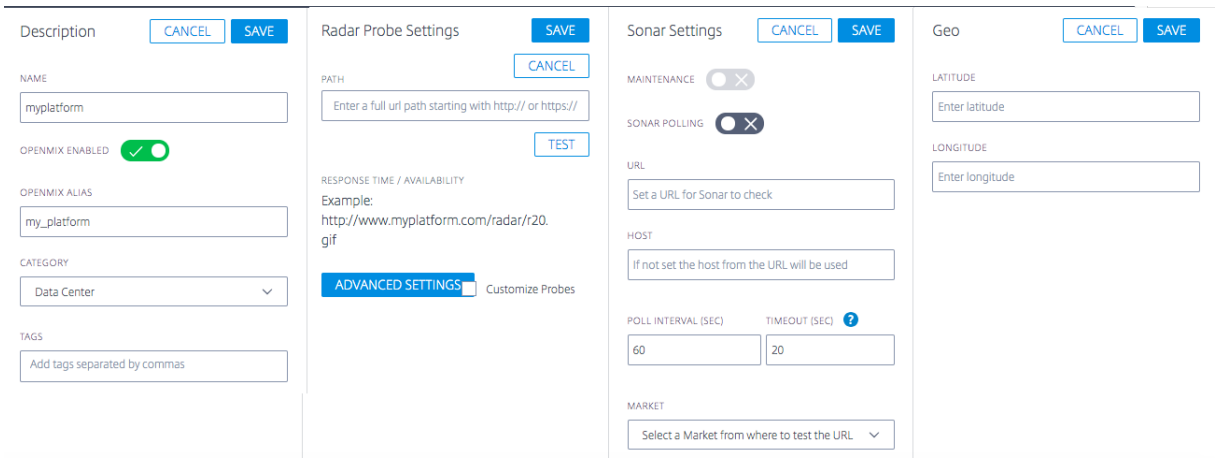
Lorsque vous sélectionnez une plate-forme existante, les champs **Nom du rapport et Alias Openmix** sont renseignés. Vous pouvez laisser ces champs avec les valeurs par défaut ou les modifier comme vous le souhaitez.

Cliquez sur **Suivant pour passer** à la configuration facultative. Lorsque vous avez terminé avec la configuration facultative, cliquez sur **Terminer** pour ajouter la plate-forme.



Modification d'une plate-forme

La modification d'une plate-forme est aussi simple que de cliquer sur la ligne de la plate-forme dans le tableau et de cliquer sur le bouton **Modifier** .



Une fois que vous avez modifié la configuration, cliquez simplement sur **Enregistrer**, comme vous le feriez avec une nouvelle application et cela vous ramènera à l'écran des plates-formes avec vos modifications enregistrées.

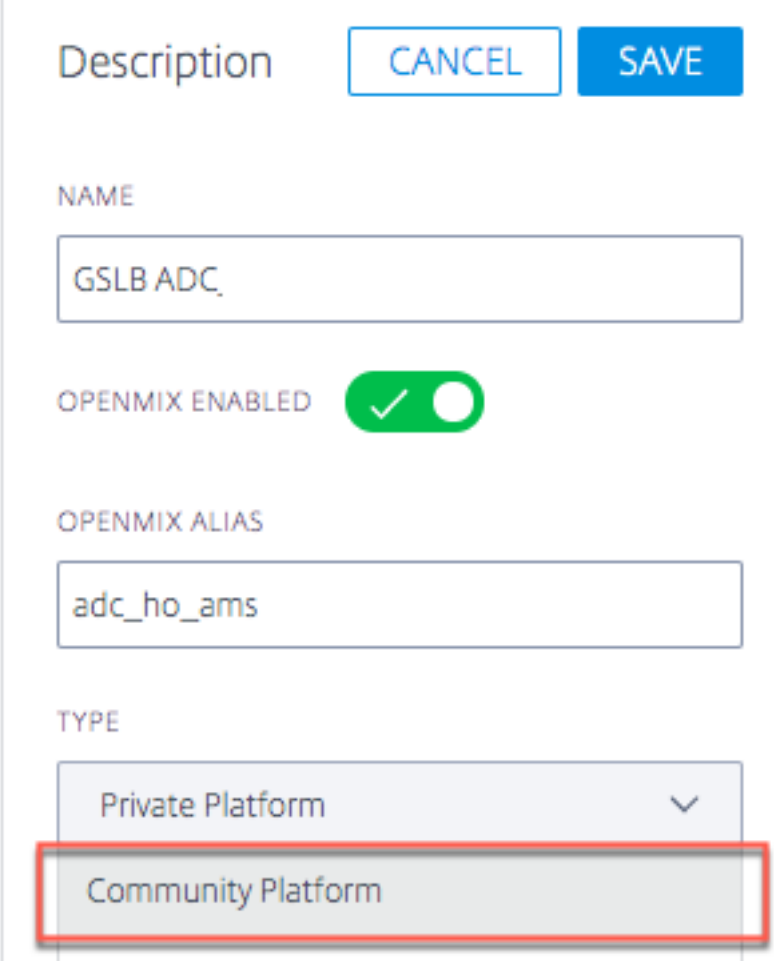
Modifier le type de plate-forme

Cette fonctionnalité est utile pour les clients dont les plates-formes privées sont hébergées dans un centre de données public ou une région cloud qui est mesurée par la communauté Radar (AWS, par exemple) et qui souhaitent hériter des données Radar de cette plate-forme communautaire. Par exemple, lorsque les clients importent des GSLB dans le portail ITM, ils sont importés en tant que centres de données privés, mais peuvent être situés dans une région de cloud public. Pour hériter des données Radar de la plate-forme communautaire, les clients peuvent modifier les paramètres actuels de la plate-forme privée ou GSLB pour référencer la plate-forme communautaire à la place.

Pour changer le type de plate-forme, telle qu'un GSLB ou un centre de données privé, en une plate-forme communautaire publique (ou de la communauté à la plate-forme privée si nécessaire), procédez comme suit.

1. Cliquez sur la ligne de plate-forme dans le tableau **Plates-formes** .
2. Dans la section **Paramètres de la plate-forme**, cliquez sur le bouton **Modifier** .
3. Accédez à **Type**. Sélectionnez **Community Platform** dans la liste si vous souhaitez changer votre plate-forme privée en plate-forme communautaire.
4. Aller à **Catégorie**. Choisissez une catégorie de plateforme dans la liste.
5. Allez sur **Plateforme**. Sélectionnez la plate-forme à modifier dans la liste déroulante **Plate-forme** .
6. Cliquez sur **Enregistrer** en haut à droite de la section **Paramètres de la plate-forme** . Vous verrez un message de confirmation vous indiquant que les paramètres de la sonde Radar pour votre plate-forme privée seront supprimés et remplacés par les paramètres de la plateforme communautaire.

7. Cliquez sur **Confirmer**.

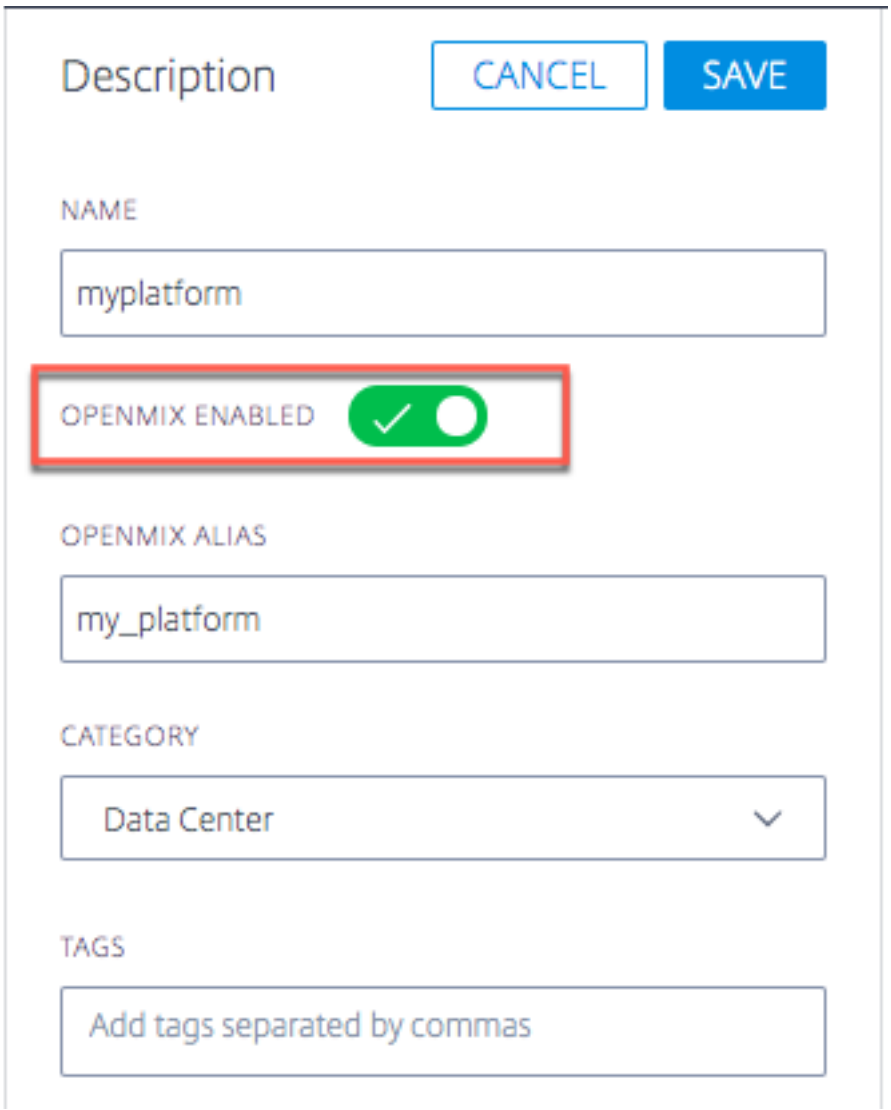


Remarque : Si vous décidez de revenir de la communauté à votre plate-forme privée, vous devrez reconfigurer les paramètres de votre sonde Radar.

Activer la plate-forme pour Openmix

Une Plateforme peut être activée ou désactivée pour Openmix en activant ou désactivant le bouton **Openmix Enabled** dans **Paramètres de la Plateforme** .

- Cliquez sur le **bouton Modifier** dans les **paramètres de la plate-forme**
- Sélectionnez le bouton pour **Openmix Enabled** pour l'activer.



Si une plate-forme particulière est désactivée pour Openmix, cette plate-forme ne sera plus prise en compte dans les décisions Openmix. Cela signifie qu'un score Radar ne sera pas généré pour cette plate-forme particulière.

Dans les applications Quickstart, la plate-forme (si elle est désactivée dans l'interface utilisateur) ne s'affiche pas en tant qu'option à sélectionner.

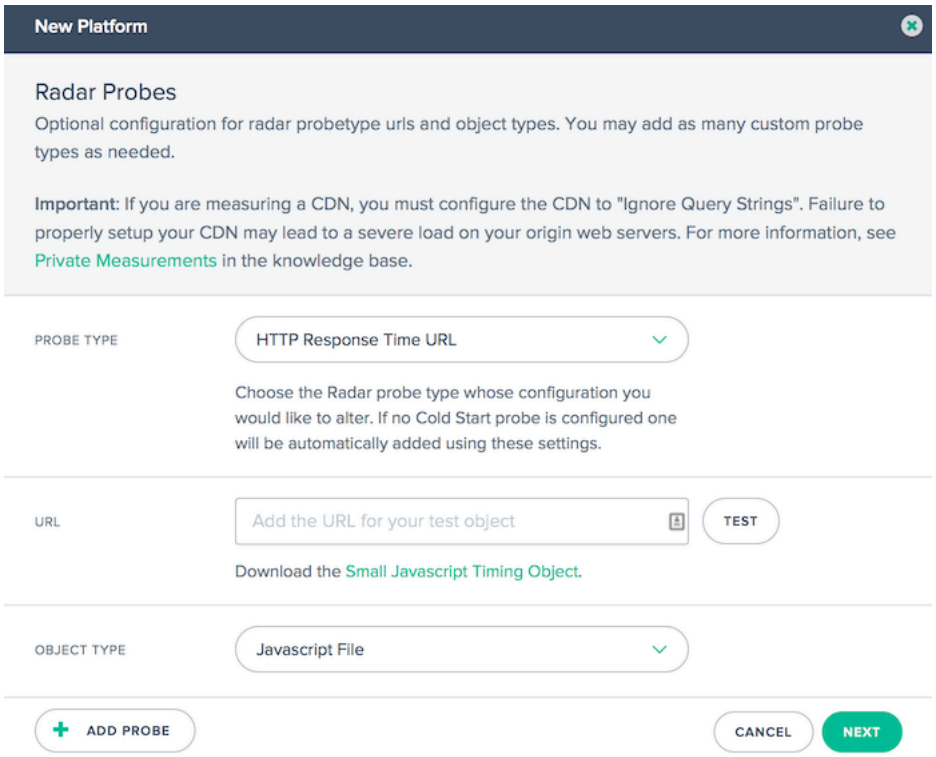
Cependant, pour les applications personnalisées, si la plate-forme est codée en dur dans la logique de l'application, il est possible qu'elle soit récupérée (même si cette plate-forme est désactivée pour Openmix dans l'interface utilisateur). Pour éviter que cela ne se produise, l'application personnalisée doit être écrite de telle sorte qu'elle inclut toujours une logique pour récupérer le score Radar. Lorsque la plate-forme est désactivée pour Openmix (dans l'interface utilisateur), il n'y aura plus de score Radar généré pour elle, et donc il sera automatiquement ignoré par l'application.

Cela peut être utilisé comme interrupteur marche/arrêt opérationnel s'il y a un problème avec une

plate-forme particulière et que le client souhaite la retirer de toutes les applications pendant ce problème.

Paramètres des sondes radar

Des sondes radar peuvent être spécifiées pour chaque plate-forme. Habituellement, cela n'est nécessaire que si vous configurez une plate-forme privée pour la surveillance Radar. Les plateformes publiques fournissent des données recueillies par la communauté et peuvent être utilisées pour la plupart des utilisations.



Il existe une sonde pour chaque type de données collectées, telles que : Temps de réponse HTTPS, Débit HTTP, Démarrage à froid HTTPS (pour la disponibilité), etc. La plupart des configurations Radar ont des sondes pour au moins Démarrage à froid et Temps de réponse, avec Débit dans certains cas.

Chaque sonde possède les paramètres suivants :

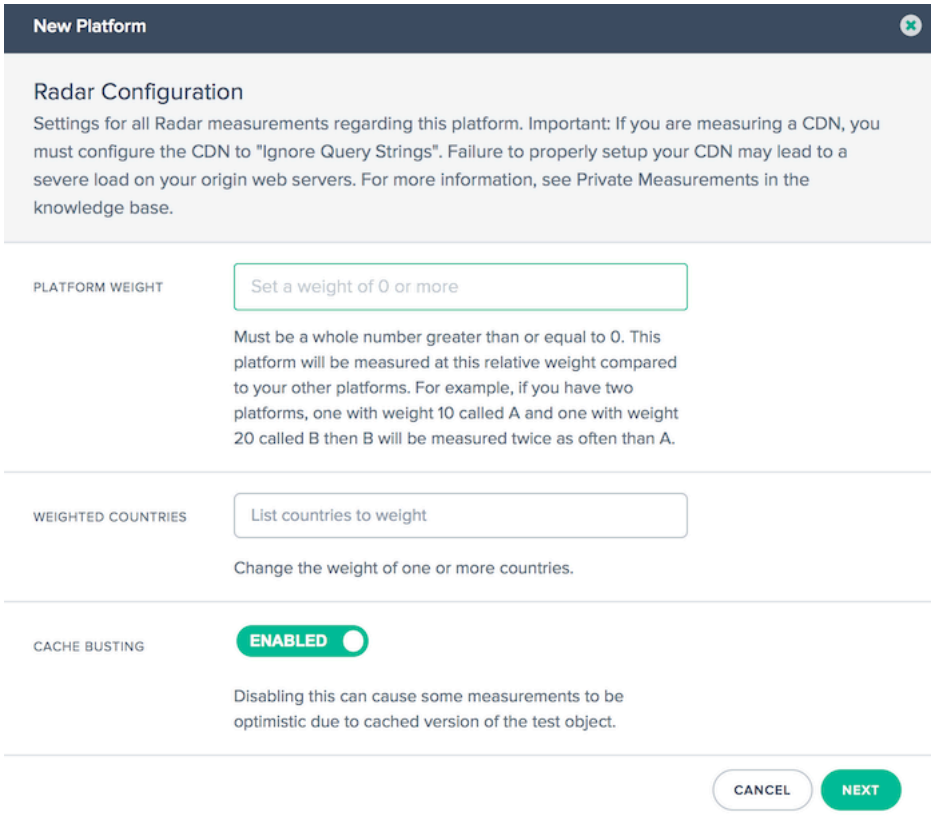
Élément de saisie	Description
Type de sonde	Valeur pour laquelle les données doivent être déclarées. Il existe des sondes distinctes pour chaque protocole (HTTP/HTTPS) et le type de données qui seront collectées (démarrage à froid, aller-retour, débit, etc.).

Élément de saisie	Description
URL	URL de l'objet de sonde.
Type d'objet	Type de fichier utilisé pour prendre la mesure. Dans la plupart des cas, vous voulez télécharger le « Timing Object » à partir du lien dans la boîte de dialogue et choisir « Image File ». Pour les sondes des services DSA, vous choisirez normalement « page Web (dynamique) ».

Cliquez sur **Ajouter une sonde** en bas à gauche de la boîte de dialogue et ajoutez des informations pour chaque sonde. Cliquez sur **Enregistrer** après avoir saisi toutes les sondes.

Paramètres radar avancés

Vous pouvez contrôler le comportement des vérifications Radar pour la plate-forme. Ceux-ci ne doivent être modifiés que si vous comprenez l'impact sur votre application Openmix.



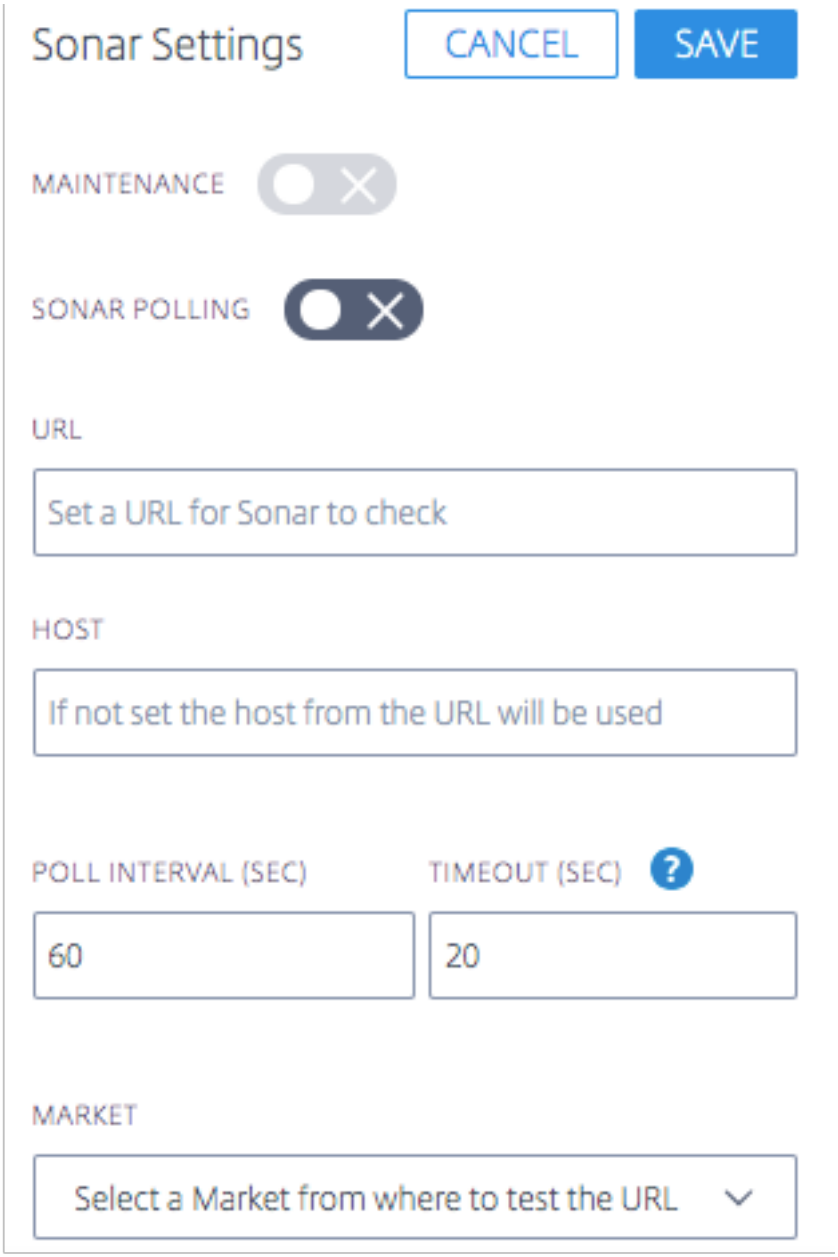
Les options suivantes sont disponibles :

Élément de saisie	Description	Mode par défaut
Poids de la plateforme	Radar utilise un système de pondération pour aider les clients à prioriser leurs tests personnalisés, plus le nombre est élevé la priorité de ce test privé est élevée. Généralement, cela est utilisé lorsque vous avez plusieurs tests personnalisés, si vous configurez un seul, laissez-le par défaut.	10, pas de pondération
Pays pondérés	Vous pouvez remplacer le poids de la plate-forme pour certains pays en saisissant les pays souhaités. Le pays est spécifié à l'aide des codes pays ISO.	0, pas de pondération
Poids Pays	Si des pays pondérés sont spécifiés, ce poids est appliqué aux pays et remplacera le poids de la plate-forme. Si le poids est défini sur zéro, la plate-forme ne sera pas mesurée dans les pays spécifiés.	
Busting du cache	La désactivation de ce paramètre peut entraîner l'optimisme de certaines mesures en raison des versions mises en cache de l'objet de test signalées.	Activé

Paramètres du sonar

Sonar est un service de vérification de la vitalité qui peut être utilisé pour surveiller la disponibilité des services Web. Sonar fonctionne en effectuant des requêtes HTTP ou HTTPS à partir de plusieurs points de présence dans le monde entier vers une URL que vous spécifiez.

Sonar est activé dans la configuration de la plate-forme. Veuillez consulter le guide de l'Sonarutilisateur pour plus d'informations.



Plateforme Geo

La plate-forme **Geo** est un emplacement (latitude et longitude) assigné à une plate-forme. Les informations géographiques vous permettent de placer des plates-formes avec précision sur la carte dans l'outil **Visualizer** .

Remarque : La zone **géographiques**'applique uniquement aux plates-formes qui ont un emplacement physique tel que les centres de données ou les régions cloud.

Pour les plates-formes privées

Par défaut, aucun emplacement **géographique** n'est attribué aux plates-formes privées. Lorsqu'un utilisateur crée une plate-forme privée et configure une sonde **Radar**, nous utilisons la sonde pour la géolocaliser. Cela signifie que lorsque vous ajoutez une URL aux paramètres **Radar**, nous géo localisons l'adresse IP que nous récupérons, et l'assignons comme **géo** pour la plate-forme privée. Vous pouvez modifier cette **zone géographique** si nécessaire. Vous pouvez également affecter manuellement un **géo** à votre plate-forme sans vous fier au chemin d'URL Radar.

Une fois le **Geo** défini, il ne se réinitialise pas par lui-même. Même si vous modifiez l'URL **Radar**, cela ne change pas le **Geo** de la plate-forme. Vous devez modifier le **Géo** manuellement pour le modifier.

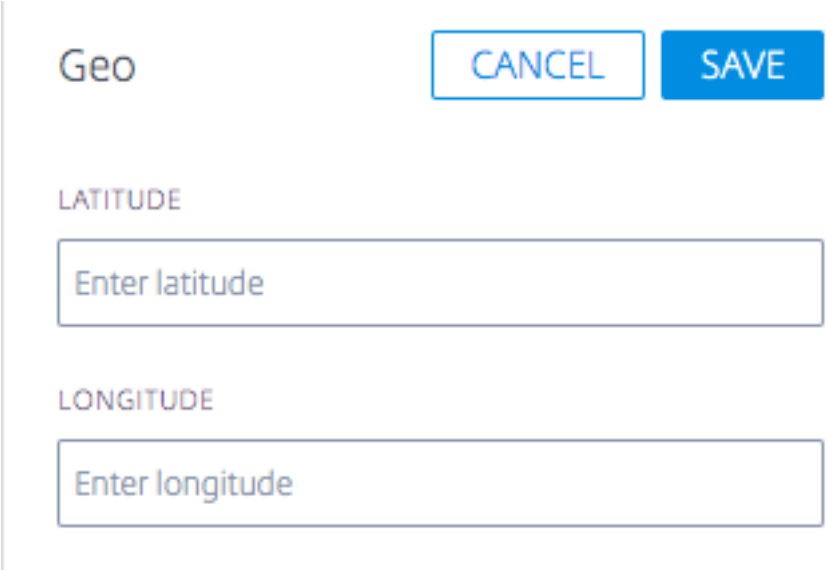
Note : Toutes les plates-formes privées ne reçoivent pas une valeur **Geo**attribuée. Les géos ne s'appliquent qu'aux plates-formes qui ont un seul emplacement physique.

Pour les plates-formes importées

Si vous importez une plate-forme via une configuration GSLB ou F5, nous géo localisons l'adresse IP publique à partir de cette configuration et l'utilisons comme **géo** de la plate-forme.

Pour les plates-formes communautaires

Lorsqu'un client ajoute une plate-forme communautaire à son compte, cette plate-forme hérite par défaut de la géo d'origine de la **plate-forme communautaire**. Cependant, le géo de cette plateforme peut être modifié par le client. Normalement, un client ne doit pas avoir à le modifier. Toutefois, si un client choisit de modifier cette zone **géographique** et entre une nouvelle latitude et une nouvelle longitude, le paramètre du client (pour la plate-forme communautaire) remplacera la zone **géographique** d'origine de la **plate-forme communautaire** .



Openmix

September 13, 2023

Vue d'ensemble

NetScaler Intelligent Traffic Management (ITM) Openmix propose une approche révolutionnaire de la gestion globale du trafic et de l'équilibrage global de la charge des serveurs (GTM/GSLB). Pour la gestion traditionnelle du trafic mondial, ITM fournit une approche basée sur le DNS pour l'équilibrage de charge. ITM utilise CNAME DNS ou des enregistrements dans lesquels les réponses DNS sont modifiées en temps réel en fonction de la logique métier requise. Openmix peut être intégré au flux de production et à la diffusion vidéo de plusieurs manières.

Les outils et services GTM ou GSLB s'appuient sur des moteurs de règles statiques propriétaires, inextensibles et pour définir et contrôler un ensemble restreint de politiques fixes pour le basculement, le round-robin et le ciblage géographique. La mission de NetScaler ITM est de mettre en œuvre des stratégies cloud de nouvelle génération basées sur des flux de données en temps réel. La plate-forme Openmix fournit un moyen très robuste d'ingérer des données en temps réel provenant de diverses sources. Il expose les métadonnées en tant que « variables » d'environnement qui peuvent être évaluées à chaque demande.

Openmix : Avantages clés

- Éliminer les dépendances d'un seul fournisseur et garantir une disponibilité à 100 %

- Contrôlez les compromis prix/performances et éliminez les maux de tête associés au multisourcing
- Supprimez les incertitudes liées aux outils de performance existants et déchargez le trafic de manière sélective et stratégique
- Appliquer des fournisseurs spécifiques pour cibler des marchés individuels

Comment fonctionne Openmix

Les clients se connectent au portail ITM Citrix pour déployer leur première application. Une bibliothèque d'exemples d'applications est disponible pour vous aider à démarrer et un assistant étape par étape permet de créer des applications avec la logique de routage la plus courante. Les applications ITM Openmix peuvent prendre en charge deux protocoles pour diriger le trafic : DNS ou HTTP.

Contrôle défini par l'application

La plateforme Openmix à la demande et distribuée dans le monde entier rapproche la prise de décision GTM/GSLB de votre public d'applications. Chaque hôte peut avoir sa propre application Openmix personnalisée qui prend en compte les métriques et variables actuelles qui fournissent la meilleure optimisation pour toute demande de routage.

Les scripts Openmix sont programmés en JavaScript, un langage accessible à la plupart des programmeurs Web et des administrateurs réseau. Bien que cette approche basée sur des scripts soit l'endroit où pratiquement n'importe quelle logique métier peut être mise en œuvre avec une complexité de codage minimale pour servir de base à des politiques de gestion du trafic réellement dynamiques. Grâce à la nature collaborative de notre communauté de clients, ITM fournit également des « applications de démarrage rapide » qui sont des applications standard qui ne nécessitent pas de code.

Quand utiliser les services HTTP ou DNS

ITM Openmix permet une large gamme d'optimisation de la diffusion de contenu. La méthode que vous utilisez pour activer Openmix dépend en grande partie des spécificités de votre cas d'utilisation. La méthode DNS est facile à mettre en œuvre, généralement transparente pour les clients et utilisable dans une grande variété de contenus. Cependant, la possibilité de changer de fournisseur est limitée par la durée de vie définie sur la réponse DNS et certains contenus ne peuvent pas être commutés vers un autre fournisseur en cours de diffusion. HTTP offre une plus grande flexibilité d'intégration et des décisions d'optimisation peuvent être prises lorsqu'il est optimal pour le client. Cette plus grande flexibilité nécessite plus de travail à intégrer à un CMS ou à un client.

Le tableau suivant résume le cas d'utilisation des interfaces DNS et HTTP par le client.

	Openmix DNS	Openmix Web Services (HTTP)
Typical Use	Webpage Optimization Mobile App Optimization Player or Game Download Initial Video/Game Request Mid-Stream Requests (TTL expiration)	Initial Video Request Initial Game Server Selection Mid-Stream Requests Mid-Play Gaming Client Requests
Radar Tag / SDK & Fusion Data Collection	Cedexis Radar RUM CDN & Cloud Performance Monitoring CDN & Cloud Costs data, 3rd Party Monitoring Metrics: Player, Server or App Health, Synthetic Process Monitoring, etc.	
Client Data Collection	Video Player Performance Metrics	
Cedexis Billing	Per Millions of DNS Queries	Per Millions of HTTP Requests

Openmix : DNS

Délégation CNAME L'intégration la plus simple pour les clients ITM consiste à utiliser la délégation CNAME DNS. La délégation CNAME fonctionne en demandant au client de pointer son nom d'hôte face à l'utilisateur final (dans l'exemple suivant `www.acme.com`) vers un nom d'hôte ITM

```
www.acme.com  600  IN  CNAME  2-02-123d-000d.cdx.cedexis.net.
<!--NeedCopy-->
```

Lorsqu'il reçoit une demande DNS d'un utilisateur final, le système ITM prend une décision en temps réel. La décision est basée sur les données Radar, la logique métier de l'application et toute information de tiers. Cette décision est articulée soit comme un autre enregistrement CNAME (dans notre exemple ci-dessous acme.cdn1.net), soit comme un enregistrement A tel que 111.222.111.222.

En fournissant un enregistrement CNAME, ITM « pointe » l'utilisateur final vers le CDN, le Cloud ou le centre de données de son choix. Dirige l'utilisateur final pour qu'il utilise ce fournisseur plutôt qu'un autre.

```
2-02-123d-000d.cdx.cedexis.net.  19  IN  CNAME acme.cdn1.net.
<!--NeedCopy-->
```

Une fois le CDN ou le CNAME Cloud fourni, la machine de l'utilisateur final poursuit la chaîne de résolution. Il demande un serveur de noms CDN, jusqu'à ce qu'une adresse IP du nœud ou du serveur soit reçue. Où sur le processus de téléchargement du contenu commence.
Si un enregistrement est fourni dans le cadre de la logique, la machine de l'utilisateur final reçoit l'adresse IP. Il se connecte directement au serveur et lance le téléchargement du contenu.


```
acme.cdn1.net.  132  IN  A  111.222.222.111
<!--NeedCopy-->
```

La délégation de zone En outre, la délégation de zone DNS faisant autorité est une option pour implémenter Openmix. Le client crée une zone DNS et délègue à une zone Predictive DNS créée dans le portail ITM. Créez un nom d'hôte dans la zone déléguée. Configurez-le pour utiliser une application Openmix ou un enregistrement DNS prédictif dynamique afin de générer une réponse.
L'avantage de cette option est qu'il n'est pas nécessaire d'avoir une délégation CNAME entre le nom d'hôte et la réponse dynamique de la plate-forme ITM. En utilisant l'exemple précédent, `www.acme.com` le nom d'hôte est directement résolu à la valeur configurée pour le CDN, le Cloud ou le centre de données optimal.

```
www.acme.com. 19 IN CNAME acme.cdn1.net.
```

Les enregistrements A/AAAA peuvent également être utilisés à la place des CNAME, et le nom d'hôte est directement résolu en enregistrement de la destination optimale.

```
www.acme.com. 19 IN A 111.222.222.111
```

Incidences sur le DNS et le temps de vie Des facteurs tels que les valeurs Time To Live (TTL) sont soigneusement pris en compte avec un temps approprié pour le contenu et la manière dont la prise de décision doit être prise pour les utilisateurs. Dans la plupart des cas, ITM recommande une durée de vie de 20 secondes pour le contenu de la page et de l'objet. Pour le contenu vidéo, le consultant ITM travaille avec le client pour trouver l'équilibre le plus approprié en fonction de la longueur du morceau et de la méthode d'intégration.

Openmix : HTTP

Une alternative au DNS consiste à utiliser l'API HTTP. Openmix utilise des requêtes HTTP pour informer un client tel qu'un lecteur vidéo ou un CMS sur quelle plate-forme utiliser à tout moment.

```
http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision
< HTTP/1.1 200 OK
< Content-Type: application/json
< Date: Mon, 22 Apr 2015 20:25:24 GMT
< Connection: keep-alive
< Content-Length: 177
<
{

  "providers" : [
    {

    "provider" : "cdn2",
```



```
14      "host" : "foo.cdn2.net"
15       }
16   ,
17      {
18
19      "provider" : "cdn1",
20      "host" : "acme.cdn1.net"
21       }
22
23    ]
24   }
25
26 <!--NeedCopy-->
```

Le service HTTP Openmix utilise la même logique d'application que son homologue basé sur le DNS. Il inclut également quelques extensions supplémentaires, permettant d'affiner le profilage d'une machine cliente. Par exemple, avec HTTP Openmix, il est possible d'examiner les en-têtes de User-Agent String, X-Forwarded-For et Referer. Fournissez des remplacements d'IP à l'aide de paramètres de chaîne

Comme la charge utile pour HTTP Openmix est plus extensible que le DNS, il est également possible de fournir la sélection de décision CDN, cloud ou serveur de différentes manières. La plus courante jusqu'à présent a été une liste ordonnée de la plate-forme la plus préférée à la moins importante (comme ci-dessus). Une liste complète permet de fournir le rang de décision au CMS ou au client, tout en permettant d'utiliser des heuristiques internes pour choisir le fournisseur.

Intégration CMS

Certains clients préfèrent gérer la sélection des fournisseurs côté serveur plutôt que de mettre en œuvre la sélection des fournisseurs dans chaque client. L'API HTTP peut être utilisée pour récupérer une décision d'optimisation d'Openmix au moment de la demande du client. Il peut être utilisé pour remplir un fichier renvoyé par le CMS au client.

Par défaut, les points de terminaison HTTP Openmix utilisent l'adresse IP de l'appelant pour la géolocalisation et les critères de décision. Si vous appelez à partir d'un CMS ou d'un autre système situé entre le client de l'utilisateur final et Openmix, vous pouvez spécifier IP comme paramètre à utiliser dans la décision.

```
1 http://hopx.cedexis.com/zones/1/customers/0/apps/1/decision?ip=1.2.3.4
2 < HTTP/1.1 200 OK
3 < Content-Type: application/json
4 < Date: Mon, 22 Apr 2015 20:25:24 GMT
5 < Connection: keep-alive
6 < Content-Length: 177
7 <
8 {
9
```



```
10    "providers" : [
11      {
12
13      "provider" : "cd1",
14      "host" : "acme.cdn1.net"
15       }
16  ,
17      {
18
19      "provider" : "cdn2",
20      "host" : "foo.cdn2.net"
21       }
22
23   ]
24  }
25
26 <!--NeedCopy-->
```

Cette méthode vous permet d'utiliser une intégration CMS pour récupérer les décisions d'Openmix. Vous pouvez également bénéficier des avantages de l'optimisation des itinéraires géographiques et ISP pour l'utilisateur final. Le nom d'hôte renvoyé par Openmix est ensuite empaqueté dans la réponse, tel qu'un fichier manifeste vidéo, et renvoyé par le CMS au client. Le client utilise la décision optimisée sans nécessiter aucune modification pour prendre en charge l'optimisation Openmix.

Applications Openmix

Les applications Openmix Quickstart sont des applications d'équilibrage de charge et de gestion du trafic. Ces applications fournissent un routage du trafic en temps réel vers le meilleur fournisseur sur la base d'un ensemble de règles.

Les demandes sont traitées pour chaque demande adressée à Openmix et une décision de routage est prise en fonction de la logique spécifiée. Un client peut avoir une application pour le contenu à forte valeur commerciale et une autre pour le contenu de moindre valeur. Ces demandes sont acheminées séparément.

Lorsque vous appelez une application, une seule demande est envoyée à l'un des équilibreurs de charge de Citrix. Pour le DNS, il s'agit d'une requête DNS unique adressée aux équilibreurs de charge DNS. Pour HTTP, il s'agit d'une requête GET ou HEAD adressée au point de terminaison HTTP Openmix.

Les applications suivantes sont actuellement disponibles via le portail de gestion intelligente du trafic NetScaler.

- Routage statique
- Basculement
- Round Robin

- Temps d'aller-retour optimal (ORTT)
- Débit
- Proximité statique

Les applications JavaScript personnalisées Openmix sont utilisées par des serveurs Openmix spécialisés pour répondre aux requêtes DNS ou HTTP en fonction de la logique des scripts. Le déploiement des scripts se fait via le portail client où l'application est configurée et publiée. Pour plus d'informations sur la possibilité de créer vos propres scripts JavaScript, consultez les informations de notre Developer Exchange.

Avant de procéder à la configuration des applications, il est important de comprendre les concepts suivants :

Seuil de disponibilité

Le seuil de disponibilité est le score de disponibilité minimum qu'une plate-forme doit atteindre pour être prise en compte pour le routage. Le seuil de disponibilité minimum par défaut pour toutes les applications est de 80 %. Cependant, vous pouvez modifier ce pourcentage et le définir sur une valeur adaptée à votre emplacement, à la disponibilité et à la fiabilité de votre réseau.

Remarque : Si aucune plate-forme n'atteint ce seuil de disponibilité minimum (la valeur par défaut de 80 %, ou la valeur que vous définissez), le routage aléatoire est effectué pour les applications Round Robin, ORTT et Throughput.

Fallback

La réponse de secours est renvoyée si l'application Openmix ne s'exécute pas correctement pour quelque raison que ce soit. Ou si Sonar confirme qu'aucune plateforme n'est disponible. Par conséquent, un enregistrement CNAME/A/AAAA de secours valide ou une adresse IP (ou un chemin en HTTP) doit être spécifié avec lequel Openmix peut répondre. Cet enregistrement d'URL ou CNAME de secours peut être destiné à une plate-forme préconfigurée dans Openmix.
La solution de secours peut également se produire dans les scénarios suivants :

- Lorsque vous passez d'une version de votre application à une autre, vous téléchargez et publiez un nouveau script. Il y a une brève période de secours de quelques millisecondes jusqu'à ce que le nouveau script s'initialise et que l'ancien soit supprimé.
- En cas de surcharge (ce qui arrive rarement), Openmix répond avec le CNAME/A/AAAA de secours puisque le repli compense la charge sur le service.

Pour le secours, vous devez entrer un nom d'hôte valide (enregistrement CNAME/A/AAAA) ou une adresse IP valide dans le DNS, et un URI valide (il peut être de la forme, `scheme:[//host[:port]][/path][?query][#fragment]`) en HTTP.

TTL

Dans Openmix, le DNS Time to Live (TTL) de l'application indique aux résolveurs combien de temps ils doivent conserver la décision avant de demander à nouveau Openmix.
La durée de vie est utilisée pour contrôler le volume de trafic généré par une application Openmix. Il contrôle également la sensibilité d'une application aux modifications des données sur lesquelles elle agit.
La durée de vie par défaut est de 20 secondes. Bien que vous puissiez modifier cette valeur, il n'est pas recommandé de le faire. Si vous réduisez la durée de vie, vous obtenez plus de volume et plus de requêtes DNS en temps réel. Cela peut entraîner des coûts supplémentaires et une baisse des performances, car les requêtes DNS prennent du temps sur le client. Par conséquent, il est préférable de ne pas modifier la valeur par défaut de TTL.

> **Remarque :** La durée de vie s'applique aux applications Quickstart, aux applications JS personnalisées si aucune durée de vie n'est spécifiée dans le code et à toutes les réponses de secours

Poids (utilisés pour Round Robin)

Vous pouvez attribuer des pondérations pour la priorisation et la sélection de chaque plateforme à l'échelle mondiale et/ou par marché ou par pays.

Supposons, par exemple, que trois plateformes soient sélectionnées pour votre application : P1, P2 et P3. Vous leur donnez les poids : 60, 50 et 10 respectivement. L'application Round Robin convertit ces valeurs en pourcentages tels que P1 = 50 %, P2 = 42 % et P3 = 8 %, ce qui correspond à 100 %. Ces pourcentages signifient que 50 % du temps, les utilisateurs sont acheminés via P1, 42 % du temps via P2 et 8 % du temps via P3.

Les poids que vous attribuez aux plateformes ne doivent pas nécessairement totaliser 100. Il peut s'agir de n'importe quel entier compris entre 0 et 1 000 000. Les pondérations données aux plateformes lorsqu'elles sont converties en pourcentage (par l'application dans le back-end) s'élèvent à 100 %. Si toutes les plateformes sélectionnées reçoivent le même poids, le trafic sera réparti uniformément entre elles au fil du temps. Si vous avez une plateforme, celle-ci est utilisée 100 % du temps, quel que soit le poids que vous lui accordez.

Les poids ne sont utilisés que pour les plateformes considérées comme disponibles selon les contrôles de disponibilité des radars et des sonars, en fonction de la configuration de l'application. L'indisponibilité des plates-formes entraîne une non-correspondance de la distribution avec les poids configurés. Par exemple, si P1 pèse 100 et P2 pèse 0 mais que P1 échoue à la vérification de disponibilité du radar, alors tout le trafic est dirigé vers P2.

Handicap (utilisé pour ORTT et Throughput)

Le **Handicap** est une valeur en pourcentage qui peut être appliquée à une plate-forme pour modifier les scores radar pour la RTT et le débit, c'est-à-dire augmenter artificiellement le temps de réponse (en millisecondes) ou diminuer le débit (en kbps). L'augmentation ou la diminution de ces valeurs réduit les performances de la plateforme de telle sorte que la probabilité qu'elle soit sélectionnée devient faible. Les handicaps peuvent être ajoutés aux plateformes à l'échelle mondiale, ou séparément pour des marchés ou des pays spécifiques.
Dans les cas où une plateforme coûte cher sur un marché ou un pays spécifique et que vous souhaitez réduire sa probabilité d'être sélectionnée lorsqu'un fournisseur équivalent est proche en termes de performances. Vous définissez une valeur Handicap comme multiplicateur pour augmenter la valeur du temps de réponse ou diminuer la valeur du débit. Par conséquent, cela réduit la probabilité qu'une plateforme soit sélectionnée.

Voici à peu près comment fonctionne **Handicap** dans le backend :

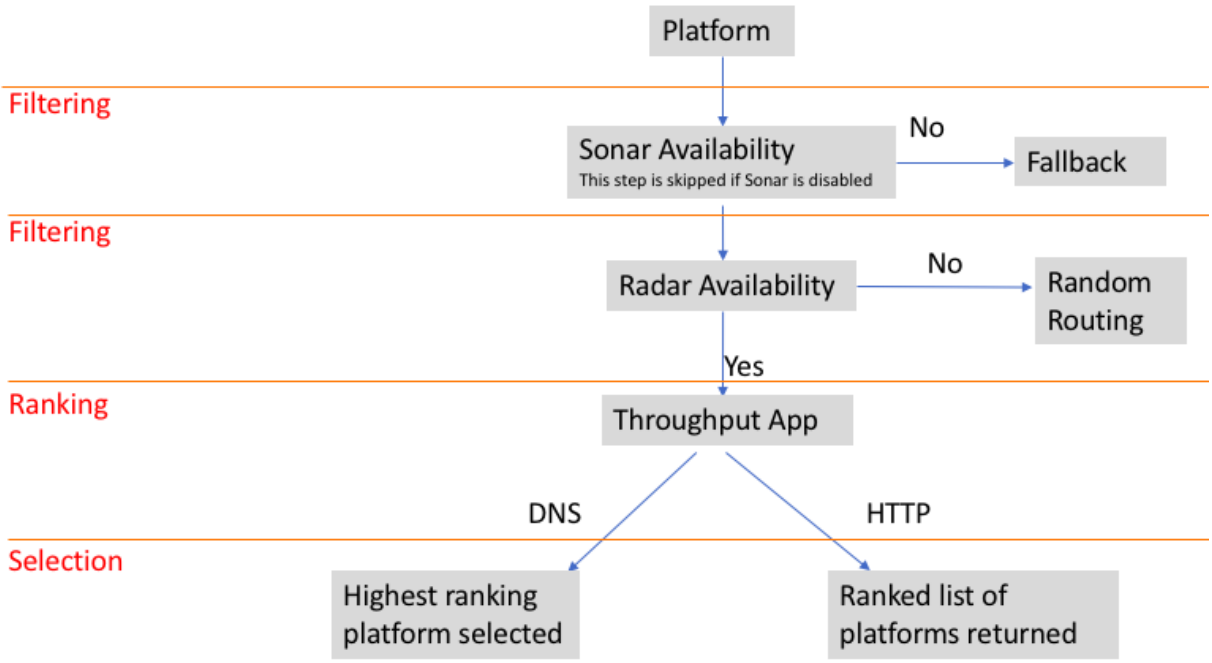
- RTT de plate-forme avec handicap appliqué = RTT (temps aller-retour en millisecondes) * (1 + handicap) ou
- Débit de la plate-forme avec handicap appliqué = (débit en Kbits/s) * (1 —Handicap)

Remarque : Les valeurs RTT et Throughput de la plate-forme sont des scores issus des données radar. Le tableau suivant montre comment Handicap affecte les deux plateformes - P1 et P2. Et comment le Handicap diminue la probabilité que P1 soit sélectionné.

	P1	P2
RTT sans handicap	50 millisecondes	60 millisecondes
RTT avec un handicap de 50 % (0,5) pour P1 et 0 % (0) pour P2	50 (1+0,5) = 75 millisecondes	60 (1+0) = 60 millisecondes
Débit sans handicap	3000 kbits/s	2800 kbits/s
Débit avec un handicap de 50 % (0,5) pour P1 et 0 % (0) pour P2	3000 (1-0.5) = 1500 kbps	2800 (1- 0) = 2800 Kbits/s

Flux de travail de filtrage, de classement et de sélection

Exemple de diagramme de flux pour Throughput App



Critères de sélection de

Les applications Openmix Quickstart utilisent les critères suivants comme filtres de 1er, 2e et 3e niveaux pour classer et sélectionner la meilleure plateforme.

Niveau de filtration	Critères de sélection	ORTT	Débit	Round Robin	Basculement	Routage statique	Proximité statique
1er niveau	Vérification de la disponi-bilité du sonar (si activé)	X	X	X	X	X	X
2e niveau	Vérification de la disponi-bilité du radar (si activé)	X	X	X	X	X	SO

Niveau de filtration	Critères de sélection	ORTT	Débit	Round Robin	Basculement	Routage statique	Proximité statique
3e niveau	Poids (définis par l'utilisateur)	SO	SO	X	SO	SO	SO
3e niveau	Temps aller-retour (en millisecondes)	X	SO	SO	SO	SO	SO
3e niveau	Débit (en Kbits/s)	SO	X	SO	SO	SO	SO

Rapports de code de raison

Les codes de raison fournissent une visibilité sur les raisons pour lesquelles la décision a été prise et permettent également de savoir quelle partie du code de l'application est exécutée. Pendant l'exécution, une application peut ajouter quelque chose au champ du code de raison à tout moment. Les codes de raison ont une signification différente pour chaque application Quickstart. Il existe des points communs entre les codes de raison de chaque application, mais ce n'est pas complet.

Remarque : Pour que les codes de motif s'affichent correctement, ils ne doivent pas dépasser la limite maximale de 200 caractères. Si cette limite est dépassée, le code de motif est affiché comme **inconnu**. Si l'utilisateur n'a pas ajouté de code de motif, il affiche **Inconnu**.

Voici les codes de motif pour les applications de démarrage rapide :

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
Optimal Avail	Le fournisseur le plus performant est disponible et a été sélectionné.	X	S/O	S/O	X	S/O	X
Optimal Unavail-Radar	Le fournisseur le plus performant n'est pas disponible ; un autre fournisseur éligible a été sélectionné et est disponible selon le radar	X	S/O	S/O	X	S/O	X
Optimal Unavail-Radar+Sonar	Le fournisseur le plus performant n'est pas disponible en raison d'un radar et/ou d'un sonar.	X	S/O	S/O	X	S/O	X

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
All Unavail-Radar	Toutes les plate-formes éligibles ne sont pas disponibles selon le radar. Demande achem-inée vers une solution de secours	X	X	S/O	X	S/O	X
All Unavail-Sonar	Toutes les plate-formes éligibles ne sont pas disponibles selon le sonar. La demande est achem-inée vers une solution de secours.	X	X	S/O	X	S/O	X

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
Data Issue	Indique les mesures radar manquantes pour une ou plusieurs plateformes. La plateforme est choisie au hasard en conséquence	X	X	S/O	X	S/O	X
Geo Default	Les paramètres Geo par défaut sont en vigueur	X	X	S/O	X	X	X
Geo Override-Country	Une dérogation nationale est en vigueur pour cette décision	X	X	S/O	X	X	X
Geo Override-Market	Une dérogation du marché est en vigueur pour cette décision	X	X	S/O	X	X	X

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
All Avail	Toutes les plate-formes éligibles sont disponibles via un sonar et un radar	X	X	S/O	X	S/O	S/O
Proximal Avail	La plate-forme géo-graphique la plus proche est disponible et a été sélection-née	X	S/O	S/O	S/O	X	S/O
Eligible Unavail-Radar	Pour Round Robin, le four-nisseur éligible n' est pas disponible selon le radar	S/O	X	S/O	S/O	S/O	S/O

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
Persistent app	La décision a servi une réponse mise en cache, aucune logique n' a été exécutée	X	X	X	X	X	X
Request Geo Unavailable	La géolocalisation de la demande ne peut pas être établie. Demande acheminée vers une solution de secours	X	S/O	S/O	S/O	X	S/O
All Unavail-Provider	Tous les fournisseurs ne sont pas disponibles. Demande acheminée vers une solution de secours	X	S/O	S/O	S/O	X	S/O

Code motif	Description	RTT optimal	Round Robin	Routage statique	Débit	Proximité statique	Basculement
Unavail-Provider-Dist	Aucun score de proximité n'a été trouvé pour aucun fournisseur. Demande acheminée vers une solution de secours	X	S/O	S/O	S/O	X	S/O

Applications de démarrage rapide Openmix

1. Connectez-vous au portail de gestion intelligente du trafic NetScaler.
2. Dans le menu de navigation de gauche, accédez à **Openmix > Configuration de l'application**.
3. Si vous configurez votre application Openmix pour la première fois, la page **Démarrer s'affiche** lorsque vous cliquez sur **Openmix > Configuration de l'application**.
4. Pour configurer une nouvelle application, cliquez sur le bouton **Démarrer** ou sur le bouton **Ajouter** dans le coin supérieur droit de la page. Si les applications Openmix ont déjà été configurées, la liste des applications s'affiche sur cette page.

Les sections suivantes vous guident tout au long du processus de configuration des applications Openmix sur le portail.

Routage statique

Ce type d'application n'utilise aucune logique d'évaluation pour décider quelle réponse DNS doit être fournie à l'utilisateur final. L'application sélectionne toujours une seule plateforme ici, spécifiée par l'utilisateur. Par conséquent, l'application n'utilise qu'une seule réponse DNS CNAME ou adresse IP. L'application de routage statique peut être configurée via le portail sur la page **Configuration de l' application** .

Remarque : Avant de configurer votre application, assurez-vous que vos plates-formes sont d'abord configurées. Voir la page Plateformes pour la configuration de la plateforme

Navigation

1. Accédez à **Openmix > Configuration de l'application**.
2. Cliquez sur le bouton **Ajouter** en haut à droite

La boîte de dialogue **Informations de base** s'ouvre.

Informations de base Suivez ces étapes pour saisir les **informations de base** :

1. Pour **Protocol**, sélectionnez DNS ou HTTP dans la liste.
2. Pour **Type d'application**, sélectionnez Routage statique. Ou si vous configurez un autre type d'application, sélectionnez-la dans la liste.
3. Donnez un **nom** à votre application (champ obligatoire) ; ajoutez une **description** (champ facultatif) ; et un **tag** (champ facultatif).
4. Cliquez sur **Suivant** pour **la configuration**.

Configuration Pour configurer l'application, procédez comme suit :

1. Sélectionnez la plate-forme associée dans la liste **Plateforme** . Il s'agit de la plate-forme que vous configurez dans la page Plateformes, représentant le CDN, le Cloud ou le centre de données.
2. Entrez un enregistrement **CNAME/A/AAAA** (pour DNS) ou une **URL** (pour HTTP). Le CNAME DNS ou l'URL HTTP de la plate-forme sélectionnée doit pointer vers une adresse IP ou un nom d' hôte valide.
3. Pour **CORS**, dans un protocole HTTP, sélectionnez None, All ou Custom pour CORS. CORS vous permet de contrôler l'accès à votre site depuis d'autres sites. Vous pouvez soit restreindre complètement l'accès à votre site à partir d'autres sites (en cliquant sur **Aucun**), autoriser l'accès à partir de tous les autres sites (en cliquant sur **Tout**), soit autoriser l'accès uniquement à partir de sites spécifiques (en cliquant sur **Personnalisé**).
4. Entrez un **TTL** (Time-To-Live) pour la réponse. La valeur par défaut est de 20 secondes, mais elle peut être remplacée.
5. Cliquez sur **Terminer**.
6. Dans la fenêtre contextuelle de confirmation, cliquez sur **Terminé** ou **Publier** pour voir votre application répertoriée sur la page des applications Openmix. Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et affiche un statut vert. Cela signifie que l'application est en cours de production. Si vous cliquez sur **Terminé**, votre application est toujours répertoriée sur la page des applications, mais elle n'est pas publiée et son état est rouge.

Basculement

L'application Failover prend en charge une logique de routage simple dans laquelle une plate-forme est choisie en fonction de sa place dans la ligne et de sa disponibilité. Le client peut créer une chaîne de basculement qui décide de la plate-forme à sélectionner en premier, deuxième, etc. Cette chaîne de basculement peut être créée pour fonctionner à l'échelle mondiale ou pour des marchés et des pays individuels.

L'application **de basculement** peut être configurée dans le portail sur la page **Configuration de l' application** .

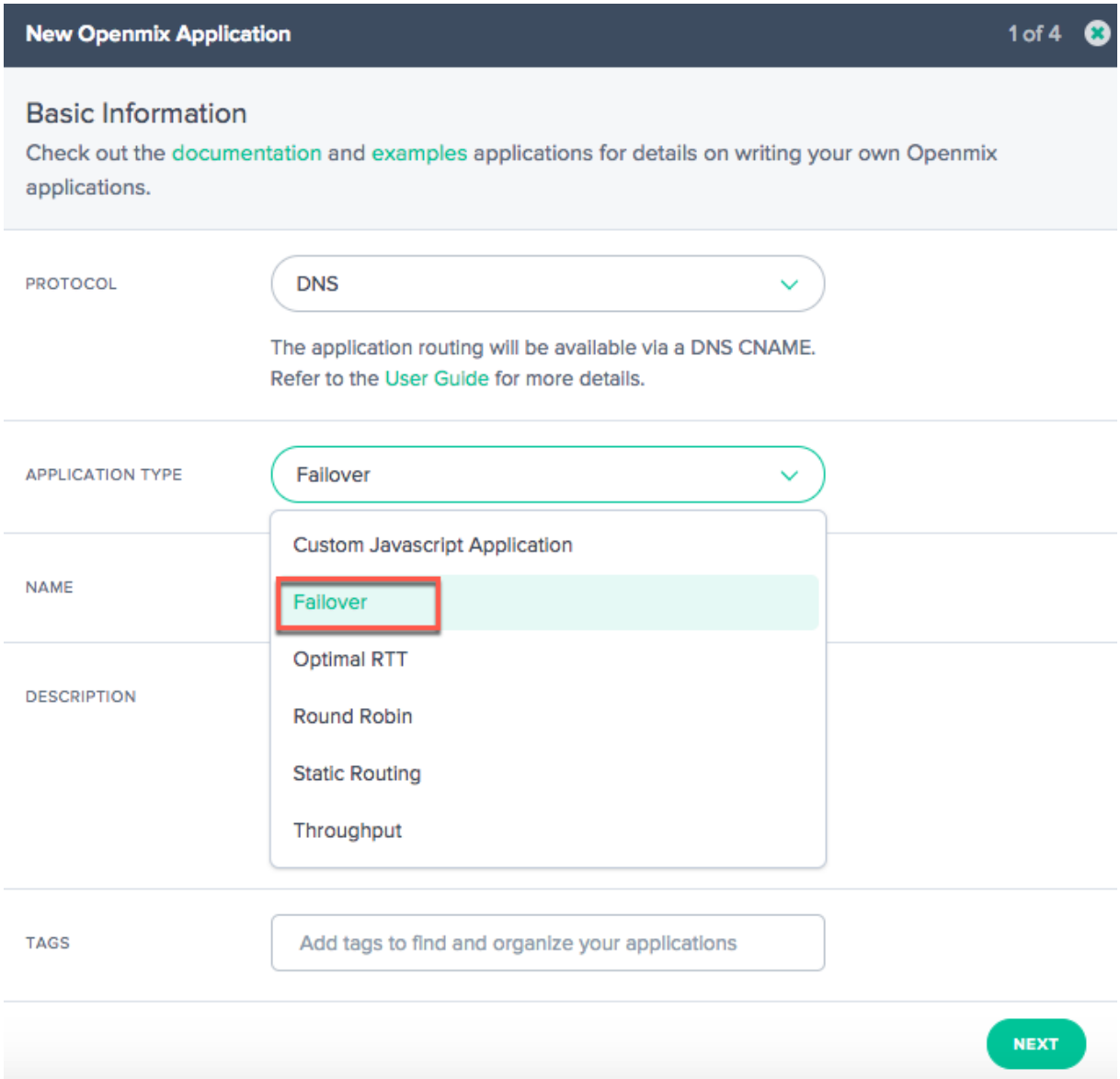
Remarque : Avant de configurer votre application, assurez-vous que vos plates-formes sont configurées en premier. Reportez-vous à la page Plateformes pour la configuration de la plateforme.

Navigation

1. Connectez-vous au portail.
2. Dans le menu de navigation de gauche, accédez à **Openmix > Configuration de l'application**.
3. Cliquez sur le bouton Ajouter en haut à droite pour accéder à la boîte de dialogue Nouvelle application Openmix, **informations de base** .

Informations de base

1. Sélectionnez **DNS** dans la liste **Protocol** .
2. Dans la liste **Type d'application**, sélectionnez **Basculement**.
3. Donnez un **nom** (champ obligatoire) à votre demande ; ajoutez une **description** (champ facultatif) ; et un **tag** (champ facultatif).
4. Lorsque vous avez terminé, cliquez sur **Suivant**.

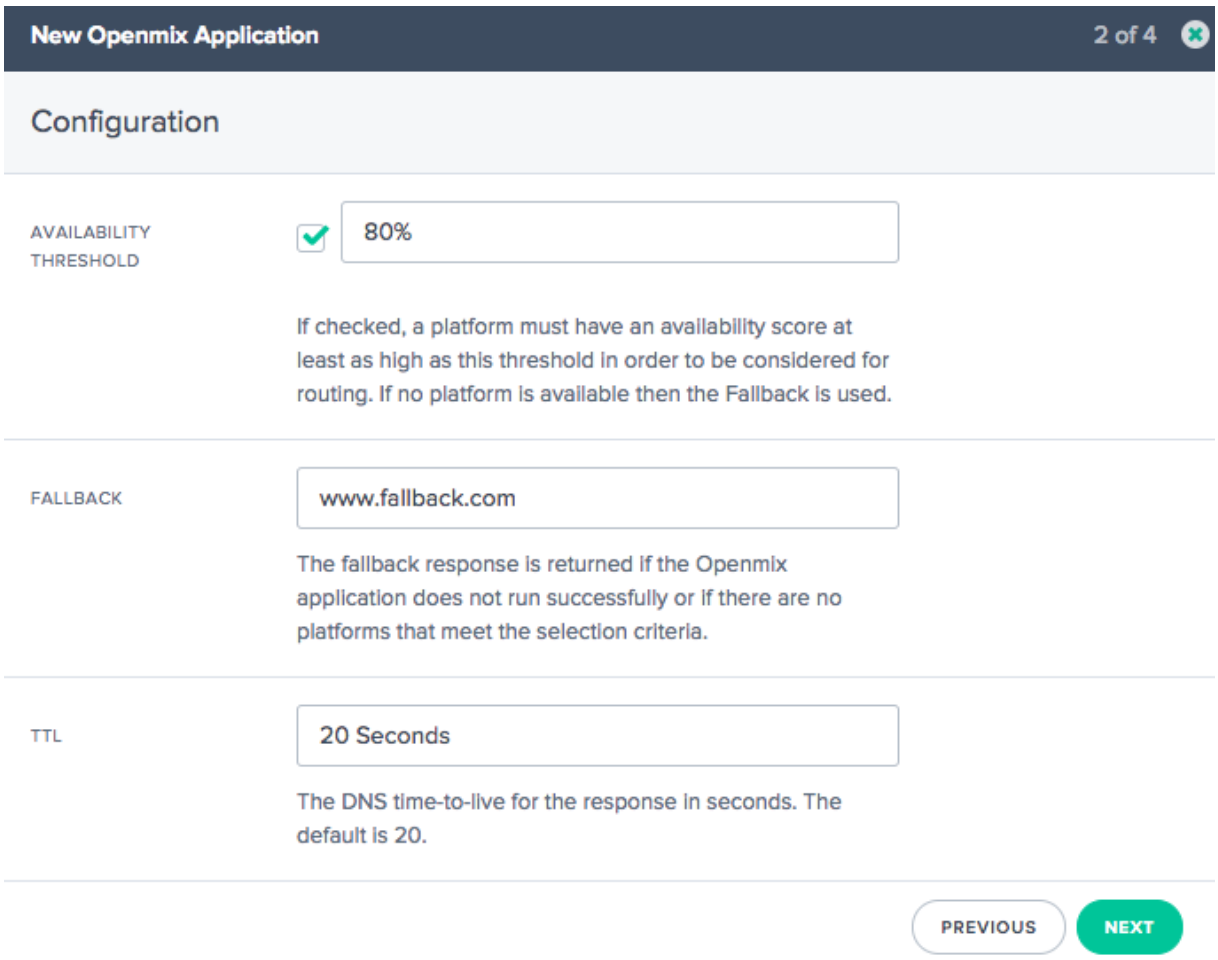


Configuration

1. Dans la boîte de dialogue Configuration, activez la case à cocher **Seuil de disponibilité** . Le seuil de disponibilité a une valeur par défaut de 80 %. Une plate-forme doit avoir un score de disponibilité au moins aussi élevé que ce seuil pour être prise en compte pour le routage.

    - Si vous souhaitez modifier le seuil de disponibilité par défaut, tapez simplement une nouvelle valeur pour remplacer la valeur par défaut.
    - Si aucune plate-forme n'a un score de disponibilité égal ou supérieur au seuil spécifié, l'adresse CNAME ou A ou AAAA ou IP de secours est utilisée.
    - Si la case n'est pas cochée, la plate-forme suppose un seuil de disponibilité nul. Cela signifie qu'il n'y a pas de vérification de disponibilité de Radar sur cette plate-forme.

2. Entrez une adresse CNAME/A/AAAA ou IP pour **Fallback**. Le CNAME/A/AAAA ou IP de secours est généralement utilisé si l'application rencontre des problèmes ou des erreurs.
3. Entrez un **TTL** (Time-To-Live) pour la réponse. La durée par défaut est de 20 secondes. Vous pouvez remplacer cette valeur si nécessaire.



Platform Information

1. Dans la boîte de dialogue **Informations sur la plate-forme**, sélectionnez une **plate-forme** dans la liste.

   - Vous pouvez sélectionner plusieurs plateformes à l'aide du bouton **Ajouter des plate-formes** . L'idée est de sélectionner toutes les plateformes disponibles applicables au routage global et géographique (marchés et pays).
   - Les plateformes de cette liste sont celles que vous avez configurées sur la page Plateformes du portail, représentant votre CDN, votre Cloud ou votre centre de données.
   - Toutes les applications Openmix nécessitent la configuration préalable d'une plateforme associée. Si vous ne trouvez pas de plateforme dans la liste, vous pouvez la configurer sur la page Plateformes du portail.

2. Entrez l'enregistrement **CNAME/A/AAAA** de la plateforme.
3. Assurez-vous que la case **Activé** est cochée (indiquant que la plate-forme est activée) avant de passer à l'étape suivante.
4. Si **Sonar** est configuré et que vous souhaitez utiliser les données Sonar pour vous aider dans le processus de prise de décision initial, assurez-vous de cocher la case **Utiliser Sonar pour la disponibilité de la plate-forme** . **Remarque** : La case à cocher Sonar s'affiche uniquement si Sonar est activé pour cette plate-forme.
5. Cliquez sur **Suivant** pour **Configuration de l'emplacement**.

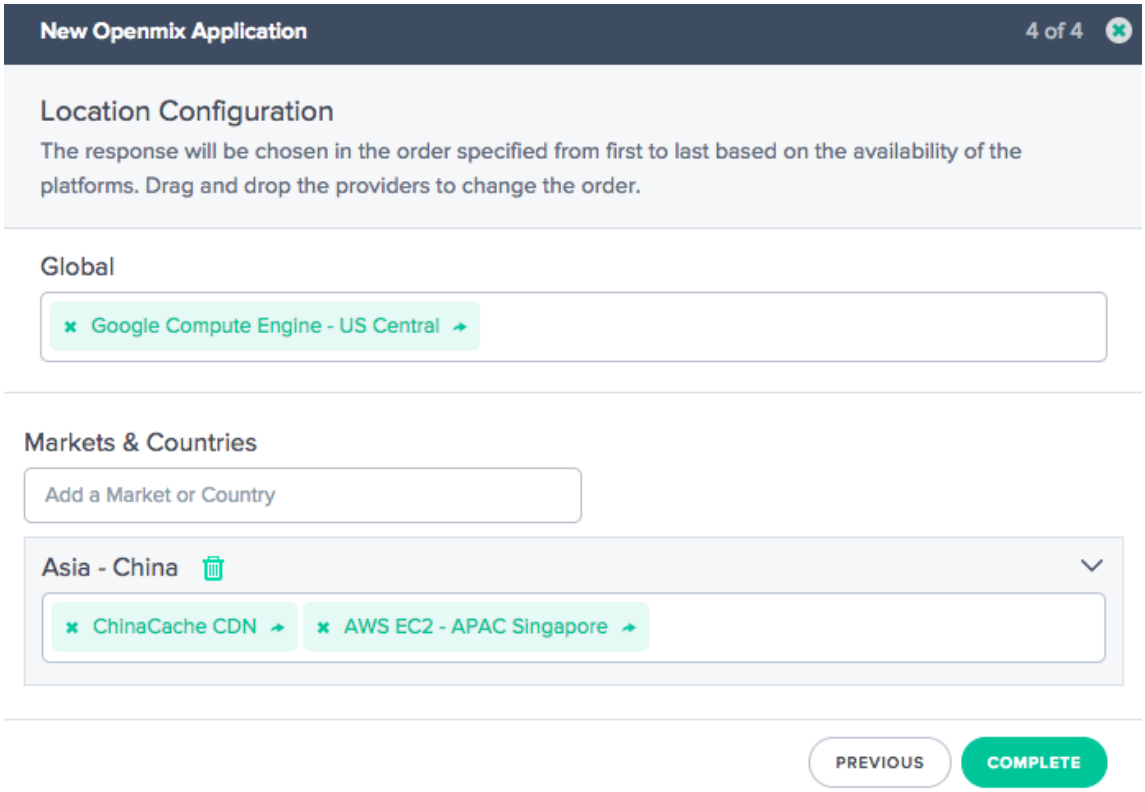
Configuration de l'emplacement

1. Dans la boîte **de dialogue Configuration de l'emplacement**, sélectionnez les plates-formes requises pour le routage **global** .

   - **Global** indique que vous êtes en train de configurer une chaîne de plateformes pour le routage global.
   - Lorsque vous cliquez dans le champ **Global**, une liste affiche toutes les plateformes que vous avez sélectionnées à l'étape **Informations sur la plate-forme** .
   - Sélectionnez les plates-formes requises dans la liste pour le routage global basé sur la disponibilité.
   - L'ordre dans lequel vous placez les noms des plateformes dans ce champ détermine la priorité de leur sélection. Par exemple, si la première plateforme de votre liste n'est pas disponible, la seconde est sélectionnée. Si aucune des plates-formes de la liste n'est disponible, alors la solution de secours est utilisée.
   - Vous pouvez faire glisser les noms des plateformes pour modifier leur ordre de priorité.

2. Cliquez sur **Marchés et pays** si vous souhaitez configurer des plateformes pour le routage géographique local.

   - Lorsque vous cliquez dans le champ **Marchés et pays**, la liste affiche toutes les plateformes que vous avez sélectionnées à l'étape **Informations sur la plateforme** .
   - Sélectionnez les plates-formes pour le routage géographique local, séparément pour chaque géo (marché/pays).
   - L'ordre dans lequel vous placez les noms des plateformes dans ce champ détermine la priorité de leur sélection. Par exemple, en Chine, vous voulez d'abord utiliser le POP chinois, et uniquement s'il n'est pas disponible, vous voudriez que votre POP de Singapour soit utilisé, que vous placerez ensuite sur la ligne, et ainsi de suite.
   - Vous pouvez faire glisser les noms des plateformes pour modifier leur ordre de priorité.



3. Cliquez sur **Terminer**pour terminer la configuration de votre application.
4. Dans la fenêtre contextuelle de confirmation, cliquez sur **Terminer** ou sur **Publier** pour voir votre application répertoriée sur la page **Openmix** .
   - Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et affiche un statut vert. Votre application est en cours de production.
   - Si vous cliquez sur **Terminé**, votre application est toujours répertoriée sur la page Openmix, mais elle n'est pas publiée et son état est rouge.

Round Robin

Cette application suit une méthodologie typique d'équilibrage de charge Global Server de Round Robin, où chaque CNAME est renvoyé aux utilisateurs finaux en alternance, au fur et à mesure des requêtes DNS. Il utilise les données Sonar (si Sonar est activé) et le seuil de **disponibilité de la plate-forme** pour évaluer la meilleure plate-forme pour l'utilisateur demandeur. Chaque plateforme est sélectionnée sur la base de la méthodologie de distribution Round Robin. Par exemple, si les plates-formes P1, P2 et P3 atteignent le seuil de disponibilité, la première demande est acheminée vers P1, la deuxième vers P2 et la troisième vers P3. La quatrième requête est routée à nouveau vers P1, et ainsi de suite.

Pour configurer une nouvelle application Round Robin, cliquez sur le bouton **Ajouter** dans le coin

supérieur droit de la page Openmix. La boîte de dialogue **Informations de base** s'ouvre.

Navigation

1. Connectez-vous au portail.
2. Dans le menu de navigation de gauche, accédez à Openmix > Configuration de l'application.
3. Cliquez sur le bouton Ajouter en haut à droite pour accéder à la boîte de dialogue Nouvelle application Openmix, informations de base .

Informations de base

1. Dans la boîte de dialogue Informations de base, sélectionnez DNS comme protocole pour Round Robin.**Remarque** : Pour l'application Round Robin, le routage n'est disponible que via un CNAME DNS.
2. Sélectionnez le **type d'application** dans la liste. Donnez à l'application un **nom** (champ obligatoire), une **description** (champ facultatif) et un **tag** (champ facultatif).
3. Cliquez sur **Suivant** pour la configuration.

Configuration

1. Le **seuil de disponibilité** a une valeur par défaut de 80 %. Pour modifier cette valeur, il suffit de saisir une nouvelle valeur pour remplacer la valeur par défaut.
2. Entrez une adresse CNAME/A/AAAA ou IP pour Fallback. Le CNAME/A/AAAA ou IP de secours est généralement utilisé si l'application rencontre des problèmes ou des erreurs.
3. Entrez un TTL (Time-To-Live) pour la réponse. La valeur par défaut est de 20 secondes, mais cette valeur peut être remplacée si nécessaire.
4. Cliquez sur **Suivant** pour obtenir des informations sur la plate-forme

Platform Information

1. Sélectionnez une plate-forme dans la liste **Plate-forme** . **Remarque** : Toutes les applications Openmix nécessitent une plateforme associée préalablement configurée. Si vous ne trouvez pas de plateforme dans la liste, vous pouvez la configurer sur la page Plateformes du portail.
2. Sélectionnez d'autres plates-formes en cliquant sur le bouton **Ajouter une plate-forme** .
3. Entrez un enregistrement CNAME ou A/AAAA ou une adresse IP (dans DNS), ou une URL (en HTTP) pour cette plate-forme. Il doit s'agir d'une URL, d'un nom d'hôte ou d'une adresse IP valide. Il peut être de la forme : `scheme:[//host[:port]][/path][?query][#fragment]`.
4. Assurez-vous que la case **Activé** est cochée (indiquant que la plate-forme est activée) avant de passer à l'étape suivante.

5. Si Sonar est disponible et que vous souhaitez utiliser les données Sonar pour vous aider dans le processus de prise de décision initial, assurez-vous de cocher la case **Utiliser Sonar pour la disponibilité de la plate-forme** .
6. Cliquez sur **Enregistrer** pour passer à l'étape 4 afin d'attribuer des poids appropriés à chaque plateforme.

Configuration de l'emplacement

1. Attribuez **des poids** pour la priorisation et la sélection de chaque plateforme au niveau mondial et/ou par marché ou par pays.
2. Pour attribuer des poids de plate-forme séparément pour le marché ou le pays, entrez le nom dans la zone de recherche Marchés et pays et faites votre choix dans la liste.
3. Cliquez sur **Terminer** pour créer votre demande.
4. Dans la fenêtre de confirmation, cliquez sur **OK** ou sur **Publier** pour voir votre application répertoriée sur la page Openmix. Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et affiche un statut vert. Votre application est en cours de production. Si vous cliquez sur **Terminé**, votre application est toujours répertoriée sur la page Openmix, mais elle n'est pas publiée et son statut est rouge.

Application Temps de trajet aller-retour optimal (ORTT)

L'application ORTT utilise le temps de réponse radar, les données du sonar, si Sonar est activé, et le seuil de disponibilité de la plate-forme pour évaluer la meilleure plateforme pour l'utilisateur qui demande. Le seuil de disponibilité est la disponibilité minimale (80 % est la valeur par défaut) que la plateforme doit atteindre pour être sélectionnée. En outre, l'application ORTT utilise également une valeur Handicap qui permet aux clients, globalement ou localement, d'influencer la manière d' acheminer les utilisateurs finaux.

Les trois premières étapes (Informations de base, Configuration et Informations sur la plate-forme) sont saisies de la même manière que pour les autres applications.

Suivez ces étapes pour configurer les informations de localisation et saisir des valeurs pour **Handicap** pour chaque plateforme, globalement ou par emplacement/marché.

Configuration de l'emplacement

1. Dans la boîte de dialogue **Configuration de l'emplacement**, entrez une valeur pour **Handicap** pour une ou toutes les plateformes sélectionnées. Vous pouvez entrer une valeur de handicap comprise entre 0 et 6 000. L'utilisation du handicap consiste à réduire manuellement les chances qu'une plate-forme particulière soit choisie pour le routage, lorsqu'il existe de meilleures plateformes disponibles, en termes de coût ou de commodité. Plus la valeur du

handicap est élevée, moins la plateforme a de chances d'être sélectionnée. Vous pouvez désélectionner une plate-forme si nécessaire en désactivant le bouton **Sélection de la plate-forme** .

2. Cliquez sur **Marchés et pays** pour sélectionner un marché ou un pays particulier dans la liste et saisir les valeurs de **handicap** séparément pour chacune des plateformes associées.
3. Cliquez sur **Terminer**pour terminer la configuration de votre application.
4. Dans la fenêtre contextuelle de confirmation, cliquez sur **Terminé** ou **Publier** pour voir votre application répertoriée sur la page de liste des applications Openmix. Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et affiche un statut vert. Votre application est en cours de production. Si vous cliquez sur **Terminé**, votre application est toujours répertoriée sur la page Applications, mais elle n'est pas publiée et son état est rouge.

Débit

L'application **Throughput** sélectionne la plate-forme en fonction des données Sonar (si Sonar est activé), du débit le plus élevé (à l'aide des données Radar) et du seuil de disponibilité de la plate-forme (qui est de 80 % par défaut). En outre, cette application vous permet d'ajouter une valeur Handicap pour réduire le débit de certaines plateformes et influencer la manière dont les utilisateurs finaux sont acheminés. Cette valeur Handicap facultative peut être attribuée globalement et/ou localement (pour des marchés ou des pays spécifiques).

Les trois premières étapes (**Informations de base, Configuration et Informations sur la plate-forme**) sont saisies de la même manière que pour les autres applications. La **configuration de l' emplacement** est saisie de la même manière que dans l'application ORTT.

Lorsque vous avez terminé, cliquez sur **Terminer** pour revenir à la page de liste des applications Openmix. Enfin, cliquez sur **Publier** pour publier votre application lorsque vous êtes prêt à être mise en ligne.

Statut de la demande

L'état de l'application indique sa configuration actuelle.

- Red signifie non publié. Lorsque vous avez terminé la configuration, si vous cliquez sur **Terminé**, votre application est répertoriée dans la page des applications avec un point rouge, indiquant qu'elle n'a pas encore été publiée.
- Green signifie publié. Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et est signalée par un point vert, ce qui signifie que l'application est en production.
- Yellow représente la dernière version inédite. Le point jaune indique que l'application est créée et modifiée, et que les derniers paramètres modifiés ne sont pas encore publiés.

Proximité statique

L'application Static Proximity répond à la plate-forme située à proximité de la latitude et de la longitude de l'utilisateur demandeur.

> **Remarque :**
>
> Toutes les applications Openmix nécessitent la configuration préalable d'un ensemble de plate-formes associées. Si vous ne trouvez aucune plateforme dans la liste, vous pouvez la configurer sur la page Plateformes du portail.

Navigation

1. Connectez-vous au portail NetScaler Intelligent Traffic Management.
2. Dans le menu de navigation de gauche, accédez à **Openmix > Configuration de l'application**.
3. Cliquez sur le bouton plus, **Add Openmix App** en haut à droite.
4. Sélectionnez l'**application Quickstart**.

Informations de base

1. Dans la boîte de dialogue **Informations de base**, sélectionnez **DNS** comme protocole.
2. Sélectionnez **Static Proximity** comme type d'application. Donnez à l'application un nom (champ obligatoire), une description (champ facultatif) et un tag (champ facultatif).
3. Cliquez sur **Suivant** pour la configuration.

Configuration

1. Si cette option est activée, le **seuil de disponibilité** a une valeur par défaut de 80 %. Entrez une nouvelle valeur pour remplacer la valeur par défaut.
2. Entrez une adresse CNAME/A/AAAA ou IP pour **Fallback**. Le CNAME/A/AAAA ou IP de secours est généralement utilisé si l'application rencontre des problèmes ou des erreurs. Ce champ ne peut pas être vide.
3. Saisissez **TTL (Time-To-Live)** pour la réponse. La valeur par défaut est de 20 secondes, mais cette valeur peut être remplacée si nécessaire.
4. Cliquez sur **Suivant** pour les contrôles de persistance.

Contrôles de persistance Configurez **la persistance locale**. Pour plus d'informations, consultez la section Persistance locale. Cliquez sur **Suivant** pour obtenir des informations sur la plate-forme

Platform Information La latitude et la longitude de chaque plate-forme doivent être configurées via la page **Plateformes** . Les alias des plateformes communautaires héritent initialement des informations géographiques de la plateforme communautaire, bien qu'après avoir créé un alias, vous puissiez les modifier. Les plateformes privées doivent être configurées lors de leur création ou ultérieurement via leur volet de configuration. Pour afficher le volet de configuration, cliquez simplement sur l'entrée Platform du tableau.

Seules les plateformes appartenant aux catégories suivantes peuvent avoir des informations géographiques et faire partie de la liste de réponses d'une application opx :

- Cloud Computing
- Stockage dans le cloud
- Centre de données

1. Sélectionnez une plate-forme dans la liste **Plate-forme** .
2. Entrez un enregistrement CNAME ou A/AAAA ou une adresse IP (dans DNS), ou une URL (en HTTP) pour la plate-forme. Il doit s'agir d'une URL, d'un nom d'hôte ou d'une adresse IP valide. Il peut se présenter sous la forme de :

   ```
   scheme:[//host[:port]][/path][?query][#fragment]
   ```

3. Assurez-vous que la case **Activé** est cochée pour indiquer que la plate-forme est activée avant de passer à l'étape suivante.
4. Si Sonar est disponible pour cette plate-forme et que vous souhaitez utiliser les données Sonar pour être prises en compte lors de la résolution DNS, assurez-vous de cocher la case **Use Sonar for Platform Availability** .
5. Vous pouvez ajouter d'autres plateformes en cliquant sur **Ajouter une plateforme**.
6. Cliquez sur **Suivant** pour **Configuration de l'emplacement**.

Configuration de l'emplacement

1. Dans la partie Global de la boîte de dialogue Configuration de l'emplacement, vous pouvez configurer une chaîne de plates-formes pour le routage global. Vous pouvez activer ou désactiver la sélection de chaque plate-forme globalement.
2. Dans Marchés et pays, vous pouvez créer différentes configurations par marché ou pays, en ayant des règles de géo-clôture pour celles-ci.
3. Cliquez sur **Terminer** pour créer votre demande.

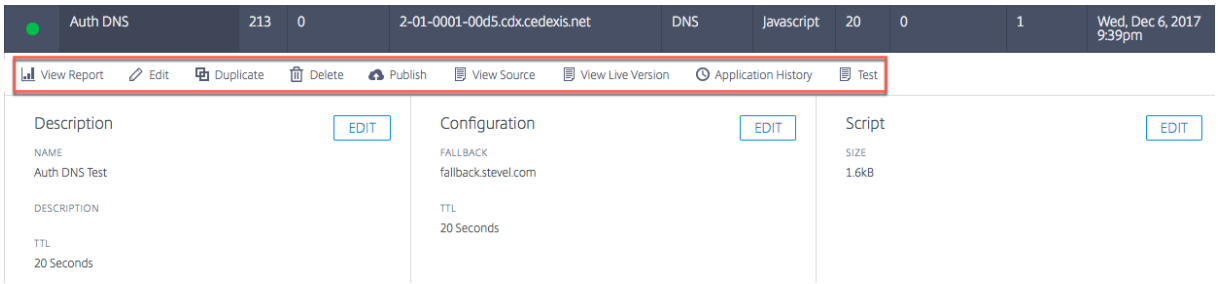
Dans la fenêtre contextuelle de confirmation cliquez sur **Publier, Ajouter un autre** ou **Terminé** :

- Si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et le statut est vert. Cela signifie que l'application est en cours de production.

- Si vous cliquez sur **Terminé**, votre application est répertoriée sur la page Openmix mais elle n'est pas publiée et son état est rouge.
- Si vous cliquez sur **Ajouter une autre**application, l'état de l'application est identique à **Done**, mais vous redémarrez le même processus pour créer une nouvelle application.

Gestion des applications Quickstart

Utilisez les onglets supérieurs du panneau du gestionnaire d'applications pour modifier, dupliquer, supprimer, tester, afficher les rapports, afficher la source et afficher l'historique des versions de l'application. Cliquez sur votre application dans la page de liste des applications Openmix pour développer le gestionnaire d'applications.



Voir le rapport

View Report vous amène à la page Openmix Decision Reports où vous pouvez voir la tendance des décisions Openmix pour chacune de vos applications, plateformes et zones géographiques.

Edit

Pour modifier votre application Openmix, cliquez simplement sur l'icône **Modifier** en haut du panneau du gestionnaire d'applications. Vous pouvez également effectuer des modifications individuelles séparément pour les informations de base, la configuration, la plate-forme ou l'emplacement en cliquant sur les boutons **Modifier** dans le panneau, comme illustré sur la figure. Lorsque vous avez terminé les modifications, cliquez sur **Terminé**pour répertorier l'application avec un statut non publié (pour d'autres modifications ultérieurement), ou cliquez sur **Publier** pour être mise en ligne instantanément.

dupliquer

Cliquez sur **Dupliquer** pour répliquer la configuration de l'application actuelle et l'enregistrer sous un nouveau nom.

Supprimer

Cliquez sur **Supprimer**pour supprimer les applications dont vous n'avez plus besoin.

Publier

Cliquez sur **Publier** pour publier directement l'application à partir du gestionnaire d'applications Openmix. Cette option n'est visible que si l'application n'est pas encore publiée.

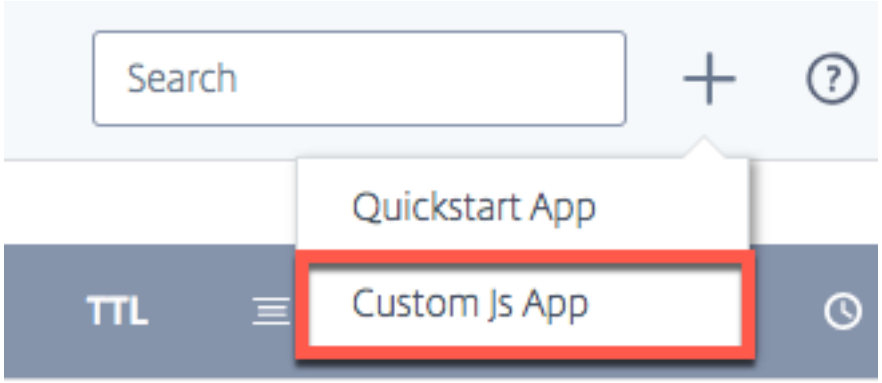
Applications JavaScript personnalisées Openmix

Les applications JavaScript Openmix sont des applications dotées de scripts Java personnalisables. Vous pouvez créer, configurer, tester et publier à l'aide de l'interface utilisateur du portail ITM.

Remarque : Ce guide ne couvre pas la création réelle du script personnalisé (syntaxes, variables, etc.). Pour plus d'informations sur la création de JavaScript personnalisé, consultez le Developer Exchange.

Navigation

1. Connectez-vous au portail ITM.
2. Dans le menu de navigation de gauche, accédez à **Openmix**.
3. Choisissez **Configuration de l'application**.
4. Pour configurer une nouvelle application Openmix, cliquez sur l'icône d'ajout dans le coin supérieur droit.
5. Sélectionnez **Custom JS App**.
6. La page de **configuration de l'application Openmix** s'ouvre.



Informations de base

1. **Nom de l'application** : donnez un nom à votre application.
2. **Description** : Donnez une description à l'application ou ajoutez une note de version ici. Il s'agit d'un champ facultatif.
3. **Tags** : entrez une balise appropriée, si nécessaire. Les balises permettent d'identifier et d'organiser votre application. Il s'agit d'un champ facultatif.
4. **Protocole** : sélectionnez DNS ou HTTP comme protocole.
   - **DNS** : si vous sélectionnez DNS, une valeur TTL doit être entrée.
   - **HTTP** : si vous sélectionnez HTTP, vous pouvez activer **l'accès sécurisé**.
5. **TTL** : entrez une durée de vie DNS pour l'application. La valeur recommandée est de 20 secondes. Remarque : Cette durée de vie s'applique si aucune durée de vie n'est définie par l'application JS personnalisée ou si la réponse est une valeur de secours.
6. **Fallback** : saisissez une adresse CNAME/A/AAAA ou IP pour **Fallback**. Le CNAME/A/AAAA ou IP de secours est généralement utilisé si l'application rencontre des problèmes ou des erreurs.
7. **Accès sécurisé** : si **Secure Access**est activé, l'API HTTP doit exiger une clé d'accès Oauth du client lors de l'appel. Consultez Sécurisation de l'API HTTP Openmix pour en savoir plus.

   Remarque : l'activation de l'accès sécurisé affiche une icône de cadenas à côté du nom de l'application dans la liste des applications sur la page d'accueil d'Openmix.

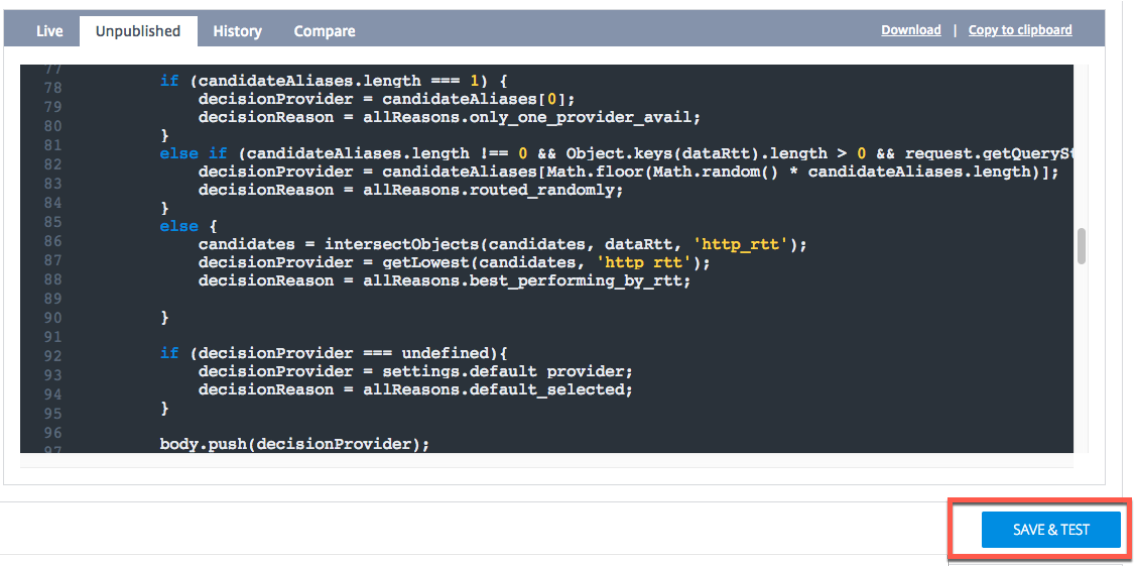
JavaScript personnalisé

Une fois que vous avez saisi les informations de configuration, vous pouvez télécharger votre code JavaScript personnalisé.

1. Cliquez sur le bouton **Choisir un fichier** et sélectionnez le fichier JavaScript que vous souhaitez télécharger. Vous pouvez télécharger un nouveau fichier pour remplacer un fichier existant à tout moment.

2. Cliquez sur **Enregistrer et tester** pour enregistrer votre application.

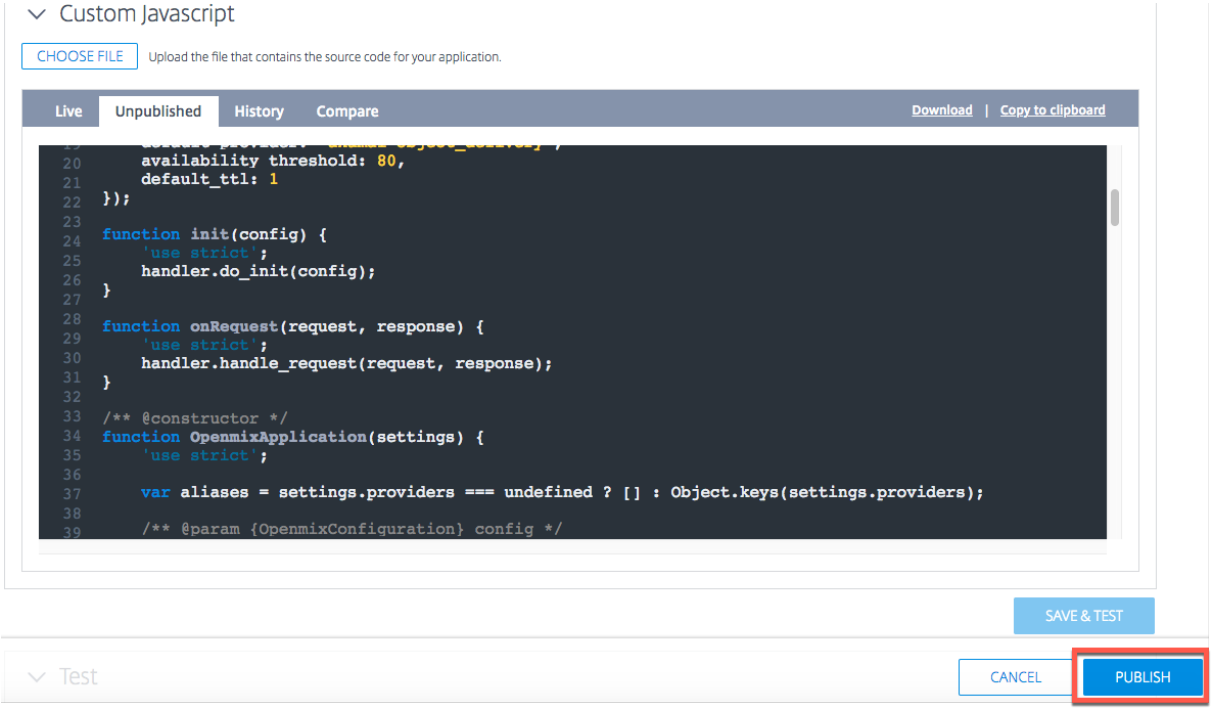
   Remarque : L'application est automatiquement testée à l'aide d'un vérificateur d'applications lorsqu'elle est téléchargée et enregistrée. S'il y a des erreurs, le vérificateur d'application affiche les informations d'erreur et l'emplacement de l'erreur. Pour plus d'informations sur les données disponibles dans le vérificateur d'applications, consultez la section Vérification des applications .



3. Cliquez sur **Annuler** pour revenir à la page Applications Openmix ou cliquez sur **Publier** si vous êtes prêt pour la mise en ligne de l'application.

   Remarque : si vous cliquez sur **Publier**, votre application est mise en ligne instantanément et affiche un statut vert. Votre application est en cours de production.

   Si vous cliquez sur **Annuler**, votre application est répertoriée sur la page des applications mais n'est pas publiée et son état est rouge. Pour en savoir plus sur le statut, consultez la section État de la demande .



Déploiement progressif des applications

Vous pouvez gérer le déploiement de votre application en envoyant un faible pourcentage de votre trafic Web via une nouvelle version, parfois appelée déploiement Canary. ITM vous permet d'envoyer un pourcentage spécifique du trafic vers la nouvelle version d'une application pour vous assurer que la logique de l'application se comporte comme prévu. Vous pouvez créer des rapports sur le comportement des versions existantes et nouvelles pour évaluer les modifications apportées à votre application dans un environnement réel. Cette option vous permet de corriger tout problème ou anomalie qui se produit avant d'acheminer 100 % de votre trafic Web via l'application nouvellement modifiée. Après avoir vérifié le comportement souhaité, vous pouvez augmenter le pourcentage de trafic vers la dernière version ou déployer l'application auprès de tous les utilisateurs.

Pour organiser le déploiement de l'application et publier une version de test de votre application récemment modifiée, procédez comme suit :

- Cliquez sur le nom de l'application (dans la page de liste des applications Openmix). Le panneau du gestionnaire d'applications s'ouvre.
- Cliquez sur l'icône **Modifier** pour modifier votre application.
- Modifiez votre application existante avec toutes les modifications nécessaires.
- Une fois que vous avez terminé les modifications, cliquez sur **Enregistrer et tester**.
- Faites défiler la page vers le bas avec les boutons **Annuler** et **Publier** . Entrez le pourcentage du trafic Web (1 % à 99 %) que vous souhaitez acheminer via cette nouvelle version modifiée.

- Cochez la case pour la répartition partielle du trafic via cette nouvelle version de l'application. Le trafic restant est envoyé vers la version live précédente.
- Cliquez sur **Publier**. Cette nouvelle version de test de l'application apparaît désormais dans la liste des applications de la page de **configuration d'Openmix** avec une nouvelle icône d'**état** . La nouvelle icône **Status** signifie que seul un trafic Web partiel circule en direct dans cette version.

Vous pouvez modifier le flux de trafic sur la version de test et modifier le pourcentage du flux de trafic pour afficher les performances.

```
1 ![Canary](/en-us/citrix-intelligent-traffic-management/media/openmix-
    jsapp-edit-canary.png)
```

Pour vérifier les performances de votre application, consultez le rapport de décision Openmix. Sélectionnez **Application** comme dimension principale et **Version** comme dimension secondaire. Cliquez ensuite sur **Appliquer les filtres** après avoir sélectionné votre application dans la liste. Le graphique montre les performances des différentes versions de votre application.

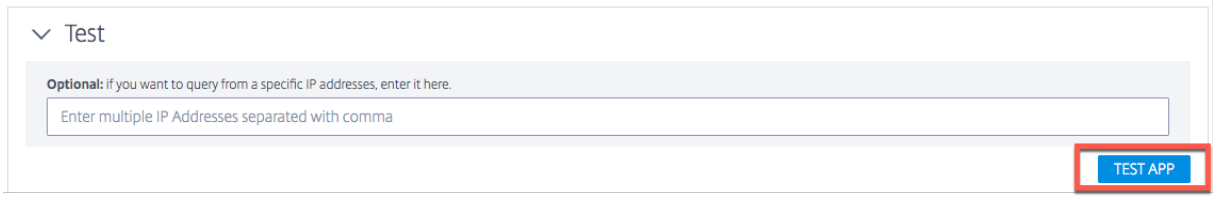
Une fois que vous êtes satisfait des performances de cette version de l'application, vous pouvez y acheminer 100 % de votre trafic Web en cliquant sur le bouton **Go Live** .

Cette version remplace la version live actuelle par la nouvelle version éditée.

Si vous ne souhaitez pas mettre cette version en ligne, cliquez sur **Dépublier**. Vos modifications sont enregistrées et apparaissent en tant qu'application non publiée dans la liste des applications de la page de **configuration d'Openmix** . Désormais, 100 % de votre trafic Web passe par la version en direct actuelle de votre application.

Tester

Vous pouvez tester votre application JavaScript à l'aide du bouton **Tester l'application** avant ou après la publication.

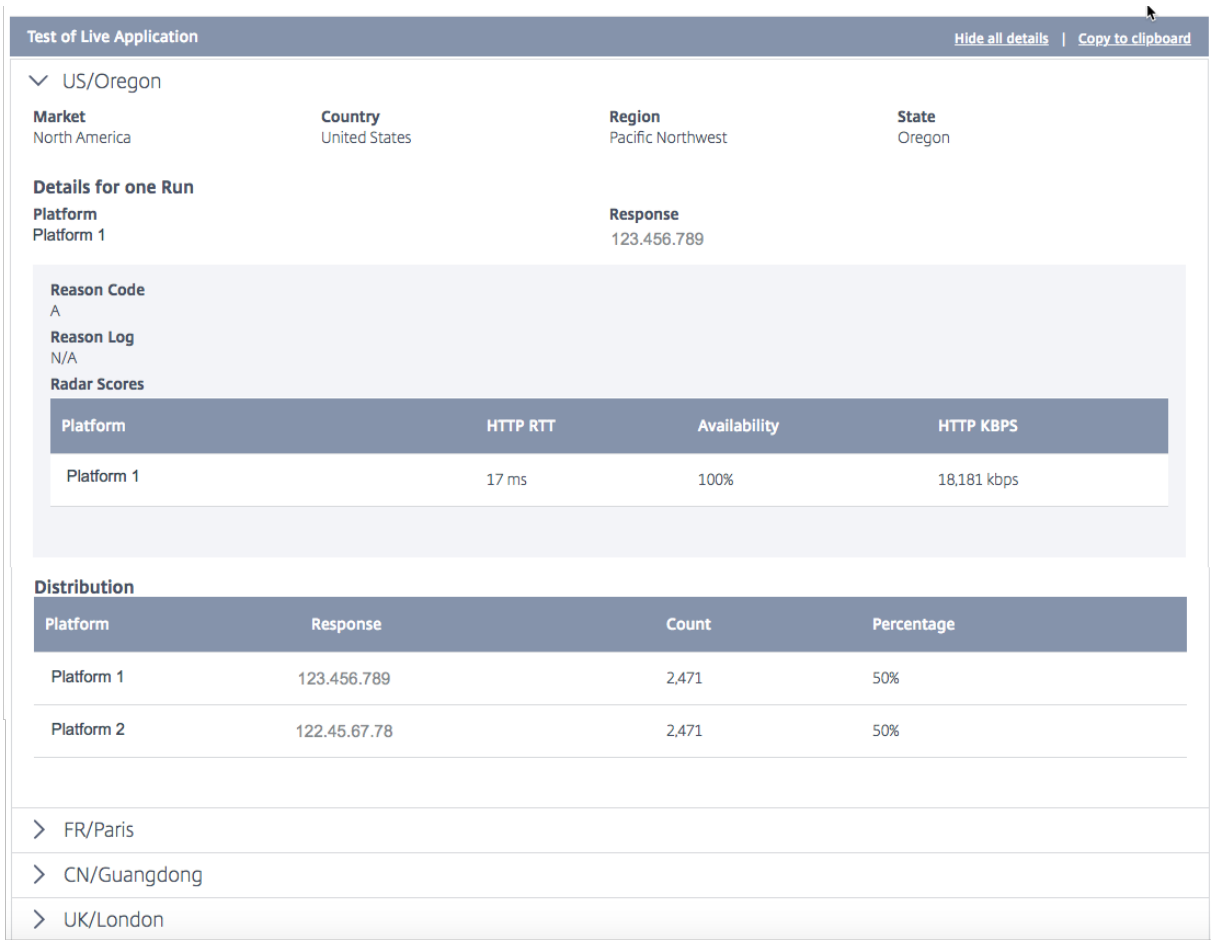


Il vous permet de visualiser les résultats des tests sur des ensembles spécifiques de marchés, de pays, de régions et d'États. Vous pouvez interroger l'application à partir d'adresses IP spécifiques.

Les résultats des tests incluent la **plate-forme** sélectionnée par l'application, la **réponse** reçue, le **code de raison, le journal**des raisons, les**scores radar**,**la distribution**, etc.

Cette fonctionnalité vous permet également de visualiser la répartition des décisions sur différentes plateformes. Par exemple, si deux plateformes sont utilisées pour le routage, vous pouvez voir le nombre de décisions et la réponse reçue pour chacune d'elles.

Cliquez sur le lien **Afficher tous les détails** pour voir les résultats des tests de votre application.



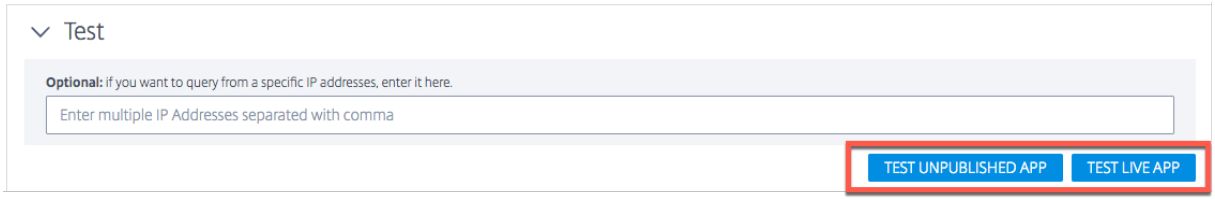
Les valeurs suivantes sont présentées sous forme de résultats de test :

Champ	Description
Marché, pays, région et État	L'endroit où l'application a été testée.
Plateforme	La plateforme sélectionnée par l'application.
Réponse	L'adresse CNAME ou IP de la plate-forme sélectionnée par l'application.
Code motif	Décrit la raison de cette décision.

Champ	Description
Journal des motifs	Sortie de l'application définie par le client. Permet aux clients de consigner des informations sur les décisions relatives aux applications.
Score radar	Les mesures du **temps de réponse (RTT)**, de **la disponibilité**et du **débit** enregistrées pour la plate-forme.
Distribution	Répartition des plateformes sélectionnées par une application pour chaque emplacement testé. Le **nombre** représente le nombre de fois où la plate-forme a été sélectionnée. Et le **pourcentage** est le pourcentage du nombre total pour la sélection de la plate-forme.

Remarque : vous pouvez exécuter ce test sur l'application en direct ou sur la version non publiée, c'est-à-dire si l'application n'est pas encore publiée.

Une fois votre application publiée, vous avez la possibilité de tester l'application en direct en cliquant sur l'option **Tester l'application en direct** . Si vous modifiez votre application ou chargez une nouvelle version, vous pouvez la tester avant de la publier en cliquant sur le bouton **Tester l'application non publiée** .



Vérification des applications

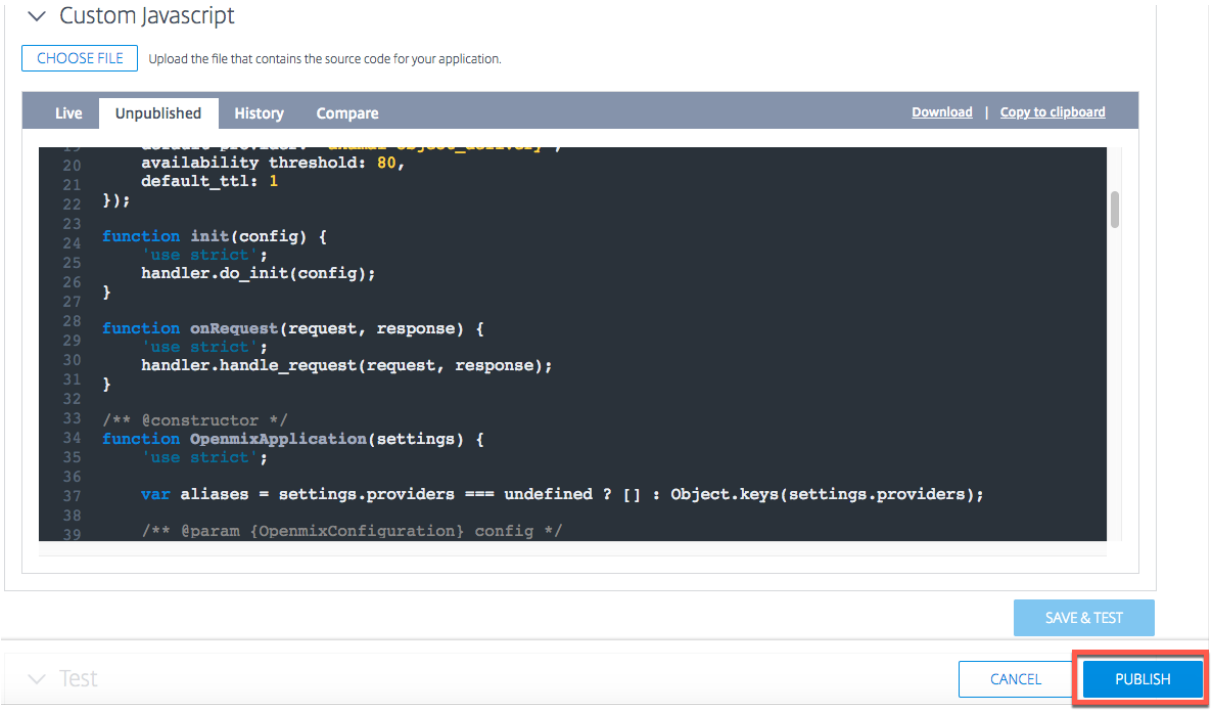
Pour vous assurer que les applications JavaScript personnalisées se comportent comme prévu, exécutez l'application via un vérificateur de code et de logique lorsque vous la téléchargez sur le portail ITM. Le vérificateur d'applications exécute l'application via un serveur de décision avec un trafic synthétique pour tester si l'application se compile et s'exécute correctement.

Si l'application s'exécute sans erreur, le vérificateur fournit des informations sur la distribution des décisions et les caractéristiques d'exécution. En revanche, si le serveur de décision rencontre une erreur lors de l'exécution de l'application, le vérificateur fournit des informations sur l'erreur. Nous recommandons que l'application ne contienne aucune erreur avant de la publier.

En cas d'erreur, vous pouvez corriger le fichier JavaScript dans votre local et le télécharger à nouveau sur le portail en cliquant sur le bouton **Choisir un fichier** .

Publier

Pour publier votre application et la mettre en ligne, cliquez sur le bouton **Publier** . Cette option est grisée si l'application n'est pas encore enregistrée ou n'est pas déjà publiée. Lorsque l'application est mise en ligne, elle apparaît dans la page du gestionnaire d'applications Openmix avec un statut vert. Pour en savoir plus sur l'état de l'application, consultez la section État de l'application .

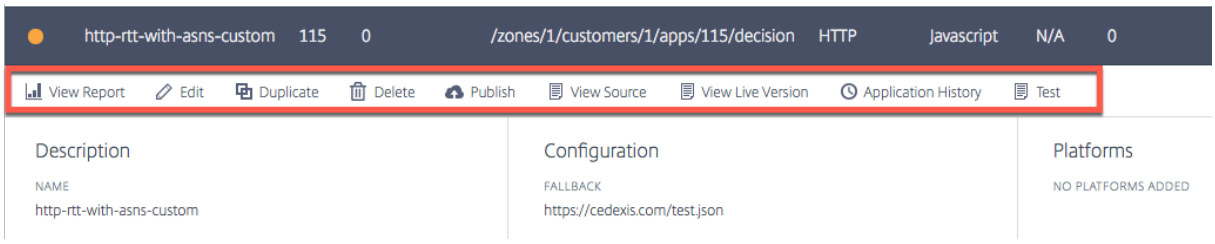


Remarque : l'application est publiée avec des erreurs si nécessaire.

Gestion des applications JavaScript personnalisées

Utilisez les onglets supérieurs du panneau du gestionnaire d'applications pour afficher les rapports, modifier, dupliquer, supprimer, publier, afficher la source, afficher la version en direct, afficher l'historique.

Cliquez sur votre application dans la page de liste des applications Openmix pour développer le panneau du gestionnaire d'applications.

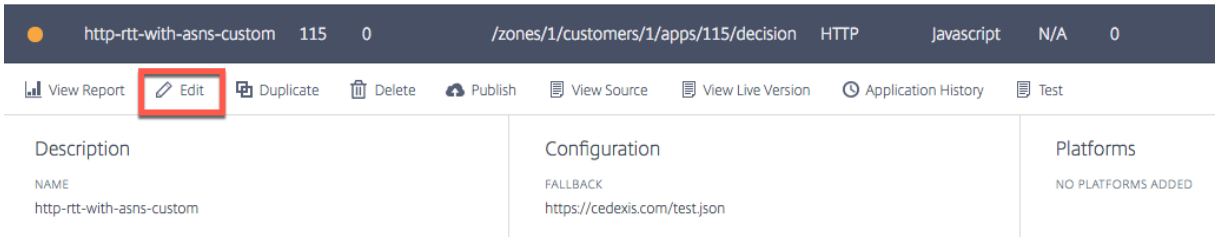


Voir le rapport

View Report vous amène à la page **Openmix Decision Reports** où vous pouvez voir la tendance des décisions Openmix pour chacune de vos applications, plateformes et zones géographiques.

Edit

Pour modifier une application Javascript personnalisée Openmix, cliquez sur le nom de l'application (dans la page de liste des applications Openmix). Le panneau du gestionnaire d'applications s'ouvre. Vous pouvez apporter des modifications et des mises à jour à la configuration en cliquant sur l'icône **Modifier** .



Afficher la source

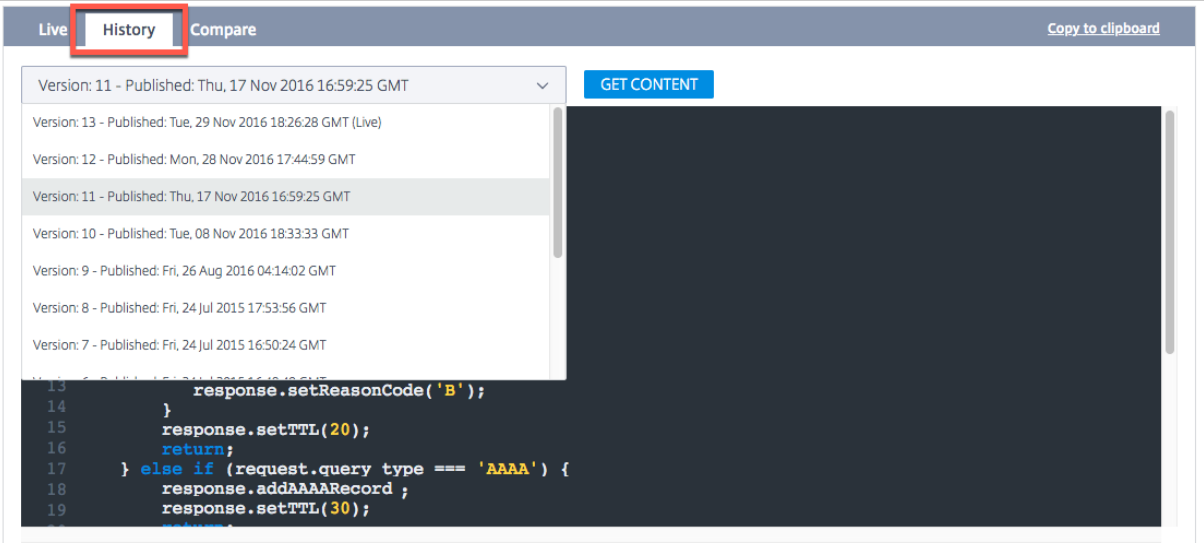
View Source vous permet d'afficher la source JavaScript de l'application, c'est-à-dire la dernière version de l'application, qu'elle ait été publiée ou non. Cette option n'est disponible que pour les applications JavaScript personnalisées.

Voir la version en direct

Vous pouvez afficher, copier et télécharger la dernière version publiée de l'application. Cette option n'est disponible que pour les applications JavaScript personnalisées.

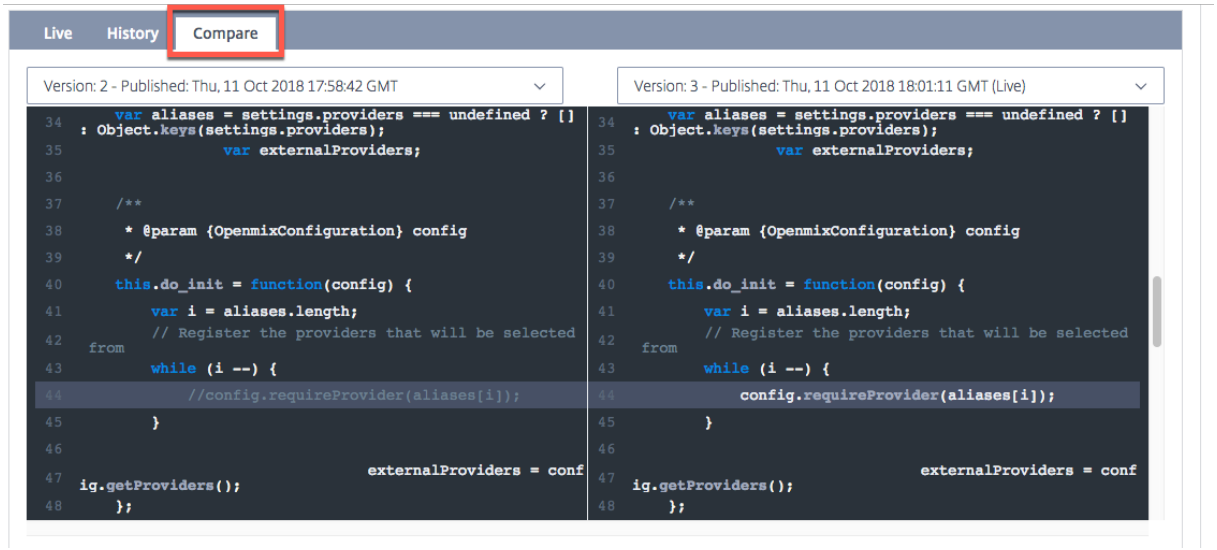
Historique des applications

L'historique des applications vous permet de visualiser différentes versions de l'application. Vous pouvez utiliser la liste **Sélectionner une version** pour passer d'une version en ligne à une ancienne version. Cliquez sur **Obtenir du contenu** pour passer à l'ancienne version. Cette option n'est disponible que pour les applications JavaScript personnalisées.



Comparez

La fonctionnalité **Comparer** vous permet de comparer différentes versions de votre fichier JavaScript. Vous pouvez voir les différences entre les deux versions de votre application clairement affichées avec des lignes de script surlignées.



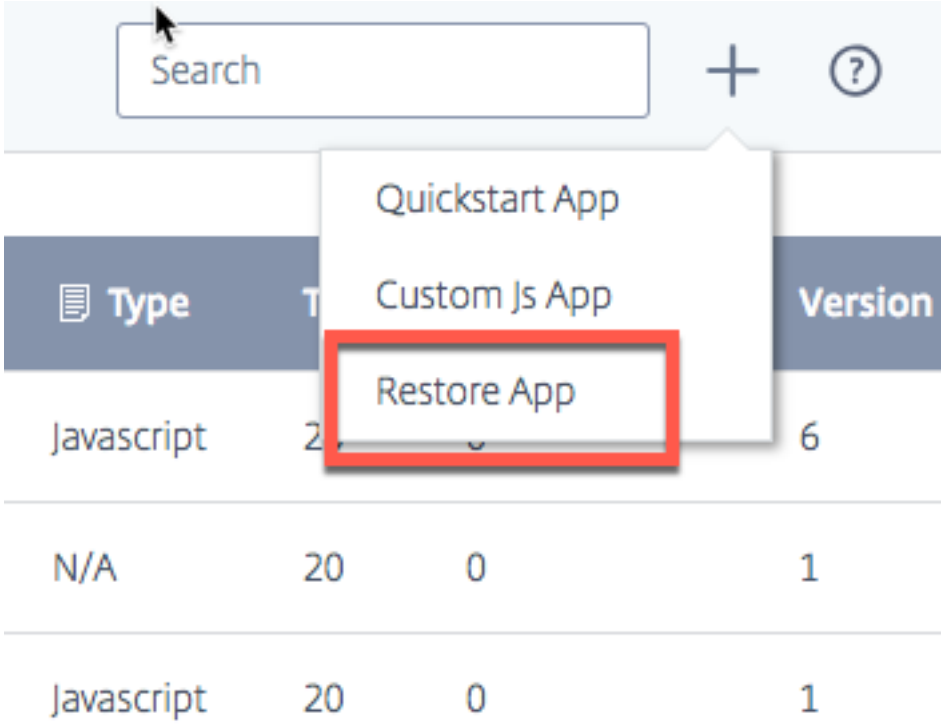
Supprimer

Pour supprimer une application Openmix, cliquez sur le nom de l'application (dans la page de liste des applications Openmix). Le panneau du gestionnaire d'applications s'ouvre. Cliquez sur l'icône **Supprimer**, puis cliquez sur le bouton **Supprimer** dans la boîte de dialogue de confirmation. L'application disparaît de la liste.

Restaurer l'application

La fonctionnalité **Restore App** vous permet de réactiver une application après sa suppression. Pour restaurer une application, procédez comme suit :

1. Cliquez sur l'icône **Ajouter +** en haut à droite de la page.
2. Choisissez **Restore App** dans le menu déroulant. La fenêtre **Restaurer l'application** s'ouvre.



3. Recherchez l'application que vous souhaitez réactiver dans la liste et cliquez sur le bouton **Restaurer** correspondant.

L'application est replacée dans la liste de la page Openmix avec le même statut.

Persistance locale

La fonctionnalité **Persistance locale** offre la capacité de stabilité des décisions lorsqu'elle est activée pour une application Openmix. Les demandes sont identifiées à l'aide du masque de sous-réseau IP, dont la longueur est configurable. Par exemple, lorsqu'un client répète une demande à la même application dans un certain délai, la décision initiale est notifiée. Cela peut être une fonctionnalité essentielle lorsqu'un client est tenu de ne pas rebondir entre différentes décisions au cours d'une session donnée. Il est disponible pour les applications DNS ou HTTP Openmix.

En raison des restrictions naturelles sous-jacentes au mécanisme, la persistance n'est pas garantie pour 100 % des demandes. L'approche « Best Effort » est appliquée à la place. Les tests ont montré que la précision de persistance attendue se situe entre 95 et 97 %.

> **Remarque :**
>
> Pour activer la fonctionnalité Persistance locale pour votre compte, ouvrez un ticket d'assistance ou contactez votre responsable de la réussite client. En outre, une zone DNS prédictive est requise, configurée avec des serveurs de noms `ns5.cedexis.net` et `ns6.cedexis.net`.

> Tenez compte du temps considérable que les mises à jour de zone DNS peuvent nécessiter pour se propager sur Internet.

Configuration

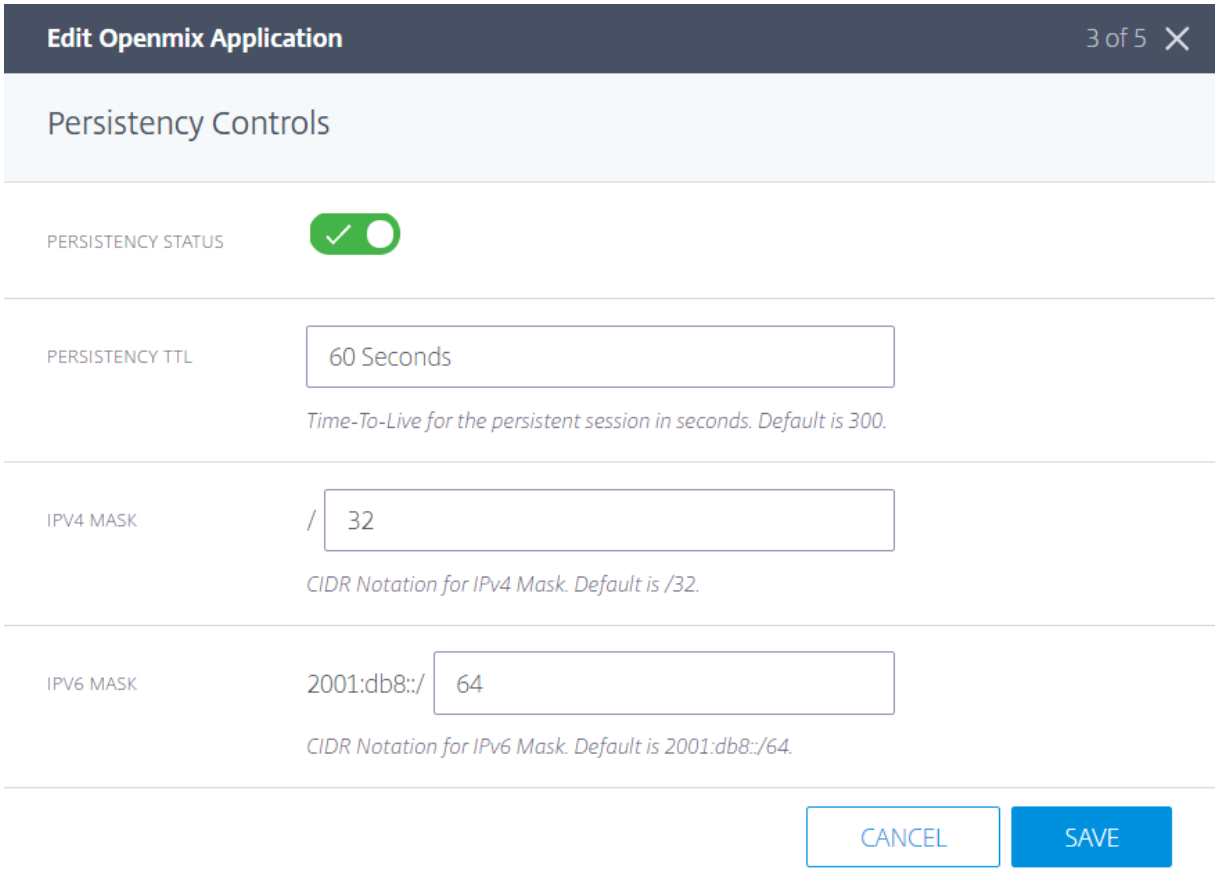
Pour activer la persistance locale, sélectionnez **Contrôles de persistance > Modifier**, sous les options de l'application Openmix.

Les paramètres disponibles sont les suivants :

1. Dans la boîte de dialogue Configuration, entrez la **durée de vie de persistance**. L'option par défaut est de 300 secondes. Les valeurs comprises entre 60 et 1 440 sont autorisées. Après une demande initiale, la décision DNS rendue est conservée pendant un maximum de 300 secondes. Si une autre demande provient de la même plage de sous-réseaux IP du système avant l'expiration, elle prend la même décision.
2. Des masques IPv4 et IPv6 sont fournis pour définir la granularité de la persistance. La valeur par défaut est "/32"et "/64", respectivement pour IPv4 et IPv6. Les valeurs autorisées sont les suivantes :

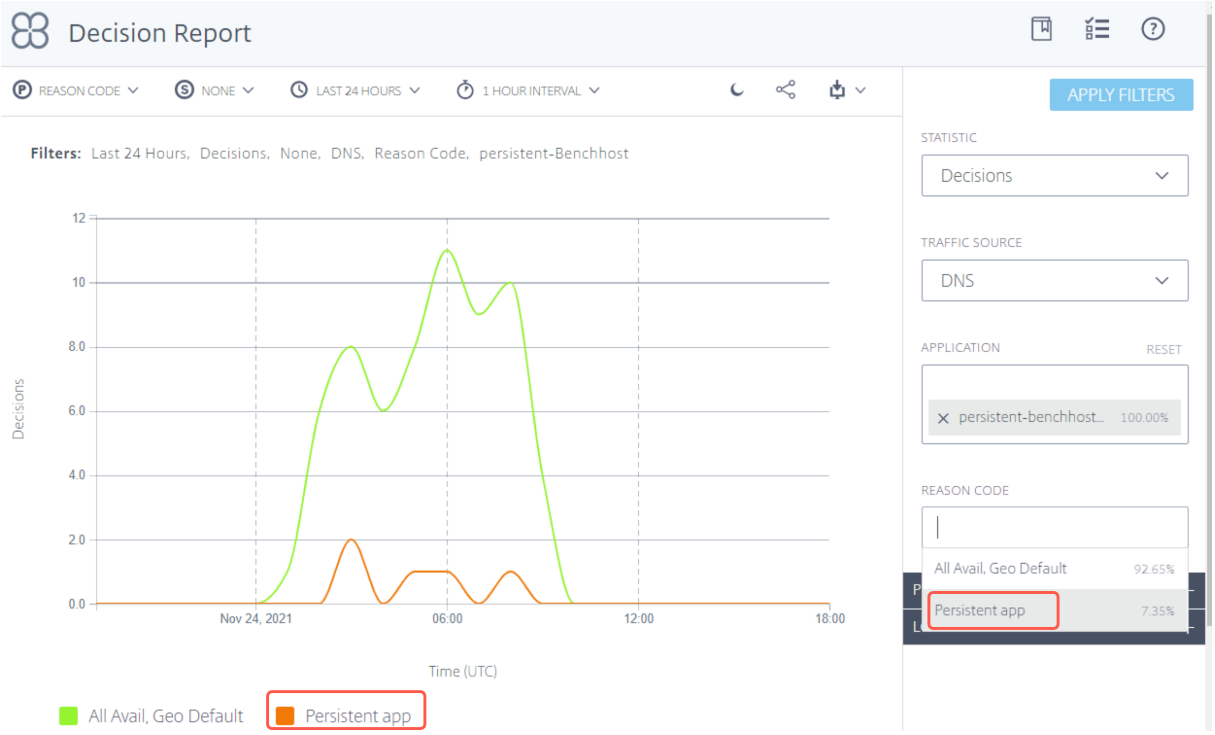
   - /8 à /32, pour IPv4
   - /32 jusqu'à /64, pour IPv6

   Ce masquage de l'adresse IP du client détermine la clé de persistance utilisée dans le magasin de données interne. Par exemple, si deux adresses IP client (ou plus) sont mappées à la même adresse IP masquée, elles sont traitées avec la même décision persistante.



Les mêmes paramètres sont également disponibles dans les paramètres de l'application prédictive.

Les décisions Openmix qui sont fournies via le magasin de données interne sont signalées avec le code de motif **Persistent app** dans le rapport de décision.



Contrôles d'intégrité

Les décisions prises à partir du cache de persistance sont soumises à des contrôles de santé supplémentaires avant d'être prises en charge :

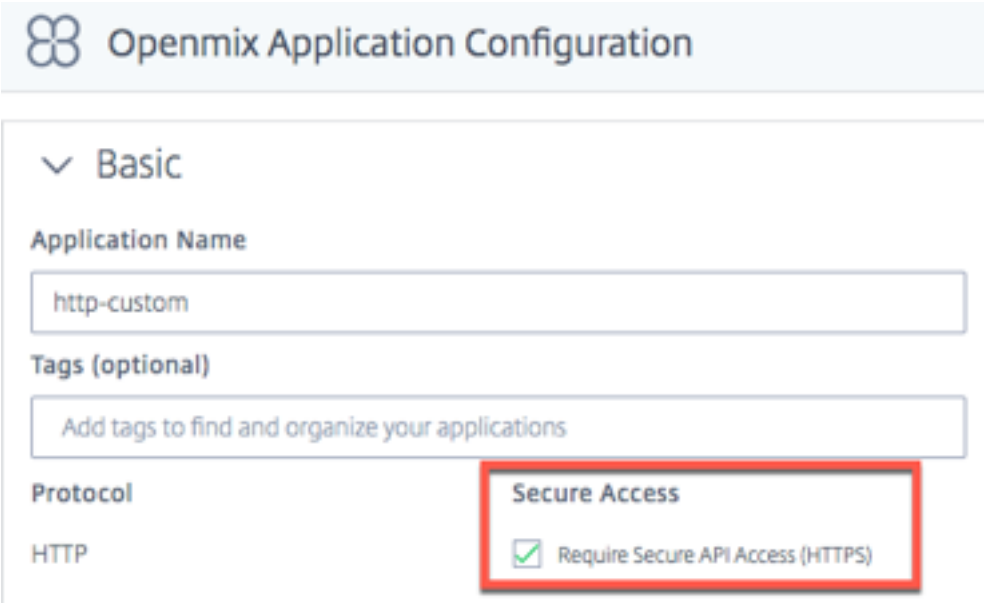
1. Si l'application est configurée avec **Sonar Availability Check**, l'intégrité de la disponibilité du Sonar est vérifiée avant qu'une décision mise en cache ne soit rendue. Si Sonar indique que la plateforme est « en panne », la décision mise en cache est ignorée et l'application OpenMix est de nouveau exécutée.
2. Si l'application est configurée avec **Radar Availability Check**, l'intégrité de la disponibilité du radar est vérifiée avant qu'une décision mise en cache ne soit rendue. Si la disponibilité de la plateforme est inférieure au seuil configuré, la décision mise en cache est ignorée.

> **Remarque :**
>
> Pour la persistance, le seuil maximal de santé de disponibilité du radar est défini sur 10 % fixe.

Sécurisation de l'API HTTP Openmix

Openmix est disponible via DNS ou une API HTTP pour une intégration dans des flux de travail non DNS. Par défaut, l'API HTTP est appelée via HTTP brut. L'API peut également être sécurisée via TLS

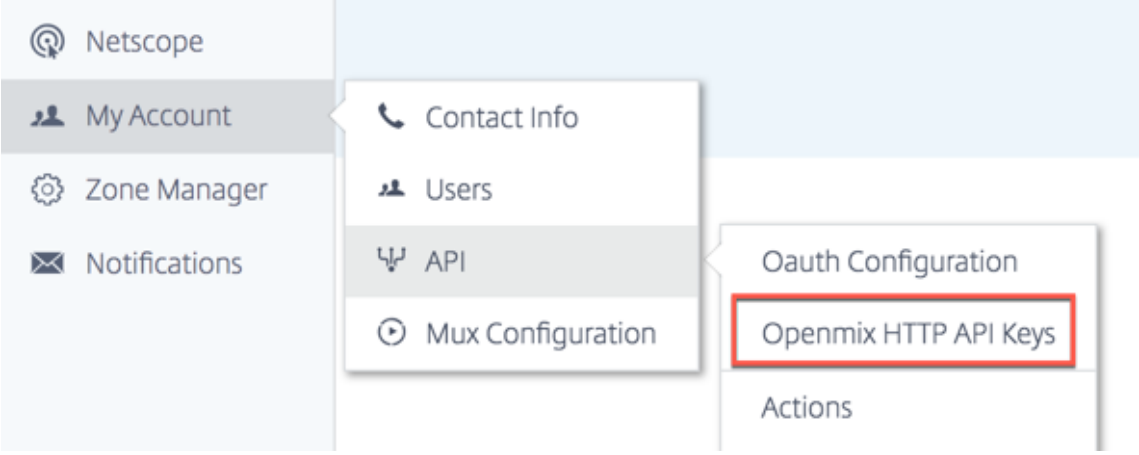
et l'authentification par clé. Cela se fait via l'interface utilisateur en cochant la case **Require Secure API Access (HTTPS)**.



Création de clés d'API

Pour activer l'authentification par clé, procédez comme suit.

1. Cochez **la case Require Secure API Access (HTTPS)** dans la page **Openmix Application Configuration** pour activer l'accès sécurisé pour chaque application.
2. Pour générer une clé d'accès sécurisée, accédez à **Mon compte** -> **API** -> **Clés API HTTP Openmix**



3. Si vous êtes un nouvel utilisateur, vous êtes invité à commencer en saisissant votre ID client. Entrez votre **ID client** dans la boîte de dialogue **Nouveau client**, puis cliquez sur **Terminer** .

4. La clé **secrète du client** est affichée à côté de l'**ID client** sur la page **Configuration de l'authentification de l'API HTTP Openmix** .

5. Vous pouvez maintenant faire une demande à l'application Openmix en utilisant l'authentification de base. Utilisez votre **ID client** comme nom d'utilisateur et le **secret client** comme mot de passe pour appeler l'application sur le navigateur.

   Pour appeler l'application à l'aide de la ligne de commande, utilisez la commande cURL suivante :

```
curl https://hopx.cedexis.com/zones/<zone>/customers/<customer_id
    >/apps/<app_id>/decision --user <client_key>:<client_secret>
<!--NeedCopy-->
```

Remarque : Les clés que vous créez vous donnent accès à n'importe laquelle de vos applications Openmix.

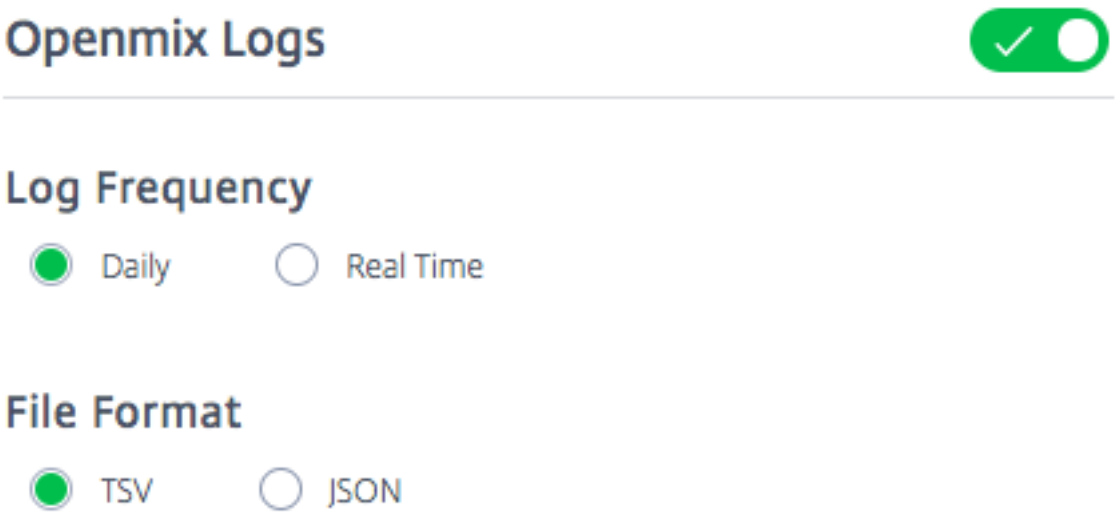
Pour plus d'informations sur l'appel de l'API HTTP Openmix, consultez la documentation d'utilisation de l'API HTTP Openmix.

Suppression de clés API

1. Pour supprimer une clé, accédez à la page **Configuration de l'authentification de l'API HTTP Openmix** .
2. Cliquez sur l'**ID client**.
3. Choisissez **Supprimer** dans la liste. La clé est retirée du système. Il n'est pas valide pour l'authentification ou l'accès sécurisé à l'application Openmix.

Accès aux journaux

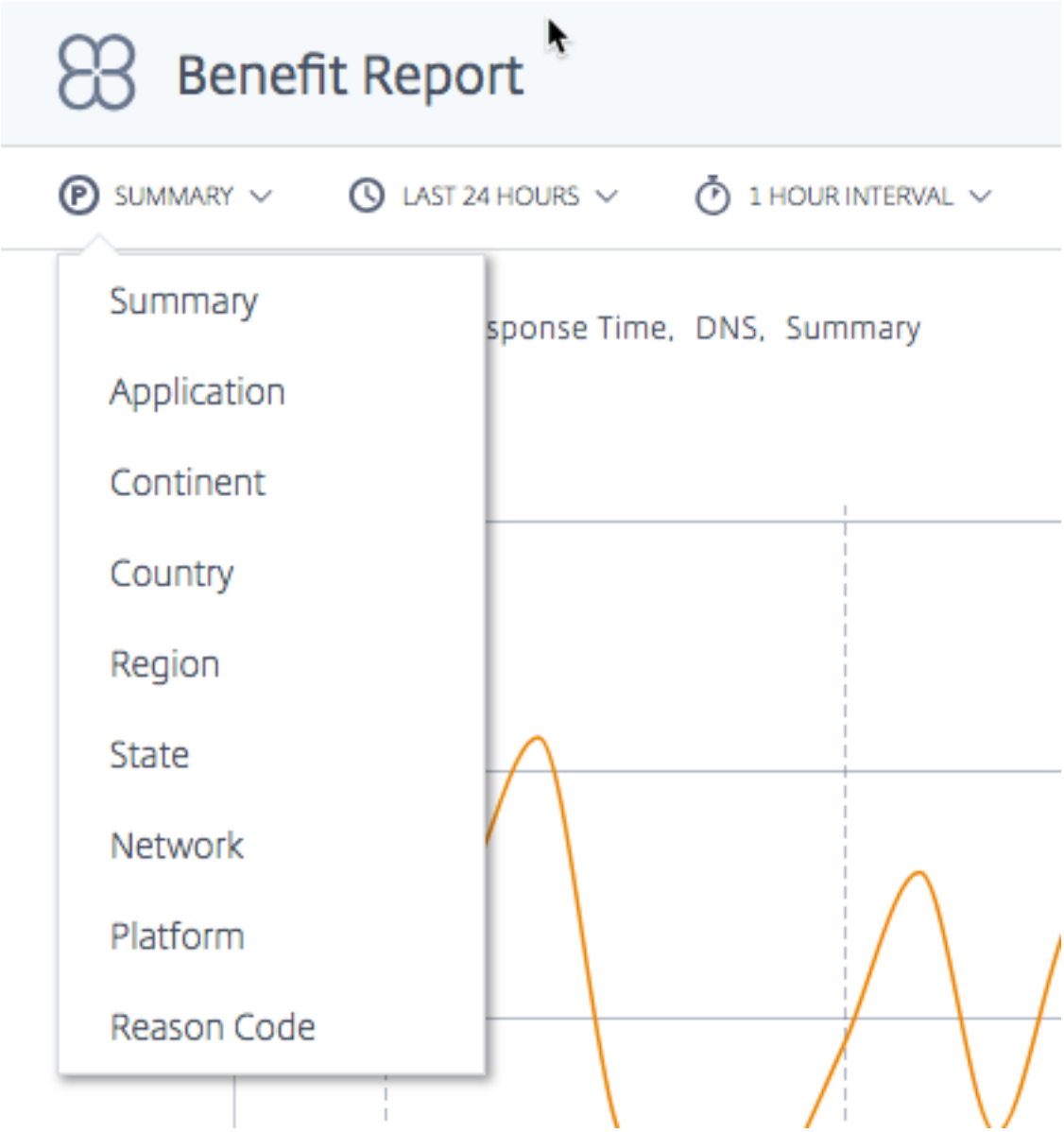
Le journal des décisions prises par Openmix peut être collecté et mis à disposition pour un téléchargement sécurisé. Ces journaux peuvent vous aider à analyser les décisions prises par votre application Openmix et le comportement des demandes de débogage. Les journaux peuvent être activés/désactivés et sécurisés au niveau du compte. Pour plus de détails sur l'activation et le téléchargement des journaux Openmix et voir la description des journaux, rendez-vous sur Netscope.



Rapports Openmix

Les rapports Openmix fournissent une visibilité puissante sur les décisions Openmix prises pour votre trafic DNS ou HTTP. Chaque rapport est défini dans la section suivante, mais voici quelques aspects importants concernant les rapports :

Dimensions principales et secondaires

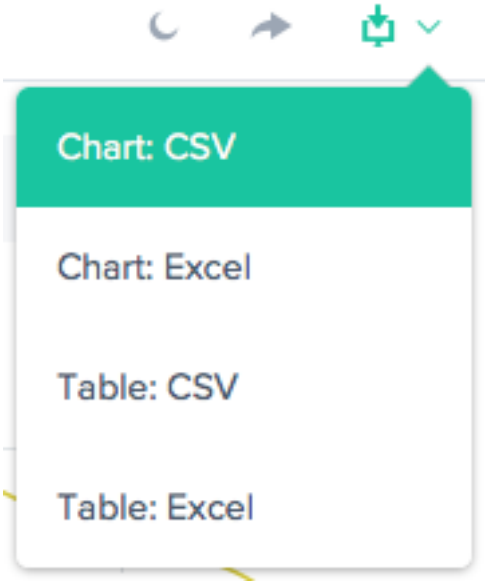


La dimension principale du graphique est sélectionnée dans une liste située au-dessus du graphique. Utilisez cette liste comme un puissant pivot du rapport. Une dimension secondaire peut également être choisie pour affiner davantage le reporting.

Contexte de visualisation Basculer

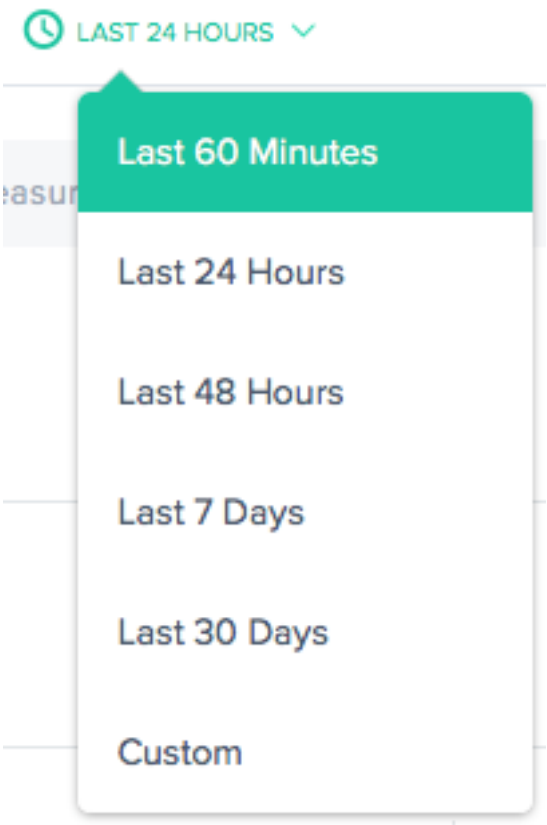
Par défaut, les graphiques sont définis sur un fond blanc. Basculez l'arrière-plan sur une couleur foncée pour les moniteurs à contraste élevé à l'aide de la bascule d'arrière-plan.

Export de données



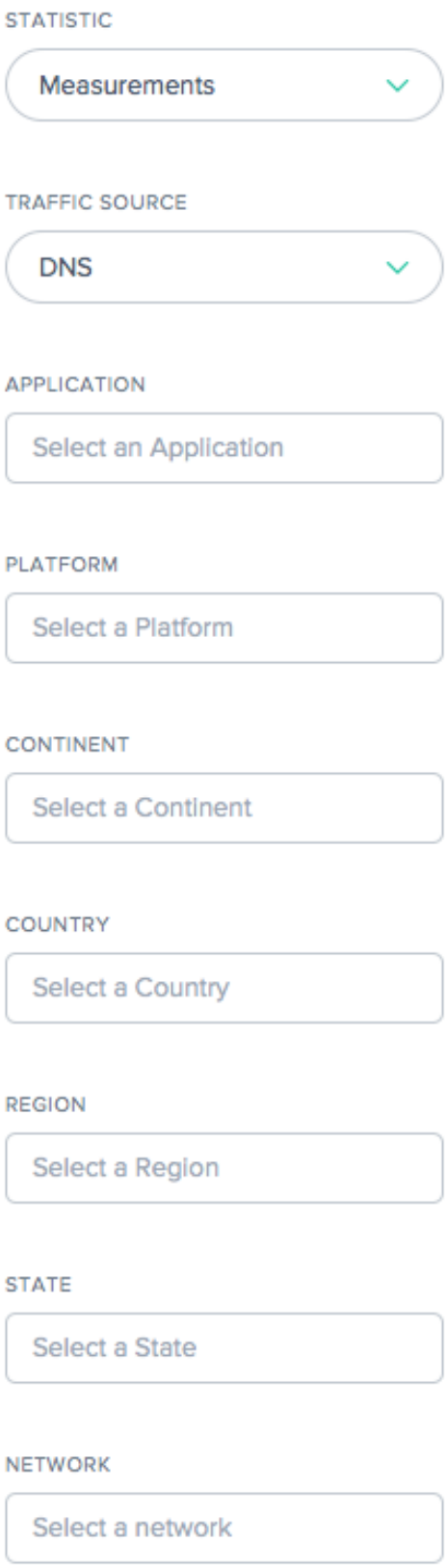
En outre, l'utilisateur final peut télécharger les données du graphique et du tableau via le lien de téléchargement en haut du rapport.

Filtre : Période du rapport



Vous pouvez générer un rapport avec une période de 60 minutes, 24 heures, 48 heures, 7 jours, 30 jours ou une plage personnalisée. La vue par défaut est la dernière 24 heures.

Filtres : puissantes fonctionnalités d'exploration



Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les plus courantes sont les suivantes :

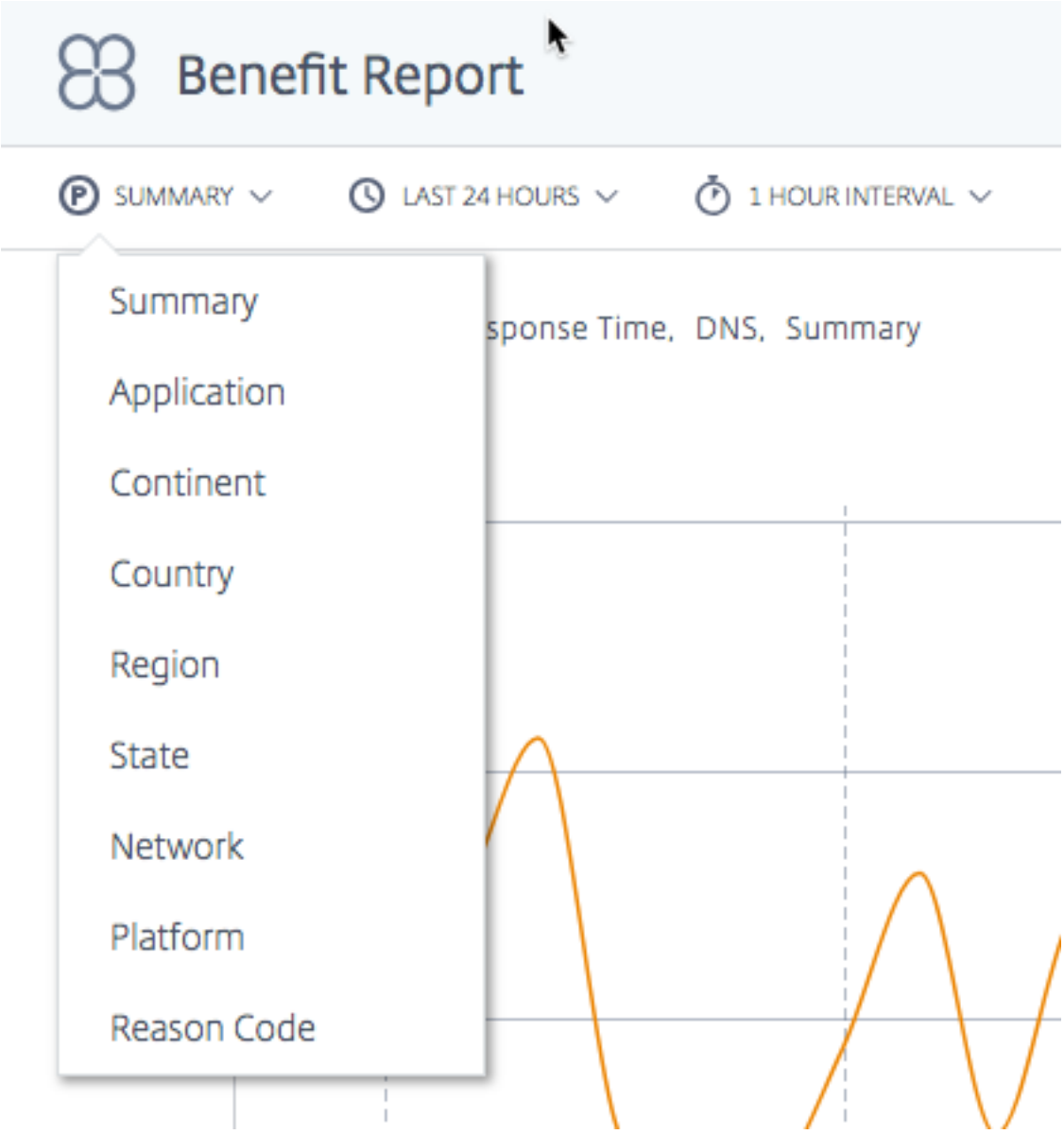
- **Statistique** - Sélectionnez la valeur affichée dans le graphique, le plus souvent le nombre de décisions.
- **Source du trafic** : sélectionnez le type de trafic à afficher : DNS ou HTTP.
- **Application** : sélectionnez une ou plusieurs applications Openmix à afficher.
- **Plateforme** : sélectionnez une ou plusieurs plateformes (fournisseur) à inclure.
- **Continent** : sélectionnez un ou plusieurs continents à inclure.
- **Pays** : sélectionnez un ou plusieurs pays à inclure.
- **Région** : sélectionnez une ou plusieurs régions géographiques (le cas échéant) à inclure.
- **État** : sélectionnez un ou plusieurs états géographiques (le cas échéant) à inclure.
- **Réseau** : sélectionnez un ou plusieurs réseaux (ASN) à inclure.

Rapport sur les avantages

Le rapport Benefit indique l'amélioration globale des performances de mise à disposition de vos applications lorsque vous utilisez le service NetScaler Intelligent Traffic Management (ITM). L'avantage se traduit par une amélioration en pourcentage du temps de réponse et du débit. Choisissez une plate-forme spécifique dans le pool de plateformes candidates pour générer le rapport.

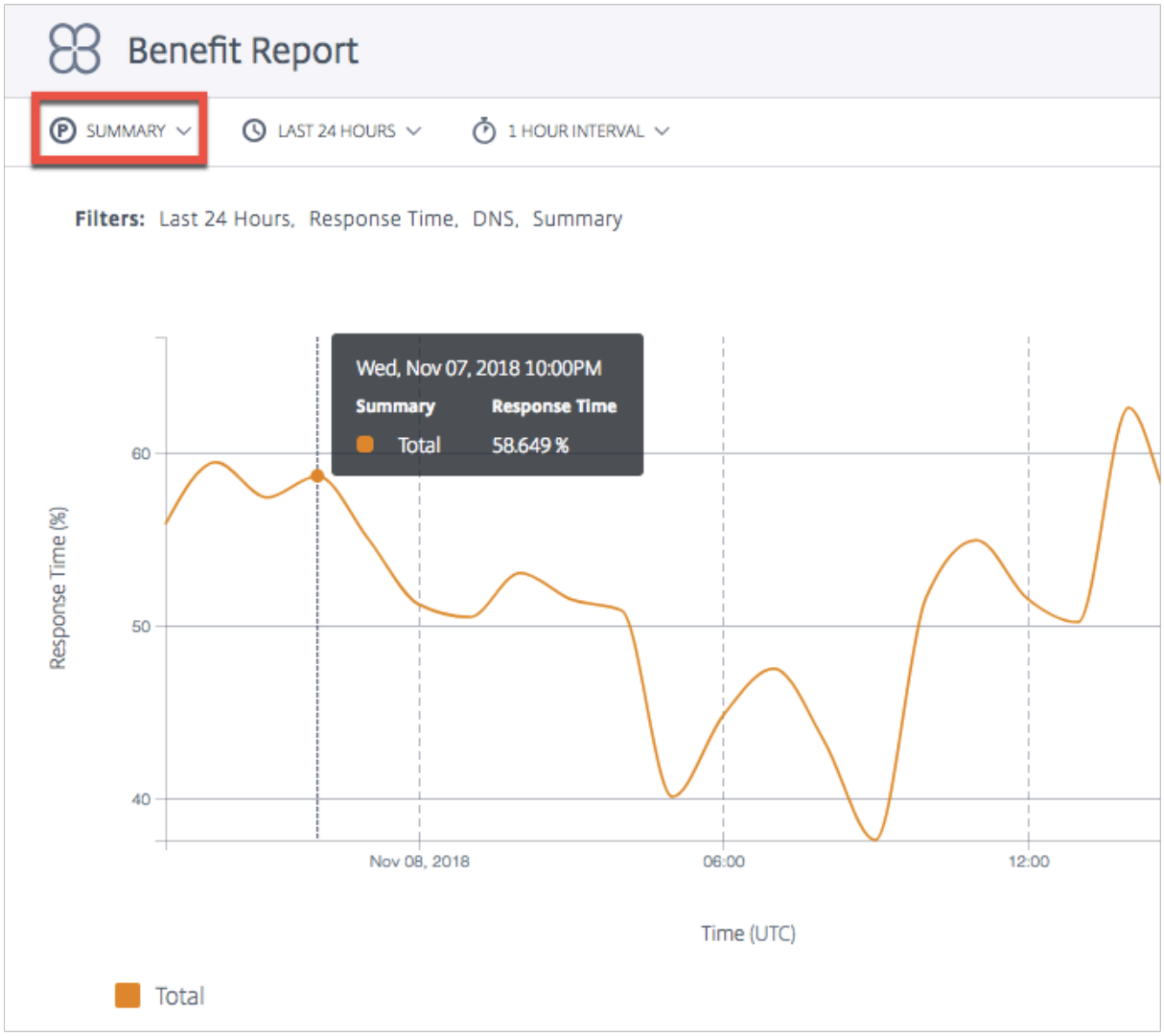
Dimensions principales du rapport sur les avantages

Les dimensions principales sont des mesures indépendantes sur la base desquelles le rapport sur les avantages est affiché. Les sections suivantes décrivent chacune de ces dimensions principales en détail.



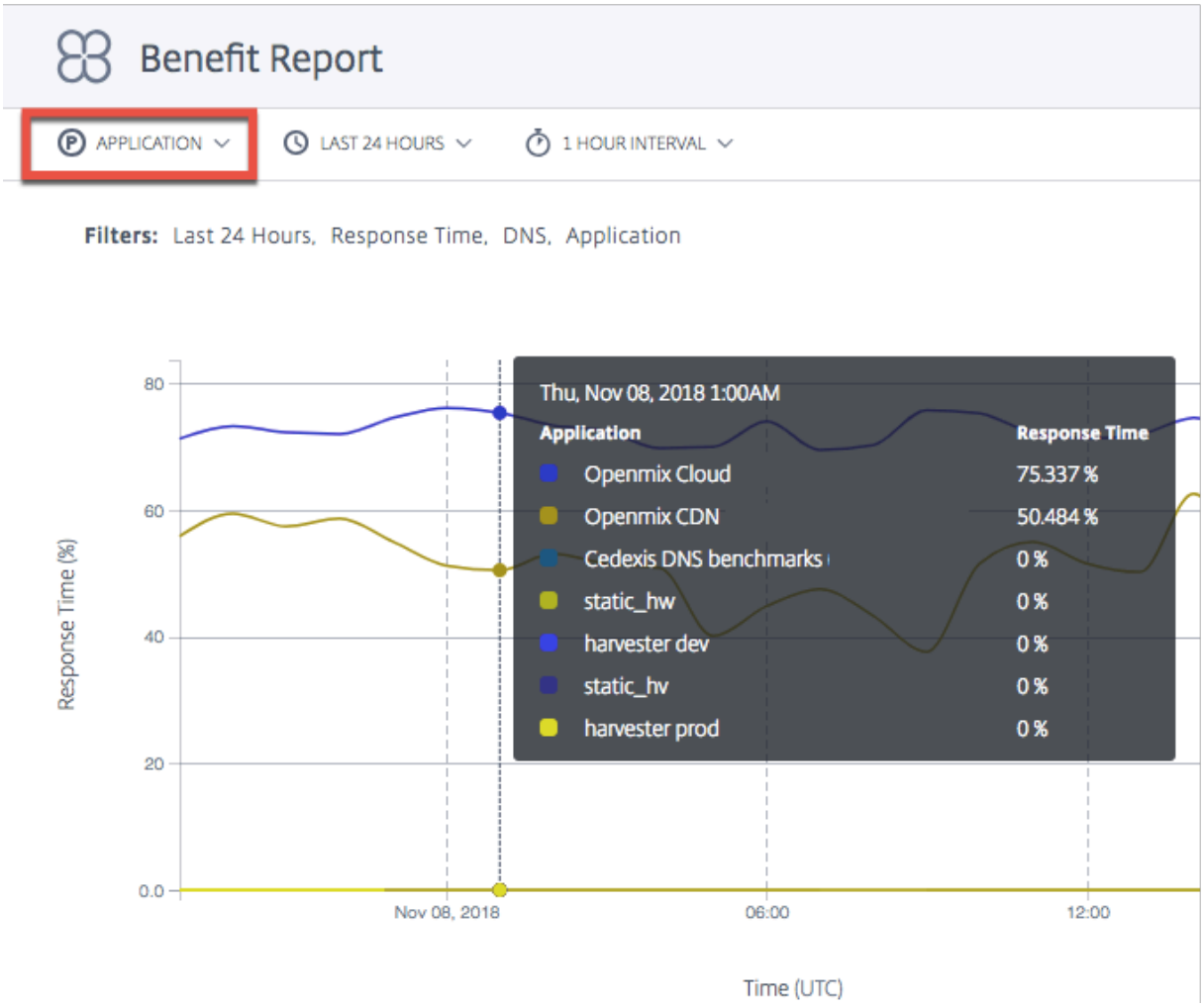
Résumé **Summary** est la dimension principale par défaut. Le graphique récapitulatif montre la moyenne du pourcentage total d'avantages (en termes de temps de réponse ou de débit) reçu de toutes les applications.

Remarque : Vous pouvez alterner entre les avantages affichés en termes de **temps de réponse** ou de **débit** en utilisant le filtre **Statistique** .



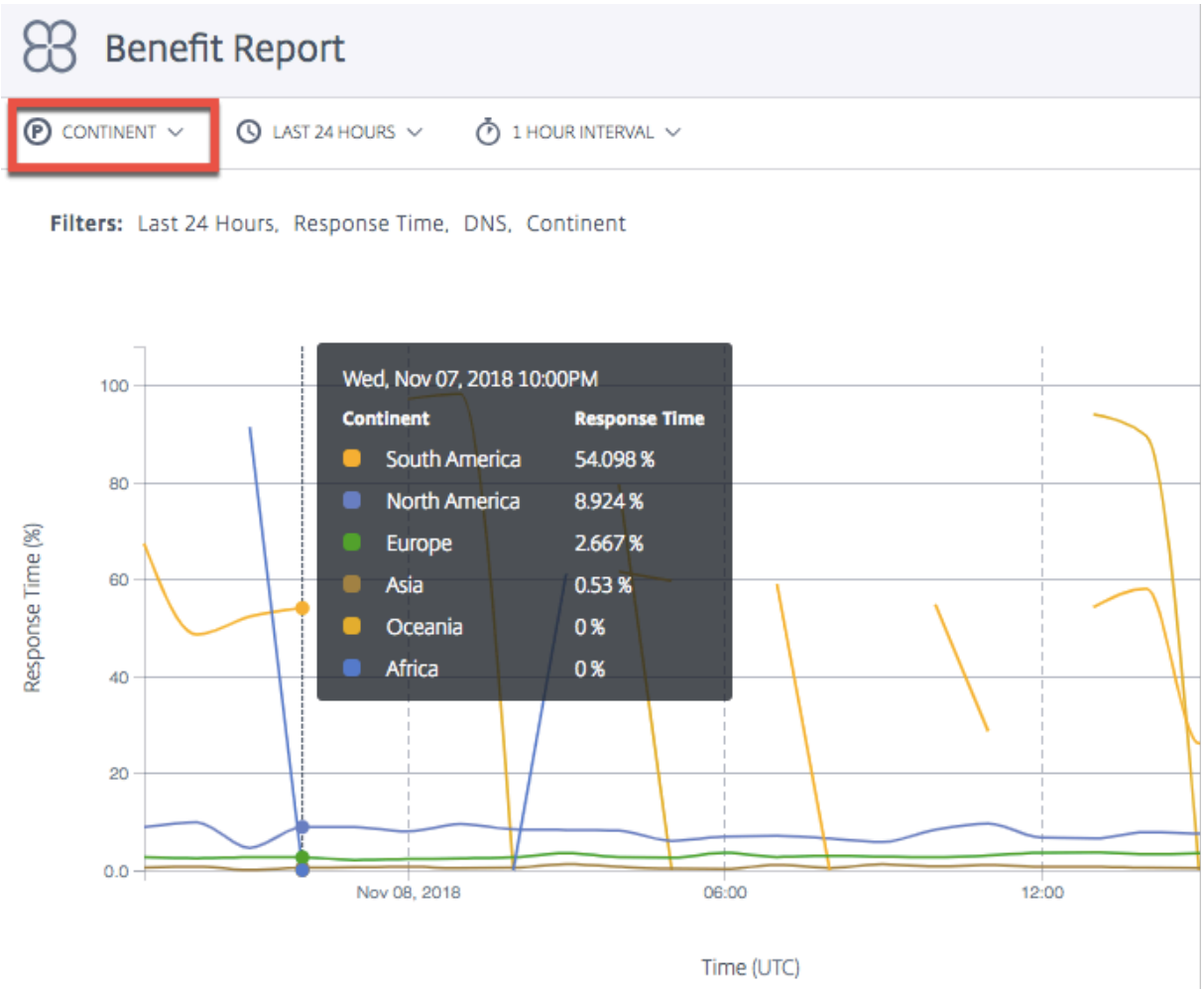
Application Lorsque **Application** est choisie comme dimension principale, le graphique montre chacune des applications et les performances correspondantes (en termes de temps de réponse ou de débit) sous forme de pourcentage d'avantage dans le choix d'une certaine plate-forme par rapport à d'autres plateformes candidates.

Remarque : 0 % signifie qu'il n'y a pas eu d'avantage ou d'amélioration supplémentaire dans le choix d'une plateforme spécifique plutôt qu'une autre.

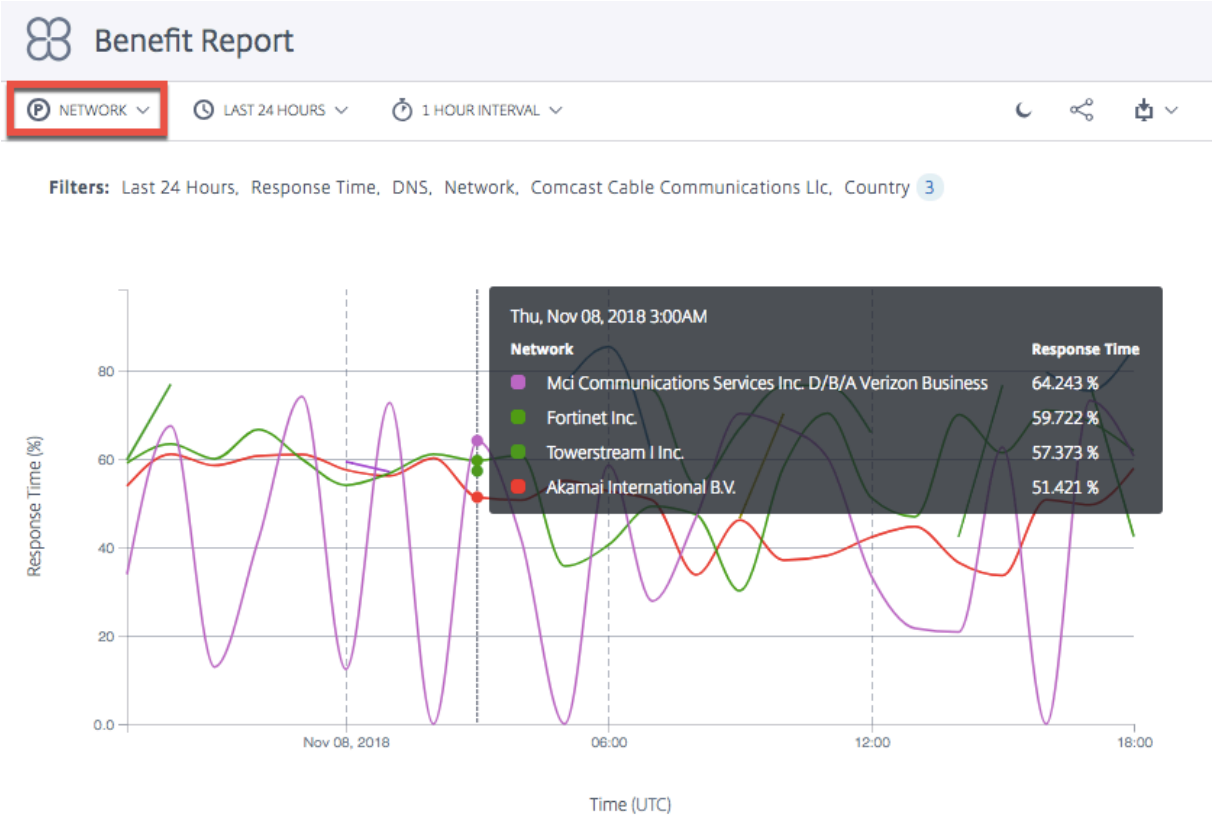


Lieu (continent, pays, région, État) Lorsque l'emplacement (**Continent**, **Pays**, **Région**ou **État**) est sélectionné comme dimension principale, le rapport sur les avantages montre la moyenne du pourcentage total d'amélioration des performances (en termes de temps de réponse ou de débit) pour chaque emplacement. Vous pouvez sélectionner l'emplacement par continent, pays, région ou État.

Remarque : Les plateformes qui ne sont pas éligibles à la sélection en raison de règles géographiques ou pour toute autre raison ne sont pas prises en compte dans le calcul. Cependant, les plateformes géo-clôturées pour l'emplacement en question sont comptées.

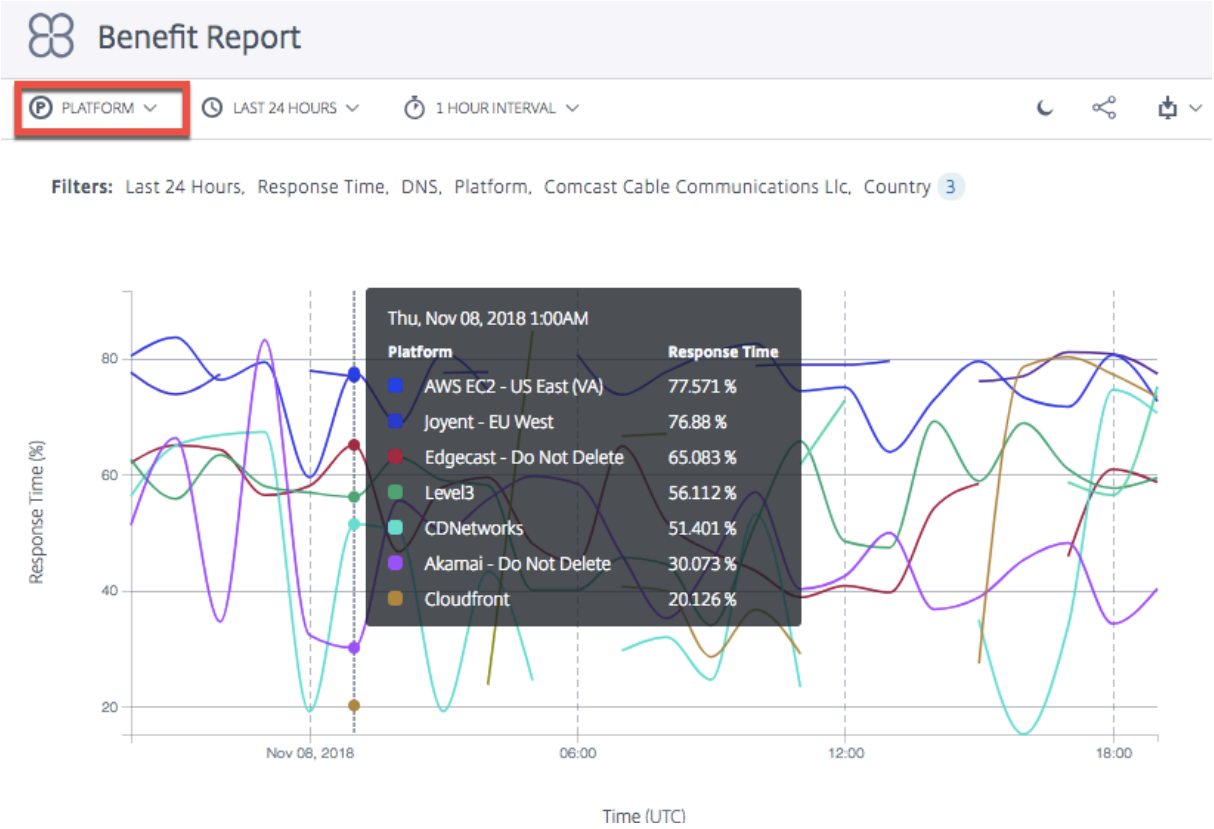


Réseau Lorsque vous sélectionnez **Réseau** comme dimension principale, vous voyez le pourcentage d'amélioration des performances des utilisateurs regroupés dans les réseaux spécifiques (ou fournisseurs de services) à partir desquels les utilisateurs accèdent à ITM. Il vous permet de savoir quels groupes d'utilisateurs voient les avantages en termes de performances lorsqu'ils proviennent de ces réseaux spécifiques.

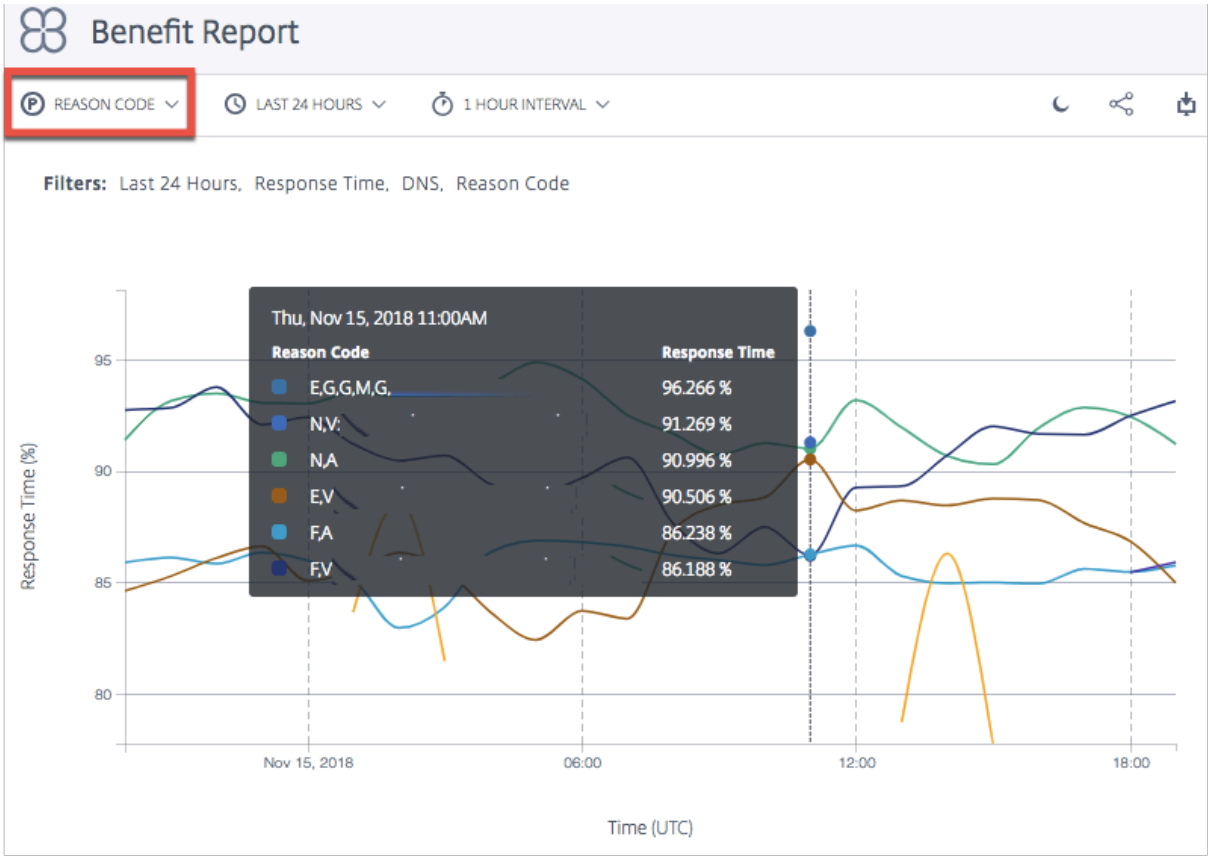


Plateforme Lorsque vous sélectionnez **Plateforme** comme dimension principale, vous voyez les plateformes individuelles choisies par différentes applications et les performances améliorées correspondantes lorsqu'elles sont choisies. L'amélioration des performances ou des avantages se situe en termes de temps de réponse ou de débit (en pourcentage).

Remarque : Le pourcentage d'amélioration des performances affiché lorsqu'une application choisit cette plateforme. La liste sur le graphique n'indique pas nécessairement un classement des performances entre ces plateformes.



Code motif Lorsque vous sélectionnez **Code de raison** comme dimension principale, le pourcentage indiqué dans le graphique est l'avantage moyen global lorsque des décisions sont prises pour un code de raison spécifique.



Ignorer les plateformes dans le rapport

Pour améliorer la précision des décisions d'**Openmix** pour votre rapport sur les avantages, vous pouvez choisir d'ignorer certaines plateformes et de configurer l'application pour qu'elle ne sélectionne que les plateformes les plus adaptées à la comparaison.

Par exemple, votre application dispose de cinq plateformes à prendre en compte à des fins de comparaison : trois en Europe pour le trafic européen et deux aux États-Unis pour le trafic américain. Les règles géographiques précisent que le trafic européen doit passer par les plateformes européennes et le trafic américain via les plateformes américaines.

Pour vous assurer que le calcul est effectué à l'aide des trois plateformes européennes, vous pouvez configurer l'application pour qu'elle ignore les deux autres plateformes non européennes. Utilisez la méthode `ignoredProvider()` dans votre JavaScript.

La méthode prend l'alias du fournisseur (par exemple `provider-1`, `provider-2`) comme argument d'entrée (un peu comme la méthode requireProvider ()). L'API doit être appelée une fois par alias.

Utilisez cet exemple de code dans votre fichier JavaScript au sein de la fonction `onRequest`:

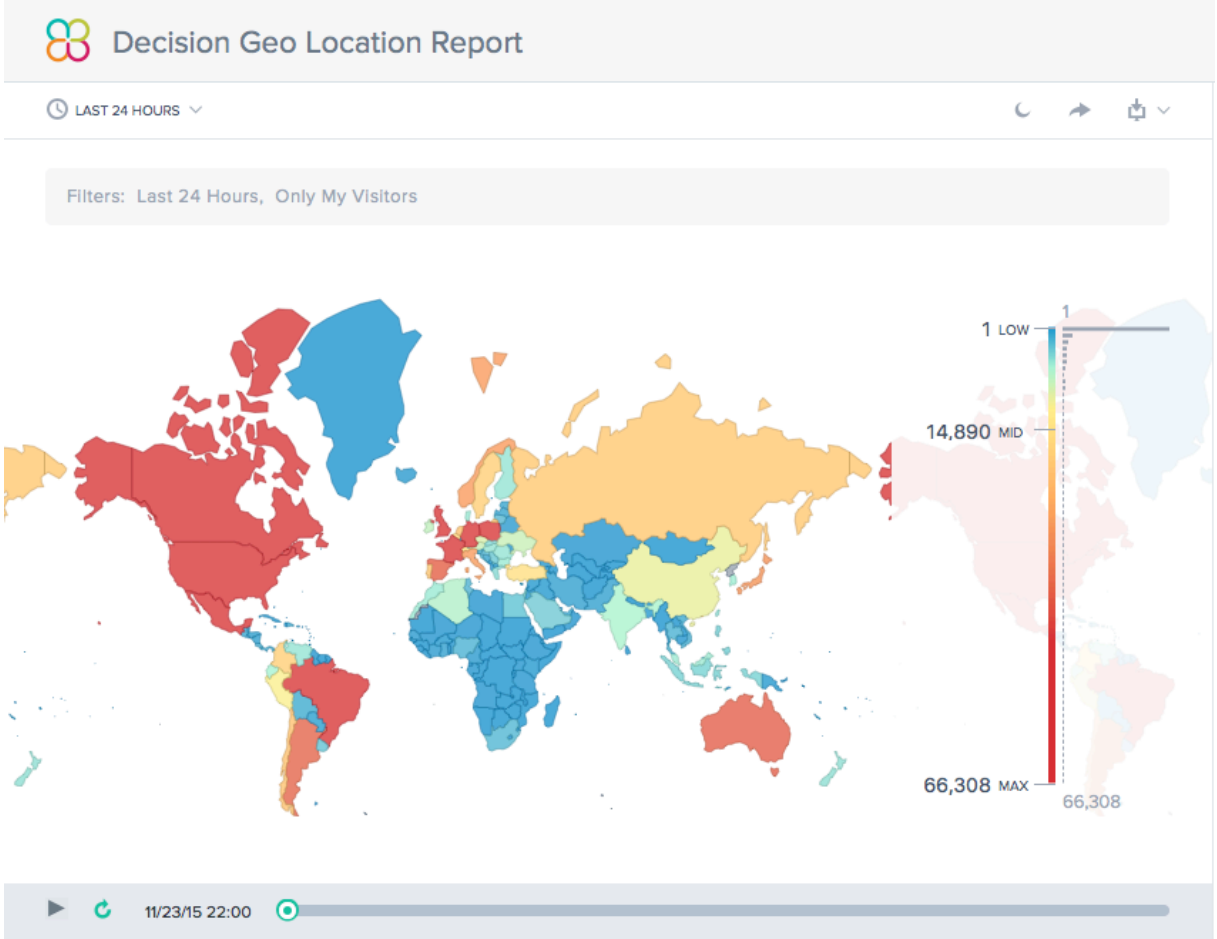

```
function onRequest(request, response) {

  response.ignoredProvider('provider-1');
  response.ignoredProvider('provider-2');
  response.setReasonCode('Ignoring provider-1 and provider-2');
  response.setTTL(this.__defaultTTL);
  response.respond('provider-3', 'cmg.test.fake.cname');
 }

<!--NeedCopy-->
```

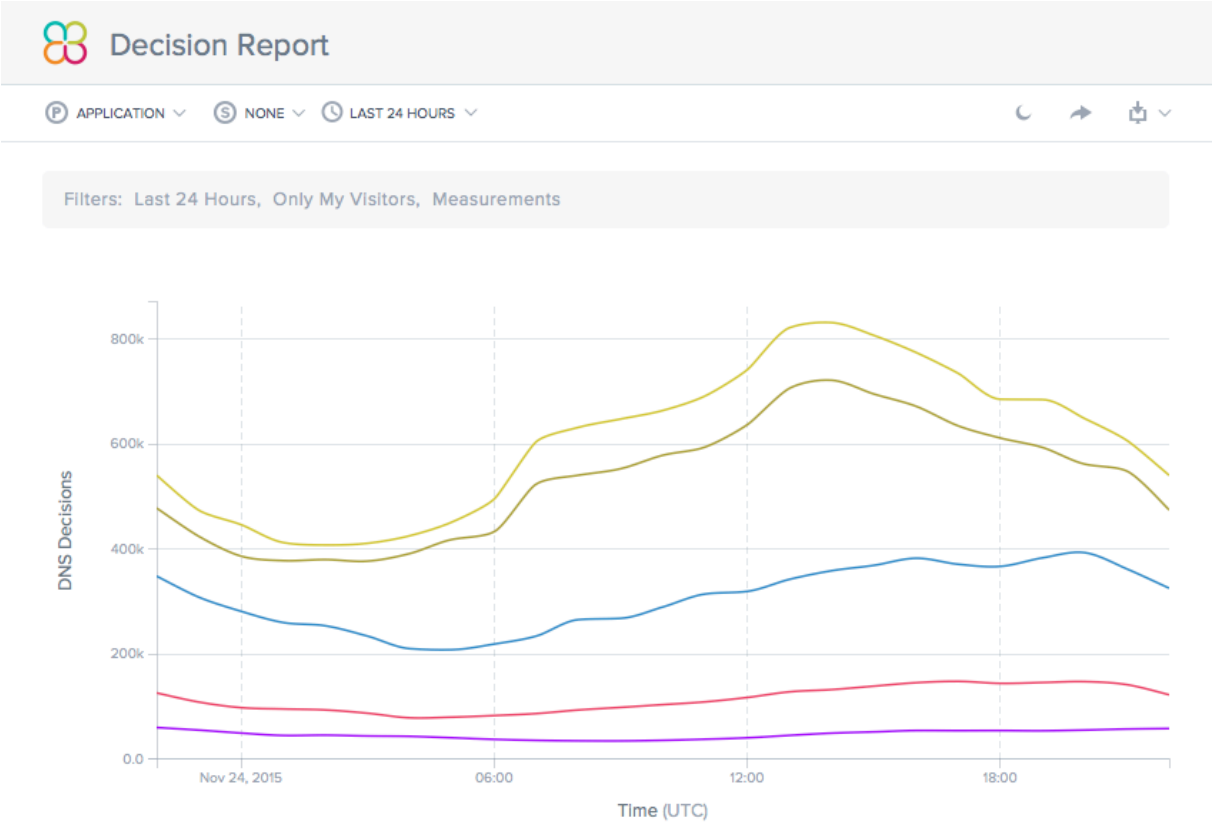
Rapport de décision par géolocalisation

Ce rapport montre le volume de décisions Openmix pour chaque pays. Cette vue cartographique peut être visualisée au fil du temps (en fonction de la plage horaire choisie pour le rapport) en sélectionnant le bouton **Lecture** en bas du graphique.



Rapport de décision

Ce rapport montre la tendance des décisions Openmix pour chacune des applications, plateformes et zones géographiques.



DNS prédictif

September 13, 2023

Vue d'ensemble

Le DNS prédictif est une plateforme DNS autoritaire basée sur l'apprentissage automatique qui gère vos zones et prend des décisions de routage en fonction de la disponibilité des services en temps réel. Il est hautement disponible, avec plusieurs réseaux anycast, qui fournissent des règles de routage flexibles et fiables. Il s'agit d'une offre d'entreprise destinée aux clients DNS sophistiqués qui attachent de l'importance à la qualité de leur processus décisionnel en matière de DNS. Il s'adresse aux clients qui ont besoin de mettre en œuvre une politique de gestion du trafic mondial intelligente, axée sur les données, sur une infrastructure robuste et performante.

Le DNS prédictif prend en charge la création de zones principales et secondaires. L'importation de zones est également prise en charge avec les types d'enregistrement les plus couramment utilisés tels que A (version IPV4), AAAA (version IPV6), NS, SOA, CNAME, MX, PTR, SRV, SPF et TXT. Nous soutenons également les clients d'Openmix grâce à une intégration fluide grâce aux enregistrements de l'application Openmix. N'importe quel nombre d'enregistrements A/AAAA/CNAME dans une zone peut être rendu totalement intelligent avec OpenMix à tout moment. Les clients peuvent également exécuter le DNS prédictif dans un environnement principal double en utilisant notre API pour piloter la configuration.

Points forts de l'intégration du DNS prédictif et d'Openmix

1. Transition fluide entre les enregistrements statiques et une politique sophistiquée de gestion du trafic basée sur les données, sans interruption de service.
2. Politiques de gestion du trafic entièrement configurables (circulaire, distribuée, basée sur la géographie, basée sur le réseau, etc.).
3. Ajout d'une connaissance des données en temps réel sur le trafic Internet mondial, l'état des terminaux, l'état de l'infrastructure, le statut des fournisseurs tiers, etc.
4. Gestion du trafic simple à configurer ou à modifier.
5. Analyses approfondies et rapports sur l'activité des demandes.

Étapes pour configurer et déléguer une zone

Avant de vous connecter au portail de gestion intelligente du trafic NetScaler, voici quelques étapes de base pour vous aider à comprendre comment configurer et déléguer une zone.

Étape 1 : Définissez et créez votre zone

Pour commencer, créez une zone portant le même nom que le nom de domaine de votre entreprise. Une zone représente un domaine parent unique contenant un ensemble d'enregistrements. Il fournit des informations sur la manière dont vous souhaitez acheminer le trafic pour votre domaine et ses sous-domaines. Si vous disposez d'un fichier de zone provenant de votre fournisseur DNS actuel, importez-le. Avec un fichier de zone importé, vous pouvez créer rapidement tous les enregistrements de votre zone.

Étape 2 : Ajoutez et testez vos enregistrements

Vous pouvez soit créer manuellement des enregistrements sur la console DNS prédictive du portail NetScaler Intelligent Traffic Management, soit importer un fichier de zone avec tous ses enreg-

istrements. Lorsque vous importez un fichier de zone, Predictive DNS réplique votre définition de zone d'origine en faisant migrer tous les enregistrements existants qu'il contient.

Vous pouvez également créer des zones et des enregistrements par programmation à l'aide de l'API DNS prédictive. L'API se trouve dans le portail sous **Mes comptes > API > Configuration > authdns**.

Les clients d'Openmix peuvent associer une application Openmix existante à un enregistrement CNAME ou A/AAAA via le type d'enregistrement Openmix App. N'importe quel nombre d'enregistrements A/AAAA/CNAME dans une zone peut être rendu totalement intelligent avec OpenMix à tout moment.

Pour tester les enregistrements de votre zone, vous pouvez utiliser un outil appelé dig qui interroge directement les serveurs DNS. Exécutez dig en utilisant le nom de votre zone comme paramètre.Par exemple :

```
dig @ns1.ourdomain.net NS mydomain.com
```

```
dig @ns1.ourdomain.net A host.mydomain.com
```

`@ns1.ourdomain.net` Indique à dig d'envoyer une requête à l'infrastructure DNS NetScaler Intelligent Traffic Management, et le type d'enregistrement (NS ou A) indique quel enregistrement demander. La commande NS demanderait les enregistrements NS pour la `mydomain.com` zone, et la seconde commande `@ns1.ourdomain.net A host.mydomain.com` serait un enregistrement A pour l'hôte de la `mydomain.com` zone.

Étape 4 : Attribuez NetScaler Intelligent Traffic Management comme DNS officiel en mettant à jour vos serveurs de noms

Pour nous attribuer le rôle de DNS faisant autorité pour gérer votre nom de domaine, mettez à jour les serveurs de noms chargés de répondre à vos requêtes DNS adressées à nos serveurs de noms. Le nouveau serveur de noms NetScaler ITM répondra alors avec autorité pour votre entreprise.

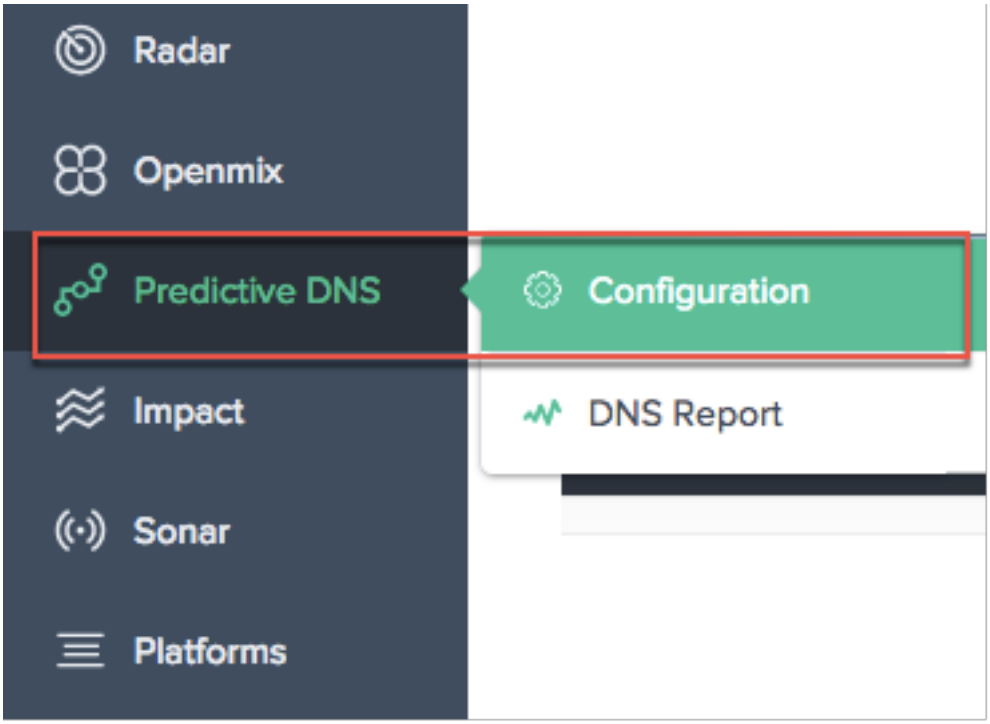
Étape 5 : Valider le flux de trafic de manière appropriée

Au départ, vous voyez du trafic s'exécuter entre les deux systèmes (votre ancien service DNS et Citrix Predictive DNS), en fonction de la longueur du TTL dans le système précédent. La migration complète du trafic peut prendre un certain temps. Si vous rencontrez des erreurs lors de la migration, revenez aux serveurs de noms fournis par votre ancien service DNS, puis déterminez ce qui s'est mal passé. Si le trafic circule comme prévu, cela signifie que vous avez migré avec succès vers Citrix Predictive DNS. Le TTL par défaut ici est de 3 600 secondes. Vous souhaiterez peut-être réduire le TTL dans un premier temps jusqu'à ce que vous vous assuriez que la migration est réussie. Une fois que vous êtes satisfait du flux de trafic, vous pouvez augmenter le TTL pour une durée plus longue, le cas échéant.

Navigation

Pour accéder à la console DNS prédictive, procédez comme suit :

1. Connectez-vous au portail de gestion intelligente du trafic NetScaler.
2. Dans le menu de navigation de gauche, choisissez **DNS prédictif > Configuration**.



Cela vous amène à la page **Ajouter une zone**, où vous pouvez commencer par créer votre zone.

Zones primaires et secondaires

Une zone représente un domaine parent unique contenant une collection d'enregistrements. Vous pouvez configurer votre zone dans Predictive DNS comme zone principale ou secondaire. Le DNS principal et secondaire permet de créer de la redondance dans le DNS. Le primaire est parfois appelé maître tandis que le secondaire est appelé esclave. Cela est dû au fait que le primaire possède la copie principale des données de zone, tandis que le secondaire clone simplement ces données par le biais de transferts de zone à intervalles réguliers ou à la demande du principal.

Ce processus est également souvent appelé transfert de zone ou transfert AXFR. Si vous configurez votre zone principale avec les transferts de zone activés, toutes les modifications apportées à la zone sont automatiquement répercutées sur tous vos serveurs secondaires. Chaque adresse IP saisie en tant que serveur secondaire reçoit cette mise à jour. De même, vous pouvez également configurer une zone secondaire.

Lorsque vous créez une zone, un enregistrement de serveur de noms (NS) et un enregistrement de début d'autorité (SOA) sont automatiquement créés pour la zone. Vous pouvez utiliser l'interface utilisateur du DNS prédictif pour ajouter, modifier, dupliquer ou supprimer des zones.

Remarque : Ces opérations (modification, duplication ou suppression) affectent l'ensemble de la zone, y compris toutes les réponses relatives aux enregistrements de la zone. Ils doivent être effectués avec une extrême prudence.

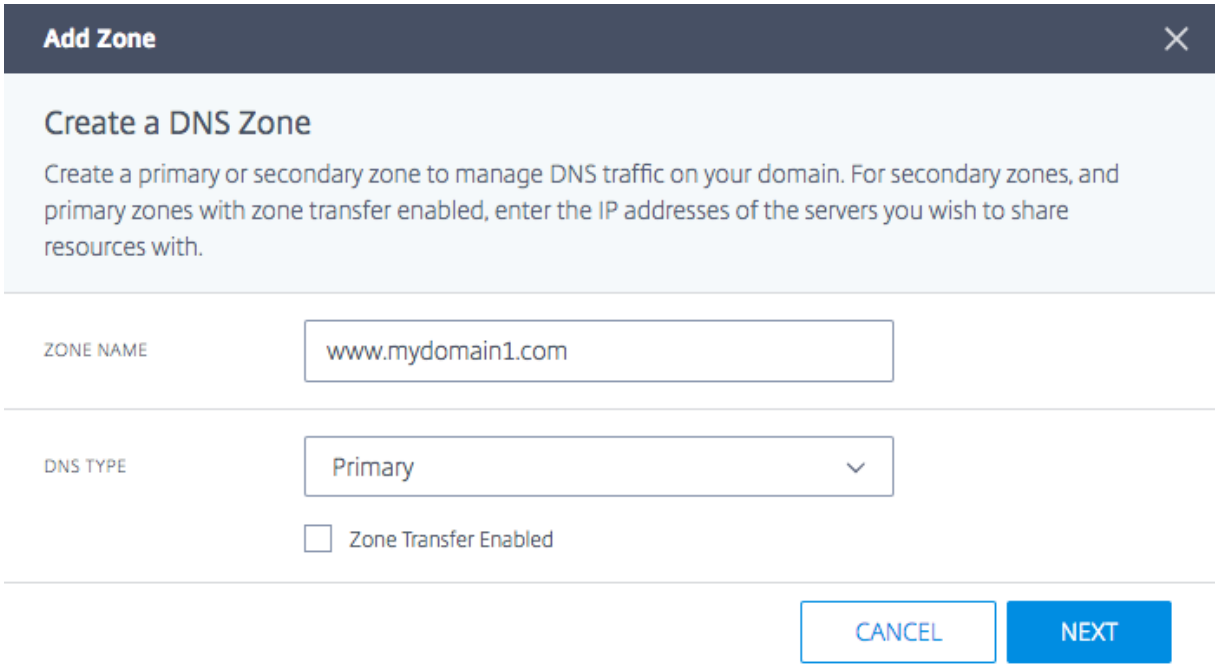
Ajouter une zone

Pour ajouter ou créer une zone :

1. Si c'est la première fois, l'écran de démarrage apparaît où vous pouvez cliquer sur **Ajouter une zone** pour commencer.
2. Cela vous amène à la boîte de dialogue **Ajouter une zone** dans laquelle vous pouvez créer une zone pour votre domaine.

Si ce n'est pas la première fois, vous voyez la liste des zones existantes (noms de domaine) créées pour les domaines de votre entreprise et le nombre d'enregistrements associés à chacune d'entre elles.

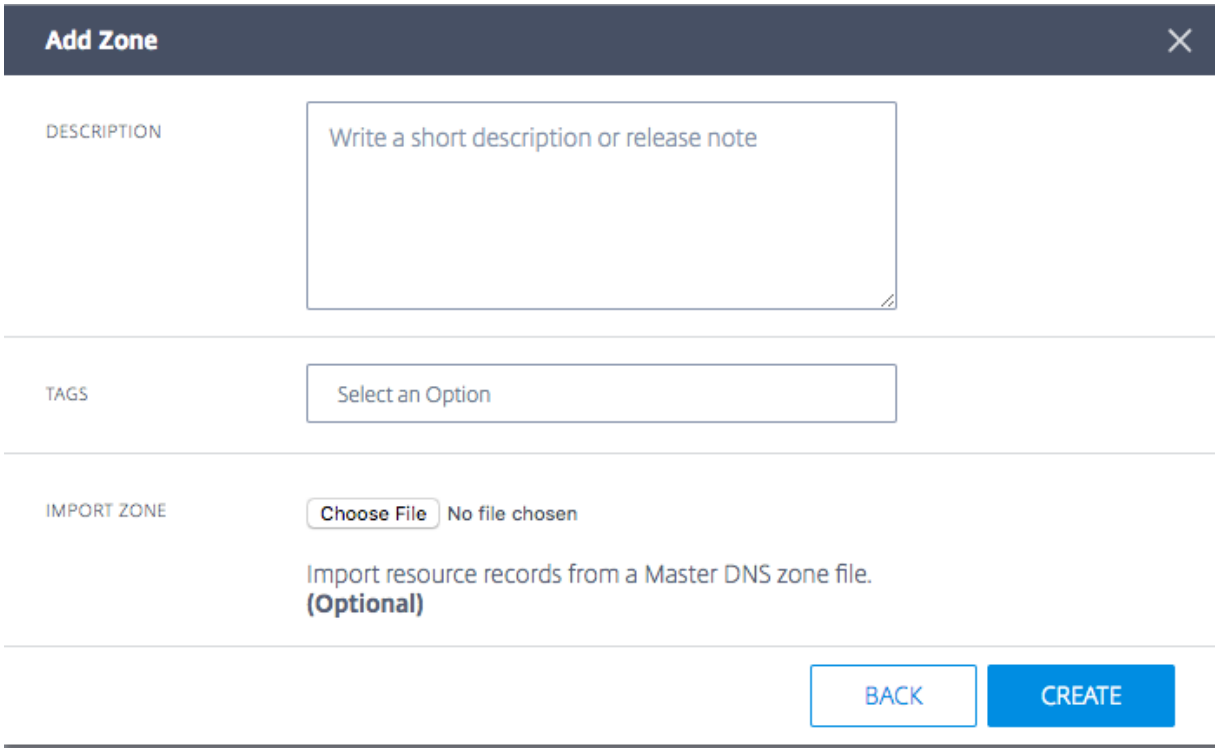
1. Cliquez sur l'icône d'ajout en haut à droite de la page pour commencer à créer une zone.
2. La boîte de dialogue **Ajouter une zone** s'ouvre.



1. Entrez votre nom de domaine comme **nom de zone**. Par exemple `www.mydomain.com`. Le nom de zone doit être globalement unique, ce qui signifie que vous ne pouvez pas créer un

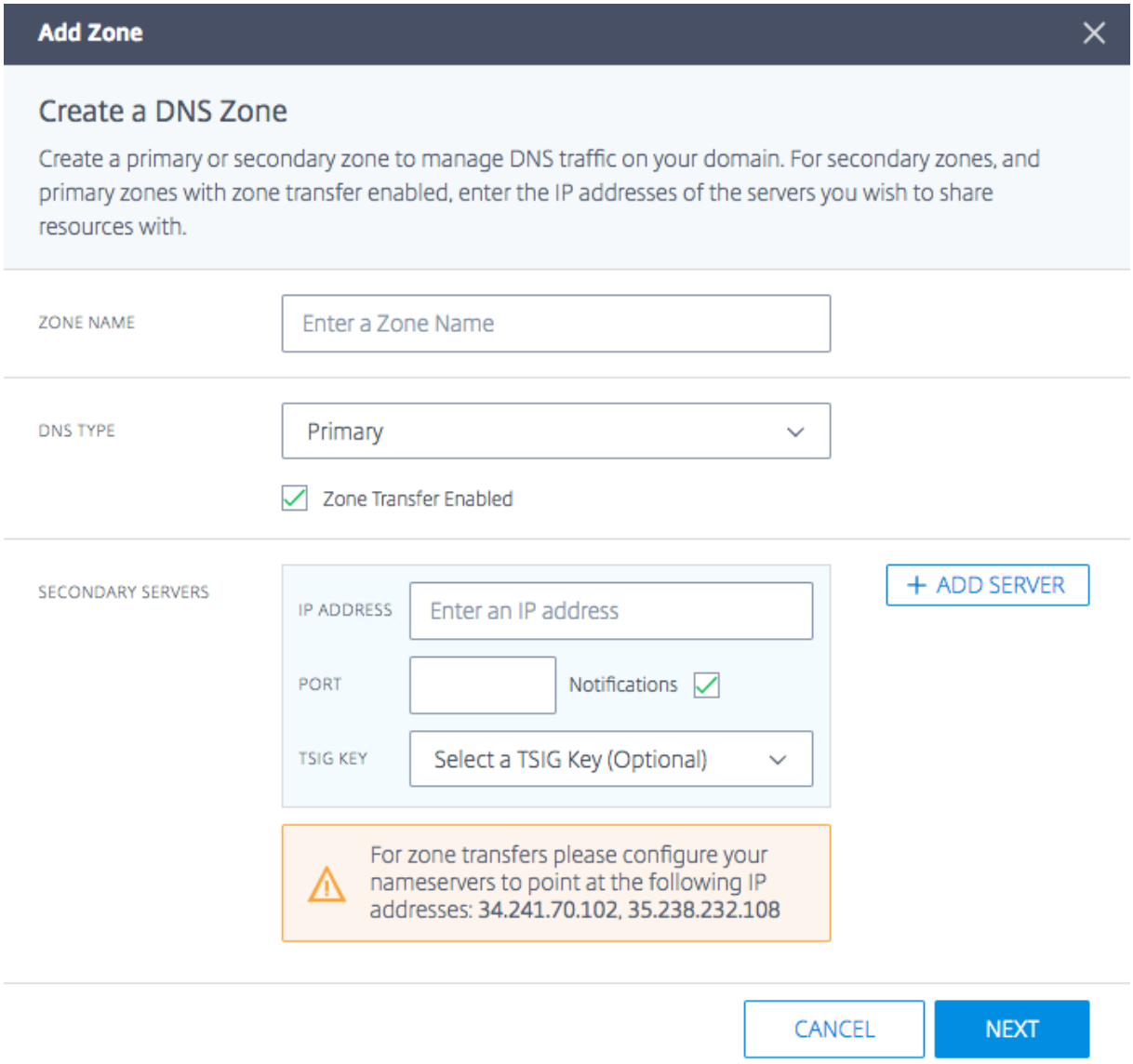
nom de zone existant, ou même partiellement superposé à un nom de zone existant. Toutefois, s'il existe un scénario valide dans lequel vous devez créer un nom de zone susceptible de se chevaucher avec un nom de zone existant, ou si vous ne parvenez pas à créer une zone pour un domaine que vous possédez, contactez le support.

2. Sélectionnez le **type de DNS** comme **principal** ou **secondaire**.
3. Cochez la case **Transfert de zone activé** pour activer le transfert de zone et entrez les informations relatives au serveur **principal** ou **secondaire** . Reportez-vous aux informations sur le serveur pour plus de détails.
4. Cliquez sur **Suivant** pour saisir des informations de zone telles qu'une **description** et des **balises**.
5. Sélectionnez **Choisir un fichier** pour importer un fichier de zone depuis votre machine (si disponible).
6. Cliquez sur **Créer** pour terminer l'ajout d'une nouvelle zone.



Lorsque de nouvelles zones sont créées, elles apparaissent dans la liste de la page **Zones** .

Informations sur le serveur



Adresse IP Entrez l'adresse IP du serveur principal ou secondaire.

Port Entrez le numéro de port associé au serveur. Il s'agit d'un champ facultatif. Il est configurable uniquement pour les serveurs secondaires. S'il est laissé vide, la valeur par défaut est 53.

Notifications Activez les notifications en cochant la case **Notifications** si vous souhaitez que votre DNS principal avertisse le DNS secondaire en cas de mise à jour. Si la case n'est pas cochée, les mises à jour du système principal sont envoyées au système secondaire à intervalles réguliers de 60 minutes.

Ajouter un serveur Le bouton **Ajouter un serveur** vous permet de configurer plusieurs serveurs pour les transferts de zones.

Clé TSIG Vous pouvez sélectionner une **clé TSIG** dans la liste. Cette liste contient les clés que vous créez et gérez dans la section Clés TSIG. Ce champ est facultatif pour une sécurité accrue. Reportez-vous à la section TSIG Keys pour plus d'informations.

Description Ajoutez une brève description ou un commentaire concernant la zone que vous êtes sur le point de créer. Il s'agit d'un champ facultatif, entièrement adapté à vos besoins. Cela n'affecte en rien les réponses DNS réelles.

Balises Les tags vous permettent de trier et de filtrer vos zones dans une liste. Ce champ est également facultatif.

Zone d'importation Si vous disposez d'un fichier d'importation de zone contenant la configuration de votre zone, vous pouvez l'importer ici. Pour importer un fichier de zone, créez d'abord une zone portant le même nom que le fichier que vous importez. Les conditions requises pour l'importation sont les suivantes :

- Le nom de la zone dans le fichier de zone doit correspondre au nom de la zone que vous créez.
- Le fichier de zone utilise un format BIND standard pour les enregistrements.
- Le fichier importé doit avoir un format de fichier de zone défini par RFC.
- Vous pouvez importer un maximum de 5 000 enregistrements. Si vous devez importer plus de 5 000 enregistrements, contactez le support.

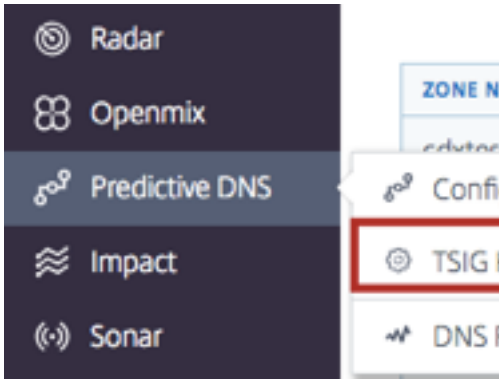
Pour importer un fichier de zone, procédez comme suit :

1. Dans la boîte de dialogue **Ajouter une zone**, accédez à **Zone d'importation**.
2. Cliquez sur **Choisir un fichier**.
3. Sélectionnez le fichier de zone que vous souhaitez utiliser pour remplir la zone.
4. Cliquez sur **Créer** pour terminer le processus.

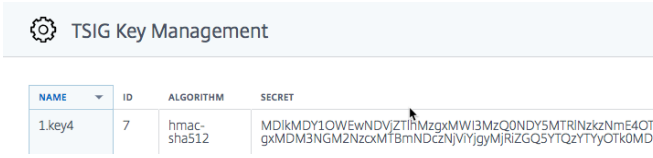
Clés TSIG

Les clés TSIG fournissent un niveau de sécurité supplémentaire pour le partage d'informations entre un serveur principal et un serveur secondaire. Le secret de la clé doit être disponible sur les deux serveurs (principal et secondaire) pour qu'une poignée de main soit réussie.

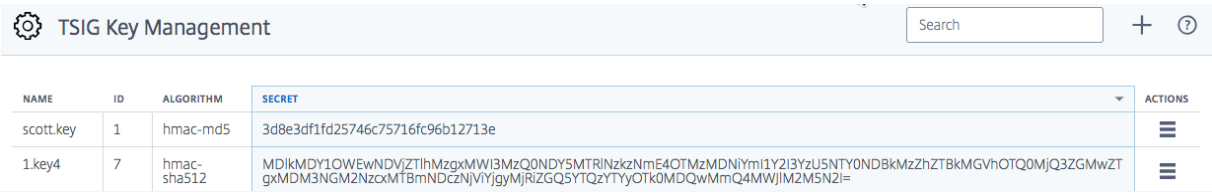
Pour générer et gérer les clés TSIG, procédez comme suit :



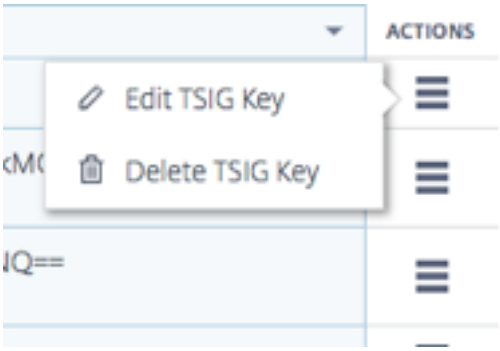
1. Dans le menu de navigation de gauche, choisissez **Predictive DNS**.
2. Cliquez sur **TSIG Key Management**.
3. La page de gestion des clés TSIG s'ouvre.



4. Cliquez sur l'icône d'ajout en haut à droite de la page.
5. La boîte de **dialogue Ajouter une clé TSIG** s'ouvre.
6. Entrez un **nom** pour le TSIG.
7. Sélectionnez un algorithme dans la liste.
8. Pour **Secret**, vous avez la possibilité de saisir n'importe quel mot ou phrase dans le champ. Tant que ce que vous entrez comporte 32 caractères (sans espaces) et qu'il est codé en base64, il est accepté comme tel. Dans le cas contraire, il est haché selon l'algorithme que vous avez sélectionné. **Remarque** : Les valeurs du secret et de l'algorithme doivent correspondre entre le système principal et le système secondaire. La valeur du secret doit être codée en base64 et avoir une longueur de 32 caractères. Le bouton de génération de hachage n'est là que pour aider à générer un hachage s'il n'en existe pas déjà un.
9. Cliquez sur **Créer** pour terminer la génération de la clé. Le TSIG nouvellement créé est répertorié sur la page de **gestion des clés TSIG** .

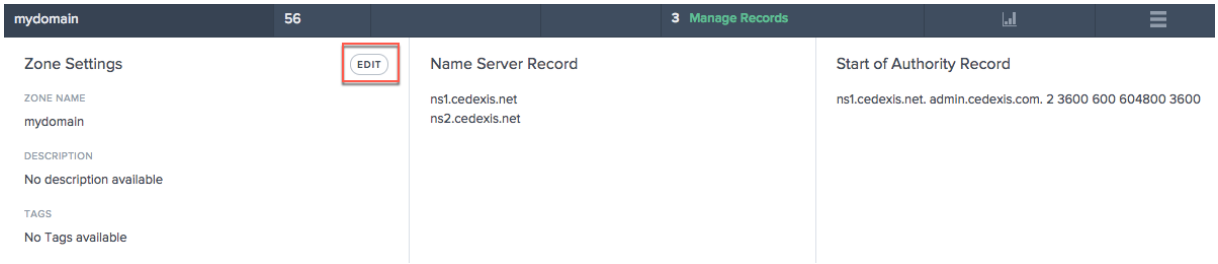


Pour modifier ou supprimer la clé **TSIG**, cliquez sur la colonne **Actions** . Choisissez **Modifier** pour modifier ou **Supprimer** pour supprimer la clé.



Modifier la zone

1. Cliquez sur le nom de la zone que vous souhaitez modifier.
2. Le tiroir d'édition s'ouvre.
3. Cliquez sur le bouton **Modifier** pour modifier le nom, la description et les balises de la zone.
4. Cliquez sur **Enregistrer** pour enregistrer vos modifications.

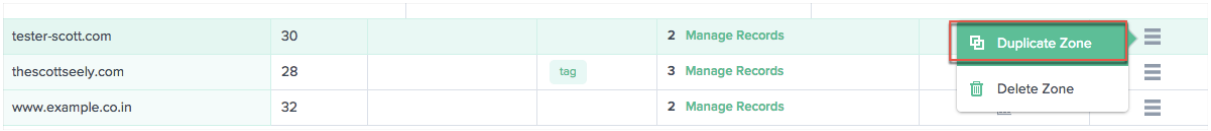


Important : soyez prudent lorsque vous modifiez le nom d'une zone. Comme tous les enregistrements de la zone sont effectivement suffixés avec le nom de la zone, le changement de nom d'une zone modifie chaque demande.

Zone dupliquée

Dupliquer une zone signifie simplement créer une autre zone avec les informations d'une zone existante, mais avec un nom de zone différent.

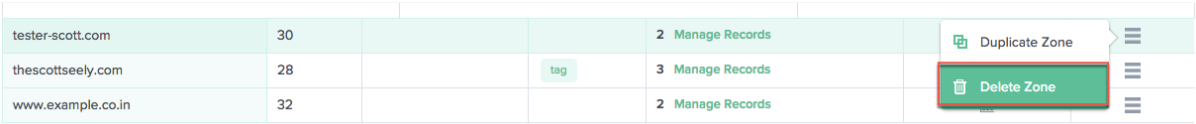
1. Pour dupliquer une zone, cliquez sur l'icône dans la colonne **Actions** .
2. Choisissez **Duplicate Zone**.
3. La boîte de dialogue **Ajouter une zone** s'ouvre avec les informations de la zone d'origine.
4. Donnez un nouveau nom à la zone et modifiez les informations dont vous avez besoin.
5. Cliquez sur **Créer** pour terminer le processus.
6. Une nouvelle zone est créée avec les enregistrements et les informations trouvés dans la zone d'origine.



Remarque : Vous pouvez modifier n'importe quelle information dans la nouvelle zone à votre propre discrétion. Mais vous devez au moins modifier le **nom de la zone** pour créer une zone dupliquée. Les noms de zone dupliqués ne sont pas autorisés.

Supprimer la zone

1. Pour supprimer une zone, cliquez sur l'icône dans la colonne **Actions** .
2. Choisissez **Supprimer la zone**.
3. Cliquez sur **Confirmer**.



Remarque : Cette opération affecte l'ensemble de la zone, y compris toutes les réponses relatives à tous les enregistrements de la zone. Cela doit être fait avec une extrême prudence.

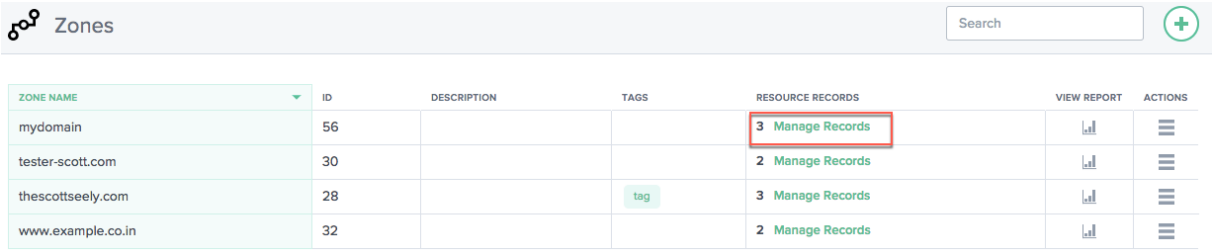
Enregistrements

Après avoir créé une zone pour votre domaine (par exemple `mydomain.com`), vous pouvez y ajouter des enregistrements. Chaque enregistrement que vous ajoutez inclura un nom, un type d'enregistrement et d'autres informations applicables au type d'enregistrement.
Tous les enregistrements d'une zone doivent avoir le nom de domaine de la zone comme suffixe. Par exemple, s'il s'`mydomain.com` agit de la zone, elle peut contenir des enregistrements nommés `www.mydomain.comwww.portal.mydomain.com`, mais ne peut pas contenir un enregistrement nommé, c'`www.mydomain.co.in` est-à-dire que le nom de chaque enregistrement est ajouté au nom de la zone.
Remarque : Lorsqu'une zone est créée, les types d'enregistrement du serveur de noms (NS) et d'enregistrement de début d'autorité (SOA) sont automatiquement créés pour cette zone.

Gérer les enregistrements

Pour accéder à la page Enregistrements et gérer vos enregistrements, cliquez sur **Gérer les enregistrements** dans la colonne **Enregistrements de ressources** de votre zone. La page **Enregistrements** s'ouvre avec une liste des enregistrements situés sous la zone sélectionnée. Même si vous n'avez pas encore créé d'enregistrement, vous pouvez voir au moins deux types d'enregistrements

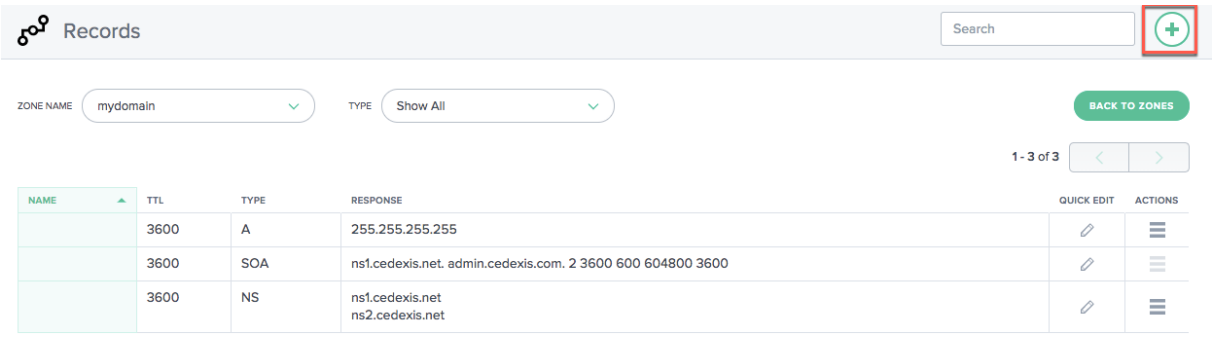
sous Enregistrements de ressources pour une ou plusieurs zones que vous avez créées. Il s'agit des enregistrements NS et SOA créés par défaut lorsque vous créez votre zone pour la première fois.



Cette page vous permet d'ajouter, de modifier, de supprimer ou de dupliquer des enregistrements. Il répertorie également le TTL, le type d'enregistrement et la réponse pour chaque sous-domaine ou enregistrement.

Ajouter un enregistrement

1. Sur la page **Zones**, cliquez sur **Gérer les enregistrements**. Cela vous amène à la **page des enregistrements**.
2. Pour ajouter un nouvel enregistrement, cliquez sur le bouton Ajouter dans le coin supérieur droit de la page **des enregistrements** .
3. La boîte de dialogue **Ajouter un enregistrement** s'ouvre.



Nom Entrez le nom de l'enregistrement. Si vous laissez ce champ vide, un enregistrement est créé au sommet de la zone. Par exemple, si votre zone l'est `mydomain.com` et que vous souhaitez un enregistrement A à la racine de ce domaine, vous devez le spécifier comme enregistrement anonyme dans la zone. `mydomain.com` D'autres spécifications et fournisseurs appellent cela l' enregistrement @.

TTL Entrez une valeur pour TTL.TTL est la durée, en secondes, pendant laquelle vous souhaitez que les résolveurs DNS récursifs mettent en cache les informations relatives à cet enregistrement. Si vous spécifiez une valeur plus longue (par exemple, 172 800 secondes ou deux jours), les résolveurs réutiliseront une réponse précédente et enverront moins souvent des demandes au serveur DNS faisant

autorité. Cela signifie toutefois que les modifications apportées à l'enregistrement prennent plus de temps pour prendre effet, car les résolveurs récursifs utilisent les valeurs de leur cache pendant de plus longues périodes au lieu de demander les dernières informations.

Type Sélectionnez le type d'enregistrement que vous souhaitez créer. Pour plus d'informations sur les différents types d'enregistrements, reportez-vous à la section Types d'enregistrements .

Type de réponse Entrez une réponse adaptée à la valeur du type d'enregistrement. Pour tous les types sauf CNAME, vous pouvez saisir plusieurs valeurs de réponse. Entrez plusieurs valeurs de réponse en cliquant sur l'icône d'ajout. Si plusieurs valeurs sont saisies, toutes les réponses spécifiées seront renvoyées pour chaque demande de ce type et de ce nom.

Cliquez sur **Créer** pour ajouter l'enregistrement. L'enregistrement nouvellement ajouté se propage vers les serveurs DNS et est diffusé en direct lorsque la modification est apportée.

Lister les enregistrements

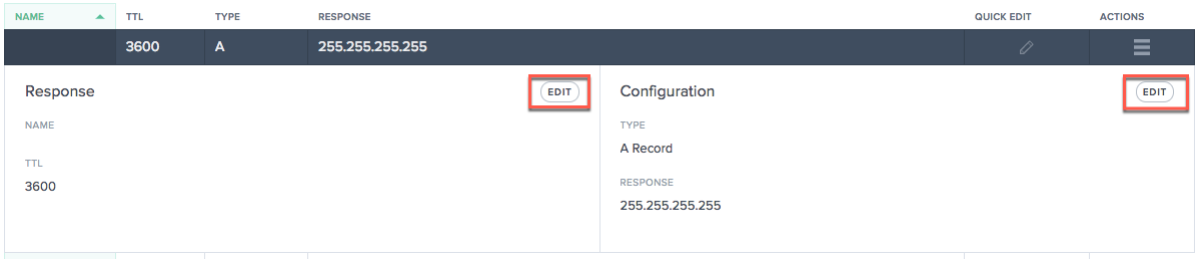
Lorsque vous ajoutez un nouvel enregistrement, il est répertorié sur la page Enregistrements. Cette page répertorie tous les enregistrements que vous avez créés sous un **nom de zone** spécifique ainsi que le **TTL**, le **type d'enregistrement**et la **réponse** pour cet enregistrement.

Tous les enregistrements de cette page appartiennent à une zone spécifique affichée dans la liste des **noms de zone** en haut à gauche de la page **des enregistrements** . Cette liste contient la liste des zones déjà créées pour votre entreprise. Vous pouvez passer à une autre zone (et consulter ses propres enregistrements) en la sélectionnant dans la liste.

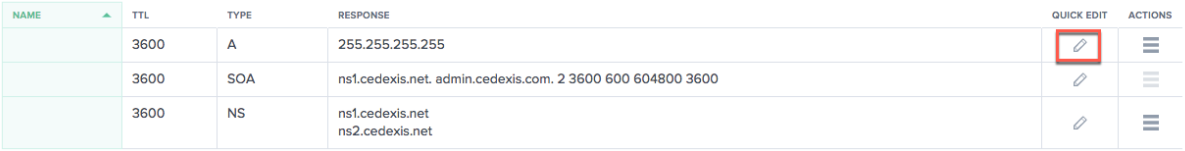
Vous pouvez également utiliser la liste des **types d'enregistrement** pour filtrer cette liste en fonction du type d'enregistrement.

Modifier l'enregistrement

Il existe deux méthodes pour modifier les enregistrements : modification détaillée et modification rapide. Pour effectuer une modification détaillée, cliquez sur Enregistrer dans la liste (sur la page **Enregistrements**). Elle s'ouvre pour afficher les détails de l'enregistrement avec des boutons à modifier. Cliquez sur le bouton **Modifier** pour afficher les informations relatives à l'enregistrement. Une fois les modifications terminées, cliquez sur **Enregistrer**pour enregistrer vos modifications.

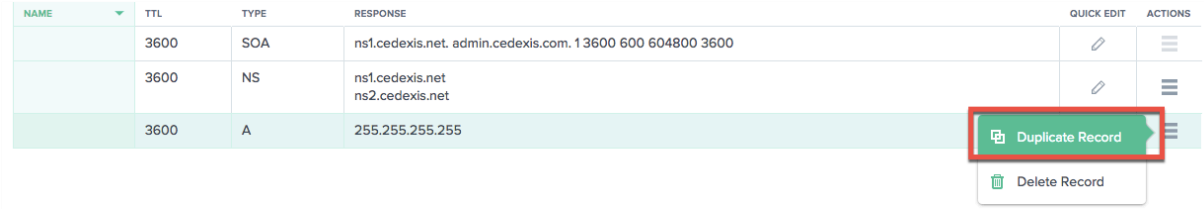


Pour utiliser l'**édition rapide**, il suffit de cliquer sur l'icône de modification (dans la colonne **Modification rapide**) de l'enregistrement que vous souhaitez modifier. Vous pourrez modifier le TTL et la réponse de l'enregistrement. Lorsque vous avez terminé les modifications, cliquez sur l'icône Enregistrer (coche) pour enregistrer vos modifications ou sur Annuler pour les annuler.



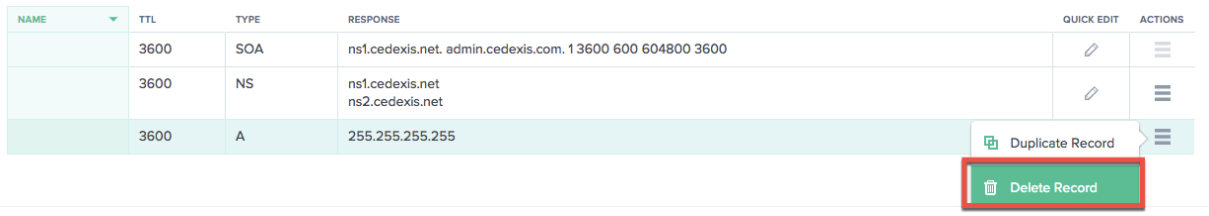
Enregistrement dupliqué

Pour dupliquer un enregistrement, cliquez sur l'icône dans la colonne **Actions** . Choisissez Dupliquer Record. La boîte de dialogue Ajouter un enregistrement s'ouvre avec les informations de l'enregistrement que vous souhaitez dupliquer. Cliquez sur Créer pour créer un enregistrement avec les informations de l'enregistrement d'origine. Veuillez noter qu'au moins le nom ou le type de l'enregistrement doit être modifié pour que le nouvel enregistrement soit créé.
Remarque : les enregistrements SOA ne peuvent pas être dupliqués.



Supprimer l'enregistrement

Pour supprimer un enregistrement, cliquez sur l'icône dans la colonne **Actions** . Choisissez Supprimer l'enregistrement. Cette action supprime l'enregistrement et Predictive DNS ne répondra plus aux requêtes relatives à l'enregistrement. Pour supprimer des réponses spécifiques dans un enregistrement, utilisez l'option d'édition rapide



Remarque : Les enregistrements NS et SOA sont des types d'enregistrement par défaut et ne peuvent pas être supprimés. Ces enregistrements ne seront supprimés que si la zone elle-même est supprimée.

Types d'enregistrements

Enregistrement NS

Les enregistrements NS ou Name Server sont chargés de déléguer une zone DNS à un serveur faisant autorité. Nous créons un enregistrement de serveur de noms (NS) qui est automatiquement attribué lorsque vous créez une zone, par exemple ns1.ourdomain.net et ns2.ourdomain.net. Il s'agit des serveurs de noms que vous devez configurer dans votre bureau d'enregistrement afin que les requêtes DNS puissent être acheminées vers votre zone.
Ces serveurs de noms servent à confirmer l'ensemble de serveurs disponibles pour répondre aux demandes de service pour la zone, en s'assurant que l'ensemble de serveurs de noms renvoyé dans la demande de délégation et par le serveur délégué correspond. Vous pouvez également modifier les serveurs de noms pour vous assurer qu'ils correspondent.

Nous vous permettons également de modifier les serveurs de noms que vous créez afin que vous puissiez rediriger n'importe lequel de vos domaines vers les serveurs de noms d'une autre entreprise susceptibles de contenir votre zone DNS et d'y gérer vos enregistrements.

Remarque : les enregistrements NS peuvent être modifiés mais ne peuvent pas être supprimés.

Enregistrement SOA

L'enregistrement SOA (Start of Authority) identifie les informations faisant autorité concernant la zone. Un enregistrement de ressource SOA est créé par défaut lorsque vous créez votre zone. Vous pouvez modifier l'enregistrement selon vos besoins.

Remarque : les enregistrements SOA ne peuvent pas être créés par l'utilisateur, mais certains paramètres peuvent être modifiés.

Le format d'un enregistrement SOA est le suivant : `[MNAME] [RNAME] [Serial Number] [Refresh Time] [Retry Interval] [Expire Time] [Minimum TTL]`

Voici un exemple : `ns1.ourdomain.net admin.mydomain.com.314 3600 600 604800 10`

Les éléments de l'enregistrement SOA incluent :

- **MNAME** : nom de domaine du serveur de noms principal, comme `ns1.ourdomain.net` dans l'exemple ci-dessus.
- **RNAME** : adresse e-mail de l'administrateur dans un format dans lequel le symbole @ est remplacé par un point, comme `admin.mydomain.com` dans l'exemple ci-dessus.
- **Numéro de série** : numéro de révision à incrémenter lorsque vous modifiez le fichier de zone et distribuez les modifications aux serveurs DNS. Un entier de 32 bits non signé, tel que 314 dans l'exemple ci-dessus.
- **Temps de rafraîchissement** : temps de rafraîchissement en secondes pendant lequel les serveurs DNS attendent avant d'interroger l'enregistrement SOA pour vérifier les modifications. Un intervalle de temps entier non signé de 32 bits en secondes, tel que 3600 dans l'exemple ci-dessus.
- **Intervalle entre**les tentatives : intervalle en secondes pendant lequel un serveur secondaire attend avant de réessayer un transfert de zone ayant échoué, par exemple 600 (10 minutes) dans l'exemple ci-dessus. Normalement, le temps de nouvelle tentative est inférieur au temps de rafraîchissement.
- **Délai d'expiration** : délai d'expiration en secondes pendant lequel un serveur secondaire continue d'essayer d'effectuer un transfert de zone, tel que 604800 (une semaine) dans l'exemple ci-dessus.
- **TTL minimum** : durée de vie minimale (TTL) en secondes, par exemple 10 secondes dans l'exemple ci-dessus.

A —Adresse IPv4

Une adresse IP au format IPv4, par exemple `192.0.2.235`. La valeur d'un enregistrement A est une adresse IPv4 en notation décimale à points.

AAAA —Adresse IPv6

Une adresse IP au format IPv6, par exemple `2001:0db8:85a3:0:0:8a2e:0370:7334`. La valeur d'un enregistrement AAAA est une adresse IPv6 au format hexadécimal séparé par des deux-points, comme indiqué dans les représentations de la RFC 4291/5952.

CNAME —Nom canonique

Il s'agit du nom de domaine complet (par exemple, `www.mydomain.com`) que vous souhaitez que Predictive DNS renvoie en réponse aux requêtes DNS relatives à cet enregistrement. Le format d'un élément de valeur CNAME est identique à celui d'un nom de domaine.

Important : Le protocole DNS ne vous permet pas de créer un enregistrement CNAME pour la racine de la zone, c'est-à-dire que nous n'autorisons pas les enregistrements CNAME sans nom. Par exemple, si votre zone l'est `mydomain.com`, vous ne pouvez pas créer d'enregistrement CNAME pour `mydomain.com`. Toutefois, vous pouvez créer des enregistrements `www.mydomain.com`CNAME pour `portal.mydomain.com`„ etc.
En outre, si vous créez un enregistrement CNAME pour un sous-domaine, vous ne pouvez pas créer d' autres enregistrements pour ce sous-domaine. Par exemple, si vous créez un enregistrement CNAME pour `www.mydomain.com`, vous ne pouvez pas créer d'autres types d'enregistrement avec ce nom. `www.mydomain.com`
Remarque : Si un sous-domaine possède un enregistrement Openmix App, vous ne pouvez pas avoir d'enregistrements A, AAAA ou CNAME dans le même sous-domaine.

MX —Échange de courrier

Il s'agit de l'enregistrement utilisé pour acheminer les demandes vers les serveurs de messagerie. Pa exemple : `1 mail.mydomain.com`

Chaque valeur d'un enregistrement MX contient deux valeurs :

1. Priorité du serveur de messagerie, qui peut être un entier de 16 bits supérieur à 0.
2. Le nom de domaine du serveur de messagerie.

Si vous spécifiez plusieurs serveurs, la valeur que vous spécifiez pour la priorité indique vers quel serveur de messagerie vous souhaitez que le courrier soit acheminé en premier, en second, etc. Par exemple, si vous avez deux serveurs de messagerie et que vous spécifiez des valeurs de 1 et 2 pour la priorité, le courrier électronique est toujours envoyé au serveur avec une priorité de 1, sauf s'il n'est pas disponible. Si vous spécifiez les valeurs 1 et 1, le courrier électronique est acheminé vers les deux serveurs de manière approximativement égale.

Openmix (A/AAAA/CNAME)

Les clients de l'application Openmix peuvent désormais gérer et servir l'intégralité de leur ensemble d'enregistrements dans la zone (y compris les enregistrements statiques) par le même ensemble de services. Cela permet aux clients de rendre Openmix intelligent n'importe lequel de leurs hôtes. Ainsi, chaque fois qu'un CNAME est attaché à une application Openmix, il est diffusé avec les mêmes fonctionnalités dynamiques, entièrement programmables et pilotées par les données qu'Openmix.

Par exemple, vous pouvez avoir plusieurs serveurs d'applications Web derrière une application Openmix pour votre enregistrement « www » et l'application Openmix décidera avec quel CNAME répondre, en utilisant sa logique intelligente intégrée.

Remarque : Une application Openmix peut renvoyer un enregistrement CNAME, A ou AAAA et vous ne pouvez donc pas avoir simultanément une application Openmix avec l'un de ces types d'enregistrement utilisant le même nom.

PTR —Enregistrement du pointeur

Les enregistrements PTR sont utilisés pour mapper une adresse IP à un nom de domaine, principalement pour le DNS inversé. Des enregistrements PTR correctement configurés peuvent être importants pour les scénarios de sécurité tels que la validation de la crédibilité des expéditeurs d'e-mails ou la recherche DNS inversée effectuée lors de l'établissement de sessions SSH. La valeur d'un enregistrement PTR a le même format qu'un nom de domaine. Par exemple, `hostname.mydomain.com`.

SPF —Cadre de politique des expéditeurs

Un enregistrement SPF identifie les serveurs de messagerie autorisés à envoyer des e-mails au nom de votre domaine. Cela commence par v=spf, par exemple, v=spf1 ip 4:192.168 .0.1/16-all.

SRV —Localisateur de services

Un enregistrement SRV est utilisé par la voix sur IP, les protocoles de messagerie instantanée, la découverte de services et d'autres applications. Un élément de valeur d'enregistrement SRV se compose de quatre valeurs séparées par des espaces. Les trois premières valeurs sont des nombres décimaux représentant la priorité, le poids et le port. La quatrième valeur est un nom de domaine.

Le format d'un enregistrement SRV est le suivant :

```
[priority] [weight] [port] [domain name]
```

Par exemple :

```
1 10 5269 xmpp-server.example.com
```

TXT —Texte

Un enregistrement de texte peut contenir du texte arbitraire et peut également être utilisé pour définir des données lisibles par machine, telles que des informations de sécurité ou de prévention des abus. Il est également souvent utilisé pour vérifier la propriété du domaine (par exemple, vous pouvez obtenir

un certificat, enregistrer des outils tiers pour opérer au nom de votre domaine, etc.).
Il doit simplement contenir du texte, par exemple un exemple de saisie de texte.

Enregistrement prédictif (A/AAAA/CNAME)

Les enregistrements prédictifs fournissent diverses options de configuration pour la gestion globale du trafic en fonction de la disponibilité des services en temps réel. Les enregistrements prédictifs vous permettent d'appliquer la configuration du routage à travers les pools d'adresses et de définir le comportement individuellement pour différents emplacements, réseaux ou blocs IPS/CIDR. Ce service combine une logique de basculement et de routage circulaire pour garantir une disponibilité maximale, l'absence de temps d'arrêt et une gestion fluide du trafic basée sur les données sur toutes les plateformes.

Les clients du DNS prédictif peuvent utiliser le type d'enregistrement prédictif pour les types de réponse CNAME, A ou AAAA.

En tant que client de Predictive DNS, lorsque vous ajoutez des enregistrements à votre zone, sélectionnez Predictive (A/AAAA/CNAME) dans la liste des types**d'enregistrements.**

Navigation

1. Accédez à la page **des enregistrements** de votre zone.
2. Cliquez sur le **bouton Ajouter un enregistrement** sur la page des enregistrements. Pour en savoir plus sur l'ajout d'enregistrements, reportez-vous à la section Ajouter un enregistrement .
3. La boîte de dialogue **Ajouter un enregistrement** s'ouvre.

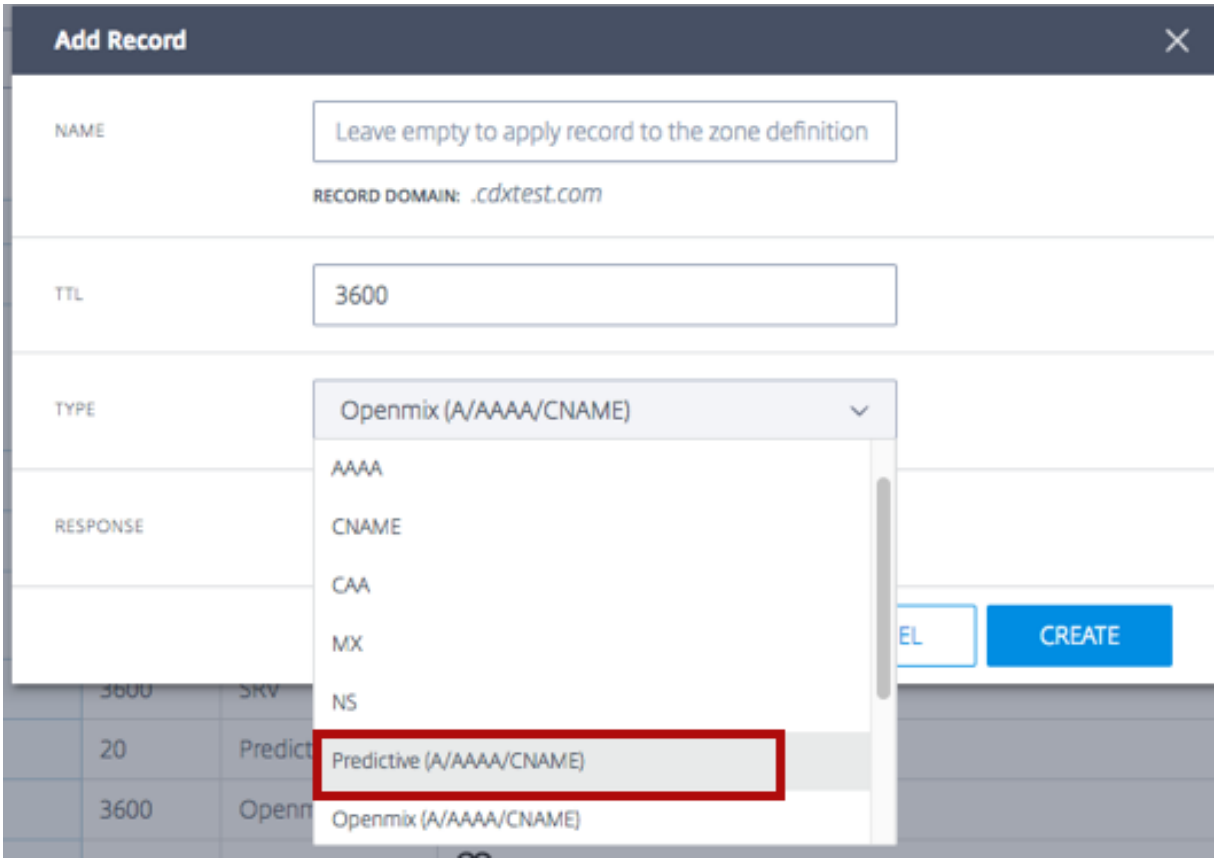
Ajouter des enregistrements prédictifs

Dans la boîte de dialogue **Ajouter un enregistrement**, entrez ce qui suit :

1. **Nom** : Entrez un nom pour l'enregistrement. S'il est laissé vide, l'enregistrement contiendra automatiquement la définition de la zone. Vous pouvez également utiliser un astérisque `*` comme caractère générique dans la partie la plus à gauche du nom pour faire correspondre les demandes relatives à tous les sous-domaines inexistants. Par exemple, vous pouvez utiliser `*`, `*.example.com`, ou `*.something.example.com`. Cependant, n'`*.` est pas valide, c'est-à-dire qu'un astérisque suivi d'un simple point n'est pas autorisé. Nous prenons en charge la fonctionnalité joker telle que définie dans les RFC.
2. **TTL** : Vous pouvez laisser le TTL par défaut tel quel ou le modifier selon vos besoins. **Remarque :** le DNS Time to Live (TTL) indique aux résolveurs pendant combien de temps ils doivent

conserver leur décision avant de demander à nouveau des mises à jour. Le TTL est utilisé pour contrôler le volume du trafic, ainsi que pour contrôler la sensibilité aux modifications des données sur lesquelles il agit. La durée de vie par défaut est de 20 secondes. Si vous réduisez la durée de vie, vous obtenez plus de volume et plus de requêtes DNS en temps réel. Cela peut toutefois entraîner des coûts supplémentaires et une baisse des performances (car les requêtes DNS prennent du temps sur le client). Il est donc recommandé de ne pas modifier la valeur par défaut de 20 secondes.

3. **Type** : cliquez sur la liste des **types**, puis sélectionnez Prédictif (A/AAAA/CNAME).
4. **Type de réponse** : cliquez sur la liste des **types** de réponse et sélectionnez le type de réponse A, AAAA ou CNAME.
5. Solution de**secours** : entrez la réponse de **secours. Un CNAME, A, AAAA valide doit être spécifié pour Fallback.** La solution de secours est utilisée en cas d'échec du traitement de la demande. **Remarque** : La réponse de **secours** doit être un CNAME valide, si le **type de réponse** que vous avez sélectionné à l'étape précédente est CNAME. Si le **type de réponse** sélectionné est A, la réponse de secours doit être un CNAME ou une adresse IPv4. Sinon, si le **type de réponse** sélectionné est AAAA, la réponse de secours doit être un CNAME ou une adresse IPv6.
6. Cliquez sur **Créer et définir le routage**.
7. La page **de configuration prédictive** s'ouvre.



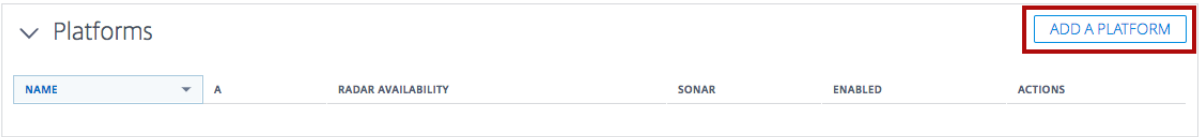
Étapes de configuration

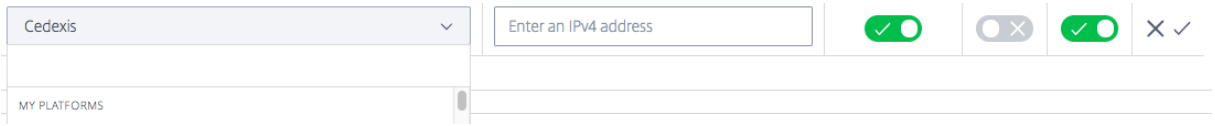
En haut de cette page se trouve la section **Général** qui affiche les informations que vous avez configurées dans la boîte de dialogue **Ajouter un enregistrement** . Il comporte également des champs facultatifs pour ajouter des **balises** ou une **description** à vos enregistrements prédictifs.

Suivez les étapes ci-dessous pour configurer l'enregistrement.

Étape 1 : Choisissez toutes les plateformes disponibles La première étape de configuration de l'enregistrement prédictif consiste à choisir toutes les plateformes que vous souhaitez disponibles pour différents emplacements, réseaux ou blocs IPS/CIDR. Si vous ne trouvez pas votre plateforme dans la liste, vous pouvez l'ajouter sur la page Plateformes .

1. Cliquez sur **Ajouter une plateforme** en haut à droite de cette section.
2. Ajoutez toutes les plateformes que vous souhaitez mettre à disposition pour le routage, y compris celles qui doivent être ajoutées aux pools d'adresses. Vous pouvez le faire en cliquant sur le champ **Choisir une plateforme** et en sélectionnant les plateformes individuellement dans la liste.
3. Selon le **type de réponse** (A, AAAA ou CNAME) que vous avez sélectionné dans la liste **Ajouter un enregistrement**, entrez une adresse IPv4, une adresse IPv6 ou un CNAME pour la plate-forme. Vous pouvez revenir à la section **Général** pour modifier le **type de réponse**, si nécessaire.
4. Une fois la plateforme sélectionnée et le **type de réponse** saisi, vous pouvez activer ou désactiver la plateforme en cliquant sur le bouton **Activé** . Vous pouvez également **activer/désactiver la disponibilité du radar et le sonar** à l'aide de boutons de bascule similaires.
5. Dans la colonne **Actions**, cliquez sur l'icône en forme de coche pour enregistrer vos modifications ou sur l'icône en forme de croix pour annuler.

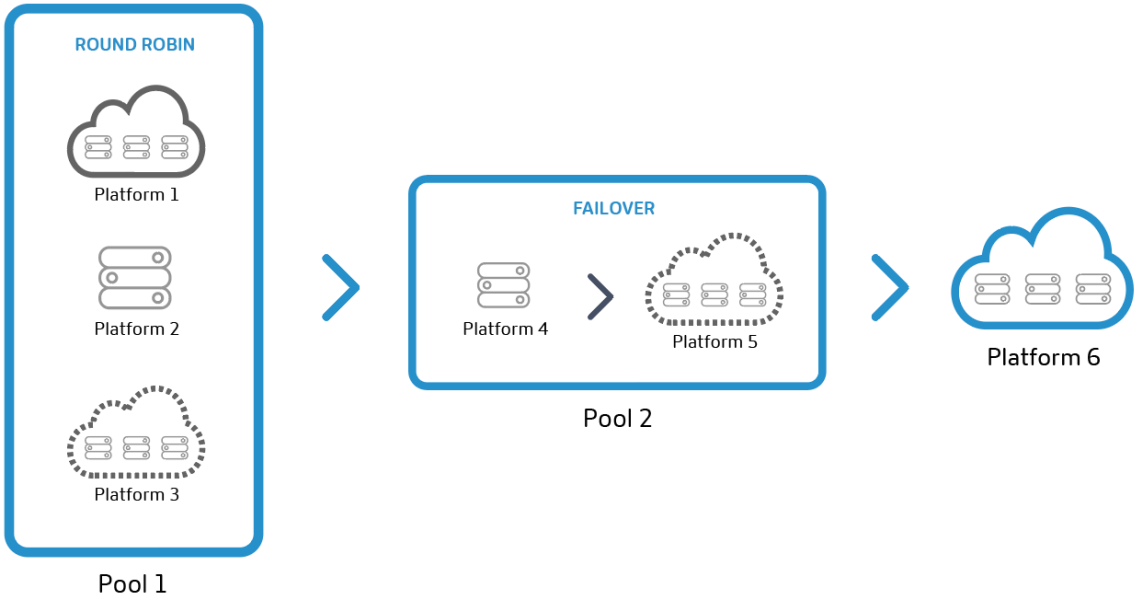




Étape 2 : Ajouter et définir des pools d'adresses

Pools d'adresses Les pools d'adresses sont un ensemble de plateformes qui suivent une méthode de routage spécifiée par l'utilisateur. Le but d'un pool d'adresses est de vous permettre de définir des groupes logiques de plateformes qui peuvent être utilisés avec n'importe quelle méthode de routage spécifique. Vous pouvez spécifier les méthodes de routage **Round Robin** ou **Failover** que les plateformes doivent suivre au sein d'un pool.

Vous pouvez ajouter autant de plateformes que vous le souhaitez dans chaque pool, et autant de pools que vous le souhaitez pour chacune de vos zones géographiques. Par exemple, vous pouvez avoir un pool européen (composé de plateformes desservant principalement la région de l'UE), un pool asiatique (avec des plateformes en Chine, en Inde et à Singapour) et un pool américain (avec des plateformes à travers les États-Unis).



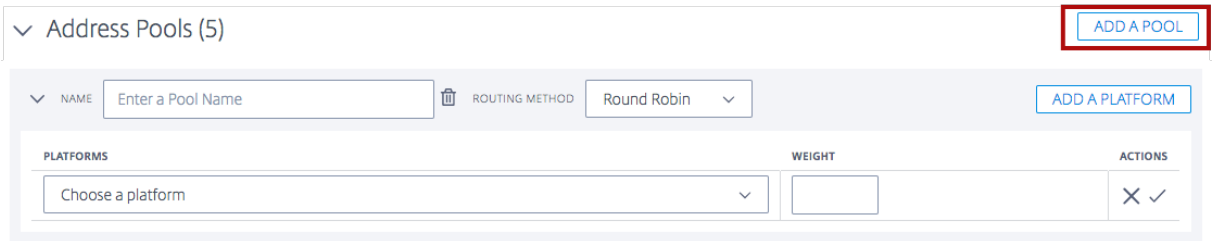
Remarque : les pools d'adresses sont facultatifs. Vous pouvez utiliser des plateformes individuelles à la place et les ajouter à la configuration de routage.

Méthode de routage Round Robin Ce type de routage suit une méthodologie typique d'équilibrage de charge des serveurs mondiaux basée sur le cycle circulaire, dans laquelle chaque CNAME/A/AAAA

est renvoyé alternativement aux utilisateurs finaux au fur et à mesure que les demandes DNS sont effectuées. Par exemple, si les plates-formes P1, P2 et P3 atteignent le seuil de disponibilité, la première demande est acheminée vers P1, la deuxième vers P2, la troisième vers P3, la quatrième vers P1, etc. Vous pouvez également attribuer des poids pour la priorisation et la sélection de chaque plateforme à l'échelle mondiale et/ou par marché ou pays.

Méthode de routage par basculement Cette méthode de routage prend en charge une logique de routage simple dans laquelle une plate-forme est choisie en fonction de sa place dans la ligne et de son seuil de disponibilité. Vous pouvez créer une chaîne de basculement qui décide de la plateforme à sélectionner en premier, en second, etc. Cette chaîne de basculement peut être créée pour fonctionner à l'échelle mondiale et/ou pour des marchés et des pays individuels.

Ajouter un pool d'adresses Pour ajouter un pool d'adresses, procédez comme suit :



1. Cliquez sur le bouton **Ajouter un pool** en haut à droite de la section.
2. Entrez un **nom** pour le pool. Le nom peut être utilisé pour identifier l'objectif du pool.
3. Sélectionnez une **méthode de routage**. Vous pouvez sélectionner **Round Robin** ou **Failover**.
4. Choisissez une **plateforme** dans la liste que vous avez créée à l'étape précédente.
5. Vous pouvez ajouter autant de plateformes que nécessaire à ce pool en cliquant sur le bouton **Ajouter une plateforme** .
6. Pour chaque plateforme que vous choisissez, entrez un **poids**approprié. Le but des pondérations est de prioriser et de sélectionner les plateformes pour la distribution du trafic. Il n'est pas nécessaire que la somme des poids que vous attribuez aux plateformes soit égale à 100. Il peut s'agir de n'importe quel entier compris entre 0 et 1 000 000. Ces pondérations, une fois converties en pourcentage (dans le back-end), s'élèveront à 100 %. Si toutes les plateformes sélectionnées reçoivent le même poids, le trafic sera réparti uniformément entre elles au fil du temps. Si vous n'avez qu'une seule plateforme, celle-ci sera utilisée 100 % du temps, quel que soit le poids que vous lui attribuez.
7. Lorsque vous avez terminé, cliquez sur l'icône en forme de coche pour enregistrer vos modifications ou sur l'icône en forme de croix pour annuler.

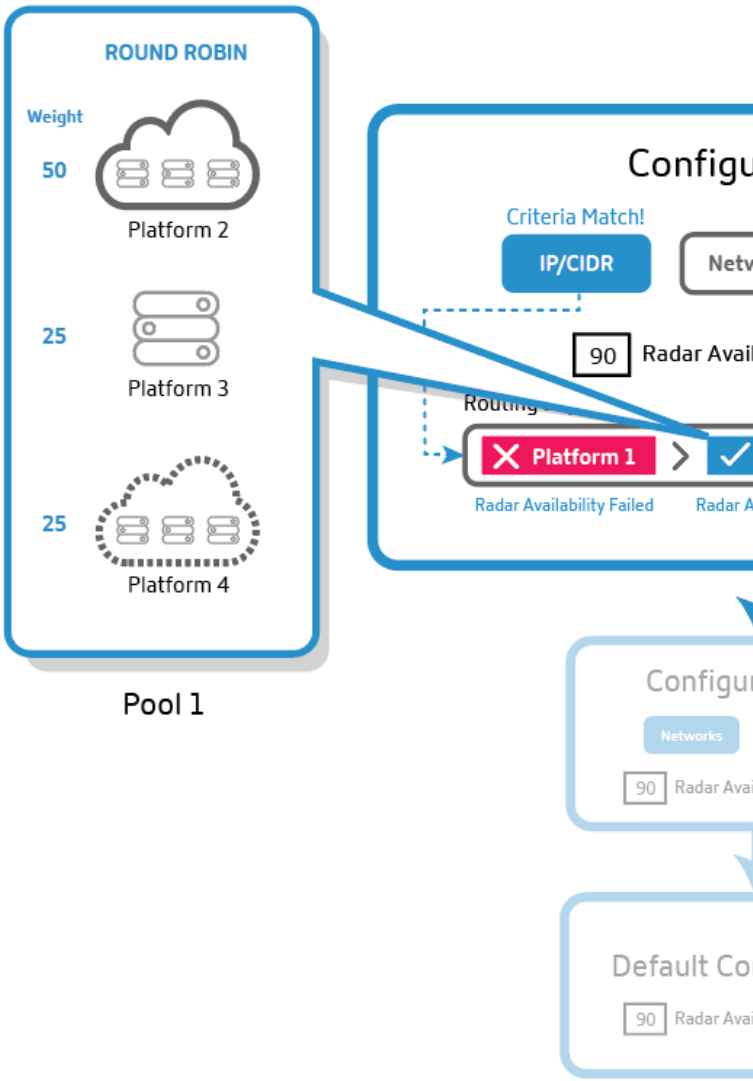
8. Vous pouvez ensuite modifier ou supprimer votre sélection de plateforme en choisissant les icônes appropriées dans la colonne **Actions** .

Étape 3 : Configuration du basculement Le failover s'applique à l'ensemble des pools d'adresses et/ou des plateformes individuelles. Il prend en charge une méthode de validation simple dans le cadre de laquelle une plate-forme ou un pool individuel est évalué pour le routage en fonction des critères suivants :

- Emplacement, réseau et/ou IP/CIDR. Au moins un de ces critères doit être spécifié.

  > **Remarque :**
  >
  > Les critères de localisation pour le basculement ne doivent pas inclure une combinaison de continents et de pays, mais vous pouvez utiliser la logique de routage pour créer plusieurs basculements.

- Disponibilité des sonars et des radars si configurés, et
- Placer en ligne

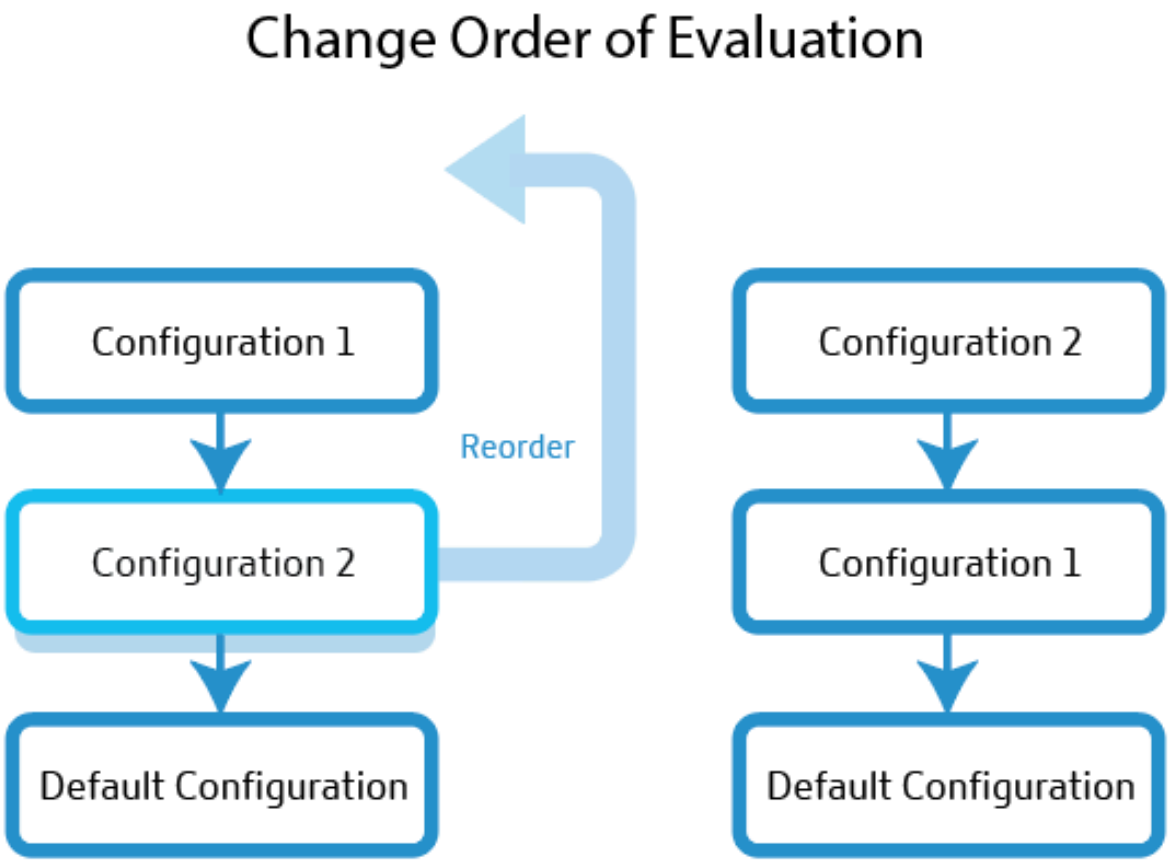


Failover pour les enregistrements prédictifs

1. L'enregistrement prédictif évalue le premier bloc de configuration en fonction des critères requis (emplacement, réseau et/ou adresses IP). Si le premier bloc de configuration de routage ne répond pas aux critères requis, il passe au second en ligne et ainsi de suite.
2. Le bloc de configuration qui répond à tous les critères requis est choisi pour la distribution du trafic.
3. Dans le bloc de configuration choisi, les pools d'adresses ou les plateformes sont évalués en fonction de leur place dans la ligne et du seuil de disponibilité (radar et sonar).
4. La première plate-forme au sein du pool d'adresses (ou en dehors de celui-ci) qui atteint le seuil de disponibilité est sélectionnée pour la distribution du trafic. La logique de routage Round Robin ou Failover entre alors en jeu.

Remarque : S'il n'y a qu'une seule plateforme dans le pool, cette plateforme est sélectionnée 100 % du temps et la logique du round robin ne s'appliquera pas à elle.

En tant qu'utilisateur, vous pouvez organiser les blocs de configuration du routage de telle sorte que celui qui a la priorité la plus élevée arrive en premier, etc. La réorganisation peut être effectuée manuellement en faisant glisser chaque piscine ou plate-forme à l'endroit où elle doit se trouver dans la ligne.



Configuration par défaut Vous devez avoir au moins une plate-forme ou un pool dans le bloc de configuration de routage par défaut. Il doit contenir une ou plusieurs plateformes ou pools que l'enregistrement prédictif utilisera si toutes les autres options ne répondent pas aux critères spécifiés. La valeur par défaut ne comporte aucun critère à spécifier et elle correspond à toutes les demandes. Si la disponibilité de la plateforme n'atteint pas le seuil de disponibilité du radar, la réponse renvoie une solution de secours.

Étapes pour configurer le basculement Pour définir la configuration, procédez comme suit :

1. Entrez un **nom**. Ce nom permet d'identifier votre bloc de configuration de routage.
2. Vous pouvez laisser le TTL par défaut tel quel ou le modifier selon vos besoins.

3. Assurez-vous que la case **Disponibilité du radar** est cochée. Vous pouvez définir le seuil de disponibilité du radar au niveau souhaité. Décochez cette case pour désactiver le radar pour l'ensemble de pools ou de plateformes.
4. Sélectionnez **les emplacements, les réseaux et/ou l'IP/CIDR**. Par exemple, si votre configuration de routage s'applique à la région Océanie, vous pouvez spécifier les emplacements, les réseaux et/ou les adresses IP des plateformes ou des pools de cette région.
5. Le champ **Configuration du basculement** vous permet de définir la priorité de sélection pour tous les pools et plateformes. L'ordre dans lequel vous placez ces pools ou plateformes déterminera leur sélection pour le routage. Et le trafic sera acheminé selon la méthode spécifiée (round robin ou failover) à l'étape précédente.
6. Pour supprimer un bloc de configuration, cliquez sur l'icône de corbeille à côté du champ **Nom** .

Rapports DNS

Les rapports DNS fournissent une visibilité puissante sur le volume de requêtes DNS en fonction de différents critères pour un domaine ou un nom d'hôte spécifique. Ils indiquent la fréquence à laquelle des types d'enregistrements spécifiques sont interrogés et fournissent un niveau d'analyse détaillé complètement différent. Ce degré de granularité permet aux utilisateurs de Predictive DNS de comprendre les tendances et les volumes de requêtes pour des zones, des noms d'hôtes, des types de demandes, des marchés, des pays, des régions, des états et des réseaux spécifiques.

Ces rapports sont principalement utilisés pour améliorer la visibilité et l'analyse. Ils fournissent des informations sur les flux de trafic pour chaque zone ou nom d'hôte et aident à diagnostiquer les problèmes liés au DNS. Ils révèlent également des anomalies telles que des pics de demandes ou d'autres irrégularités, en ventilant le volume de demandes par type d'enregistrement et par emplacement géographique.

Vous pouvez également filtrer les bruits inutiles en identifiant les zones les plus fréquentées et en vous concentrant uniquement sur les zones ou les types d'enregistrements qui vous intéressent.

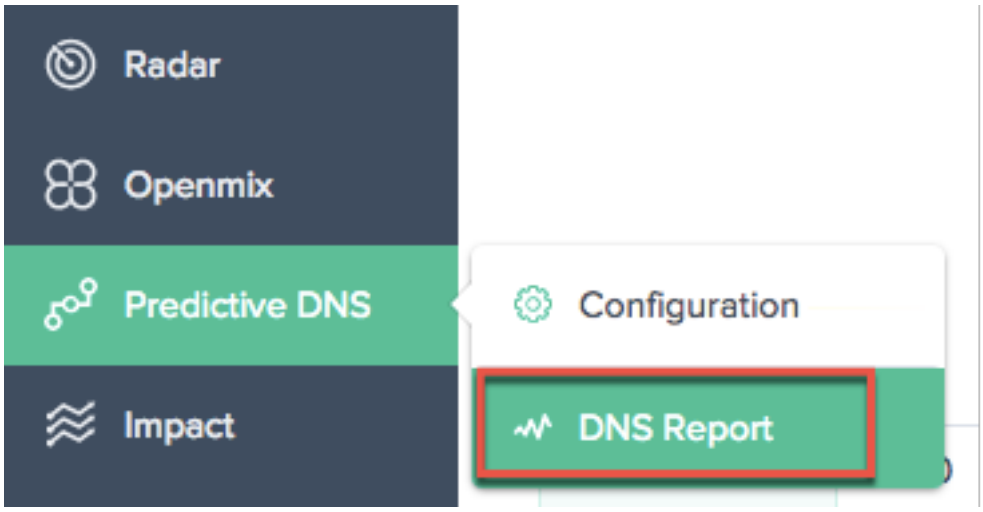
DNS contre Rapports Openmix

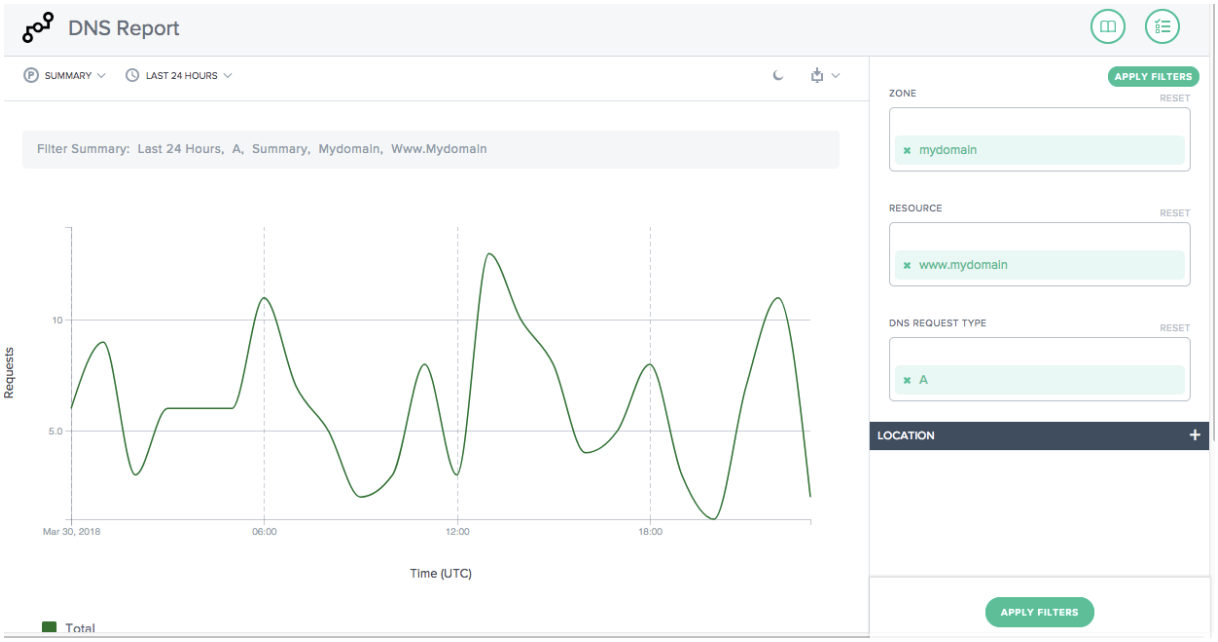
Pour les clients d'Openmix, les rapports apparaissent dans les rapports DNS et dans les rapports de décision Openmix. Les rapports DNS fournissent des informations sur les demandes adressées à nos zones autorisées, tandis qu'Openmix fournit des rapports indiquant à quel moment la plateforme intelligente Openmix a été utilisée pour répondre à une demande, soit via un enregistrement d'application Openmix, soit directement vers un Openmix CNAME.

Navigation

Pour accéder à la section **Rapport DNS** :

1. Cliquez sur **DNS prédictif** dans le menu de navigation de gauche.
2. Accédez au **rapport DNS**.
3. La page **du rapport DNS** s'ouvre.

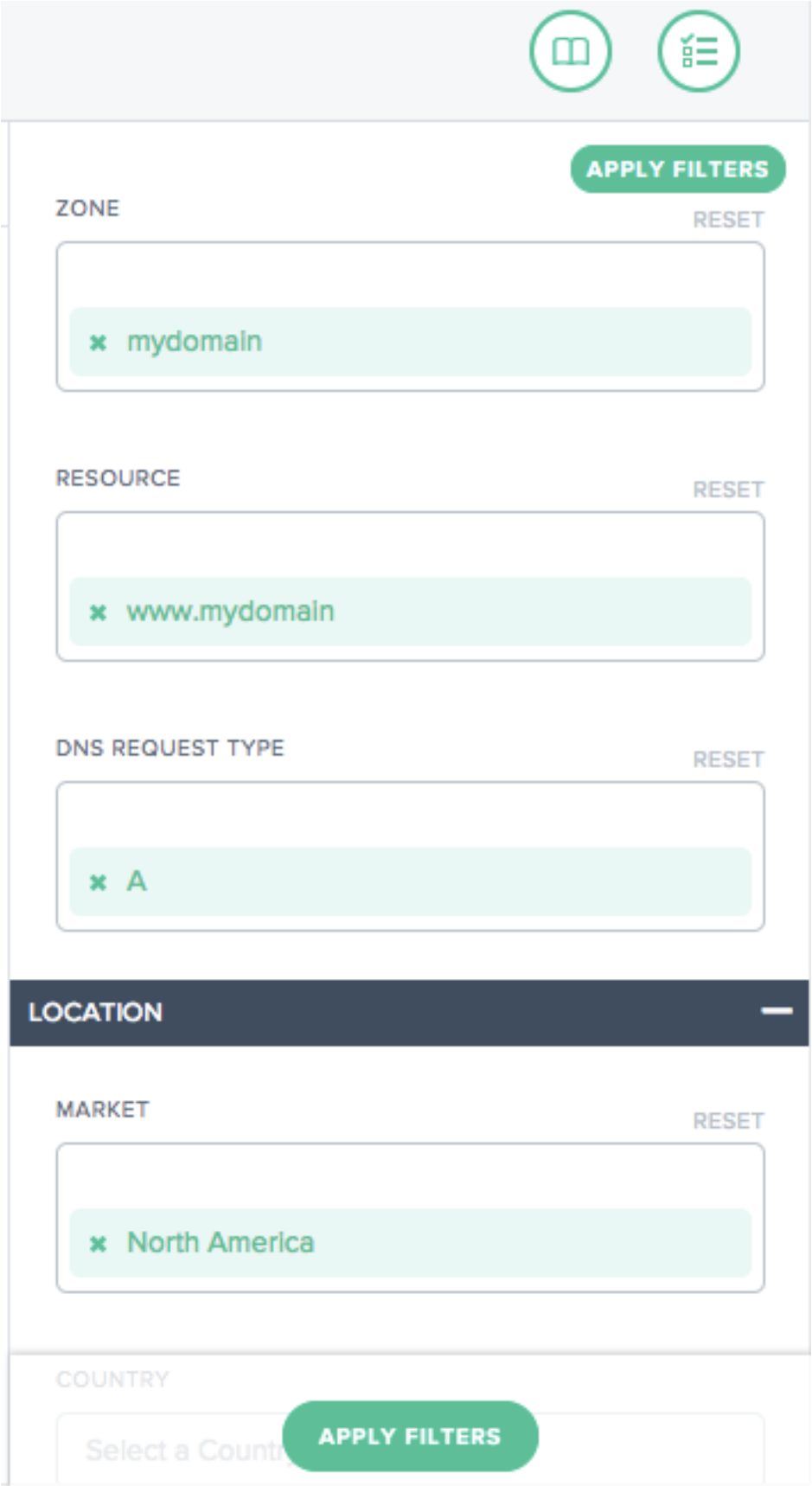




Appliquer des filtres

Le panneau **Appliquer les filtres** sur la droite vous permet de sélectionner et d'afficher uniquement les données que vous souhaitez afficher dans le rapport.
Vous pouvez filtrer en fonction des critères suivants :

- **Zone** : sélectionnez une ou plusieurs zones à inclure.
- **Ressource** —Sélectionnez un ou plusieurs noms d'hôtes à inclure.
- **Type de demande DNS** —Sélectionnez un ou plusieurs types de demande DNS à inclure.
- **Emplacement** : sélectionnez un ou plusieurs emplacements géographiques (marché, région, État ou réseau) à inclure.



Dimension principale

Les dimensions principales sont sélectionnées dans les listes situées au-dessus du graphique. Vous pouvez vous en servir comme d'un puissant pivot dans le rapport.

Résumé Le résumé indique le nombre total de demandes avec l'ensemble complet des filtres appliqués.

Filtrer par plages de temps prédéfinies

Des plages de temps prédéfinies relatives peuvent être choisies comme filtre supplémentaire pour affiner davantage les rapports.

Rapports de mise en favoris

Une fois que vous avez généré un rapport en fonction des critères de filtre, vous pouvez enregistrer les filtres appliqués en ajoutant le rapport à vos favoris. Chaque fois que vous visitez ce signet, un rapport mis à jour est généré en fonction de tous les filtres sélectionnés.
Pour ajouter un rapport à vos favoris, procédez comme suit :

- Cliquez sur l'icône de signet en haut à droite de la page.
- Dans la boîte de dialogue Ajouter un nouveau signet, attribuez un nom approprié au signet et cliquez sur Créer.
- Un nouveau signet est maintenant créé. Vous pouvez accéder au signet en cliquant sur l'icône de signet (dans le coin supérieur droit de chaque page de rapport) et en sélectionnant le signet.

Sonar

June 4, 2021

Sonar est un service de vérification de la vitalité qui peut être utilisé pour surveiller la disponibilité des services Web. Sonar fonctionne en effectuant des requêtes HTTP ou HTTPS à partir de plusieurs points de présence dans le monde entier vers une URL que vous spécifiez.

Notions de base du sonar

Les points de terminaison testés par Sonar sont considérés vers le haut ou vers le bas selon les critères suivants :

- Les demandes qui aboutissent à HTTP 2xx sont considérées comme des succès et tout autre résultat, y compris les problèmes réseau et les délais d'expiration, est traité comme des échecs.
- Sonar suit les réponses de redirection qui retournent des codes d'état 3xx, pour un maximum de 6 redirections, jusqu'à ce qu'il reçoive une réponse non-3xx ou qu'une erreur se produise.
- Le statut du paramètre est déterminé en fonction du quorum des emplacements déclarants. Sonar signale le résultat (succès ou échec) qui est retourné par la plupart des points de présence.

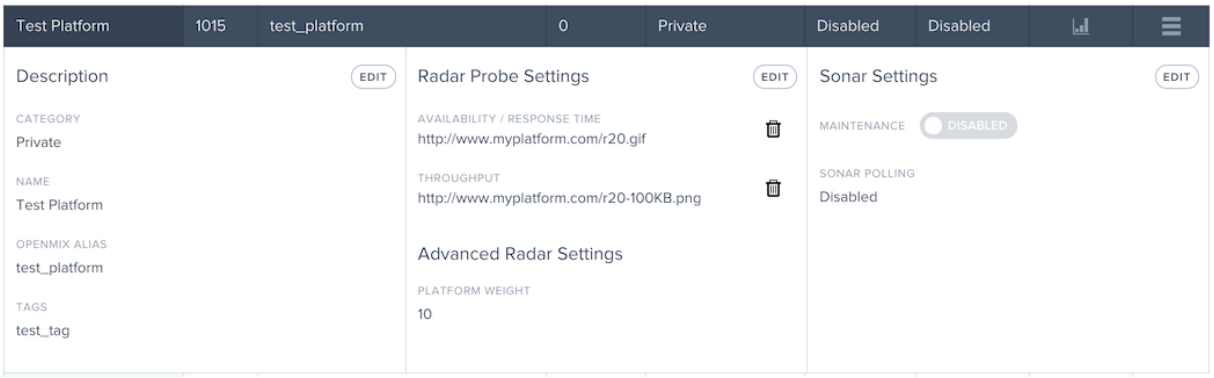
Les contrôles sonar sont effectués à partir de plusieurs sites d'essai du monde entier. Les emplacements comprennent :

- Singapour
- South Carolina, États-Unis
- Tokyo, Japon
- St Ghislain, Belgique
- Washington, Etats Uni
- New York, États-Unis
- Londres, Angleterre
- Hong Kong
- Francfort, Allemagne
- Dublin, Irlande
- Iowa, États-Unis
- Virginia, États-Unis
- Amsterdam, Pays-Bas

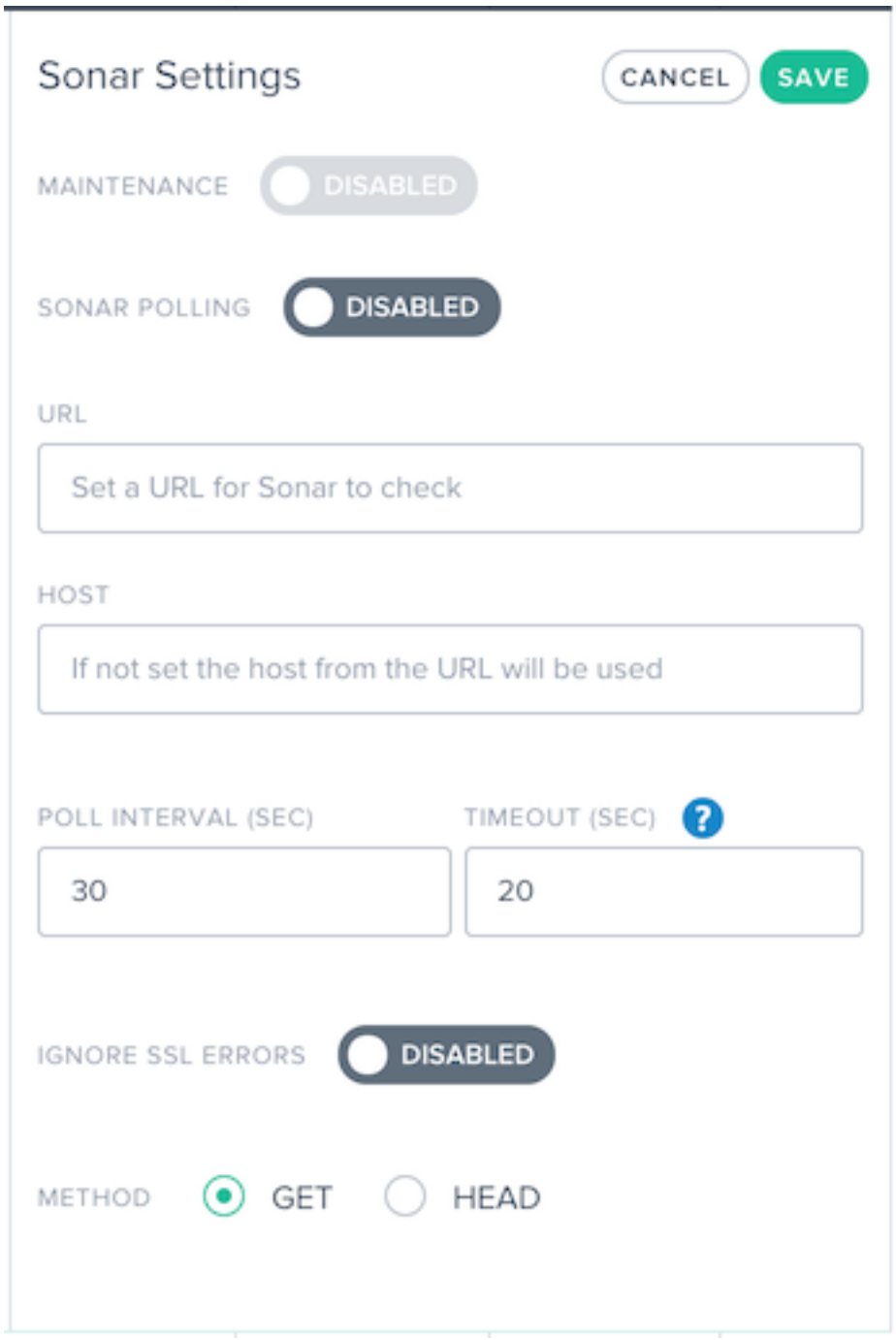
La plateforme Sonar est étroitement intégrée aux services de plateforme Radar, Fusion et Openmix. Les données sonar sont transmises en temps réel à tous les nœuds Openmix à travers le monde, pour être utilisées comme une entrée supplémentaire pour la prise de décision.

Configuration du sonar de plate-forme

Sonar est configuré pour chaque plate-forme de laPlates-formespage. Cliquez sur une plate-forme dans la liste pour voir la section **Paramètres du sonar** .



Pour ajouter la surveillance Sonar à la plate-forme, cliquez sur le bouton **Modifier** dans la section **Paramètres Sonar** .

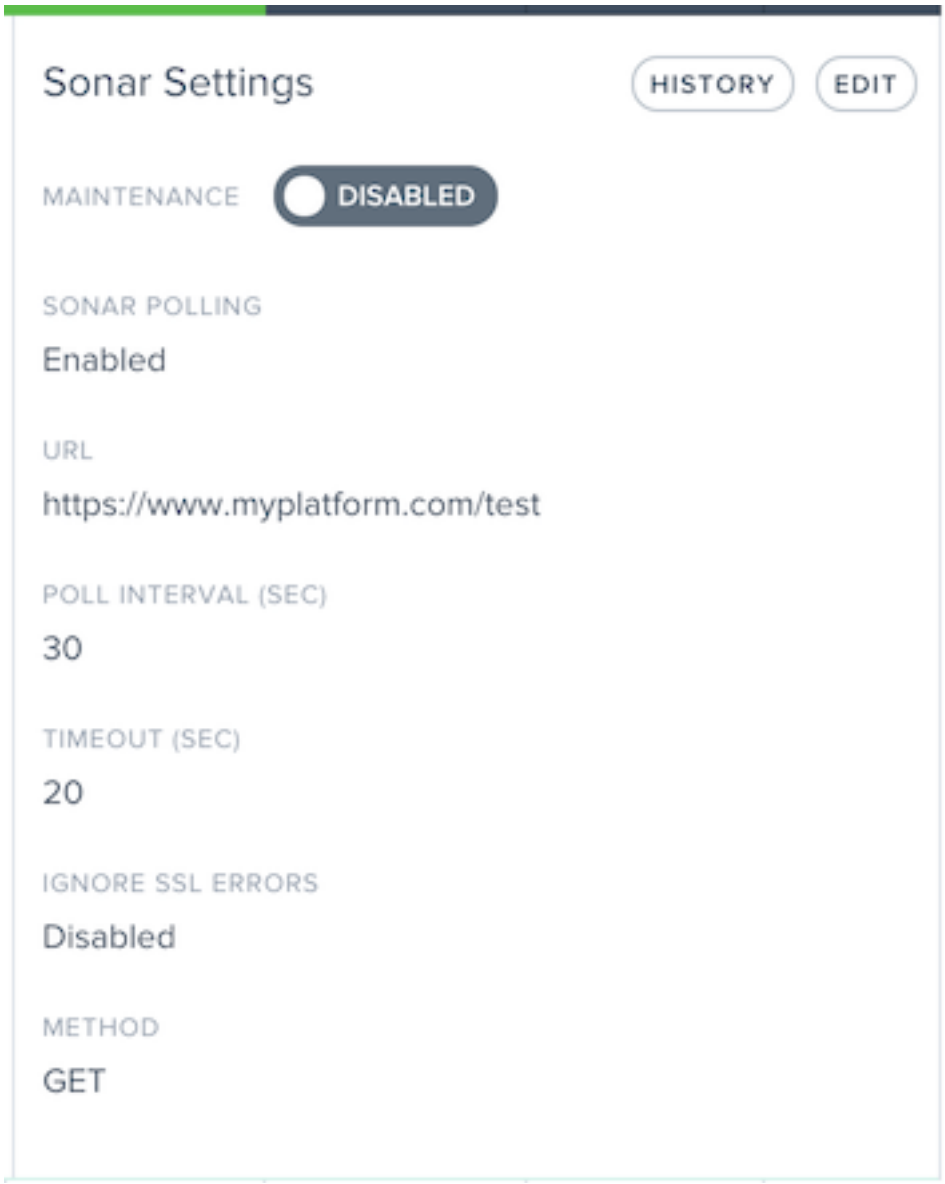


Une description des champs est ci-dessous :

Élément de saisie	Description	Mode par défaut
Maintenance	Lorsque cette option est activée, Sonar signale que le service est en panne, quel que soit l'état réel. Ceci est utile lorsque vous souhaitez supprimer une plate-forme du routage Openmix en prévision de temps d'arrêt.	Désactivé
Sonar Sondage	Si cette option est activée, Sonar vérifiera l'URL configurée.	Désactivé
URL	L'URL Sonar appelle pour vérifier la disponibilité du service.	
Hôte	Valeur qui doit être utilisée pour la valeur d'en-tête Host dans la demande.	v
Intervalle de sondage	Fréquence spécifiée en secondes pour tester la disponibilité du service. Les contrôles peuvent avoir un intervalle minimum de 1 seconde jusqu'à 300 secondes (5 minutes).	60 v
Délai d'expiration	Durée spécifiée en secondes pour attendre une réponse avant de supposer qu'une vérification échoue au service. Les contrôles peuvent avoir un délai d'expiration minimum de 1 seconde jusqu'à 30 secondes. Pour les intervalles de sondage inférieurs, par exemple en dessous de 5 secondes, le délai d'attente est limité à 4 secondes.	20

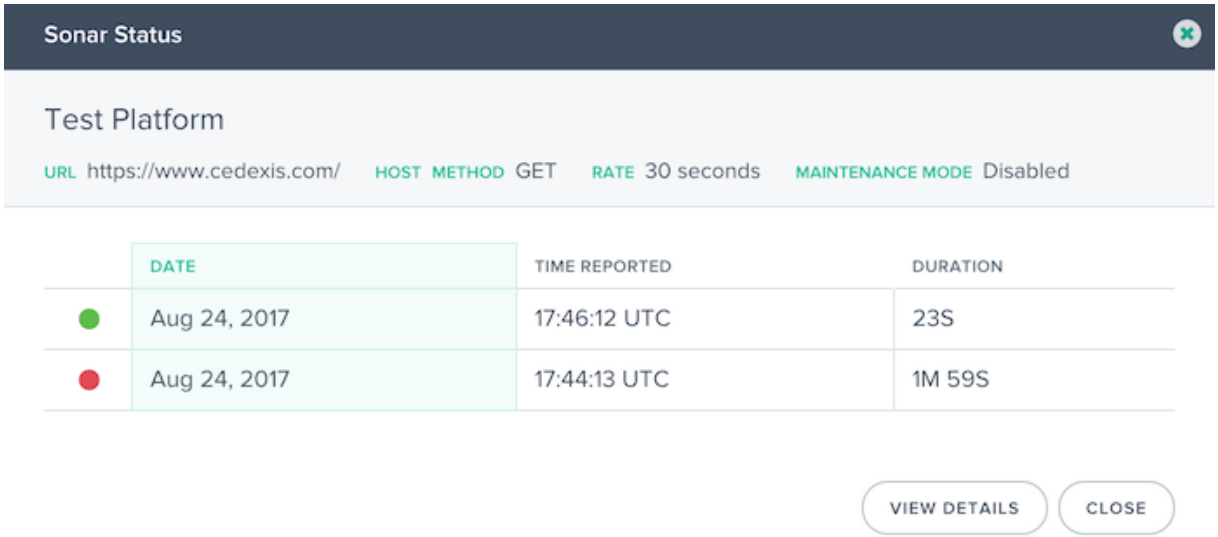
Élément de saisie	Description	Mode par défaut
Ignorer les erreurs SSL	Lorsque cette option est activée, Sonar ignore les erreurs SSL qui se produisent pendant la demande, telles qu'un certificat SSL mal configuré.	Désactivé
Méthode	La méthode HTTP utilisée pour la vérification : GET ou HEAD.	

Pour activer Sonar, basculez l'**interrogation Sonar** sur **Activé** et entrez l'URL du service. Cliquez sur **Enregistrer** et les vérifications démarrent.



Lorsque le Sonar est activé, les paramètres affichent les paramètres Sonar actuels.

Une fois le Sonar activé, vous pouvez cliquer sur le bouton **Historique** dans la section **Paramètres du Sonar** pour voir les changements récents d'état et la durée. Cliquez sur le bouton **Afficher les détails** pour accéder à la page État de la plate-forme Sonar pour plus de détails et des rapports d'état à long terme.



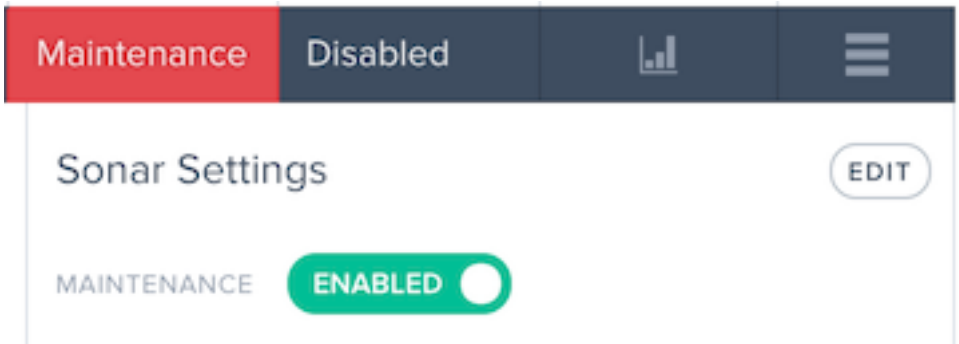
Statut du sonar de la plate-forme

Lorsque le Sonar est activé pour une plate-forme, l'état du Sonar est affiché dans la liste des plates-formes de la colonne **Sonar** . Lorsque la surveillance du sonar est vérifiée par rapport à la plate-forme, la cellule de colonne est verte et affiche le temps pendant lequel la plate-forme a été accessible.

Si les vérifications de surveillance de la plate-forme ont échoué, la cellule **Sonar** est rouge et affiche le temps pendant lequel la plate-forme est inaccessible.

Mode de maintenance

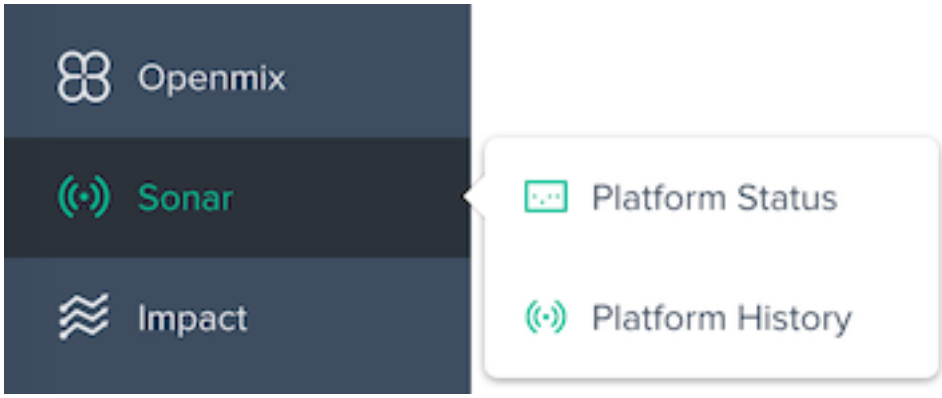
L'état Sonar affiche la disponibilité du service en fonction du succès ou de l'échec des contrôles synthétiques. Si vous souhaitez marquer la plate-forme comme étant **abaissée** même si elle est accessible, en prévision de la maintenance sur la plate-forme par exemple, vous pouvez activer le mode Maintenance. Ce mode signale que la plate-forme n'est pas disponible dans les applications Openmix et empêche automatiquement le trafic d'être livré à la plate-forme dans toute application Openmix sur laquelle Sonar est activé.



Activer le mode Maintenance, basculez l'option **Maintenance** sur **Activé** .

Une fois activé, l'élément de liste de plate-forme affiche l'état du sonar comme **Maintenance**.

Menu Sonar



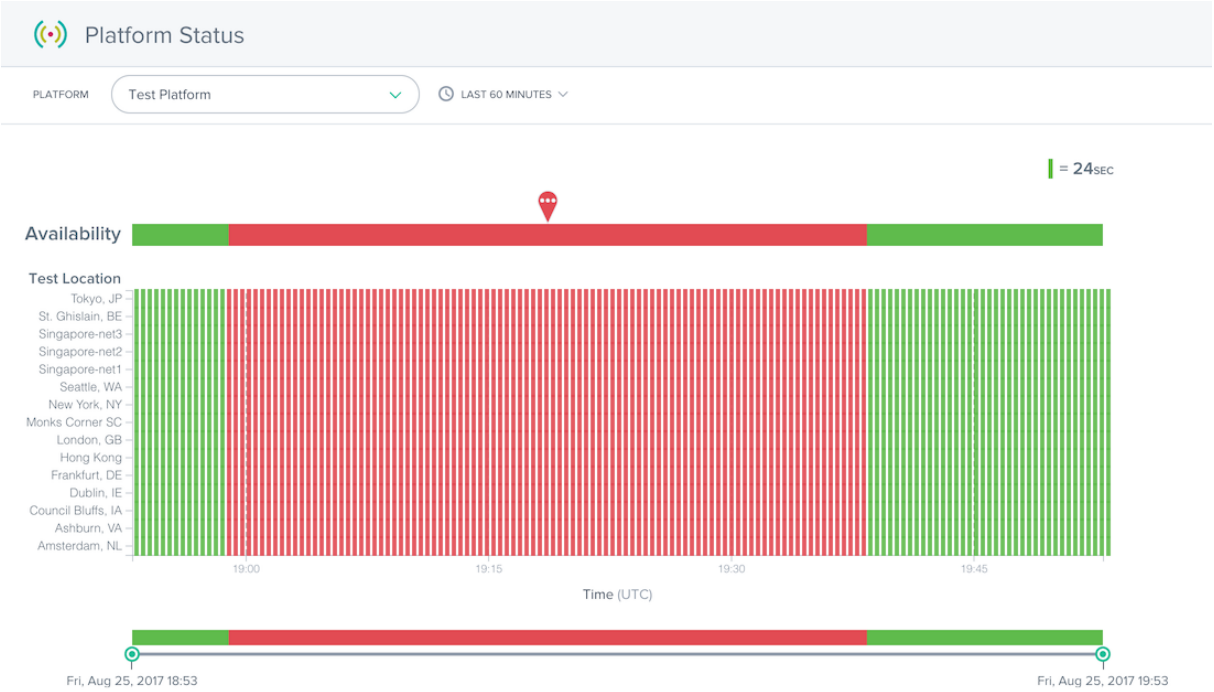
Le menu **Sonar** se compose des options suivantes :

1. **État de la plate-forme** —Résultats détaillés par emplacement de test et état de disponibilité global.
2. **Historique de la plateforme** —Vue d'ensemble de l'état de disponibilité au cours des trois derniers mois.

État de la plate-forme

Le rapport Sonar Platform Status présente les détails des vérifications effectuées par chaque emplacement de test et l'état global calculé à partir des données agrégées.

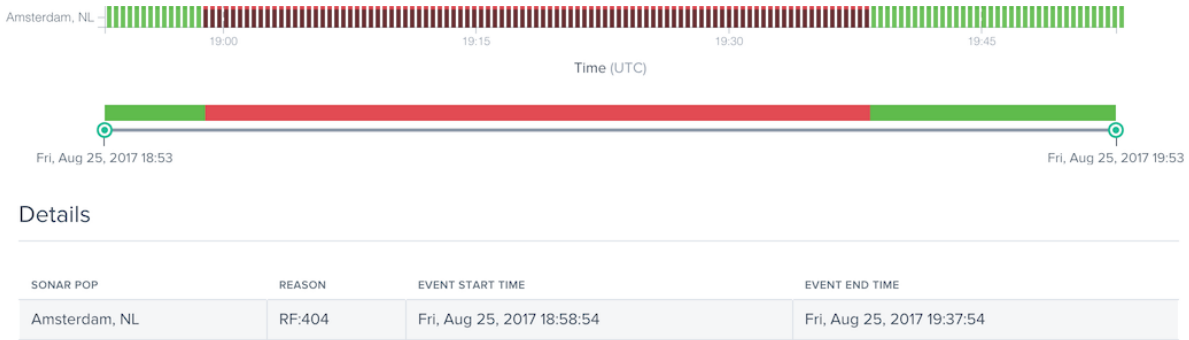
Pour obtenir des informations sur une plate-forme spécifique, sélectionnez une plate-forme dans le menu **Plateformes**.



Le rapport Statut contient les sections suivantes :

- Disponibilité : en haut du rapport se trouve la disponibilité signalée à Openmix sur la base des résultats agrégés des emplacements de test individuels. Il s'agit du statut Sonar utilisé dans les applications Openmix pendant les durées spécifiées.
- Emplacements de test : Les résultats de chaque emplacement de test sont affichés.
- Curseur temporel : Le curseur temporel vous permet de percer facilement des périodes détaillées. Faites glisser les curseurs de temps pour ajuster la période du rapport et afficher des intervalles de temps plus détaillés.

Les détails des vérifications échouées peuvent être affichés en cliquant sur un marqueur rouge dans une ligne d'emplacement de test. Les détails des échecs d'essai seront présentés dans la section **Détails** sous le rapport.

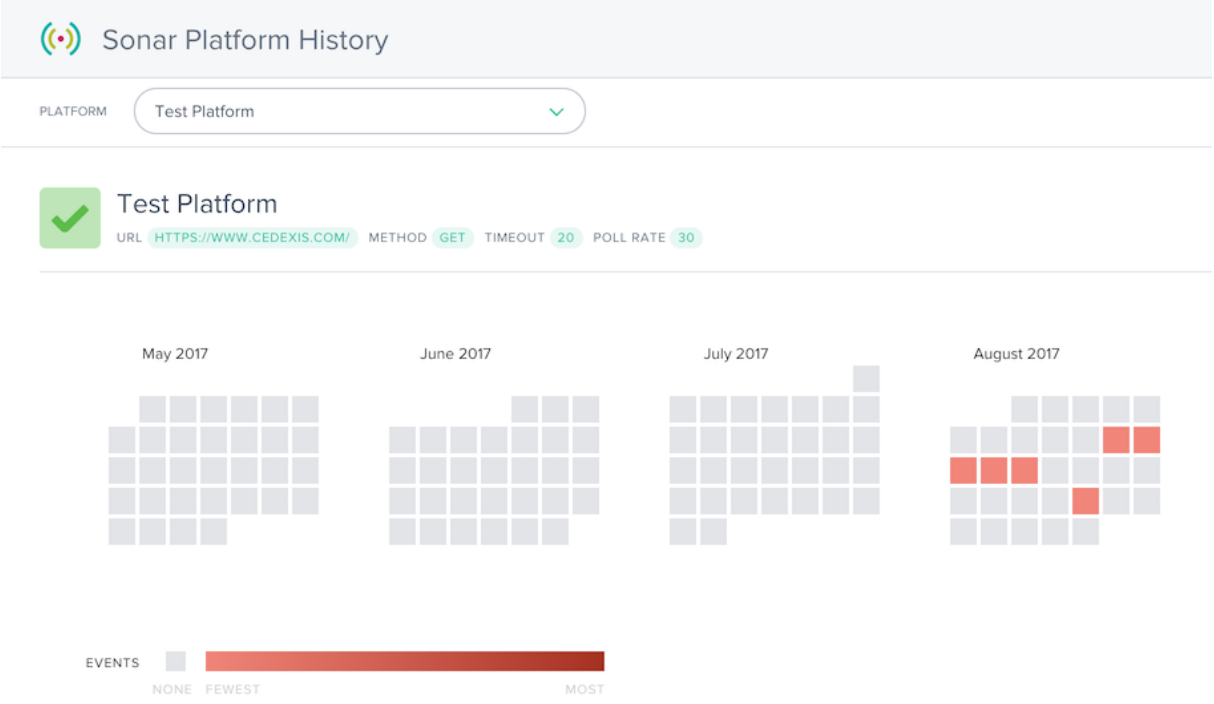


La colonne **Motif** fournit des détails tels que le code d'erreur qui a été renvoyé à partir des vérifications sonar effectuées dans cet emplacement de test.

Historique de la plateforme

Le rapport Sonar Platform History présente l'état de disponibilité des contrôles agrégés effectués par chaque emplacement de test au cours des derniers mois.

Pour obtenir des informations sur une plate-forme spécifique, sélectionnez une plate-forme dans le menu **Plateformes**.



Le rapport Historique affiche un calendrier des derniers mois. Les jours qui ont des pannes de service sont affichés en dégradés de rouge. Plus il y a d'événements de disponibilité qui se sont produits le jour, plus il est affiché.

Sous le calendrier se trouve une liste des pannes de service qui se sont produites et quelques détails de base sur les événements.

Details

DATE	OUTAGES	START TIME - FIRST OUTAGE	END TIME - LAST OUTAGE	DURATION
2017-08-11	1	21:29:35	23:59:59	2 hours, 30 minutes, 25 seconds
2017-08-12	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-13	1	00:00:00	23:59:59	24 hours, 0 minutes, 0 seconds
2017-08-14	1	00:00:00	21:21:18	2 days, 23 hours, 51 minutes, 43 seconds
2017-08-15	3	14:50:00	15:50:05	0 hours, 4 minutes, 3 seconds
2017-08-24	3	17:44:12	18:03:21	0 hours, 15 minutes, 25 seconds

Vous pouvez cliquer sur le jour calendrier ou la date dans les colonnes **Détails** pour charger le rapport

Statut pour plus de détails sur la panne de service.

Impact

June 4, 2021

Impact offre une vue puissante des données sur les performances et les indicateurs de performance clés de l'entreprise collectées pendant que les visiteurs sont sur votre site. Cliquez sur le lien correspondant aux données de reporting qui vous intéressent pour en savoir plus.

Rapports de visualisation de la plate-forme cloud

Le menu **Impact** se compose des options suivantes :

1. Données de synchronisation de navigation —Détails de performances au niveau de la page, également connus sous le nom de rapports sur le temps de chargement des pages.
2. Données de lecture vidéo —Qualité de l'expérience et données de livraison vidéo.
3. Données de synchronisation des ressources —Détails des performances des ressources individuelles sur les pages.

Données de synchronisation de navigation

September 13, 2023

Les rapports de chronométrage de navigation offrent un aperçu puissant des données détaillées sur le chargement des pages et les performances des événements collectées lorsque les visiteurs consultent votre site. Après une brève description des rapports, vous trouverez des détails sur la manière de faire pivoter, de filtrer et de personnaliser les rapports de synchronisation de navigation.

Rapports de chronométrage de navigation

Le menu **Navigation Timing** inclut les rapports suivants :

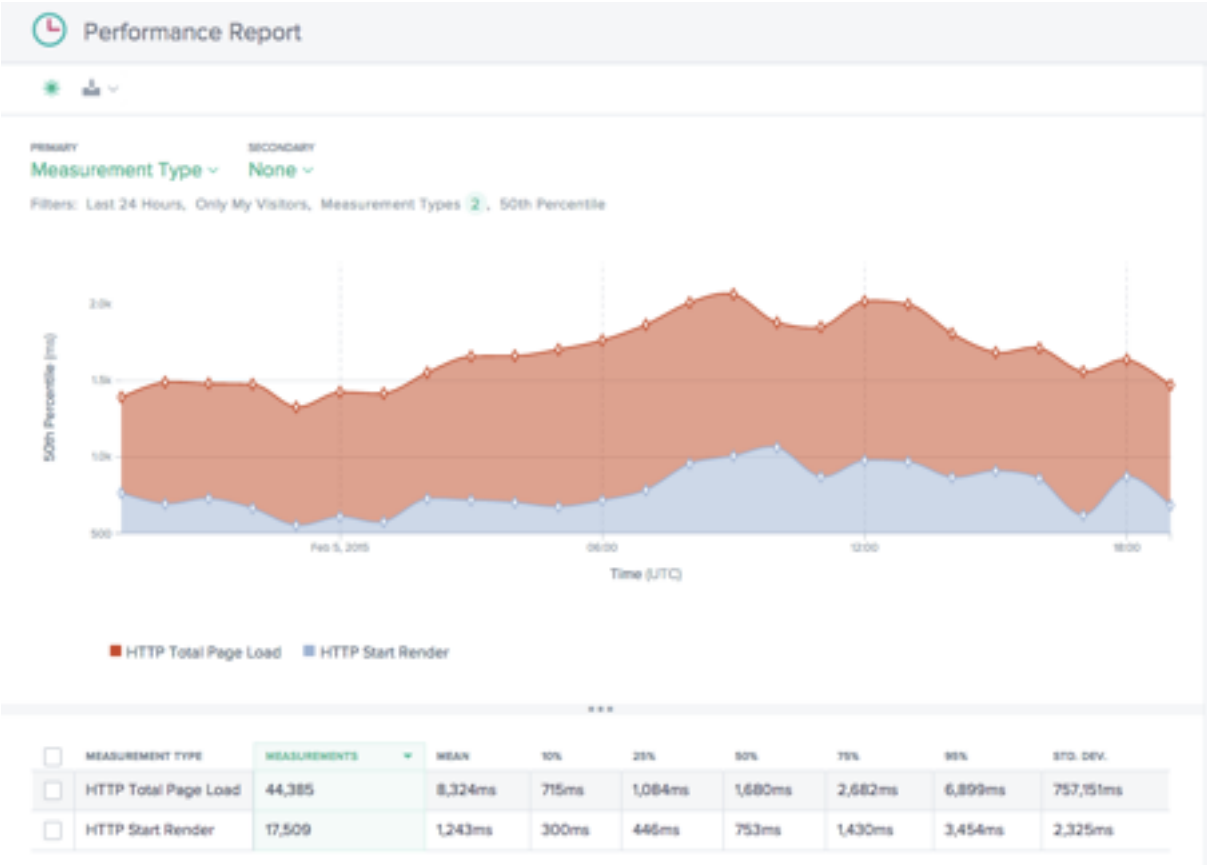
1. Rapport**de géolocalisation** —**Rapport** sur le temps de navigation par dimension géographique.
2. **Rapport de performance** —Données de mesure du temps de navigation au fil du temps.
3. **Rapport de distribution statistique** —Vue des données de chronométrage de navigation par le biais d'une vue de rapport de distribution statistique.

Rapport de géolocalisation

Ce rapport indique les performances en matière de temps de chargement des pages pour chaque pays. Zoomez sur la carte pour obtenir une plus grande granularité selon les besoins.

Le tableau répertorie chaque pays avec les performances associées au temps de chargement des pages, ainsi que le nombre de mesures (pages vues).

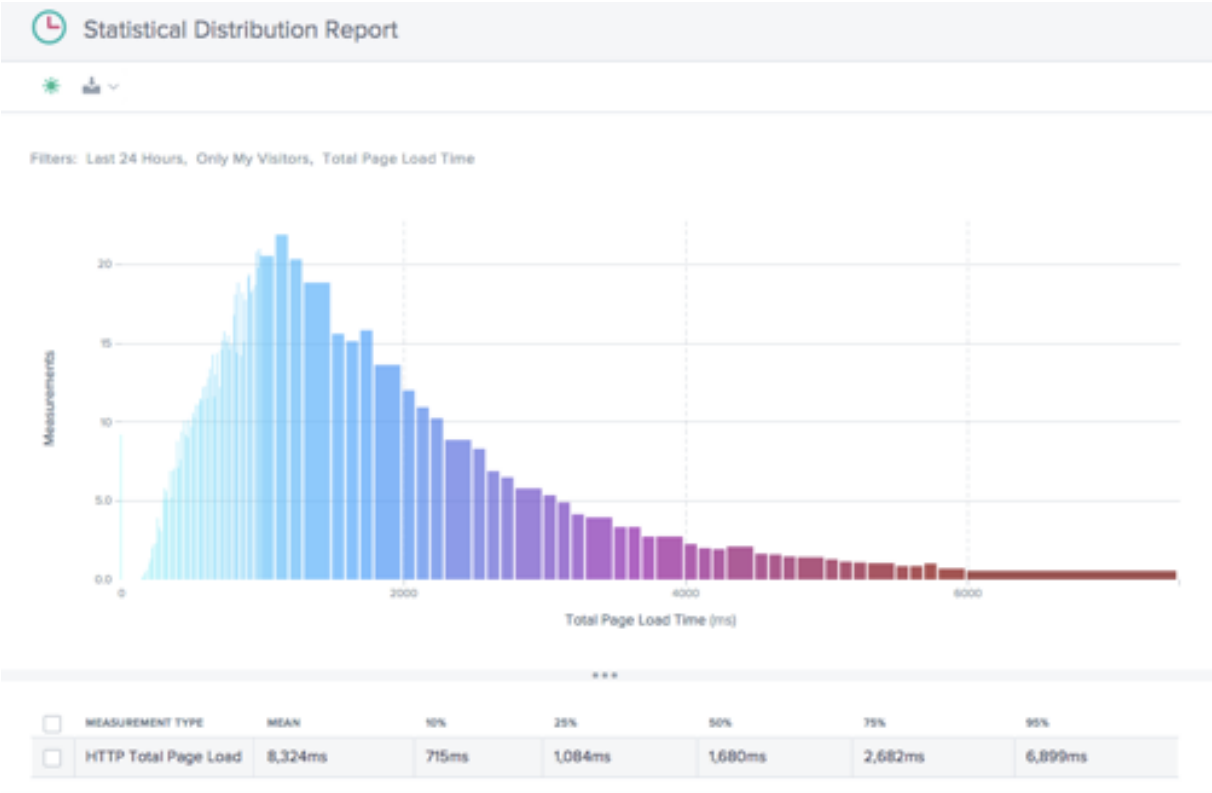
Rapport sur le rendement



Ce rapport présente les performances du KPI de synchronisation de navigation au fil du temps, ventilées par type de mesure.

Par défaut, Démarrer le rendu et Temps de chargement total de la page sont sélectionnés. D'autres types de mesures peuvent être ajoutés selon les besoins.

Rapport de distribution statistique



Ce rapport présente la distribution statistique des valeurs relatives au temps de navigation et au temps de chargement des pages.

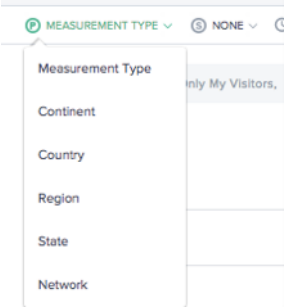
Le rapport donne un aperçu du nombre de mesures (pages vues) collectées par valeur de temps de chargement de page.

Utilisation des rapports de chronométrage de navigation

Pour affiner et personnaliser les vues des rapports en fonction de besoins spécifiques en matière de rapports, utilisez les fonctionnalités suivantes dans les rapports de synchronisation de navigation.

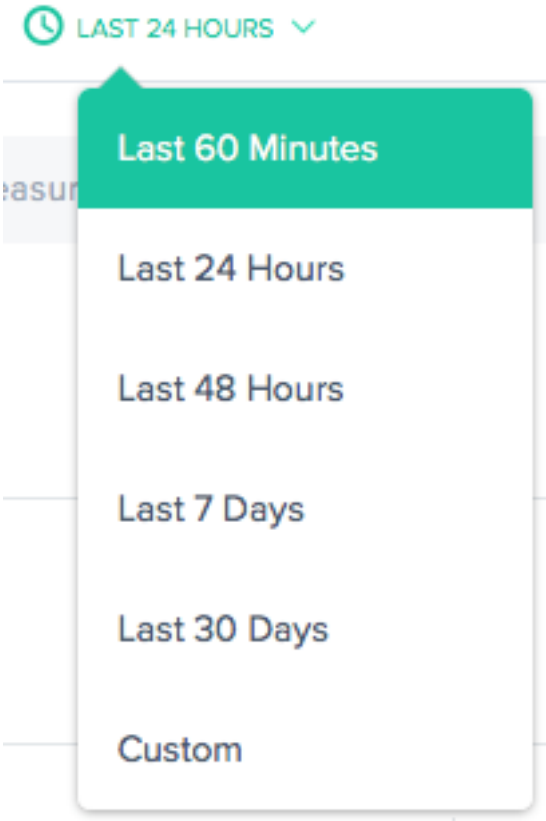
Outre les fonctionnalités standard des rapports telles que le partage de rapports, le basculement en arrière-plan, l'exportation de données, etc., les fonctionnalités suivantes sont disponibles :

Dimensions principales et secondaires



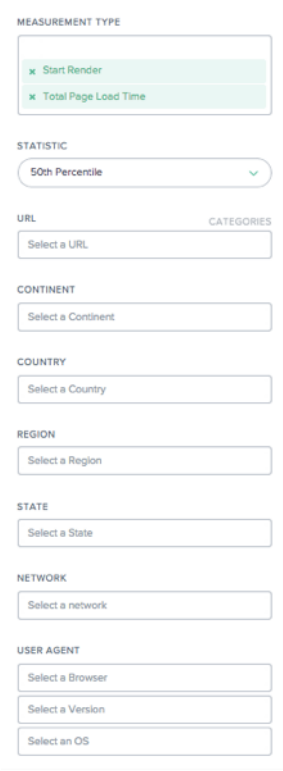
La dimension principale du graphique est sélectionnée via une liste de sélection située au-dessus du graphique. Utilisez-le comme un puissant pivot dans le rapport pour exprimer les données en termes de type de mesure (par défaut), de continent, de pays, de région, d'État ou de réseau (ASN). Une dimension secondaire peut également être choisie pour affiner davantage le rapport.

Filtre : Période du rapport



Les rapports peuvent être générés avec une plage de temps comprise entre les 60 dernières minutes, les 24 dernières heures, les 48 dernières heures, les 7 derniers jours, les 30 derniers jours ou une plage personnalisée. La vue par défaut est la dernière 24 heures.

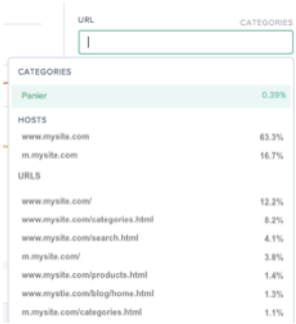
Filtres : puissantes fonctionnalités d'exploration vers le bas



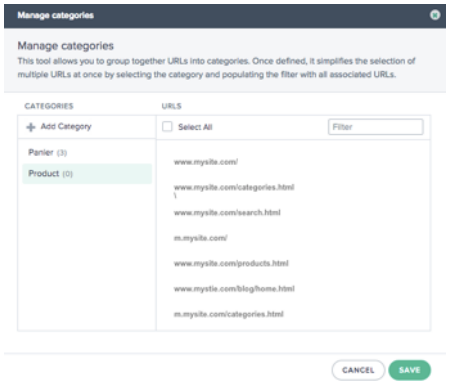
Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les informations suivantes sont disponibles dans les rapports de synchronisation de navigation :

- **Type de mesure** : sélectionnez un ou plusieurs types de mesures à afficher. Lancer le rendu et le temps de chargement total de la page sont sélectionnés par défaut.
- **Statistique** : sélectionnez une mesure statistique pour afficher les données.
- **URL** —Sélectionnez une ou plusieurs URL à afficher. Vous pouvez également sélectionner un nom d'hôte ou une catégorie d'URL (voir ci-dessous).
- **Continent** —Sélectionnez un ou plusieurs continents à inclure
- **Pays** —Sélectionnez un ou plusieurs pays à inclure
- **Région** —Sélectionnez une ou plusieurs régions géographiques (le cas échéant) à inclure
- **État** —Sélectionnez un ou plusieurs états géographiques (le cas échéant) à inclure
- **Réseau** —Sélectionnez un ou plusieurs réseaux (ASN) à inclure
- **Agent utilisateur** —Sélectionnez un ou plusieurs navigateurs, une version de navigateur et/ou un système d'exploitation pour affiner davantage les données de reporting.

Catégories d'URL



Les rapports de chronométrage de navigation peuvent être filtrés par URL, hôtes ou catégories. Trouvez rapidement un ou plusieurs éléments intéressants en les saisissant dans le champ de **recherche de l'URL** .



Pour créer une catégorie, cliquez sur **CATÉGORIES** sur le côté droit de la zone **URL** . La boîte de dialogue **Gérer les catégories** apparaît.

Sélectionnez **Ajouter une catégorie** pour créer une catégorie et la nommer comme vous le souhaitez. Sélectionnez ensuite les URL qui vous intéressent pour la nouvelle catégorie. Pour trouver des URL, commencez simplement à taper dans le champ de recherche et la liste d'URL sera filtrée en fonction du texte de recherche.

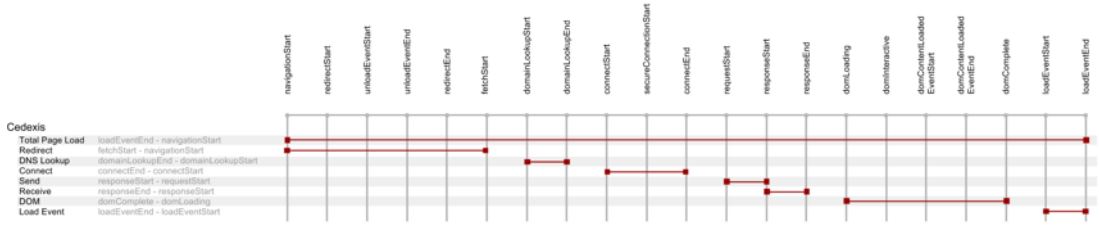
Lorsque toutes les URL ont été sélectionnées pour la catégorie, cliquez sur le bouton **Enregistrer** pour terminer la définition de la **catégorie** .

Données relatives au temps de navigation et au temps de chargement des pages

La balise Radar est capable de collecter des informations détaillées sur les performances de téléchargement des pages qui implémentent la balise. Les informations de performance de l'API NavTiming sont collectées à partir des navigateurs compatibles avec l'API (Chrome 6.5+, Firefox 8+, IE9+).

NetScaler affiche ces informations sur le portail du client, où il lui permet de voir les performances réelles des utilisateurs finaux lorsqu'ils interagissent avec vos pages Web.

Vous trouverez ci-dessous un schéma et une description de chacune des mesures de chargement de page fournies par Radar via Navigation Timing :



Mesure	Description	Calcul du temps de navigation
Chargement total de la page	Le téléchargement complet de la page Web et de ses composants correspondants.	`loadEventEnd - navigationStart`
Rediriger	Durée initiale utilisée pour la redirection vers la page.	`fetchStart - navigationStart`
Recherche DNS	Le temps nécessaire à la résolution DNS pour terminer l'URI de la page de base.	`domainLookupEnd - domainLookupStart`
Connecter	Le moment d'établir une connexion TCP, y compris le protocole SSL s'il est utilisé.	`connectEnd - connectStart`
Envoyer	Le temps de requête et de réponse HTTP de la page de base initiale, à l'exclusion de tout corps de message. C'est un bon indicateur de la latence du serveur principal.	`responseStart - requestStart`
Recevez	Le temps nécessaire pour recevoir le corps HTML du document de base.	`responseEnd - responseStart`
DOM	Il est temps de télécharger tous les médias, les objets appelés à partir du code HTML de base et de les charger dans le navigateur.	`domComplete - domLoading`

Mesure	Description	Calcul du temps de navigation
Charger l'événement	Durée d'exécution de tout code JavaScript et de rendu de la page dans le navigateur.	`loadEventEnd` – `loadEventStart`
Démarrer le rendu	L'heure de début du rendu est le premier moment où un élément a été mis à disposition à l'écran.	Plus de timing ajouté par Chrome/IE en tant qu' extension à l'API NavTiming.

Données de lecture vidéo

June 4, 2021

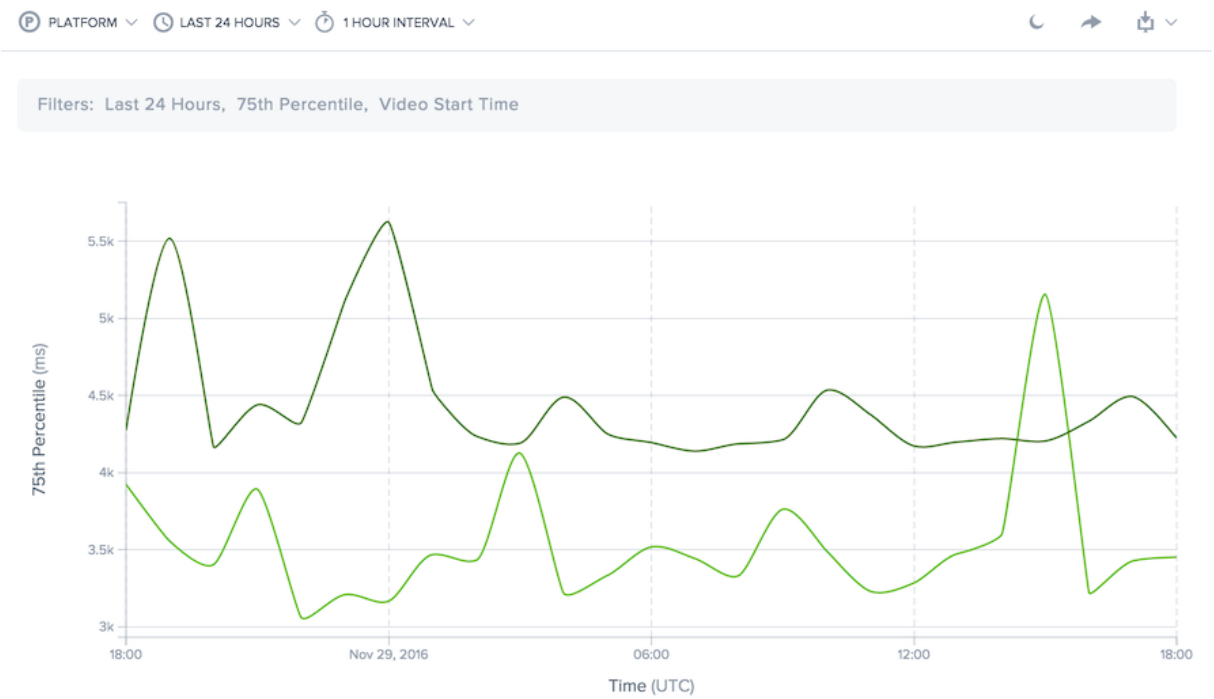
Cloud Platform Visualization recueille les performances de livraison de réseau vidéo les plus pertinentes et la qualité des données d'expérience pour la création de rapports. La qualité vidéo de l' expérience est directement influencée par la qualité de la livraison de morceaux vidéo. Openmix optimise en fonction des mesures de diffusion du réseau Radar pour offrir la meilleure expérience de visualisation possible aux utilisateurs. Après une brève description des rapports, vous trouverez des détails sur la façon de faire pivoter, filtrer et personnaliser les rapports.

Rapports de lecture vidéo

Le menu **Données de lecture vidéo** comprend les rapports suivants :

1. **Rapport de performance** —Expérience vidéo et données de livraison au fil du temps.
2. **Rapport de distribution statistique** —Variation de l'expérience de visionnement vidéo au fil du temps.
3. **Rapport de comparaison des histogrammes** - Comparez les données de livraison de morceaux vidéo avec les indicateurs de qualité d'expérience.

Rapport sur le rendement



Ce rapport présente l'expérience de visionnage vidéo au fil du temps. Il vous permet de visualiser les tendances de diffusion au fil du temps, de voir la quantité de vidéos regardées et la qualité globale de l'expérience de visionnage.

Les données peuvent être visualisées avec des dimensions qui permettent de comparer plusieurs valeurs. Par exemple, les données peuvent être visualisées par domaine pour comparer les performances de la diffusion sur plusieurs domaines vidéo.

La période de temps pour le rapport peut être personnalisée depuis les 60 minutes les plus récentes jusqu'à 30 jours au cours des 13 derniers mois.
Les données peuvent être filtrées en fonction de la plate-forme utilisée pour servir le contenu, le nom d'hôte et le chemin d'accès du contenu ou des morceaux vidéo, de l'emplacement géographique, du réseau ou de l'agent utilisateur de la visionneuse.

Rapport sur la distribution statistique

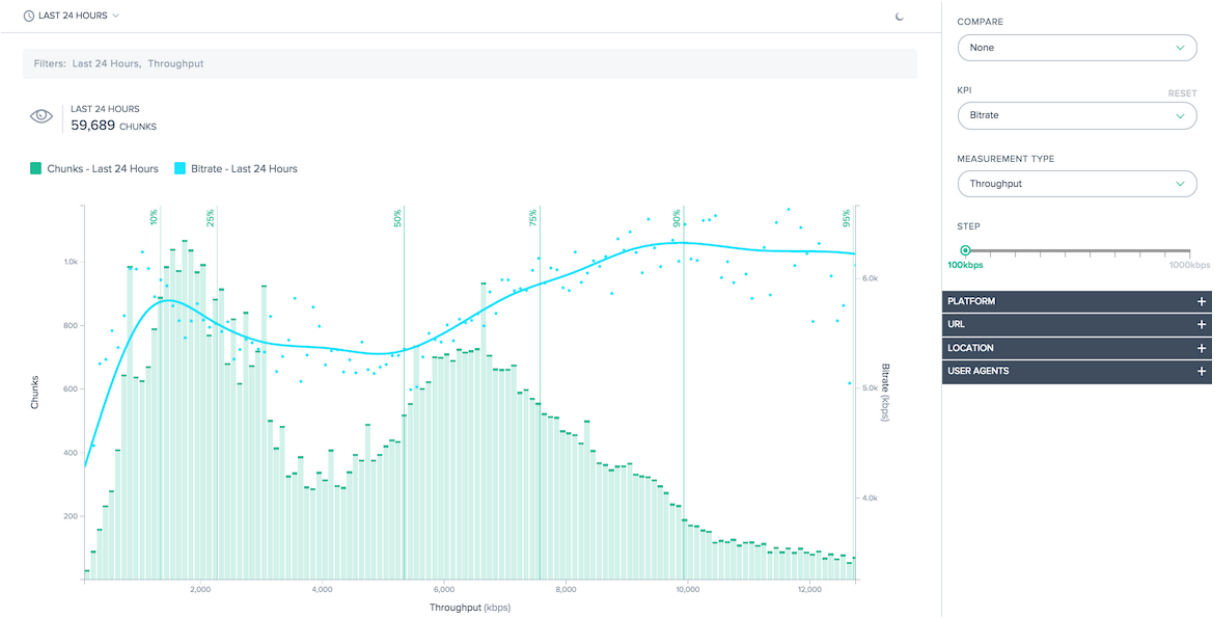
Ce rapport montre la variation de l'expérience de visionnement vidéo au fil du temps. Il vous permet de visualiser la manière dont la vidéo est diffusée de manière cohérente et de mieux comprendre les expériences de visionnage pour l'ensemble de la population d'utilisateurs. Le rapport calcule les performances de l'utilisateur aux 10e, 25e, 50e, 75e et 95e percentiles et la moyenne.

À l'instar du rapport sur les performances, les données peuvent être affichées avec des dimensions qui permettent de comparer plusieurs valeurs. Par exemple, les données peuvent être visualisées par plate-forme (fournisseur de services ou serveur) afin de comparer la cohérence de la livraison pour plusieurs plates-formes.

La période de temps pour le rapport peut être personnalisée depuis les 60 minutes les plus récentes jusqu'à 30 jours au cours des 13 derniers mois.

Les données peuvent être filtrées en fonction de la plate-forme utilisée pour servir le contenu, le nom d'hôte et le chemin d'accès du contenu ou des morceaux vidéo, de l'emplacement géographique, du réseau ou de l'agent utilisateur de la visionneuse.

Rapport de comparaison des histogrammes



Ce rapport traite des relations entre les données de distribution de morceaux vidéo et la qualité de l'expérience KPI.

Ce rapport comporte deux caractéristiques principales :

- L'histogramme montre la fréquence à laquelle des morceaux vidéo ont été livrés avec un niveau de qualité spécifié, soit Temps de réponse, soit Débit.
- Les indicateurs de clés individuels peuvent être superposés sur l'histogramme. Les lignes graphiques de l'indicateur de performance clé produit lorsqu'un morceau a été livré avec le niveau de qualité spécifié.

Par exemple, l'histogramme montrerait le débit de bloc mesuré par Radar. Les indicateurs de performances clés montreront probablement que le débit binaire est plus élevé et que la mise en mémoire tampon est plus faible lorsque le débit mesuré est plus élevé. Ensemble, ces fonctionnalités permettent de quantifier la relation entre la qualité de la livraison et la qualité de l'expérience produite pour le spectateur.

Si la génération de rapports par défaut n'est pas suffisante, la taille du compartiment de l'histogramme peut être personnalisée et des sections spécifiques de la distribution peuvent être sélectionnées pour l'affichage.

En plus de lier les histogrammes aux indicateurs de résultats clés, les données peuvent être comparées directement. Plusieurs indicateurs de performance clés peuvent être sélectionnés pour être consultés et les périodes précédentes peuvent être comparées pour afficher les changements dans les performances au fil du temps.

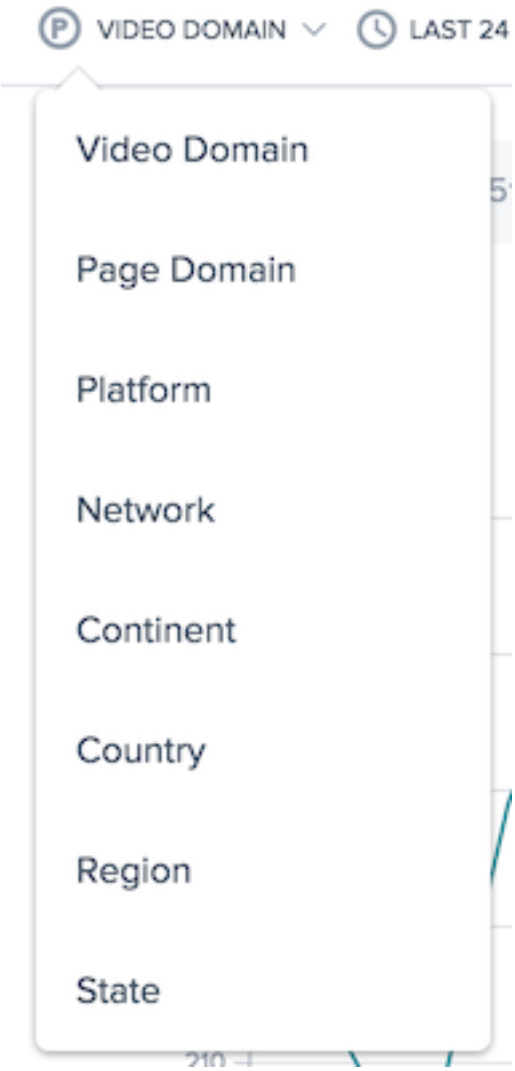
Les données peuvent être filtrées en fonction de la plate-forme utilisée pour servir le contenu, le nom d'hôte et le chemin d'accès du contenu ou des morceaux vidéo, de l'emplacement géographique, du réseau ou de l'agent utilisateur de la visionneuse.

Utilisation des rapports de lecture vidéo

Pour affiner et personnaliser les affichages de rapport en fonction des besoins spécifiques de création de rapports, utilisez les fonctionnalités suivantes dans les rapports Performance et Statistical Distribution Video Playback.

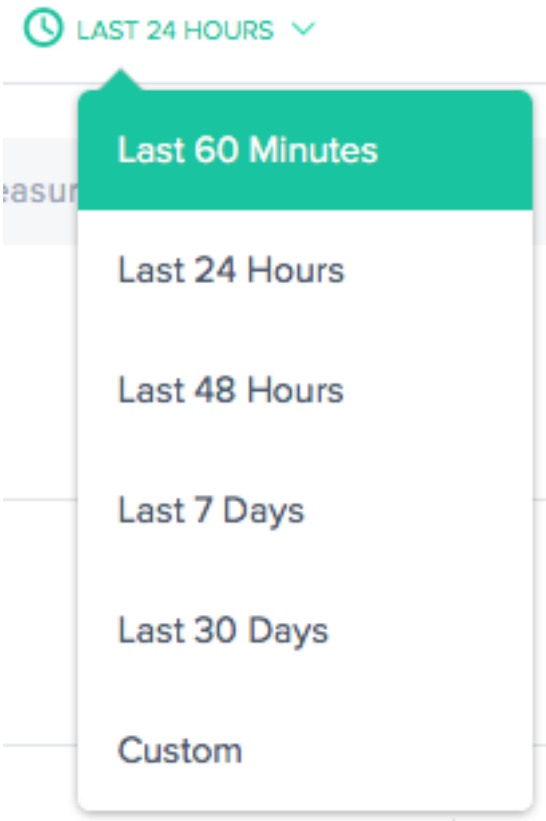
Outre les fonctionnalités standard des rapports, telles que le partage de rapports, le basculement en arrière-plan, l'exportation de données, etc., les fonctionnalités suivantes sont disponibles :

Dimension principale



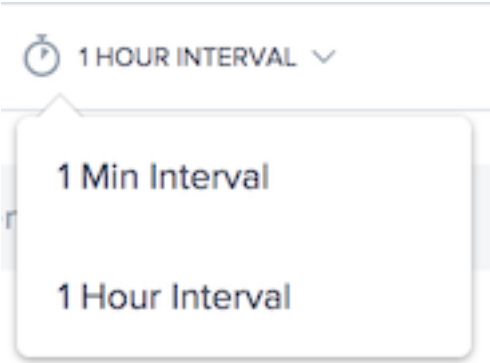
La dimension principale du graphique est sélectionnée dans une liste de sélection située au-dessus du graphique. Utilisez ceci comme un pivot puissant sur le rapport pour exprimer les données en termes de domaine vidéo, de domaine de page, de plate-forme, de réseau (ASN), de continent, de pays, de région ou d'état.

Filtre : Plage de temps du rapport



Les rapports peuvent être générés avec une plage de temps de 60 dernières minutes, 24 dernières heures, 48 dernières heures, 7 derniers jours, 30 derniers jours ou une plage personnalisée. La vue par défaut est la dernière 24 heures.

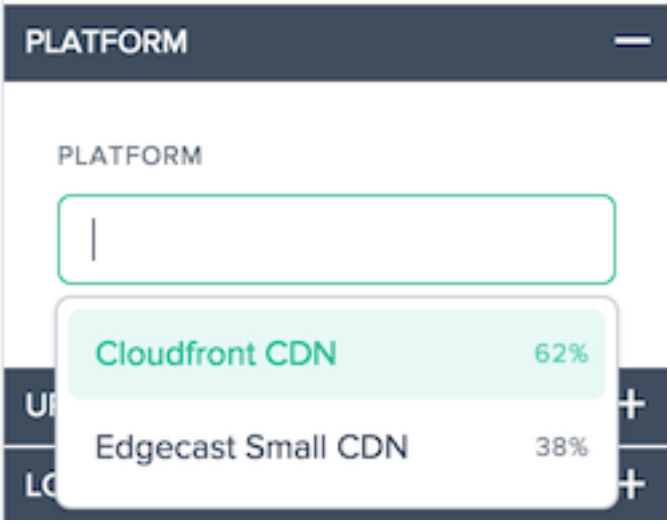
Intervalle de rapport



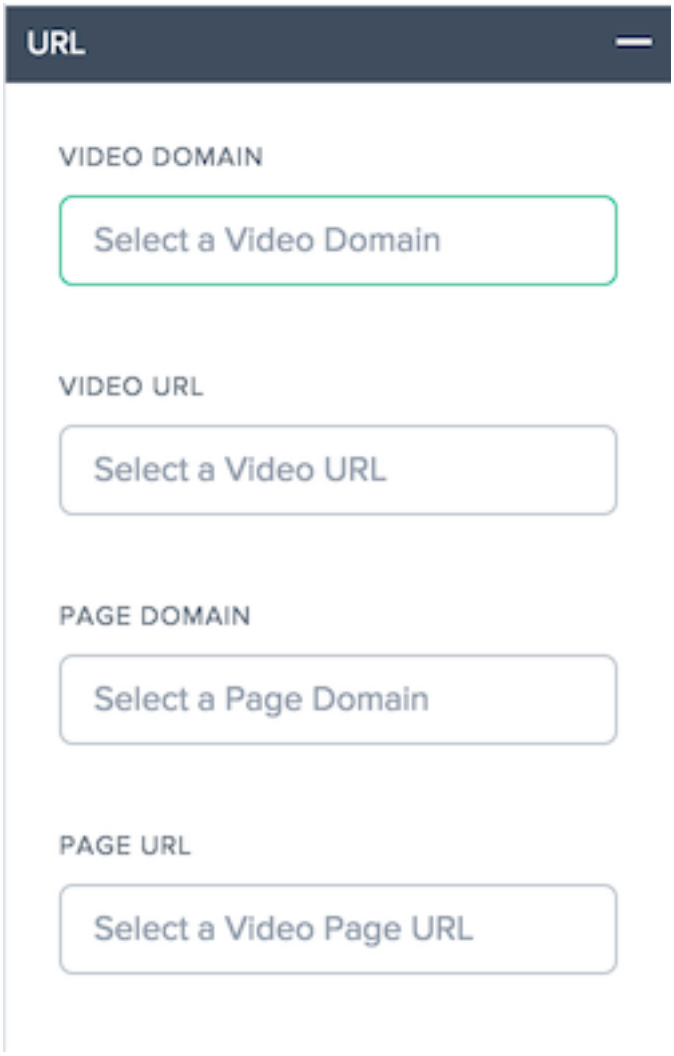
La dimension principale du graphique est sélectionnée dans une liste de sélection située au-dessus du graphique. Cela permet de produire des rapports granulaires sur les données de performance.

Filtres : Puissantes capacités d'exploration vers le bas

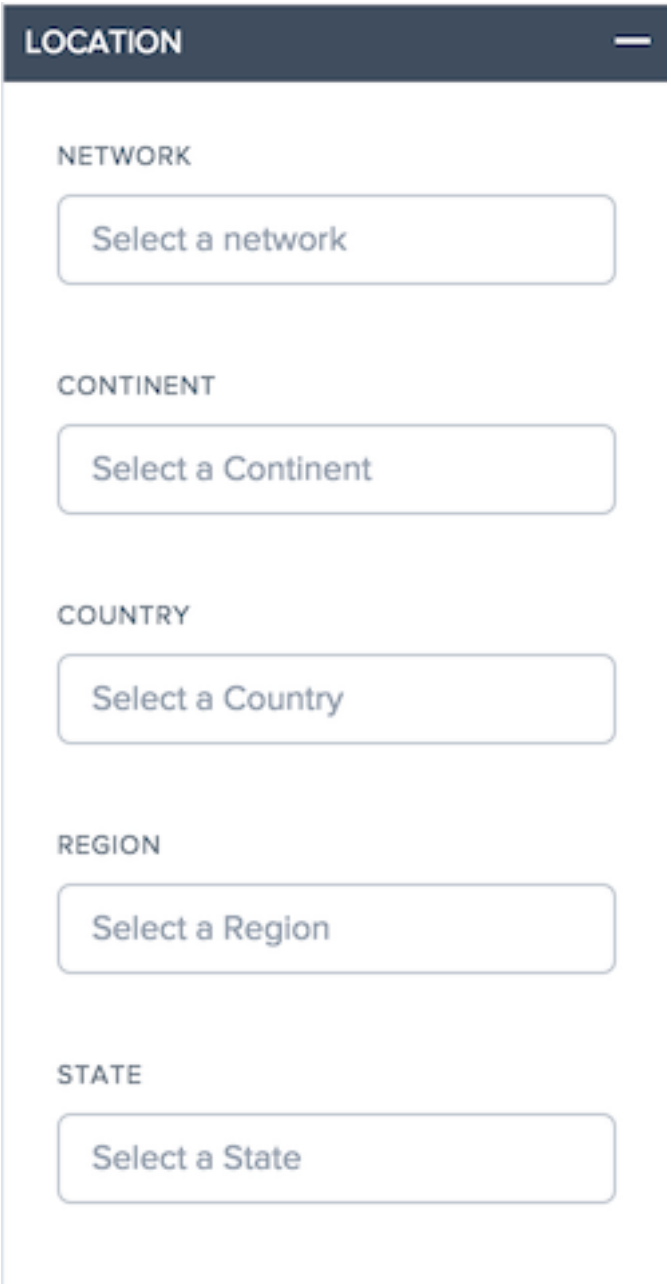
Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les informations suivantes sont disponibles dans les rapports Lecture vidéo :



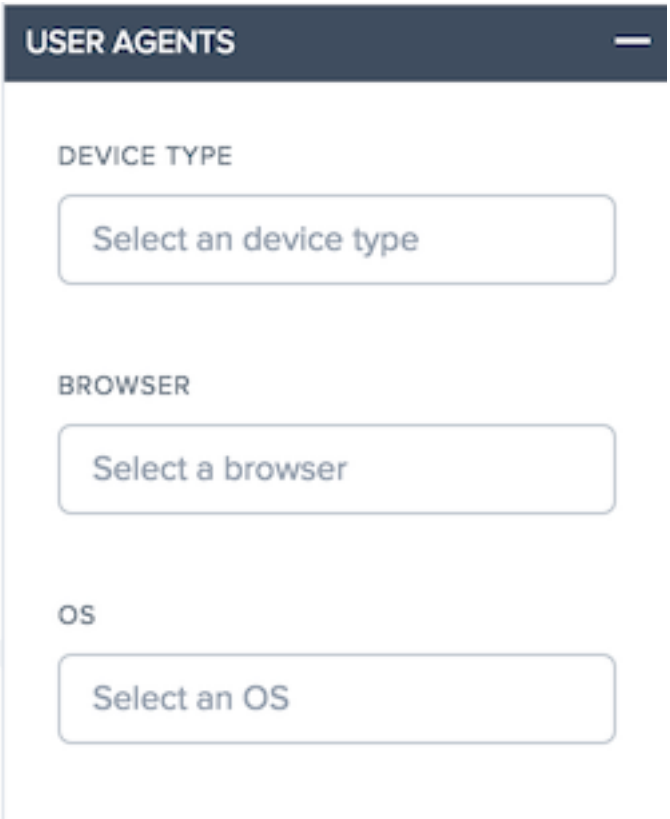
- **Plateforme** - Sélectionnez une ou des plates-formes à filtrer, par défaut toutes les plates-formes sont incluses dans le rapport.



- **Domaine vidéo** : sélectionnez un ou plusieurs noms d'hôte sur lesquels les vidéos sont hébergées. Par défaut, tous les noms d'hôte sont inclus dans le rapport.
- **URL de la vidéo** - Sélectionnez un ou plusieurs chemins pour les vidéos, par défaut tous les chemins sont inclus dans le rapport.
- **Domaine de page** : sélectionnez un ou plusieurs noms d'hôte sur lesquels les pages sont hébergées. Par défaut, tous les noms d'hôte sont inclus dans le rapport.
- **URL de la page** - Sélectionnez un ou plusieurs chemins pour les pages, par défaut tous les chemins sont inclus dans le rapport.



- **Réseau** —Sélectionnez un ou plusieurs réseaux (ASN) à inclure
- **Continent** —Sélectionnez un ou plusieurs continents à inclure
- **Pays** —Sélectionnez un ou plusieurs pays à inclure
- **Région** —Sélectionnez une ou plusieurs régions géographiques (le cas échéant) à inclure
- **État** —Sélectionnez un ou plusieurs états géographiques (le cas échéant) à inclure

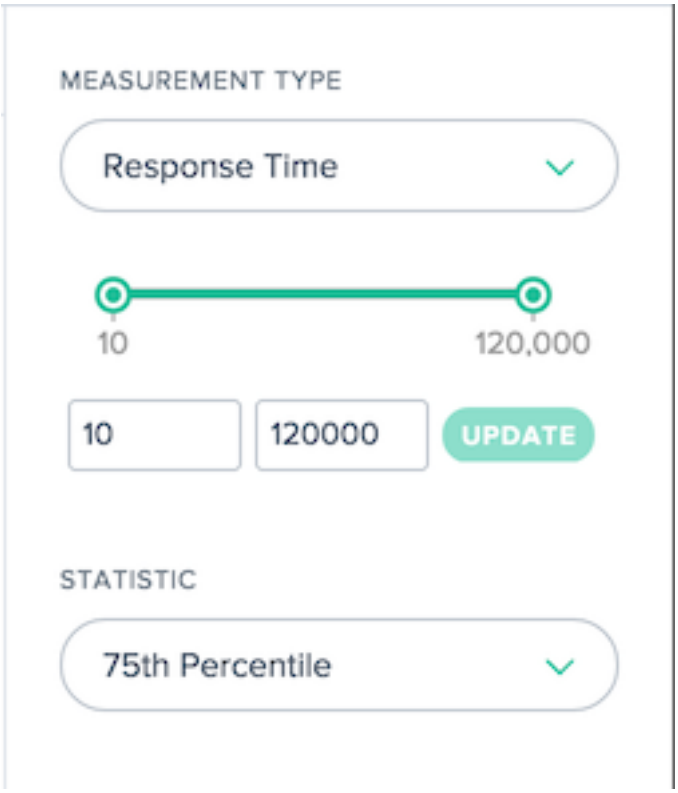


- **Agent utilisateur** : sélectionnez un ou plusieurs types de périphériques, navigateurs et/ou types de système d'exploitation pour affiner les données de rapport.

Utilisation du rapport de performances de lecture vidéo

Pour affiner et personnaliser le rapport sur les performances en fonction des besoins spécifiques de reporting, utilisez les fonctionnalités suivantes dans le rapport Performances.

Filtres : Puissantes capacités d'exploration vers le bas



Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les informations suivantes sont disponibles dans les rapports Lecture vidéo :

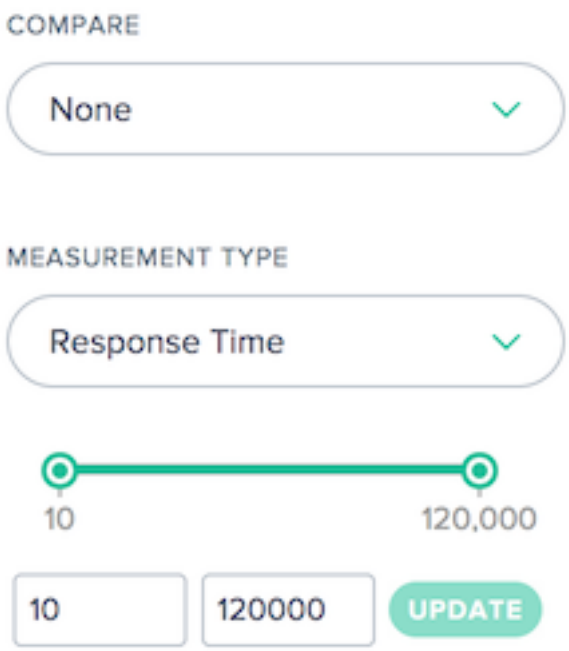
- **Type de mesure** : sélectionnez le type de mesure à afficher, le temps de réponse est initialement sélectionné.
- **Curseur de compte** - Filtrer les données en fonction du nombre de mesures minimum et maximum requis pour être inclus dans le rapport.
- **Statistique** : sélectionnez la mesure statistique à afficher.

En plus de ces filtres spécifiques au rapport, les filtres de lecture vidéo standard sont disponibles pour personnaliser les résultats.

Utilisation du rapport de distribution statistique de lecture vidéo

Pour affiner et personnaliser le rapport en fonction des besoins spécifiques de reporting, appliquez les fonctionnalités suivantes dans le rapport Distribution statistique.

Filtres : Puissantes capacités d'exploration vers le bas



Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les informations suivantes sont disponibles dans les rapports Lecture vidéo :

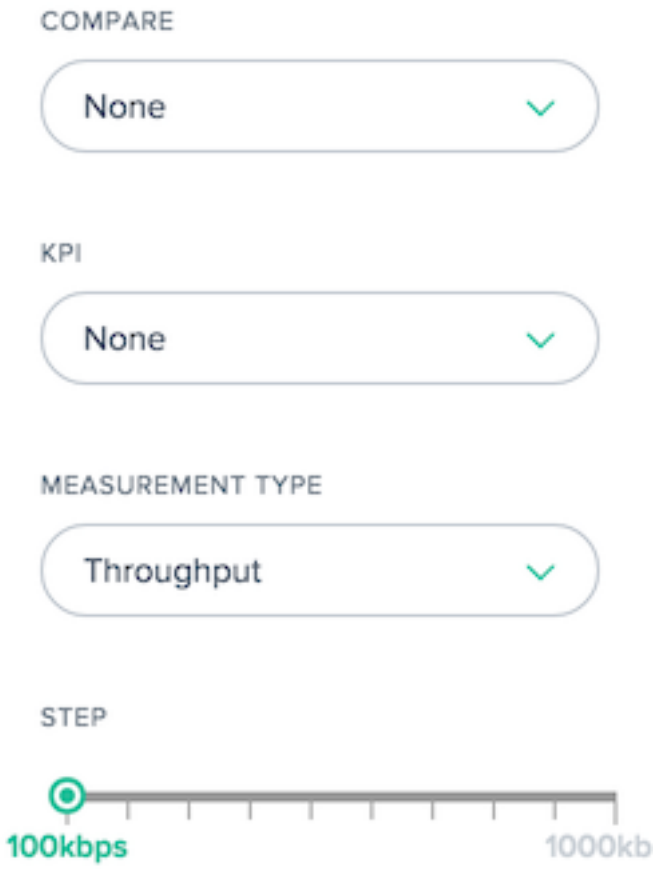
- **Comparer** : sélectionnez la valeur utilisée pour créer une comparaison dans le rapport. En fonction de la sélection effectuée, les valeurs spécifiques utilisées pour comparer doivent être sélectionnées. Les distributions résultantes seront affichées côte à côte afin qu'elles puissent être facilement comparées.
- **Type de mesure** : sélectionnez le type de mesure à afficher, le temps de réponse est initialement sélectionné.
- **Curseur de compte** - Filtrer les données en fonction du nombre de mesures minimum et maximum requis pour être inclus dans le rapport.

En plus de ces filtres spécifiques au rapport, les filtres de lecture vidéo standard sont disponibles pour personnaliser les résultats.

Utilisation du rapport de comparaison des histogrammes de lecture vidéo

Pour affiner et personnaliser le rapport en fonction des besoins spécifiques de reporting, appliquez les fonctionnalités suivantes dans le rapport Comparaison des histogrammes.

Filtres : Puissantes capacités d'exploration vers le bas



Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les rapports suivants sont disponibles dans les rapports Comparaison des histogrammes :

- **Comparer** : sélectionnez la valeur utilisée pour créer une comparaison dans le rapport. En fonction de la sélection effectuée, les valeurs spécifiques utilisées pour comparer doivent être sélectionnées. Les histogrammes et les indicateurs clés qui en résultent seront superposés les uns aux autres afin qu'ils puissent être facilement comparés.
- **Indicateur de performance clé** : sélectionnez l'indicateur de performance clé qui est représenté sous forme de graphique par rapport au type de mesure de l'histogramme.
- **Type de mesure** : sélectionnez le type de mesure utilisé pour remplir l'histogramme.
- **Step Slider** - Définit la taille des compartiments utilisés pour générer l'histogramme.

En plus de ces filtres spécifiques au rapport, les filtres de lecture vidéo standard sont disponibles pour personnaliser les résultats.

Données de lecture vidéo

Les données sont collectées en utilisant les propriétés et les événements de l'Élément vidéo HTML5 pour la qualité des données d'expérience et l'API de synchronisation des ressources pour les données de bloc vidéo, à partir des navigateurs qui prennent en charge les API.

Les données vidéo sont affichées dans le portail, où des rapports peuvent être générés avec des informations sur la qualité de l'expérience de l'utilisateur final et les performances de la fourniture du réseau.

Voici un diagramme et une description de chacune des mesures vidéo collectées :

Mesure	Description
Temps de réponse par segment	Le temps nécessaire pour que les morceaux commencent la livraison en fonction des mesures de temporisation des ressources (`responseStart – requestStart`)
Débit par segment	Vitesse à laquelle les morceaux vidéo ont été téléchargés en fonction des mesures de synchronisation des ressources. (kbps)
Débit fourni	Débit binaire par seconde de la vidéo basé sur la taille des morceaux livrés. (ko)
Ratio de mise en mémoire tampon	Pourcentage de temps passé à mettre en mémoire tampon pendant la lecture. (%)
Échecs de démarrage vidéo	Temps de requête et de réponse HTTP de la page de base initiale, à l'exclusion de tout corps de message. Un bon indicateur de latence du serveur back-end.
Heure de démarrage de la vidéo	Le temps nécessaire pour démarrer la lecture vidéo après la tentative de lecture est effectuée. (ms)

Données de synchronisation des ressources

June 4, 2021

Généralités

Les données Resource Timing offrent une vue puissante de la performance des ressources individuelles au niveau objet de votre site Web.

Resource Timing aide les clients à examiner les performances réseau des objets de niveau page, en fonction des données que nous fournissons sur le temps de connexion, le temps de téléchargement et les différents temps de réponse. Exemples d'objets au niveau de la page : images, fichiers JavaScript, appels d'API, etc. Il offre aux clients une meilleure visibilité sur les performances au niveau de la page. Le résultat final est que les clients peuvent mieux gérer leur livraison et assurer une meilleure qualité globale de l'expérience utilisateur.

Les sections suivantes vous indiquent la configuration, la description des données et le reporting des données de synchronisation des ressources.

Configuration de la synchronisation des ressources

L'interface utilisateur du portail vous permet d'entrer directement les paramètres pour la configuration Resource Timing comme alternative au codage JSON.

Remarque : Même si la configuration via le codage JSON est toujours disponible, il est fortement recommandé d'utiliser l'interface utilisateur pour la configuration.

Navigation

Dans le volet de navigation gauche, choisissez Impact -> Resource Timing Data -> Resource Timing Configuration.

Première configuration

- Sélectionnez **Démarrer maintenant** dans la page d'ouverture pour commencer.
- Une boîte de dialogue **Paramètres de configuration par défaut** s'ouvre pour inclure ou exclure des ressources et entrer une fréquence d'échantillonnage.

Paramètres de configuration par défaut Les paramètres de configuration par défaut sont les paramètres minimum requis pour démarrer. Il existe trois principaux paramètres de configuration par défaut :

- Ressources à inclure et à exclure
- Taux d'échantillonnage
- Détection du fournisseur par défaut

Ressources à inclure ou à exclure Cette fonctionnalité vous permet d'inclure ou d'exclure des ressources spécifiques à partir de laquelle collecter des données de synchronisation. S'il est laissé vide, toutes les ressources sont incluses par défaut (c'est-à-dire que rien n'est exclu).

Vous pouvez entrer des ressources telles que, un nom de fichier, une extension de nom de fichier, un nom de dossier, un chemin d'accès de fichier ou même une chaîne. Tout ce qui se trouve dans la chaîne sera récupéré en tant que ressource.

Appuyez sur **Entrée** ou sur la touche **Retour** chaque fois que vous saisissez un nom de ressource pour la soumettre. Si vous saisissez des ressources spécifiques dans le champ **Inclure**, seules ces ressources sont incluses et toutes les autres ressources sont exclues. Pour exclure des ressources spécifiques, saisissez-les dans le champ **Exclure**, et tout le reste sera inclus. Vous pouvez même écrire une logique regex personnalisée pour personnaliser le processus d'inclusion ou d'exclusion.

Taux d'échantillonnage Le **taux d'échantillonnage** vous permet d'entrer un petit échantillon de visiteurs à partir de laquelle vous souhaitez collecter des données IRT. Entrez une valeur comprise entre 0 et 100 (prise en pourcentage). Idéalement, vous devez entrer le pourcentage le plus bas pour la fréquence d'échantillonnage - une valeur suffisante pour recueillir le nombre requis de mesures de synchronisation des ressources.

Remarque : La collecte des données de synchronisation des ressources impose une lourde charge au système. Cette fonctionnalité permet aux clients d'échantillonner des données et n'est pas destinée à collecter des données pour chaque session Radar.

Attention : Pour les clients disposant d'un volume élevé de données, commencez par un taux d'échantillonnage de 1 %. Augmentez-le lentement jusqu'à ce qu'un taux statistiquement utile soit atteint. Un taux d'échantillonnage élevé peut potentiellement provoquer une surcharge du serveur, un ralentissement ou même un plantage.

Étapes pour le premier réglage de la fréquence d'échantillonnage

1. Commencez par un taux d'échantillonnage de 1%. Attendez 24 à 48 heures jusqu'à ce que vous receviez quelques mesures.
2. Vérifiez le **graphique IRT** pour voir s'il semble lisse sur plusieurs actifs.
3. Si oui, laissez le taux d'échantillonnage à cette valeur, sauf si le client a un trafic Web élevé.
4. Sinon, si le graphique semble agité en raison du faible volume de données, tournez-le lentement.
5. Répétez tous les contrôles et continuez à augmenter lentement le taux (idéalement toutes les 24-48 heures) jusqu'à ce que vous receviez suffisamment de données (environ 10%).
6. Pour les clients à faible trafic Web, vous pouvez monter plus de 10%. Mais pour chaque petite augmentation, assurez-vous d'effectuer tous les contrôles mentionnés.

Sélectionnez **Suivant** pour accéder à la boîte de dialogue **Paramètres de détection du fournisseur par défaut** .

Détection du fournisseur par défaut La détection du fournisseur vous permet d'identifier le fournisseur ou la plate-forme à partir duquel la ressource est desservie. Entrez un nom d'hôte configuré pour détecter le fournisseur qui dessert la ressource. Vous pouvez entrer plusieurs noms d'hôtes et configurer la détection de fournisseur pour chacun d'eux individuellement. Reportez-vous à laDétection du fournisseursection pour plus d'informations sur la configuration de la détection de fournisseur.

Sélectionnez **Terminer** pour terminer la première configuration.

Sites

Les **données relatives au calendrier des ressources** sont réparties autour de trois domaines principaux :

1. **Sites**
2. **Configuration**
3. **Détection du fournisseur**

- Dans le volet de navigation gauche, accédez à **Impact -> Resource Timing Data -> Resource Timing**.
- La page **Sites** sous **Données de synchronisation des ressources** s'ouvre.

Entrez le nom d'hôte du site à partir de lequel vous souhaitez collecter les données de synchronisation des ressources. Sous **Sites**, vous trouverez la liste des noms d'hôtes qui se trouvent déjà dans le système. Si vous ne trouvez pas le site requis (nom d'hôte), vous pouvez l'entrer en cliquant sur le bouton **Ajouter** . La boîte de dialogue **Ajouter un site** vous permet d'ajouter un nouveau site pour configurer les données de synchronisation des ressources.

Configuration

Accédez à **Impact > Données temporelles des ressources > Configuration de synchronisation des ressources** dans le menu de navigation latéral du portail. La page **Sites** s'ouvre sous **Données de synchronisation des ressources** .

Dans la barre de navigation supérieure, choisissez **Configuration**.

Vous pouvez ajouter une nouvelle configuration en cliquant sur le bouton Ajouter dans le coin supérieur droit de la page.

Remarque : Vous pouvez également voir une liste de configurations, y compris la configuration par défaut, sur la page. Au lieu d'ajouter une nouvelle configuration, vous pouvez sélectionner une configuration par défaut ou en modifier une dans la liste.

Ajouter une configuration

Pour ajouter une nouvelle configuration, cliquez sur le bouton **Ajouter** dans le coin supérieur droit de la page.

La boîte de dialogue **Ajouter une configuration de temps de ressource** s'ouvre. Cela vous permet d'entrer un nouveau **nom**de configuration, d'ajouter **des ressources à inclure ou à exclure**, et d' ajouter le **taux d'échantillonnage**.

Modifier la configuration

Pour modifier une configuration existante, cliquez sur le bouton **Modifier la configuration** à côté du nom de la configuration.

Détection du fournisseur

La détection du fournisseur détermine quelle plate-forme gère une requête pour un domaine lorsque ce domaine est équilibré en charge derrière Openmix. Il est recommandé que tous les clients qui ont activé les données de synchronisation des ressources, configurent les services de détection des fournisseurs.

- Pour configurer la détection du fournisseur, accédez à **Impact > Resource Timing Data > Resource Timing Configuration** dans le volet de navigation gauche.
- La page **Sites** sous **Données de synchronisation des ressources** s'ouvre. Dans la barre de navigation supérieure, choisissez **Provider Detection**.

Cliquez sur le bouton Ajouter dans le coin supérieur droit de la page.

Dans la boîte de dialogue **Ajouter une configuration de détection de fournisseur**, entrez ce qui suit.

Nom de configuration

Entrez un nom pour la configuration. Le nom ne peut pas contenir d'espaces, ni de caractères spéciaux, et doit être unique.

Nom d'hôte

Entrez le nom d'hôte pour lequel vous souhaitez configurer la détection du fournisseur. Vous pouvez entrer plusieurs noms d'hôtes et spécifier des méthodes de détection pour chacun d'eux individuellement.

Méthode de détection

La méthode de détection implique de spécifier le type d'objet de test (standard ou personnalisé) et le chemin d'accès (vers l'objet de test) pour chaque nom d'hôte que vous avez entré.

Objets de test standard Dans le cas d'objets de test standard, le chemin d'accès peut être spécifié sous la forme, **/provider-detection/platform.html** et **/provider-detection/platform.png**. Pour cette configuration, **/provider-detection/** serait votre chemin d'accès au répertoire.

Remarque : Il n'est pas obligatoire d'entrer le chemin décrit ci-dessus. Cependant, pour tout chemin d'accès que vous entrez, assurez-vous que les fichiers **platform.html** et **platform.png** se trouvent dans le chemin d'accès au répertoire.

Objets de test personnalisés Dans le cas d'objets de test personnalisés, vous devez vous assurer que les objets de test sont trouvés dans le chemin exact que vous entrez. Par exemple, pour le nom d'hôte `foo.com` et le chemin d'accès `static/bar.css`, l'URL `http://foo.com/static/bar.css` doit être valide.

En-têtes

En-tête de plate-forme Si vous sélectionnez **En-tête de plate-forme**, assurez-vous que `X-CDN-Forward: <CDN name>` est envoyé sur les objets de test. Si `X-CDN-Forward: <CDN name>` est introuvable dans les en-têtes de réponse, le client passe au test suivant, qui peut être spécifié à l'aide de **Custom**.

Personnaliser Si vous sélectionnez **Personnalisé**, assurez-vous que l'expression régulière que vous entrez correspond exactement à l'un des en-têtes de réponse du CDN.

Si vous ajoutez plusieurs en-têtes de réponse, ils sont tous testés par rapport aux expressions régulières dans le même ordre que celui entré dans le portail.

Cliquez sur **Créer** pour terminer le processus. Vous voyez maintenant la configuration nouvellement créée dans la liste sous **Provider Detection**. Cliquez sur les icônes de modification ou de suppression si vous souhaitez modifier la configuration ou la supprimer.

Votre configuration est maintenant terminée. Pour configurer la détection de fournisseur alternativement via le codage JSON, contactez votre représentant de compte.

Description de la mesure du calendrier des ressources

Le tableau suivant présente les mesures de synchronisation des ressources collectées.

Mesure	Description	Calcul du calendrier des ressources
Heure de recherche DNS	Temps requis pour la résolution DNS de la ressource. Connue sous le nom de phase DNS.	`domainLookupEnd – domainLookupStart`
Heure de connexion TCP	Temps nécessaire à un navigateur pour établir la connexion avec un serveur. Connue sous le nom de phase TCP.	`connectEnd – connectStart`
Temps d'attente du premier octet (TTFB)	TTFB est la durée pendant laquelle un navigateur attend avant le début de la réception de la ressource.	`responseStart – startTime`
Temps aller-retour (RTT)	Temps écoulé entre le début de la demande et le début de la réponse. Connue sous le nom de phase de demande.	`responseStart – requestStart`
Temps d'attente	Différence entre le début de la réponse et la fin de la réponse. Connue sous le nom de phase de réponse. La réponse provient généralement d'un serveur, d'un cache ou d'une ressource locale.	`responseEnd – responseStart`
Durée	Temps total entre le début du processus et la réception complète de la ressource.	`responseEnd – startTime`

Pour en savoir plus, consultez https://www.w3.org/TR/resource-timing-1/#process

Rapports sur le calendrier des ressources

Le menu **Synchronisation des ressources** comprend les états suivants :

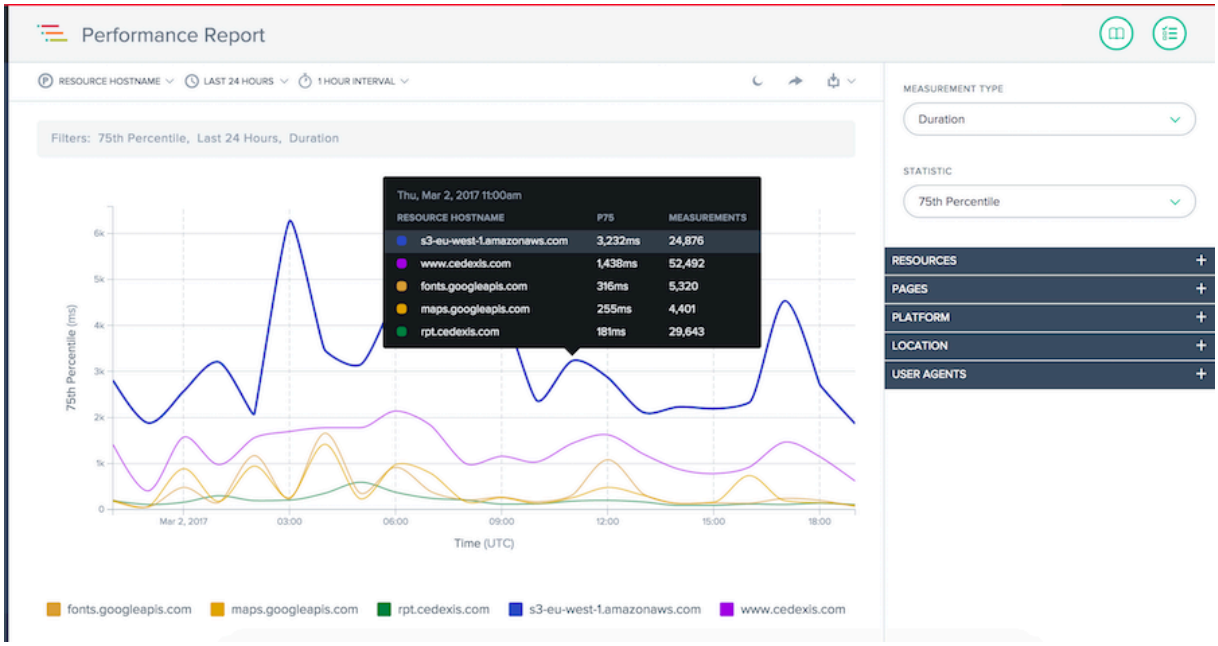
1. **Rapport sur le rendement** —Données sur la mesure du calendrier des ressources au fil du temps.
2. **Rapport de distribution statistique** : vue des données de synchronisation des ressources via une vue de rapport de distribution statistique.

Rapport sur le rendement

Le rapport donne un aperçu des données de performance relatives à la synchronisation des ressources dans le temps par valeur sélectionnée.

Affichage des rapports par défaut :

1. Dimension : Nom d'hôte de la ressource
2. Mesure : Durée
3. Plage de temps : dernières 24 heures



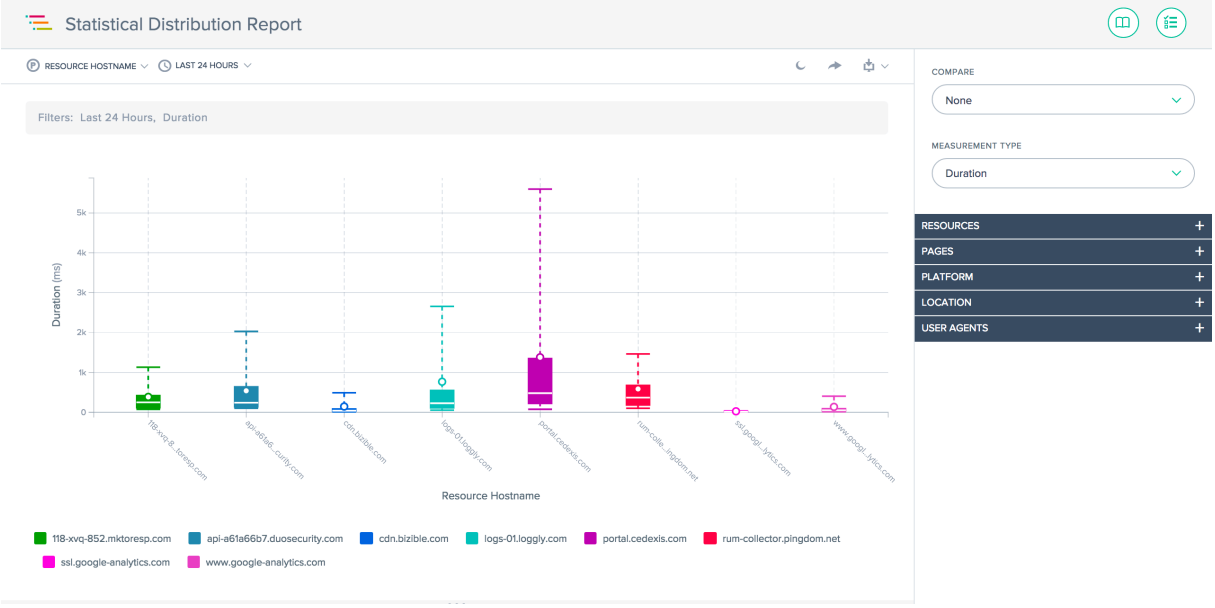
Rapport sur la distribution statistique

Le présent rapport montre la distribution statistique du calendrier des ressources. Le rapport donne un aperçu du nombre de mesures recueillies par valeur de ressource. Vous pouvez filtrer en fonction

de la ressource, de la page, de la plate-forme, de l'emplacement et de l'agent utilisateur, basculer entre les types de mesure et effectuer des comparaisons entre les détails de la page, de l'emplacement et de l'agent utilisateur spécifiques.

Affichage des rapports par défaut :

1. Dimension : Nom d'hôte de la ressource
2. Mesure : Durée
3. Plage de temps : dernières 24 heures

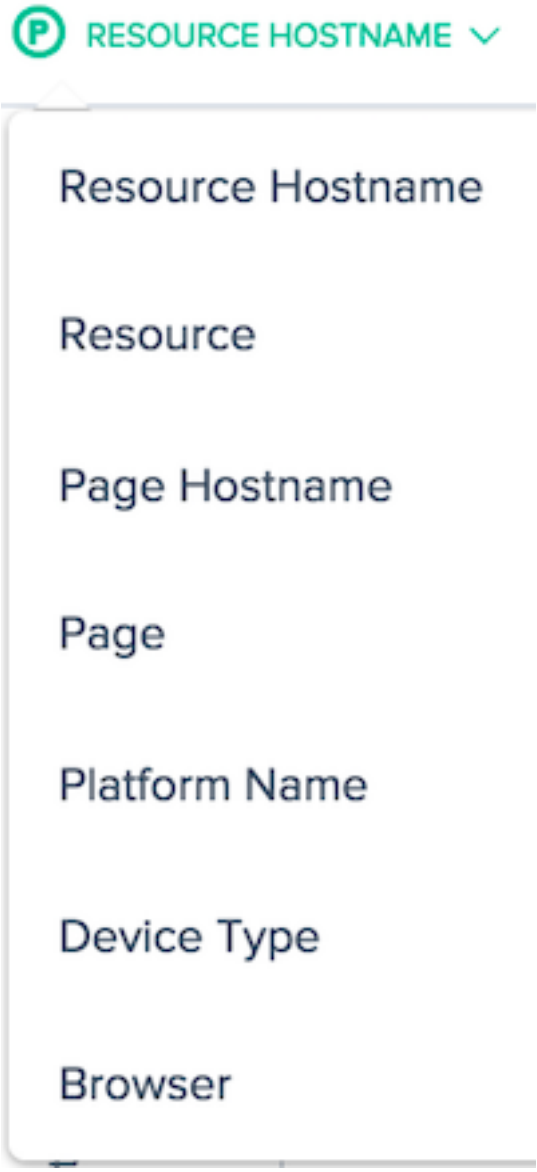


Le graphique en boîte à moustaches

Utilisation des rapports

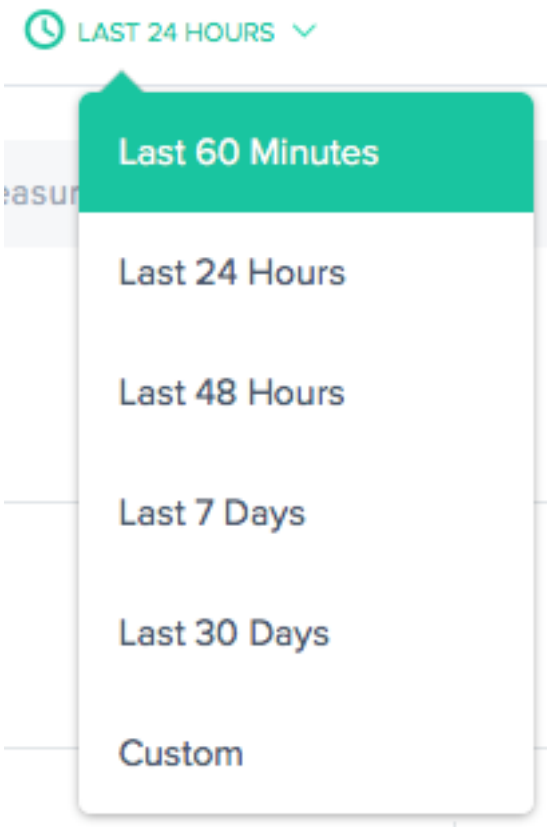
Pour affiner et personnaliser les affichages de rapport en fonction des besoins spécifiques de reporting, utilisez les fonctionnalités suivantes dans les rapports Performances et Distribution statistique. Outre les fonctionnalités standard des rapports, telles que le partage de rapports, le basculement en arrière-plan, l'exportation de données, etc., les fonctionnalités suivantes sont disponibles :

Dimension principale



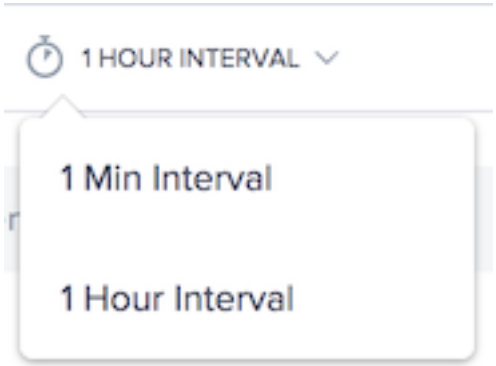
La dimension principale du graphique est sélectionnée dans un menu situé au-dessus du graphique. Vous pouvez l'utiliser comme pivot puissant sur le rapport pour exprimer des données en termes de nom d'hôte de ressource, nom d'hôte de page, page et nom de la plate-forme.

Filtre : Plage de temps du rapport



Les rapports peuvent être générés avec une plage de temps de 60 dernières minutes, 24 dernières heures, 48 dernières heures, 7 derniers jours, 30 derniers jours ou une plage personnalisée. La vue par défaut est la dernière 24 heures.

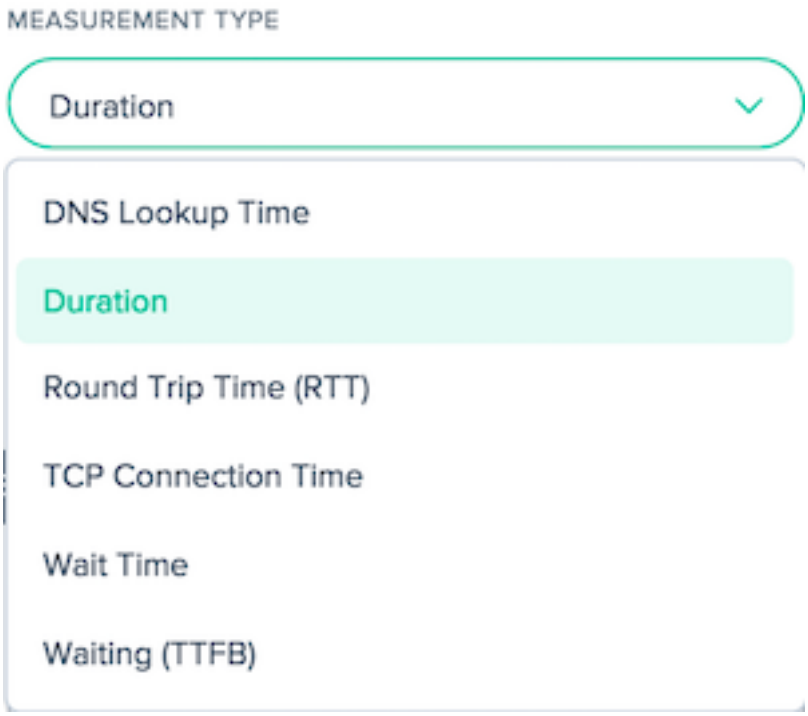
Intervalle de rapport



Sélectionnez l'intervalle de synchronisation dans lequel vous souhaitez afficher le graphique de tendance. Selon la plage de dates que vous consultez, vous pouvez afficher le graphique à intervalles d'

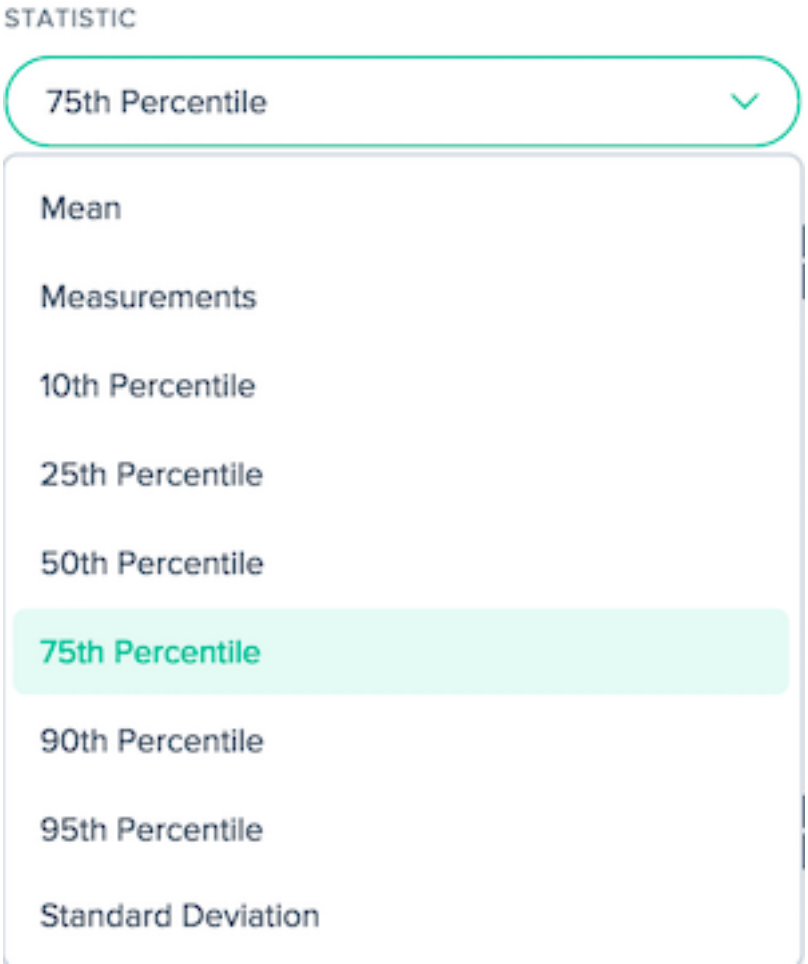
une minute, d'une heure ou d'un jour.

Types de mesure



Sélectionnez le type de mesure auquel vous souhaitez afficher le calendrier de la ressource. Choisissez entre la durée, le temps de recherche DNS, le temps d'aller-retour (RTT), le temps de connexion TCP, le temps d'attente et d'attente (TTFB).

Sélectionnez une mesure statistique pour afficher les données.



Filtres : Puissantes capacités d'exploration vers le bas

Les rapports varient légèrement en ce qui concerne les filtres appropriés en fonction des données. Les options de filtre suivantes sont disponibles dans les rapports :

Nom d'hôte de la ressource :

RESOURCE HOSTNAME

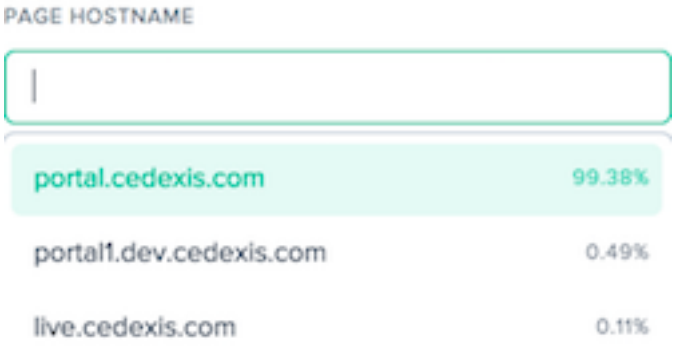
portal.cedexis.com	56.84%
www.google-analytics.com	14.7%
cdn.bizible.com	9.9%
logs-01.loggly.com	9.02%
118-xvq-852.mktoresp.com	7.46%
rum-collector.pingdom.net	2.02%
api-a61a66b7.duosecurity.com	0.05%
ssl.google-analytics.com	0.01%
api-ext.intricately.com	0.01%

Ressources :

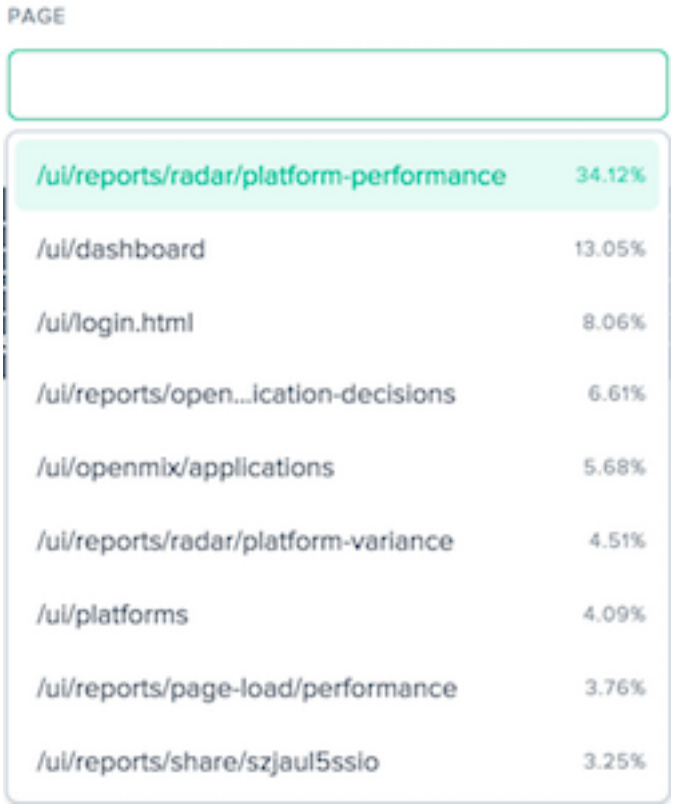
RESOURCE

/collect	11.92%
/m/ipv	9.25%
/inputs/9260e0ca...-24a42dc71056.gif	9.02%
/api/v2/reporting/radar.json	5.73%
/webevents/visitWebPage	5.67%
/api/v2/reporting/openmix.json	4.67%
/r/collect	2.77%
/provider-detection/platform.htm	2.25%
/api/v2/reporting/session.json	2.03%

Nom de l'hôte de la page :

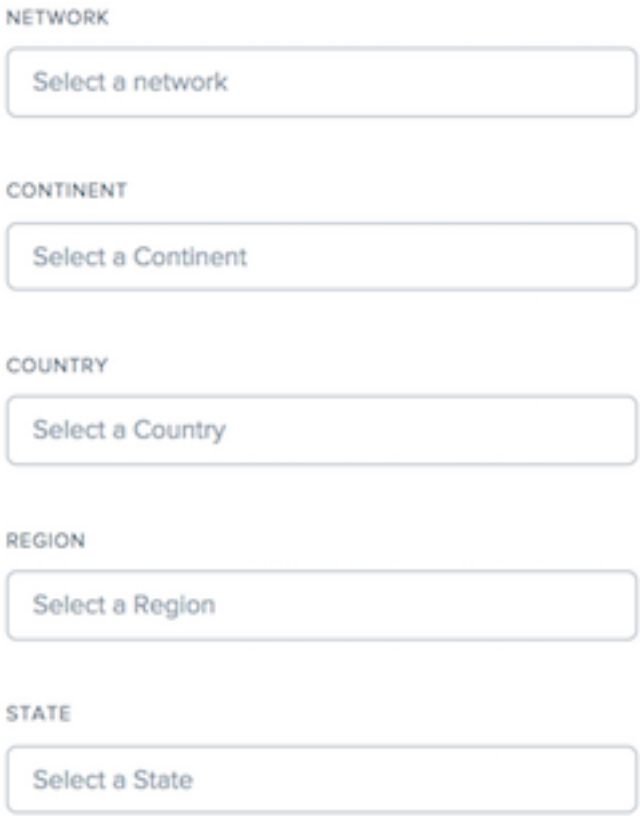


Page :

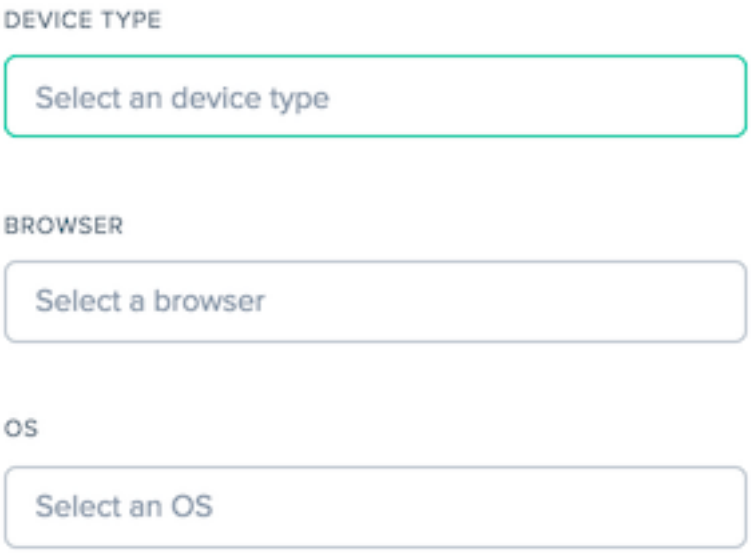


Nom de la plateforme :

Emplacement : Réseau, Continent, Pays, Région et État :



Agents utilisateur : Type de périphérique, navigateur et IOS :

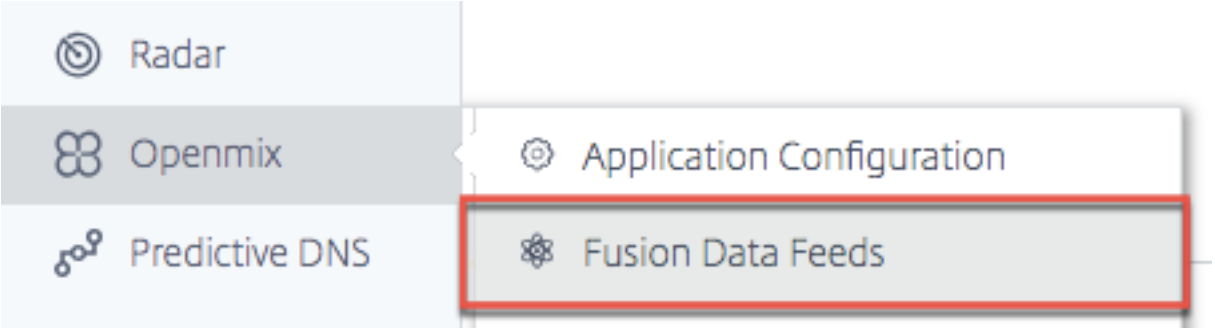


Intégrations Fusion

September 13, 2023

En plus des données Radar et Sonar, Openmix peut utiliser des données tierces dans ses critères de décision. Par exemple, vous pouvez intégrer un service de surveillance synthétique existant que vous utilisez déjà. Vous pouvez également prendre des décisions basées sur les coûts en utilisant les données d'utilisation actualisées de votre fournisseur de CDN.

Menu Fusion



Les flux de données Fusion sont accessibles depuis le menu de navigation, sous **Openmix**.

Par exemple, certains flux de données Fusion courants qui fonctionnent avec les applications Openmix :

1. **Disponibilité du serveur** —Ingère les données de fournisseurs tiers tels que CatchPoint, Rigor et Pingdom pour déterminer l'accessibilité d'un hôte ou d'une application spécifique.
2. **Surveillance des serveurs** —Les indicateurs fournis par des fournisseurs tels que Rackspace et New Relic permettent à Openmix de prendre en compte les indicateurs de temps d'exécution du serveur tels que l'utilisation de la mémoire, la consommation du processeur, l'espace disque disponible et la latence du réseau dans la décision de routage. Openmix peut utiliser les métriques pour prendre des décisions de routage activation/désactivation ou pour apporter des modifications de routage progressives en éliminant le trafic d'un serveur chargé.
3. **Contrôle des coûts du CDN** - Ingère les statistiques de bande passante et d'utilisation de tous les principaux CDN et rend ces données disponibles en temps réel dans les applications Openmix afin d'influencer les décisions de routage.
4. **Flux de données personnalisés définis par le client** - Toutes les données d'un point de terminaison que vous fournissez peuvent être ingérées et mises à disposition dans une application Openmix personnalisée pour être utilisées dans la décision de routage.

Intégrations Fusion

Service	Type
Akamai	Bande passante du CDN, utilisation du CDN
AWS CloudFront	Utilisation du CDN
AWS Cloud Watch	Mesures d'instance
ÉTAIT ELB	Métriques de l'équilibreur de charge
AWS S3	Flux de données personnalisé
Azure	Mesures d'instance
Catchpoint	Alertes
CDNetworks	Bande passante du CDN, utilisation du CDN
ChinaCache	Bande passante CDN
ChinaNetCenter	Bande passante CDN
NetScaler	Flux de données personnalisé
Datadog	Alertes
Edgecast	Bande passante du CDN, utilisation du CDN
Fastly	Utilisation du CDN
Fusion Direct	Flux de données personnalisé
Highwinds	Utilisation du CDN
HTTP GET	Flux de données personnalisé
HTTP GET avec disponibilité	Flux de données personnalisé
JSON	Flux de données personnalisé
Keynote	Moniteur Web
Level3	Bande passante du CDN, utilisation du CDN
Limelight	Utilisation du CDN
MaxCDN	Bande passante du CDN, utilisation du CDN
Apdex New Relic	Score de l'application
Surveillance des serveurs New Relic	Mesures d'instance
NGINX	Métriques de l'équilibreur de charge
NGINX +	Métriques de l'équilibreur de charge

Service	Type
Pingdom	Moniteur Web
Qbrick	Utilisation du CDN
Rackspace	Mesures d'instance
Rigueur	Moniteur Web
SFR	Bande passante du CDN, utilisation du CDN
Ping TCP	Moniteur Web
Touchstream	Surveillance vidéo

Flux de fusion

L'écran suivant affiche tous les flux de données Fusion configurés. La liste fournit un aperçu des flux de données et de l'état actuel.

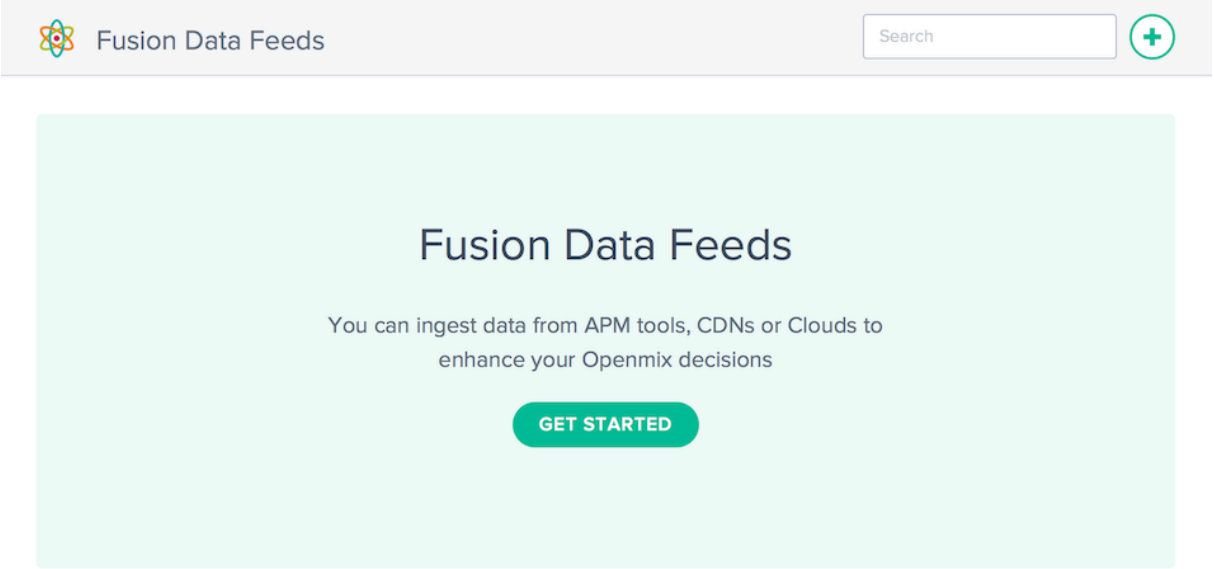
Les colonnes fournissent les informations suivantes :

Rubrique	Description
État	État actuel du flux de données. L'état indique soit : + vert signifie que le flux récupère correctement les données du service ; + jaune signifie que le flux attend que les données soient récupérées par le service ; ou + rouge signifie que le flux ne peut pas être récupéré depuis le service
Nom du flux de données	Le nom indiqué dans le flux de données. Facultatif, sera défini par défaut dans « Nom du service - plate-forme » s'il n'est pas spécifié.
Service	Nom du service utilisé par le flux de données.

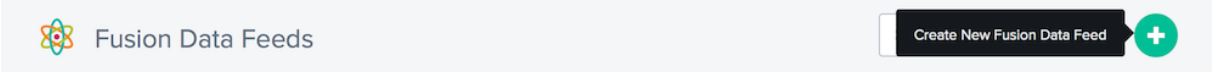
Rubrique	Description
ID	L'ID du flux de données. Cela est nécessaire pour accéder à Fusion via l'API.
Nom de la plateforme	Le nom de la plateforme associée au flux de données.
Exécutez chaque	Fréquence à laquelle le flux de données est mis à jour depuis le service.

Création de flux de données

Si aucun flux de données Fusion n'est configuré, un écran de bienvenue vous invite à créer un flux de données.

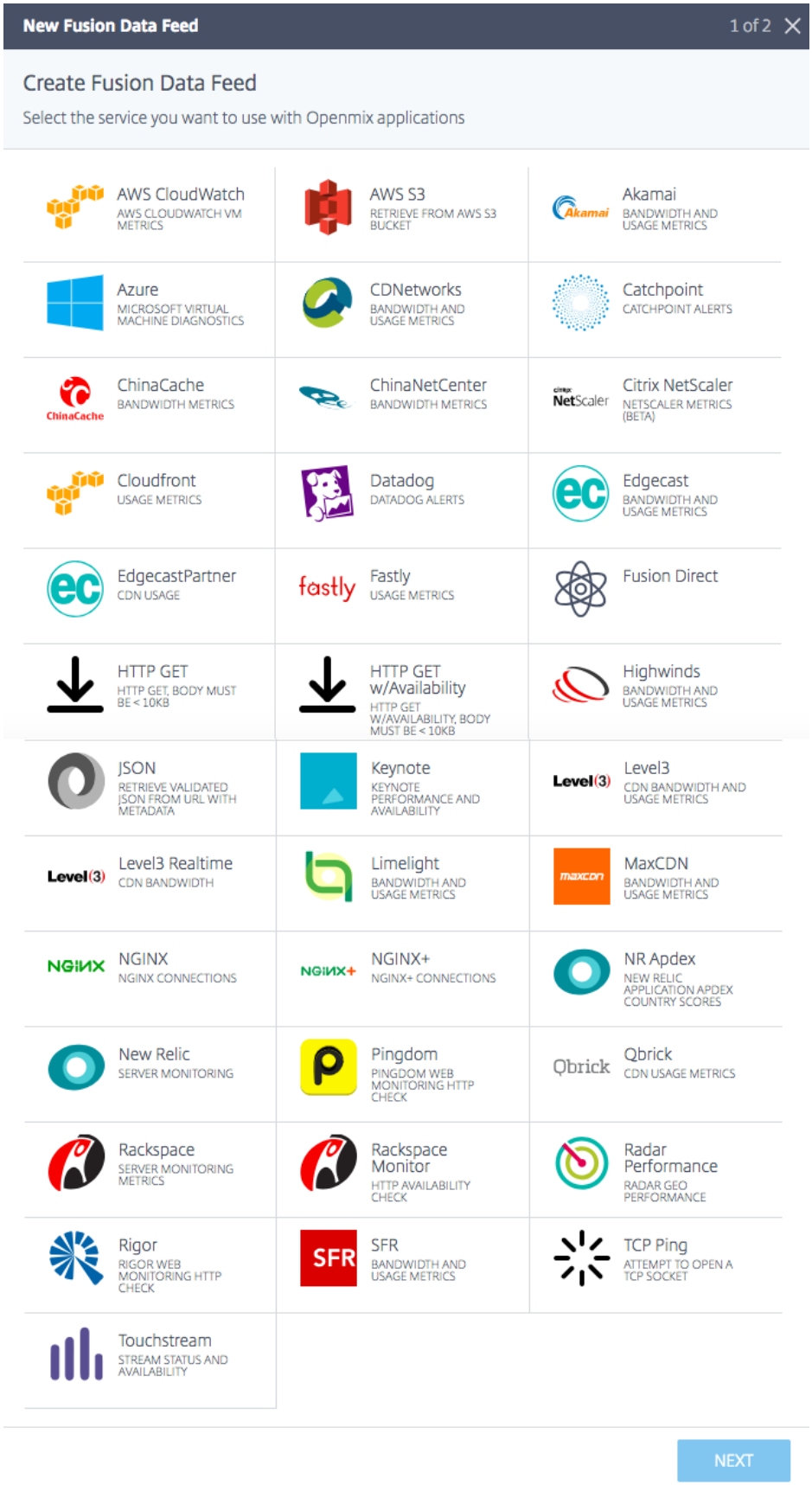


Cliquez sur le bouton **Commencer** ou sur le bouton **+** pour configurer un nouveau flux de données.

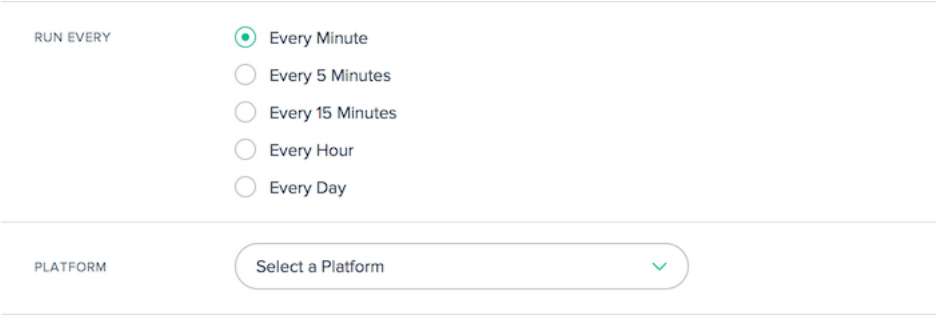


Nouveaux flux de données

Cliquez sur l'icône du service que vous souhaitez intégrer et remplissez les champs de configuration requis.



Chaque service nécessite des paramètres de configuration différents. Vous avez besoin d'un nom d'utilisateur et d'un mot de passe ou d'un jeton généré pour l'authentification et pour toute configuration supplémentaire spécifique au service.



Tous les flux de données Fusion sont associés à une plate-forme précédemment créée dans le portail NetScaler Intelligent Traffic Management. Cela permet à l'application Openmix d'interroger les données Fusion externes pour chaque plate-forme et, en fonction de la logique de routage, de déterminer si la plate-forme doit être considérée comme disponible pour une décision de routage.

La plupart des flux nécessitent de configurer les valeurs suivantes :

Élément d'entrée	Description
Exécutez chaque	Fréquence à laquelle le flux de données est mis à jour par le service externe. Fusion appelle le service à l'intervalle spécifié et met à jour les applications Openmix en fonction des nouvelles données.
Plateforme	Plateforme associée aux données Fusion dans l'application Openmix.

Modification des flux de données

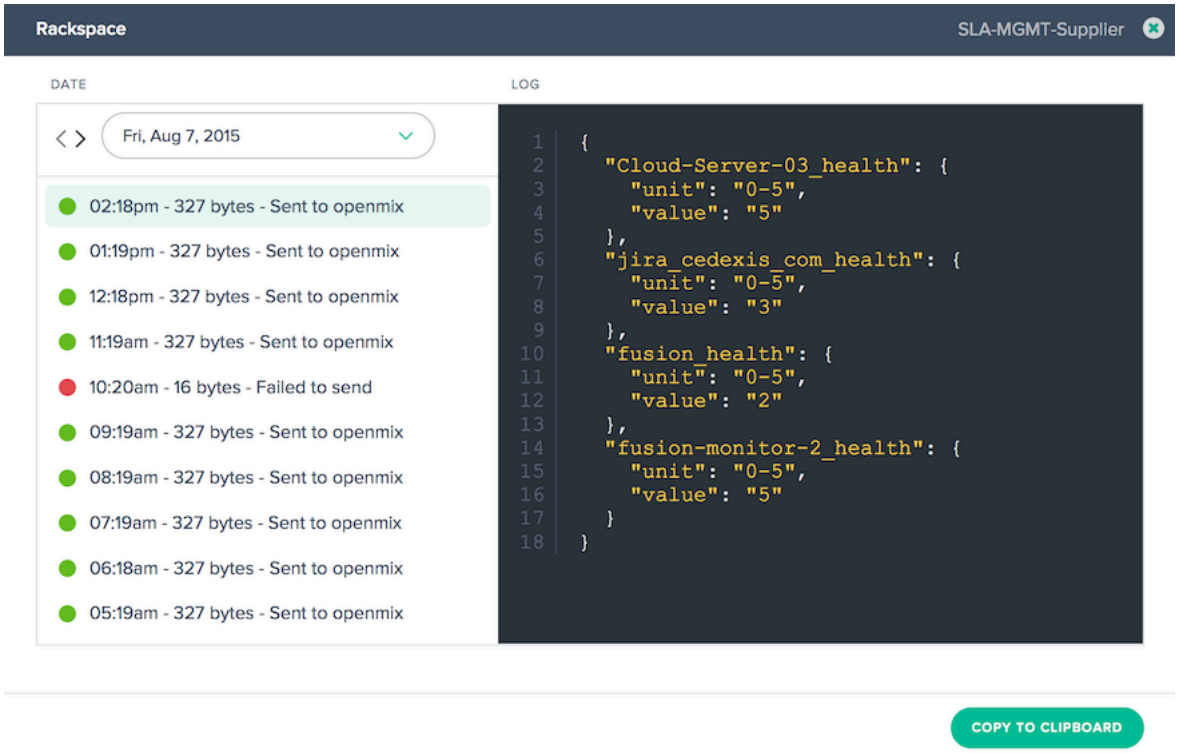
Pour modifier un flux de données Fusion, il suffit de cliquer sur le flux de données dans le tableau et de cliquer sur le bouton **Modifier** .

Une fois que vous avez modifié la configuration, cliquez sur **Enregistrer**. Cela vous ramène dans la liste des flux de données avec vos modifications enregistrées et appliquées dans le flux de données.

Historique des flux de données

Fusion collecte les 100 dernières réponses de chaque exécution dans l'historique des flux de données. Vous pouvez consulter l'état de la source de données, des informations sur les données et la charge

utile renvoyée par le service. Après avoir sélectionné le flux de données spécifique dans la liste, cliquez sur le bouton **Historique du journal** pour afficher l'historique du flux de données.



Pour modifier la date sélectionnée, vous pouvez cliquer sur les boutons **<** ou ** pour reculer ou avancer par rapport à la date actuellement sélectionnée ou choisir une date spécifique dans la liste. Sélectionnez l'horodatage de l'instance spécifique et les données renvoyées par le service seront affichées.

Flux de données défaillants

Fusion Quarantine pour les flux de
fusion défaillants La quarantaine de fusion s'applique au flux de données Fusion défaillant d'un client, si le flux est configuré pour être exécuté à un intervalle d'interrogation inférieur à 24 heures. Fusion applique une logique de quarantaine pour empêcher l'exécution de ces flux défaillants. Cela permet d'économiser des ressources (CPU/mémoire) et d'éviter tout impact négatif sur les autres flux de données Fusion valides.

La logique de quarantaine est appliquée en « arrêtant » le flux Fusion défaillant à intervalles réguliers. Cela se produit jusqu'à ce que le flux Fusion soit mis en quarantaine pendant 24 heures. À ce stade, le flux Fusion essaiera de s'exécuter toutes les 24 heures. Le flux de données de fusion défaillant n'est jamais complètement arrêté. Il continuera à fonctionner, au moins deux fois toutes les 24 heures.

Important :

- Le flux de données Fusion s'exécute toujours au moins deux fois de suite et échoue deux fois avant d'entrer dans la logique de quarantaine. Par exemple, si un flux d'une minute s'exécute et échoue deux fois de suite, il entrera dans la logique de quarantaine.
- Si, à un moment ou à un autre, le flux de données Fusion s'exécute correctement, il est supprimé de la logique de quarantaine et sera réexécuté à intervalles réguliers.
- Si le flux Fusion est mis à jour à tout moment (c'est-à-dire si l'utilisateur a saisi une URL incorrecte et l'a corrigée), le flux Fusion essaiera de s'exécuter à nouveau dans la minute, quel que soit l'intervalle d'interrogation. En cas de succès, il sera supprimé de la logique de quarantaine. Si elle continue en échec, la logique de quarantaine sera appliquée.

Purge du CDN global

June 4, 2021

La purge de CDN globale est un moyen de purger des données de plusieurs CDN en même temps, ce qui facilite la gestion de plusieurs CDN. Il vous permet de connecter les CDN à purger, de spécifier les URI à purger sur tous les services attachés et de cliquer sur le bouton **Purger** . La purge est lancée sur tous les CDN connectés.

La fonctionnalité de purge CDN globale repose sur trois composants principaux :

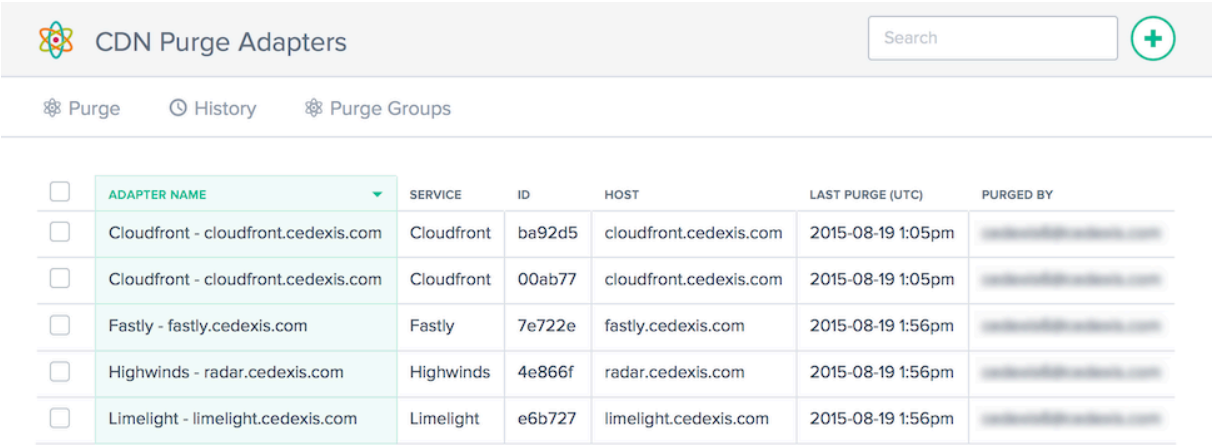
1. **Adaptateur de purge** CDN : un adaptateur de purge CDN doit être créé pour chaque combinaison CDN/nom d'hôte que vous souhaitez purger. L'adaptateur de purge CDN collecte les informations nécessaires à l'exécution des purges, telles que la sélection du service, les informations d'authentification, le nom d'hôte et d'autres informations spécifiques au service. Vous avez besoin d'un adaptateur de purge CDN pour chaque nom d'hôte qui doit être purgé sur un CDN.
2. **URI** —Les purges sont exécutées sur un emplacement spécifique sur les CDN.
3. **Groupe de purge** : les groupes de purge vous permettent de créer une collection logique d'adaptateurs de purge CDN et d'URI qui sont purgés à l'aide d'une seule commande. Par exemple, vous pouvez purger le répertoire '/media'sur 2 CDN différents ou sur un répertoire existant dans l'environnement de développement, de test et de production.

Les adaptateurs de purge CDN doivent être configurés pour exécuter des purges.URIS et plusieurs purges CDN peuvent être spécifiées individuellement, mais il est recommandé que vos groupes de purge d'installation pour gérer les purges courantes qui sont souvent exécutées.

La purge CDN globale est accessible à partir du niveau supérieur du menu de navigation en tant que purge CDN.

Adaptateurs de purge CDN

L'écran suivant affiche toutes les cartes de purge CDN configurées. La liste fournit une vue d'ensemble des adaptateurs CDN configurés et permet l'exécution de purge.

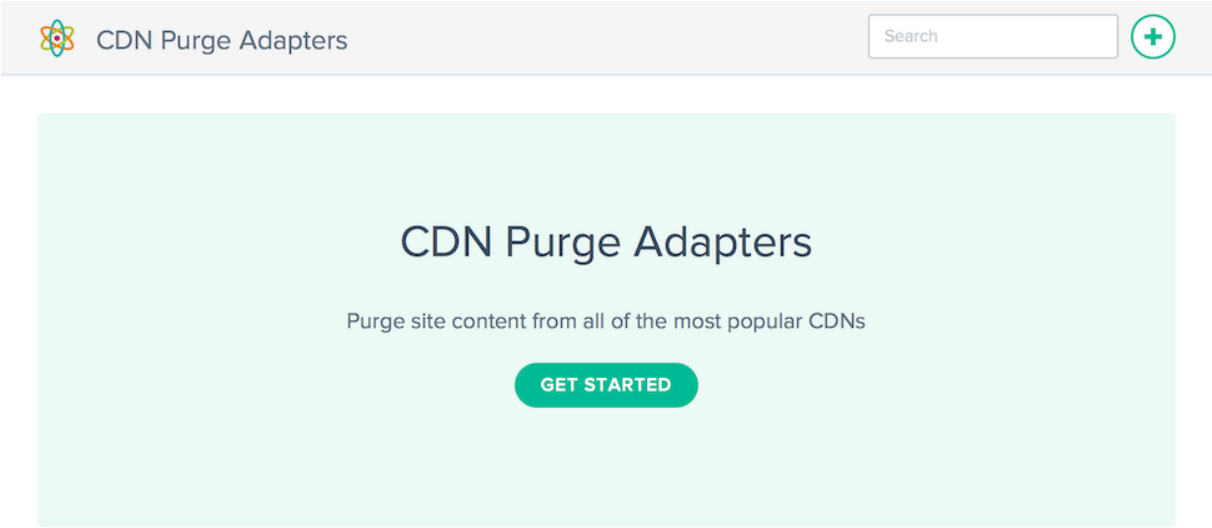


Les colonnes fournissent les informations suivantes :

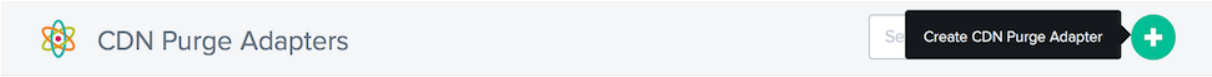
En-tête	Description
Nom de l'adaptateur	Nom donné à l'adaptateur. Facultatif, la valeur par défaut « Service - Hôte » s'il n'est pas spécifié.
Service	Nom du service CDN que la purge est configurée pour utiliser.
ID	ID de la carte CDN. Ceci est nécessaire pour accéder à Fusion via l'API.
Hôte	Hôte sur lequel la purge est configurée pour s'exécuter. Les services appellent parfois ce paramètre : hôte, nom d'hôte, plateforme, etc.
Dernière purge (UTC)	Heure et date, en UTC, de la dernière exécution de la purge.
Purgé par	Utilisateur qui a exécuté une purge pour la dernière fois.

Création d'adaptateurs de purge CDN

Pour utiliser la purge de CDN globale, vous devez ajouter vos configurations de CDN et de nom d'hôte. Lorsque vous ouvrez la **purge CDN**pour la première fois, vous êtes invité à créer un adaptateur de purge CDN.

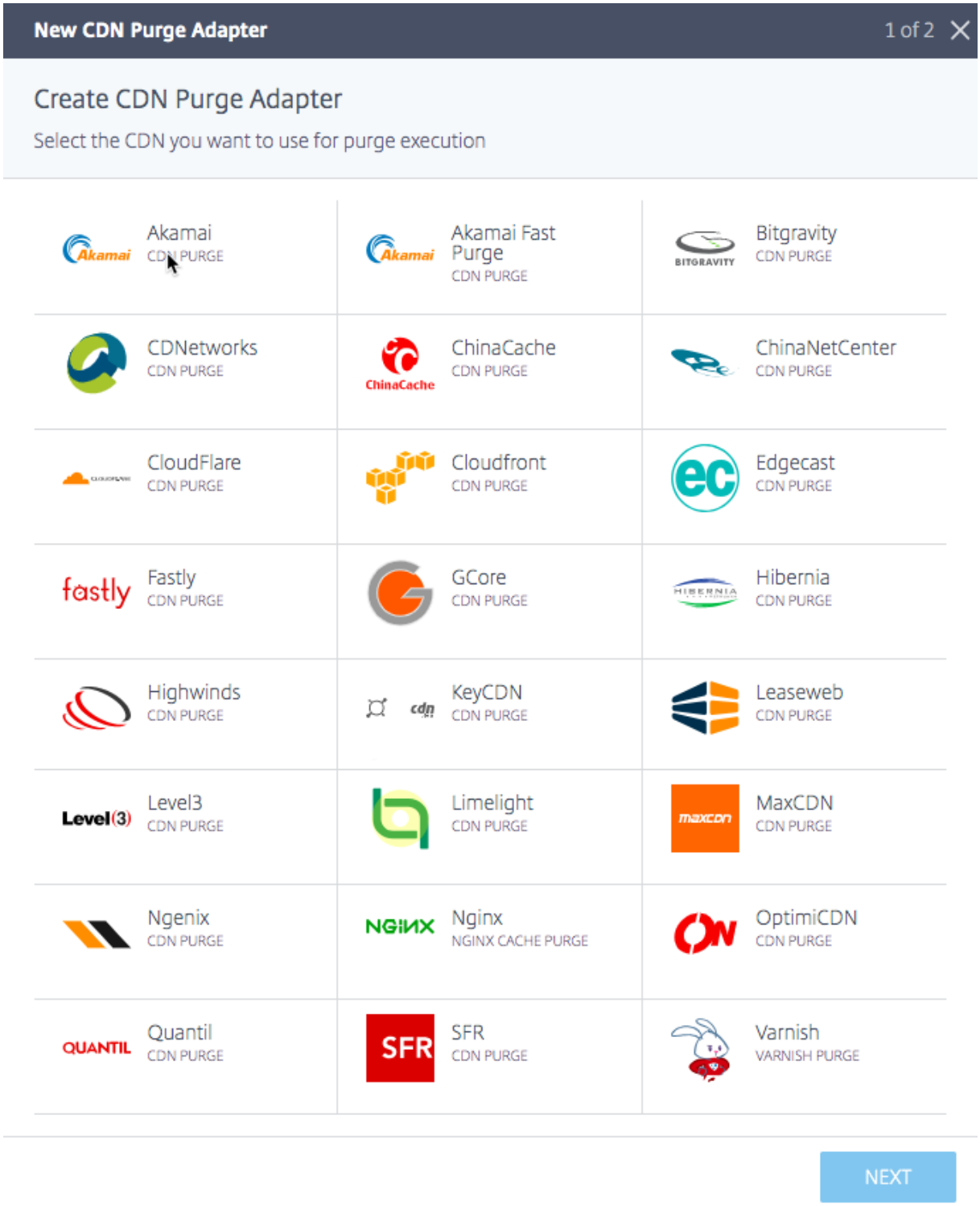


Cliquez sur le bouton **Démarrer** ou **+** pour configurer un CDN disponible à purger.

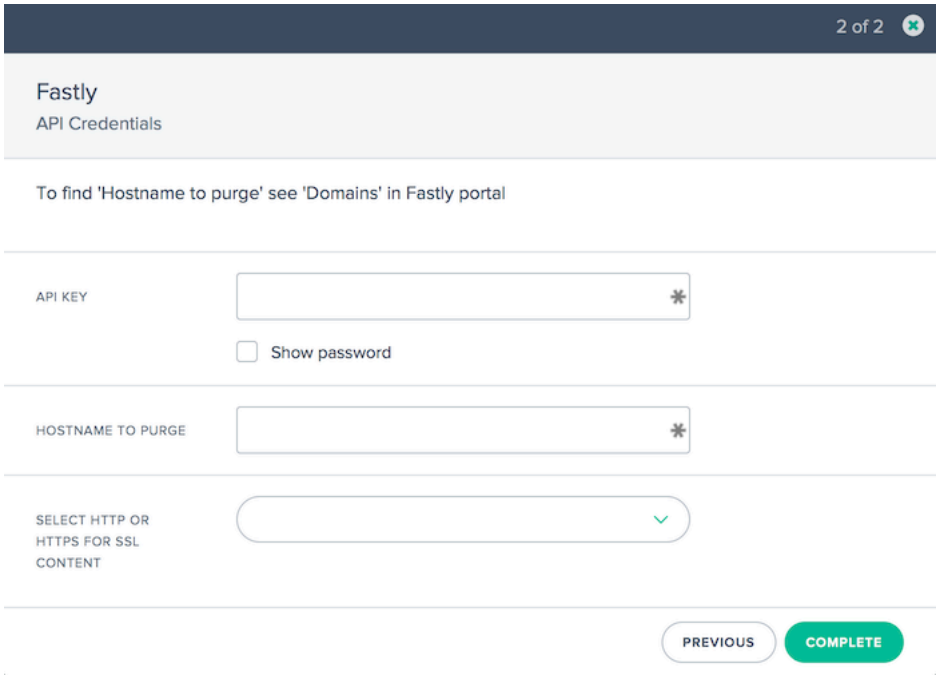


Nouveaux adaptateurs de purge CDN

Cliquez sur l'icône du service pour lequel vous souhaitez créer un adaptateur de purge CDN et remplissez les champs de configuration requis.



Chaque adaptateur de purge nécessite des paramètres de configuration différents. Vous auriez besoin d'un nom d'utilisateur et d'un mot de passe ou d'un jeton généré pour l'authentification et toute configuration spécifique au service supplémentaire.



Modification des adaptateurs de purge CDN

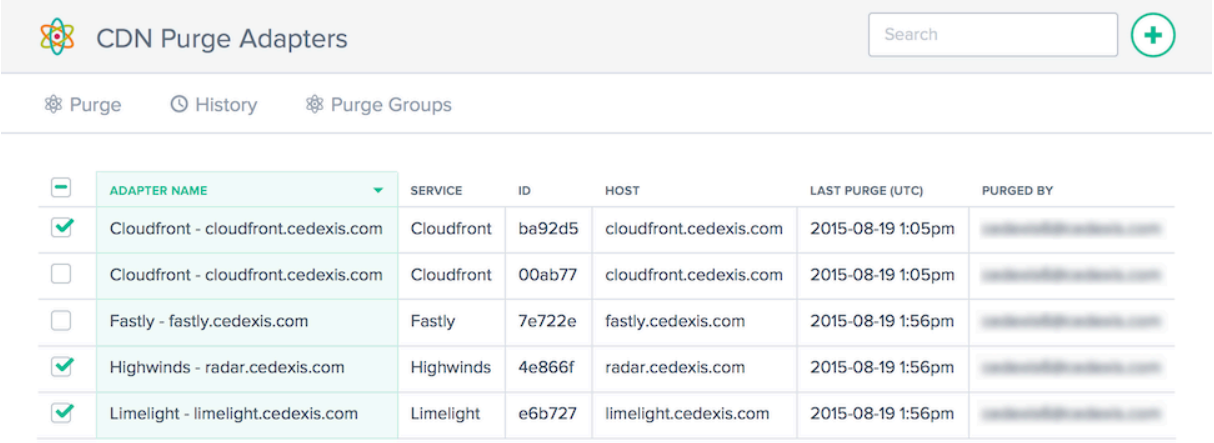
La modification d'un adaptateur de purge CDN est aussi simple que de cliquer sur l'adaptateur de purge CDN dans le tableau et de cliquer sur le bouton **Modifier** .

Une fois la configuration modifiée, cliquez sur **Enregistrer**. Cela vous ramène à la liste des adaptateurs de purge avec vos modifications enregistrées et appliquées à l'adaptateur de purge CDN spécifique.

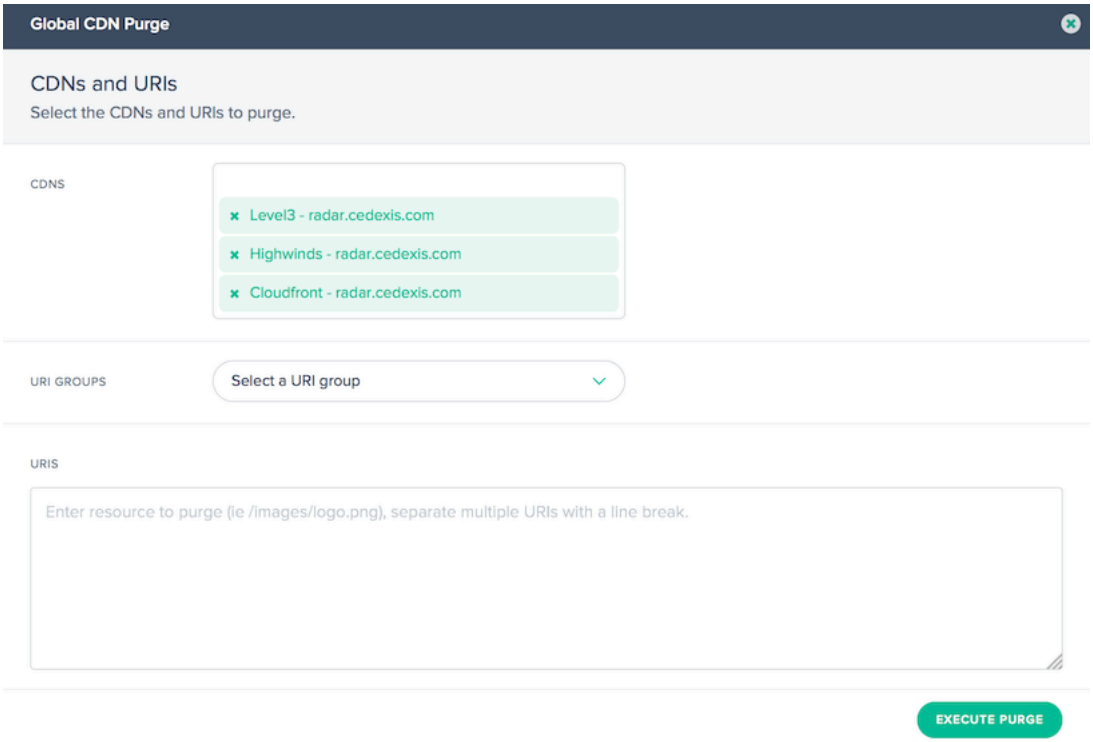
Exécution d'une purge

Pour exécuter une purge, sélectionnez les adaptateurs de purge CDN qui doivent être inclus dans l'exécution de purge.

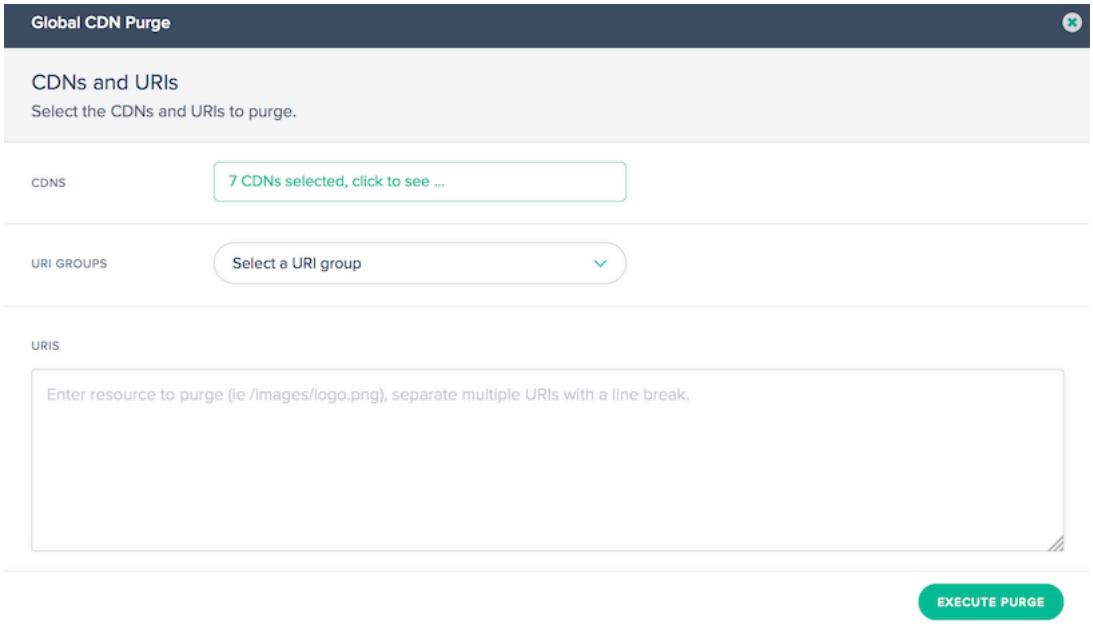
Cliquez sur le bouton **Purger** pour lancer le processus de purge.



La boîte de dialogue **Purge CDN globale** s'ouvre. La boîte de dialogue affiche les adaptateurs de purge CDN sélectionnés et les URI utilisés dans l'exécution de purge.

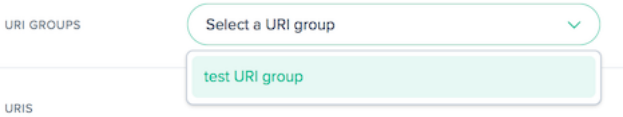


Si 5 adaptateurs de purge CDN ou moins sont sélectionnés, la boîte de dialogue de purge affiche la liste complète des adaptateurs de purge CDN sélectionnés. Si tous les adaptateurs de purge CDN ne sont pas affichés, cliquez sur la zone de texte **CDN** indiquant **X CDN sélectionné, cliquez pour voir…** pour afficher toutes les adaptateurs de purge sélectionnés.

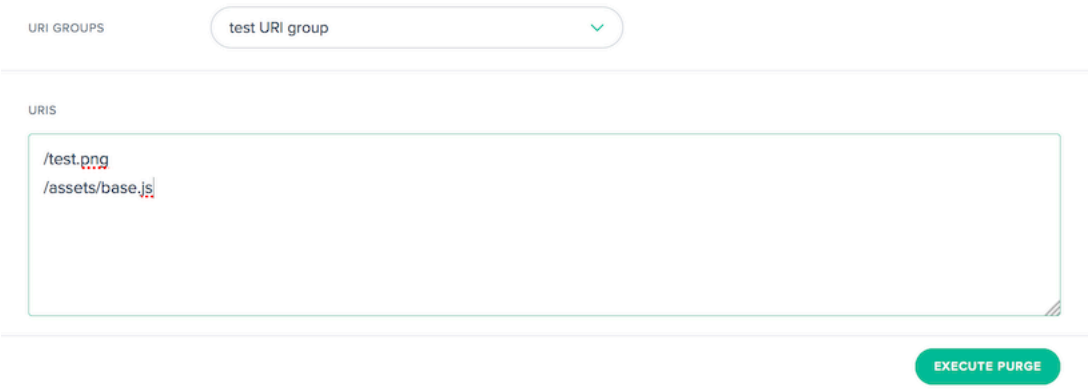


Vous pouvez masquer la liste en cliquant sur le bouton **Masquer** situé à droite de la liste des adaptateurs de purge.

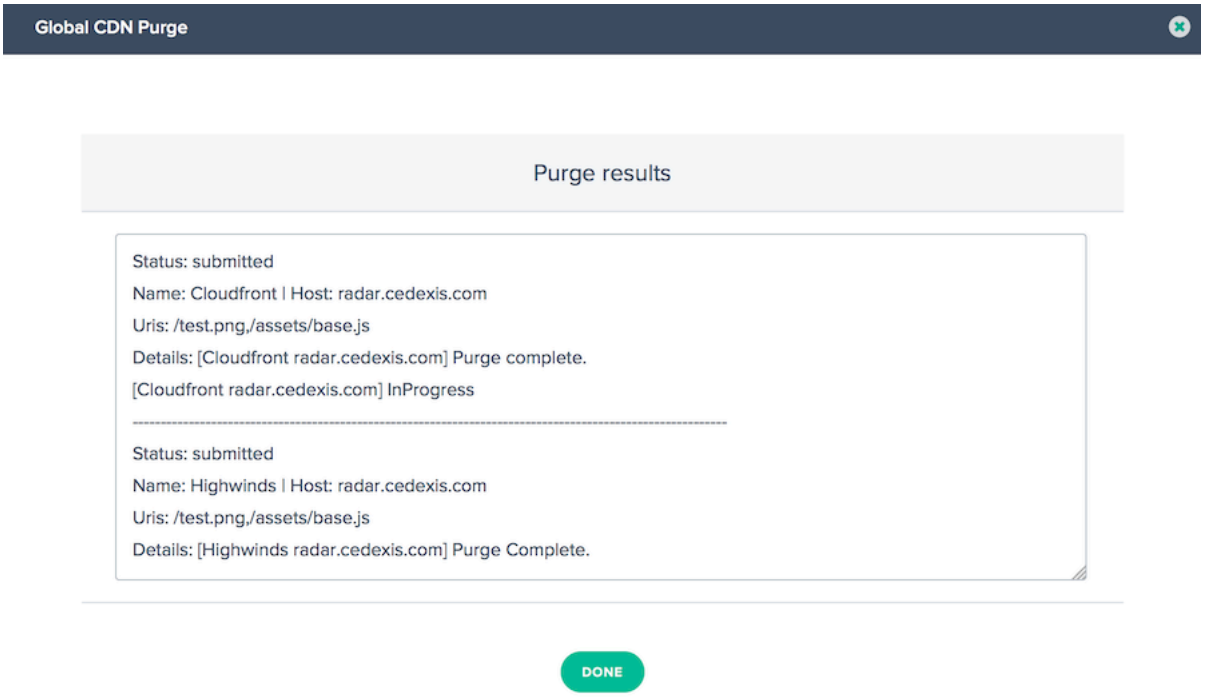
Vous pouvez remplir les URI utilisées dans la purge en saisissant manuellement les URI ou en sélectionnant parmi les groupes d'URI disponibles. La sélection d'un groupe URI remplit les URI entrés avec les URI du groupe de purge sélectionné.



Entrez ou modifiez les URI des ressources qui doivent être purgées.

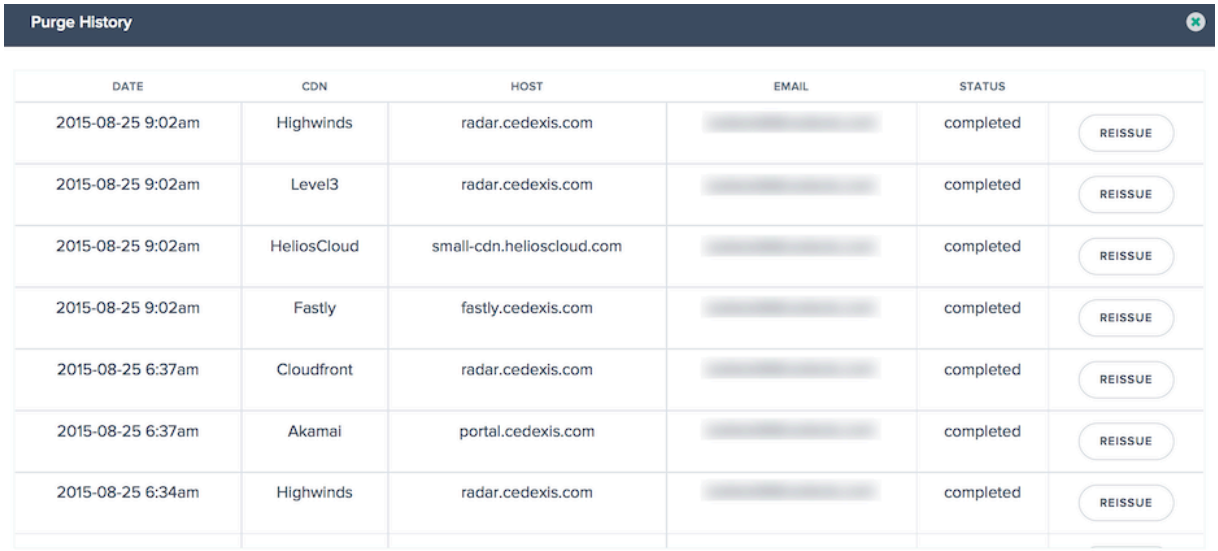


Lorsque vous êtes prêt à soumettre la demande de purge, cliquez sur le bouton **Exécuter la purge** . La purge est soumise à tous les CDN sélectionnés. Les soumissions et les réponses API sont affichées dans la boîte de dialogue **Résultats de la purge** .

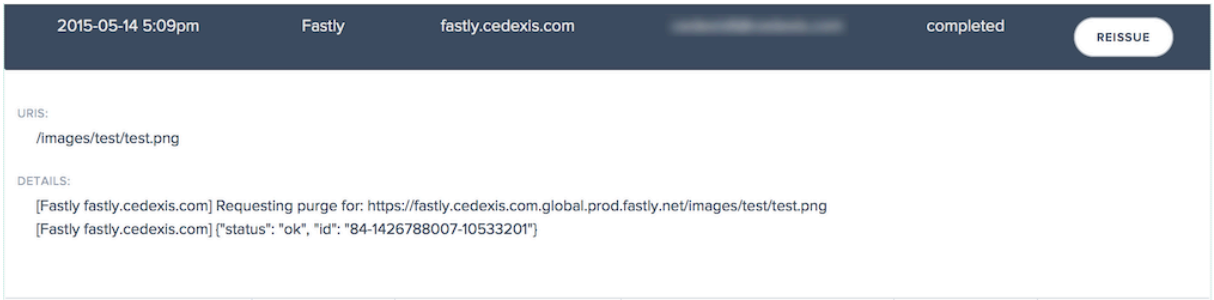


Historique de l'adaptateur de purge CDN

Fusion recueille l'historique de purge chaque fois qu'il s'exécute. Vous pouvez afficher l'état de purge, les informations sur la purge et les messages renvoyés par le service. Pour afficher l'historique de purge, cliquez sur le bouton **Historique** des écrans **Adaptateurs de purge CDN ou Purger les groupes**.



La liste inclut l'heure et l'état des 100 dernières exécutions de purge. Vous pouvez voir les détails d'une demande de purge envoyée au service CDN en cliquant sur la ligne souhaitée dans le tableau. Les informations détaillées incluent les URI spécifiés pour la purge et les réponses API renvoyées par le service pendant la purge.



Si vous souhaitez réexécuter une purge spécifique contenant l'historique, cliquez sur le bouton **Réémettre** à droite des informations d'état de purge. La boîte de dialogue de purge s'affiche avec les données de la purge précédente préchargées pour l'exécution.

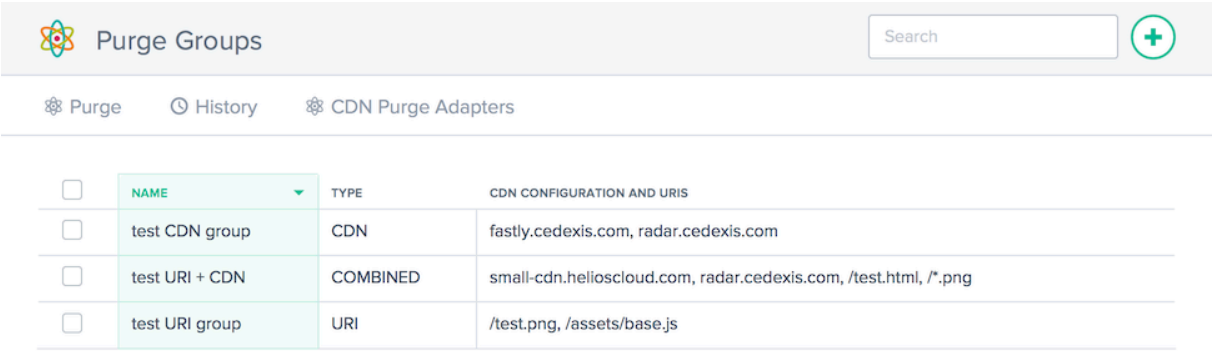
Purger les groupes

Les groupes de purge vous permettent d'organiser les adaptateurs de purge CDN et les URI pour faciliter la purge d'un ensemble logique de ressources. Par exemple, vous pouvez regrouper les environnements de développement, de test et de production et les purger tous en même temps. Vous pouvez également purger toutes les ressources d'image sur plusieurs CDN à la fois.

Les groupes de purge peuvent être constitués d'une collection d'adaptateurs de purge CDN, d'URI de purge ou des deux. Généralement, un groupe contenant uniquement des adaptateurs de purge CDN est utilisé pour purger différentes ressources sur plusieurs services. Un groupe combiné est souvent

utilisé pour préspécifier une purge standard et réutilisable telle que « tous les médias sur tous mes sites Web régionaux et CDN ».

Lorsque vous avez au moins une configuration de groupe de purge, cet écran s'affiche lors de l'ouverture de la purge CDN.



Les colonnes fournissent les informations suivantes :

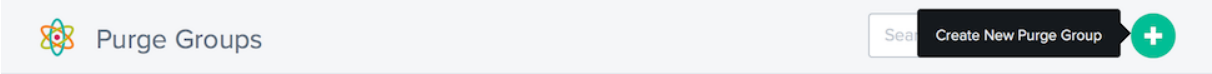
En-tête	Description
Nom	Nom du groupe de purge.
Type	Type de contenu du groupe. + CDN —le groupe de purge contient uniquement des adaptateurs de purge CDN et l'utilisateur doit spécifier des URI lors de l'exécution de l'URI de purge + - le groupe de purge contient uniquement des URI et l'utilisateur devra spécifier des services lors de l'exécution de la purge + Combiné - le groupe de purge contient à la fois CDN purger les adaptateurs et les URI ; l'utilisateur pourra exécuter la purge sans avoir besoin de spécifier plus d'informations
Configuration du CDN et URI	Les adaptateurs de purge CDN et/ou URI inclus dans la définition du groupe.

Création de groupes de purge

Pour utiliser des groupes de purge, vous devez spécifier les adaptateurs de purge CDN ou URI qui doivent être inclus. Il existe deux façons de créer des groupes :

Dans la page Purge des adaptateurs CDN, vous pouvez vérifier les adaptateurs de purge souhaités, puis cliquez sur **Créer un groupe de purge**.

Dans la page Purger les groupes, cliquez sur **+** pour créer un groupe.

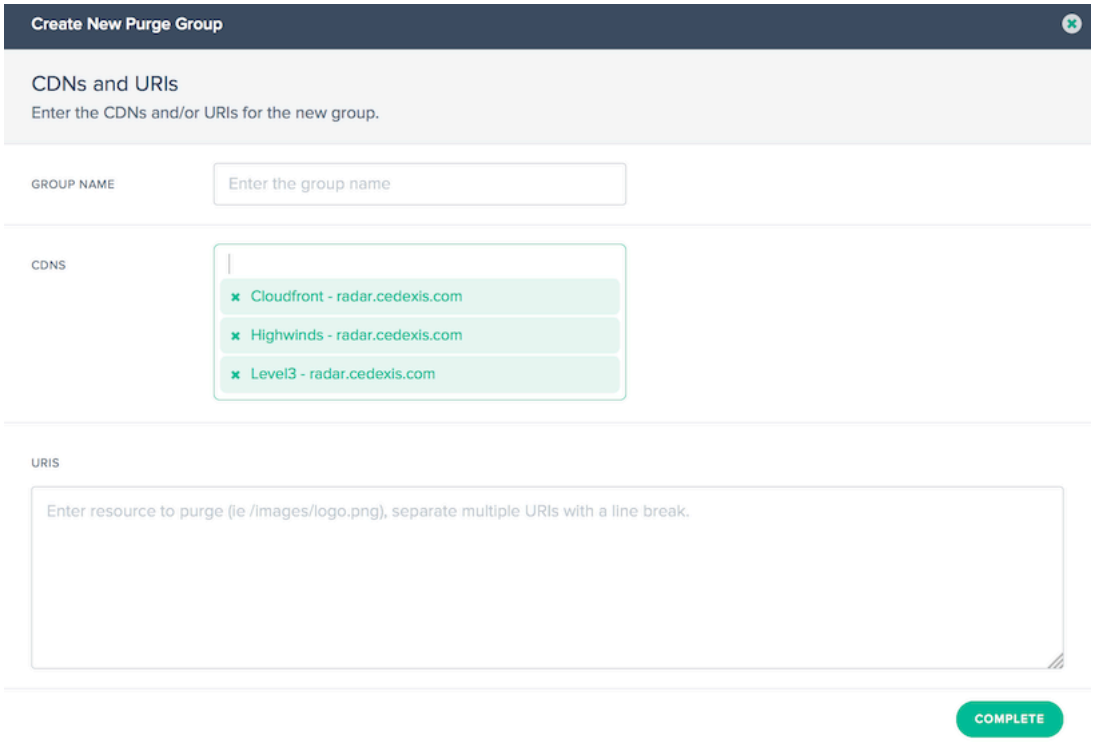


Dans les deux cas, la boîte de dialogue **Créer un groupe** s'affiche.

Entrez le nom du groupe de purge.

> **REMARQUE :** Vous pouvez ajouter ou supprimer des adaptateurs de purge CDN de la liste.

Cliquez sur **Terminer** pour créer le groupe.



Exécution d'une purge de groupe

Dans la page Purger un groupe, sélectionnez un ou plusieurs groupes, puis cliquez sur le bouton **Purger**. La boîte de dialogue **Purge CDN** s'ouvre avec les paramètres spécifiés par la définition du groupe de purge.

Cliquez sur le bouton **Exécuter la purge**pour démarrer la purge configurée.

Alertes

September 13, 2023

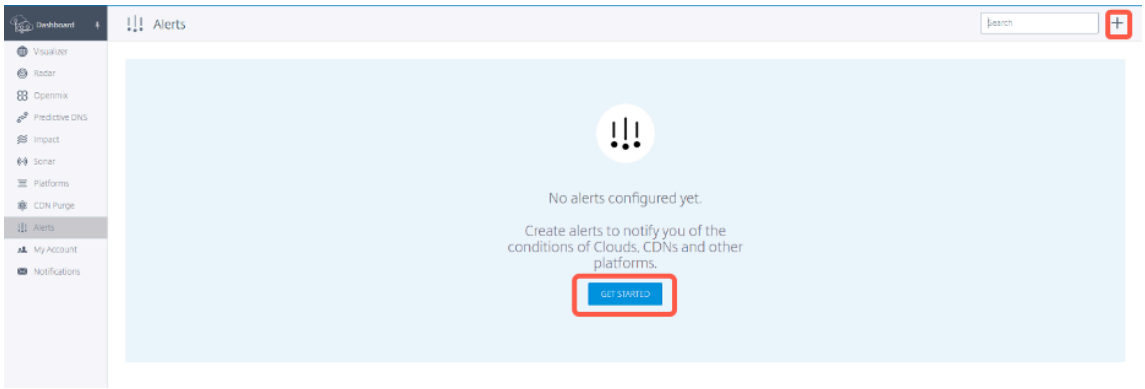
La fonction **Alertes** surveille les problèmes de performances ou les anomalies de vos plateformes configurées à partir d'un réseau d'utilisateurs finaux dans le monde entier.

Création d'alertes

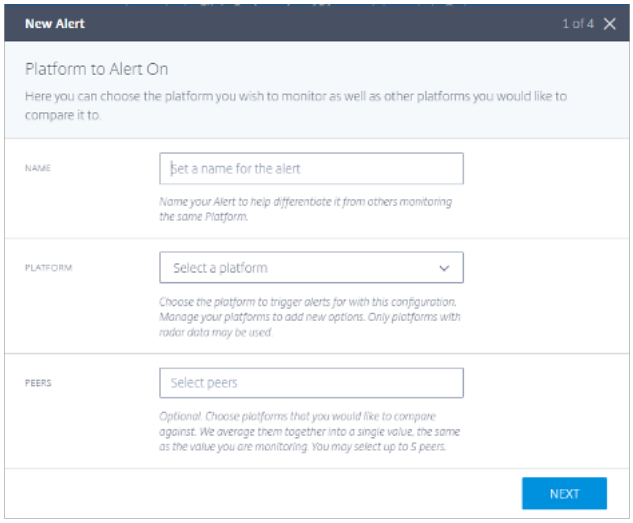
Pour créer des alertes qui surveillent les performances de vos plateformes, vous devez d'abord les configurer. Dans la barre latérale gauche, cliquez sur **Plateformes** pour accéder à l'écran de la plateforme et configurer vos plateformes.

Pour ajouter une nouvelle alerte :

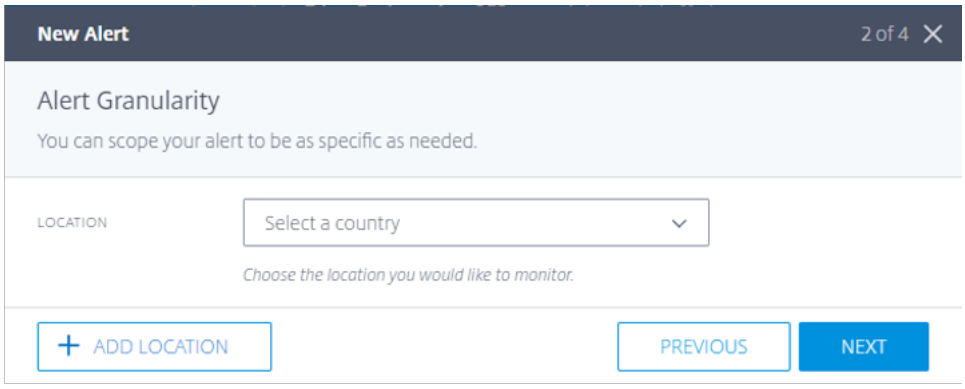
1. Dans la barre latérale gauche, cliquez sur **Alertes** pour accéder à la page des alertes et créer des alertes.
2. Sur la page des alertes, cliquez sur **DÉMARRER** ou sur le symbole **+** dans le coin supérieur droit.



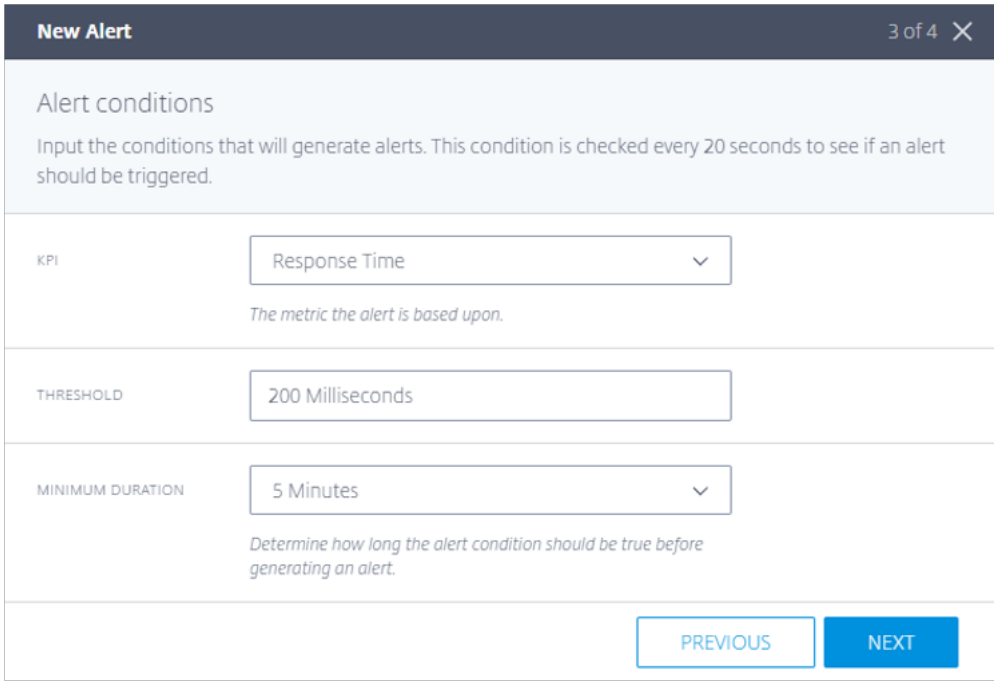
3. Dans la fenêtre **Nouvelle alerte** :
   - entrez le nom de l'alerte
   - sélectionnez la plateforme relative à surveiller
   - sélectionnez des plateformes homologues avec lesquelles comparer (vous pouvez sélectionner jusqu'à 5 pairs). Ce paramètre est facultatif.
   - cliquez sur **Suivant**.



4. Sélectionnez l'**emplacement** et le **réseau** pour lesquels vous souhaitez surveiller les alertes, puis cliquez sur **Suivant**.



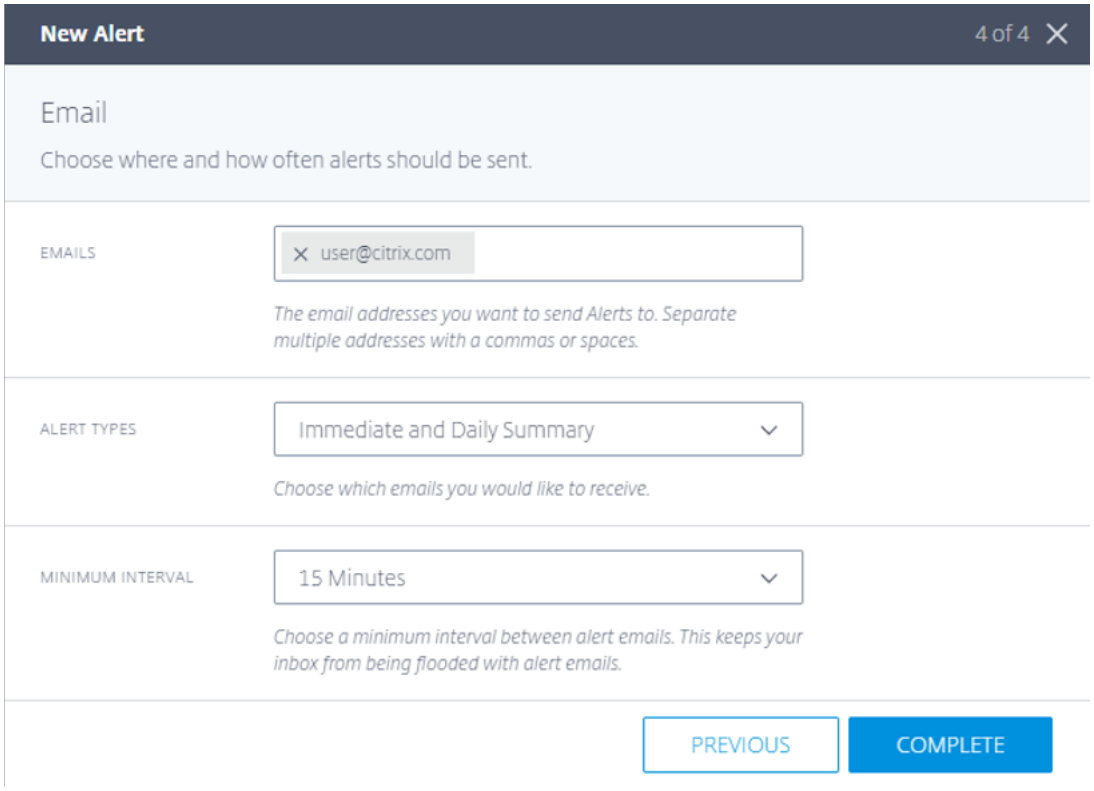
5. Sélectionnez l'**indicateur de performance clé**, le **seuil**et la **durée minimale** de l'événement qui déclenche l'alerte.



NetScaler Intelligent Traffic Management fournit les KPI suivants :

- **Temps de réponse :** La valeur du seuil indique la valeur maximale (en millisecondes) acceptée avant le déclenchement de l'alerte. Pour qu'une alerte soit déclenchée, la mesure doit être supérieure au seuil pendant au moins une **durée ≥ minimum_duration** sélectionnée par un utilisateur. La même alerte se déclenche après avoir reçu de nouveau une mesure en dessous du seuil pendant au moins une durée ≥ minimum.
- **Disponibilité :** La valeur du seuil indique la valeur minimale acceptée avant le déclenchement de l'alerte. Pour qu'une alerte soit déclenchée, la mesure doit être inférieure au seuil pendant au moins une **durée ≥ minimum_duration** sélectionnée par un utilisateur. La même alerte se déclenche après avoir reçu de nouveau une mesure au-dessus du seuil pendant au moins une durée supérieure ou égale à ≥ une durée minimale.
- **Débit :** La valeur du seuil indique la valeur minimale (en Kbits/s) acceptée avant le déclenchement de l'alerte. Pour qu'une alerte soit déclenchée, la mesure doit être inférieure au seuil pendant au moins une **durée ≥ minimum_duration** sélectionnée par un utilisateur. La même alerte se déclenche après avoir reçu de nouveau une mesure au-dessus du seuil pendant au moins une durée supérieure ou égale à ≥ une durée minimale.

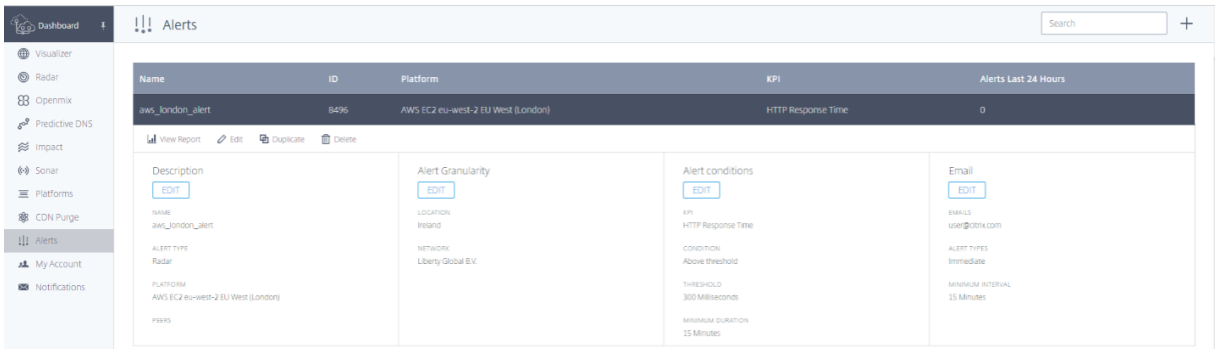
6. Entrez les adresses e-mail auxquelles vous souhaitez envoyer des alertes, sélectionnez le type d'alerte et sélectionnez l'intervalle minimum entre les e-mails d'alerte.



Les types d'alerte sont les suivants :

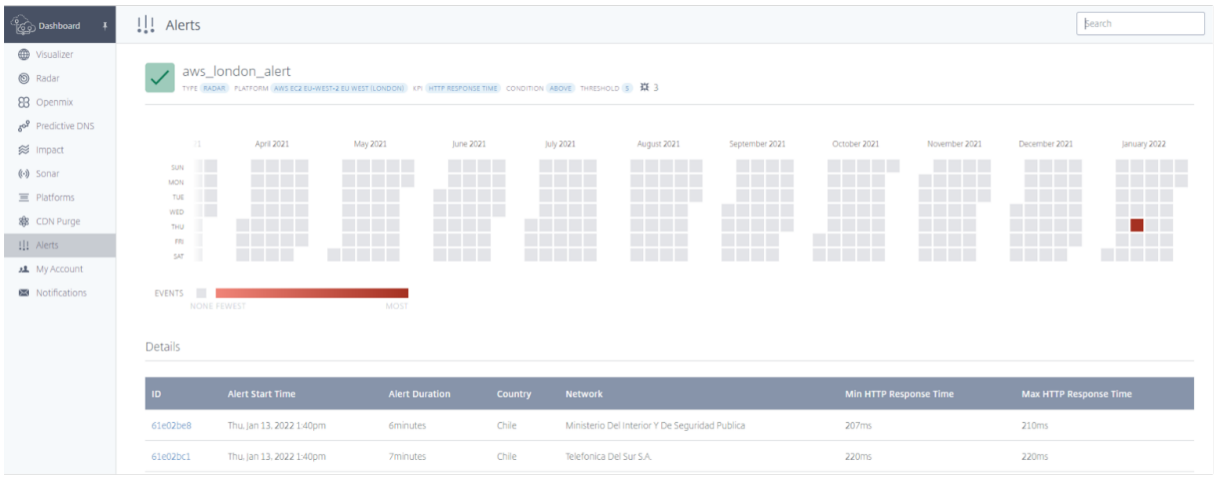
- **Immédiat :** Cette option envoie un e-mail immédiatement lorsqu'une alerte est déclenchée.
- **Résumé quotidien :** Cette option envoie un seul e-mail tous les minuit en temps universel coordonné (UTC), y compris tous les événements qui sont déclenchés.
- **Résumé immédiat et quotidien :** Cette option est une combinaison d'envoi de courrier électronique immédiat et quotidien.

7. Après avoir configuré une alerte, vous pouvez voir les alertes dans l'onglet **Alertes** et la carte globale dans l'onglet **Visualizer** . Pour afficher le rapport d'une alerte spécifique, cliquez sur **Afficher le rapport** dans l'onglet **Alertes** .



La page de rapport suivante affiche les événements qui sont surveillés chaque jour pendant chaque

mois. Par exemple, dans la capture d'écran suivante, 3 incidents ont été surveillés le même jour de janvier 2022.



Vous pouvez cliquer sur un incident ou un événement spécifique pour voir les détails, comme le montre l'image suivante :

Surveillance de l'expérience réseau

September 13, 2023

Vue d'ensemble

Le service **Citrix Network Experience Monitoring (NEM)**(anciennement **Netscope**) permet aux fournisseurs de services, aux entreprises, aux FAI et aux fournisseurs de services tiers d'accéder à des journaux de mesure Radar détaillés et à des rapports standard sous la forme de données exploitables

résumées. NEM propose plusieurs journaux et rapports standard que les clients peuvent utiliser pour mesurer la qualité de leurs services.

Cette solution inclut la fourniture « brute » de mesures radar et l'accès à l'API Citrix ITM Data. NEM fournit à la fois les données granulaires (sous forme de mesures brutes ou d'agrégats de données) et les alertes de seuil de données. Ces services aident à la découverte, isolent la disponibilité de la plateforme et les problèmes de performances des homologues de la plateforme et des FAI sous-jacents.

Mesures « brutes » radar: Les mesures radar fournissent des informations granulaires par événement qui sont groupées quotidiennement. Les mesures radar incluent les données de mesure publiques, communautaires et privées collectées par le tag. Les données telles que la disponibilité, le temps de réponse, le débit pour les mesures HTTP et HTTPS sont incluses. Les champs de données suivants sont fournis :

- ID du fournisseur, adresse IP du résolveur, adresses IP client masquées (/28)
- En-tête de référence obscurci, agent utilisateur, ASN de l'utilisateur final
- Données géographiques pour les champs du résolveur et du client

Les mesures radar disponibles dans les mesures « brutes » sont les suivantes :

- Disponibilité, temps de réponse et débit (lorsqu'ils sont mesurés)
- Heure de recherche DNS (en option), heure de connexion TCP (en option) et heure de connexion sécurisée (en option)
- Latence (facultatif)
- Heure de téléchargement (facultatif)

Les mesures radar sont disponibles pour permettre aux clients d'effectuer leur propre analyse des données collectées. L'ensemble de données comprend des informations sur les performances et la disponibilité des fournisseurs (erreurs) pour une gamme de protocoles de communication.

Les données du fichier journal sont disponibles pendant 7 jours à partir d'un compartiment AWS S3 ou Google Cloud Storage. Les clients peuvent récupérer les fichiers journaux des données communautaires et privées à l'aide des méthodes d'accès aux compartiments standard.

Mesures « brutes » radar en temps réel (en option) : Les mesures radar brutes sont fournies en temps réel à un compartiment AWS S3. Ces journaux sont généralement disponibles dans les 5 minutes suivant leur collecte. Ils fournissent autant de granularité que les mesures brutes radar mentionnées précédemment.

API de données : L'API de données Citrix ITM Radar fournit des agrégats de la communauté Radar publique et des données de mesure privées. Les données sont mises à jour en continu et mises en lots environ toutes les 60 secondes pour être récupérées par l'API. L'API de données est fournie pour permettre aux clients d'intégrer les données Radar dans leurs propres rapports et tableaux de bord.

Partage et livraison de journaux

- Les journaux radar peuvent être fournis en temps réel et quotidiennement.
- Les rapports sont exécutés quotidiennement.
- Les résultats sont enregistrés dans AWS S3 (S3) ou Google Cloud Storage (GCS).
- Les journaux et les rapports ont tous deux une période de conservation de 7 jours et sont automatiquement supprimés une semaine après leur création.
- Les rapports sont généralement au format TSV (valeur séparée par des tabulations) ou JSON selon le type de rapport.

Les clients reçoivent des informations de connexion pour accéder aux compartiments S3 et GCS. Un outil de ligne de commande tel que s3cmd ou l'interface de ligne de commande AWS pour S3 ou le gsutil pour GCS peut être utilisé pour vous connecter. Le fichier de configuration S3cmd reconnaît les clés d'accès reçues via l'interface utilisateur du portail et aide l'utilisateur à se connecter au compartiment S3.

L'interface de ligne de commande AWS doit être installée sur l'ordinateur du client pour se connecter à S3 et accéder aux journaux. Pour GCS, le client reçoit le fichier de clé d'accès sous forme de téléchargement via l'interface utilisateur du portail, qui peut être utilisé avec l'outil gsutil. Pour plus d'informations, consultez la FAQ.

Les clients reçoivent des notifications par e-mail dès que des rapports sont disponibles.

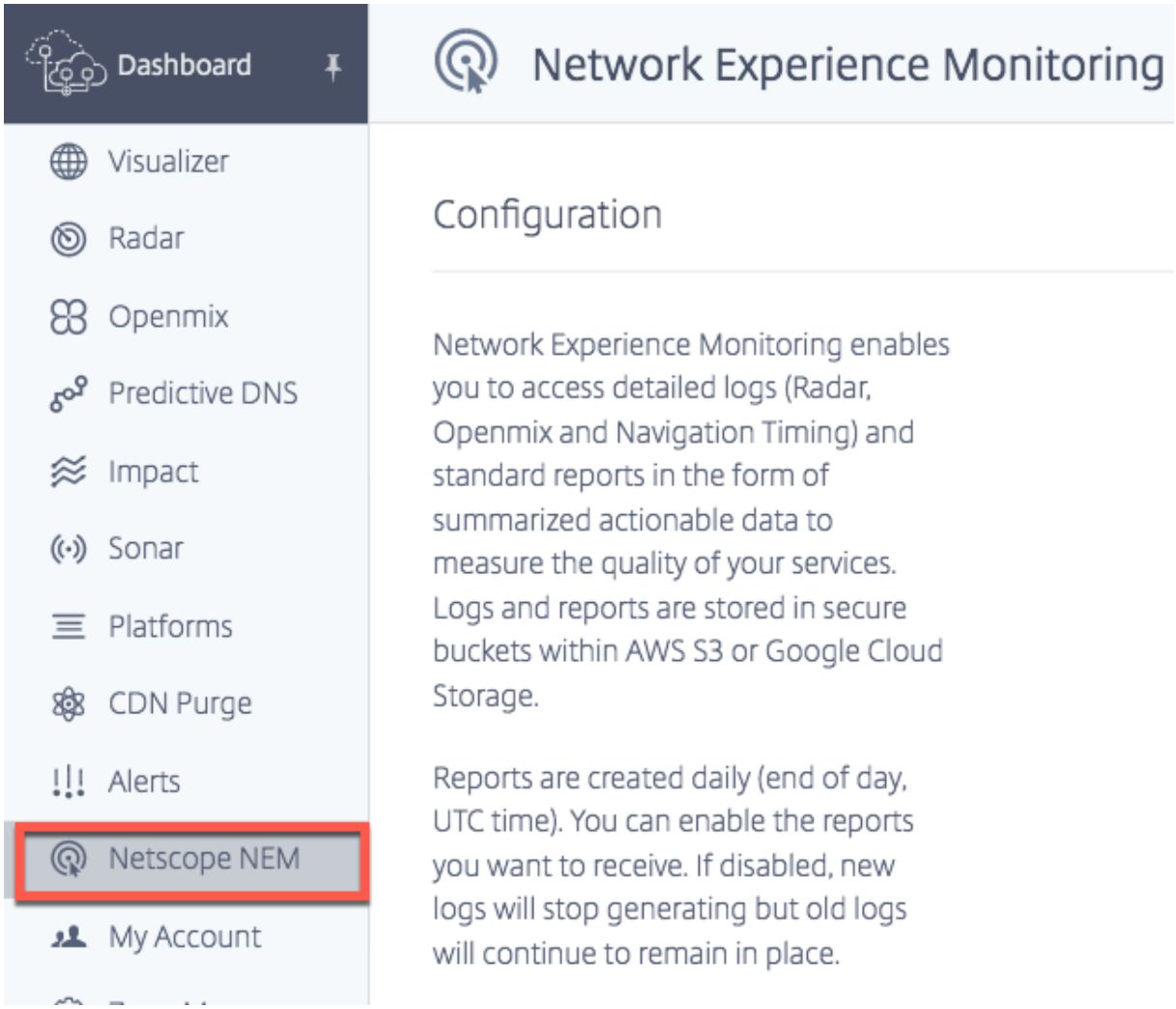
Paramètres de la plate-forme

Vous devez configurer votre plate-forme pour prendre en charge et produire les données requises pour Netscope NEM. Avant de commencer, assurez-vous que les paramètres suivants sont activés pour votre plateforme :

- Pour les rapports Anonymous Best, activez les **paramètres de la sonde radar**.
  - Pour Anonymous Best RTT, activez **Temps de réponse et Disponibilité**.
  - Pour un meilleur débit anonyme, activez **Throughput et Availability**.
- Pour les rapports d'ID de nœud de cache, activez **les paramètres de la sonde radar**et, dans **Paramètres radar avancés**, activez l'**ID de nœud**.
- Pour les détails de synchronisation des ressources, activez **Inclure les horodatages** dans **les paramètres radar avancés**.

Navigation

Dans le menu principal, sélectionnez **Netscope NEM**. La page Configuration de la **surveillance de l' expérience réseau** s'ouvre.



Plateformes et réseaux

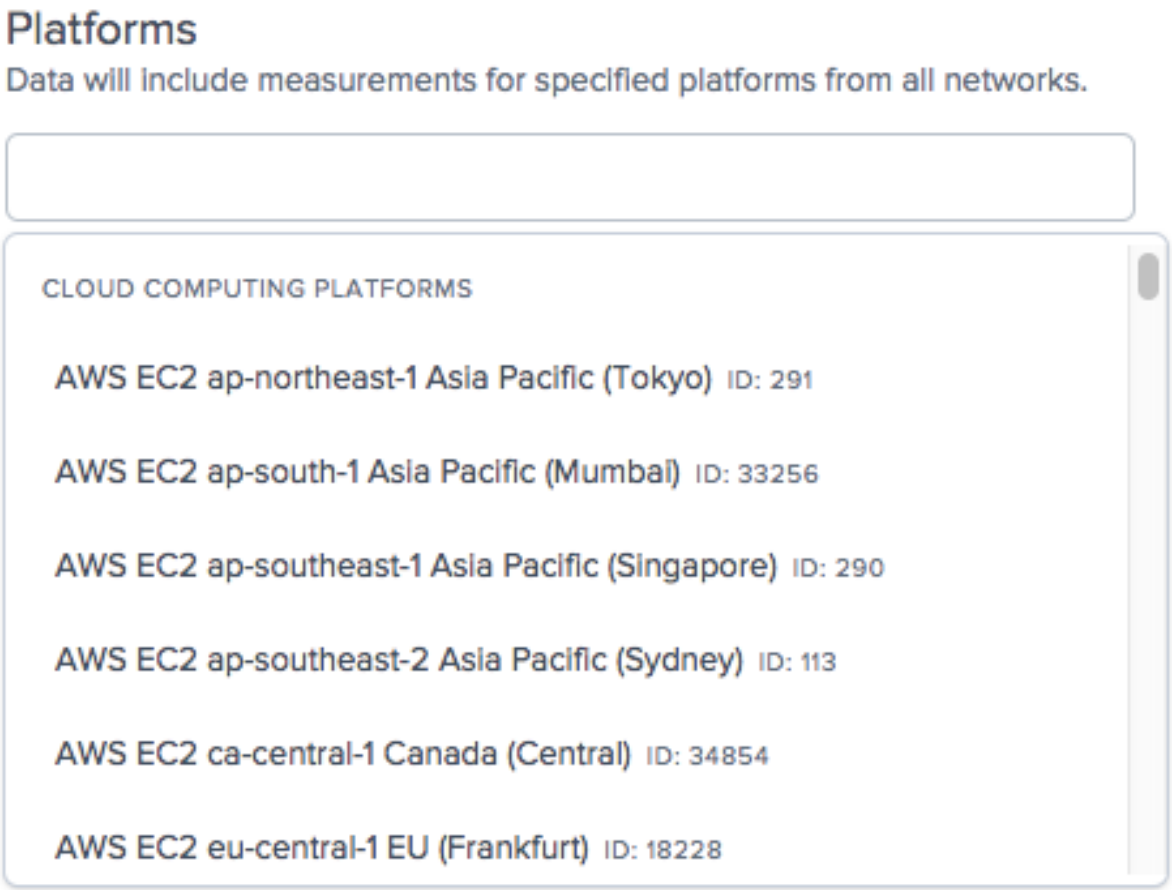
Sélectionnez **Plateformes** ou **Réseaux** requis (ou les deux) pour démarrer le processus de configuration.

> **REMARQUE :**
>
> Les journaux et les rapports peuvent être configurés et générés uniquement si au moins une **plate-forme** ou un **réseau** est sélectionné.

Les données résumées que le client reçoit comprennent les mesures radar de plateformes sélectionnées (pour tous les réseaux associés) ou de réseaux sélectionnés (pour toutes les mesures de plateforme associées).

Sélection de plates-formes

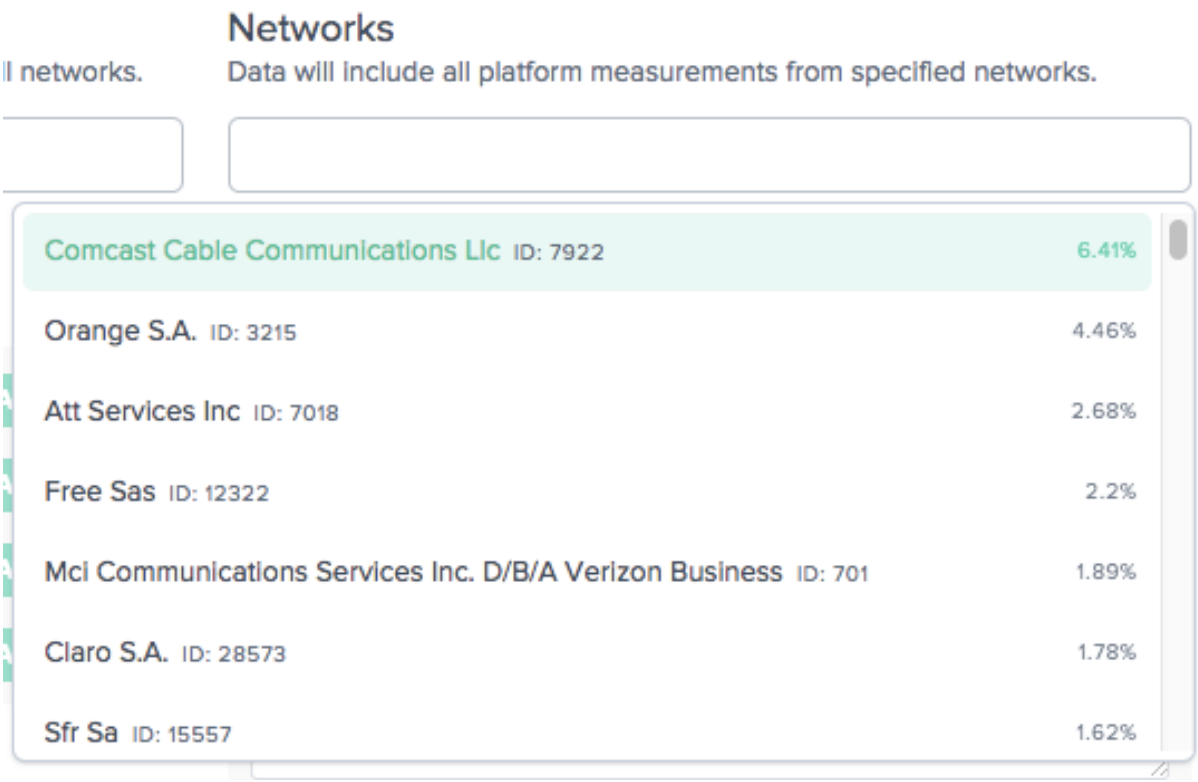
Pour les fournisseurs de services de contenu ou les entreprises, sélectionnez des plateformes telles que des CDN, des clouds, des centres de données ou d'autres points de terminaison. Sélectionnez les plateformes pour lesquelles des mesures sont requises.



Sélection des réseaux

Pour les FAI, sélectionnez **Réseaux** dans la liste associée à différentes plates-formes ou points de terminaison pour lesquels des mesures sont requises.

> **REMARQUE :**
>
> Si vous ne trouvez pas la plate-forme requise dans la liste, vous pouvez la configurer dans la section **Plateforme** du portail. Pour les réseaux non disponibles, contactez l'équipe d'assistance .



Rapports de plateforme

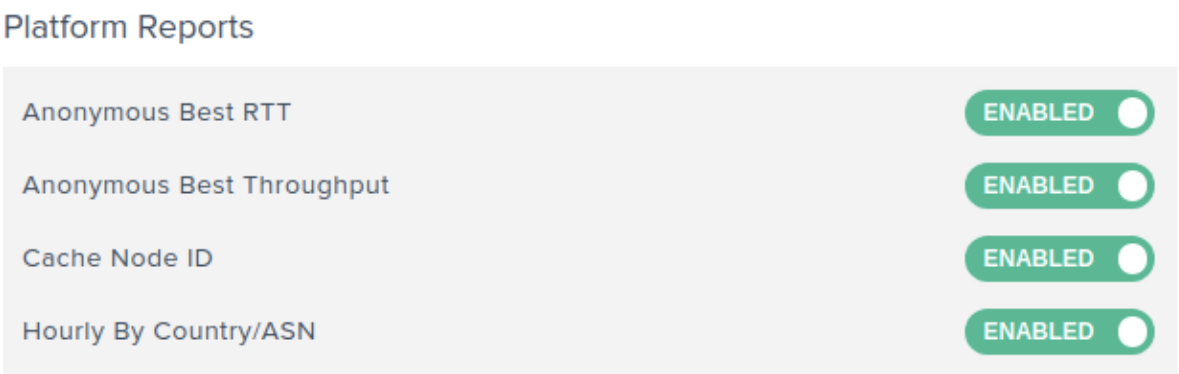
Il existe quatre types de **rapports de plate-forme** :

1. **Meilleur Anonyme pour le temps aller-retour (RTT)**
2. **Anonyme idéal pour le débit**
3. **ID du nœud de cache**
4. **Horaire par pays/ASN**

Pour les descriptions des journaux, consultez Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises.

Activer les rapports de plate-forme

Cliquez sur le bouton bascule pour activer ou désactiver les rapports que vous souhaitez recevoir. Si vous désactivez un rapport existant, les nouveaux journaux ne sont pas générés mais les anciens rapports restent à l'emplacement actuel.



Meilleur rapport anonyme pour les plateformes

- Ces rapports aident les fournisseurs à comparer leurs performances à celles d'autres plateformes au sein de leur groupe de pairs, c'est-à-dire dans le même pays, région ou ASN.
- Les données de performance des 15 meilleurs fournisseurs du groupe homologue sont agrégées sur la base des mêmes catégories. Le meilleur est répertorié à côté du meilleur rapport qualité-prix du fournisseur spécifique.
- Anonymous Best Report for SSL Platforms est disponible afin que leurs performances puissent être comparées à d'autres plates-formes SSL.
- Les adresses IP du client sont tronquées à /28.
- Les résultats du « meilleur » fournisseur aident les Cloud/CDN à concentrer les efforts de performance sur les ASN à volume élevé ou critiques pour l'entreprise qui sont peu compétitifs par rapport à leurs pairs.
- Le rapport fournit des détails sur les performances ventilées par IP du résolveur DNS, IP du client /28 et le nœud de mise en cache qui a servi les objets. La même chose est comparée à la « meilleure » plateforme pour les mêmes critères.

Disponible pour RTT et Débit.

- Pour la description des journaux, voir Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises.

Rapport d'ID de nœud de cache pour les plates-formes

- Ce rapport est utilisé pour identifier le serveur ou le centre de données spécifique qui a répondu à une demande et aider à diagnostiquer les problèmes de serveur.
- Il fournit l'ID du centre de données ou de la machine qui a répondu à une demande spécifique.
- Il aide à comprendre pourquoi les performances via un nœud spécifique (POP ou machine, ou ID de nœud), étaient bonnes ou mauvaises.

- Les performances comprennent le temps de réponse, le débit, la disponibilité (type de sonde), l'adresse IP du résolveur DNS, l'adresse IP du client /28 et le nœud de mise en cache qui a servi les objets.
- Pour les descriptions des journaux, voir [Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises] (#radar -log-descriptions-and-reports-for-service-providers-and-enterprises)

Horaire par pays/ASN

- Ce rapport permet de vérifier si les performances de vos fournisseurs varient considérablement au cours d'une journée.
- Il montre l'heure à laquelle les mesures ont été prises (arrondies à l'heure), par exemple `2018-03-11T23:00:00`.
- Pour la description des journaux, voir Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises.

Rapports réseau

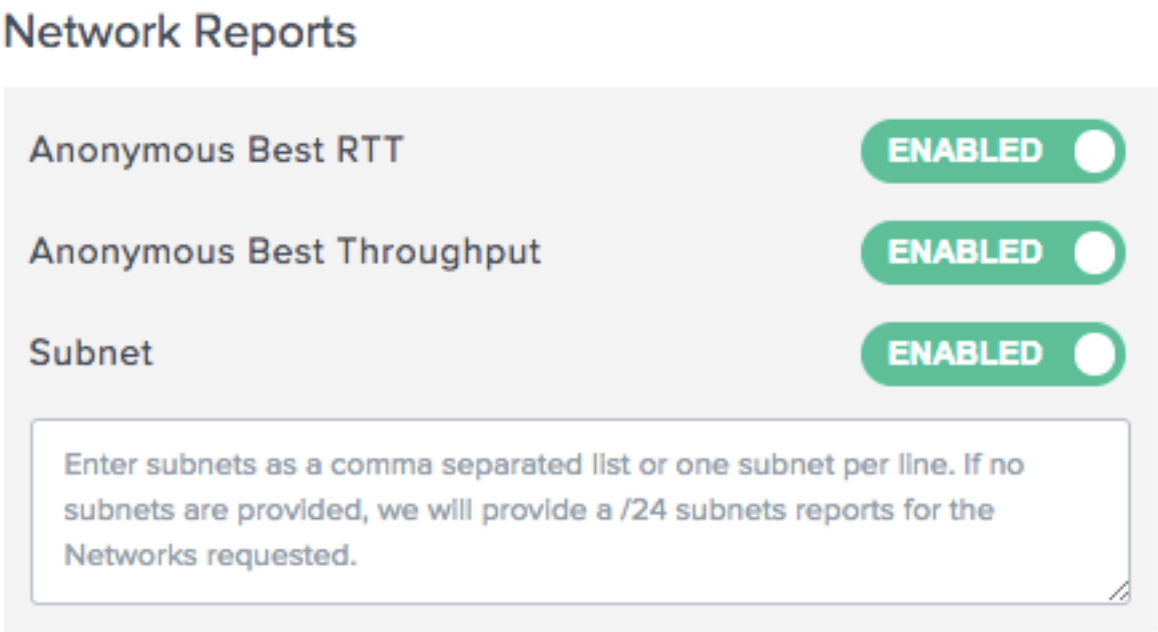
Il existe trois types de **rapports réseau** :

1. **Meilleur Anonyme pour le temps aller-retour (RTT)**
2. **Anonyme idéal pour le débit**
3. **Sous-réseau**

Pour la description des journaux, reportez-vous à la section Descriptions et rapports des journaux radar pour les FAI.

Activer les rapports réseau

Cliquez sur le bouton bascule pour activer ou désactiver les rapports que vous souhaitez recevoir. Lorsque cette option est désactivée, les nouveaux journaux cessent de générer mais les anciens rapports sont en place.
Pour générer un rapport de sous-réseau, entrez les sous-réseaux spécifiques de vos réseaux. Si aucun sous-réseau n'est entré, les rapports sont générés à l'aide du bloc CIDR ASN comme sous-réseau par défaut.



Meilleur rapport anonyme pour les FAI

- Dans le rapport Anonymous Best pour les FAI, un groupe de pairs est utilisé pour la « meilleure » comparaison. Le groupe d'homologues est basé sur l'emplacement du fournisseur de services Internet. Il s'agit généralement des 10 FAI les plus mesurés dans un pays donné, avec un minimum de plus de 1 000 sessions.
- Les résultats du « meilleur » FAI aident les FAI à concentrer leurs efforts de performance sur les plateformes à volume élevé ou critiques et sur les domaines où la concurrence est faible par rapport à leurs pairs.
- Le rapport fournit des détails sur les performances ventilées par géographie et plateforme, et les compare avec le « meilleur » FAI pour les mêmes critères.
- Disponible pour RTT et Débit.
- Pour la description des journaux, reportez-vous à la section Descriptions et rapports des journaux radar pour les FAI.

Rapport de sous-réseau pour les FAI

- Ce rapport fournit aux FAI des informations sur les performances des sous-réseaux spécifiques de leurs réseaux pour les utilisateurs via les plateformes que nous mesurons.
- Il fournit des informations sur le fournisseur de services qui a répondu à une demande spécifique.
- Cela permet de comprendre les performances d'un sous-réseau réseau.

- Les performances comprennent le temps de réponse, le débit, la disponibilité (types de sondes), l'adresse IP du résolveur DNS, l'adresse IP du client /28 et le sous-réseau de l'utilisateur.
- Pour la description des journaux, reportez-vous à la section Descriptions et rapports des journaux radar pour les FAI.

Journaux radar

- Les journaux radar sont disponibles pour les plateformes et les réseaux.
- Ils incluent un sous-ensemble des champs disponibles dans les journaux bruts, avec certaines données anonymisées : IP du client /28, hachage Referer MD5.
- Toutes les mesures prises pour les plates-formes publiques sont fournies, quelle que soit la page qui a généré la mesure.

> **REMARQUE :**
>
> NEM n'expose jamais les adresses IP complètes des clients. Au lieu de cela, il expose le /28. Par exemple, une adresse IP de 255.255.255.255 est affichée dans un rapport sous la forme 255.255.255.240/28.

Fréquence du journal

Les journaux radar peuvent être générés quotidiennement (toutes les 24 heures), c'est-à-dire en fin de journée, heure UTC. Les journaux peuvent également être générés en temps réel (minute par minute).

Format de fichier

Choisissez **TSV ou JSON** pour recevoir les journaux et les rapports dans l'un de ces formats.

Type de mesure

Vous pouvez configurer les journaux pour les types de mesure suivants : disponibilité, temps de réponse et débit. Dans le rapport, 1 : Disponibilité, 0 : Temps de réponse HTTP et 14 : Débit HTTP.

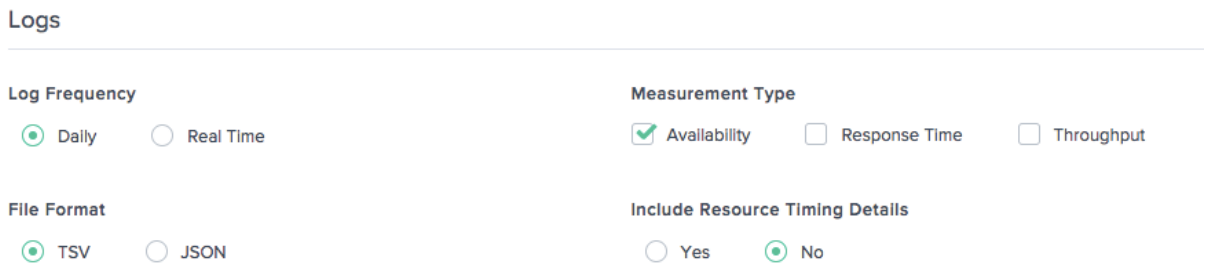
Détails du calendrier des ressources

Vous pouvez choisir d'inclure également les détails de synchronisation des ressources en cliquant sur les boutons **Oui** ou Non. Les détails de la synchronisation des ressources incluent,

- Heure de recherche DNS

- Heure de connexion TCP
- Temps de connexion sécurisé
- Heure de téléchargement

Pour la description des journaux, voir Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises.



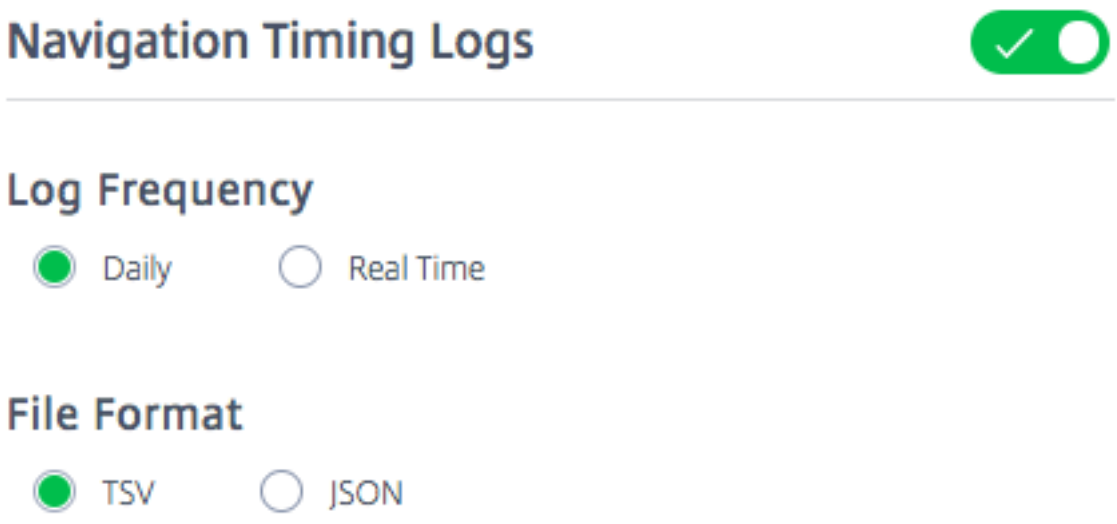
Journaux de synchronisation de navigation

Fréquence du journal

Les journaux de synchronisation de navigation peuvent être générés tous les jours (toutes les 24 heures), c'est-à-dire en fin de journée, heure UTC. Les journaux peuvent également être générés en temps réel (minute par minute).

Format de fichier

Choisissez **TSV** ou **JSON** pour recevoir les journaux de synchronisation de navigation dans l'un de ces formats. Pour la description des journaux, voir Descriptions des journaux de synchronisation de navigation.



Journaux Openmix

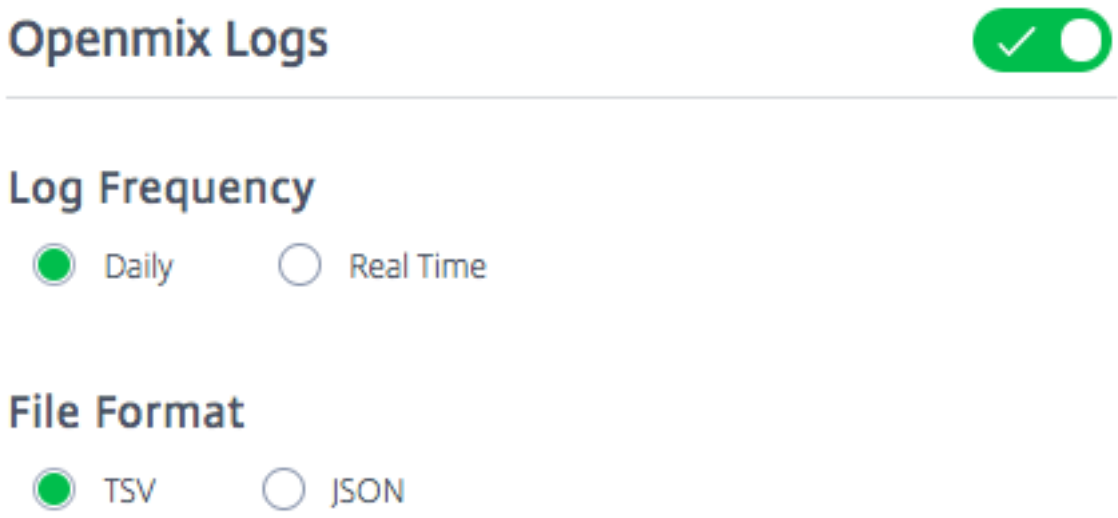
Fréquence du journal

Les journaux Openmix sont générés en temps réel (c'est-à-dire minute par minute). Ces journaux fournissent des mesures en temps réel pour les clients Openmix.

Format de fichier

Choisissez **TSV** ou **JSON** pour recevoir les journaux Openmix et HTTP Openmix dans l'un de ces formats. JSON est cependant le format recommandé.

Pour la description des journaux, consultez la section Descriptions des journaux Openmix.



Prestation de services cloud

Cette option vous permet de sélectionner le mode de livraison. Vous pouvez choisir de recevoir des journaux et des rapports dans le compartiment AWS S3 ou dans le compartiment Google Cloud Storage (GCS).
Vous pouvez accéder aux compartiments S3 et GCS avec les informations de connexion fournies et utiliser s3cmd ou l'interface de ligne de commande AWS pour S3. Et la ligne de commande gsutil pour GCS.

AWS S3

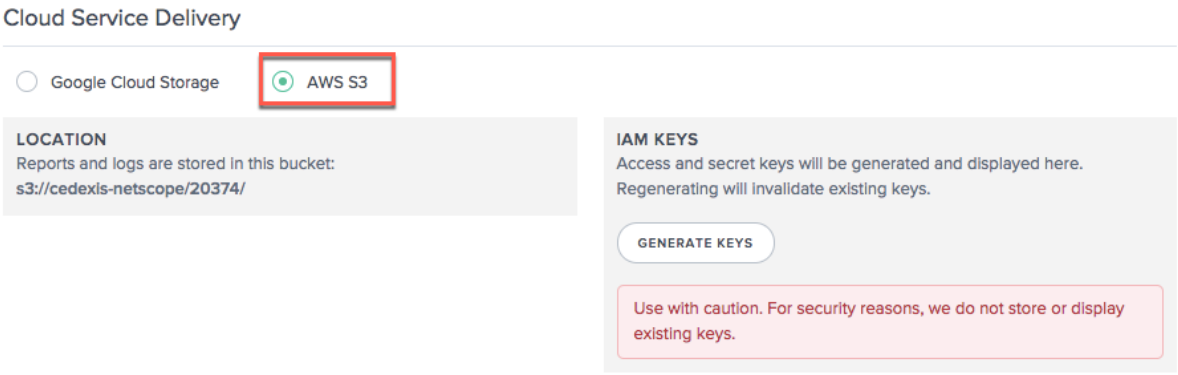
Pour les journaux et les rapports à livrer au compartiment AWS S3, sélectionnez **AWS S3**.

Emplacement L'emplacement représente le compartiment dans AWS S3 où les journaux et les rapports sont enregistrés.

Clés IAM Si vous sélectionnez le bouton **Generate Keys** sous AWS S3, les clés AWS IAM (clés d'accès et clés secrètes) sont générées et affichées sous IAM Keys. Assurez-vous d'enregistrer les clés, car elles ne sont stockées nulle part pour être consultées ultérieurement.

> **REMARQUE :**
>
> La paire de clés d'accès et de clé secrète est la seule copie des clés privées. Le client doit les stocker en toute sécurité. La régénération des nouvelles clés invalide les clés existantes.
> Le fichier de configuration S3cmd reconnaît les clés d'accès (reçues via l'interface utilisateur du portail) et aide le client à se connecter au compartiment S3. L'interface de ligne de commande AWS doit être installée sur la machine du client pour se connecter à S3.

Pour plus d'informations sur l'utilisation des clés d'accès et secrètes avec s3cmd pour télécharger des rapports depuis le compartiment S3, consultez la FAQ.



Stockage Google Cloud

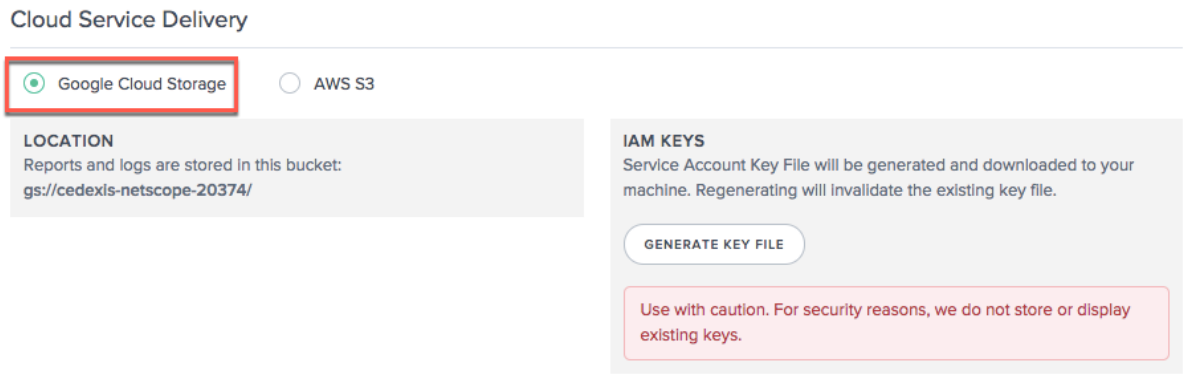
Pour que les journaux et les rapports soient envoyés à GCS, sélectionnez **Google Cloud Storage**.

Emplacement L'emplacement représente le compartiment dans Google Cloud Storage où les journaux et les rapports sont enregistrés.

Clés IAM Lorsque vous sélectionnez le bouton **Générer un fichier de clé**, le fichier de clé de compte de service Google est téléchargé sur votre ordinateur.

> **REMARQUE :**
>
> Ce fichier clé constitue la seule copie de la clé privée. Prenez note de l'adresse e-mail de votre compte de service et stockez en toute sécurité le fichier de clé privée du compte de service. La régénération d'un nouveau fichier clé invalide le fichier existant.

Ce fichier de clé peut être utilisé avec l'outil gsutil pour télécharger des journaux et des rapports à partir du compartiment GCS. Pour plus de détails sur l'utilisation du fichier clé pour télécharger des fichiers journaux, consultez la FAQ.



Descriptions et rapports des journaux radar pour les fournisseurs de services et les entreprises

Journaux radar pour les fournisseurs

- Ces journaux fournissent des mesures radar pour les partenaires de référence.
- Ils fournissent toutes les mesures prises pour les plateformes publiques, quelle que soit la page qui a généré la mesure.
- Les journaux radar comprennent un sous-ensemble des champs disponibles dans les journaux bruts, avec certaines données anonymisées : client IP /28, Referer MD5 haché.
- Voici un exemple de Platform Radar Log Share au format de fichier TSV.

> **REMARQUE :**
>
> - NEM n'expose jamais les adresses IP complètes des clients. Au lieu de cela, il expose le /28. Par exemple, une adresse IP de 255.255.255.255 est affichée dans un rapport sous la forme 255.255.255.240/28.
> - Les informations GEO du client sont extraites en fonction de l'IPv4 du client, qui est plus détaillé.

Descriptions du journal Voici les en-têtes de colonnes et les descriptions des journaux radar. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie :

Journal	Description
Timestamp	Il s'agit de l'heure UTC de la requête au format AAAA-MM-JJTHH:MI:SSZ. La valeur réelle (à la seconde près) dans les tables de journaux est arrondie à l'heure (2018-03-30T 23:00:00 Z) ou au jour (2018-03-30T 00:00:00 Z) le plus proche dans les tables heure/jour, respectivement. L' horodatage est toujours en UTC dans tous les jeux de données.
ID de nœud unique	Également appelé ID de nœud de cache. C'est une valeur arbitraire. En général, il s'agit d'une adresse IP renvoyée par les serveurs CDN Edge pour aider les CDN à identifier en interne quel serveur a traité une demande particulière. » (chaîne vide) : provient de clients Radar qui ne prennent pas en charge la détection UNI. 0 : L' agent utilisateur ne prend pas en charge les fonctionnalités nécessaires à la détection UNI.1 : Le client a rencontré une erreur lors de la détection UNI, telle qu'une erreur HTTP 404 ou une autre réponse infructueuse.2 : La détection UNI a été tentée mais a entraîné une erreur.
ID du fournisseur	ID interne de la plateforme en cours de mesure.
Type de sonde	Type de sonde mesuré (par exemple : 1 : Temps de connexion HTTP, 0 : Temps de réponse HTTP, 14 : Débit HTTP, etc.). Pour indiquer que le service est disponible, utilisez les informations renvoyées avec succès dans le délai imparti.
Code de réponse	Résultat de la mesure.e.g.0 : réussite, 1 : délai d' attente, 4 : erreur. Pour les calculs de disponibilité, le pourcentage de mesures est pris avec une réponse 0 (succès) par rapport au nombre total de mesures (total, quelle que soit la réponse). Pour les autres types de sonde (RTT et débit), le filtre doit uniquement prendre en compte les points de données RTT avec un code de réussite 0 lors du calcul des statistiques sur le RTT. Idem pour le débit.

Journal	Description
Valeur de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il représente les mesures de disponibilité (1) /temps de réponse (0) en millisecondes, et le débit (14) en kbits/s.
Marché des résolveurs	Le marché du résolveur DNS qui a traité la demande. Généralement le continent où se trouve le résolveur DNS, où, 0 : Inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).
Pays de résolution	Le pays du résolveur DNS qui a traité la Request. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région de résolution	La région du résolveur DNS qui a traité la requête.Les ID peuvent être mappés avec des noms dans https://community-radar.citrix.com/ref/regions.json.gz **Remarque :** Tous les pays du monde n'ont pas de régions définies.
État de résolution	L'état du résolveur DNS qui a traité la requête.Les ID peuvent être mappés aux noms dans https://community-radar.citrix.com/ref/states.json.gz Remarque : Tous les pays du monde n'ont pas d'états définis.
Ville de résolution	Ville du résolveur DNS qui a traité la requête.La ville du résolveur est ajoutée en recherchant une adresse IP de résolveur. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/cities.json.gz
ASN de résolution	Numéro de système autonome (NSA) de la résolution DNS qui a traité la demande. En règle générale, l'ASN qui possède les ID de résolveur DNS peut être mappé avec des noms sur https://community-radar.citrix.com/ref/asns.json.gz

Journal	Description
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
Marché client	Le marché de l'utilisateur final qui a généré cette mesure. Généralement le continent où se trouve l'adresse IP du client ; où, 0 : inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).
Pays client	Le pays de l'utilisateur final qui a généré cette mesure. Les identifiants peuvent être mappés avec des noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région cliente	Région de l'utilisateur final qui a généré cette mesure. Généralement, la région géographique dans laquelle se trouve l'adresse IP du client. Les ID peuvent être mappés avec des noms à https://community-radar.citrix.com/ref/regions.json.gz Remarque : Tous les pays du monde n'ont pas de régions définies.
État du client	État de l'utilisateur final qui a généré cette mesure. Généralement, l'état où se trouve l' adresse IP du client.Les ID peuvent être mappés à des noms à https://community-radar.citrix.com/ref/states.json.gz Remarque, que tous les pays du monde n'ont pas d'états définis.
Ville client	La ville de l'utilisateur final qui a généré cette mesure. Généralement, la ville où se trouve l' adresse IP du client. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/cities.json.gz

Journal	Description
ASN client	Numéro de système autonome (ASN) de l'utilisateur final qui a généré cette mesure. En règle générale, l'ASN qui contient l'adresse IP du client. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/asns.json.gz
IP du client	L'adresse IP de l'utilisateur final qui a généré cette mesure.
Hôte référent MD5	Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar. L'hôte référent est haché MD5.
User Agent	Il s'agit de la chaîne de l'agent utilisateur de la page du navigateur qui héberge la balise. Par exemple, si vous utilisez Chrome et que vous parcourez une page contenant la balise Radar, les mesures radar en arrière-plan enregistrent l'agent utilisateur à partir de votre navigateur Chrome. Les mesures incluent le navigateur Chrome, la version de Chrome, des informations sur le système d'exploitation sur lequel Chrome est exécuté, etc.
Heure de recherche DNS (facultatif)	Avec l'API Resource Timing, la différence entre la fin de la recherche de domaine et le début de la recherche de domaine est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : DomainLookupEnd - DomainLookupStart.
Heure de connexion TCP (facultatif)	Avec l'API Resource Timing, la différence entre la fin de la connexion et le début de la connexion est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - ConnectStart.

Journal	Description
Durée de connexion sécurisée (facultatif)	Avec l'API Resource Timing, la différence entre Connect End et Secure Connection Start est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - SecureConnectionStart.
Latence (facultatif)	Avec l'API Resource Timing, la différence entre Response Start et Request Start est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de début de la réponse est supérieure à l'heure de début de la demande. Il est calculé comme ResponseStart - RequestStart
Heure de téléchargement (Facultatif)	Avec l'API Resource Timing, la différence entre la fin de la réponse et le début de la réponse est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme ResponseEnd - ResponseStart.
Profil du client	Ce champ permet de déterminer si les données proviennent d'applications mobiles ou de navigateurs. Il nous permet également de différencier les applications iOS, Android et les navigateurs. Un numéro est utilisé pour identifier chaque profil client. Les valeurs de ce champ sont : null, 0, 1, 2, 3, 4. Où, null : implique généralement un ancien client Radar qui ne prend pas en charge l'envoi de la valeur client_profile. 0 : Navigateur ; 1 : iOS - Application Radar Runner pour iOS écrite en Swift ; 2 : Android ; 3 : Navigateur sur la version mobile du site Web ; 4 : iOS - Application Radar Runner pour iOS écrite en Objective-C.

Journal	Description
Version du profil client	La version du profil client nous indique quelle version du code Radar Runner (pour iOS) ou du SDK AndroidRadar (pour Android) a été utilisée dans l'application mobile. Ce champ est réservé à un usage interne.
Catégorie d'appareils	Tous les appareils sont classés dans l'une des catégories suivantes : smartphone, tablette, PC, Smart TV et autres. « Autre » est utilisé comme valeur par défaut si l'analyseur n'est pas en mesure de déterminer la valeur de l'un des champs.
Appareil	Type d'appareil sur lequel se trouve l'utilisateur, par exemple un iPhone Apple. La chaîne de l' agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
Navigateur	Type de navigateur utilisé par l'utilisateur, par exemple Mobile Safari UI/WKWebView 0.0.0. La chaîne de l'agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
OS	Le système d'exploitation utilisé. Par exemple, iOS 11.0.3. La chaîne de l'agent utilisateur le détecte à partir du navigateur exécuté sur la page hébergeant la balise Radar.
IP du client Reporting	Cette adresse IP est l'adresse IP publique masquée /48 de l'utilisateur effectuant la mesure. Il peut s'agir d'IPv4 ou d'IPv6 (lorsqu'il est pris en charge).

Meilleur rapport anonyme

- Les meilleurs rapports anonymes aident les fournisseurs à comparer leurs performances à celles du groupe de pairs de l'autre plateforme, c'est-à-dire au sein du même pays, de la même région ou de la même ASN.
- Les données de performance des 15 meilleurs fournisseurs du groupe homologue sont agrégées sur la base des mêmes catégories. Le meilleur est répertorié à côté du meilleur rapport qualité-

prix du fournisseur spécifique.
- Anonymous Best Report pour les plates-formes SSL est disponible afin que leurs performances puissent être comparées avec d'autres plates-formes SSL.
- Les adresses IP du client sont tronquées à /28.
- Les résultats du « meilleur » fournisseur aident les Cloud/CDN à concentrer les efforts de performance sur les ASN à volume élevé ou critiques pour l'entreprise qui sont peu compétitifs par rapport à leurs pairs.
- Le rapport fournit des détails sur les performances en fonction de l'adresse IP du résolveur DNS, de l'adresse IP du client /28 et du nœud de mise en cache qui a servi les objets. Elle est comparée à la « meilleure » plateforme pour les mêmes critères.
- Disponible pour RTT ou Débit.
- Ce qui suit est un exemple de meilleur rapport anonyme de plate-forme pour RTT au format de fichier TSV.

Descriptions du journal Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions du meilleur rapport anonyme. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie.

Journal	Description
Pays de résolution	Pays du résolveur DNS qui a traité la demande.
Région de résolution	Région du résolveur DNS qui a traité la demande.
État de résolution	État du résolveur DNS qui a traité la demande.
ID ASN du résolveur	Numéro de système autonome du résolveur DNS qui a traité la demande. Généralement, l'ASN qui possède le résolveur DNS.
Nom de l'ASN du résolveur	Le nom de l'ASN.
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
Pays client	Le pays de l'utilisateur final qui a généré cette mesure.
Région cliente	Région de l'utilisateur final qui a généré cette mesure.
État du client	État de l'utilisateur final qui a généré cette mesure.
ID ASN du client	Numéro ASN (Autonomous System Number) de l'utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client.

Journal	Description
Nom de l'ASN client	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
IP du client	L'adresse IP de l'utilisateur final qui a généré la mesure.
Succès	Nombre total de mesures réussies.Conseil : Succès/Total == Disponibilité.
Délais d'expiration	Le nombre de mesures dont le délai a expiré.
Erreurs	Le nombre de mesures qui comportaient des erreurs.
Total :	Le nombre total de mesures.
Moyenne	La moyenne de toutes les valeurs de mesure pour cette ligne.
Meilleure moyenne	La meilleure moyenne parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures moyennes	Nombre total de mesures ayant produit le meilleur décompte moyen.
Médiane	La valeur du 50e centile est la valeur médiane des mesures pour un fournisseur particulier, lorsque les mesures sont répertoriées dans l' ordre.
Meilleure médiane	La meilleure valeur du 50e centile (en dessous de laquelle se trouvent 50 % des mesures) des 15 meilleurs fournisseurs du groupe homologue.
Meilleures mesures médianes	Nombre total de mesures ayant produit la meilleure médiane
5th	Valeur du 5e centile pour le fournisseur.
Meilleur 5e	La meilleure valeur du 5e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures 5èmes mesures	Nombre total de mesures ayant produit le meilleur_5e
10th	Valeur du 10e centile pour le fournisseur.
Meilleur 10e	La meilleure valeur du 10e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures 10e	Nombre total de mesures ayant produit le meilleur_10e
90th	Valeur du 90e centile pour le fournisseur.

Journal	Description
Meilleur 90e	La meilleure valeur du 90e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures du 90e	Nombre total de mesures ayant produit le meilleur 90e
95th	Valeur du 95e centile pour le fournisseur.
Meilleur 95e	La meilleure valeur au 95e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures de la 95e	Nombre total de mesures ayant produit le meilleur 95e
Stdev	L'écart type pour le fournisseur
Best Stdev	Le meilleur écart type parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures Stdev	Nombre total de mesures ayant produit le meilleur std.dev.
Disponibilité	La disponibilité en pourcentage pour le fournisseur. La disponibilité est le taux de réussite de la sonde, c.-à-d. Succès/(Succès + Échecs + Délais)
Meilleure disponibilité	La meilleure valeur de disponibilité parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures de disponibilité	Le nombre de mesures ayant produit la meilleure disponibilité
Importance	Valeurs synthétiques générées pour aider à trouver des données exploitables.
ID de nœud unique	Ces ID sont une liste séparée par des virgules des ID de nœud uniques pour les mesures de cette ligne.
Type de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s' agit de HTTP_COLD (disponibilité), HTTP_RTT (temps aller-retour) ou HTTP_KBPS (débit).
ID du fournisseur	Numéro d'identification NetScaler ITM interne de ce fournisseur.

Rapport d'ID de nœud de cache (précédemment rapport du fournisseur de services multiples)

Ce rapport est utilisé pour identifier le serveur ou le centre de données spécifique qui a répondu à une demande et aider à diagnostiquer les problèmes de serveur.

- Il fournit l'ID du centre de données ou de la machine qui a répondu à une demande spécifique.
- Il aide à comprendre pourquoi les performances via un nœud spécifique (POP ou machine, ou ID de nœud), étaient bonnes ou mauvaises.
- Les performances comprennent le temps de réponse, le débit, la disponibilité (type de sonde), l'adresse IP du résolveur DNS, l'adresse IP du client /28 et le nœud de mise en cache qui a servi les objets.
- Voici un exemple de rapport Platform Cache Node ID au format de fichier TSV.

Descriptions du journal Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions du rapport d'ID de nœud de cache. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie :

Journal	Description
Nom du fournisseur	C'est le nom du fournisseur qui est mesuré.
Valeur de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s' agit des mesures connect (1) /RTT (0) en millisecondes et des mesures de débit (14) en kbps.
ID de nœud unique	Il est connu sous le nom d'ID de nœud de cache. Une valeur arbitraire, généralement une adresse IP renvoyée par les serveurs CDN Edge pour aider les CDN à identifier en interne quel serveur a traité une requête particulière. » (chaîne vide) : provient de clients Radar qui ne prennent pas en charge la détection UNI. 0 : L'agent utilisateur ne prend pas en charge les fonctionnalités nécessaires à la détection UNI.1 : Le client trouve une erreur lors de la détection UNI, telle qu'une erreur HTTP 404 ou une autre réponse infructueuse.2 : La détection UNI a été tentée mais a entraîné une erreur.
Pays de résolution	Pays du résolveur DNS qui a traité la demande.

Journal	Description
Région de résolution	Région du résolveur DNS qui a traité la demande.
État de résolution	État du résolveur DNS qui a traité la demande.
ASN de résolution	Numéro de système autonome du résolveur DNS qui a traité la demande. Généralement, l'ASN qui possède le résolveur DNS.
Nom de l'ASN du résolveur	Le nom de l'ASN.
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
Pays client	Le pays de l'utilisateur final qui a généré cette mesure.
Région cliente	Région de l'utilisateur final qui a généré cette mesure.
État du client	État de l'utilisateur final qui a généré cette mesure.
ASN client	Numéro ASN (Autonomous System Number) de l'utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client.
Nom de l'ASN client	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
IP du client	L'adresse IP de l'utilisateur final qui a généré la mesure.
Succès	Nombre total de mesures réussies.Conseil : Succès/Total == Disponibilité.
Délai d'expiration	Le nombre de mesures dont le délai a expiré.
Erreur	Le nombre de mesures qui comportaient des erreurs.
Total :	Le nombre total de mesures.
Moyenne	La moyenne des valeurs de mesure pour chaque ligne.
Médiane	La valeur du 50e centile est la valeur médiane des mesures pour un fournisseur particulier, lorsque les mesures sont répertoriées dans l'ordre.
5th	Valeur du 5e centile pour le fournisseur.
10th	Valeur du 10e centile pour le fournisseur.

Journal	Description
90th	Valeur du 90e centile pour le fournisseur.
95th	Valeur du 95e centile pour le fournisseur.
Stdev	L'écart type pour le fournisseur.
Disponibilité	La disponibilité en pourcentage pour le fournisseur.
Importance	Valeurs synthétiques générées pour aider à trouver des données exploitables.

Rapport horaire par pays/ASN

- Ce rapport permet de vérifier si les performances de vos fournisseurs varient considérablement au cours d'une journée.
- Il montre l'heure à laquelle les mesures ont été prises (arrondies à l'heure), par exemple `2018-03-11T23:00:00`.
- Voici un exemple de rapport Platform Hourly by Country/ASN au format de fichier TSV.

Descriptions du journal Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions du rapport horaire par pays/ASN. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie :

Journal	Description
Horodatage 60 minutes	L'heure UTC à laquelle les mesures ont été prises est tronquée à l'heure, par exemple2018-03-11T 23:00:00.
Nom du fournisseur	C'est le nom du fournisseur qui est mesuré.
Type de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s' agit de HTTP_COLD (disponibilité), HTTP_RTT (temps aller-retour) ou HTTP_KBPS (débit).
Pays client	Le pays de l'utilisateur final qui a généré cette mesure.
ASN client	Numéro ASN (Autonomous System Number) de l' utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client.

Journal	Description
Nom de l'ASN client	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
Succès	Nombre total de mesures réussies.Conseil : Succès/Total == Disponibilité.
Délai d'expiration	Le nombre de mesures dont le délai a expiré.
Erreur	Le nombre de mesures qui comportaient des erreurs.
Total :	Le nombre total de mesures.
Moyenne	La moyenne des valeurs de mesure pour chaque ligne.
Médiane	La valeur du 50e centile est la valeur médiane des mesures pour un fournisseur particulier, lorsque les mesures sont répertoriées dans l' ordre.
5th	Valeur du 5e centile pour le fournisseur.
10th	Valeur du 10e centile pour le fournisseur.
90th	Valeur du 90e centile pour le fournisseur.
95th	Valeur du 95e centile pour le fournisseur.
Stdev	L'écart type pour le fournisseur.
Disponibilité	La disponibilité en pourcentage pour le fournisseur.
Importance	Valeur synthétique générée pour aider à trouver des données exploitables.
ID du fournisseur	Numéro d'identification NetScaler ITM interne de ce fournisseur.

Descriptions et rapports des journaux radar pour les FAI

Journaux radar pour les FAI

Les journaux radar permettent aux FAI de mesurer en détail leurs performances par rapport aux plateformes mondiales. Les FAI peuvent utiliser ces données pour trouver les domaines dans lesquels des améliorations doivent être apportées ou pour vérifier les performances attendues.

- Permet d'accéder aux mesures radar.

- Fournit des mesures prises auprès des FAI sur des plateformes publiques, quelle que soit la page qui a généré la mesure.
- Les journaux radar incluent un sous-ensemble des champs disponibles dans les journaux bruts, avec certaines données anonymisées : IP du client /28, hachage MD5 du référent.
- Les fichiers journaux sont au format TSV.
- Voici un exemple de partage de journaux Network Radar au format de fichier TSV.

Descriptions du journal Voici les en-têtes de colonnes et les descriptions des journaux Radar pour les FAI. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie.

Journal	Description
Timestamp	Il s'agit de l'heure UTC de la requête au format YYYY-MM-DDTHH:MI:SSZ. La valeur réelle (à la seconde près) dans les tables de journaux est arrondie à l'heure (2018-03-30T 23:00:00 Z) ou au jour (2018-03-30T 00:00:00 Z) le plus proche dans les tables heure/jour, respectivement. L' horodatage est toujours en UTC dans tous les jeux de données.
ID du fournisseur	ID interne de la plateforme en cours de mesure.
Type de sonde	Type de sonde mesuré (par exemple : 1 : Temps de connexion HTTP, 0 : Temps de réponse HTTP, 14 : Débit HTTP, etc.). Les informations renvoyées avec succès dans le délai imparti sont utilisées pour indiquer que le service est disponible.
Code de réponse	Résultat de la mesure.e.g.0 : réussite, 1 : délai d' attente, 4 : erreur. Pour les calculs de disponibilité, le pourcentage de mesures est pris avec une réponse 0 (succès) par rapport au nombre total de mesures (total). Pour les autres types de sonde (RTT et débit), le filtre doit uniquement prendre en compte les points de données RTT avec un code de réussite 0 lors du calcul des statistiques sur le RTT. Idem pour le débit.

Journal	Description
Valeur de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s'agit des mesures de disponibilité (1)/Temps de réponse (0) en millisecondes et de Débit (14) en Kbits/s.
Marché des résolveurs	Le marché du résolveur DNS qui a traité la demande. Généralement le continent où se trouve le résolveur DNS, où, 0 : Inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).
Pays de résolution	Le pays du résolveur DNS qui a traité les ID de demande peut être mappé aux noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région de résolution	La région du résolveur DNS qui a traité les ID de demande peut être mappée aux noms sur https://community-radar.citrix.com/ref/regions.json.gz. Tous les pays du monde n'ont pas de régions définies.
État de résolution	L'état du résolveur DNS qui a traité les ID de demande peut être mappé aux noms sur https://community-radar.citrix.com/ref/states.json.gz. Tous les pays du monde n'ont pas d'États définis.
ASN de résolution	Numéro de système autonome (NSA) de la résolution DNS qui a traité la demande. En général, l'ASN qui possède les ID de résolveur DNS peut être mappé aux noms sur https://community-radar.citrix.com/ref/asns.json.gz.
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.

Journal	Description
Marché client	Le marché de l'utilisateur final qui a généré cette mesure. Généralement le continent où se trouve l'adresse IP du client ; où, 0 : inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).
Pays client	Le pays de l'utilisateur final qui a généré cette mesure. Les identifiants peuvent être mappés avec des noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région cliente	Région de l'utilisateur final qui a généré cette mesure. Généralement la région géographique dans laquelle se trouve l'adresse IP du client. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/regions.json.gz. Tous les pays du monde n'ont pas de régions définies.
État du client	État de l'utilisateur final qui a généré cette mesure. En général, l'état dans lequel se trouve l'adresse IP du client. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/states.json.gz. Tous les pays du monde n'ont pas d'États définis.
ASN client	Numéro de système autonome (ASN) de l' utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/asns.json.gz
IP du client	L'adresse IP de l'utilisateur final qui a généré cette mesure.
Hôte référent MD5	Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar. L'hôte référent est haché MD5.

Journal	Description
User Agent	Il s'agit de la chaîne de l'agent utilisateur de la page du navigateur qui héberge la balise. Par exemple, si vous utilisez Chrome et que vous parcourez une page contenant la balise Radar, les mesures radar en arrière-plan enregistrent l'agent utilisateur à partir de votre navigateur Chrome. Les mesures incluent le navigateur Chrome, la version de Chrome, des informations sur le système d'exploitation sur lequel Chrome est exécuté, etc.
Heure de recherche DNS (facultatif)	Avec l'API Resource Timing, la différence entre la fin de la recherche de domaine et le début de la recherche de domaine est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : DomainLookupEnd - DomainLookupStart.
Heure de connexion TCP (facultatif)	Avec l'API Resource Timing, la différence entre la fin de la connexion et le début de la connexion est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - ConnectStart.
Durée de connexion sécurisée (facultatif)	Avec l'API Resource Timing, la différence entre la fin de connexion et le démarrage de la connexion sécurisée est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - SecureConnectionStart.
Latence (facultatif)	Avec l'API Resource Timing, la différence entre Response Start et Request Start est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de début de la réponse est supérieure à l'heure de début de la demande. Il est calculé comme ResponseStart - RequestStart

Journal	Description
Heure de téléchargement (Facultatif)	Avec l'API Resource Timing, la différence entre la fin de la réponse et le début de la réponse est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme ResponseEnd - ResponseStart.
Profil du client	Ce champ permet de déterminer si les données proviennent d'applications mobiles ou de navigateurs. Il nous permet également de différencier les applications iOS, Android et les navigateurs. Un numéro est utilisé pour identifier chaque profil client. Les valeurs de ce champ sont : null, 0, 1, 2, 3, 4. Où, null : implique généralement un ancien client Radar qui ne prend pas en charge l'envoi de la valeur client_profile. 0 : Navigateur ; 1 : iOS - Application Radar Runner pour iOS écrite en Swift ; 2 : Android ; 3 : Navigateur sur la version mobile du site Web ; 4 : iOS - Application Radar Runner pour iOS écrite en Objective-C.
Version du profil client	La version du profil client nous indique quelle version du code Radar Runner (pour iOS) ou du SDK AndroidRadar (pour Android) a été utilisée dans l'application mobile. Ce champ est réservé à un usage interne.
Catégorie d'appareils	Tous les appareils sont classés dans l'une des catégories suivantes : smartphone, tablette, PC, Smart TV et autres. « Autre » est utilisé comme valeur par défaut si l'analyseur n'est pas en mesure de déterminer la valeur de l'un des champs.
Appareil	Type d'appareil sur lequel se trouve l'utilisateur, par exemple un iPhone Apple. La chaîne de l' agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.

Journal	Description
Navigateur	Type de navigateur utilisé par l'utilisateur, par exemple Mobile Safari UI/WKWebView 0.0.0. La chaîne de l'agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
OS	Système d'exploitation utilisé, par exemple iOS 11.0.3. La chaîne de l'agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.

Rapport de sous-réseau pour les FAI

- Le rapport fournit aux FAI des informations sur les performances des sous-réseaux spécifiques de leurs réseaux pour leurs utilisateurs via les plateformes mesurées.
- Il fournit des informations sur le fournisseur de services qui a répondu à une demande spécifique.
- Cela aide à comprendre les performances du sous-réseau réseau.
- Les performances comprennent le temps de réponse, le débit, la disponibilité (type de sonde), l'adresse IP du résolveur DNS, l'adresse IP du client /28 et le nœud de mise en cache qui a servi les objets.
- Voici un exemple de rapport de sous-réseau réseau au format de fichier TSV.

Descriptions du journal Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions du rapport de sous-réseau pour les FAI. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie :

Journal	Description
Nom de l'ASN	Le nom du système autonome à partir duquel la mesure a été prise.
Valeur de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s'agit des mesures connect (1) /RTT (0) en millisecondes et des mesures de débit (14) en kbps.
Sous-réseau	Sous-réseau de l'utilisateur d'où provient la demande.

Journal	Description
ASN de résolution	Numéro de système autonome du résolveur DNS qui a traité la demande. Généralement, l'ASN qui possède le résolveur DNS.
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
ASN client	Numéro ASN (Autonomous System Number) de l'utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client.
IP du client	L'adresse IP de l'utilisateur final qui a généré la mesure.
ID de la plate-forme	ID de la plateforme du fournisseur de services sur laquelle la requête a été effectuée.
Nom de la plateforme	Le nom de la plateforme du fournisseur de services sur laquelle la requête a été effectuée
Succès	Nombre total de mesures réussies.Conseil : Succès/Total == Disponibilité.
Délai d'expiration	Le nombre de mesures dont le délai a expiré.
Erreur	Le nombre de mesures qui comportaient des erreurs.
Total :	Le nombre total de mesures.
Moyenne	La moyenne des valeurs de mesure pour chaque ligne.
Médiane	La valeur du 50e centile est la valeur médiane des mesures pour un fournisseur particulier, lorsque les mesures sont répertoriées dans l'ordre.
5th	Valeur du 5e centile pour le fournisseur.
10th	Valeur du 10e centile pour le fournisseur.
90th	Valeur du 90e centile pour le fournisseur.
95th	Valeur du 95e centile pour le fournisseur.
Stdev	L'écart type pour le fournisseur.
Disponibilité	La disponibilité en pourcentage pour le fournisseur.

Journal	Description
Importance	Valeurs synthétiques générées pour aider à trouver des données exploitables.
Type de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s'agit de HTTP_COLD (disponibilité), HTTP_RTT (temps aller-retour) ou HTTP_KBPS (débit).

Meilleur rapport anonyme pour les FAI

- Dans le rapport Anonymous Best, un groupe de pairs est utilisé pour la « meilleure » comparaison. Le groupe d'homologues est basé sur l'emplacement du fournisseur de services Internet. Il s'agit généralement des 10 FAI les plus mesurés dans un pays donné, avec un minimum de plus de 1 000 sessions.
- Les résultats du « meilleur » FAI aident les FAI à concentrer leurs efforts de performance sur les plateformes à volume élevé ou critiques et sur les domaines où la concurrence est faible par rapport à leurs pairs.
- Le rapport fournit des détails sur les performances ventilées par géographie et plateforme, et les compare avec le « meilleur » FAI pour les mêmes critères.
- Disponible pour RTT et Débit.
- Voici un exemple de meilleur rapport Network Anonymous pour RTT au format de fichier TSV.

Descriptions du journal Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions du meilleur rapport anonyme. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie.

Journal	Description
Type de mesure	Valeur de mesure enregistrée, dont la signification varie selon le type de sonde. Il s'agit de HTTP_COLD (disponibilité), HTTP_RTT (temps aller-retour) ou HTTP_KBPS (débit).
Pays client	Le pays de l'utilisateur final qui a généré cette mesure.
Région cliente	Région de l'utilisateur final qui a généré cette mesure.
État du client	État de l'utilisateur final qui a généré cette mesure.

Journal	Description
ID ASN du client	Numéro ASN (Autonomous System Number) de l'utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client.
Nom de l'ASN client	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
Pays de résolution	Pays du résolveur DNS qui a traité la demande.
Région de résolution	Région du résolveur DNS qui a traité la demande.
État de résolution	État du résolveur DNS qui a traité la demande.
ID de la plate-forme	ID de la plate-forme du fournisseur de services sur laquelle la requête a été tentée.
Nom de la plateforme	Nom de la plate-forme du fournisseur de services sur laquelle la requête a été tentée.
Succès	Nombre total de mesures réussies.Conseil : Succès/Total == Disponibilité.
Délais d'expiration	Le nombre de mesures dont le délai a expiré.
Erreurs	Le nombre de mesures qui comportaient des erreurs.
Total :	Le nombre total de mesures.
Moyenne	La moyenne de toutes les valeurs de mesure pour cette ligne.
Meilleure moyenne	La meilleure moyenne parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures moyennes	Nombre total de mesures ayant produit le meilleur décompte moyen.
Médiane	La valeur du 50e centile est la valeur médiane des mesures pour un fournisseur particulier, lorsque les mesures sont répertoriées dans l'ordre.
Meilleure médiane	La meilleure valeur du 50e centile (en dessous de laquelle se trouvent 50 % des mesures) des 15 meilleurs fournisseurs du groupe homologue.
Meilleures mesures médianes	Nombre total de mesures ayant produit la meilleure médiane
5th	Valeur du 5e centile pour le fournisseur.

Journal	Description
Meilleur 5e	La meilleure valeur du 5e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures 5èmes mesures	Nombre total de mesures ayant produit le meilleur_5e
10th	Valeur du 10e centile pour le fournisseur.
Meilleur 10e	La meilleure valeur du 10e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures 10e	Nombre total de mesures ayant produit le meilleur_10e
90th	Valeur du 90e centile pour le fournisseur.
Meilleur 90e	La meilleure valeur du 90e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures du 90e	Nombre total de mesures ayant produit le meilleur 90e
95th	Valeur du 95e centile pour le fournisseur.
Meilleur 95e	La meilleure valeur au 95e centile parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures de la 95e	Nombre total de mesures ayant produit le meilleur 95e
Stdev	L'écart type pour le fournisseur.
Best Stdev	Le meilleur écart type parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures Stdev	Nombre total de mesures ayant produit le meilleur std.dev.
Disponibilité	La disponibilité en pourcentage pour le fournisseur. La disponibilité est le taux de réussite de la sonde, c'est-à-dire Succès/(Succès + Échecs + Délais d'expiration)
Meilleure disponibilité	La meilleure valeur de disponibilité parmi les 15 meilleurs fournisseurs du groupe de pairs.
Meilleures mesures de disponibilité	Le nombre de mesures ayant produit la meilleure disponibilité.
Importance	Valeurs synthétiques générées pour aider à trouver des données exploitables.

Description des journaux de synchronisation de navigation

Données de synchronisation de navigation

Les données de synchronisation de la navigation fournissent des informations sur les différentes parties du processus de chargement de la page pour une page Web.

Ces données varient en fonction de la localisation de l'utilisateur final, des problèmes de réseau, des modifications apportées par le fournisseur, etc. Les clients peuvent utiliser les données de synchronisation de navigation pour optimiser l'expérience de l'utilisateur final lors du chargement de la page Web surveillée.

Des mesures peuvent être prises pour chaque session Radar (si elle est activée). Chaque session est associée à un numéro d'identification qui permet de suivre toutes les mesures d'une session. Ces mesures sont partagées avec les clients sous forme de journaux de synchronisation de navigation via NEM.

Voici un exemple de données de synchronisation de navigation au format de fichier TSV.

Vous trouverez ci-dessous les en-têtes de colonnes et les descriptions des journaux de synchronisation de navigation. Les champs apparaissent dans l'ordre suivant dans les fichiers de sortie :

Journal	Description
Timestamp	Il s'agit de l'heure UTC de la requête au format YYYY-MM-DDTHH:MI:SSZ. La valeur réelle (à la seconde près) dans les tables de journaux est arrondie à l'heure (2018-03-30T 23:00:00 Z) ou au jour (2018-03-30T 00:00:00 Z) le plus proche dans les tables heure/jour, respectivement. Il est toujours en UTC dans tous les ensembles de données.
Code de réponse	Résultat de la mesure.e.g.0 : réussite, 1 : délai d' attente, 4 : erreur. Pour les calculs de disponibilité, le pourcentage de mesures est pris avec une réponse 0 (succès) par rapport au nombre total de mesures (total). Pour les autres types de sonde (RTT et débit), le filtre doit uniquement prendre en compte les points de données RTT avec un code de réussite 0 lors du calcul des statistiques sur le RTT. Idem pour le débit.

Journal	Description
Marché des résolveurs	Le marché du résolveur DNS qui a traité la demande. Généralement le continent où se trouve le résolveur DNS, où, 0 : Inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).
Pays de résolution	Le pays du résolveur DNS qui a traité la Request. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région de résolution	La région du résolveur DNS qui a traité la requête.IDs peut être mappée aux noms sur https://community-radar.citrix.com/ref/regions.json.gz. Tous les pays du monde n'ont pas de régions définies.
État de résolution	L'état du résolveur DNS qui a traité la requête.ID peut être mappé aux noms sur https://community-radar.citrix.com/ref/states.json.gz. Tous les pays du monde n'ont pas d'États définis.
ASN de résolution	Numéro de système autonome (NSA) de la résolution DNS qui a traité la demande. Généralement, l'ASN qui possède le résolveur DNS. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/asns.json.gz
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
Marché client	Le marché de l'utilisateur final qui a généré cette mesure. Généralement le continent où se trouve l'adresse IP du client ; où, 0 : inconnu (XX), 1:Amérique du Nord (NA) 5 : Afrique (AF), 3 : Europe (UE), 4 : Asie (AS), 2 : Océanie (OC), 6 : Amérique du Sud (SA).

Journal	Description
Pays client	Le pays de l'utilisateur final qui a généré cette mesure. Les identifiants peuvent être mappés avec des noms sur https://community-radar.citrix.com/ref/countries.json.gz
Région cliente	Région de l'utilisateur final qui a généré cette mesure. Généralement la région géographique dans laquelle se trouve l'adresse IP du client. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/regions.json.gz. Tous les pays du monde n'ont pas de régions définies.
État du client	État de l'utilisateur final qui a généré cette mesure. En général, l'état dans lequel se trouve l'adresse IP du client. Les ID peuvent être mappés aux noms sur https://community-radar.citrix.com/ref/states.json.gz. Tous les pays du monde n'ont pas d'États définis.
ASN client	Numéro de système autonome (ASN) de l'utilisateur final qui a généré cette mesure. Généralement, l'ASN qui possède l'adresse IP du client. Les ID peuvent être mappés à des noms sur https://community-radar.citrix.com/ref/asns.json.gz
IP du client	L'adresse IP de l'utilisateur final qui a généré la mesure.
Hôte référent	Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar.
Protocole Referer	Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar.
Chemin du référent	Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar.

Journal	Description
Catégorie d'appareils	Tous les appareils sont classés dans l'une des catégories suivantes : smartphone, tablette, PC, Smart TV et autres. « Autre » est utilisé comme valeur par défaut si l'analyseur n'est pas en mesure de déterminer la valeur de l'un des champs.
Appareil	Type d'appareil sur lequel se trouve l'utilisateur, par exemple un iPhone Apple. La chaîne de l' agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
Navigateur	Type de navigateur utilisé par l'utilisateur, par exemple Mobile Safari UI/WKWebView 0.0.0. La chaîne de l'agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
OS	Système d'exploitation utilisé, par exemple iOS 11.0.3. La chaîne de l'agent utilisateur le détecte dans le navigateur qui s'exécute sur la page hébergeant la balise Radar.
Heure de recherche DNS	Avec l'API Resource Timing, la différence entre la fin de la recherche de domaine et le début de la recherche de domaine est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : DomainLookupEnd - DomainLookupStart.
Temps de connexion TCP	Avec l'API Resource Timing, la différence entre la fin de la connexion et le début de la connexion est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - ConnectStart.

Journal	Description
Temps de connexion sécurisée	Avec l'API Resource Timing, la différence entre la fin de connexion et le démarrage de la connexion sécurisée est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme suit : ConnectEnd - SecureConnectionStart.
Charger l'événement	Il s'agit de la durée ou du temps écoulé entre le début et la fin de l'événement de chargement. Il est calculé comme LoadEventEnd - LoadEventStart, lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.
Rediriger	Il s'agit de la durée ou du temps nécessaire pour passer du début de la navigation au début de la récupération. Elle est calculée comme suit : FetchStart - NavigationStart, lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.
Chargement total de la page	Il s'agit de la durée ou du temps écoulé entre le début de la navigation et la fin de l'événement de chargement de page. Il est calculé comme suit : - Fin de l'événement de chargement - Début de la navigation lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.
DOM	La durée ou le temps nécessaire pour passer du chargement DOM au DOM est terminée. Il est calculé comme DOMComplete - DOMLoading lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.
Latence	Avec l'API Resource Timing, la différence entre Response Start et Request Start est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de début de la réponse est supérieure à l'heure de début de la demande. Il est calculé comme ResponseStart - RequestStart

Journal	Description
Heure de téléchargement	Avec l'API Resource Timing, la différence entre la fin de la réponse et le début de la réponse est calculée. Il calcule quand les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début. Il est calculé comme ResponseEnd - ResponseStart.
DOM interactif	Durée ou temps nécessaire pour passer de Navigation Start à DOM Interactive. Il est calculé comme DOMInteractive - NavigationStart lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.
Démarrer le rendu	Durée ou temps nécessaire pour passer de Navigation Start à Start Render. Il est calculé comme StartRender - NavigationStart lorsque les deux valeurs ne sont pas nulles et que l'heure de fin est supérieure à l'heure de début.

Journaux Openmix et HTTP Openmix

Les journaux Openmix et HTTP Openmix permettent aux clients d'utiliser des mesures en temps réel pour surveiller le comportement de leurs applications Openmix. Ils peuvent utiliser ces données pour trouver des domaines d'amélioration ou pour vérifier les performances attendues de leurs applications.

- Ces journaux fournissent des mesures en temps réel pour les clients Openmix.
- Le format de fichier recommandé pour ces journaux est JSON, mais ils sont également disponibles au format TSV.
- Voici des exemples de données de partage de journaux Openmixet HTTP Openmix au format de fichier TSV.

Description du journal OpenMix

Journal	Description
Timestamp	Il s'agit de l'heure UTC de la requête au format YYYY-MM-DDTHH:MI:SSZ. La valeur réelle (à la seconde près) dans les tables de journaux est arrondie à l'heure (2018-03-30T 23:00:00 Z) ou au jour (2018-03-30T 00:00:00 Z) le plus proche dans les tables heure/jour, respectivement. L' horodatage est toujours en UTC dans tous les jeux de données.
ID de zone du propriétaire de l'application	ID de zone du propriétaire de l'application qui traite la demande. Cette valeur est toujours égale à 1.
ID client du propriétaire de l'application	L'ID client du propriétaire de l'application qui répond à la demande. Pour les requêtes HTTP, codez cet ID dans le chemin de la requête et utilisez-le pour rechercher l'application à exécuter.
ID de l'application	L'ID de l'application dans le compte du client qui répond à la demande. Cet ID est également codé dans le chemin de la requête HTTP. Les ID d'application commencent à 1 et sont uniques au client. Vous devez pleinement qualifier les requêtes pour un ID d'application spécifique en interrogeant l'AppOwnerCustomerID.
Version de l'application	Version de l'application qui a géré le compte. Chaque fois qu'une application est mise à jour via le portail ou l'API, la version est incrémentée. La version en cours d'exécution au moment de la demande est enregistrée. Ces informations peuvent être utilisées pour séparer la logique versionnée au fil du temps lorsque les applications sont mises à jour. Les hôtes du réseau reçoivent généralement des mises à jour dans des délais similaires, mais presque jamais exactement au même moment. Il est probable que des décisions qui se chevauchent dans le temps utilisent différentes versions d'une application au cours du processus de mise à jour.

Journal	Description
Nom de l'application	Le nom de l'application qui a géré le compte.
Marchés	Le marché de l'utilisateur final qui a généré cette mesure.
Pays	Le pays de l'utilisateur final qui a généré cette mesure.
Région	Région de l'utilisateur final qui a généré cette mesure.
État	État de l'utilisateur final qui a généré cette mesure.
ID ASN	Numéro de système autonome (ASN) de l' utilisateur final qui a généré cette mesure. Généralement, le numéro de système autonome qui possède l'adresse IP du client.
Nom de l'ASN	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
IP efficace	L'IP effective est l'IP utilisée pour traiter la demande. Il s'agit de l'adresse IP spécifiée par la chaîne de requête qui remplace l'adresse IP de la demande (par rapport à l'ID Resolver/ECS/EDNS pour le flux DNS). C'est l'adresse que le système considère comme la cible lors du traitement des informations. Cette adresse IP est soit l'adresse IP du résolveur demandeur, soit l'adresse IP ECS du client si EDNS ECS est pris en charge. Donc, toutes les données de performance de la sonde, les informations géographiques, etc.passées à la logique de l'application est basée sur cette IP.
Marché des résolveurs	Le marché du résolveur DNS qui a traité la demande.
Pays de résolution	Pays du résolveur DNS qui a traité la demande.
Région de résolution	Région du résolveur DNS qui a traité la demande.
État de résolution	État du résolveur DNS qui a traité la demande.
ID ASN du résolveur	Numéro de système autonome (NSA) de la résolution DNS qui a traité la demande. Généralement le numéro de système autonome qui possède le résolveur DNS.

Journal	Description
Nom de l'ASN du résolveur	Le nom de l'ASN du résolveur qui a traité la demande.
IP de la résolution	Adresse IP du résolveur DNS à partir duquel notre infrastructure a reçu la demande DNS.
Nom du fournisseur de décision	Alias de la plateforme sélectionnée par une application.
Code motif	Code de motif défini dans l'application décrivant la raison de la décision.
Journal des motifs	Ce journal est une sortie définie par le client depuis l'application Openmix. Il s'agit d'un champ de chaîne facultatif qui permet aux clients de consigner des informations sur leurs décisions relatives à l'application Openmix.
Mode de secours	Ce mode indique si l'application était en mode de secours lorsqu'elle a traité la demande. Le repli se produit lorsque quelque chose a échoué pendant la préparation de la demande d'exécution.
EDNS d'occasion	Cette propriété a la valeur True si l'application utilise une extension de sous-réseau client EDNS.
TTL	Le TTL (Time To Live) qui a été rendu.
Réponse	Le CNAME renvoyé par la demande.
Résultat	La valeur de ce champ est toujours 1.
Contexte	Il s'agit du résumé des données Radar qui étaient disponibles pour Openmix lorsque la requête a été traitée. Openmix résout les données Radar par rapport aux valeurs effectives pour chaque requête, de sorte que deux clients qui font des demandes en même temps peuvent avoir des chaînes de contexte différentes.

Description du journal de l'API HTTP Openmix

Journal	Description
Timestamp	Il s'agit de l'heure UTC de la requête au format YYYY-MM-DDTHH:MI:SSZ. La valeur réelle (à la seconde près) dans les tables de journaux est arrondie à l'heure (2018-03-30T 23:00:00 Z) ou au jour (2018-03-30T 00:00:00 Z) le plus proche dans les tables heure/jour, respectivement. L' horodatage est toujours en UTC dans tous les jeux de données.
ID de zone du propriétaire de l'application	ID de zone du propriétaire de l'application qui traite la demande. Cette valeur est toujours égale à 1.
ID client du propriétaire de l'application	L'ID client du propriétaire de l'application qui répond à la demande. Pour les requêtes HTTP, codez cet ID dans le chemin de la requête et il est utilisé pour rechercher l'application à exécuter.
ID de l'application	L'identifiant de l'application dans le compte du client qui répond à la demande. Cet ID est également codé dans le chemin de la requête HTTP. Les ID d'application commencent à 1 et sont uniques au client. Vous devez pleinement qualifier les requêtes pour un ID d'application spécifique en interrogeant l' AppOwnerCustomerID.
Version de l'application	Version de l'application qui a géré le compte. Chaque fois qu'une application est mise à jour via le portail ou l'API, la version est incrémentée. La version en cours d'exécution au moment de la demande est enregistrée. Ces informations peuvent être utilisées pour séparer la logique versionnée au fil du temps lorsque les applications sont mises à jour. Les hôtes du réseau reçoivent généralement des mises à jour dans des délais similaires, mais presque jamais exactement au même moment. Il est probable que des décisions qui se chevauchent dans le temps utilisent différentes versions d'une application au cours du processus de mise à jour.

Journal	Description
Nom de l'application	Le nom de l'application qui a géré le compte.
Marchés	Le marché de l'utilisateur final qui a généré cette mesure.
Pays	Le pays de l'utilisateur final qui a généré cette mesure.
Région	Région de l'utilisateur final qui a généré cette mesure.
État	État de l'utilisateur final qui a généré cette mesure.
ID ASN	L'ID du numéro de système autonome (ASN) de l'utilisateur final qui a généré cette mesure, c'est-à-dire le numéro d'identification réseau associé au nom ASN
Nom de l'ASN	Nom de l'ASN de l'utilisateur final qui a généré la mesure.
IP efficace	L'IP effective est l'IP utilisée pour traiter la demande. Il s'agit de l'adresse IP spécifiée par la chaîne de requête qui remplace l'adresse IP de la demande (par rapport à l'ID Resolver/ECS/EDNS pour le flux DNS). C'est l'adresse que le système considère comme la cible lors du traitement des informations. Cette adresse IP est soit l'adresse IP du résolveur demandeur, soit l'adresse IP ECS du client si EDNS ECS est pris en charge. Toutes les données de performance de sonde, les informations géographiques, etc., transmises à la logique de l'application sont basées sur cette adresse IP.
Nom du fournisseur de décision	Alias de la plateforme sélectionnée par une application.
Code motif	Code de motif défini dans l'application décrivant la raison de la décision.
Journal des motifs	Ce journal est une sortie définie par le client depuis l'application Openmix. Il s'agit d'un champ de chaîne facultatif qui permet aux clients de consigner des informations sur leurs décisions relatives à l'application Openmix.

Journal	Description
Mode de secours	Ce mode indique si l'application était en mode de secours lorsqu'elle a traité la demande. Le repli se produit lorsque quelque chose a échoué pendant la préparation de la demande d'exécution.
Code de réponse	Résultat de la mesure.e.g.0 : réussite, 1 : délai d'attente, 4 : erreur. Pour les calculs de disponibilité, le pourcentage de mesures est pris avec une réponse 0 (succès) par rapport au nombre total de mesures (total, quelle que soit la réponse). Pour les autres types de sonde (RTT et débit), le filtre doit uniquement prendre en compte les points de données RTT avec un code de réussite 0 lors du calcul des statistiques sur le RTT. Idem pour le débit.
Méthode HTTP	La méthode HTTP (Get/Post/Options/etc) concerne la demande qui a été faite au serveur HTTP Openmix par un service client. Ensemble, ces méthodes constituent des parties de l'URL entrante et des réponses HTTP sortantes.
URI	C'est le chemin de la requête. Si les clients n'obtiennent pas le comportement qu'ils souhaitent, cela peut être dû à une demande mal structurée. Les journaux indiquent ce que nos serveurs reçoivent (protocole, hôte et chemin). Les informations du référent (protocole, hôte et chemin) proviennent de l'en-tête du référent de la requête HTTP vers Radar. Pour HTTP OPX, l'intégralité du Referer (protocole, hôte et chemin) est incluse dans une chaîne intitulée Referer.

Journal	Description
User Agent	Il s'agit de la chaîne de l'agent utilisateur de la page du navigateur qui héberge la balise. Par exemple, si vous utilisez Chrome et que vous parcourez une page contenant la balise Radar, les mesures radar en arrière-plan enregistrent l'agent utilisateur à partir de votre navigateur Chrome. Les mesures incluent le navigateur Chrome, la version de Chrome, des informations sur le système d'exploitation sur lequel Chrome est exécuté, etc.
Contexte	Il s'agit du résumé des données Radar qui étaient disponibles pour Openmix lorsque la requête a été traitée. Openmix résout les données Radar par rapport aux valeurs effectives pour chaque requête, de sorte que deux clients qui font des demandes en même temps peuvent avoir des chaînes de contexte différentes.

Rapports personnalisés pour les organisations tierces

Les clients peuvent travailler avec NetScaler pour obtenir des rapports personnalisés basés sur les données Radar collectées par NetScaler. NetScaler peut générer des rapports à exécuter selon un calendrier. Les rapports sont disponibles sous forme de fichiers de données, généralement au format TSV.

Questions fréquentes

Radar

À quelle fréquence les fichiers sont-ils transférés vers S3 et GCS ? La fréquence des dépôts de fichiers est d'une fois par minute pour Radar et quotidienne pour les rapports.

Où sont stockés les rapports ? S3 Legacy (emplacement 1) :

```
s3://public-radar/[customer name]/
```

S3 (emplacement 2) :

`s3://cedexis-netscope/[customer id]/`

GCS (Emplacement 3) :

`gs://cedexis-netscope-[customer id]/`

Comment obtenir des informations d'identification d'accès S3 si vous ne les avez pas déjà ? Le portail fournit une clé « Accès » et une clé « Secret ». Utilisez les touches avec « s3cmd », « awscli » ou d'autres outils pour accéder à S3. Pour Google Storage, le portail télécharge un fichier contenant des informations d'identification à utiliser avec l'outil « gsutil ».

Comment utiliser les clés d'accès et secrètes avec s3cmd pour télécharger des journaux et des rapports à partir du compartiment S3 ? Vous devez d'abord télécharger et installer `s3cmd` depuis https://s3tools.org/download, et vous reporter à https://s3tools.org/usage pour l'utilisation, les options et les commandes. Exécutez ensuite la commande suivante :

```
s3cmd --access_key=[access key] --secret_key=[secret key] ls s3://
    cedexis-netscope/<customer id>/radar/
<!--NeedCopy-->
```

Pour télécharger les fichiers, exécutez la commande suivante :

```
s3cmd --access_key=[access_key] --secret_key=[secret_key] get s3://
    cedexis-netscope/<customer id>/radar/[the_filename_to_download] [
    the_name_of_the_local_file]
<!--NeedCopy-->
```

Comment utiliser la configuration s3cmd pour répertorier les fichiers dans le compartiment S3
La première étape consiste à installer `s3cmd`. Vous pouvez l'installer depuis http://s3tools.org/download

Pour configurer s3cmd, exécutez la commande suivante

```
s3cmd ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```

Si vous utilisez`s3cmd` déjà un autre jeu de clés d'accès et de clés secrètes, procédez comme suit :

Si vous l'utilisez déjà `s3cmd`, faites une copie de la configuration par défaut, à l'adresse `~/.s3cfg`. Par exemple, faites une copie et nommez-la comme `~/.s3cfg_netscope`. Remplacez les entrées de clé d'accès et de clé secrète `~/.s3cfg_netscope` par celles que nous fournissons.
Utilisez la nouvelle configuration au lieu de celle par défaut (celle de votre entreprise) pour accéder au compartiment S3 avec la commande suivante :

```
s3cmd -c ~/.s3cfg_netscope ls s3://cedexis-netscope/[customer id]/
<!--NeedCopy-->
```


La principale différence est que vous devez mettre dans un `-c` et où le fichier de configuration est avec l'accès fourni par Citrix et les clés secrètes.

Si vous souhaitez basculer entre les jeux de clés, intégrez-les dans un fichier. Reportez-vous au fichier avec l'option `-c` pour spécifier la paire de clés que vous utilisez.

> **REMARQUE :** `-c` le paramètre indique où se trouve le fichier de configuration, qui contient les clés d'accès et secrètes.

Comment utiliser le fichier clé avec gsutil ou gcloud pour télécharger des fichiers journaux
Une fois que vous avez téléchargé le fichier de clé JSON du compte de service Google, vous pouvez l'utiliser pour authentifier les informations d'identification de votre compte Google, afficher ou télécharger vos fichiers journaux. Par exemple, voici un moyen de le faire à l'aide de Google `gcloud` et des utilitaires de ligne de `gsutil` commande :

Étape 1 : Activer le fichier de clé

Les commandes d'authentification `gcloud auth activate-` ou `gsutil config -e` sont nécessaires pour authentifier le fichier clé pour l'exécution des commandes gcloud ou gsutil.

Pour gcloud :

Exécutez la commande suivante à l'aide du fichier clé téléchargé :

```
gcloud auth activate-service-account --key-file [downloaded config file
    ]
<!--NeedCopy-->
```

Ou

```
gcloud auth activate-service-account --key-file=[path and file name of
    key file]
<!--NeedCopy-->
```

Pour gsutil :

Exécutez la commande suivante à l'aide du fichier de configuration téléchargé :

```
gsutil config -e
<!--NeedCopy-->
```

Étape 2 : Liste des fichiers dans le compartiment GCS (Google Cloud Storage)

Une fois que vous avez activé le fichier clé du compte de service comme décrit à l'étape précédente, utilisez la commande suivante pour répertorier les fichiers dans le compartiment GCS :

```
gsutil ls gs://cedexis-netscope-<customer id>
<!--NeedCopy-->
```


Étape 3 (si nécessaire) : Restaurer les informations d'identification d'origine (ou basculer d'un compte à l'autre)

Vous pouvez passer du compte NetScaler ITM aux autres informations d'identification Google Cloud que vous avez authentifiées en procédant comme suit.

Exécutez d'abord la commande suivante pour répertorier tous vos comptes :

```
gcloud auth list
<!--NeedCopy-->
```

Utilisez ensuite la commande suivante pour passer à un autre compte :

```
gcloud config set account [email of the account to switch to as shown
    in gcloud auth list]
<!--NeedCopy-->
```

Vous pouvez passer d'un compte à l'autre à l'aide de la même commande, en remplaçant l'e-mail par l'adresse e-mail du compte vers laquelle vous souhaitez basculer.

À quoi ressemble le nom du fichier ? Héritage Quotidien :

Les noms ShareFile du journal journalier Radar ont la structure suivante :

`<prefix><date: YYYY-MM-DD>.<customer_id>.part<uniq_id>.kr.txt.gz`

Par exemple`Cedexis_Daily-2017-11-07.21222.part-cc901e1dd55eal4e.kr.txt.gz` (exemple non standard)

Legacy en temps réel :

Les noms ShareFile du journal en temps réel Radar ont la structure suivante :

`<prefix><customer_id>-YYYY-MM-DDTHH:MM<uniq_id>.txt.gz`

Par exemple `Cedexis_3-32291-2017-11-08T20:56-cc907e8fd71eaf4e.txt.gz`

Format NEM Netscope :

Le format Netscope NEM pour les fichiers de partage de journaux quotidiens et en temps réel a la structure suivante :

`<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.gz`

Où,

- `freq: "daily"| "rt"| "hr"`
- `log_type: "radar"| "opx"| "hopx"`
- `prefix: log_share.prefix`
- `id_type: "customer"| "provider"| "asn"`

- `id`: `log_share.match_id`
- `iso_dt`: `iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id`: `hash(UUID)`
- `line_format`: `"tsv"| "json"`

Par exemple `rt-radar-TestRadar1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

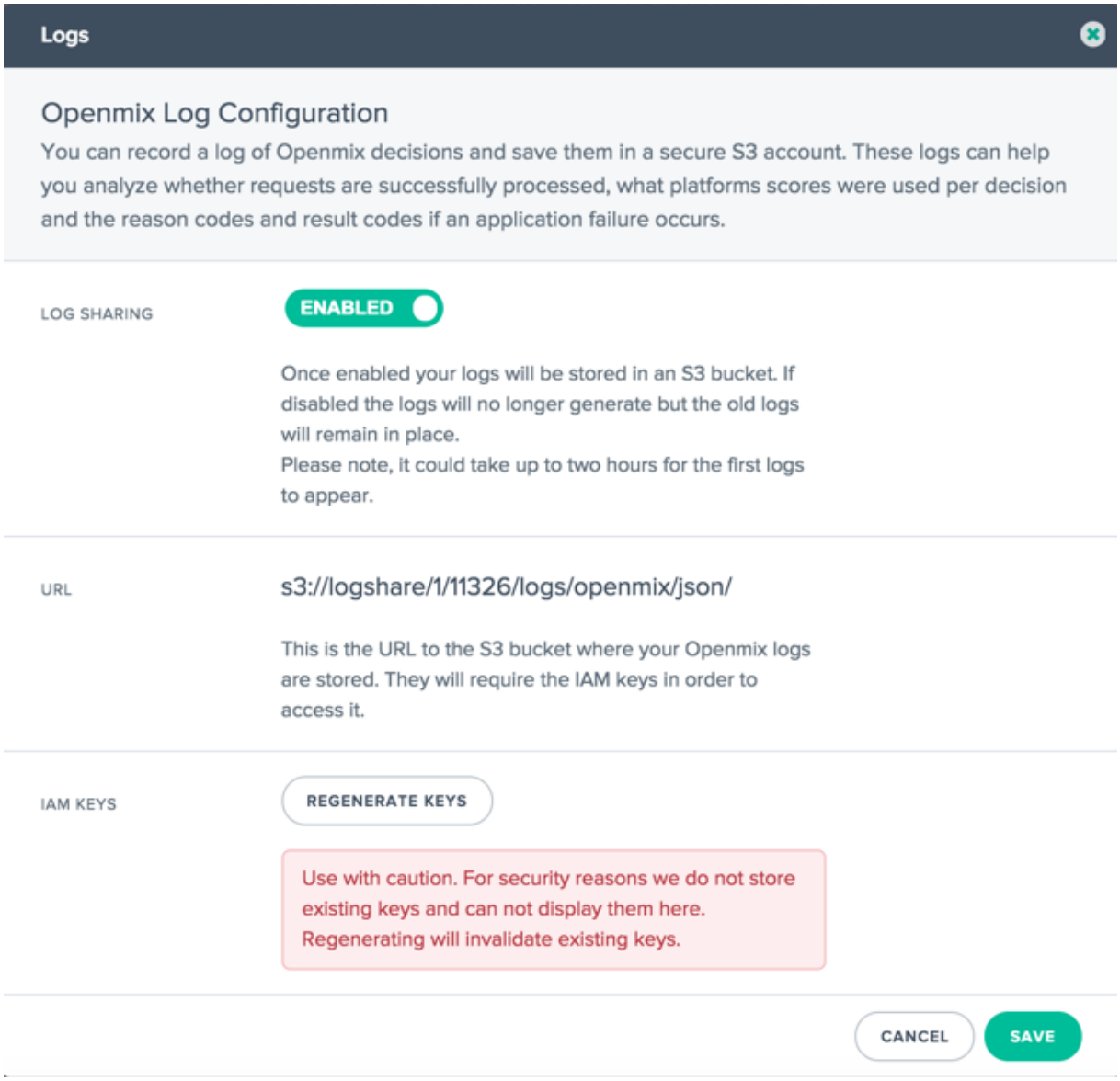
Quel est le format du fichier de sortie ? Pour Radar, le format de fichier de sortie est TSV (valeur séparée par des tabulations), gzippé.

API HTTP Openmix et Openmix

À quelle fréquence les fichiers sont-ils transférés vers S3 ? La fréquence des dépôts de fichiers est une fois par minute pour Openmix et HTTP Openmix.

Que se passe-t-il si vous ne voyez pas l'option permettant de configurer le partage de journaux en temps réel Openmix et Openmix HTTP API ? Votre responsable de compte peut activer le rôle requis pour configurer et activer le partage de journaux en temps réel Openmix et Openmix HTTP API.

Comment activer Openmix et une API HTTP Openmix pour partager des journaux en temps réel et accéder aux fichiers ? Une fois que le rôle est activé sur votre compte, l'icône **Gérer les journaux** s'affiche. Cliquez pour ouvrir la boîte de dialogue **Logs** dans laquelle vous pouvez accéder aux paramètres de configuration des journaux Openmix. Ces paramètres sont essentiellement tout ce dont vous avez besoin pour activer le partage de journaux en temps réel Openmix et HTTP Openmix et accéder aux fichiers.



Qu'est-ce que le processus back-end ? L'activation du partage des journaux Openmix permet également le partage des journaux de l'API HTTP Openmix. Les services de partage de journaux de l'API HTTP Openmix et Openmix doivent commencer à générer des journaux pour le client dans les 10 minutes.

Où sont stockés les rapports Openmix et HTTP Openmix ? S3 Legacy (emplacement 1) :

```
s3://logshare/[zone ID]/[customer ID]/logs/openmix/json/[YYYY]/[MM]/[DD]/[HH]/.
```

S3 (emplacement 2) :

```
s3://cedexis-netscope/[customer id]/
```


GCS (Emplacement 3) :

```
gs://cedexis-netscope-[customer id]/
```

À quoi ressemble le nom du fichier ? La structure des noms de fichiers pour Openmix et HTTP Openmix ressemble généralement à ceci :

Legacy en temps réel :

```
[zone ID, 1][customerID]-openmix-json[YYYY][MM][DD][HH][mm][ss]Z-m1-
w9-c0.gz
```

Format NEM Netscope :

Le format Netscope NEM pour les fichiers de partage de journaux quotidiens et en temps réel a la structure suivante :

```
<freq><log_type><prefix><id_type><id><iso_dt><uniq_id>.<line_format>.
gz
```

Où,

- `freq`: `"daily"| "rt"| "hr"`
- `log_type`: `"radar"| "opx"| "hopx"`
- `prefix`: `log_share.prefix`
- `id_type`: `"customer"| "provider"| "asn"`
- `idv`: `log_share.match_id`
- `iso_dt`: `iso 8601 Date_time "YYYYMMDDTHHMMSSZ"`
- `uniq_id`: `hash(UUID)`
- `line_format`: `"tsv"| "json"`

Par exemple `hr-opx-TestOpenmix1-provider-20363-20171209183034Z-cc907e8fd71eaf4e.tsv.gz`

Quel est le format de fichier de sortie ? Le format de fichier pour Openmix et une API HTTP Openmix est JSON (gzippé).

Administration

September 13, 2023

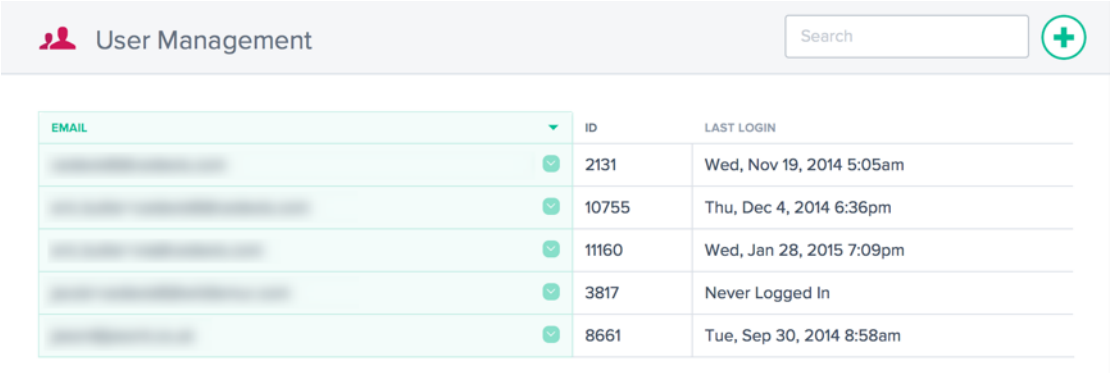
La section **Mon compte** permet à l'utilisateur final d'administrer le compte, aux utilisateurs qui peuvent accéder au compte et aux utilisateurs qui peuvent accéder aux fonctionnalités de purge de Fusion.

En outre, dans le menu, vous pouvez consulter les factures échues et gérer les informations d'identification de l'API OAuth.

Gérer les utilisateurs

Dans le menu Utilisateurs, vous pouvez ajouter/supprimer des utilisateurs et réinitialiser l'accès au compte par mot de passe.

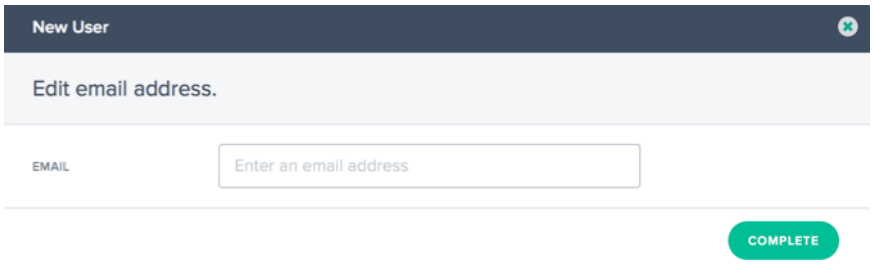
Outre la gestion des utilisateurs, vous pouvez saisir des adresses e-mail pour les notifications de service et voir quand un utilisateur s'est connecté pour la dernière fois.



Ajouter ou supprimer des utilisateurs et réinitialiser les mots de passe

Lorsque vous créez ou ajoutez des utilisateurs, assurez-vous d'utiliser une adresse e-mail valide. Les mots de passe sont créés automatiquement et envoyés par e-mail à l'adresse e-mail saisie comme nom d'utilisateur.

Pour ajouter un nouvel utilisateur, cliquez sur le **signe +** dans le coin supérieur droit. Entrez une adresse e-mail valide et cliquez sur **Terminer**.



Pour réinitialiser le mot de passe d'un utilisateur, cliquez sur la flèche vers le bas à droite de l'adresse e-mail de l'utilisateur, choisissez **Réinitialiser le mot de passe**et confirmez l'action dans la boîte de dialogue en cliquant sur **Oui**. Un e-mail de réinitialisation du mot de passe est envoyé à l'utilisateur.

Un utilisateur peut être supprimé du système en cliquant sur la flèche vers le bas à droite de son adresse e-mail et en choisissant **Supprimer**. Confirmez l'action et l'utilisateur sera supprimé du système.

Authentification unique

Nous prenons en charge le recours à des fournisseurs d'identité tiers pour la connexion unique au portail via SAML 2.0.

L'authentification unique est utilisée pour authentifier les connexions des utilisateurs. Nous ne transmettons actuellement aucune information d'autorisation via le SSO SAML. Pour pouvoir se connecter, un utilisateur doit exister sur le portail NetScaler Intelligent Traffic Management avec la même adresse e-mail qu'un utilisateur du fournisseur d'identité SSO.

L'authentification unique est gérée par compte. Une fois le SSO activé pour un compte, tous les utilisateurs doivent utiliser un identifiant SSO pour accéder au portail.

Les informations de configuration SAML se trouvent dans l'élément de menu **Configuration SSO** . Les informations sont spécifiques à votre compte et vous permettent de configurer le SSO dans votre fournisseur d'identité. Si vous ne trouvez pas le menu de **configuration SSO**, contactez l'équipe d' assistance .

La configuration est différente pour chaque fournisseur d'identité, mais vous avez besoin des informations suivantes, qui sont affichées sur la page de configuration SSO :

- URL du service Assertion Consumer (ACS)
- ID de l\'entité
- URL de déconnexion (facultatif, selon le fournisseur)
- URL de démarrage (facultatif, selon le fournisseur)
- Format du nom : e-mail
- Réponse signée : Non

Activer l'authentification unique

Étapes génériques pour ajouter l'authentification unique au portail de gestion intelligente du trafic NetScaler :

1. À l'aide des données de l'écran de configuration SSO, configurez le fournisseur d'identité
2. Téléchargez le fichier de métadonnées SSO IDP auprès du fournisseur d'identité
3. Téléchargez le fichier sur la page de configuration SSO
4. **Lorsque vous êtes prêt à activer le SSO, cliquez sur Activer**
5. Les utilisateurs devront désormais se connecter via la page de connexion SSO.

Désactiver l'authentification unique

Si le SSO est configuré et activé, cliquez sur le bouton **Désactiver** .

Tout utilisateur du compte qui souhaite se connecter devra désormais utiliser un mot de passe Citrix sur l'écran de connexion standard. Si un utilisateur ne connaît pas son mot de passe, l'administrateur du compte peut envoyer un e-mail de réinitialisation du mot de passe ou demander un e-mail de réinitialisation du mot de passe depuis l'écran de connexion.

Étapes de configuration pour Google G Suite

Voici les étapes nécessaires pour utiliser l'authentification unique avec les connexions à Google G Suite :

Dans Google G Suite :

1. Ouvrez la console d'administration G Suite dans la section Applications
2. Cliquez sur la catégorie des **applications SAML**
3. Cliquez sur le bouton **Activer l'authentification unique pour une application SAML**
4. Au bas de la boîte de dialogue, choisissez **SETUP MY OWN CUSTOM APP**
5. Dans la boîte de dialogue Google IDP Informations, téléchargez le fichier de métadonnées IDP dans le cadre de l'option 2.
6. Dans les informations de base de votre application personnalisée, le nom de l'application peut être « NetScaler Intelligent Traffic Management »
7. Renseignez les informations suivantes à partir de la configuration SSO dans Portal :
   - URL ACS : à partir des informations de configuration SSO
   - ID d'entité : à partir des informations de configuration SSO
   - URL de démarrage : depuis les informations de configuration SSO (facultatif)
   - Format du nom et de l'identifiant : EMAIL
8. Laissez la boîte de dialogue de mappage d'attributs vide, cliquez sur **TERMINER** pour créer l' application SAML
9. Dans la liste des applications, cliquez sur les points verticaux à droite de l'élément du portail et choisissez **ON pour tout le monde**

Sur le portail :

1. Sur la page de configuration SSO, chargez le fichier de métadonnées IDP ; cliquez sur le bouton **Choisir un fichier** pour ouvrir le navigateur de fichiers et sélectionner le fichier de métadonnées IDP téléchargé depuis G Suite.

2. Si le fichier de métadonnées est correctement validé, une coche verte apparaît.
3. Cliquez sur **Activer** pour activer l'authentification unique pour tous les utilisateurs du compte.

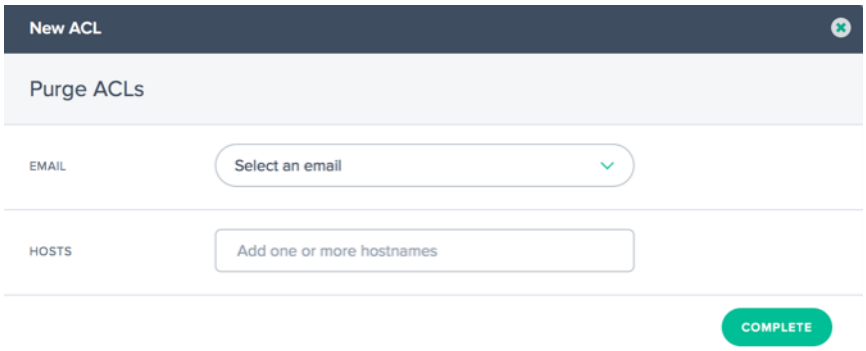
Les utilisateurs peuvent désormais se connecter au portail de gestion intelligente du trafic NetScaler à partir de la page de connexion SSO oudu**menu Applications de G Suite.**

Pour plus d'informations sur le SSO de Google G Suite, consultez l'aidede Google.

Configuration des ACL de purge

Dans le menu **Purger les ACL**, les utilisateurs peuvent avoir des limites quant à leur capacité à exécuter la fonctionnalité Fusion Purge. Par défaut, les utilisateurs peuvent exécuter une purge sur n'importe quel hôte configuré dans les paramètres de **Fusion Purge** . Les ACL de purge sont utilisées pour limiter les utilisateurs afin d'autoriser uniquement une purge sur des hôtes spécifiques.

Ajoutez de nouvelles restrictions pour un utilisateur en cliquant sur le bouton « **+** » dans le coin supérieur droit. La boîte de dialogue suivante s'affiche :



Champ	Description
E-mail	Sélectionnez l'e-mail de l'utilisateur pour lequel vous souhaitez configurer un accès limité à la purge.
Hôtes	Entrez les noms d'hôte que l'utilisateur doit utiliser pour exécuter les purges. Tout nom d'hôte non inclus dans la liste pour l'utilisateur ne pourra pas être purgé par l'utilisateur.

Factures

L'option de menu **Factures** fournit toutes les factures relatives aux services NetScaler Intelligent Traffic Management que vous avez utilisés. En cas de problème avec les factures, contactez votre représentant commercial ou contactez l'équipe d'assistance .

API

Gérer OAuth

L'option du menu **API** fournit des détails sur les jetons d'API OAuth authentifiés que vous souhaiterez peut-être utiliser. Si vous souhaitez utiliser cette fonctionnalité, contactez votre responsable de compte.

Limites de débit de l'API REST

Les API REST peuvent être utilisées pour accéder aux données et aux paramètres stockés sur la plateforme. Cependant, nous limitons le nombre de demandes (pour accéder à ces données) en leur imposant une limite de débit, c'est-à-dire en limitant le nombre d'appels d'API qu'un client peut effectuer au cours d'une période donnée. Ceci est fait pour équilibrer la charge sur le système.

Attributs de limite de taux Les limites de taux présentent les caractéristiques suivantes :

- Plage de temps (en minutes)
- Nombre de demandes autorisées
- Demandes simultanées

Les clients peuvent demander des augmentations de leurs limites tarifaires pour leur cas d'utilisation spécifique.

Limites de taux par défaut Le tableau suivant répertorie les différents types d'appels d'API et les limites de débit par défaut qui s'appliquent à chacun d'entre eux.

Types d'API	Limites de taux par défaut
Points de terminaison des rapports	**GET**

`/v2/reporting/radar.json`
`/v2/reporting/plt.json`
`/v2/reporting/openmix.json`
`/v2/reporting/sonar.json`
	15 demandes par 15 minutes. 3 demandes simultanées

Mise à jour des applications	**METTRE, PUBLIER**
`/v2/config/applications/dns.json`	10 demandes par minute. 3 demandes simultanées
Purge par fusion	**GET**
`/v2/actions/fusion/purge.json`	150 demandes par minute

Types d'API	Limites de taux par défaut
Purge par fusion	**POST**
`/v2/actions/fusion/purge.json`	1 demande par minute. 3 demandes simultanées