Concepts avancés

Machine translated content

Disclaimer

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

Contents

Conception

January 23, 2020

Conception de référence validée Citrix Cloud Native Networking pour Red Hat OpenShift 3.11

La pile Citrix ADC répond aux exigences de base en matière de fonctionnalités de disponibilité des applications (ADC), de ségrégation des fonctionnalités de sécurité (WAF), de mise à l'échelle des topologies d'applications agiles (SSL et GSLB) et d'observabilité proactive (Service Graph) dans un environnement Cloud Native hautement orchestré. Cette conception de référence validée vous guide tout au long du déploiement de Citrix Cloud Native Networking pour Red Hat OpenShift 3.11.

Modèle de conception validé Citrix ADC et Microsoft Azure

Citrix ADC est un contrôleur de mise à disposition d'applications tout-en-un qui permet d'exécuter les applications jusqu'à cinq fois mieux, réduit les coûts de propriété des applications, optimise l'expérience utilisateur et garantit que les applications sont toujours disponibles.

Citrix ADC CPX, Citrix Ingress Controller et Application Delivery Management sur Google Cloud

Modèle de conception validé du clustering Citrix ADC

Un cluster Citrix ADC est un groupe d'appliances Citrix ADC nCore qui travaillent ensemble sous la forme d'une image système unique. Chaque appliance du cluster est appelée nœud. Un cluster Citrix ADC peut inclure aussi peu que 2 ou 32 appliances virtuelles Citrix ADC nCore en tant que nœuds.

Le trafic client est distribué entre les nœuds pour fournir une haute disponibilité, un débit élevé et une évolutivité.

Conception de référence validée de capacité groupée Citrix ADC

La capacité groupée Citrix ADC est une infrastructure de licences qui comprend un pool de bande passante et un pool d'instances virtuelles hébergé sur Citrix Application Delivery Management et desservi par Citrix Application Delivery Management.

Citrix ADC CPX dans Kubernetes avec modèle de conception validé Diamanti et Nirmata

Citrix ADC est un contrôleur de mise à disposition d'applications qui effectue une analyse de trafic spécifique à l'application pour distribuer, optimiser et sécuriser intelligemment le trafic réseau L4-L7 pour les applications Web. Son ensemble de fonctionnalités peut être constitué de fonctionnalités de commutation, de sécurité et de protection, et d'optimisation de la batterie de serveurs.

Modèle de conception validé des profils SSL de Citrix ADC

Utilisez un profil SSL pour spécifier comment un Citrix ADC traite le trafic SSL. Le profil est un ensemble de paramètres SSL pour les entités SSL, telles que les serveurs virtuels, les services et les groupes de services, et offre une configuration facile et une flexibilité. Vous n'êtes pas limité à la configuration d'un seul ensemble de paramètres globaux. Vous pouvez créer plusieurs ensembles (profils) de paramètres globaux et affecter différents ensembles à différentes entités SSL.

Modèle de conception validé Citrix ADC et Amazon Web Services

Citrix Networking VPX est disponible en tant qu'Amazon Machine Image (AMI) sur AWS Marketplace. Citrix Networking VPX on AWS permet aux clients de tirer parti des capacités de cloud computing AWS et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic de Citrix ADC pour leurs besoins professionnels. Citrix ADC sur AWS prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance Citrix ADC physique. Les instances Citrix ADC exécutées dans AWS peuvent être déployées en tant qu'instances autonomes ou en tant que paires HA.

Conception de référence validée des partitions Admin Citrix ADC

NetScaler Admin Partitions permet la multi-location au niveau logiciel dans une seule instance NetScaler. Chaque partition a son propre plan de contrôle et plan réseau. Ce document décrit en détail les cas d'utilisation habituels qui sont activés par les partitions d'administration et les directives relatives à l'utilisation des partitions d'administration dans l'environnement client.

Conception de référence validée par Citrix Gateway SaaS et O365 Cloud

Software as a Service (SaaS) est un modèle de distribution de logiciels permettant de fournir des logiciels à distance en tant que service Web. Applications SaaS couramment utilisées, y compris les abonnements Microsoft Office 365.

Les applications SaaS sont désormais accessibles à l'aide de Citrix Workspace à l'aide du service Citrix Gateway. Le service Citrix Gateway associé à Citrix Workspace offre une expérience utilisateur

unifiée pour les applications SaaS configurées, les applications virtuelles configurées ou toute autre ressource d'espace de travail.

La livraison d'applications SaaS à l'aide du service Citrix Gateway vous offre une solution simple, sécurisée, robuste et évolutive pour gérer les applications.

Conception de référence validée de référence de Citrix Gateway Service avec contrôle d'accès

Grâce au service de contrôle d'accès, les administrateurs peuvent offrir une expérience cohérente qui intègre l'authentification unique, l'accès à distance et l'inspection du contenu dans une solution unique pour le contrôle d'accès de bout en bout. Les administrateurs informatiques peuvent régir l'accès aux applications SaaS approuvées avec une expérience d'authentification unique simplifiée. Grâce au service Contrôle d'accès, les administrateurs peuvent également protéger le réseau et les périphériques des utilisateurs finaux de l'entreprise contre les programmes malveillants et les fuites de données en filtrant l'accès à des sites Web et à des catégories de sites Web spécifiques. Les administrateurs peuvent appliquer des stratégies de sécurité d'accès améliorées pour un accès sécurisé aux applications SaaS. Une fois authentifiés, les employés ont accès à toutes les applications métier critiques à partir de n'importe quel appareil, qu'ils se trouvent au bureau, à la maison ou en voyage.

Conception de référence validée pour haute disponibilité Citrix ADC avec IP frontale Azure Load Balancer

Implémentez un déploiement NetScaler haute disponibilité dans Microsoft Azure en utilisant l'équilibreur de charge Azure (ALB) comme équilibreur de charge frontal (FE).

Conception de référence validée Citrix Cloud Native Networking pour Red Hat OpenShift 3.11

January 8, 2020

La pile Citrix ADC répond aux exigences de base en matière de fonctionnalités de disponibilité des applications (ADC), de ségrégation des fonctionnalités de sécurité (WAF), de mise à l'échelle des topologies d'applications agiles (SSL et GSLB) et d'observabilité proactive (Service Graph) dans un environnement Cloud Native hautement orchestré.

La transformation numérique alimente la nécessité de déplacer les déploiements d'applications modernes vers des architectures basées sur des microservices. Ces architectures Cloud Native utilisent

des plates-formes de calcul modernes telles que des conteneurs d'applications et des clusters informatiques. Certains fournisseurs open source, tels que Docker et Kubernetes, sont des technologies de déploiement courantes pour les applications cloud natives.

La nouvelle ère du déploiement d'applications modernes a également changé les disciplines traditionnelles du modèle commercial des datacenters, notamment les versions mensuelles et annuelles de logiciels et les contrats, les ressources de calcul en silo et le budget, ainsi que le modèle de consommation des fournisseurs.

L'approche Cloud Native des applications modernes a également transformé le cycle de vie du développement, y compris des workflows agiles, des jeux d'outils de déploiement d'automatisation et des langages et plates-formes de développement.

Et bien que toute cette modernisation se produise dans l'écosystème, il existe encore des exigences de base pour les fonctionnalités de disponibilité des applications (ADC), la ségrégation des fonctionnalités de sécurité (WAF), la mise à l'échelle des topologies d'applications agiles (SSL et GSLB) et l'observabilité proactive (Service Graph) en un environnement.

Pourquoi Citrix for Modern Application Delivery

L'approche logicielle Citrix pour le déploiement d'applications modernes nécessite l'intégration d'un flux de travail agile au sein de nombreuses équipes au sein de l'organisation. L'un des avantages du développement et de la livraison d'applications agiles est le framework connu sous le nom de CI/CD.

CI/CD est un moyen de fournir vitesse, sécurité et fiabilité dans le cycle de vie moderne des applications.

L'intégration continue (CI) permet une base de code commune qui peut être mise à jour en temps réel plusieurs fois par jour et s'intégrer dans une plate-forme de construction automatisée.
Les trois phases de l'intégration continue sont Push, Test, Fix.

Continuous Delivery (CD) intègre le pipeline de déploiement directement dans le processus de développement CI, optimisant ainsi et améliorant le modèle de livraison de logiciels pour les applications modernes.

Voici quelques-unes des méthodes Canary prises en charge pour CI/CID :

- Essais A/B
- Bleu/vert (aka rouge/noir) déploiement Canary
- Déploiement progressif de l'analyse Canary automatique
- Tests de singe Chaos

Voici quelques-unes des plates-formes CI/CID prises en charge :

- Jenkins— peut également être utilisé pour CD avec ses plug-ins pipeline en tant que code, Ansible ou Terraforme

- Pipelines Azure—contient une section de définition de version que vous pouvez intégrer à une étape de construction de CI.
- Spinnaker—qui gagne en popularité, et c'est l'outil que Netflix utilise pour faire des versions sur CD.
- CI GitLab—vous permet de configurer les pipelines de déploiement et de libération avec GitLab.
- GoCD—l'offre ThoughtWorks qui applique les principes dont j'ai parlé dans ce post.

Une solution pour toutes les parties prenantes

Citrix a créé une solution logicielle dédiée qui répond aux exigences interfonctionnelles lors du déploiement d'applications modernes et intègre les différents composants de l'infrastructure CI/CD.

Les organisations traditionnelles qui adoptent des techniques CI/CD pour déployer des applications modernes ont reconnu la nécessité de fournir un cadre commun de prestation et de disponibilité à tous les membres qui participent à CI/CD, ces ressources sont généralement définies comme les « intervenants » de l'unité opérationnelle et, bien que chaque intervenant est investi dans le succès global de l'organisation, chaque intervenant a généralement des exigences et des différences distinctes.

Voici quelques exemples courants d'intervenants dans l'activité moderne de prestation de services :

- Équipe plates-formes : déployez une infrastructure de datacenter comme IaaS, PaaS, SDN, ADC, WAF
- DevOps et équipe d'ingénierie : développez et maintenez le référentiel de code unifié, les outils d'automatisation et l'architecture logicielle
- Équipe d'ingénierie de fiabilité des services (SRE) : réduisez les silos organisationnels, la gestion des erreurs, l'automatisation du déploiement et les mesures
- Équipe des opérations de sécurité : stratégies de sécurité proactives, gestion des incidents, déploiement des correctifs, renforcement du portefeuille

Explication de la pile logicielle Citrix

Single Code Base - il est tout le même code pour vous

- Déploiements sur site, déploiements de cloud public, déploiements de cloud privé, déploiements de cloud GOV

Choix de plates-formes : pour répondre à toute exigence agile, choisissez n'importe quel modèle Citrix ADC

- CPX — Citrix ADC CPX est un Citrix ADC livré en tant que conteneur Docker
- VPX : le produit Citrix ADC VPX est une appliance virtuelle qui peut être hébergée sur une grande variété de plateformes de virtualisation et de cloud offrant des performances allant de 10 Mo/s à 100 Gbit/s.

- MPX : le Citrix ADC MPX est un dispositif de livraison d'applications matérielles offrant des performances allant de 500 Mo/s à 200 Gbit/s.
- SDX : l'appliance Citrix ADC SDX est une plate-forme multilocataire sur laquelle vous pouvez provisionner et gérer plusieurs machines Citrix ADC (instances) virtuelles.
- BLX : l'appliance Citrix ADC BLX est un facteur de forme logiciel de Citrix ADC. Il est conçu pour fonctionner en mode natif sur Bare-Metal-Linux sur des serveurs commerciaux (COTS)

Environnements conteneurisés : créez des superpositions et configurez automatiquement votre Citrix ADC

- Contrôleur d'entrée Citrix – construit autour de Kubernetes Ingress et configure automatiquement un ou plusieurs Citrix ADC en fonction de la configuration des ressources Ingress
- Contrôleur de nœud Citrix – crée un réseau de superposition basé sur VXLAN entre les nœuds Kubernetes et le Citrix ADC Ingress
- Contrôleur IPAM Citrix – Affecte automatiquement le serveur virtuel d'équilibrage de charge sur un Citrix ADC avec une adresse IP (adresse IP virtuelle ou VIP)

Licences de capacité groupée — une licence globale

- Un pool de licences mondial omniprésent découple les plates-formes et les licences pour une flexibilité totale de conception et de performance

Application Delivery Manger — la seule vitre de verre

- Gérez la flotte, orchestrez les politiques et les applications, surveillez et dépannez en temps réel

Topologies flexibles — datacenter traditionnel ou clouds modernes

- Un seul niveau, deux niveaux et un maillage de service allégé

La valeur de Citrix ADC

Kubernetes et CNCF Open Source Tools
The Perfect Proxy — un Controller de distribution d'applications Layer7 éprouvé pour les applications modernes

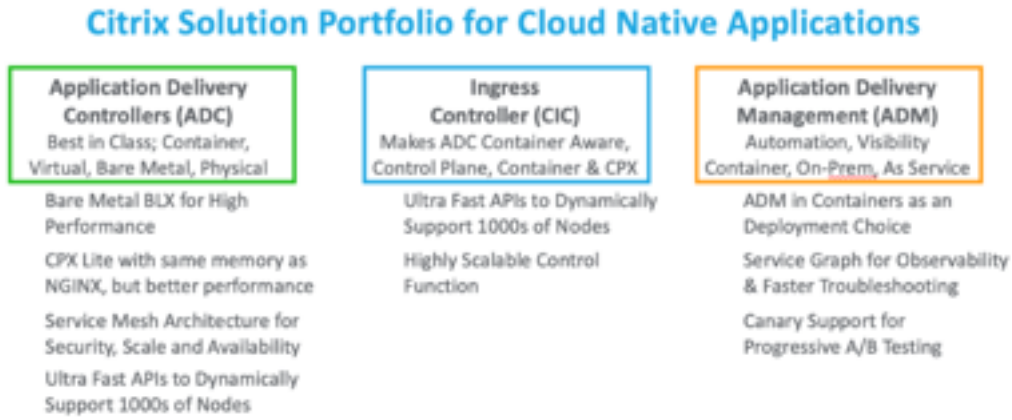
- Conteneur ADC haute performance dans un déploiement Pod ou Sidecar
- Accès à faible latence au cluster Kubernetes à l'aide de plusieurs options

API riche en fonctionnalités : implémentez et orchestrez facilement les fonctionnalités de sécurité sans limite
Advanced Traffic Steering et déploiement Canary pour la surveillance
intégrée CI/CD pour les déploiements d'applications héritées et modernes Insights
exploitables et Graphiques de service pour la visibilité

Avantages de Citrix ADC

- Déplacer les applications héritées sans avoir à les réécrire
- Les développeurs peuvent sécuriser des applications avec des stratégies Citrix ADC à l'aide des API Kubernetes (Utilisation de CRD — conviviale pour les développeurs)
- Déployer des microservices hautes performances pour le réseau Nord-Sud et Service Mesh
- Utiliser un graphique Application Service pour tous les microservices
- Résoudre les problèmes de microservices plus rapidement sur TCP, UDP, HTTP/S, SSL
- Sécurisez les API et configurez à l'aide des API Kubernetes
- Améliorer le processus CICD pour les déploiements Canary

Composants d'architecture



L'avantage de Citrix ADC Suite

Citrix est synonyme de choix. Que vous viviez avec des datacenters et des composants hérités ou que vous ayez lancé une nouvelle application moderne native dans le cloud, Citrix ADC s'intègre parfaitement à toutes les exigences de plateforme que vous pourriez avoir. Nous fournissons des fonctionnalités ADC natives dans le cloud pour les plates-formes et outils cloud basés sur abonnement, nous permettons de diriger et d'orchestration du trafic vers votre cluster Kubernetes sur site grâce à l'orchestration facile du Controller d'entrée, et nous traitons les architectures Service Mesh de simple à complexe.

Citrix est validé. Des modèles de conception validés et des exemples d'applications permettent de répondre rapidement et complètement à un état désiré et à une exigence métier. Nous avons documenté et publié des exemples de configuration dans un emplacement central pour faciliter la consultation entre les équipes DevOps, SecOps et Plateformes.

Citrix est agile et moderne. Créez une architecture de base permettant aux clients d'utiliser les nouvelles fonctionnalités de Citrix Cloud Native Stack avec leurs ADC existants et de nouveaux modules

(CNC, IPAM, etc.)

Citrix est ouvert. Aidez les clients à comprendre notre intégration avec les écosystèmes partenaires. Dans ce document, nous utilisons à la fois les outils OpenSource CNCF et les produits Citrix de qualité entreprise.

Ecosystème partenaire

Cette rubrique fournit des détails sur diverses plates-formes Kubernetes, topologies de déploiement, fonctionnalités et CNI pris en charge dans les déploiements Cloud-Native qui incluent Citrix ADC et Citrix Ingress Controller.

Citrix Ingress Controller est pris en charge sur les plates-formes suivantes :

- Kubernetes v1.10 sur métal nu ou auto-hébergé sur des clouds publics tels que AWS, GCP ou Azure.
- Google Kubernetes Engine (GKE)
- Elastic Kubernetes Service (EKS)
- Azure Kubernetes Service (AKS)
- Red Hat OpenShift version 3.11 et versions ultérieures
- Pivotal Container Service (PKS)
- Plateforme Kubernetes Diamanti Enterprise

Notre écosystème de partenaires comprend également les éléments suivants :

- Prometheus — outil de surveillance des mesures, des alertes et des informations
- Grafana — une plateforme d'analyse et de suivi
- Spinnaker — un outil pour la livraison continue multi-cloud et l' analyse Canary
- Elasticsearch — un service de recherche d'application ou de site
- Kibana — un outil de visualisation pour les données de recherche élastique et un outil de navigation de pile élastique
- Fluentd — un outil de collecte de données

Le thème de cette section suivante est la conception/architecture avec OpenShift.

Présentation d'OpenShift

Red Hat OpenShift est une plate-forme Kubernetes destinée aux déploiements axés sur l'utilisation de microservices et de conteneurs pour créer et mettre à l'échelle des applications plus rapidement. Automatisation, installation, mise à niveau et gestion de la pile de conteneurs, OpenShift rationalise Kubernetes et facilite les tâches quotidiennes de DevOps.

- Les développeurs mettent à disposition des applications l'accès à des solutions validées et à des partenaires qui sont poussés à la production via des flux de travail rationalisés.

- Les opérations peuvent gérer et mettre à l'échelle l'environnement à l'aide de la console Web et de la journalisation et de la surveillance intégrées.

Avantages et composants d'OpenShift supplémentaires :

- Choix de l'infrastructure
- Nœuds maître et travailleur
- Registre d'images
- Couche de routage et de service
- Fonctionnement du développeur (introduit mais dépasse le champ d'application de ce document)

Les cas d'utilisation pour intégrer Red Hat OpenShift à Citrix Native Stack sont les suivants :

- Prise en charge des applications héritées
- Stratégies de réécriture/répondeur déployées en tant qu'API
- Dépannage des microservices
- Opérations quotidiennes avec correctifs de sécurité et améliorations des fonctionnalités

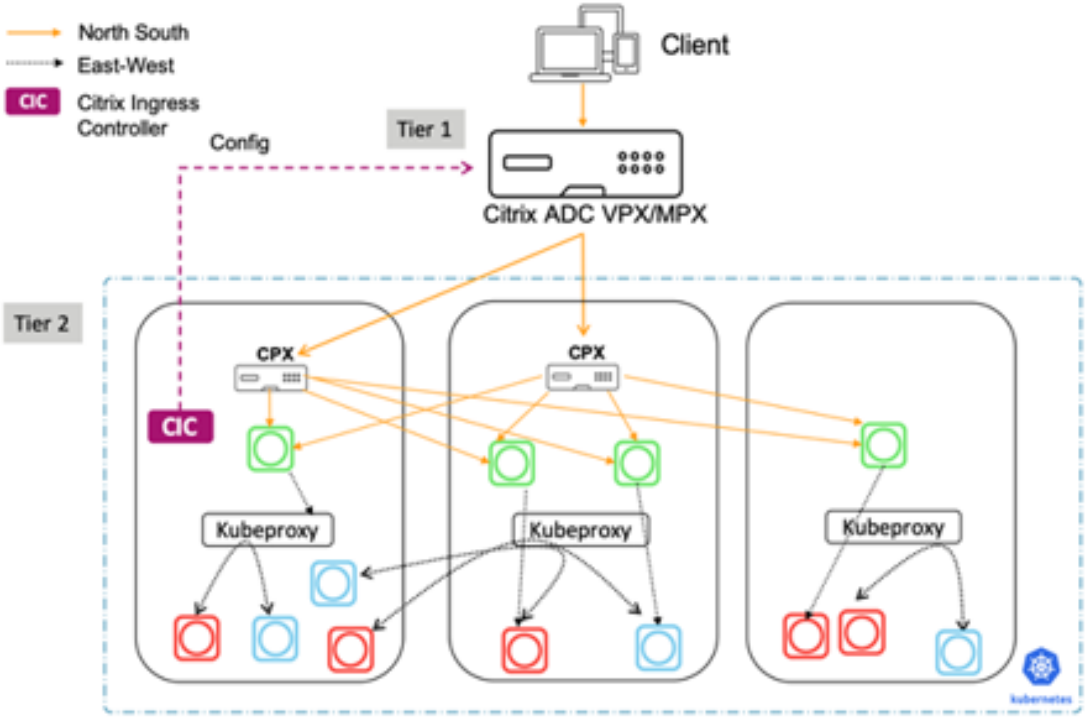
Dans ce document, nous décrivons comment Citric ADC fournit une intégration solide de la couche Routing/Service.

Projets OpenShift

Le premier nouveau concept OpenShift ajoute est le projet, qui enveloppe efficacement un espace de noms, avec l'accès à l'espace de noms étant contrôlé via le projet. L'accès est contrôlé par un modèle d'authentification et d'autorisation basé sur les utilisateurs et les groupes. Les projets dans OpenShift fournissent donc des murs entre les espaces de noms, ce qui garantit que les utilisateurs, ou les applications, ne peuvent voir et accéder que ce à quoi ils sont autorisés.

Espaces de noms OpenShift

Le concept de regroupement principal dans Kubernetes est l'espace de noms. Les espaces de noms sont également un moyen de diviser les ressources de cluster entre plusieurs utilisations. Cela étant dit, il n'y a pas de sécurité entre les espaces de noms dans Kubernetes. Si vous êtes un « utilisateur » dans un cluster Kubernetes, vous pouvez voir tous les différents espaces de noms et les ressources qui y sont définies.



Réseau SDN (Software Defined Networking) OpenShift

OpenShift Container Platform utilise une approche SDN (Software-defined Networking) pour fournir un réseau de cluster unifié qui permet la communication entre les modules à travers le cluster OpenShift Container Platform. Ce réseau de modules est établi et géré par le SDN OpenShift, qui configure un réseau de superposition à l'aide d'Open vSwitch (OVS).

OpenShift SDN fournit trois plug-ins SDN pour configurer le réseau de modules :

- Le plug-in ovs-subnet est le plug-in d'origine, qui fournit un réseau de pod « plat » où chaque pod peut communiquer avec tous les autres modules et services.
- Le plug-in ovs-multitenant fournit une isolation au niveau du projet pour les modules et les services. Chaque projet reçoit un identifiant de réseau virtuel (VNID) unique qui identifie le trafic provenant des pods affectés au projet. Les pods provenant de différents projets ne peuvent pas envoyer ou recevoir des paquets provenant de pods et de services d'un projet différent.
- Cependant, les projets qui reçoivent VNID 0 sont plus privilégiés en ce qu'ils sont autorisés à communiquer avec tous les autres pods, et tous les autres pods peuvent communiquer avec eux. Dans les clusters OpenShift Container Platform, le projet par défaut a VNID 0.Cela facilite certains services, tels que l'équilibreur de charge, à communiquer avec tous les autres modules du cluster et vice versa.
- Le plug-in ovs-networkpolicy permet aux administrateurs de projet de configurer leurs propres stratégies d'isolement à l'aide d'objets NetworkPolicy.

Routage OpenShift et plug-ins

Un administrateur OpenShift peut déployer des routeurs dans un cluster OpenShift, ce qui permet aux itinéraires créés par les développeurs d'être utilisés par des clients externes. La couche de routage dans OpenShift est enfichable, et deux plug-ins de routeur sont disponibles et pris en charge par défaut.

Les routeurs OpenShift fournissent un mappage de noms d'hôte externe et un équilibrage de charge des services sur des protocoles qui transmettent des informations distinctives directement au routeur ; le nom d'hôte doit être présent dans le protocole pour que le routeur pour déterminer où l'envoyer.

Les plug-ins de routeur supposent qu'ils peuvent se lier aux ports d'hôte 80 et 443. Ceci permet au trafic externe d'acheminer vers l'hôte et par la suite via le routeur. Les routeurs supposent également que la mise en réseau est configurée de manière à pouvoir accéder à tous les modules du cluster.

Le routeur OpenShift est le point d'entrée pour tout le trafic externe destiné aux services dans votre OpenShift Installation. OpenShift fournit et prend en charge les plug-ins de routeur suivants :

- Le routeur de modèle HAProxy est le plug-in par défaut. Il utilise openshift3/ose-haproxy-routerimage pour exécuter une instance HAProxy à côté du plug-in de routeur modèle dans un conteneur sur OpenShift. Il prend actuellement en charge le trafic HTTP (S) et le trafic TLS via SNI. Le conteneur du routeur écoute sur l'interface réseau hôte, contrairement à la plupart des conteneurs qui écoutent uniquement sur des adresses IP privées. Le routeur transfert via proxy les demandes externes de noms de routage vers les adresses IP des pods réels identifiés par le service associé à l'itinéraire.
- Le Controller d'entrée Citrix peut être déployé en tant que plug-in de routeur dans le cluster OpenShift pour s'intégrer aux Citrix ADC déployés dans votre environnement. Le Controller d'entrée Citrix vous permet d'utiliser les fonctionnalités avancées d'équilibrage de charge et de gestion du trafic de Citrix ADC avec votre cluster OpenShift. Voir Déployer le Controller d'entrée Citrix en tant que plug-in de routeur dans un cluster OpenShift.

Routes OpenShift et méthodes d'entrée

Dans un cluster OpenShift, les clients externes ont besoin d'un moyen leur permettent d'accéder aux services fournis par les pods. OpenShift offre deux ressources pour communiquer avec les services exécutés dans le cluster : itinéraires et Entrée.

Itinéraires

Dans un cluster OpenShift, une route expose un service sur un nom de domaine donné ou associe un nom de domaine à un service. Les routeurs OpenShift acheminent les demandes externes vers les services à l'intérieur du cluster OpenShift selon les règles spécifiées dans les itinéraires. Lorsque vous

utilisez le routeur OpenShift, vous devez également configurer le DNS externe pour vous assurer que le trafic atterrit sur le routeur.

Le Controller d'entrée Citrix peut être déployé en tant que plug-in de routeur dans le cluster OpenShift pour s'intégrer aux Citrix ADC déployés dans votre environnement. Le Controller d'entrée Citrix vous permet d'utiliser les fonctionnalités avancées d'équilibrage de charge et de gestion du trafic de Citrix ADC avec votre cluster OpenShift.
Les routes OpenShift peuvent être sécurisées ou non sécurisées. Les itinéraires sécurisés spécifient la terminaison TLS de l'itinéraire.

Le Controller d'entrée Citrix prend en charge les routes OpenShift suivantes :

- **Routes non sécurisées** : pour les routes non sécurisées, le trafic HTTP n'est pas chiffré.
- **Terminaison Edge** : Pour la terminaison Edge, TLS est terminé au niveau du routeur. Le trafic entre le routeur et les points de terminaison sur le réseau interne n'est pas chiffré.
- **Terminaison passthrough** : Avec la terminaison passthrough, le routeur n'est pas impliqué dans le déchargement TLS et le trafic crypté est envoyé directement à la destination.
- **Terminaison de re-cryptage** : Lors de la terminaison de re-cryptage, le routeur met fin à la connexion TLS, puis établit une autre connexion TLS au point de terminaison.

Entrée

Kubernetes Ingress vous fournit un moyen d'acheminer des demandes vers des services en fonction de l'hôte ou du chemin de requête, en centralisant un certain nombre de services en un seul point d'entrée.

Le contrôleur Citrix Ingress est construit autour de Kubernetes Ingress, configurant automatiquement un ou plusieurs appliances Citrix ADC en fonction de la ressource Ingress.

Le routage avec Ingress peut être fait par :

- Routage basé sur le nom d'hôte
- Routage basé sur le chemin
- Routage basé sur des caractères génériques
- Correspondance exacte du chemin
- Routage sans nom d'hôte
- Back-end par défaut

Pour obtenir des exemples et plus d'informations, reportez-vous à la section Configurations d'entrée.

Déployer le Controller d'entrée Citrix en tant que plug-in de routeur OpenShift

Selon la façon dont vous souhaitez utiliser Citrix ADC, il existe deux façons de déployer Citrix Ingress Controller en tant que plug-in de routeur dans le cluster OpenShift :

- En tant que conteneur sidecar à côté de Citrix ADC CPX dans le même conteneur : dans ce mode, le Controller d'entrée Citrix configure le Citrix ADC CPX. Voir Déployer Citrix ADC CPX en tant que routeur au sein du cluster OpenShift.
- En tant que conteneur autonome dans le cluster OpenShift : dans ce mode, vous pouvez contrôler l'appliance Citrix ADC MPX ou VPX déployée en dehors du cluster. Voir Déployer Citrix ADC MPX/VPX en tant que routeur en dehors du cluster OpenShift.

Architectures recommandées

Nous recommandons les architectures suivantes pour les clients lors de la conception de leurs architectures de microservices :

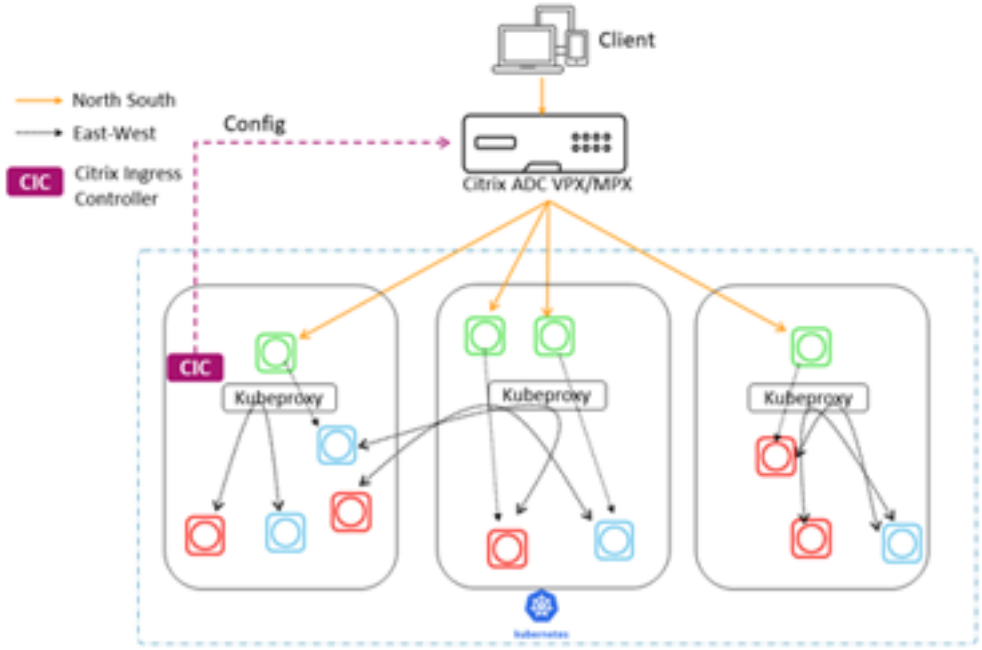
- Citrix Unified Ingress
- Citrix 2-Tier Ingress
- Citrix Service Mesh Lite

Citrix Unified Ingress

Dans un déploiement Unified Ingress, les périphériques Citrix ADC MPX ou VPX transfèrent le trafic Nord-Sud des clients vers les applications professionnelles déployées en tant que microservices à l'intérieur du cluster. Le Controller d'entrée Citrix est déployé en tant que pod ou sidecar dans le cluster Kubernetes pour automatiser la configuration des périphériques Citrix ADC (MPX ou VPX) en fonction des modifications apportées aux microservices ou aux ressources Ingress.

Vous pouvez commencer à implémenter le modèle d'entrée unifiée lorsque votre application est toujours un monolithe. Placez simplement le Citrix ADC en tant que proxy inverse devant votre serveur d'applications et implémentez les fonctionnalités décrites plus loin. Vous êtes alors en bonne position pour convertir votre application en microservices.

La communication entre les microservices est gérée par un mécanisme de votre choix (kube-proxy, IPVS, etc.).



Fonctionnalités fournies dans différentes catégories

Les capacités de l'architecture Unified Ingress se répartissent en trois groupes.

Les fonctionnalités du premier groupe optimisent les performances :

- Équilibrage de charge
- Connectivité à faible latence
- Haute disponibilité

Les fonctionnalités du deuxième groupe améliorent la sécurité et facilitent la gestion des applications :

- Limitation du taux
- Terminaison SSL/TLS
- Prise en charge HTTP/2
- Vérifications de santé

Les caractéristiques du groupe final sont spécifiques aux microservices :

- Point central de communication pour les services
- Fonctionnalité de Gateway API

Résumé

Les fonctionnalités du modèle d'entrée unifiée incluent un équilibrage de charge robuste pour les services, un point de communication central, la découverte dynamique des services, la connectivité à faible latence, la haute disponibilité, la limitation du débit, la terminaison SSL/TLS, HTTP/2, et bien plus encore.

Le modèle Unified Ingress facilite la gestion du trafic, des demandes d'équilibrage de charge et la réponse dynamique aux modifications apportées à l'application de microservices back-end.

Les avantages comprennent :

- Les flux de trafic Nord-Sud offrent une bonne scalabilité, sont visibles pour l'observation et la surveillance, et fournissent une livraison continue avec des outils tels que Spinnaker et Citrix ADM
- Un niveau unique unifie l'équipe d'infrastructure qui gère les services réseau et de plate-forme, et réduit les sauts pour réduire la latence
- Convient pour les applications internes qui n'ont pas besoin de Web App Firewall et de déchargement SSL, mais peuvent être ajoutées ultérieurement

Les inconvénients comprennent :

- Pas de sécurité Est-Ouest avec kube-proxy, mais possibilité d'ajouter Calico pour la segmentation L4
- La scalabilité Kube-proxy est inconnue
- Il n'y a que peu de visibilité du trafic Est-Ouest puisque kube-proxy ne donne pas de visibilité, de contrôle ou de journaux, ce qui réduit l'intégration des outils ouverts et la livraison continue
- L'équipe de la plateforme doit également être avisé du réseau

Citrix 2-Tier Ingress

Le modèle architectural Ingress à 2 niveaux est une excellente solution pour les novices Cloud Native. Dans ce modèle, Citrix ADC de niveau 1 gère le trafic entrant, mais envoie les demandes au ADC à 2 niveaux géré par les développeurs plutôt que directement aux instances de service. Le modèle Ingress de niveau 2 applique des stratégies écrites par l'équipe Platform and Developers uniquement au trafic entrant, et permet l'évolutivité et la multilocation du Cloud.

Fonctionnalités fournies par le niveau 1

L'ADC de premier niveau, géré par l'équipe réseau traditionnelle, fournit l'équilibrage de charge L4, le Citrix Web App Firewall, le déchargement SSL et les services proxy inversé. Les périphériques Citrix ADC MPX ou VPX de niveau 1 transfèrent le trafic (Nord-Sud) entre le client et Citrix ADC CPX dans niveau 2.

Par défaut, Citrix Ingress Controller programmera les configurations suivantes sur le niveau 1 :

- Proxy inverse des applications aux utilisateurs :

- Serveurs virtuels de commutation de contenu
- Serveur virtuel (frontal, présenté à l'utilisateur)
- Groupes de services
- Déchargement SSL
- Journalisation NetScaler/débogage
- Surveillance sanitaire des services

Fonctionnalités fournies par le niveau 2

Alors que l'ADC de premier niveau fournit des services de proxy inverse, l'ADC de deuxième niveau, géré par l'équipe de la Plateforme, sert de point de communication pour les microservices, fournissant :

- Découverte dynamique des services
- Équilibrage de charge
- Visibilité et mesures enrichies

Le Citrix ADC CPX de niveau 2 achemine ensuite le trafic vers les microservices du cluster Kubernetes. Le Controller d'entrée Citrix déployé en tant que module autonome configure les périphériques de niveau 1. De plus, le Controller side-car dans un ou plusieurs pods Citrix ADC CPX configure le Citrix ADC CPX associé dans le même conteneur.

Résumé

L'architecture de mise en réseau pour les microservices dans le modèle à deux niveaux utilise deux ADC configurés pour des rôles différents. L'ADC de niveau 1 agit comme un serveur proxy orienté utilisateur et l'ADC de niveau 2 comme proxy pour les microservices.

Le partage de différents types de fonctions entre deux niveaux différents offre vitesse, contrôle et opportunités d'optimiser la sécurité. Dans le deuxième niveau, l'équilibrage de charge est rapide, robuste et configurable.

Avec ce modèle, il existe une séparation claire entre l'administrateur ADC et le développeur. C'est BYOL pour les développeurs.

Les avantages comprennent :

- Les flux de trafic Nord-Sud offrent une bonne scalabilité, sont visibles pour l'observation et la surveillance, et fournissent une livraison continue avec des outils tels que Spinnaker et Citrix ADM
- Déploiement le plus simple et plus rapide pour un Cloud Native Novice avec un apprentissage limité pour les équipes Network et Platform

Les inconvénients comprennent :

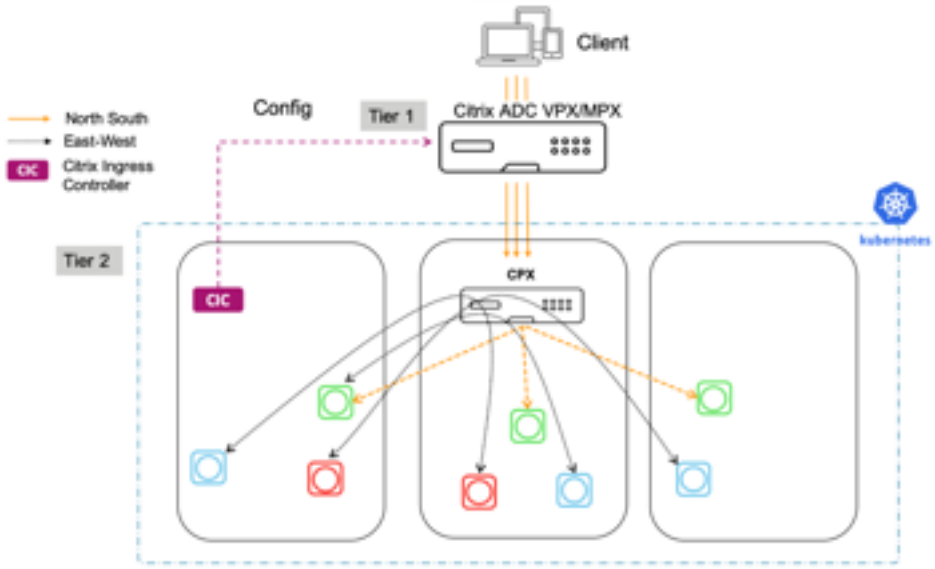
- Pas de sécurité Est-Ouest avec kube-proxy, mais possibilité d'ajouter Calico pour la segmentation L4
- La scalabilité Kube-proxy est inconnue
- Il n'y a que peu de visibilité du trafic Est-Ouest puisque kube-proxy ne donne pas de visibilité, de contrôle ou de journaux, ce qui réduit l'intégration des outils ouverts et la livraison continue.

Citrix Service Mesh Lite

Le Service Mesh Lite est la plus riche en fonctionnalités des trois modèles. Il est sécurisé, rapide, efficace et résilient en interne et peut être utilisé pour appliquer des stratégies pour le trafic entrant et inter-conteneurs.

Le modèle Service Mesh Lite est adapté à plusieurs cas d'utilisation, notamment :

- Applications de santé et de finances — Les exigences réglementaires et des utilisateurs exigent une combinaison de sécurité et de rapidité pour les applications financières et de santé, avec des milliards de dollars de valeur financière et de réputation en jeu.
- Applications de commerce électronique — La confiance des utilisateurs est un problème énorme pour le commerce électronique et la vitesse est un facteur de différenciation concurrentiel clé. La combinaison de vitesse et de sécurité est donc cruciale.



Résumé

Les avantages comprennent :

- Une approche plus robuste de la mise en réseau, avec un équilibreur de charge

- CPX applique des stratégies au trafic entrant et inter-conteneurs, en déployant des stratégies L7 complètes
- Une observabilité, des analyses, une livraison continue et une sécurité plus riches pour le trafic Nord-Sud et Est-Ouest
- Canary pour chaque conteneur avec un Citrix ADC intégré
- Un niveau unique unifie l'équipe d'infrastructure qui gère les services réseau et de plate-forme, et réduit les sauts pour réduire la latence

Les inconvénients comprennent :

- Modèle plus complexe à déployer
- L'équipe de la plateforme doit être avisé du réseau

Résumé de Architecture Choices

Citrix Unified Ingress

- **Trafic d'applications Nord-Sud (NS)** - un Citrix ADC est responsable du trafic L4 et L7 NS, de la sécurité et de l'équilibrage de charge externe en dehors du cluster K8s.
- **Trafic d'application Est-Ouest (EW)** - kube-proxy est responsable du trafic EW L4.
- **Sécurité** - L'ADC est responsable de la sécurisation du trafic NS et de l'authentification des utilisateurs. Kube-proxy est responsable du trafic L4 EW.
- **Scalabilité et performances** - Le trafic NS offre une bonne scalabilité, et le clustering est une option. Le trafic EW et la scalabilité kube-proxy sont inconnus.
- **Observabilité** - l'ADC offre une excellente observabilité pour le trafic NS, mais il n'y a pas d'observabilité pour le trafic EW.

Citrix 2-Tier Ingress

- **Trafic d'applications Nord-Sud (NS)** - ADC de niveau 1 est responsable du déchargement SSL, de Web App Firewall et du trafic L4 NS. Il est utilisé pour les applications monolithe et CN. Le CPX de niveau 2 gère le changement rapide du trafic k8s et L7 NS.
- **Trafic d'application Est-Ouest (EW)** - kube-proxy est responsable du trafic EW L4.
- **Sécurité** - L'ADC de niveau 1 est responsable de la sécurisation du trafic NS. L'authentification peut se produire sur l'un ou l'autre des ADC. Le trafic EW n'est pas sécurisé avec Kube-proxy.Add Calico pour la segmentation L4.
- **Scalabilité et performances** - Le trafic NS offre une bonne scalabilité, et le clustering est une option. Le trafic EW et la scalabilité kube-proxy sont inconnus.
- **Observabilité** - L'ADC de niveau 1 offre une excellente observabilité pour le trafic NS, mais il n'y a pas d'observabilité pour le trafic EW.

Citrix Service Mesh Lite

- **Trafic d'applications Nord-Sud (NS)** - ADC de niveau 1 est responsable du déchargement SSL, de Web App Firewall et du trafic L4 NS. Il est utilisé pour les applications monolithe et CN. Le CPX de niveau 2 gère le changement rapide du trafic k8s et L7 NS.
- **Trafic d'application Est-Ouest (EW)** - le CPX de niveau 2 ou tout proxy open source est responsable du trafic L4 EW. Les clients peuvent sélectionner les applications qui utilisent le CPX et celles qui utilisent kube-proxy.
- **Sécurité** - L'ADC de niveau 1 est responsable de la sécurisation du trafic NS. L'authentification peut se produire sur l'un ou l'autre des ADC. Citrix CPX est responsable de l'authentification, du déchargement SSL et de la sécurisation du trafic EW. Le chiffrement peut être appliqué au niveau de l'application.
- **Évolutivité et performances** - Le trafic NS et EW est bien évolutif, mais il ajoute 1 saut en ligne.
- **Observabilité** - L'ADC de niveau 1 offre une excellente observabilité du trafic NS. Le CPX de niveau 2 permet d'observer le trafic EW, mais il peut être désactivé pour réduire l'encombrement CPX ou CPU.

Comment déployer

Citrix Unified Ingress

Pour valider un déploiement Citrix Unified Ingress avec OpenShift, utilisez un exemple d'application "hello-world" avec un Citrix ADC VPX ou MPX. L'espace de noms par défaut d'OpenShift, « default », est utilisé pour ce déploiement.

1. Une instance de Citrix ADC est conçue manuellement et configurée avec un NSIP/SNIP. Vous pouvez trouver l'installation de Citrix ADC sur XenServer ici.
2. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le application.yaml.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-world
spec:
  selector:
    matchLabels:
      run: load-balancer-example
  replicas: 2
  template:
    metadata:
```



```
12        labels:
13          run: load-balancer-example
14      spec:
15        containers:
16          -  name: hello-world
17            image: gcr.io/google-samples/node-hello:1.0
18            ports:
19              -  containerPort: 8080
20                protocol: TCP
21  <!--NeedCopy-->
```

3. Déployez l'application.

   ```
   oc apply -f application.yaml
   ```

4. Assurez-vous que les pods sont en cours d'exécution.

   ```
   oc get pods
   ```

5. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le service.yaml.

   ```
   1  apiVersion: v1
   2  kind: Service
   3  metadata:
   4    name: hello-world-service
   5  spec:
   6    type: NodePort
   7    ports:
   8    -  port: 80
   9      targetPort: 8080
   10   selector:
   11     run: load-balancer-example
   12 <!--NeedCopy-->
   ```

6. Exposez l'application via NodePort avec un service.

   ```
   oc apply -f service.yaml
   ```

7. Vérifiez que le service a été créé.

   ```
   oc get service
   ```

8. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le Ingress.yaml.Vous devez changer l'annotation « ingress.citrix.com/frontend-ip » en une adresse IP libre pour être transformé en VIP sur Citrix ADC.

   ```
   1  apiVersion: extensions/v1beta1
   ```



```
kind: Ingress
metadata:
  name: hello-world-ingress
  annotations:
   kubernetes.io/ingress.class: "vpx"
   ingress.citrix.com/insecure-termination: "redirect"
   ingress.citrix.com/frontend-ip: "10.217.101.183"
spec:
  rules:
  -  host:  helloworld.com
    http:
      paths:
      -  path:
        backend:
          serviceName: hello-world-service
          servicePort: 80
<!--NeedCopy-->
```

9. Déployez le fichier Ingress YAML.

   ```
   oc apply -f ingress.yaml
   ```

10. Maintenant, il y a des pods d'application que nous avons exposés en utilisant un service, et peuvent acheminer le trafic vers eux en utilisant Ingress. Installez Citrix Ingress Controller (CIC) pour pousser ces configurations vers notre VPX ADC de niveau 1. Avant de déployer le CIC, déployez un fichier RBAC qui donne au CIC les autorisations appropriées pour s'exécuter.

    > **Note :**
    >
    > Le fichier rbac yaml spécifie l'espace de noms et il devra être modifié, en attendant quel espace de noms est utilisé.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
rules:
  -  apiGroups: [""]
    resources: ["services", "endpoints", "ingresses", "pods", "
       secrets", "nodes", "routes", "routes/status", "tokenreviews
       ", "subjectaccessreviews"]
    verbs: ["\*"]
  -  apiGroups: ["extensions"]
    resources: ["ingresses", "ingresses/status"]
    verbs: ["\*"]
  -  apiGroups: ["citrix.com"]
```



```
    resources: ["rewritepolicies"]
    verbs: ["\*"]
  -  apiGroups: ["apps"]
    resources: ["deployments"]
    verbs: ["\*"]

<!--NeedCopy-->
```

```
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cpx
subjects:
-  kind: ServiceAccount
  name: cpx
  namespace: default

<!--NeedCopy-->
```

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: cpx
  namespace: default
<!--NeedCopy-->
```

11. Déployez le fichier RBAC.

    ```
    oc apply -f rbac.yaml
    ```

12. Avant de déployer le CIC, modifiez le fichier YAML. Sous spec, ajoutez le NSIP ou le SNIP tant que la gestion est activée sur le SNIP, du ADC de niveau 1. Notez que l'argument « ingress-classes » est le même que l'annotation de classe d'entrée spécifiée dans le fichier Ingress YAML.

    ```
    apiVersion: v1
    kind: Pod
    metadata:
      name: hello-world-cic
      labels:
        app: hello-world-cic
    spec:
    ```



```
8    serviceAccountName: cpx
9    containers:
10   -  name: hello-world-cic
11     image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3"
12     env:
13      # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has to be
            enabled)
14      -  name: "NS_IP"
15        value: "10.217.101.193"
16      # Set username for Nitro
17      # Set log level
18      -  name: "NS_ENABLE_MONITORING"
19        value: "NO"
20      -  name: "NS_USER"
21        value: "nsroot"
22      -  name: "NS_PASSWORD"
23        value: "nsroot"
24      -  name: "EULA"
25        value: "yes"
26      -  name: "LOGLEVEL"
27        value: "DEBUG"
28     args:
29       -  --ingress-classes
30         vpx
31       -  --feature-node-watch
32         false
33     imagePullPolicy: IfNotPresent
34 <!--NeedCopy-->
```

13. Déployez le CIC.

    ```
    oc apply -f cic.yaml
    ```

14. Vérifiez que tous les pods sont en cours d'exécution.

    ```
    oc get pods
    ```

15. Modifiez le fichier hosts sur votre machine locale avec une entrée pour helloworld.com et le VIP sur Citrix ADC spécifié dans le fichier YAML Ingress.

16. Accédez à helloworld.com dans un navigateur."Hello Kubernetes!" devrait apparaître.

> **Remarque :** Ce qui suit sont des commandes de suppression
>
> - `oc delete pods (pod name)-n (namespace name)`
> - `oc delete deployment (deployment name)-n (namespace name)`
> - `oc delete service (service name)-n (namespace name)`

- `oc delete ingress (ingress name)-n (namespace name)`
- `oc delete serviceaccounts (serviceaccounts name)-n (namespace name)`

Citrix 2-Tier Ingress

Pour valider un déploiement Citrix Ingress à 2 niveaux avec OpenShift, utilisez un exemple d'application "hello-world" avec un Citrix ADC VPX ou MPX. L'espace de noms par défaut "tier-2-adc" est utilisé pour ce déploiement.

Remarque : Lors du déploiement de pods, de services et d'Ingress, l'espace de noms doit être spécifié à l'aide du paramètre "-n (nom d'espace de noms)".

1. Une instance de Citrix ADC est créée manuellement et configurée avec un NSIP/SNIP.L'installation de Citrix ADC sur XenServer peut être trouvée [ici. Si l'instance était déjà configurée, effacez tous les serveurs virtuels dans l'équilibrage de charge ou la commutation de contenu qui ont été transmis à ADC afin de ne pas déployer hello-world en tant qu'entrée unifiée.
2. Créez un espace de noms appelé "tier-2-adc".

   ```
   oc create namespace tier-2-adc
   ```

3. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le `application-2t.yaml`.

```
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-world
spec:
  selector:
    matchLabels:
      run: load-balancer-example
  replicas: 2
  template:
    metadata:
      labels:
        run: load-balancer-example
    spec:
      containers:
        -  name: hello-world
          image: gcr.io/google-samples/node-hello:1.0
          ports:
            -  containerPort: 8080
              protocol: TCP

<!--NeedCopy-->
```


4. Déployez l'application dans l'espace de noms.

   ```
   oc apply -f application-2t.yaml -n tier-2-adc
   ```

5. Assurez-vous que les pods sont en cours d'exécution.

   ```
   oc get pods
   ```

6. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le `service-2t.yaml`.

   ```
   apiVersion: v1
   kind: Service
   metadata:
     name: hello-world-service-2
   spec:
     type: NodePort
     ports:

     -port: 80
       targetPort: 8080
     selector:
       run: load-balancer-example
   <!--NeedCopy-->
   ```

7. Exposer l'application via NodePort avec un service.

   ```
   oc apply -f service-2t.yaml -n tier-2-adc
   ```

8. Vérifiez que le service a été créé.

   ```
   oc get service -n tier-2-adc
   ```

9. Copiez l'exemple de fichier YAML suivant dans un répertoire OpenShift et nommez-le `ingress-2t.yaml`.

   ```
       apiVersion: extensions/v1beta1
       kind: Ingress
       metadata:
         name: hello-world-ingress-2
         annotations:
          kubernetes.io/ingress.class: "cpx"
       spec:
         backend:
           serviceName: hello-world-service-2
           servicePort: 80
   <!--NeedCopy-->
   ```


10. Déployez le fichier Ingress YAML.

```
oc apply -f ingress-2t.yaml -n tier-2-adc
```

11. Déployez un fichier RBAC qui donne au CIC et CPX les autorisations correctes à exécuter.

> **Remarque :**
>
> Le fichier rbac yaml spécifie l'espace de noms et il devra être modifié, en attendant quel espace de noms est utilisé.

```
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
rules:
  -apiGroups: [""]
    resources: ["services", "endpoints", "ingresses", "pods", "
       secrets", "nodes", "routes", "routes/status", "tokenreviews
       ", "subjectaccessreviews"]
    verbs: ["\*"]
  -apiGroups: ["extensions"]
    resources: ["ingresses", "ingresses/status"]
    verbs: ["\*"]
  -apiGroups: ["citrix.com"]
    resources: ["rewritepolicies"]
    verbs: ["\*"]
  -apiGroups: ["apps"]
    resources: ["deployments"]
    verbs: ["\*"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1beta1
metadata:
  name: cpx
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cpx
subjects:
-  kind: ServiceAccount
  name: cpx
  namespace: tier-2-adc
---
apiVersion: v1
kind: ServiceAccount
metadata:
```



```
35    name: cpx
36    namespace: tier-2-adc
37  <!--NeedCopy-->
```

12. Déployez le fichier RBAC.

    ```
    oc apply -f rbac-2t.yaml
    ```

13. Le compte de service a besoin d'autorisations élevées pour créer un CPX.

    ```
    oc adm policy add-scc-to-user privileged system:serviceaccount:tier-2-adc:cpx
    ```

14. Modifiez le fichier CPX YAML et appelez-le `cpx-2t.yaml`. Cela déploie le CPX et le service qui l'expose. Notez que l'argument de classe Ingress correspond à l'annotation dans le fichier `ingress-2t.yaml`.

```
1      apiVersion: extensions/v1beta1
2      kind: Deployment
3      metadata:
4        name: hello-world-cpx-2
5      spec:
6        replicas: 1
7        template:
8          metadata:
9            name: hello-world-cpx-2
10           labels:
11             app: hello-world-cpx-2
12             app1: exporter
13           annotations:
14             NETSCALER_AS_APP: "True"
15         spec:
16           serviceAccountName: cpx
17           containers:
18             -  name: hello-world-cpx-2
19               image: "quay.io/citrix/citrix-k8s-cpx-ingress
                    :13.0-36.28"
20               securityContext:
21                  privileged: true
22               env:
23               -  name: "EULA"
24               value: "yes"
25               -  name: "KUBERNETES_TASK_ID"
26                 value: ""
27               imagePullPolicy: Always
28         # Add cic as a sidecar
```



```
29              -  name: cic
30                image: "quay.io/citrix/citrix-k8s-ingress-controller
                     :1.1.3"
31                env:
32                -  name: "EULA"
33                  value: "yes"
34                -  name: "NS_IP"
35                  value: "127.0.0.1"
36                -  name: "NS_PROTOCOL"
37                  value: "HTTP"
38                -  name: "NS_PORT"
39                  value: "80"
40                -  name: "NS_DEPLOYMENT_MODE"
41                  value: "SIDECAR"
42                -  name: "NS_ENABLE_MONITORING"
43                  value: "YES"
44                -  name: POD_NAME
45                  valueFrom:
46                    fieldRef:
47                      apiVersion: v1
48                      fieldPath: metadata.name
49                -  name: POD_NAMESPACE
50                  valueFrom:
51                    fieldRef:
52                      apiVersion: v1
53                      fieldPath: metadata.namespace
54                args:
55                  -  --ingress-classes
56                     cpx
57                imagePullPolicy: Always
58          apiVersion: v1
59          kind: Service
60          metadata:
61            name: lb-service-cpx
62            labels:
63              app: lb-service-cpx
64          spec:
65            type: NodePort
66            ports:
67            -  port: 80
68              protocol: TCP
69              name: http
70              targetPort: 80
71            selector:
72              app: hello-world-cpx-2
```



```
73
74 <!--NeedCopy-->
```

15. Déployez le CPX.

```
oc apply -f cpx-2t.yaml -n tier-2-adc
```

16. Vérifiez que le module est en cours d'exécution et que le service a été créé.

```
oc get pods -n tier-2-adc
oc get service -n tier-2-adc
```

17. Créez une entrée pour acheminer du VPX vers le CPX. L'adresse IP frontale doit être une adresse IP libre sur l'ADC. Donnez au fichier un nom :`ingress-cpx-2t.yaml`.

```
1  apiVersion: extensions/v1beta1
2  kind: Ingress
3  metadata:
4    name: hello-world-ingress-vpx-2
5    annotations:
6     kubernetes.io/ingress.class: "helloworld"
7     ingress.citrix.com/insecure-termination: "redirect"
8     ingress.citrix.com/frontend-ip: "10.217.101.183"
9  spec:
10   rules:
11     -  host:  helloworld.com
12
13     http:
14       paths:
15       -  path:
16         backend:
17           serviceName: lb-service-cpx
18           servicePort: 80
19 <!--NeedCopy-->
```

18. Déployez l'entrée.

```
oc apply -f ingress-cpx-2t.yaml -n tier-2-adc
```

19. Avant de déployer le CIC, modifiez le fichier YAML. Sous spec, ajoutez le NSIP ou le SNIP tant que la gestion est activée sur le SNIP, du ADC de niveau 1.

```
1  apiVersion: v1
2  kind: Pod
3  metadata:
4    name: hello-world-cic
5    labels:
```



```
6       app: hello-world-cic
7   spec:
8         serviceAccountName: cpx
9         containers:
10        -  name: hello-world-cic
11          image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3
                "
12          env:
13           # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has
                 to be enabled)
14           -  name: "NS_IP"
15          value: "10.217.101.176"
16        # Set username for Nitro
17        # Set log level
18        -  name: "NS_ENABLE_MONITORING"
19          value: "NO"
20        -  name: "NS_USER"
21          value: "nsroot"
22        -  name: "NS_PASSWORD"
23          value: "nsroot"
24        -  name: "EULA"
25          value: "yes"
26        -  name: "LOGLEVEL"
27          value: "DEBUG"
28      args:
29        -  --ingress-classes
30          helloworld
31        -  --feature-node-watch
32          false
33      imagePullPolicy: IfNotPresent
34  <!--NeedCopy-->
```

20. Déployez le CIC.

    ```
    oc apply -f cic-2t.yaml -n tier-2-adc
    ```

21. Vérifiez que tous les pods sont en cours d'exécution.

    ```
    oc get pods -n tier-2-adc
    ```

22. Modifiez le fichier hosts sur votre machine locale avec une entrée pour helloworld.com et le VIP sur Citrix ADC spécifié dans le fichier YAML Ingress qui roule du VPX au CPX.

23. Accédez à helloworld.com dans un navigateur."Hello Kubernetes!" devrait apparaître.

Citrix Service Mesh Lite

Service Mesh Lite permet l'introduction de CPX (ou d'autres appliances Citrix ADC) en remplacement des fonctionnalités HAProxy intégrées. Cela nous permet d'étendre nos capacités N/S à Kubernetes et de fournir l'équilibrage de la charge de trafic E/W, le routage et l'observabilité.
Citrix ADC (MPX, VPX ou CPX) peut offrir de tels avantages pour le trafic E-W, tels que :

- Déchargement TLS ou SSL mutuel
- Routage basé sur le contenu pour autoriser ou bloquer le trafic basé sur les paramètres d'en-tête HTTP ou HTTPS
- Algorithmes avancés d'équilibrage de charge (par exemple, moins de connexions, moins de temps de réponse, etc.)
- Observabilité du trafic est-ouest grâce à la mesure des signaux dorés (erreurs, latences, saturation ou volume de trafic) .Service Graph de Citrix ADM est une solution d'observabilité permettant de surveiller et de déboguer les microservices.
- Dans ce scénario de déploiement, nous déployons l'application Bookinfo et observons son fonctionnement par défaut. Ensuite, nous passons à extraire et remplacer les services Kubernetes par défaut et utilisons CPX et VPX pour proxy notre trafic E/W.

Citrix Service Mesh Lite avec CPX

Pour valider un déploiement Citrix Unified Ingress avec OpenShift, utilisez un exemple d'application "hello-world" avec un Citrix ADC VPX ou MPX. L'espace de noms par défaut pour OpenShift, « default », est utilisé pour ce déploiement.

1. Une instance de Citrix ADC est créée manuellement et configurée avec un NSIP/SNIP.L'installation de Citrix ADC sur XenServer peut être trouvée ici.
2. Créez un espace de noms pour ce déploiement. Dans cet exemple, `sml` est utilisé.

   ```
   oc create namespace sml
   ```

3. Copiez le YAML suivant pour créer le déploiement et les services pour Bookinfo. Nommez-le bookinfo.yaml.

```
1  ##################################################################################################
2  # Details service
3  ##################################################################################################
4  apiVersion: v1
5  kind: Service
6  metadata:
7    name: details
8    labels:
```



```
    app: details
    service: details
spec:
  ports:
  -  port: 9080
    name: http
  selector:
    app: details
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: details-v1
  labels:
    app: details
    version: v1
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
        app: details
        version: v1
    spec:
      containers:
      -  name: details
        image: docker.io/maistra/examples-bookinfo-details-v1:0.12.0
        imagePullPolicy: IfNotPresent
        ports:
        -  containerPort: 9080
---
##################################################################################

# Ratings service
##################################################################################

apiVersion: v1
kind: Service
metadata:
  name: ratings
  labels:
    app: ratings
    service: ratings
```



```
spec:
  ports:
  -  port: 9080
    name: http
  selector:
    app: ratings
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: ratings-v1
  labels:
    app: ratings
    version: v1
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
        app: ratings
        version: v1
    spec:
      containers:
      -  name: ratings
        image: docker.io/maistra/examples-bookinfo-ratings-v1:0.12.0
        imagePullPolicy: IfNotPresent
        ports:
        -  containerPort: 9080
---
##################################################################################################

# Reviews service
##################################################################################################

apiVersion: v1
kind: Service
metadata:
  name: reviews
  labels:
    app: reviews
    service: reviews
spec:
  ports:
```



```
95    -  port: 9080
96      name: http
97    selector:
98      app: reviews
99  ---
100 apiVersion: extensions/v1beta1
101 kind: Deployment
102 metadata:
103   name: reviews-v1
104   labels:
105     app: reviews
106     version: v1
107 spec:
108   replicas: 1
109   template:
110     metadata:
111       annotations:
112         sidecar.istio.io/inject: "false"
113       labels:
114         app: reviews
115         version: v1
116     spec:
117       containers:
118       -  name: reviews
119         image: docker.io/maistra/examples-bookinfo-reviews-v1:0.12.0
120         imagePullPolicy: IfNotPresent
121         ports:
122         -  containerPort: 9080
123 ---
124 apiVersion: extensions/v1beta1
125 kind: Deployment
126 metadata:
127   name: reviews-v2
128   labels:
129     app: reviews
130     version: v2
131 spec:
132   replicas: 1
133   template:
134     metadata:
135       annotations:
136         sidecar.istio.io/inject: "false"
137       labels:
138         app: reviews
139         version: v2
```



```
    spec:
      containers:
      -  name: reviews
        image: docker.io/maistra/examples-bookinfo-reviews-v2:0.12.0
        imagePullPolicy: IfNotPresent
        ports:
        -  containerPort: 9080
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: reviews-v3
  labels:
    app: reviews
    version: v3
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
        app: reviews
        version: v3
    spec:
      containers:
      -  name: reviews
        image: docker.io/maistra/examples-bookinfo-reviews-v3:0.12.0
        imagePullPolicy: IfNotPresent
        ports:
        -  containerPort: 9080
---
##################################################################################

# Productpage services
##################################################################################

apiVersion: v1
kind: Service
metadata:
  name: productpage-service
spec:
  type: NodePort
  ports:
  -  port: 80
```



```
    targetPort: 9080
  selector:
    app: productpage
---
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: productpage-v1
  labels:
    app: productpage
    version: v1
spec:
  replicas: 1
  template:
    metadata:
      annotations:
        sidecar.istio.io/inject: "false"
      labels:
        app: productpage
        version: v1
    spec:
      containers:
      -  name: productpage
        image: docker.io/maistra/examples-bookinfo-productpage-v1
           :0.12.0
        imagePullPolicy: IfNotPresent
        ports:
        -  containerPort: 9080
---
<!--NeedCopy-->
```

1. Déployez le bookinfo.yaml dans l'espace de noms sml.

   ```
   oc apply -f bookinfo.yaml -n sml
   ```

2. Copiez et déployez le fichier d'entrée qui correspond au service de page de produit. Ce fichier peut être nommé `ingress-productpage.yaml`. L'IP frontale doit être un VIP gratuit sur Citrix ADC VPX/MPX.

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: productpage-ingress
  annotations:
   kubernetes.io/ingress.class: "bookinfo"
   ingress.citrix.com/insecure-termination: "redirect"
```



```
8     ingress.citrix.com/frontend-ip: "10.217.101.182"
9  spec:
10   rules:
11   -  host: bookinfo.com
12     http:
13       paths:
14       -  path:
15         backend:
16           serviceName: productpage-service
17           servicePort: 80
18 <!--NeedCopy-->
```

`oc apply -f ingress-productpage.yaml -n sml`

1. Copiez le fichier YAML suivant pour le fichier RBAC dans l'espace de noms sml et déployez-le. Nommez le fichier `rbac-cic-pp.yaml` tel qu'il est utilisé pour le CIC devant le microservice de la page produit.

```
1  kind: ClusterRole
2  apiVersion: rbac.authorization.k8s.io/v1beta1
3  metadata:
4    name: cpx
5  rules:
6    -  apiGroups: [""]
7      resources: ["services", "endpoints", "ingresses", "pods", "secrets"
           , "routes", "routes/status", "nodes", "namespaces"]
8      verbs: ["\*"]
9    -  apiGroups: ["extensions"]
10     resources: ["ingresses", "ingresses/status"]
11     verbs: ["\*"]
12   -  apiGroups: ["citrix.com"]
13     resources: ["rewritepolicies", "vips"]
14     verbs: ["\*"]
15   -  apiGroups: ["apps"]
16     resources: ["deployments"]
17     verbs: ["\*"]
18   -  apiGroups: ["apiextensions.k8s.io"]
19     resources: ["customresourcedefinitions"]
20     verbs: ["get", "list", "watch"]
21 ---
22 kind: ClusterRoleBinding
23 apiVersion: rbac.authorization.k8s.io/v1beta1
24 metadata:
25   name: cpx
26 roleRef:
```



```
27    apiGroup: rbac.authorization.k8s.io
28    kind: ClusterRole
29    name: cpx
30  subjects:
31  -   kind: ServiceAccount
32    name: cpx
33    namespace: sml
34  apiVersion: rbac.authorization.k8s.io/v1
35  ---
36  apiVersion: v1
37  kind: ServiceAccount
38  metadata:
39    name: cpx
40    namespace: sml
41  <!--NeedCopy-->
```

```
oc apply -f rbac-cic-pp.yaml -n sml
```

1. Élevez les privilèges du compte de service pour déployer CIC et CPX.

   ```
   oc adm policy add-scc-to-user privileged system:serviceaccount:sml:cpx
   ```

2. Modifiez le fichier hosts sur la machine locale avec bookinfo.com mappé à l'adresse IP frontale spécifiée dans `ingress-productpage.yaml`.

3. Copiez et déployez la page produit avec un CIC. Nommez le fichier `cic-productpage.yaml`.Le NS_IP doit être le NS_IP du ADC de niveau 1.

```
1  apiVersion: v1
2  kind: Pod
3  metadata:
4    name: productpage-cic
5    labels:
6      app: productpage-cic
7  spec:
8        serviceAccountName: cpx
9        containers:
10       -   name: productpage-cic
11         image: "quay.io/citrix/citrix-k8s-ingress-controller:1.1.3"
12         env:
13          # Set NetScaler NSIP/SNIP, SNIP in case of HA (mgmt has to be
               enabled)
14          -   name: "NS_IP"
15            value: "10.217.101.176"
16          # Set username for Nitro
17          # Set log level
18          -   name: "NS_ENABLE_MONITORING"
```



```
            value: "NO"
          -  name: "NS_USER"
            value: "nsroot"
          -  name: "NS_PASSWORD"
            value: "nsroot"
          -  name: "EULA"
            value: "yes"
          -  name: "LOGLEVEL"
            value: "DEBUG"
          -  name: "NS_APPS_NAME_PREFIX"
            value: "BI-"
        args:
          -  --ingress-classes
            bookinfo
          -  --feature-node-watch
            false
        imagePullPolicy: IfNotPresent
<!--NeedCopy-->
```

```
oc apply -f cic-productpage.yaml -n sml
```

1. Accédez à bookinfo.com et cliquez sur Utilisateur normal. La page du produit doit afficher les détails, les avis et les évaluations, qui sont d'autres microservices. HAProxy est responsable de l'acheminement du trafic entre les microservices (Est-Ouest).
2. Supprimez le service devant les détails. Actualisez la page Web Bookinfo et notez que la page du produit n'a pas pu extraire le microservice pour plus de détails.

   ```
   oc delete service details -n sml
   ```

3. Copiez et déployez un service sans tête afin que le trafic provenant de la page du produit vers les détails passe par un CPX. Appelez ce fichier detailsheadless.yaml.

```
apiVersion: v1
kind: Service
metadata:
  name: details
spec:
  ports:
  -  port: 9080
    name: http
  selector:
    app: cpx
<!--NeedCopy-->
```

```
oc apply -f detailsheadless.yaml -n sml
```


1. Copiez et déployez un nouveau service de détails, qui devrait être des noms detailsservice.yaml, pour s'asseoir devant le microservice de détails.

```
apiVersion: v1
kind: Service
metadata:
  name: details-service
  labels:
    app: details-service
    service: details-service
spec:
  clusterIP: None
  ports:
  -  port: 9080
    name: http
  selector:
    app: details
<!--NeedCopy-->
```

```
oc apply -f detailsservice.yaml -n sml
```

1. Exposer le service de détails avec une entrée et le déployer. Appelez ce fichier details-ingress.yaml.

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: details-ingress
  annotations:
   kubernetes.io/ingress.class: "cpx"
   ingress.citrix.com/insecure-port: "9080"
spec:
  rules:
  -  host: details
    http:
      paths:
      -  path:
        backend:
          serviceName: details-service
          servicePort: 9080
<!--NeedCopy-->
```

```
oc apply -f detailsingress.yaml -n sml
```

1. Copiez et déployez le fichier CPXEastWest.yaml.


```
apiVersion: extensions/v1beta1
kind: Deployment
metadata:
  name: cpx
  labels:
    app: cpx
    service: cpx
spec:
  replicas: 1
  template:
    metadata:
      name: cpx
      labels:
        app: cpx
        service: cpx
      annotations:
        NETSCALER_AS_APP: "True"
    spec:
      serviceAccountName: cpx
      containers:
        -  name: reviews-cpx
          image: "quay.io/citrix/citrix-k8s-cpx-ingress:13.0-36.28"
          securityContext:
             privileged: true
          env:
          -  name: "EULA"
            value: "yes"
          -  name: "KUBERNETES_TASK_ID"
            value: ""
          -  name: "MGMT_HTTP_PORT"
            value: "9081"
          ports:
          -  name: http
            containerPort: 9080
          -  name: https
            containerPort: 443
          -  name: nitro-http
            containerPort: 9081
          -  name: nitro-https
            containerPort: 9443
# readiness probe?
          imagePullPolicy: Always
        # Add cic as a sidecar
        -  name: cic
```



```
45            image: "quay.io/citrix/citrix-k8s-ingress-controller:1.2.0"
46            env:
47            -  name: "EULA"
48              value: "yes"
49            -  name: "NS_IP"
50              value: "127.0.0.1"
51            -  name: "NS_PROTOCOL"
52              value: "HTTP"
53            -  name: "NS_PORT"
54              value: "80"
55            -  name: "NS_DEPLOYMENT_MODE"
56              value: "SIDECAR"
57            -  name: "NS_ENABLE_MONITORING"
58              value: "YES"
59            -  name: POD_NAME
60              valueFrom:
61                fieldRef:
62                  apiVersion: v1
63                  fieldPath: metadata.name
64            -  name: POD_NAMESPACE
65              valueFrom:
66                fieldRef:
67                  apiVersion: v1
68                  fieldPath: metadata.namespace
69            args:
70              -  --ingress-classes
71                cpx
72            imagePullPolicy: Always
73  <!--NeedCopy-->
```

```
oc apply -f CPXEastWest.yaml -n sml
```

1. Actualisez bookinfo.com et les détails doivent être tirés des détails MicroService.Un CPX a été déployé avec succès pour le trafic EW proxy.

Citrix Service Mesh Lite avec un VPX/MPX

1. Exécutez les commandes suivantes pour supprimer le CPX utilisé comme proxy EW. Un nouveau fichier est déployé pour configurer le VPX en tant que proxy EW entre la page produit et les microservices de détails.

   ```
   oc delete -f detailsheadless.yaml -n sml
   oc delete -f detailsservice.yaml -n sml
   oc delete -f detailsingress.yaml -n sml
   oc delete -f CPXEastWest.yaml -n sml
   ```


2. Copiez et déployez un service, nommez le fichier DetailsToVPX.yaml, pour renvoyer le trafic depuis la page du produit vers le VPX. Le paramètre IP doit être un VIP gratuit sur Citrix ADC VPX/MPX.

```
---
kind: "Service"
apiVersion: "v1"
metadata:
  name: "details"
spec:
  ports:
    -
      name: "details"
      protocol: "TCP"
      port: 9080
---
kind: "Endpoints"
apiVersion: "v1"
metadata:
  name: "details"
subsets:
  -
    addresses:
      -
        ip: "10.217.101.182" # Ingress IP in MPX
    ports:
      -
        port: 9080
        name: "details"
<!--NeedCopy-->
```

`oc apply -f detailstoVPX.yaml -n sml`

1. Redéployez le detailsservice.yaml devant le microservice de détails.

   `oc apply -f detailsservice.yaml -n sml`

2. Copiez et déployez l'entrée pour exposer le microservice de détails au VPX. Son nom est `detailsVPXingress.yaml`. L'IP frontale doit correspondre au VIP sur l'ADC de niveau 1.

```
apiVersion: extensions/v1beta1
kind: Ingress
metadata:
  name: details-ingress
  annotations:
   kubernetes.io/ingress.class: "vpx"
```



```
    ingress.citrix.com/insecure-port: "9080"
    ingress.citrix.com/frontend-ip: "10.217.101.182"
spec:
  rules:
  -  host: details
    http:
      paths:
      -  path:
        backend:
          serviceName: details-service
          servicePort: 9080
<!--NeedCopy-->
```

```
oc apply -f detailsVPXingress.yaml
```

1. Actualiser bookinfo.com et les détails doivent être tirés du microservice de détails. Un VPX a été déployé avec succès sur le trafic EW proxy.

Migrations Canary

La version Canary est une technique pour réduire le risque d'introduire une nouvelle version logicielle en production en déployant d'abord le changement à un petit sous-ensemble d'utilisateurs, puis en le déployant à une grande base d'utilisateurs après validation réussie. Citrix Adc Integrated Canary Deployment Solution rassemble tous les composants de la livraison continue (CD) et facilite le déploiement de Canary pour les développeurs d'applications. Cette solution utilise Spinnaker comme plate-forme de livraison continue et Kayenta comme plug-in Spinnaker pour l'analyse Canary. Voir Déployer la solution de déploiement Canary intégrée à Citrix ADC.

Une fois qu'une nouvelle version logicielle est entièrement intégrée à la production, supprimez le routeur par défaut dans OpenShift avant de déployer Citrix ADC CPX en tant que routeur dans une topologie Service Mesh Lite. Lorsque vous déployez Citrix ADC CPX en tant que routeur, des conflits de port peuvent survenir avec le routeur par défaut dans OpenShift. Pour supprimer le routeur par défaut, reportez-vous aux étapes 1 et 2 de Déployer Citrix ADC CPX en tant que routeur au sein du cluster OpenShift.

Intégration avec CNCF

Exportateur de mesures Citrix

Vous pouvez utiliser l'exportateur de mesures Citrix ADC et Prometheus-Operator pour surveiller les périphériques d'entrée Citrix ADC VPX ou CPX et les périphériques Citrix ADC CPX (est-ouest). Voir Afficher les métriques des Citrix ADC à l'aide de Prometheus et Grafana.

Modèle de conception validé Citrix ADC et Microsoft Azure

January 8, 2020

Citrix ADC sur Microsoft Azure garantit aux entreprises l'accès à des applications et des ressources sécurisées et optimisées déployées dans le cloud et offre la flexibilité nécessaire pour établir une base de mise en réseau qui s'adapte aux besoins changeants d'un environnement. Cette conception validée guide les organisations à travers la configuration de la fonction Autoscale frontale dans Azure afin de fournir des applications de manière fiable et rentable.

Présentation Citrix ADC VPX

Citrix ADC est un contrôleur de mise à disposition d'applications tout-en-un qui accélère les performances des applications Web internes et externes. La solution matérielle-logicielle réduit les coûts de propriété des applications, optimise l'expérience utilisateur et garantit que les applications sont toujours disponibles en utilisant :

- Services d'équilibrage de charge et gestion du trafic avancés de couche 4-7
- Accélération éprouvée des applications comme la compression HTTP et la mise en cache
- Un pare-feu intégré pour la sécurité des applications
- Déchargement des serveurs pour réduire considérablement les coûts et consolider les serveurs

En tant que leader incontesté de la prestation de services et d'applications, Citrix ADC est déployé sur des milliers de réseaux à travers le monde. Citrix ADC est exploité pour optimiser, sécuriser et contrôler la fourniture des services d'entreprise et de cloud. L'appliance est déployée directement devant les serveurs Web et de base de données. Citrix ADC combine l'équilibrage de charge et la commutation de contenu à grande vitesse, la compression HTTP, la mise en cache du contenu, l'accélération SSL, la visibilité du flux d'applications et un pare-feu puissant pour une plate-forme intégrée et facile à utiliser. Il est beaucoup plus simple de respecter les SLA grâce à une surveillance de bout en bout qui transforme les données réseau en Business Intelligence exploitable. Citrix ADC permet de définir et de gérer les stratégies à l'aide d'un moteur de stratégie déclarative simple sans expertise en programmation requise.

Présentation de Citrix ADC dans Microsoft Azure

L'appliance virtuelle Citrix ADC VPX est disponible sous forme d'image dans le Marketplace Microsoft Azure. Citrix ADC VPX sur Microsoft Azure Resource Manager (ARM) permet aux clients d'utiliser les fonctionnalités de cloud computing Azure et d'appliquer les fonctionnalités d'équilibrage de charge et de gestion du trafic de Citrix ADC pour leurs besoins professionnels. Vous pouvez déployer des in-

stances Citrix ADC VPX sur ARM en tant qu'instances autonomes ou en tant que paires haute disponibilité en mode actif-actif ou en mode veille actif-actif.

Limitations et directives d'utilisation

- L'architecture Azure ne prend pas en charge les fonctionnalités suivantes :
  - Clustering
  - IPv6
  - Gratuitous ARP (GARP)
  - Mode L2
  - VLAN taggé
  - Routage dynamique
  - MAC virtuel (vMac)
  - USIP
  - Connecteur CloudBridge
- La fonctionnalité IP Intranet (IIP) n'est pas prise en charge, car Azure ne fournit pas le pool d'adresses IP requis pour cette fonctionnalité. IIP est fréquemment utilisé dans le déploiement VOIP, SIP ou de connexion initiée par le serveur.
- Si vous vous attendez à devoir arrêter et désallouer temporairement la machine virtuelle Citrix ADC VPX à tout moment, attribuez une adresse IP interne statique lors de la création de la machine virtuelle. Si vous n'affectez pas d'adresse IP interne statique, Azure peut affecter à la machine virtuelle une adresse IP différente chaque fois qu'elle redémarre, et la machine virtuelle risque de devenir inaccessible.
- Dans un déploiement Azure, seuls les modèles Citrix ADC VPX suivants sont pris en charge : VPX 10, VPX 200 et VPX 1000. Ces appliances virtuelles peuvent être déployées sur n'importe quel type d'instance disposant de deux cœurs ou plus et de plus de 2 Go de mémoire. Consultez la section Fiche technique Citrix ADC VPX.
- L' **ID de déploiement** généré par Azure lors du provisioning de la machine virtuelle n'est pas visible par l'utilisateur dans ARM. Vous ne pouvez pas utiliser l'ID de déploiement pour déployer Citrix ADC VPX sur ARM.

Cas d'utilisation

Comparé aux solutions alternatives qui nécessitent le déploiement de chaque service en tant qu'appliance virtuelle distincte, Citrix ADC sur Azure combine les fonctionnalités essentielles de mise à disposition d'applications dans une seule instance VPX. Cela inclut l'équilibrage de charge L4, la gestion du trafic L7, le déchargement du serveur, l'accélération des applications, la sécurité des applications et d'autres services facilement disponibles via Azure Marketplace. En outre, un cadre

politique unique régit tout. Citrix ADC est géré à l'aide du même ensemble puissant d'outils que celui utilisé pour administrer les déploiements Citrix ADC locaux. Le résultat net est que Citrix ADC sur Azure active plusieurs cas d'utilisation convaincants. Citrix ADC prend en charge non seulement les besoins immédiats des entreprises d'aujourd'hui, mais aussi l'évolution continue des infrastructures informatiques héritées vers les datacenters cloud d'entreprise.

Livraison de production

De nombreuses entreprises adoptent activement Azure comme une offre d'infrastructure en tant que service (IaaS) pour la livraison de production d'applications. Maintenant, les entreprises peuvent front-end ces applications avec la même plate-forme de mise en réseau cloud utilisée par les plus grands sites Web et fournisseurs de services cloud au monde. Les capacités étendues de déchargement, d'accélération et de sécurité peuvent être exploitées pour améliorer les performances et réduire les coûts.

Conceptions cloud hybrides

Avec Citrix ADC sur Azure, les clouds hybrides qui couvrent les datacenters d'entreprise et s'étendent dans Azure peuvent bénéficier de la même plate-forme de mise en réseau de cloud Citrix ADC, facilitant considérablement la transition des applications et des charges de travail entre un datacenter privé et Azure. La suite complète de fonctionnalités Citrix ADC, allant de l'équilibrage de charge de base de données intelligent avec Data Stream à la visibilité sans précédent des applications avec AppFlow® et de la surveillance et de la réponse en temps réel avec Action Analytics, peut être exploitée avec Citrix ADC sur Azure.

Continuité des activités

Les entreprises qui souhaitent utiliser Azure dans le cadre de leurs plans de reprise après sinistre et de continuité d'activité peuvent s'appuyer sur l'équilibrage global de charge du serveur Citrix ADC s'exécutant à la fois sur site et au sein d'Azure pour surveiller en permanence la disponibilité et les performances des datacenters d'entreprise et des environnements Azure, garantissant ainsi une sont toujours envoyés à l'emplacement optimal.

Développement et test

Les entreprises exécutant la livraison de production sur site mais utilisant Azure pour le développement et les tests peuvent désormais inclure Citrix ADC dans leurs environnements de test Azure, ce qui accélère le délai de production grâce à une meilleure imitation de la mise en œuvre de la production dans leurs environnements de test. Dans chaque cas d'utilisation, les architectes réseau peuvent également tirer parti de Citrix CloudBridge — configuré soit en tant qu'instance autonome, soit en

tant que fonctionnalité d'une instance Citrix ADC Platinum Edition — pour sécuriser et optimiser la connexion entre les datacenters d'entreprise et Azure Cloud, accélérant ainsi le transfert de données / synchronisation et réduction des coûts réseau

Architecture de réseau

Dans ARM, une machine virtuelle (VM) Citrix ADC VPX réside dans un réseau virtuel. Par défaut, un Citrix ADC VPX provisionné dans Azure fonctionne en mode IP unique décrit dans la section suivante.

Une carte réseau virtuelle est créée sur chaque machine virtuelle Citrix ADC. Le groupe de sécurité réseau configuré dans le réseau virtuel est lié à la carte réseau. Ensemble, ils contrôlent le trafic entrant dans la machine virtuelle et sortant de la machine virtuelle.

Le groupe de sécurité réseau transmet les demandes à l'instance Citrix ADC VPX, et l'instance VPX les envoie aux serveurs. Les réponses des serveurs suivent le même chemin à l'envers. Vous pouvez configurer un groupe de sécurité réseau pour contrôler une seule machine virtuelle VPX, ou avec des sous-réseaux et des réseaux virtuels et contrôler le trafic dans plusieurs déploiements de machines virtuelles VPX.

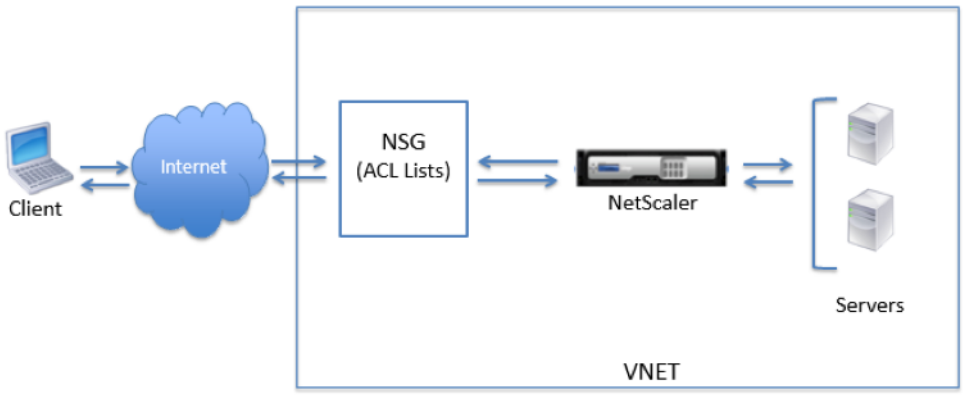
La carte réseau contient des détails de configuration réseau tels que le réseau virtuel, les sous-réseaux, l'adresse IP interne et l'adresse IP publique.

Sur ARM, il est bon de connaître les adresses IP suivantes utilisées pour accéder aux machines virtuelles :

- L'adresse IP publique (PIP) est l'adresse IP Internet configurée directement sur la carte réseau virtuelle de la machine virtuelle Citrix ADC. Le PIP vous permet d'accéder directement à une machine virtuelle à partir du réseau externe sans avoir à configurer les règles entrantes et sortantes sur le groupe de sécurité réseau.
- L'adresse IP Citrix ADC (NSIP) est une adresse IP interne configurée sur la machine virtuelle. Il n'est pas routable.
- L'adresse IP virtuelle (VIP) est configurée à l'aide du NSIP et d'un numéro de port. Les clients accèdent aux services Citrix ADC via l'adresse PIP, et lorsque la demande atteint la carte réseau de la machine virtuelle Citrix ADC VPX ou de l'équilibreur de charge Azure, le VIP est traduit en IP interne (NSIP) et en numéro de port interne.
- L'adresse IP interne est l'adresse IP interne privée de la machine virtuelle à partir du pool d'espace d'adressage du réseau virtuel. Cette adresse IP ne peut pas être atteinte à partir du réseau externe. Cette adresse IP est dynamique par défaut, sauf si vous la définissez sur statique. Le trafic d'Internet est acheminé vers cette adresse selon les règles créées sur le groupe de sécurité réseau. Le groupe de sécurité réseau et la carte réseau envoient sélectivement le bon type de trafic vers le bon port de la carte réseau, ce qui dépend des services configurés sur la machine virtuelle.

> **Remarque :**
>
> Dans ce document, PIP, VIP et PIP de niveau d'instance (ILPIP) signifient la même chose et sont utilisés de manière interchangeable.

La figure suivante montre comment le trafic circule d'un client vers un serveur via une instance Citrix ADC VPX provisionnée dans ARM.



Fonctionnement de Citrix ADC VPX sur Azure

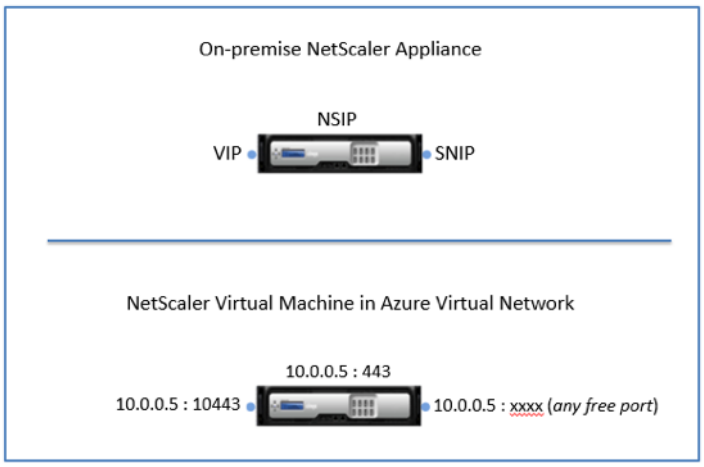
Dans un déploiement local, une instance Citrix ADCVPX nécessite au moins trois adresses IP :

- Adresse IP de gestion, appelée adresse IP Citrix ADC (NSIP)
- Adresse IP de sous-réseau (SNIP) pour communiquer avec la batterie de serveurs
- Adresse IP du serveur virtuel (VIP) pour accepter les demandes des clients

Dans un déploiement Azure, une seule adresse IP (une adresse privée (interne)) est attribuée à une instance lors du provisioning via DHCP.

Pour éviter cette limitation, vous pouvez déployer une instance Citrix ADC VPX dans Azure avec une architecture IP unique. De cette façon, les trois fonctions IP d'un dispositif Citrix ADC sont multiplexées sur une seule adresse IP. Cette adresse IP unique utilise différents numéros de port pour fonctionner comme NSIP, SNIP et VIP.

L'image suivante illustre comment une seule adresse IP est utilisée pour exécuter les fonctions de NSIP, SNIP et VIP.

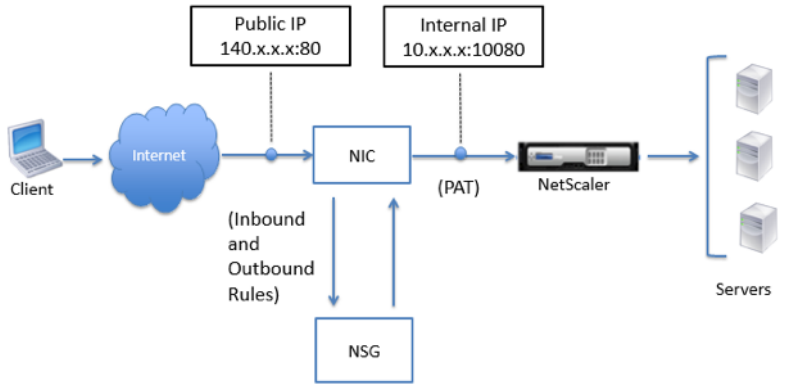


Flux de trafic via la traduction d'adresse de port

Dans un déploiement Azure, lorsque vous provisionnez l'instance Citrix ADC VPX en tant que machine virtuelle (VM), Azure affecte une adresse IP publique et une adresse IP interne (non routable) à la machine virtuelle Citrix ADC. Les règles entrantes et sortantes sont définies sur le groupe de sécurité réseau pour l'instance du Citrix ADC, ainsi qu'un port public et un port privé pour chaque règle définie. L'instance du Citrix ADC écoute sur l'adresse IP interne et le port privé.

Toute demande externe est reçue sur la carte réseau virtuelle de la machine virtuelle Citrix ADC VPX. La carte réseau est liée au groupe de sécurité réseau, qui spécifie la combinaison IP privée et port privé pour où traduire l'adresse et le port de destination de la requête (adresse IP publique et port). ARM effectue la traduction d'adresse de port (PAT) pour mapper l'adresse IP publique et le port à l'adresse IP interne et au port privé de la machine virtuelle Citrix ADC. Enfin, ARM transfère ensuite le trafic à la machine virtuelle.

La figure suivante montre comment Azure effectue PAT pour diriger le trafic vers l'adresse IP interne Citrix ADC et le port privé.



Dans cet exemple, l'adresse IP publique est attribuée à la machine virtuelle est 140.x.x.x et l'adresse IP

interne est 10.x.x.x. Lorsque les règles entrantes et sortantes sont définies, le port HTTP public 80 est défini comme le port sur lequel les demandes client sont reçues. Un port privé correspondant, 10080, est défini comme le port sur lequel la machine virtuelle Citrix ADC écoute. La demande du client est reçue sur l'adresse IP publique 140.x.x.x au port 80. Azure effectue PAT pour mapper cette adresse et ce port à l'adresse IP interne 10.x.x.x sur le port privé 10080 et transmet la demande du client.

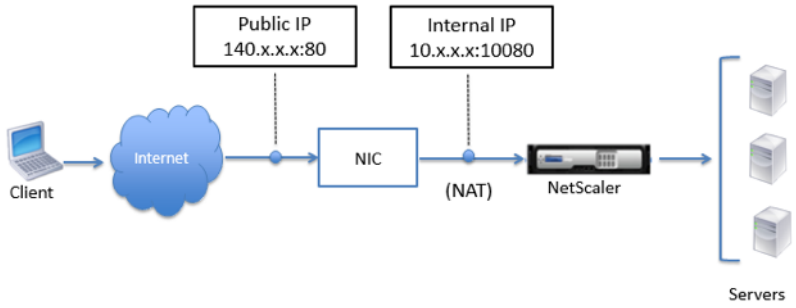
Pour plus d'informations sur les instructions d'utilisation des ports, reportez-vous à laInstructions relatives à l'utilisation des portssection.

Pour plus d'informations sur les groupes de sécurité réseau et les listes de contrôle d'accès, cliquez surici.

Flux de trafic via la traduction d'adresses réseau

Vous pouvez également demander une adresse IP publique (PIP) pour votre machine virtuelle Citrix ADC (niveau d'instance). Si vous utilisez ce PIP direct au niveau de la machine virtuelle, vous n'avez pas besoin de définir des règles entrantes et sortantes pour intercepter le trafic réseau. La demande entrante d'Internet est reçue directement sur la machine virtuelle. Azure effectue la traduction d'adresses réseau (NAT) et transfère le trafic à l'adresse IP interne de l'instance de Citrix ADC.

La figure suivante montre comment Azure effectue la traduction d'adresse réseau pour mapper l'adresse IP interne Citrix ADC.



Dans cet exemple, l'adresse IP publique attribuée au groupe de sécurité réseau est 140.x.x.x et l'adresse IP interne est 10.x.x.x. Lorsque les règles entrantes et sortantes sont définies, le port HTTP public 80 est défini comme le port sur lequel les demandes client sont reçues. Un port privé correspondant, 10080, est défini comme le port sur lequel la machine virtuelle Citrix ADC écoute. La demande du client est reçue sur l'adresse IP publique (140.x.x). Azure effectue la traduction d'adresse réseau pour mapper le PIP à l'adresse IP interne 10.x.x.x sur le port 10080, et transmet la demande du client.

> **Remarque :**
>
> Les machines virtuelles Citrix ADC VPX en haute disponibilité sont contrôlées par des équilibreurs de charge externes ou internes. Ces équilibreurs de charge ont des règles d'entrée en stock

> définies pour contrôler le trafic d'équilibrage de charge. Tout d'abord, le trafic externe est intercepté par ces équilibreurs de charge. Ensuite, le trafic est détourné selon les règles d'équilibrage de charge configurées. Cela inclut les pools principaux, les règles NAT et les sondes d'intégrité définies sur les équilibreurs de charge.

Attribuer plusieurs adresses IP

Une machine virtuelle Azure (VM) est associée à une ou plusieurs interfaces réseau (NIC). Toute carte réseau peut avoir une ou plusieurs adresses IP publiques et privées statiques ou dynamiques qui lui sont assignées. L'attribution de plusieurs adresses IP à une machine virtuelle permet les fonctionnalités suivantes :

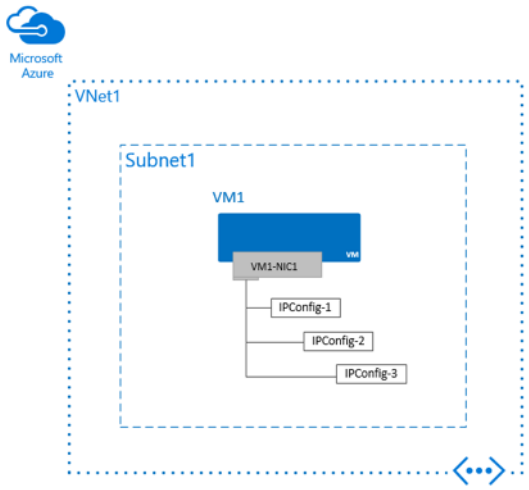
- Hébergement de plusieurs sites Web ou services avec différentes adresses IP et certificats SSL sur un seul serveur.
- Servir d'appliance virtuelle réseau, par exemple un pare-feu ou un équilibreur de charge.
- Possibilité d'ajouter n'importe quelle adresse IP privée pour n'importe quelle des cartes réseau à un pool d'arrière-plan Azure Load Balancer. Dans le passé, seule l'adresse IP principale de la carte réseau principale pouvait être ajoutée à un pool principal. Pour en savoir plus sur l'équilibrage de la charge de plusieurs configurations IP, lisez leArticle sur l'équilibrage de charge de plusieurs configurations IP.

Scénario

Une machine virtuelle avec une seule carte réseau est créée et connectée à un réseau virtuel. La machine virtuelle nécessite trois adresses IP privées différentes et deux adresses IP publiques.

Les adresses IP sont affectées aux configurations IP suivantes :

- IPConfig-1 : Attribue une adresse IP privée dynamique (par défaut) et une adresse IP publique statique.
- IPConfig-2 : Assigne une adresse IP privée statique et une adresse IP publique statique.
- IPConfig-3 : Assigne une adresse IP privée dynamique et aucune adresse IP publique.



Chaque carte réseau connectée à une machine virtuelle est associée à une ou plusieurs configurations IP. Chaque configuration se voit attribuer une adresse IP privée statique ou dynamique. Chaque configuration peut également avoir une ressource d'adresse IP publique associée. Une ressource d'adresse IP publique a une adresse IP publique dynamique ou statique qui lui est assignée. Pour en savoir plus sur les adresses IP dans Azure, lisez l'article Adresses IP dans Azure. Vous pouvez attribuer jusqu'à 250 adresses IP privées à chaque carte réseau. Bien que vous puissiez attribuer plusieurs adresses IP publiques à chaque carte réseau, le nombre d'adresses IP publiques pouvant être utilisées dans un abonnement Azure est limité. Pour plus de détails, consultez l'article Limites Azure.

> **Remarque :**
>
> Plusieurs adresses IP ne peuvent pas être affectées aux ressources créées via le modèle de déploiement classique.

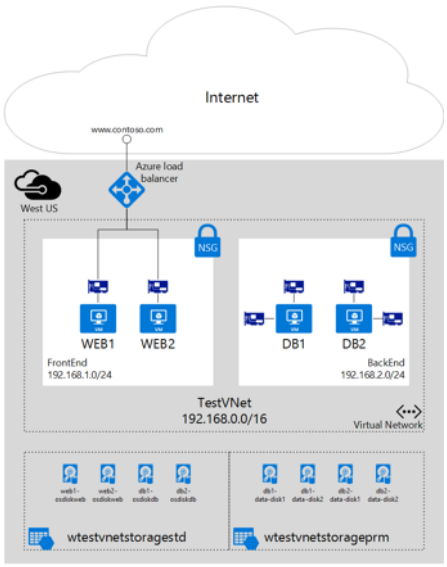
Créer une machine virtuelle avec plusieurs interfaces NIC

Vous pouvez créer des machines virtuelles (VM) dans Azure et attacher plusieurs interfaces réseau (NIC) à chacune de vos machines virtuelles. La multicarte réseau est une exigence pour de nombreuses appliances virtuelles réseau, telles que la livraison d'applications et les solutions d'optimisation WAN. Multi-NIC offre également plus de fonctionnalités de gestion du trafic réseau. Les exemples incluent l'isolement du trafic entre une carte réseau frontale et une carte réseau principale, et la séparation du trafic du plan de données du trafic du trafic du plan de gestion.

Scénario

Ce document décrit un déploiement qui utilise plusieurs cartes réseau dans des machines virtuelles dans un scénario spécifique. Dans ce scénario, vous disposez d'une charge de travail IaaS à deux niveaux hébergée dans Azure. Chaque niveau est déployé dans son propre sous-réseau dans un réseau virtuel (VNet). Le niveau frontal est composé de plusieurs serveurs Web, regroupés dans un

ensemble d'équilibrage de charge pour une haute disponibilité. Le niveau principal est composé de plusieurs serveurs de base de données. Ces serveurs de base de données sont déployés avec deux cartes réseau chacune, l'une pour l'accès à la base de données et l'autre pour la gestion. Le scénario inclut également des groupes de sécurité réseau pour contrôler le trafic autorisé à chaque sous-réseau et une carte réseau dans le déploiement. La figure suivante illustre l'architecture de base de ce scénario.



Instructions relatives à l'utilisation des ports

Vous pouvez configurer des règles supplémentaires entrantes et sortantes dans un groupe de sécurité réseau lors de la création de la machine virtuelle Citrix ADC ou après le provisioning de la machine virtuelle. Chaque règle entrante et sortante est associée à un port public et à un port privé.

Avant de configurer les règles de groupe de sécurité réseau, notez les instructions suivantes concernant les numéros de port que vous pouvez utiliser :

1. Les ports suivants sont réservés par la machine virtuelle Citrix ADC. Vous ne pouvez pas les définir en tant que ports privés lorsque vous utilisez l'adresse IP publique pour les requêtes provenant d'Internet.

   Ports 21, 22, 80, 443, 8080, 67, 161, 179, 500, 520, 3003, 3008, 3009, 3010, 3011, 4001, 5061, 9000, 7000.

   Toutefois, si vous souhaitez que des services Internet tels que le VIP utilisent un port standard (par exemple, le port 443), vous devez créer un mappage de ports à l'aide du groupe de sécurité réseau. Le port standard est ensuite mappé à un autre port configuré sur Citrix ADC pour ce service VIP.

   Par exemple, un service VIP peut s'exécuter sur le port 8443 sur l'instance du Citrix ADC, mais être mappé sur le port public 443. Ainsi, lorsque l'utilisateur accède au port 443 via l'IP publique,

la requête est dirigée vers le port privé 8443.

2. L'adresse IP publique ne prend pas en charge les protocoles dans lesquels le mappage de ports est ouvert dynamiquement, tels que FTP passif ou ALG.
3. L'équilibrage de charge Azure ne fonctionne pas avec l'adresse IP publique. La haute disponibilité ne fonctionne pas pour le trafic qui utilise PIP associé à l'instance VPX au lieu de PIP configuré sur l'équilibreur de charge. Pour plus d'informations sur la configuration de Citrix ADC VPX HA dans ARM, consultez Configuration de Citrix ADC VPX en mode haute disponibilité dans Azure.
4. Dans un déploiement Citrix ADC Gateway, vous n'avez pas besoin de configurer une adresse SNIP, car le NSIP peut être utilisé en tant que SNIP lorsqu'aucun SNIP n'est configuré.

> **Remarque :** Vous devez configurer l'adresse VIP à l'aide de l'adresse NSIP et d'un numéro de port non standard. Pour la configuration de rappel sur le serveur principal, le numéro de port VIP doit être spécifié avec l'URL VIP (par exemple, url : port).
> **Remarque :** dans ARM, une machine virtuelle Citrix ADC VPX est associée à deux adresses IP. Adresse IP publique et adresse IP interne. Pendant que le trafic externe se connecte au PIP, l'adresse IP interne ou le NSIP n'est pas routable. Pour configurer VIP dans VPX, utilisez cette combinaison d'adresse IP interne et de numéro de port.
> **Exemple :** Si le nom de domaine complet du serveur virtuel VPN est vip.test.com et que le serveur virtuel VPN s'exécute sur le port 8443, l'URL de rappel est :https://vip.test.com:8443 .

Étapes de configuration

Les étapes suivantes décrivent comment configurer les groupes de ressources, les groupes de sécurité, les réseaux virtuels et les configurations de traduction nécessaires pour avoir un ADC fonctionnel.

Provisioning du groupe de ressources

Sur lePage Portail Microsoft Azure, connectez-vous au portail Azure Resource Manager avec votre nom d'utilisateur et votre mot de passe. (Dans le portail ARM, le fait de cliquer sur une option dans un volet ouvre un nouveau volet à droite. Naviguez d'un volet à l'autre pour configurer votre appareil.)

Créez un groupe de ressources pour servir de conteneur pour toutes vos ressources. Utilisez le groupe de ressources pour déployer, gérer et surveiller vos ressources en tant que groupe.

Créer un groupe de sécurité réseau

Créez un groupe de sécurité réseau pour affecter des règles entrantes et sortantes pour contrôler le trafic entrant et sortant au sein du réseau virtuel. Les groupes de sécurité réseau vous permettent de

définir des règles de sécurité pour une seule machine virtuelle et également de définir des règles de sécurité pour un sous-réseau virtuel.

Configuration d'un réseau virtuel et de sous-réseaux

Les réseaux virtuels dans ARM fournissent une couche de sécurité et d'isolement à vos services. Les machines virtuelles et les services qui font partie d'un même réseau virtuel peuvent accéder les uns aux autres.

Par exemple, créez un réseau virtuel avec un bloc CIDR réservé de 192.168.0.0/16 et deux sous-réseaux ayant respectivement les blocs CIDR 192.168.1.0/24 et 192.168.2.0/24.

1. Dans le volet **Créer un réseau virtuel** , entrez les valeurs suivantes, puis cliquez sur **Créer** .
    - Nom du réseau virtuel
    - Espace d'adressage : saisissez le bloc d'adresse IP réservé pour le réseau virtuel
    - Sous-réseau : saisissez le nom du premier sous-réseau (vous créez le deuxième sous-réseau plus tard dans cette étape)
    - Plage d'adresses de sous-réseau : saisissez le bloc d'adresses IP réservé du sous-réseau
    - Groupe de ressources : sélectionnez le groupe de ressources créé précédemment dans la liste déroulante

Configuration du deuxième sous-réseau

1. Sélectionnez le réseau virtuel nouvellement créé dans le volet **Toutes les ressources** et, dans le volet **Paramètres** , cliquez sur **Sous-réseaux** .
2. Cliquez sur **+ Sous-réseau** et créez le second sous-réseau en entrant les détails suivants.
    - Nom du deuxième sous-réseau
    - Plage d'adresses : saisissez le bloc d'adresses IP réservées du deuxième sous-réseau
    - Groupe de sécurité réseau : sélectionnez le groupe de sécurité réseau dans la liste déroulante

Configuration d'un compte de stockage

Le stockage de l'infrastructure ARM IaaS inclut tous les services où nous pouvons stocker des données sous forme de blobs, de tables, de files d'attente et de fichiers. Vous pouvez également créer des applications à l'aide de ces formes de données de stockage dans ARM.

Créer un compte de stockage pour stocker toutes vos données

1. Cliquez sur **+ Nouveau > Stockage > Compte de stockage**.

2. Dans le volet **Créer un compte de stockage** , entrez les détails suivants :
    - Nom du compte
    - Mode de déploiement : assurez-vous de sélectionner **Resource Manager**
    - Type de compte : sélectionnez **Usage général** dans la liste déroulante
    - Réplication : sélectionnez **Stockage localement redondant** dans la liste déroulante
    - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
3. Cliquez sur **Créer**.

Configuration d'un jeu de disponibilité

Un jeu de disponibilité garantit qu'au moins une machine virtuelle est maintenue en service en cas de maintenance planifiée ou non planifiée. Deux machines virtuelles ou plus sous le même « jeu de disponibilité » sont placées sur différents domaines de panne pour obtenir des services redondants.

1. Cliquez sur **+ Nouveau** et recherchez le jeu de disponibilité.
2. Sélectionnez Entité **Jeu de disponibilité** dans la liste. Cliquez sur **Créer**.
3. Dans le volet **Créer un jeu de disponibilité** , entrez les détails suivants :
    - Nom de l'ensemble
    - Groupe de ressources : sélectionnez le groupe de ressources nouvellement créé dans la liste déroulante
4. Cliquez sur **Créer**

Provisioning de l'instance de Citrix ADC

Créez une instance de Citrix ADC VPX dans le réseau virtuel. Ensuite, procurez-vous l'image Citrix ADC VPX à partir de la Place de marché Azure. Utilisez le portail Azure Resource Manager pour créer une instance Citrix ADC VPX.

Avant de commencer à créer l'instance Citrix ADC VPX, assurez-vous que vous avez créé un réseau virtuel avec les sous-réseaux requis dans lesquels l'instance réside. Vous pouvez créer des réseaux virtuels pendant le provisioning de machines virtuelles, mais sans la possibilité de créer différents sous-réseaux. Pour plus d'informations, consultezCréer un réseau virtuel à l'aide du portail Azurel'article.

Facultatif : configurez le serveur DNS et la connectivité VPN pour permettre à une machine virtuelle d'accéder aux ressources Internet.

> **Remarque :** Citrix vous recommande de créer un groupe de ressources, un groupe de sécurité réseau, un réseau virtuel et d'autres entités avant de provisionner la machine virtuelle Citrix ADC VPX. De cette façon, les informations réseau sont disponibles pendant le provisioning.

1. Cliquez sur **+ Nouveau > Mise en réseau**.
2. Cliquez sur **Voir tout** et dans le volet **Mise en réseau** , cliquez sur **Citrix ADC VPX Apportez votre propre licence** .
3. Cliquez sur **Créer**.

   > **Remarque :** Pour trouver rapidement n'importe quelle entité sur le portail ARM, vous pouvez également taper le nom de l'entité dans la zone de recherche Marketplace Azure et appuyer sur`<Enter>` . Tapez **Citrix ADC** dans la zone de recherche pour rechercher les images Citrix ADC.

4. Sélectionnez **Citrix ADC 12.0 VPX Apportez votre propre licence**.
5. Remplissez vos coordonnées.
6. Achetez et déployez mon Citrix ADC, après avoir passé la validation.
7. Il est recommandé de définir vos adresses IP sur Static.

> **Remarque :** Assurez-vous de sélectionner la dernière image. Votre image Citrix ADC peut avoir le numéro de version dans le nom.

Créer une machine virtuelle avec plusieurs adresses IP à l'aide de PowerShell

Les étapes suivantes expliquent comment créer un exemple de machine virtuelle avec plusieurs adresses IP, comme décrit dans le scénario. Modifiez les noms de variables et les types d'adresses IP selon les besoins de votre implémentation.

Les étapes de configuration couvertes sont les suivantes :

1. Créer une machine virtuelle avec plusieurs adresses IP
2. Ajouter des adresses IP à une machine virtuelle
3. Ajouter des adresses IP à un système d'exploitation VM
4. Validation (Windows)
5. Validation (Linux)

Veuillez vous référer à la documentation Microsoft Azure suivante :Affecter plusieurs adresses IP à des machines virtuelles à l'aide de PowerShell.

Configurer la traduction du port Citrix ADC

1. Cliquez sur **Interfaces réseau** pour votre machine virtuelle, Citrix ADC.
2. Cliquez sur votre **groupe de sécurité réseau**.
3. Cliquez sur **Règles de sécurité entrantes**.
4. Autoriser **SSH** et **HTTP** dans le groupe de sécurité pour les connexions entrantes.

À ce stade, vous pouvez vous connecter à l'instance de Citrix ADC et configurer les fonctionnalités et les paramètres souhaités pour votre environnement Azure.

> **Remarque :** lors de la première connexion à Citrix ADC, l'Assistant peut demander une adresse IP de sous-réseau. Ceci n'est pas requis sur les instances Citrix ADC Azure car elles n'utilisent qu'une seule adresse IP pour toutes les fonctions. Ignorez cette étape lorsque vous y êtes invité et passez à la page de connexion de configuration par défaut.

Portail Microsoft Azure Resource Manager

L'infrastructure de votre application est généralement composée de nombreux composants, notamment d'une machine virtuelle, d'un compte de stockage et d'un réseau virtuel, d'une application web, d'une base de données, d'un serveur de base de données et de services tiers. Ces composants ne sont pas considérés comme des entités distinctes. Au lieu de cela, vous les voyez comme des parties liées et interdépendantes d'une seule entité. Vous souhaitez les déployer, les gérer et les surveiller en tant que groupe. Azure Resource Manager vous permet de travailler avec les ressources de votre solution en tant que groupe. Vous pouvez déployer, actualiser ou supprimer toutes les ressources de votre solution en une seule opération coordonnée. Vous utilisez un modèle pour le déploiement et ce modèle peut fonctionner pour différents environnements tels que le test, la mise en scène et la production. Le Gestionnaire de ressources fournit des fonctionnalités de sécurité, d'audit et de balisage pour vous aider à gérer vos ressources après le déploiement.

Terminologie

Si vous êtes nouveau dans Azure Resource Manager, il existe certains termes que vous ne connaissez peut-être pas :

- **resource** - Un élément gérable qui est disponible via Azure. Certaines ressources courantes sont une machine virtuelle, un compte de stockage, une application Web, une base de données et un réseau virtuel, mais il y en a beaucoup plus.
- **groupe de ressources** - Conteneur qui contient des ressources associées pour une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous souhaitez gérer en tant que groupe. Vous décidez de la manière dont vous souhaitez allouer des ressources aux groupes de ressources en fonction de ce qui est le plus pertinent pour votre organisation. Reportez-vous à la section Groupes de ressources.

- **fournisseur de ressources** : service qui fournit les ressources que vous pouvez déployer et gérer via Resource Manager. Chaque fournisseur de ressources propose des opérations pour travailler avec les ressources déployées. Certains fournisseurs de ressources courants sont`Microsoft.Compute`, qui fournit la ressource de machine virtuelle`Microsoft.Storage`, qui fournit la ressource de compte de stockage et`Microsoft.Web`, qui fournit des ressources liées à applications web. Voir Fournisseurs de ressources.
- **Modèle Gestionnaire de ressources** : fichier JSON (JavaScript Object Notation) qui définit une ou plusieurs ressources à déployer dans un groupe de ressources. Il définit également les dépendances entre les ressources déployées. Le modèle peut être utilisé pour déployer les ressources de manière cohérente et répétée. Voir Déploiement de modèles.
- **syntaxe déclarative** - Syntaxe qui vous permet d'indiquer « Voici ce que j'ai l'intention de créer » sans avoir à écrire la séquence des commandes de programmation pour le créer. Le modèle Gestionnaire de ressources est un exemple de syntaxe déclarative. Dans le fichier, vous définissez les propriétés de l'infrastructure à déployer sur Azure.

Référence : Présentation d'Azure Resource Manager

Présentation de la multicarte réseau Citrix ADC

Les instances virtuelles Citrix ADC s'exécutant sur la plate-forme Azure sont capables d'attacher plusieurs cartes réseau virtuelles à un dispositif Citrix ADC virtuel autonome.

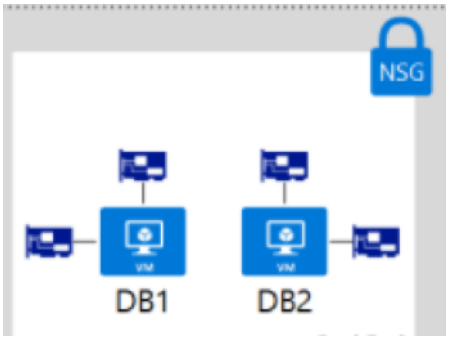
Il s'agit d'un scénario courant lorsque des architectures distribuées sont souhaitées dans Azure, telles que les niveaux d'application et les niveaux de base de données.

Un deuxième cas d'utilisation commun Citrix ADC pour plusieurs cartes réseau est le désir de séparer les zones réseau dans l'environnement Azure. Un exemple de ségrégation pourrait être de permettre au trafic provenant de l'Internet de se terminer sur une interface (DMZ ou Public), et les services internes Web et Application d'être privés.

Dans ce scénario de mise en réseau à deux bras, l'appliance virtuelle Citrix ADC requiert au moins deux cartes réseau virtuelles pour être présentées. Une carte réseau virtuelle pour le réseau public et une carte réseau virtuelle pour le réseau privé.

En outre, la configuration multi-carte réseau dans Azure nécessite l'utilisation de plusieurs sous-réseaux pour accueillir les cartes réseau séparées. Ce composant est configuré à l'aide du composant VNET du portail Azure.

Exemple : plusieurs cartes réseau virtuelles attachées à une machine virtuelle Azure



> **Remarque :** différentes tailles de machines virtuelles prennent en charge un nombre variable de cartes réseau, alors dimensionnez votre machine virtuelle en conséquence. https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes

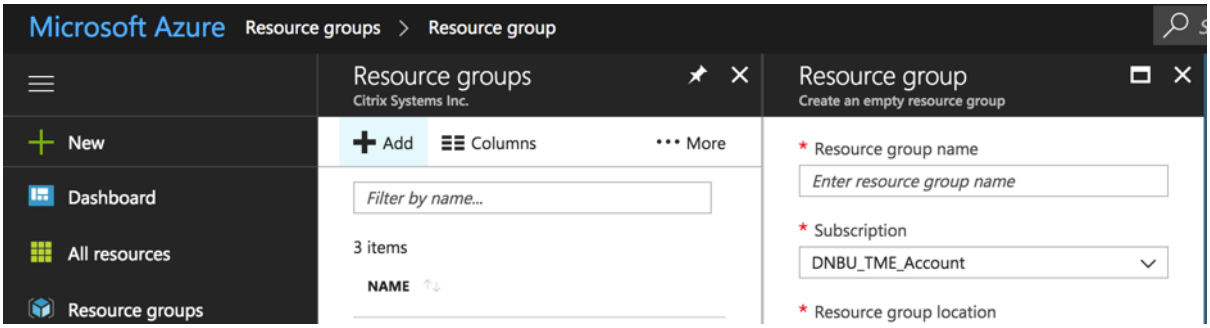
Configuration multi-carte réseau Citrix ADC

Les configurations suivantes décrivent comment créer facilement le sous-réseau et les réseaux virtuels nécessaires pour avoir une configuration multi-carte réseau sur un ADC.

Créer le groupe de ressources

PowerShellCopy

```
New-AzureRmResourceGroup -Name "myResourceGroup" -Location "EastUS"
<!--NeedCopy-->
```



Créer le VNET et les sous-réseaux

Un scénario courant est qu'un réseau virtuel ait deux sous-réseaux ou plus. Un sous-réseau peut être pour le trafic frontal, l'autre pour le trafic principal. Pour vous connecter aux deux sous-réseaux, vous utilisez ensuite plusieurs cartes réseau sur votre machine virtuelle.

Définissez deux sous-réseaux de réseau virtuel à l'aide de`New-AzureRmVirtualNetworkSubnetConfig`. L'exemple suivant définit les sous-réseaux pour`mySubnetFrontEnd` et`mySubnetBackEnd` :

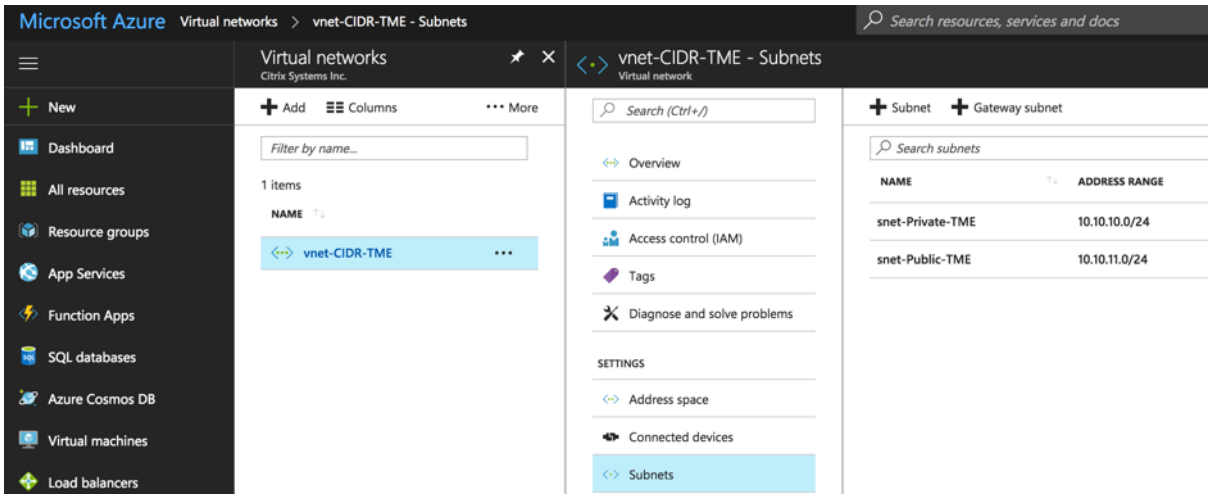
PowerShellCopy


```
$mySubnetFrontEnd = New-AzureRmVirtualNetworkSubnetConfig -Name "
    mySubnetFrontEnd" `
 -AddressPrefix "192.168.1.0/24"
$mySubnetBackEnd = New-AzureRmVirtualNetworkSubnetConfig -Name "
    mySubnetBackEnd" `
 -AddressPrefix "192.168.2.0/24"
 <!--NeedCopy-->
```

Créez votre réseau virtuel et vos sous-réseaux avecNew-AzureRmVirtualNetwork. L'exemple suivant crée un réseau virtuel nommé MyVNet :

PowerShellCopy

```
$myVnet = New-AzureRmVirtualNetwork -ResourceGroupName "myResourceGroup
    " `
 -Location "EastUs" `
 -Name "myVnet" `
 -AddressPrefix "192.168.0.0/16" `
 -Subnet $mySubnetFrontEnd,$mySubnetBackEnd
 <!--NeedCopy-->
```



Créer le groupe de sécurité réseau

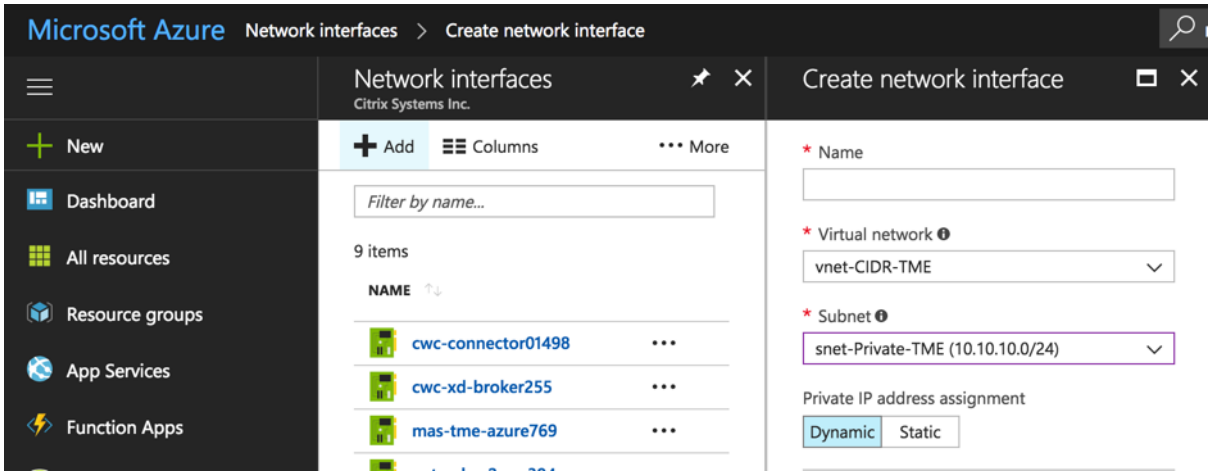
En règle générale, vous créez également un groupe de sécurité réseau pour filtrer le trafic réseau vers la machine virtuelle et un équilibreur de charge pour distribuer le trafic sur plusieurs machines virtuelles.

Créer et configurer des cartes virtuelles

Créez deux cartes réseau à l'aide de`New-AzureRmNetworkInterface`. Attachez une carte réseau au sous-réseau frontal et une carte réseau au sous-réseau principal. L'exemple suivant crée des cartes réseau nommées myNic1 et myNic2 :

PowerShellCopy

```
$frontEnd = $myVnet.Subnets|?{
 $\_.Name -eq 'mySubnetFrontEnd' }

$myNic1 = New-AzureRmNetworkInterface -ResourceGroupName "
    myResourceGroup" `
 -Name "myNic1" `
 -Location "EastUs" `
 -SubnetId $frontEnd.Id
$backEnd = $myVnet.Subnets|?{
 $\_.Name -eq 'mySubnetBackEnd' }

$myNic2 = New-AzureRmNetworkInterface -ResourceGroupName "
    myResourceGroup" `
 -Name "myNic2" `
 -Location "EastUs" `
 -SubnetId $backEnd.Id
 <!--NeedCopy-->
```



Créer une machine virtuelle et attacher des vNIC

Commencez maintenant à construire votre configuration de machine virtuelle. Chaque taille de machine virtuelle a une limite pour le nombre total de cartes réseau que vous pouvez ajouter à une machine virtuelle. Pour plus d'informations, voir tailles de machines virtuelles Windows.

Joignez les deux cartes réseau que vous avez créées précédemment avec`Add-AzureRmVMNetworkInterface` :

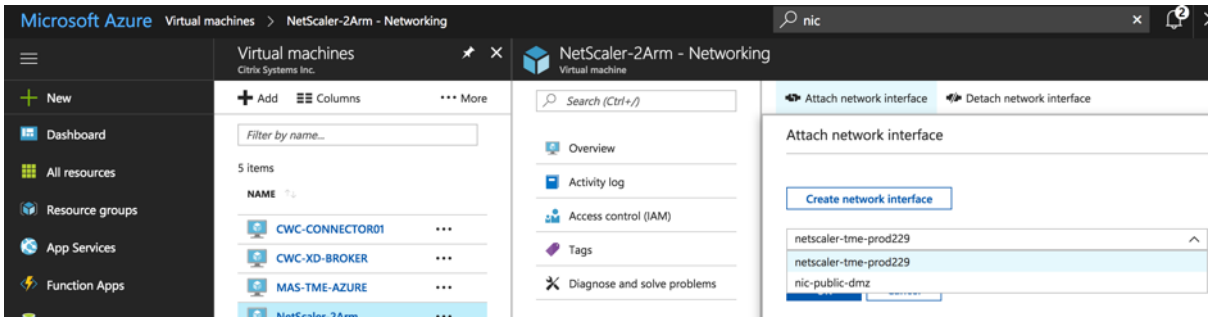
PowerShellCopy

```
$vmConfig = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $myNic1.Id
    -Primary
$vmConfig = Add-AzureRmVMNetworkInterface -VM $vmConfig -Id $myNic2.Id
<!--NeedCopy-->
```

Enfin, créez votre machine virtuelle avec`New-AzureRmVM` :

PowerShellCopy

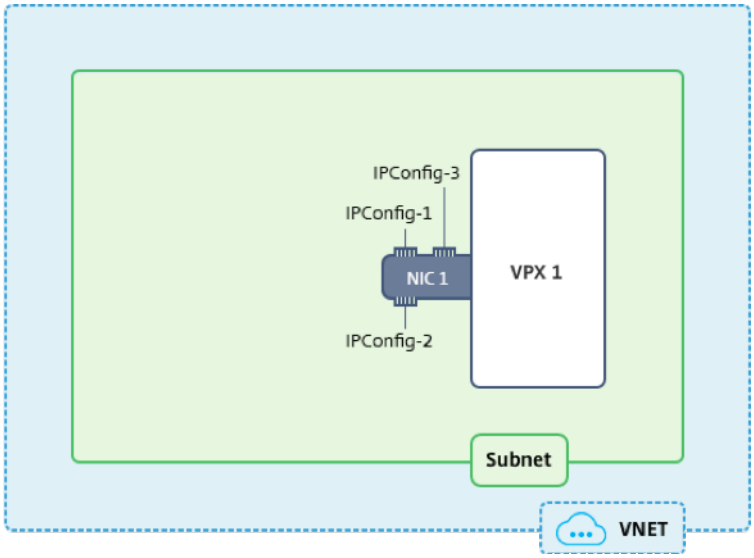
```
New-AzureRmVM -VM $vmConfig -ResourceGroupName "myResourceGroup" -
    Location "EastUs"
<!--NeedCopy-->
```



Vue d’ensemble des adresses IP multiples de Citrix ADC

Dans ce cas d’utilisation, une appliance Citrix ADC VPX autonome peut être configurée avec une ou plusieurs cartes réseau virtuelles connectées à un réseau virtuel (VNET). La vNIC est associée à trois configurations IP (ipconfig), chacune ayant un but différent.

Exemple : plusieurs VIP attachés à un vNIC



Lorsque vous affectez plusieurs configurations IP à une carte réseau, une configuration doit être affectée en tant que -Primary.

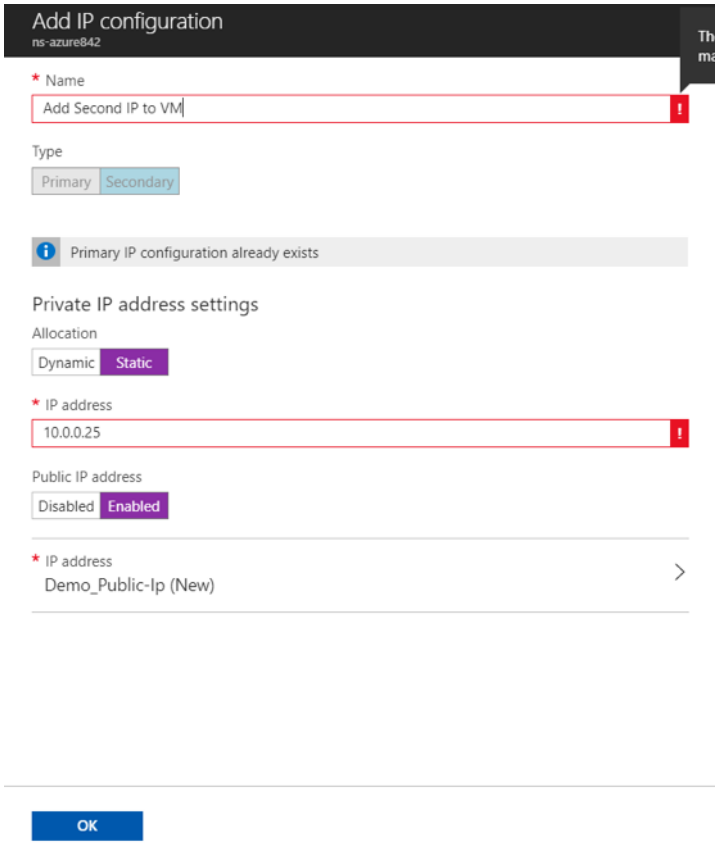
```
$MyNIC.IpConfigurations | Format-Table Name, PrivateIPAddress,
   PublicIPAddress, Primary
<!--NeedCopy-->
```

> **Remarque** :
>
> Les adresses IP publiques ont des frais nominaux. Pour en savoir plus sur la tarification des adresses IP, consultez la page Tarification des adresses IP. Le nombre d'adresses IP publiques pouvant être utilisées dans un abonnement est limité. Pour en savoir plus sur les limites, consultez l'article Limites Azure.

Ajouter une adresse IP privée

Pour ajouter une adresse IP privée à une carte réseau, vous devez créer une configuration IP. La commande suivante crée une configuration avec une adresse IP statique 10.0.0.7. Lorsque vous spécifiez une adresse IP statique, il doit s'agir d'une adresse inutilisée pour le sous-réseau. Nous vous recommandons de tester d'abord l'adresse pour vous assurer qu'elle est disponible en entrant la`Test-AzureRmPrivateIPAddressAvailability -IPAddress 10.0.0.7 -VirtualNetwork $myVnet` commande. Si l'adresse IP est disponible, la sortie est renvoyée`True`. Si l'adresse n'est pas disponible, la sortie renvoie`False`et inclut une liste d'adresses disponibles.

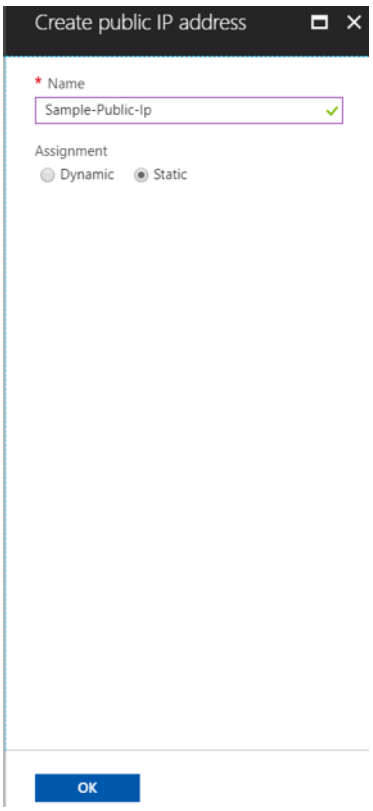
```
Add-AzureRmNetworkInterfaceIpConfig -Name IPConfig-4 -NetworkInterface
    `
$MyNIC -Subnet $Subnet -PrivateIpAddress 10.0.0.7
<!--NeedCopy-->
```

Ajouter une adresse IP publique

Une adresse IP publique est ajoutée en associant une ressource d'adresse IP publique à une nouvelle configuration IP ou à une configuration IP existante. Suivez les étapes décrites dans l'une des sections suivantes, selon vos besoins.

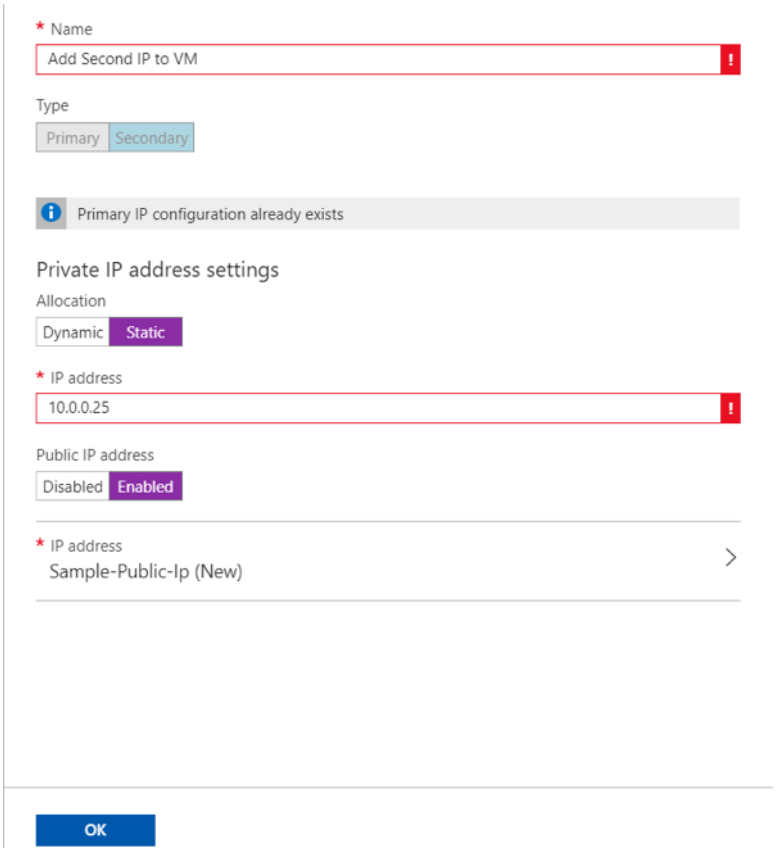
```
$MyPublicIp3 = New-AzureRmPublicIpAddress `
 -Name "MyPublicIp3" `
 -ResourceGroupName $RgName `
 -Location $Location -AllocationMethod Static
 <!--NeedCopy-->
```

Associer la ressource d'adresse IP publique à une machine virtuelle existante

Une ressource d'adresse IP publique ne peut être associée qu'à une configuration IP qui n'a pas déjà associé

```
Set-AzureRmNetworkInterfaceIpConfig `
 -Name IpConfig-3 `
 -NetworkInterface $mynic `
 -Subnet $Subnet `
 -PublicIpAddress $myPublicIp3
<!--NeedCopy-->
```

Présentation de Citrix ADC HA

Vous pouvez déployer une paire d'appliances virtuelles Citrix ADC avec plusieurs cartes réseau dans une configuration active-passive haute disponibilité (HA) sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP. Un déploiement actif-passif nécessite :

- Configuration de réseau indépendant HA (Independent Network Configuration)
- L'équilibrage de charge Azure (ALB) en mode retour direct du serveur (DSR)

Tout le trafic passe par le nœud principal. Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

Dans un déploiement actif-passif, les adresses IP publique flottante (PIP) ALB sont ajoutées en tant qu'adresses VIP dans chaque nœud Citrix ADC. Dans la configuration HA-INC, les adresses VIP sont flottantes et les adresses SNIP sont spécifiques à l'instance. ALB surveille chaque instance de Citrix ADC en envoyant une sonde d'intégrité toutes les 5 secondes. L'ADC redirige le trafic uniquement vers l'instance qui envoie la réponse des sondes d'intégrité à intervalles réguliers. Ainsi, dans une configuration HA, le nœud principal répond aux sondes d'intégrité et le nœud secondaire ne le fait pas. Si l'instance principale manque deux sondes d'intégrité consécutives, ALB ne redirige pas le trafic vers cette instance. Lors du basculement, la nouvelle base commence à répondre aux sondes d'intégrité et l'ALB redirige le trafic vers elle. Le temps de basculement standard de Citrix ADC HA est de trois

secondes. Le temps de basculement total qui peut prendre pour la commutation de trafic peut être de 13 secondes maximum.

Vous pouvez déployer une paire Citrix ADC en mode HA actif-passif de deux façons à l'aide de :

- Modèle HA standard Citrix ADC : utilisez cette option pour configurer une paire HA avec l'option par défaut de trois sous-réseaux et de six cartes réseau.
- Commandes Windows PowerShell : utilisez cette option pour configurer une paire HA en fonction des exigences de votre sous-réseau et de votre carte réseau.

Configuration de Citrix ADC HA - PowerShell

VérifiezConfiguration d'une configuration HA avec plusieurs adresses IP et cartes réseau à l'aide de commandes PowerShellles commandes Azure PowerShell.

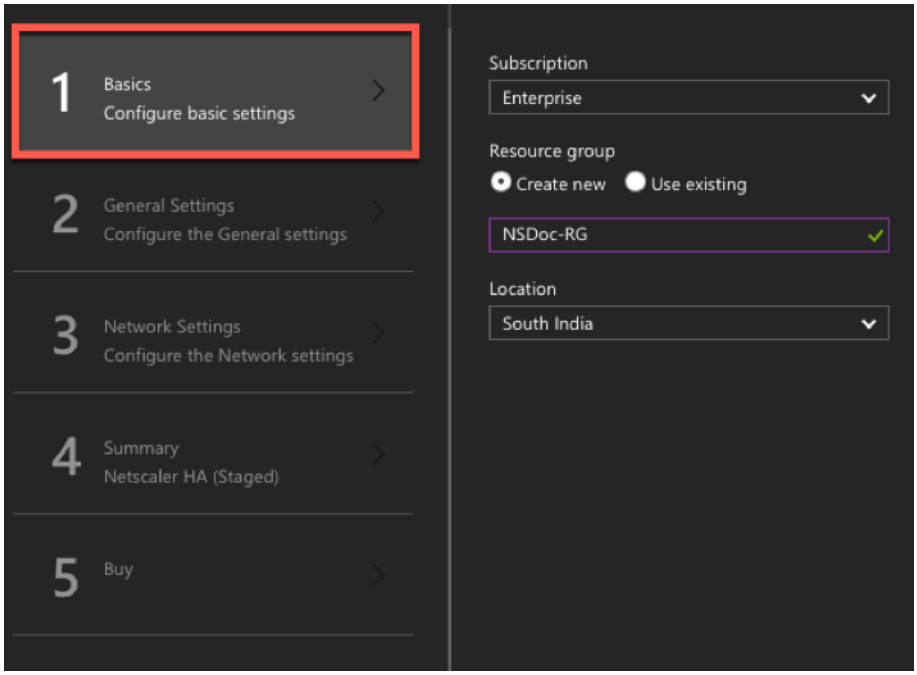
Configuration de Citrix ADC HA - Portail Azure

Vous pouvez déployer rapidement et efficacement une paire d'instances Citrix ADC en mode HA-INC à l'aide du modèle standard. Le modèle crée deux nœuds, avec trois sous-réseaux et six cartes réseau. Les sous-réseaux sont destinés au trafic de gestion, client et côté serveur, et chaque sous-réseau dispose de deux cartes réseau pour les deux instances VPX.

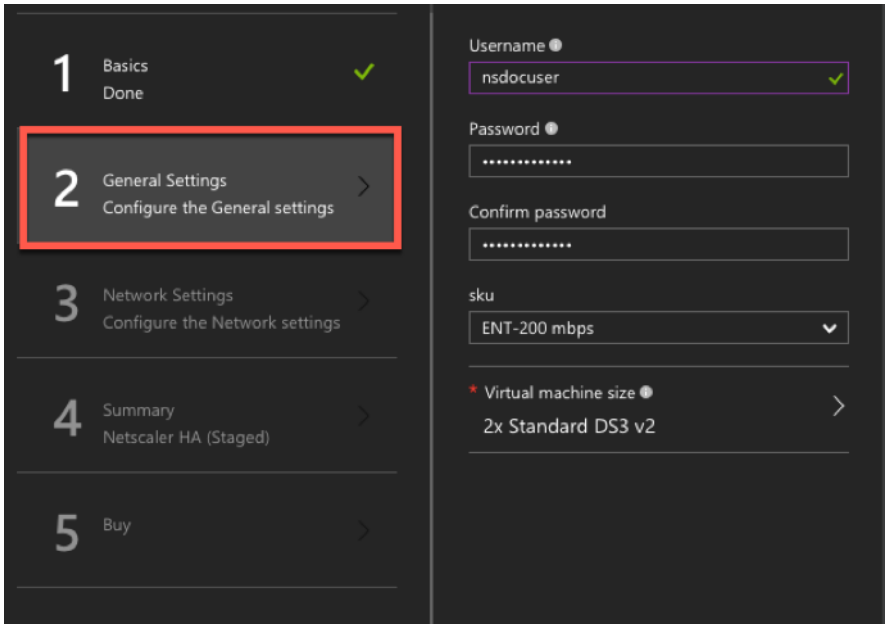
L'Modèle de paire Citrix ADC 12.0 HAest disponible sur la Place de marché Azure.

Pour utiliser le modèle :

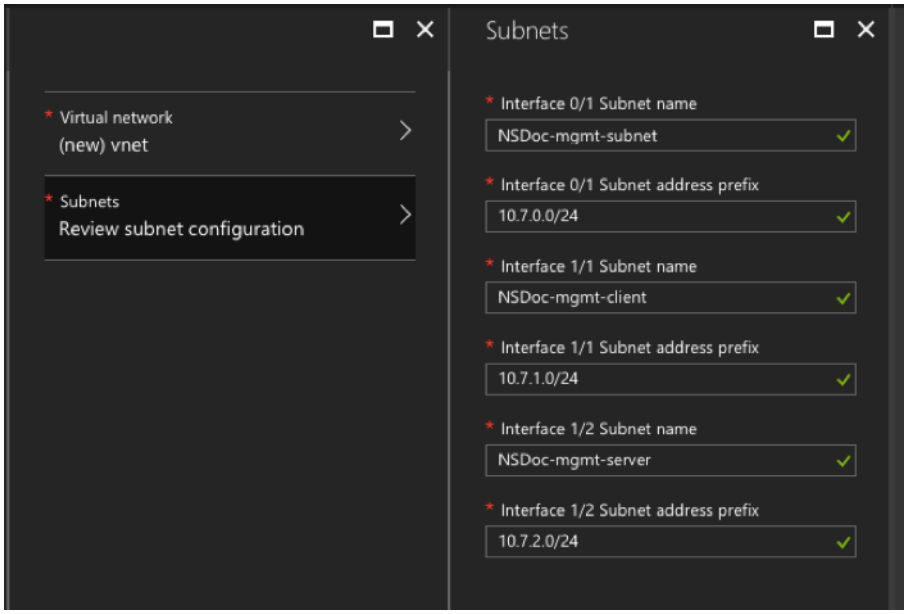
1. À partir de la Place de marché Azure, sélectionnez et lancez le modèle de solution Citrix. Le modèle apparaît.
2. Assurez-vous que le type de déploiement est **Gestionnaire de ressources** et sélectionnez **Créer** .
3. La page Notions de base s'affiche. Créez un **groupe de ressources** et sélectionnez **OK** .



4. La page **Paramètres généraux** s'affiche. Tapez les détails et sélectionnez **OK**.



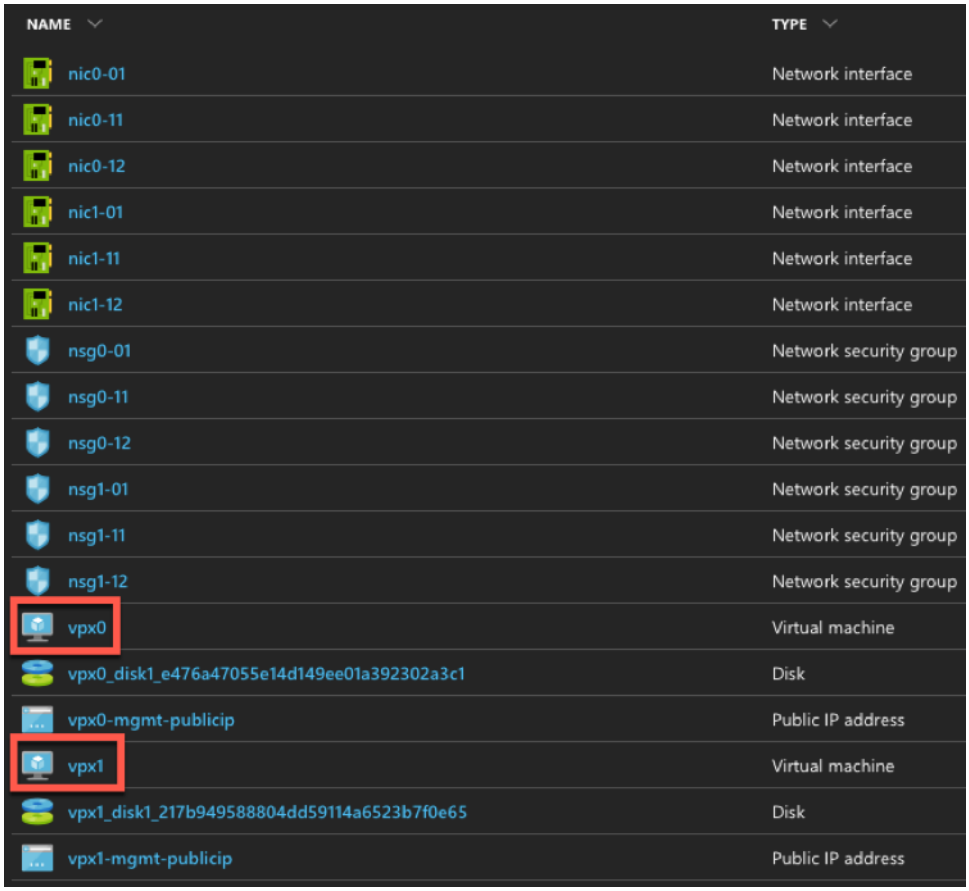
5. La page **Paramètres réseau** s'affiche. Vérifiez les configurations de vnet et de sous-réseau, modifiez les paramètres requis et sélectionnez **OK**.



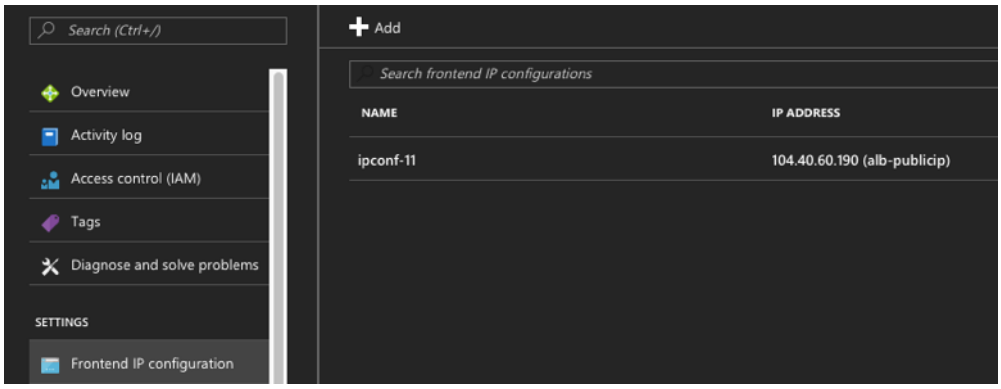
6. La page **Récapitulatif** s'affiche. Vérifiez la configuration et modifiez en conséquence. Sélectionnez **OK** pour confirmer.
7. La page **Acheter** apparaît. Sélectionnez **Achat** pour terminer le déploiement.

Il peut prendre un moment avant que le groupe de ressources Azure soit créé avec les configurations requises. Une fois terminé, sélectionnez le groupe de ressources pour afficher les détails de la configuration. Cela peut inclure des règles LB, des pools principaux, des sondes d'intégrité, etc. dans le portail Azure. La paire HA apparaît en tant que VPX0 et VPX1.

Si d'autres modifications sont nécessaires pour votre configuration HA, telles que la création de règles et de ports de sécurité supplémentaires, vous pouvez le faire à partir du portail Azure.



Ensuite, vous devez configurer le vserver d'équilibrage de charge avec l'adresse IP publique ALB (PIP), sur chaque nœud. Pour trouver le PIP ALB, sélectionnez **ALB > Configuration IP frontend**.



Citrix ADC GSLB et Autoscale principal des services basés sur le domaine avec équilibrage de charge cloud

Vue d'ensemble GSLB et DBS

Citrix ADC GSLB prend en charge l'utilisation de DBS (Domain Based Services) pour les équilibreurs de charge Cloud. Cela permet la découverte automatique des services cloud dynamiques à l'aide d'une solution d'équilibrage de charge cloud. Cette configuration permet à Citrix ADC d'implémenter les services GSLB (Global Server Load Balancing Domain-Name Based Services) dans un environnement Active-Active. DBS permet la mise à l'échelle des ressources principales dans un environnement Amazon Web Services (AWS) et Microsoft Azure à partir de la découverte DNS. Cette section couvre les intégrations entre Citrix ADC dans les environnements AWS et Azure Auto Scaling. La dernière section du document décrit en détail la possibilité de configurer une paire HA de Citrix ADC couvrant deux zones de disponibilité (AZs) différentes spécifiques à une région AWS ou Azure.

Pré-requis :

Les conditions préalables pour les groupes de services Citrix ADC GSLB incluent un environnement Amazon Web Services / Microsoft Azure fonctionnel avec les connaissances et la capacité de configurer des groupes de sécurité, des serveurs Web Linux, des Citrix ADC au sein d'AWS, des adresses IP Elastic et des équilibreurs de charge Elastic.

L'intégration du service GSLB DBS nécessite Citrix ADC version 12.0.57 pour les instances d'équilibrage de
charge AWS ELB et Microsoft Azure ALB.

Améliorations des fonctionnalités du groupe de services Citrix ADC GSLB

Entité Groupe de services GSLB : Citrix ADC version 12.0.57

GSLB Service Group prend en charge Autoscale à l'aide de la découverte dynamique DBS.

Les composants de fonctionnalités DBS (service basé sur le domaine) doivent être liés au groupe de services GSLB

Exemple :

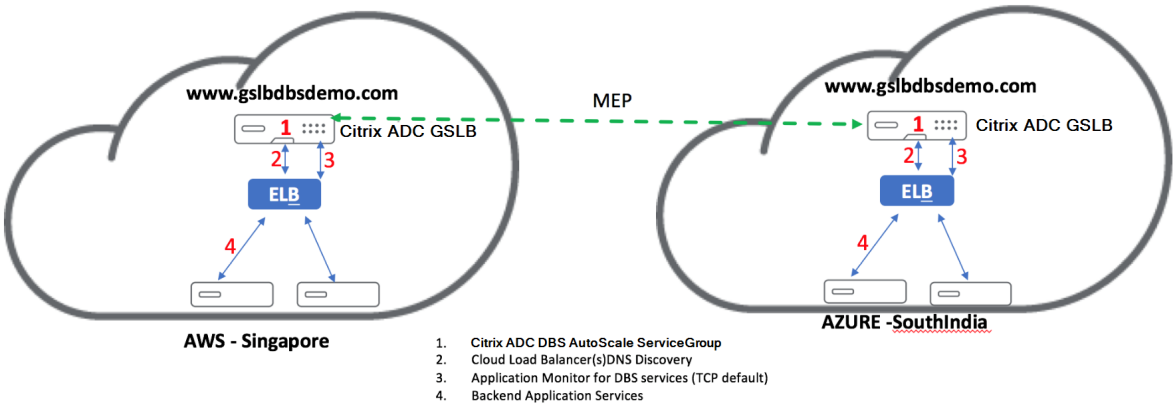
```
1  > add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
      amazonaws.com
2  > add gslb serviceGroup sydney_sg HTTP -autoscale DNS -siteName sydney
3  > bind gslb serviceGroup sydney_sg sydney_server 80
4 <!--NeedCopy-->
```

Services basés sur le nom de domaine — Azure ALB

GLSB DBS utilise le nom de domaine complet de votre équilibreur de charge Azure pour actualiser dynamiquement les groupes de services GSLB afin d'inclure les serveurs principaux créés et supprimés

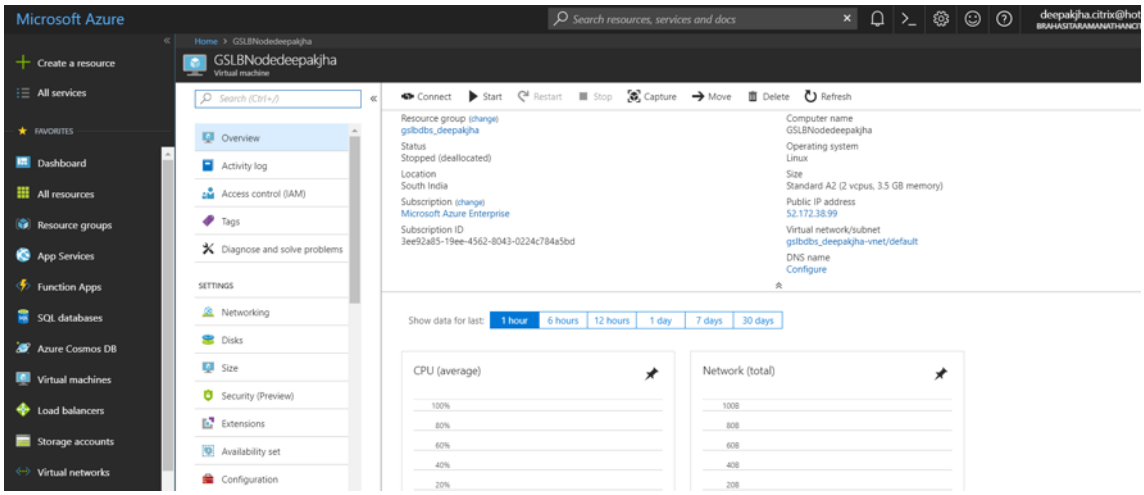
dans Azure. Pour configurer cette fonctionnalité, nous pointons le Citrix ADC vers notre équilibreur de charge Azure pour acheminer dynamiquement vers différents serveurs dans Azure. Nous pouvons le faire sans avoir à actualiser manuellement le Citrix ADC chaque fois qu'une instance est créée et supprimée dans Azure. La fonctionnalité DBS Citrix ADC pour les groupes de services GSLB utilise la découverte de service prenant en charge DNS pour déterminer les ressources de service membre de l'espace de noms DBS identifié dans le groupe autoscaler.

Diagramme : Composants AutoScale DBA Citrix ADC GSLB avec équilibreurs de charge cloud

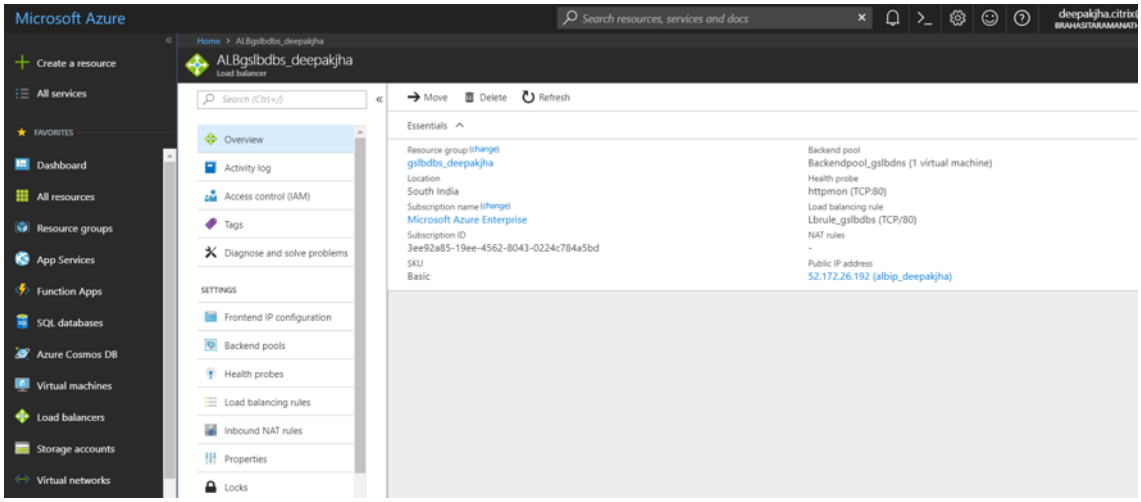


Configuration des composants Azure

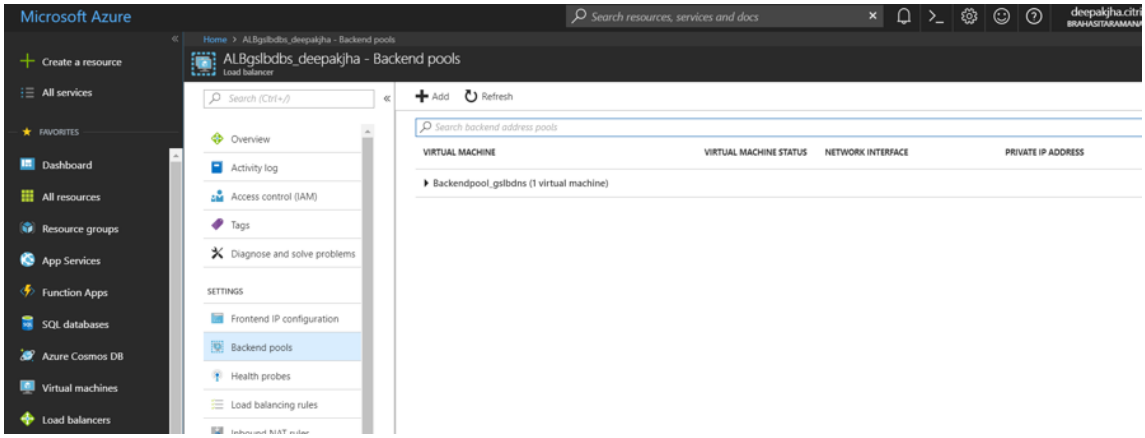
1. Connectez-vous à votre portail Azure et créez une nouvelle machine virtuelle à partir d'un modèle Citrix ADC



2. Créer un équilibreur de charge Azure



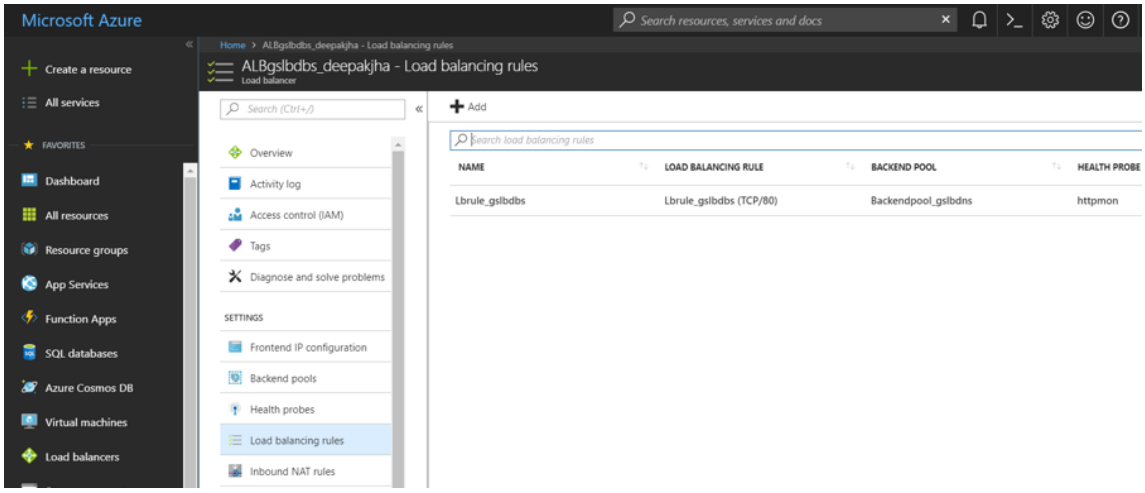
3. Ajouter les pools d'arrière-plan Citrix ADC créés



4. Créez une sonde d'intégrité pour le port 80.

   Créez une règle d'équilibrage de charge en utilisant l'IP frontend créée à partir de l'équilibreur de charge.

   a) Protocole : TCP
   b) Port principal : 80
   c) Pool principal : Citrix ADC créé à l'étape 1
   d) Sonde d'intégrité : créé à l'étape 4
   e) Persistance de la session : Aucun



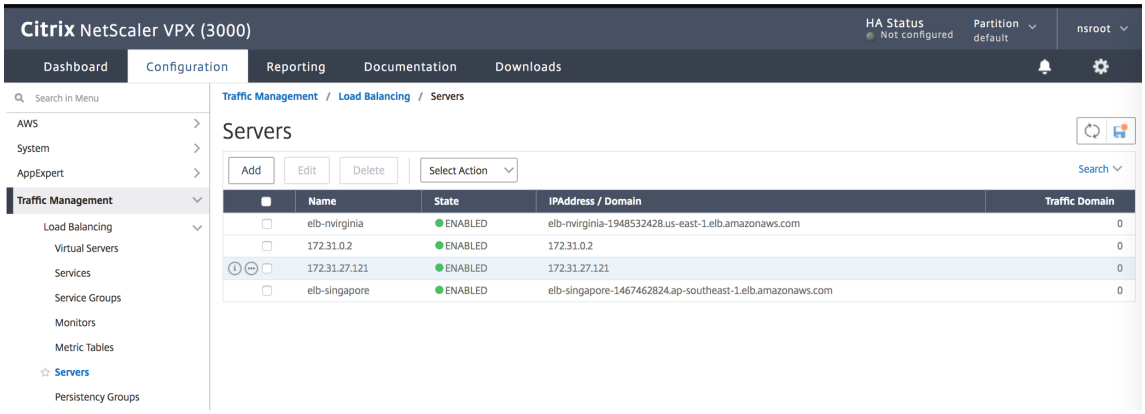
Configurer le service basé sur le domaine Citrix ADC GSLB

Les configurations suivantes résument ce qui est requis pour activer les services basés sur le domaine pour la mise à l'échelle automatique des ADC dans un environnement GSLB activé.

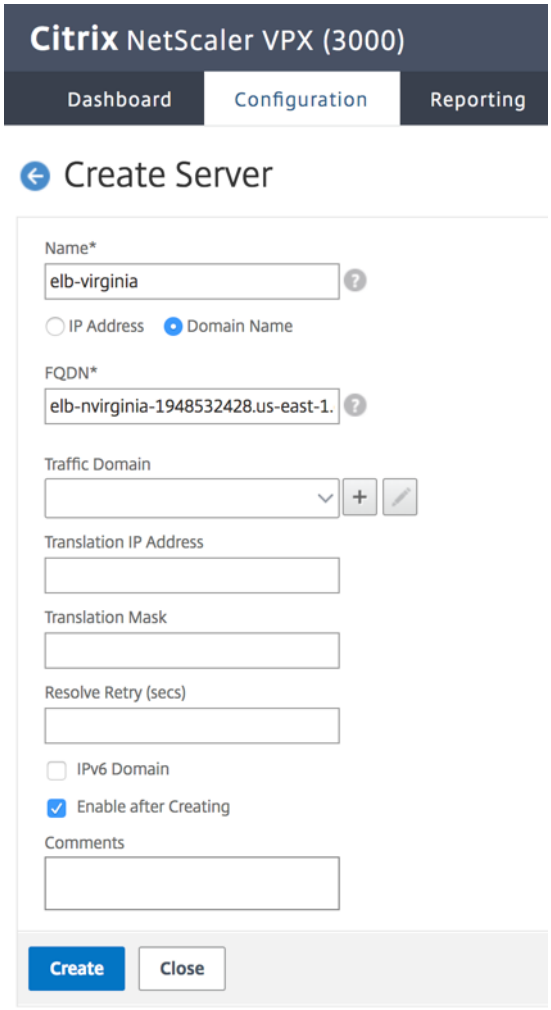
Configurations de gestion du trafic

> **Remarque :** Il est nécessaire de configurer le Citrix ADC avec unserveur de noms ou un serveur DNS via lequel les domaines ELB/ALB seront résolus pour les groupes de services DBS.

1. Accédez à **Gestion du trafic - > Équilibrage de charge - > Serveurs**



2. Cliquez sur **Ajouter** pour créer un serveur, fournissez un nom et un nom de domaine complet correspondant à l'enregistrement A (nom de domaine) dans Azure pour l'équilibrage de charge Azure (ALB)



3. Répétez l'étape 2 pour ajouter le deuxième ALB à partir de la deuxième ressource dans Azure.

Configurations GSLB

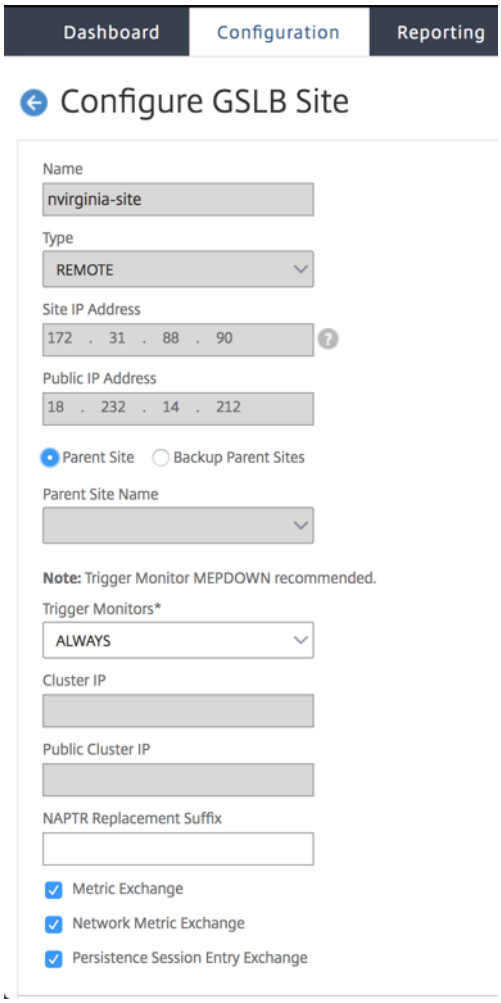
1. Cliquez sur le bouton **Ajouter** pour configurer un site GSLB
2. Nommez le site.

   Type est configuré comme Remote ou Local en fonction de quel Citrix ADC vous configurez le site. L'adresse IP du site est l'adresse IP du site GSLB. Le site GSLB utilise cette adresse IP pour communiquer avec les autres sites GSLB. L'adresse IP publique est requise lors de l'utilisation d'un service cloud où une adresse IP particulière est hébergée sur un pare-feu externe ou un périphérique NAT. Le site doit être configuré en tant que site parent. Assurez-vous que les moniteurs de déclenchement sont réglés sur ALWAYS. Veillez également à cocher les trois cases en bas pour l'échange de métriques, l'échange de métriques réseau et l'échange d'entrées de session de persistance.

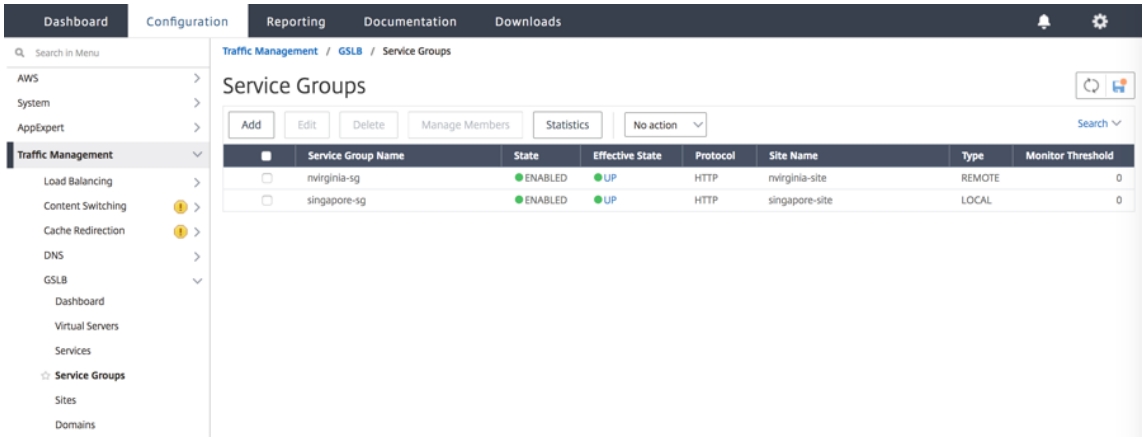
   La recommandation est de définir le paramètre du moniteur de déclenchement sur MEPDOWN,

veuillez vous référer àConfiguration d'un groupe de services GSLB.

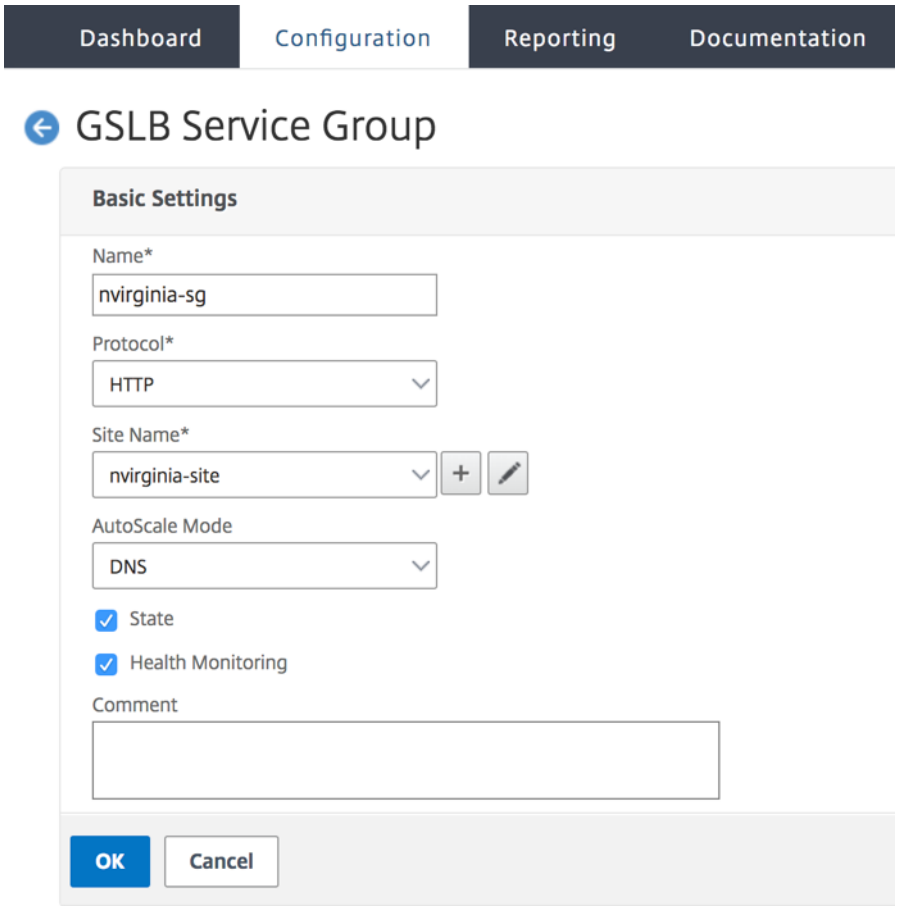
![image-citrix-adc-and-microsoft-azure-28]/en-us/advanced-concepts/media/image-citrix-adc-and-microsoft-azure-28.png)



3. Cliquez sur **Créer**, répétez les étapes 3 et 4 pour configurer le site GSLB pour l'autre emplacement de ressource dans Azure (cela peut être configuré sur le même Citrix ADC)
4. Accédez à **Gestion du trafic - > GSLB - > Groupes de services**

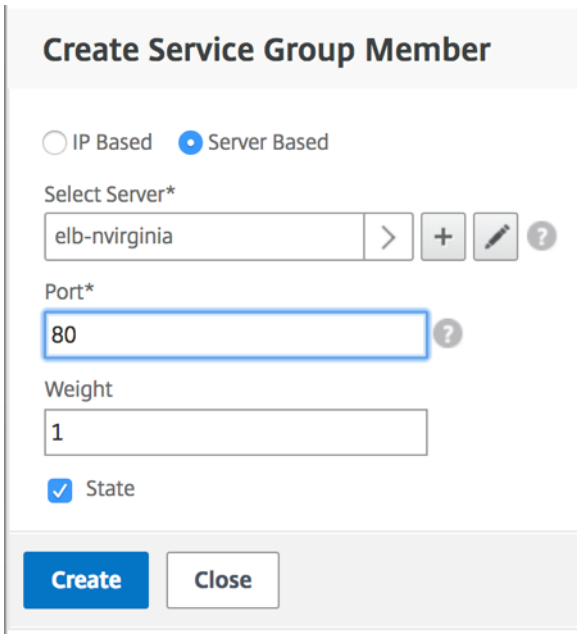


Cliquez sur **Ajouter** pour ajouter un nouveau groupe de services. Nommez le groupe de services, utilisez le protocole HTTP, puis sous Nom du site, choisissez le site correspondant qui a été créé lors des étapes précédentes. Assurez-vous de configurer le mode AutoScale en tant que DNS et cochez les cases État et Contrôle de l'intégrité. Cliquez sur **OK** pour créer le groupe de services

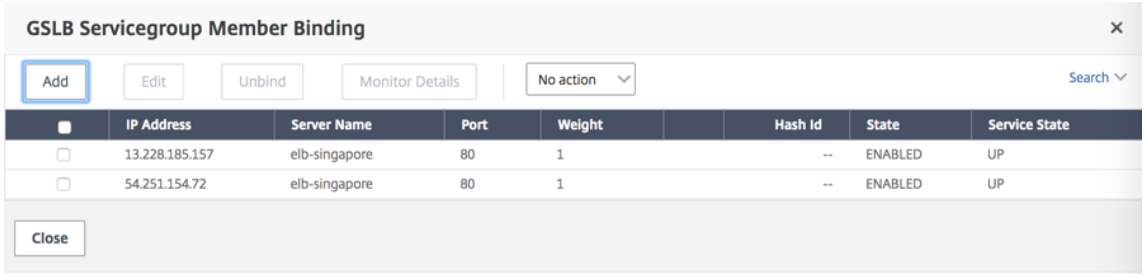


5. Cliquez sur **Membres du groupe de services** et sélectionnez **Basé sur serveur**. Sélectionnez le serveur Elastic Load Balancing correspondant qui a été configuré au début du guide

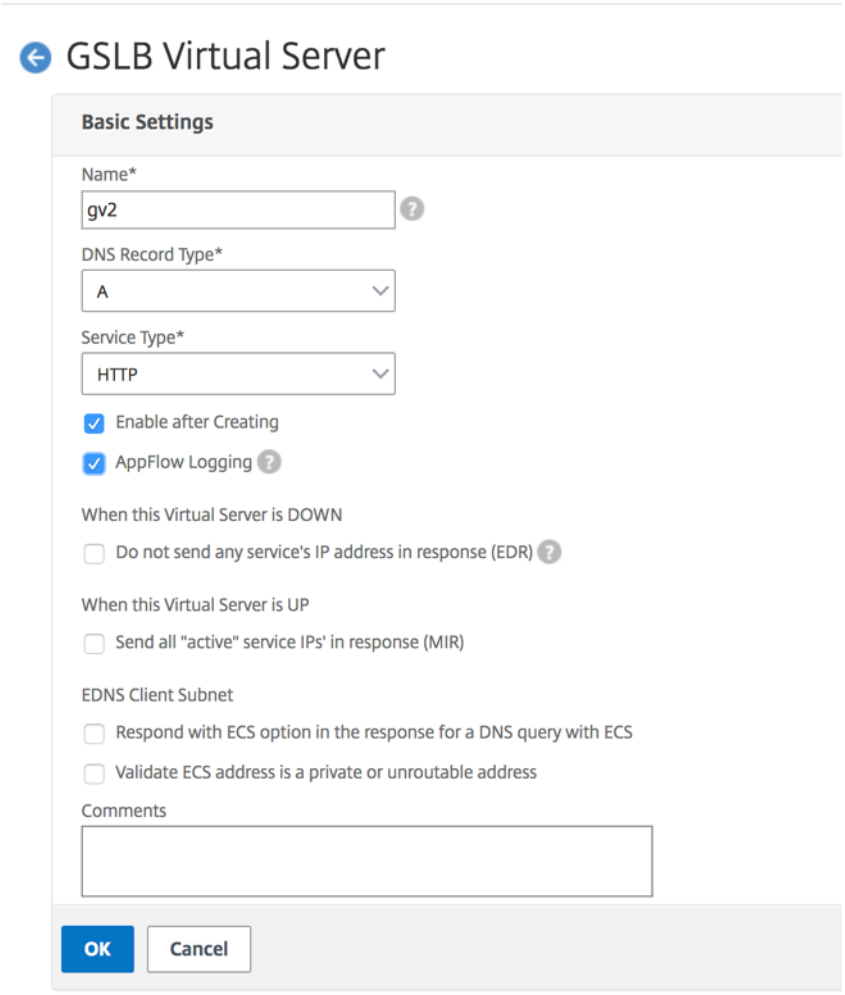
d'exécution. Configurez le trafic pour passer par le port 80. Cliquez sur **Créer**.



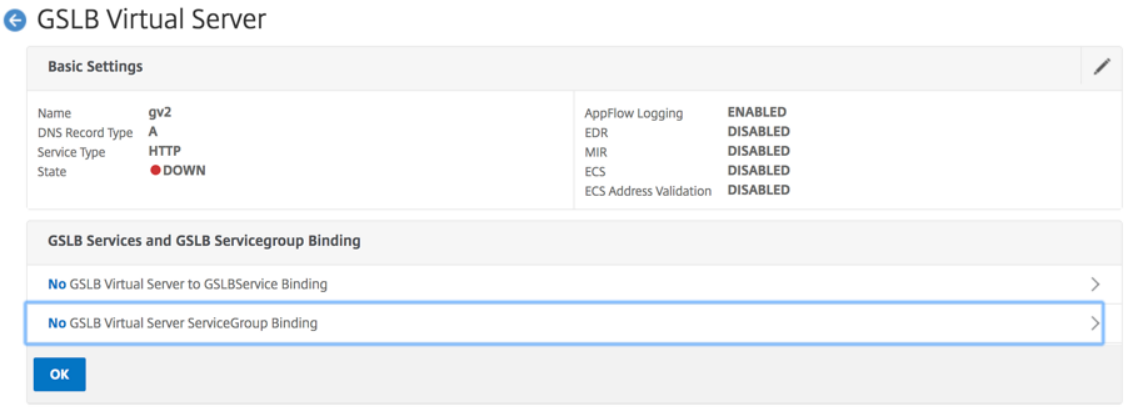
6. La liaison de membre Servicegroup doit être remplie avec 2 instances qu'elle reçoit de l'Elastic Load Balancer.



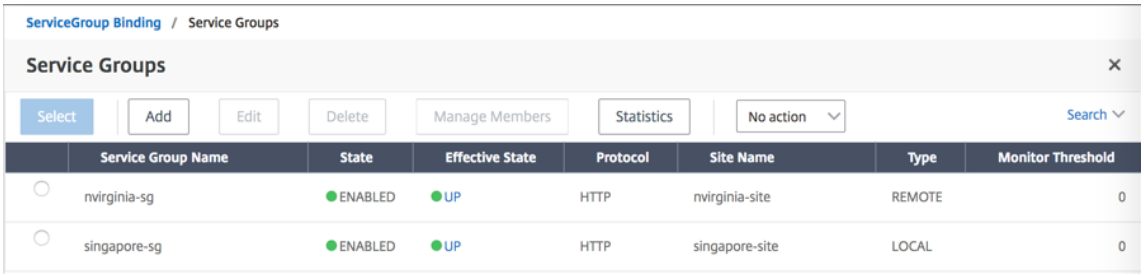
7. Répétez les étapes 5 et 6 pour configurer le groupe de services pour le deuxième emplacement de ressource dans Azure. (Cela peut être fait à partir de la même interface graphique Citrix ADC).
8. La dernière étape consiste à configurer un serveur virtuel GSLB. Accédez à **Gestion du trafic - > GSLB - > Serveurs virtuels**.
9. Cliquez sur **Ajouter** pour créer le serveur virtuel. Nommez le serveur, le type d'enregistrement DNS est défini comme A, le type de service est défini comme HTTP et cochez les cases Activer après la création et la journalisation AppFlow. Cliquez sur **OK** pour créer le serveur virtuel GSLB.



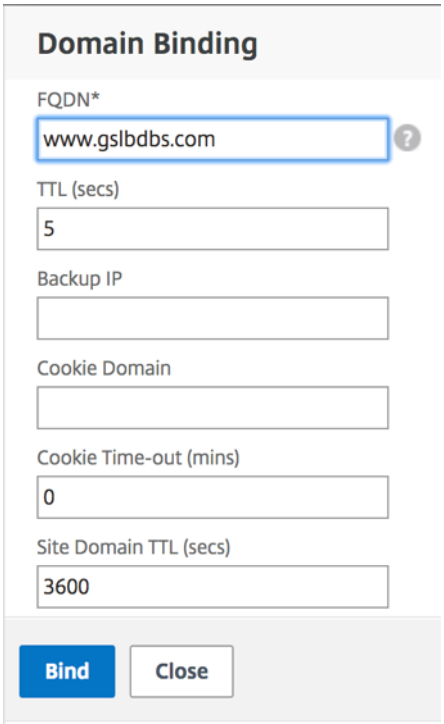
10. Une fois le serveur virtuel GSLB créé, cliquez sur **Aucune liaison GSLB ServiceGroup Service-Group**.



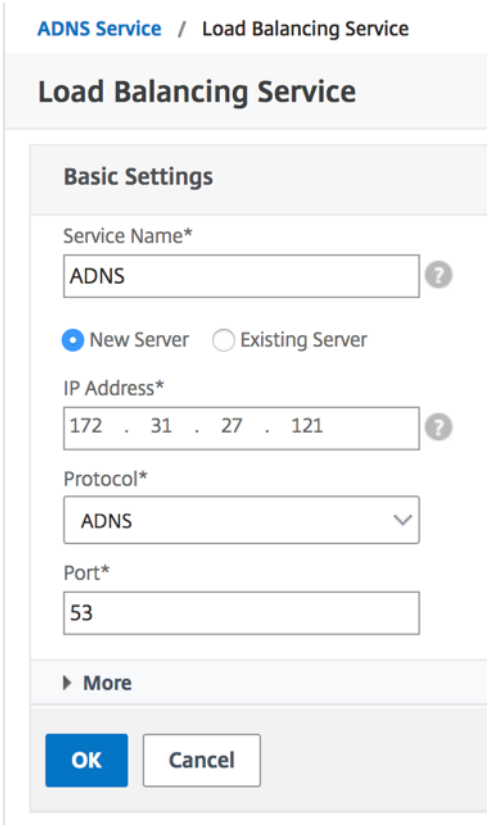
11. Sous Liaison ServiceGroup, utilisez **Sélectionner le nom du groupe** de services pour sélectionner et ajouter les groupes de services créés lors des étapes précédentes.



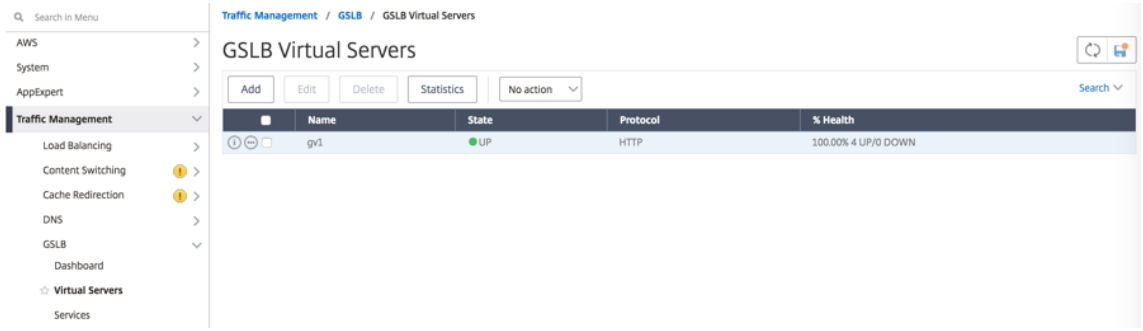
12. Configurez ensuite la liaison de domaine de serveur virtuel GSLB en cliquant sur **Aucune liaison de domaine de serveur virtuel GSLB**. Configurez le nom de domaine complet et la liaison, les autres paramètres peuvent être laissés comme valeurs par défaut.



13. Configurez le service ADNS en cliquant sur **Aucun service**. Ajoutez un nom de service, cliquez sur **Nouveau serveur** et entrez l'adresse IP du serveur ADNS. En outre, si votre ADNS est déjà configuré, vous pouvez sélectionner **Serveur existant** , puis choisir votre ADNS dans le menu déroulant. Assurez-vous que le protocole est ADNS et que le trafic est sur le port 53.



14. Configurez la méthode comme LEASTCONNECTION et la méthode de sauvegarde comme ROUNDROBIN.
15. Cliquez sur **Terminé** et vérifiez que votre serveur virtuel GSLB est affiché en haut.



Autoscale frontal dans Azure avec VPX à l'aide des groupes Autoscale dans Citrix Application Delivery Management

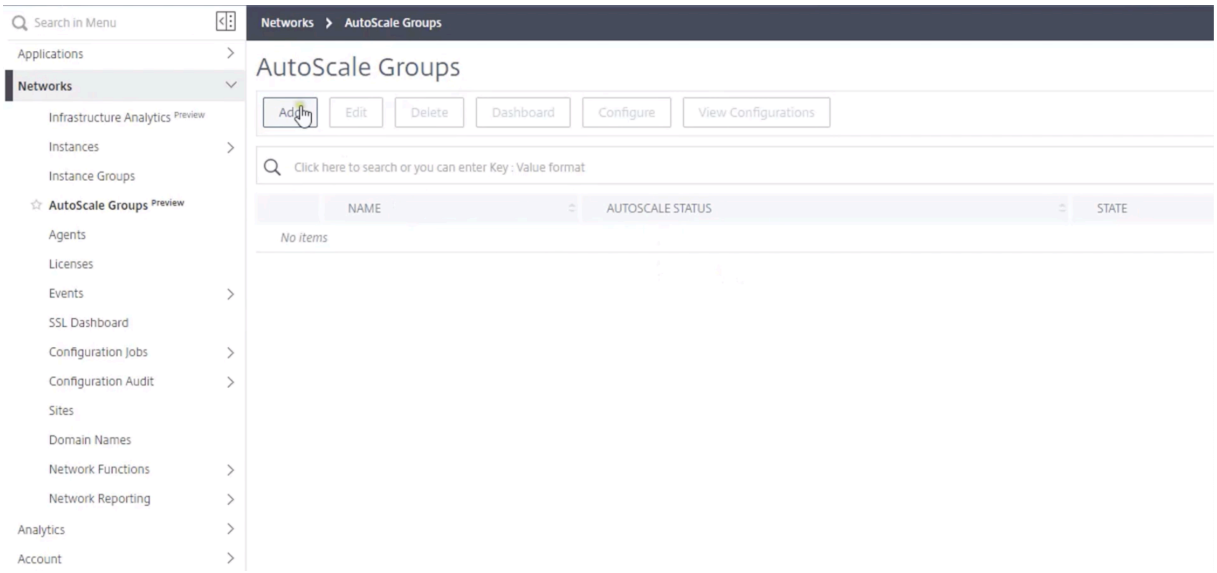
Autoscaling est une méthode de cloud computing qui ajoute ou supprime automatiquement des ressources en fonction de l'utilisation réelle. La mise à l'échelle automatique est utile lorsque votre site ou application a besoin d'une allocation de ressources à la demande pour satisfaire le nombre fluctuant de demandes client ou de travaux de traitement.

La demande d'applications ou de services Web peut varier considérablement. Il est important de maintenir le nombre correct d'instances Citrix ADC pour différents besoins de trafic. Vous pouvez augmenter ou diminuer les ressources réseau sur Microsoft Azure en fonction de la demande. Ainsi, il offre une optimisation des coûts sans compromettre les performances.

La mise à l'échelle automatique de Citrix Application Delivery Management (ADM) conserve le nombre exact d'instances Citrix ADC pour fluctuer la consommation des ressources. Citrix ADM détermine le flux de trafic en fonction de la consommation fluctuante des ressources, il décide d'évoluer ou d'évoluer dynamiquement dans les instances Citrix ADC.

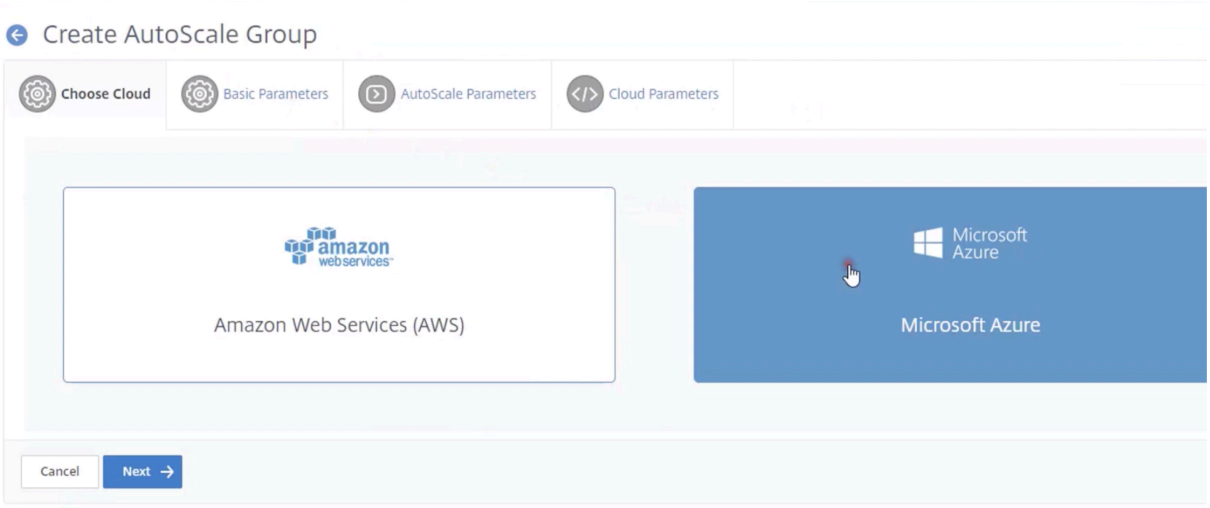
Créer un groupe Autoscale

- Dans l'utilitaire de console de gestion ADC, accédez à **Networks > Autoscale**.
- Sélectionnez **Ajouter**.



Choisissez le cloud

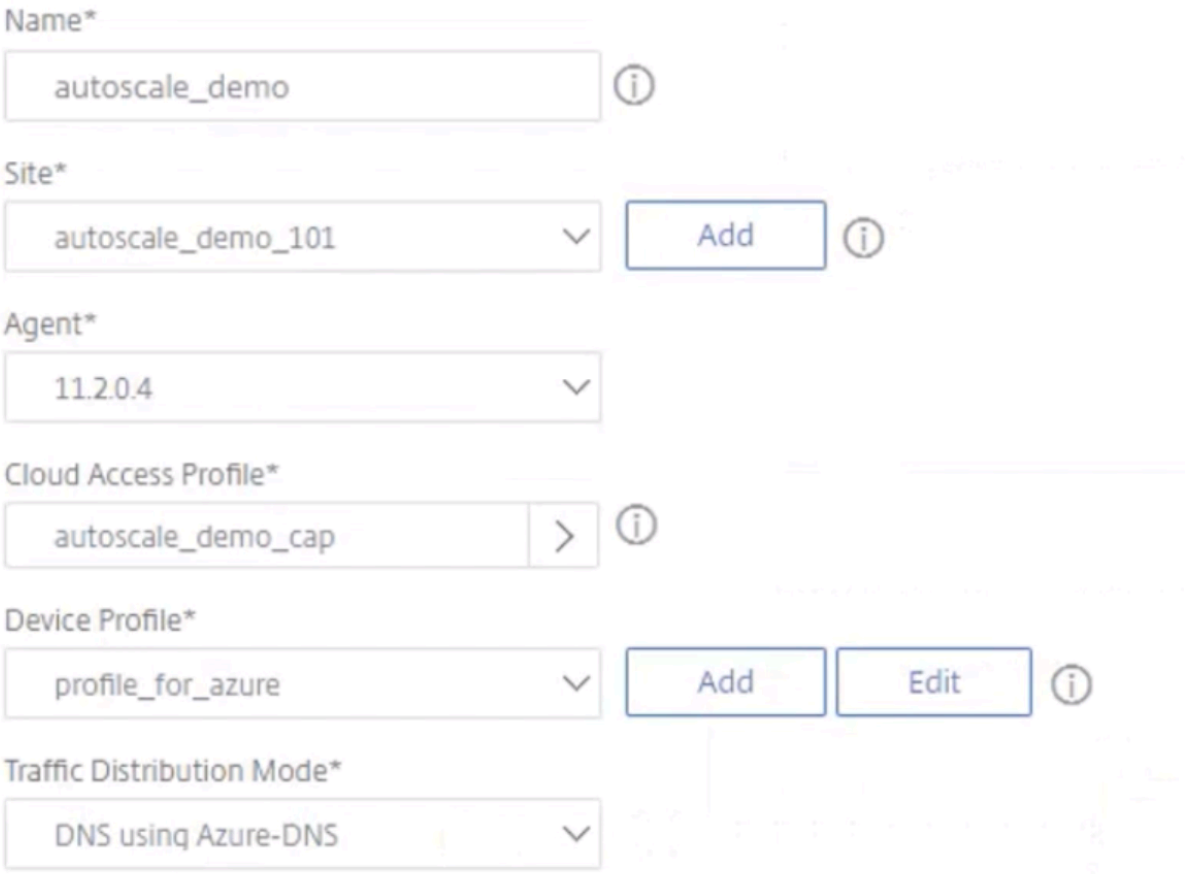
Dans l'onglet **Create autoscale Group**, cliquez sur **Microsoft Azure** , puis sur **Add**.



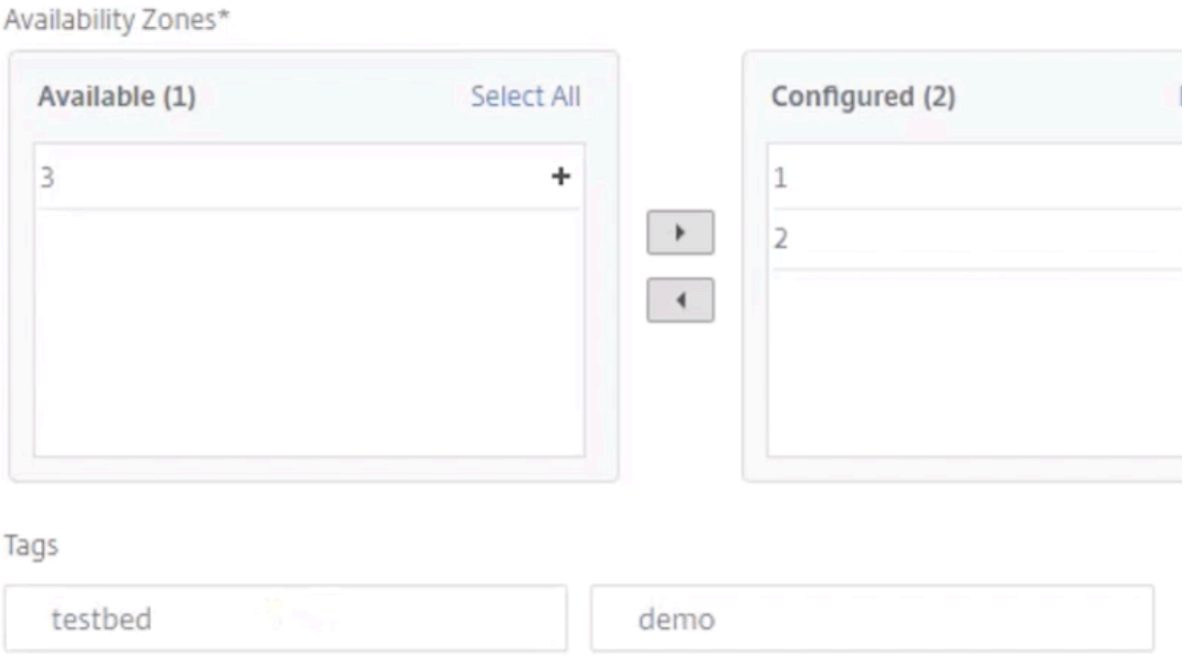
Paramètres de base

Configurez les paramètres de base pour le groupe Autoscale :

1. **Nom** : autoscale_demo
2. **Site** : autoscale_demo_101
3. **Agent** : 11.2.0.4
4. **Profil d'accès au cloud** : autoscale_demp_cap
5. **Périphérique** : profile_for_azure
6. **Mode de distribution du trafic** : DNS utilisant Azure DNS



Ne sélectionnez pas encore **Suivant** . Ajoutez les zones de disponibilité 1 et 2 en cliquant sur le signe plus et définissez les balises sur **Testbed**.



Sélectionnez **Next**.

Paramètres Autoscale

Configurez les paramètres Autoscale pour le groupe Autoscale :

1. Utilisation du processeur : 10 — 30
2. Utilisation de la mémoire : 10 — 30
3. Utilisation du débit : 10 — 30
4. Instances minimales : 4
5. Nombre maximal d'instances : 6
6. Temps de montre : 2
7. Période de recharge : 1
8. Temps d'attente pendant l'arrêt : 1
9. DNS Temps de vie : 10

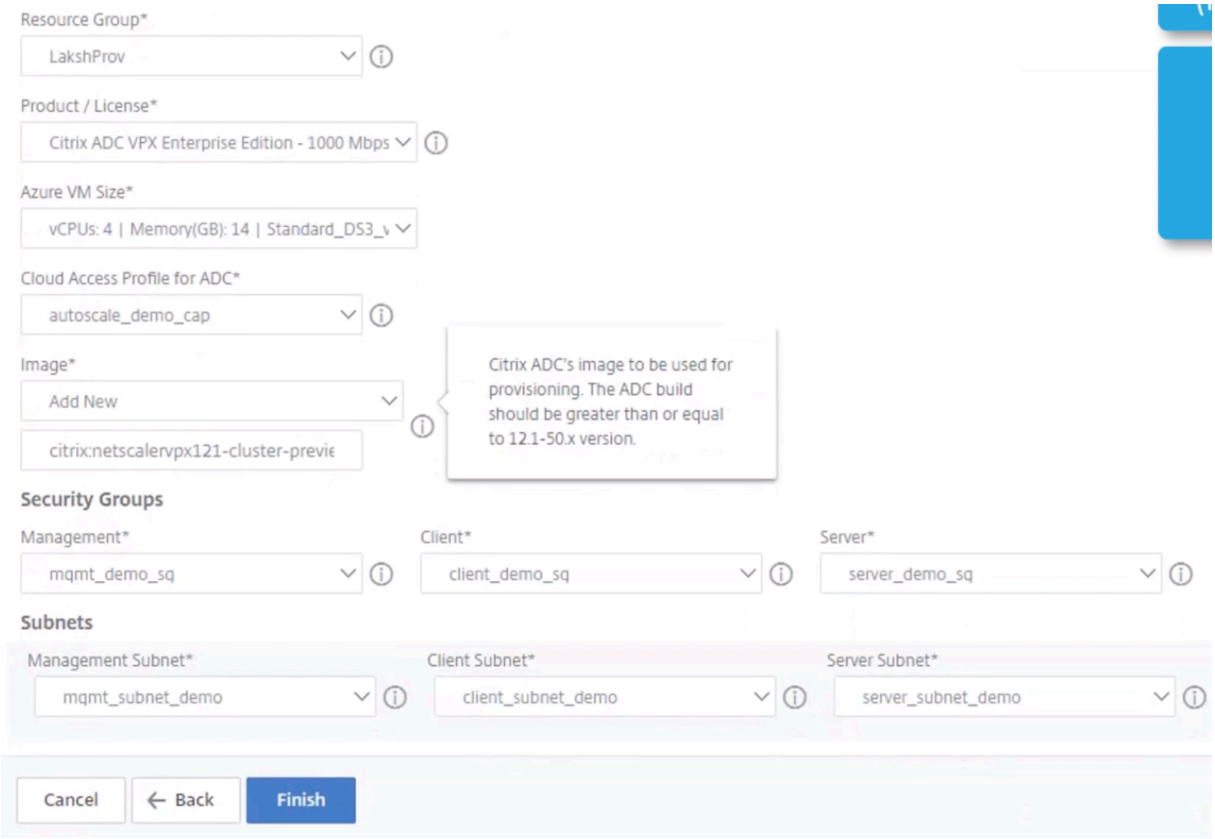
Cliquez sur **Suivant**.

Paramètres cloud

Configurez les paramètres cloud pour le groupe Autoscale :

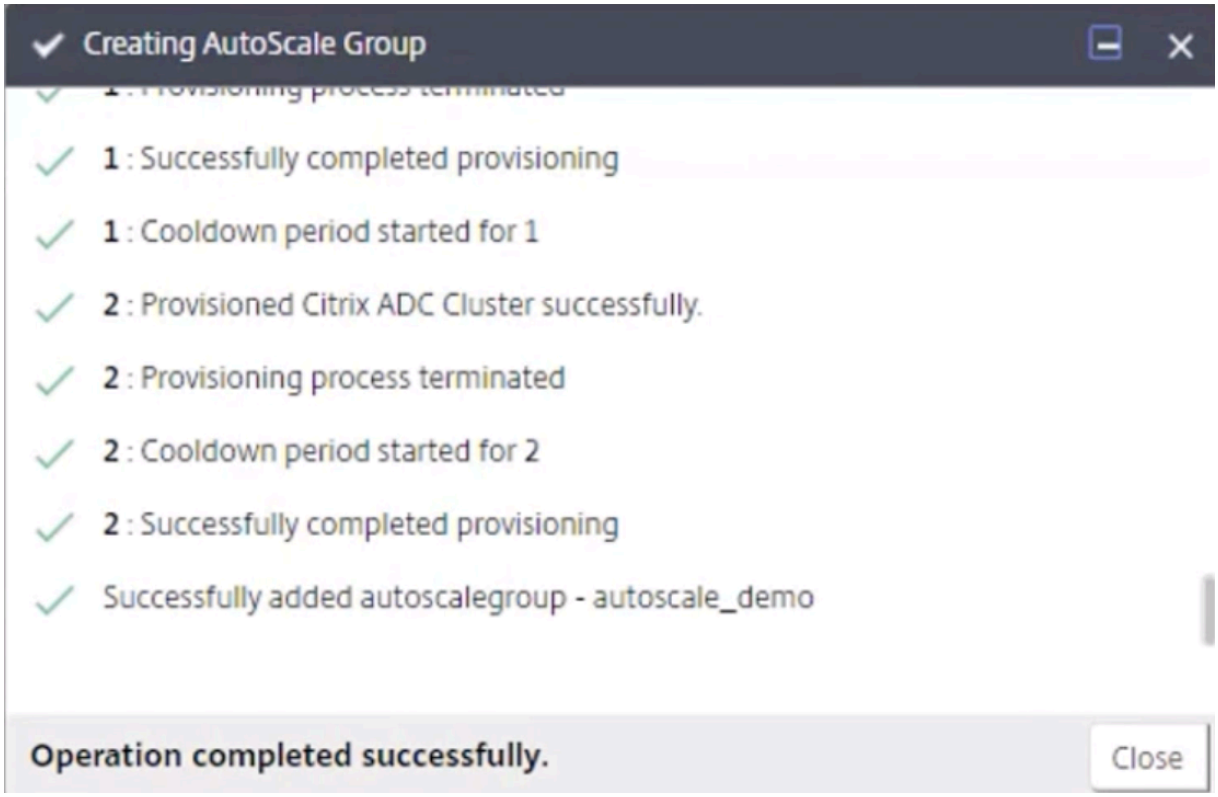
1. Groupe de ressources : LakshProv
2. Produit / Licence : Citrix ADC VPX Enterprise Edition - 1000 Mbps
3. Taille de la machine virtuelle Azure : vCPU : 4 | Mémoire (Go) : 14 | Standard_DS3_V2

4. Profil d'accès au cloud pour ADC : autoscale_demo_cap
5. Image : par défaut
6. Gestion : mgmt_demo_sq
7. Client : client_demo_sq
8. Serveur : server_demo_sq
9. Sous-réseau de gestion : mgmt_subnet_demo
10. Sous-réseau client : client_subnet_demo
11. Sous-réseau serveur : server_subnet_demo



Sélectionnez **Next**.

Une boîte de dialogue apparaît. Assurez-vous que le groupe Autoscale est créé correctement.



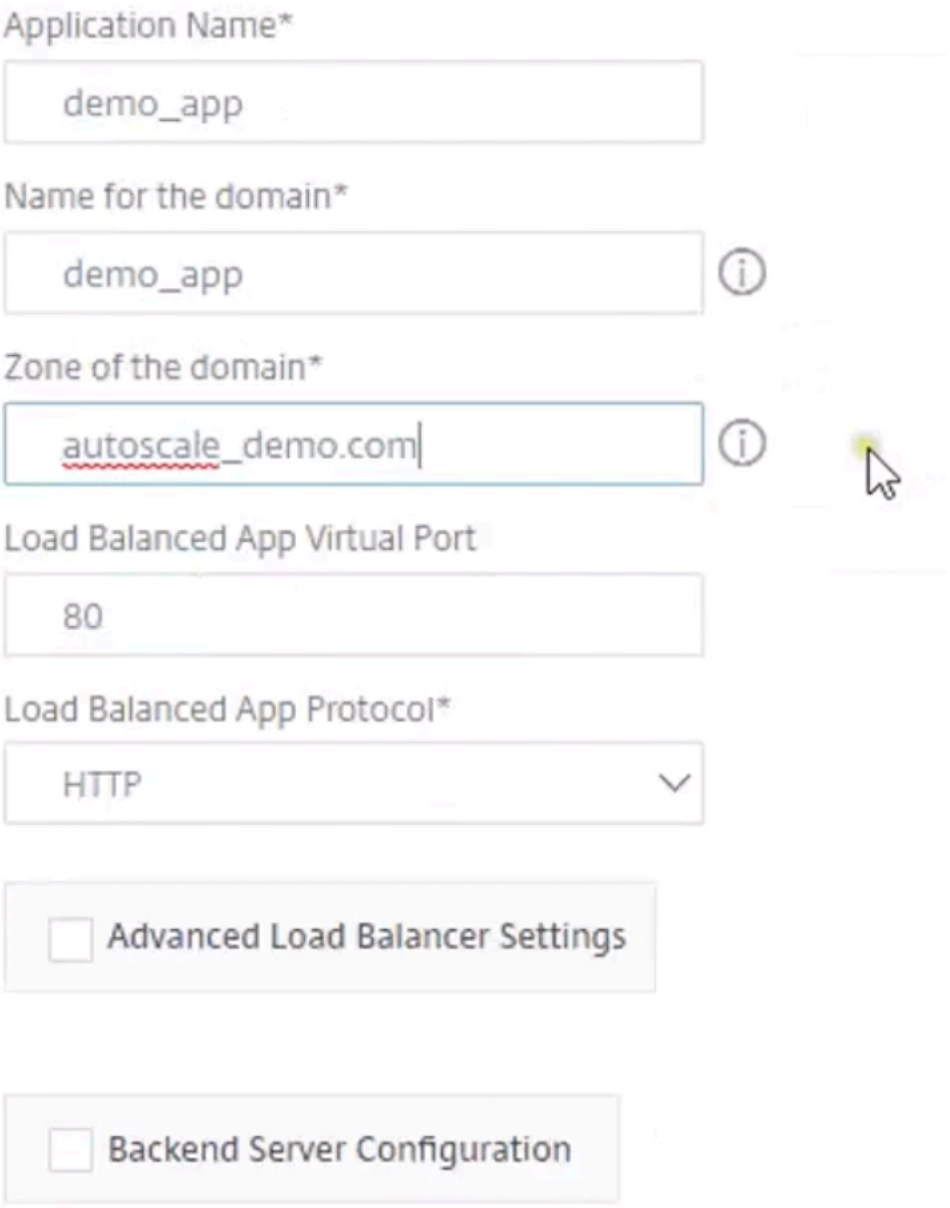
Configurer le groupe Autoscale

1. Dans l'utilitaire de console de gestion ADC, accédez à **Networks > Autoscale**.
2. Sélectionnez l'échelle automatique créée et assurez-vous qu'elle est activée.
3. Cliquez sur **Configurer**.
4. Sur la page Choisir le StyleBook, sélectionnez`HTTP/SSL LoadBalancing StyleBook`.

Détails de la configuration

Entrez les détails de configuration à créer avec le StyleBook :

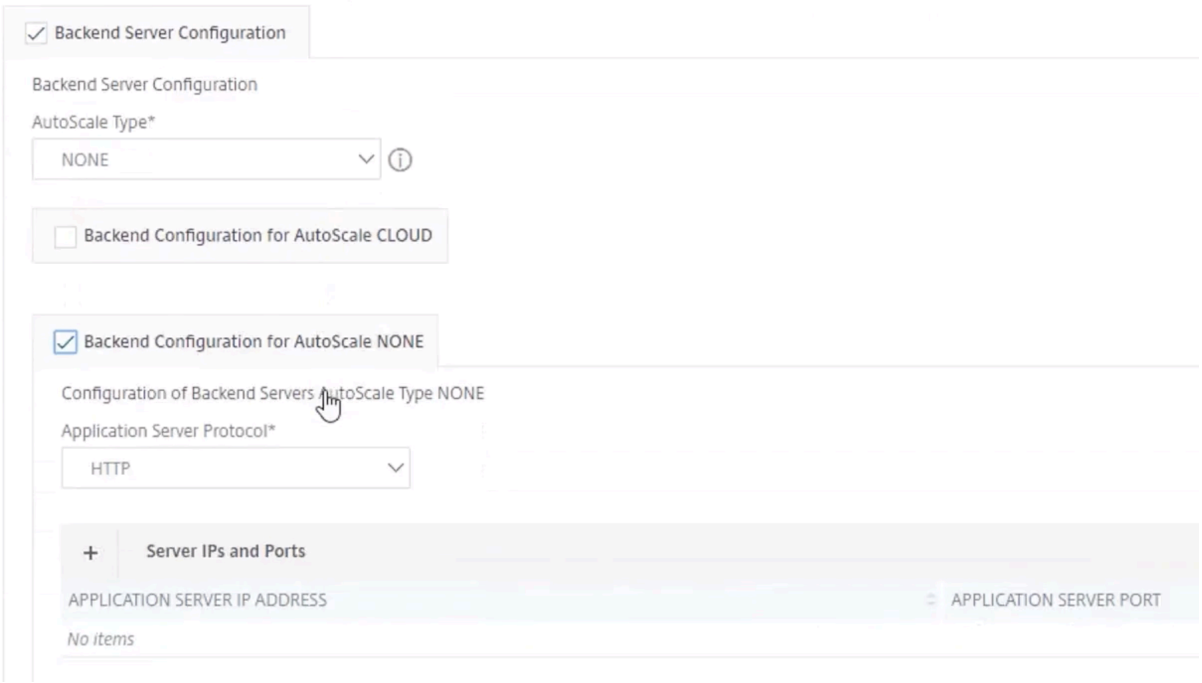
1. Application Name: demo_app
2. Name for the domain: demo_app
3. Zone of the domain: autoscale_demo.com
4. Load Balanced App Virtual Port: 80
5. Load Balanced App Protocol: HTTP



Cochez **Backend Server Configuration**.

1. Autoscale Type: None

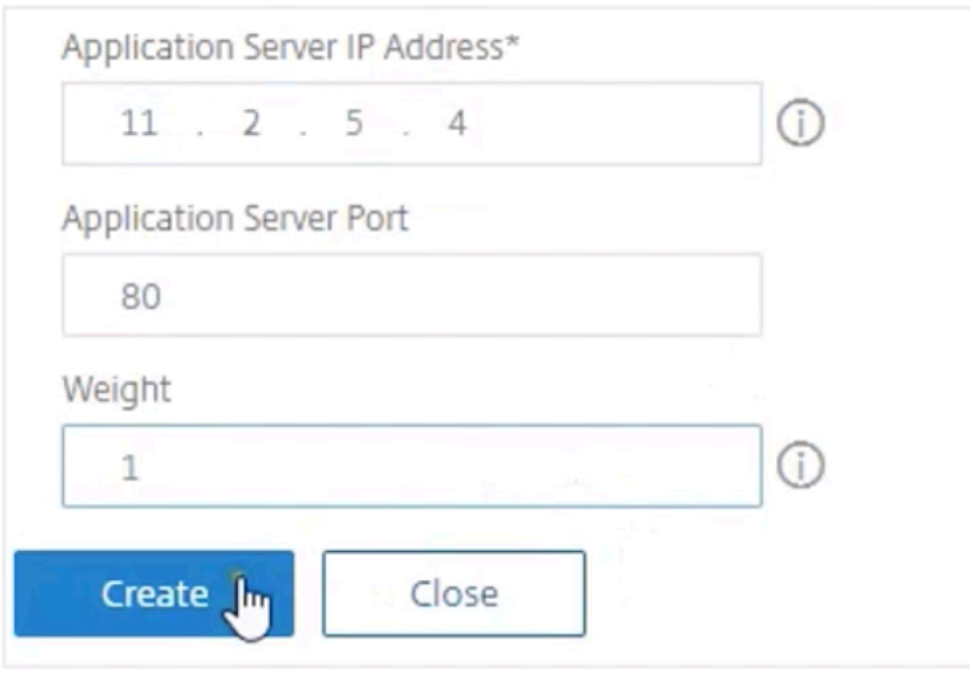
Cochez **Backend Configuration for autoscale NONE**



Cliquez sur le signe plus en regard de **Server IPs and Ports**.

1. Application Server IP Address: 11.2.5.4
2. Port du serveur d'applications : 80
3. Poids : 1

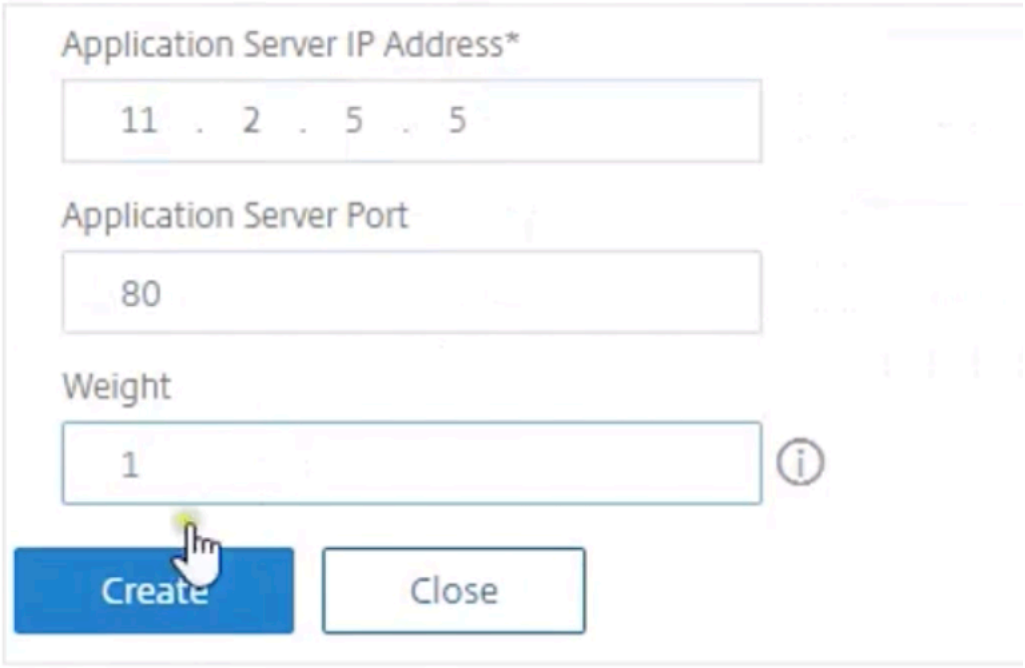
Cliquez sur **Créer**.



Répétez l'étape précédente :

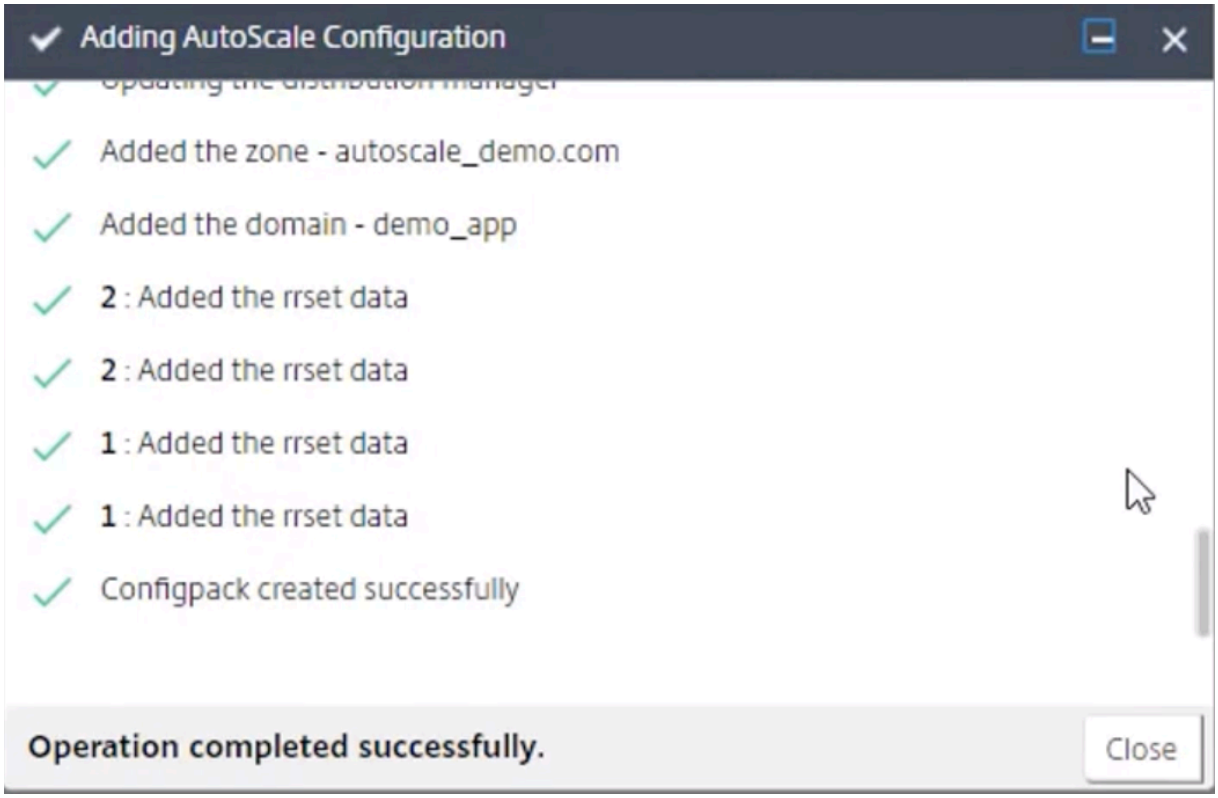
1. Application Server IP Address: 11.2.5.5
2. Port du serveur d'applications : 80
3. Poids : 1

Cliquez sur **Créer**.



Sur la page principale de configuration du StyleBook, cliquez sur **Create**.

Une boîte de dialogue apparaît. Assurez-vous que la configuration de StyleBook est créée correctement.



Références supplémentaires

Déployer une instance de VPC Citrix ADC sur Microsoft Azure

Documentation Microsoft Azure

Affecter plusieurs adresses IP à des machines virtuelles à l'aide de PowerShell

Créer une machine virtuelle avec plusieurs cartes réseau à l'aide de PowerShell

Machines virtuelles de service principal Autoscale dans Azure Public Cloud avec Citrix ADC VPX

Documentation produit Citrix

Configurer plusieurs adresses IP pour une instance autonome Citrix ADC VPX

Configurer plusieurs adresses IP pour une instance Citrix ADC VPX en mode autonome à l'aide des commandes PowerShell

Configurer plusieurs VIP Azure pour une instance VPX autonome

Citrix ADC CPX, Citrix Ingress Controller et Application Delivery Management sur Google Cloud

January 8, 2020

Présentation du produit Citrix pour l'architecture et les composants de GCP K8

Les cinq principaux composants Citrix de GCP

1. **Citrix ADC VPX en tant que ADC de niveau 1 pour le trafic client Internet basé sur l'entrée.**

   Une instance VPX dans GCP vous permet de tirer parti des capacités informatiques GCP et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic Citrix pour vos besoins professionnels. Vous pouvez déployer VPX dans GCP en tant qu'instance autonome. Les configurations de cartes d'interface réseau (NIC) simples et multiples sont prises en charge.

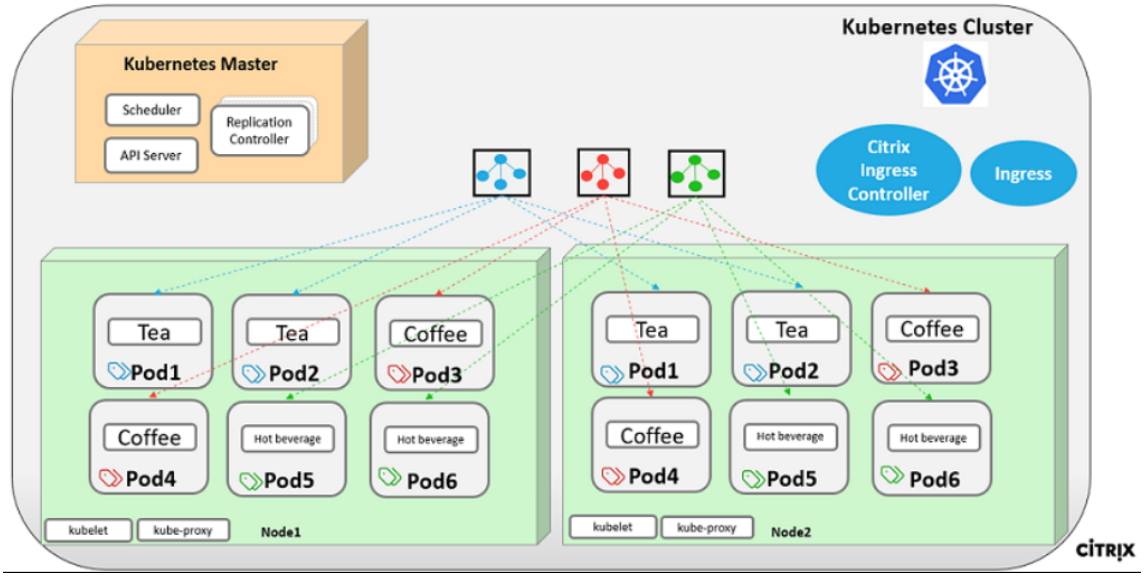
2. **Le cluster Kubernetes utilisant Google Kubernetes Engine (GKE) pour former la plate-forme conteneur.**

   Kubernetes Engine est un environnement géré et prêt à la production pour le déploiement d'applications conteneurisées. Il permet un déploiement et une gestion rapides de vos applications et services.

3. **Déployez un exemple d'application Web Citrix à l'aide de la bibliothèque de fichiers YAML.**

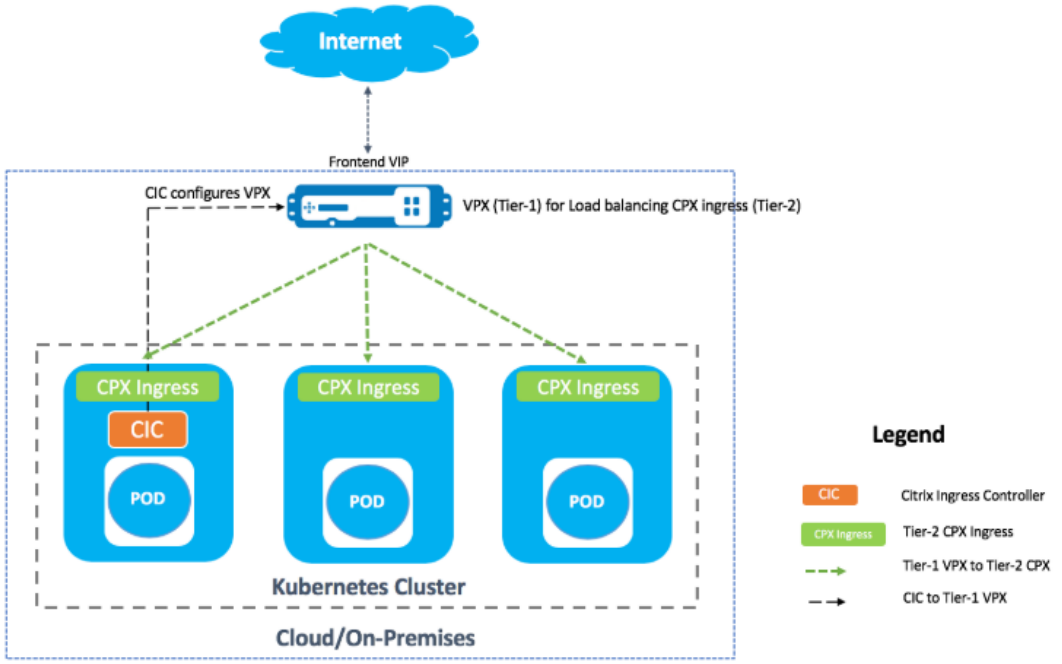
   Citrix a fourni un exemple d'application Web de microservice pour tester la topologie d'application à deux niveaux sur GCP. Nous avons également inclus les éléments suivants dans les fichiers exemples de preuve de concept :

   - Exemple de service Web de boisson chaude dans le fichier Kubernetes YAML
   - Exemple de service Web Colddrink dans le fichier Kubernetes YAML
   - Exemple de service Web Livre d'or dans le fichier Kubernetes YAML
   - Exemple de service de cartographie Grafana dans le fichier YAML Kubernetes
   - Exemple de service de journalisation Prometheus dans le fichier Kubernetes YAML



4. **Déployez le contrôleur d'entrée Citrix pour l'automatisation Citrix ADC de niveau 1 dans le cluster GKE.**

   Le contrôleur d'entrée Citrix construit autour de Kubernetes configure automatiquement un ou plusieurs Citrix ADC en fonction de la configuration des ressources d'entrée. Un contrôleur d'entrée est un contrôleur qui surveille le serveur d'API Kubernetes pour les mises à jour de la ressource d'entrée et reconfigure l'équilibrage de charge d'entrée en conséquence. Le contrôleur d'entrée Citrix peut être déployé directement à l'aide de fichiers YAML ou par Helm Charts.



Citrix a fourni des exemples de fichiers YAML pour l'automatisation du contrôleur d'entrée Citrix de l'instance VPX de niveau 1. Les fichiers automatisent plusieurs configurations sur le VPX de niveau 1, y compris :

- Réécrire des stratégies et des actions
- Politiques et actions des intervenants
- Contenu Changement de règles d'URL
- Ajout/Suppression de services d'équilibrage de charge CPX

Le fichier YAML du contrôleur d'entrée Citrix pour GCP se trouve ici : https://github.com/citrix/example-cpx-vpx-for-kubernetes-2-tier-microservices/tree/master/gcp

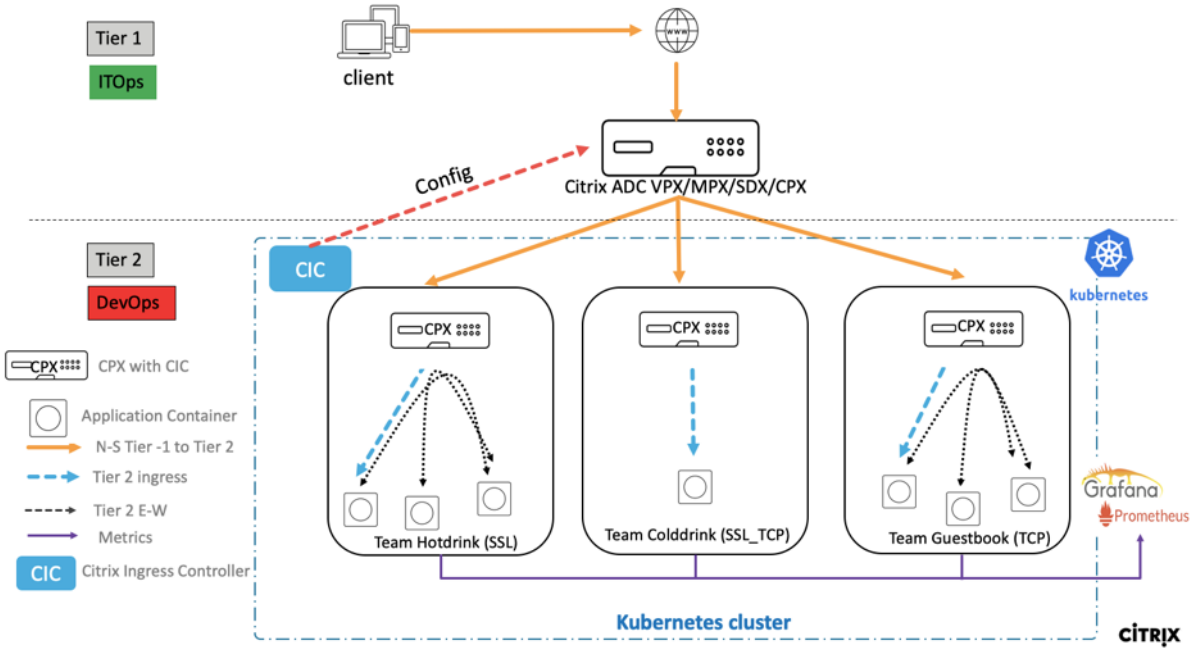
Déploiement d'entrée à deux niveaux sur GCP

Dans un déploiement d'entrée à deux niveaux, déployez Citrix ADC VPX/MPX à l'extérieur du cluster Kubernetes (Tier 1) et Citrix ADC CPX à l'intérieur du cluster Kubernetes (Tier 2).

Le VPX/MPX de niveau 1 équilibrerait la charge du CPX de niveau 2 dans le cluster Kubernetes. Il s'agit d'un modèle de déploiement générique largement utilisé indépendamment de la plate-forme, qu'il s'agisse de Google Cloud, d'Amazon Web Services, d'Azure ou d'un déploiement local.

Automatisation du niveau 1 VPX/MPX

La charge VPX/MPX de niveau 1 équilibre automatiquement les CPX de niveau 2. Le contrôleur d'entrée Citrix complète les configurations d'automatisation en s'exécutant en tant que module à l'intérieur du cluster Kubernetes. Il configure une classe d'entrée distincte pour le VPX/MPX de niveau 1 afin que la configuration ne se supervise pas avec d'autres ressources d'entrée.



Présentation du déploiement Citrix

Installer et configurer le Citrix ADC de niveau 1 sur GCP

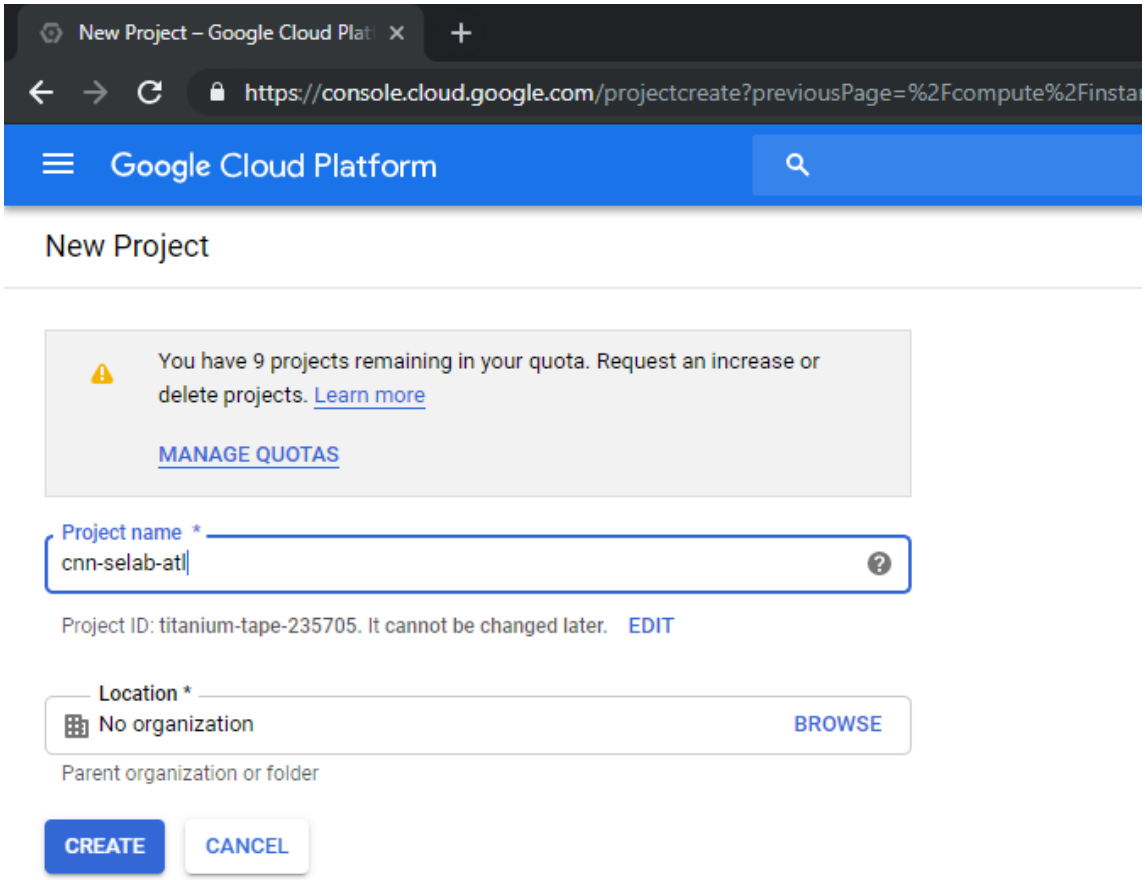
Vous pouvez déployer Citrix ADC à l'aide de l'une des options suivantes :

- **Interface graphique Google Cloud Platform :** pour plus d'informations sur la configuration du Citrix ADC de niveau 1 sur Google Cloud Platform via l'interface graphique, reportez-vous à la section Déployer une instance Citrix ADC VPX.
- **Gestionnaire de déploiement Google :** pour plus d'informations sur la configuration du Citrix ADC de niveau 1 sur Google Cloud Platform via des modèles GDM, reportez-vous à la section Déployer une instance Citrix ADC VPX à l'aide de modèles GDM.

Maintenant, vous devez déployer Citrix VPX (niveau 1-adc) à l'aide du modèle GDM 3-NIC.

Prérequis (obligatoire) :

1. Créer un compte GCP à l'aide de votre identifiant de messagerie Citrix uniquementhttp://console.cloud.google.com
2. Créez cnn-selab-atl comme nom de projet sur la console GCP :



3. Installez l'`gcloud` utilitaire sur votre appareil. Suivez le lien pour trouver l'utilitaire :https://cloud.google.com/sdk/install.
4. Authentifiez votre compte Google en utilisant gcloud API **gcloud auth login**.
5. Installez kubectl sur votre client :https://kubernetes.io/docs/tasks/tools/install-kubectl/
6. Exécutez la commande suivante sur l'`gcloud` utilitaire pour créer une image.

```
gcloud compute images create netscaler12-1 --source-uri=gs://tme-cpx-storage/NSVPX-GCP-12.1-50.28_nc.tar.gz --guest-os-features=MULTI_IP_SUBNET
<!--NeedCopy-->
```

Cela peut prendre un moment pour que l'image soit créée. Une fois l'image créée, elle apparaît sous **Calculer > Moteur de calcul** dans la console GCP.

Déployer un Citrix VPX (niveau 1-adc) sur GCP

1. **Instances VPC GCP :**
   pour traiter la séparation des réseaux externes, internes et DMZ à des fins de sécurité. Nous devons créer trois cartes réseau comme indiqué dans le tableau suivant :

Réseau	Commentaires
192.168.10.0/24	Réseau de gestion (vpx-snet-mgmt)
172.16.10.0/24	Réseau client (vpx-snet-vip)
10.10.10.0/24	Réseau serveur (vpx-snet-snip)

> Remarque :
>
> Construisez les VPC réseau à trois bras avant de déployer des instances de VM.

Un VPC peut être créé par SDK à l'aide d'API gcloud ou via Google Cloud Platform Console

VPC par l'API gcloud

Créer un VPC pour le trafic de gestion ou NSIP

```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-mgmt --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-mgmt --network=vpx-snet-mgmt --region=us-east1 --range=192.168.10.0/24
<!--NeedCopy-->
```

Créer un VPC pour le trafic client ou VIP

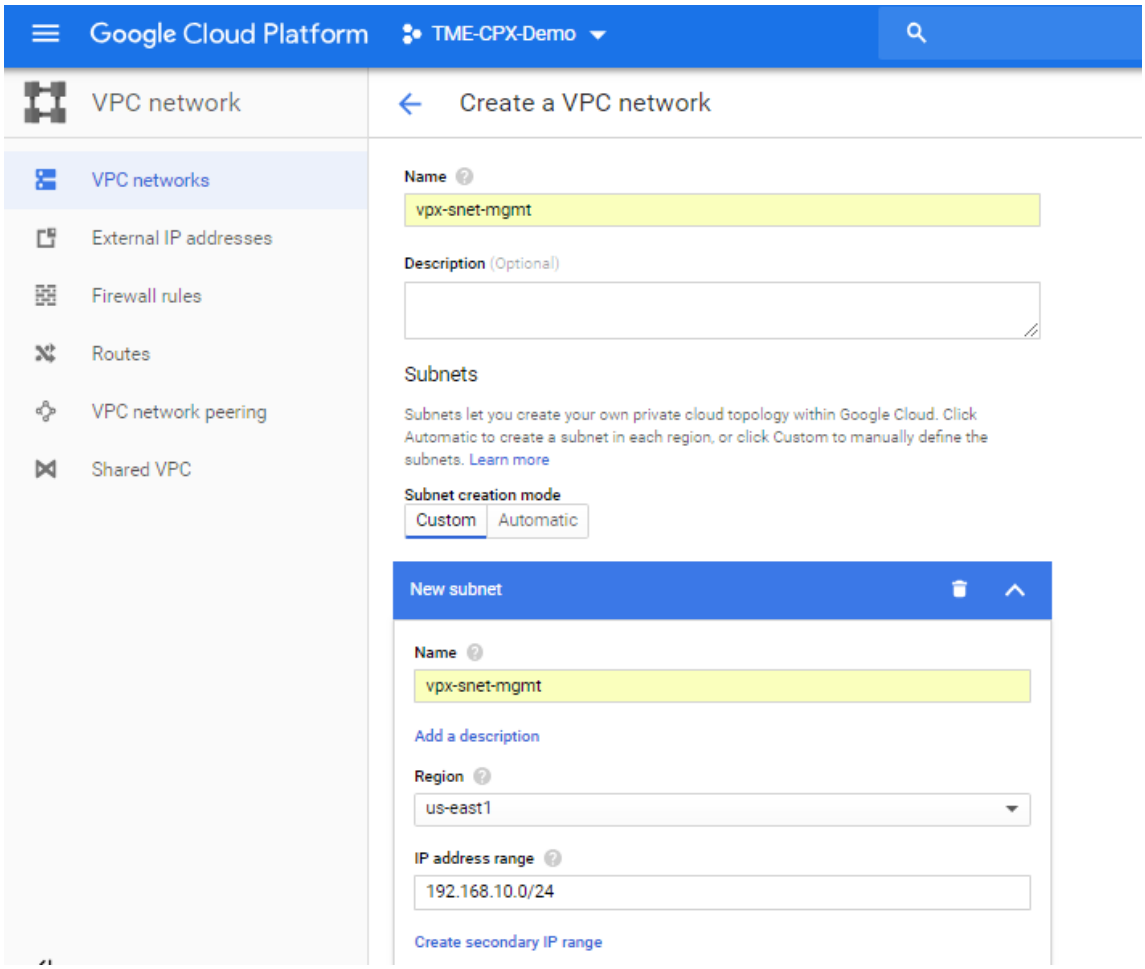
```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-vip --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-vip --network=vpx-snet-vip --region=us-east1 --range=172.16.10.0/24
<!--NeedCopy-->
```

Créer un VPC pour le trafic serveur ou SNIP où vous hébergez votre cluster kubernetes

```
gcloud compute --project=cnn-selab-atl networks create vpx-snet-snip --subnet-mode=custom
gcloud compute --project=cnn-selab-atl networks subnets create vpx-snet-snip --network=vpx-snet-snip --region=us-east1 --range=10.10.10.0/24
<!--NeedCopy-->
```


Console GUI VPC by GCP

Depuis la console Google, sélectionnez **Réseau > Réseau VPC > Créer un réseau VPC**et entrez les champs requis, comme indiqué ci-dessous. Cliquez ensuite sur **Créer**.



De même, créez des réseaux VPC pour les cartes réseau client et côté serveur pour créer trois sous-réseaux.

> Remarque :
>
> Les trois réseaux VPC devraient être dans la même région, qui est us-east1 dans ce scénario.

VPC networks CREATE VPC NETWORK REFRESH

Name	Region	Subnets	Mode	IP addresses ranges	Gateways
vpx-snet-vip		1	Custom		
	us-east1	vpx-snet-vip		172.16.10.0/24	172.16.10.1
vpx-snet-snip		1	Custom		
	us-east1	vpx-snet-snip		10.10.10.0/24	10.10.10.1
vpx-snet-mgmt		1	Custom		
	us-east1	vpx-snet-mgmt		192.168.10.0/24	192.168.10.1

2. Après avoir créé trois réseaux et trois sous-réseaux sous **VPC Network**, déployez l'instance Citrix ADC VPX à l'aide du modèle GDM. Assurez-vous que **configuration.yml** et **template.py** sont dans le même dossier ou répertoire. Utilisez la commande suivante du SDK Google pour déployer l'instance.

```
1  gcloud deployment-manager deployments create tier1-vpx --config
      configuration.yml
2  <!--NeedCopy-->
```

3. Après un déploiement réussi, accédez à **Compute Engine** pour vérifier la section **citrix-adc-tier1-vpx** et valider les adresses IP internes.

Name	Network	Subnetwork	Primary internal IP	Alias IP ranges	External IP
nic0	vpx-snet-mgmt	vpx-snet-mgmt	192.168.10.20	—	static-external-mgmt-ip-tier1-vpx (35.196.91.86)
nic1	vpx-snet-vip	vpx-snet-vip	172.16.10.20	—	static-external-traffic-ip-tier1-vpx (34.73.141.54)
nic2	vpx-snet-snip	vpx-snet-snip	10.10.10.20	—	None

Le contrôleur d'entrée Citrix peut automatiser la configuration d'itinéraire statique dans le VPX

de niveau 1. Configurez l'adresse IP du sous-réseau (SNIP) qui doit être du même cloud privé sous-net/virtuel du cluster Kubernetes.

> Remarque :
>
> Le VPX/MPX de niveau 1 déployé va équilibrer la charge CPX dans le cluster Kubernetes. Configurez le SNIP dans le VPX de niveau 1.

À partir d'une session PuTTY sur le VPX de niveau 1, exécutez les commandes suivantes pour ajouter SNIP et activer l'accès de gestion à SNIP :

```
clear config -force full
add ns ip 10.10.10.20 255.255.255.0 -type snip -mgmt enabled
enable ns mode mbf
<!--NeedCopy-->
```

Déployer un cluster Kubernetes à l'aide de GKE

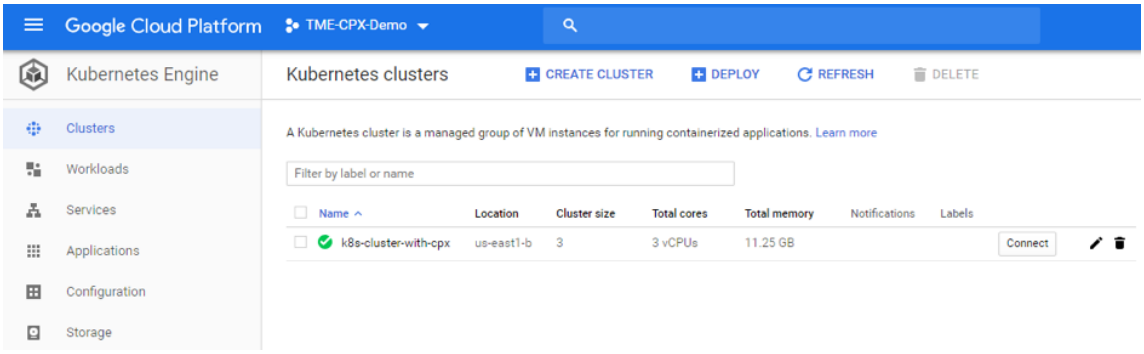
On peut déployer le cluster Kubernetes soit par ***Google Cloud SDK ou via la console graphique Google Cloud Platform***.

Commande de l'API Gcloud pour créer un cluster k8s

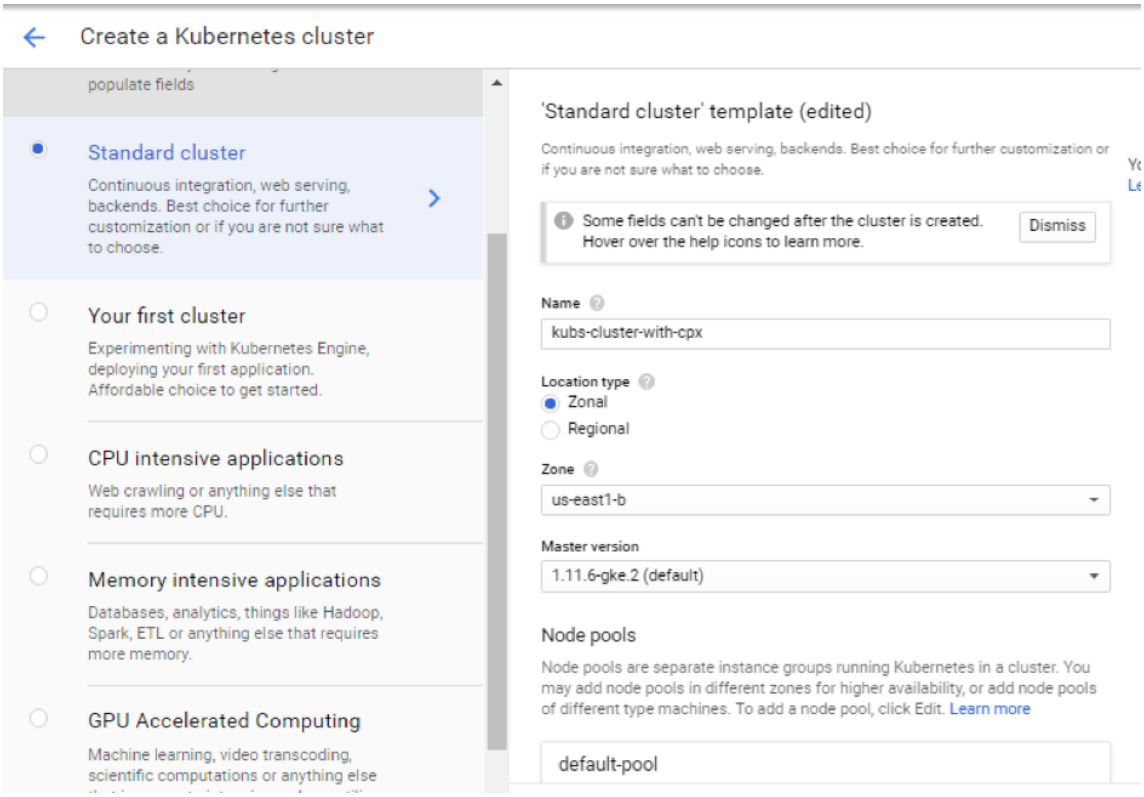
```
gcloud beta container --project "cnn-selab-atl" clusters create "k8s-
    cluster-with-cpx" --zone "us-east1-b" --username "admin" --cluster-
    version "1.11.7-gke.12" --machine-type "n1-standard-1" --image-type
    "COS" --disk-type "pd-standard" --disk-size "100" --scopes "https://
    www.googleapis.com/auth/devstorage.read_only","https://www.
    googleapis.com/auth/logging.write","https://www.googleapis.com/auth/
    monitoring","https://www.googleapis.com/auth/servicecontrol","https
    ://www.googleapis.com/auth/service.management.readonly","https://www
    .googleapis.com/auth/trace.append" --num-nodes "3" --enable-cloud-
    logging --enable-cloud-monitoring --no-enable-ip-alias --network "
    projects/cnn-selab-atl/global/networks/vpx-snet-snip" --subnetwork "
    projects/cnn-selab-atl/regions/us-east1/subnetworks/vpx-snet-snip"
    --addons HorizontalPodAutoscaling,HttpLoadBalancing --enable-
    autoupgrade --enable-autorepair
<!--NeedCopy-->
```

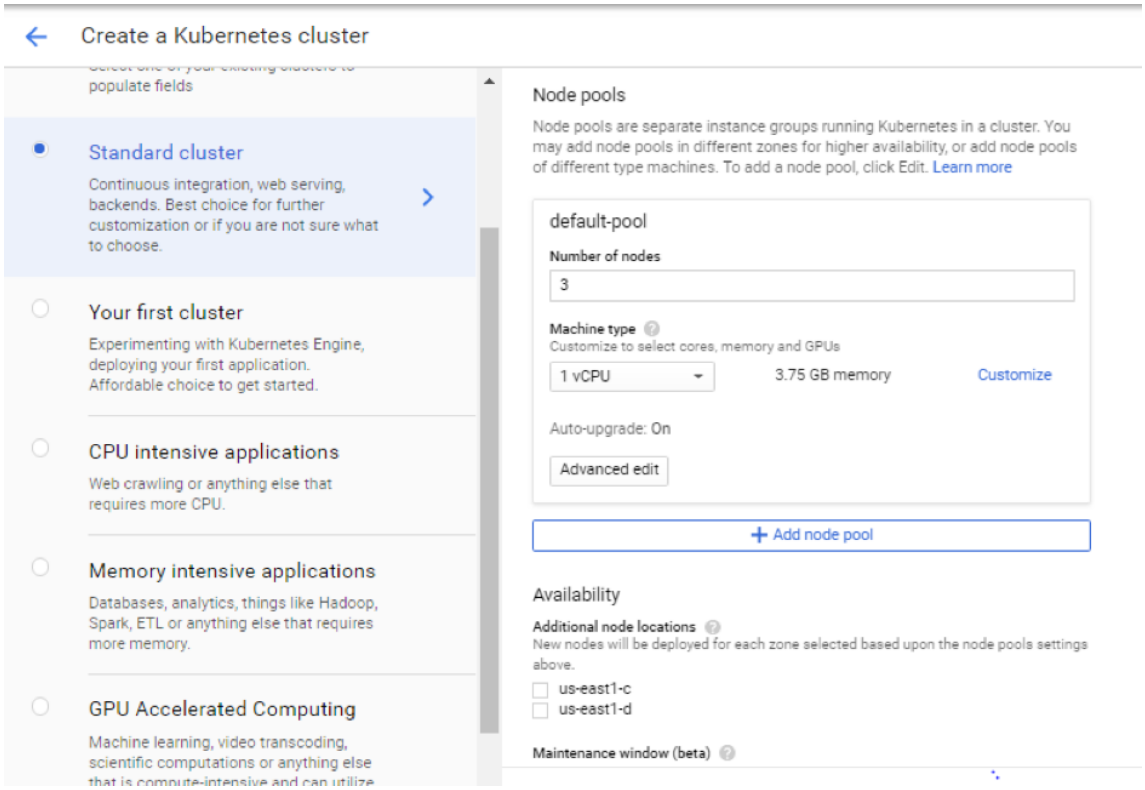
Procédure de console de Google Cloud Platform

1. Recherchez un moteur Kubernetes sur la console GCP et cliquez sur **Créer un cluster**.

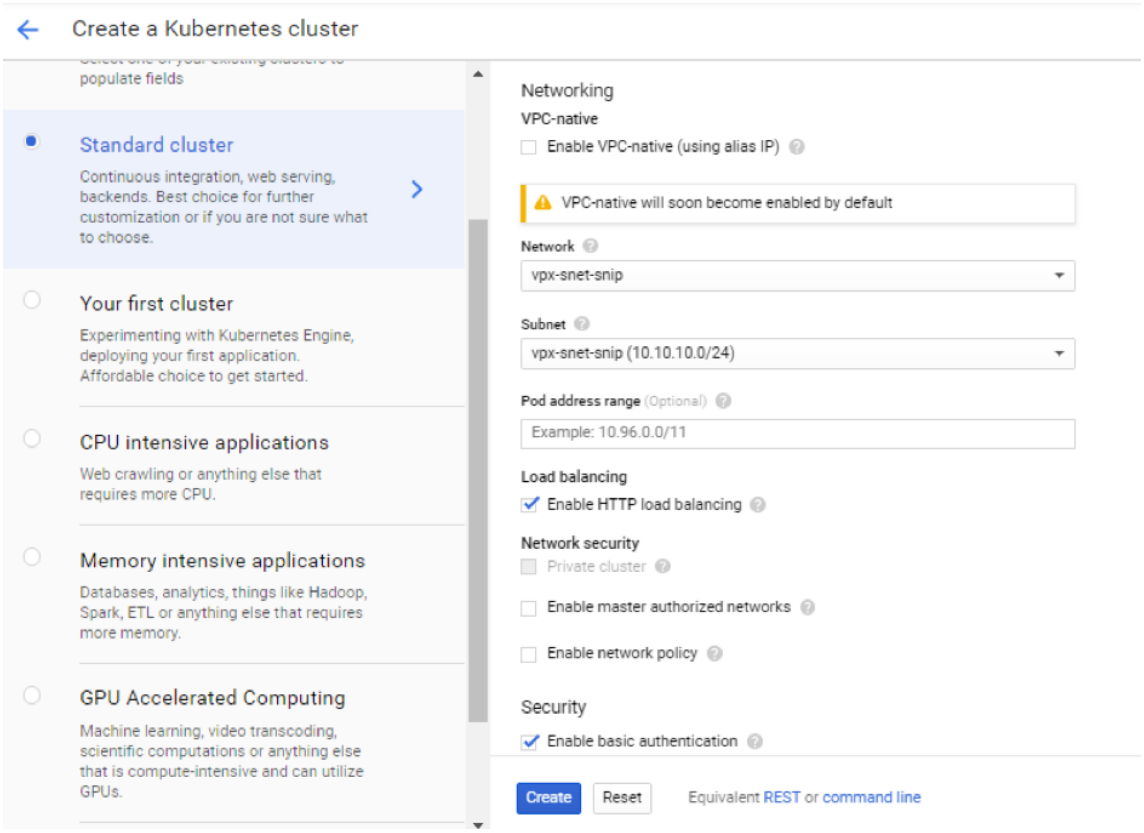


2. Créez un cluster dans le même sous-réseau où se trouve votre SNIP VPX (vpx-snet-snip). Ce cluster automatise la poussée de configuration dans l'ADC de niveau 1 à partir du contrôleur d'entrée Citrix dans le cluster K8s.





3. Cliquez sur **Options avancées** pour modifier le sous-réseau`vpx-snet-snip` et sélectionner les champs suivants.



4. Pour accéder à ce cluster à partir du SDK cloud, cliquez sur le bouton Kubernetes **Connect to the cluster** et collez la commande dans le SDK cloud.

5. Validez le déploiement du cluster GKE en exécutant la commande suivante :

```
kubectl get nodes
<!--NeedCopy-->
```

```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get nodes
NAME                                                STATUS    ROLES     AGE       VERSION
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-l15t   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xbvf   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xs47   Ready     <none>    2d        v1.11.6-gke.2
```


Déployer un exemple d'application à l'aide de l'exemple de bibliothèque de fichiers YAML

Citrix ADC offre la solution de déploiement d'architecture à deux niveaux pour équilibrer la charge des applications de niveau entreprise déployées dans des microservices et accessibles via Internet. Le niveau 1 dispose d'équilibreurs de charge lourds tels que VPX/SDX/MPX pour équilibrer la charge du trafic North-South. Le niveau 2 dispose d'un déploiement CPX pour gérer les microservices et équilibrer le trafic East-West.

1. Si vous exécutez votre cluster dans GKE, assurez-vous que vous avez utilisé la liaison de rôle de cluster pour configurer un cluster-admin. Vous pouvez le faire en utilisant la commande suivante.

```
kubectl create clusterrolebinding citrix-cluster-admin --
   clusterrole=cluster-admin --user=<email-id of your google
   account>.
<!--NeedCopy-->
```

2. Accédez au répertoire courant où vous avez les fichiers YAML de déploiement. Exécutez la commande suivante pour obtenir l'état du nœud.

```
kubectl get nodes
<!--NeedCopy-->
```

```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get nodes
NAME                                                STATUS    ROLES     AGE       VERSION
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-l15t   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xbvf   Ready     <none>    2d        v1.11.6-gke.2
gke-k8s-cluster-with-cpx-default-pool-8c0d6de1-xs47   Ready     <none>    2d        v1.11.6-gke.2
```

3. Créez les espaces de noms :

```
kubectl create -f namespace.yaml
<!--NeedCopy-->
```

   Vérifiez la commande namespace :

```
kubectl get namespaces
<!--NeedCopy-->
```



```
C:\Program Files (x86)\Google\Cloud SDK\GCP_SE_2019\Multitier-Hairpin>kubectl get namespaces
NAME              STATUS    AGE
default           Active    2d
kube-public       Active    2d
kube-system       Active    2d
monitoring        Active    10h
team-colddrink    Active    10h
team-guestbook    Active    10h
team-hotdrink     Active    10h
tier-2-adc        Active    10h
```

4. Déployez le rbac.yaml dans l'espace de noms par défaut.

```
kubectl create -f rbac.yaml
<!--NeedCopy-->
```

5. Déployez le CPX pour les microservices de boissons chaudes, de boissons froides et de livres d'or à l'aide des commandes suivantes.

```
kubectl create -f cpx.yaml -n tier-2-adc
kubectl create -f hotdrink-secret.yaml -n tier-2-adc
<!--NeedCopy-->
```

6. Déployez les microservices à trois boissons chaudes — le microservice de type SSL avec l'architecture à épingle à cheveux.

```
kubectl create -f team_hotdrink.yaml -n team-hotdrink
kubectl create -f hotdrink-secret.yaml -n team-hotdrink
<!--NeedCopy-->
```

7. Déployez le microservice de boisson froide — le microservice de type SSL_TCP.

```
kubectl create -f team_colddrink.yaml -n team-colddrink
kubectl create -f colddrink-secret.yaml -n team-colddrink
<!--NeedCopy-->
```

8. Déployez le livre d'or — un microservice de type NoSQL.

```
kubectl create -f team_guestbook.yaml -n team-guestbook
<!--NeedCopy-->
```

9. Valider le CPX déployé pour les trois applications ci-dessus. Tout d'abord, obtenez les pods CPX déployés en tant que niveau 2-adc, puis obtenez l'accès CLI à CPX.

   ‘‘‘

   Pour obtenir les pods CPX dans l'espace de noms de niveau 2-adc, entrez : kubectl get pods -n tier-2-adc

Pour obtenir un accès CLI (bash) au conteneur CPX (hotdrinks-cpx pod), entrez :`kubectl exec -it "copy and paste hotdrink CPX pod name from the above step"bash -n tier-2-adc`.

Par exemple,

```
kubectl exec -it cpx-ingress-hotdrinks-768b674f76-pcnw4 bash -n tier-2-adc
```

Pour vérifier si le serveur CS est en cours d'exécution dans le hotdrink-cpx, entrez la commande suivante après l'accès root à CPX :`cli-script"sh csvs"`.

Par exemple,

```
root@cpx-ingress-hotdrinks-768b674f76-pcnw4:/## cli_script.sh "sh csvs"
```

10. Déployez le contrôleur d'entrée et d'entrée VPX dans l'espace de noms de niveau 2, qui configure VPX automatiquement. Citrix Ingress Controller (CIC) automatise l'adc de niveau 1 (VPX).

```
1 kubectl create -f ingress_vpx.yaml -n tier-2-adc
2 kubectl create -f cic_vpx.yaml -n tier-2-adc
3 <!--NeedCopy-->
```

11. Ajoutez les entrées DNS dans les fichiers hôtes de votre machine locale pour accéder aux microservices via Internet.

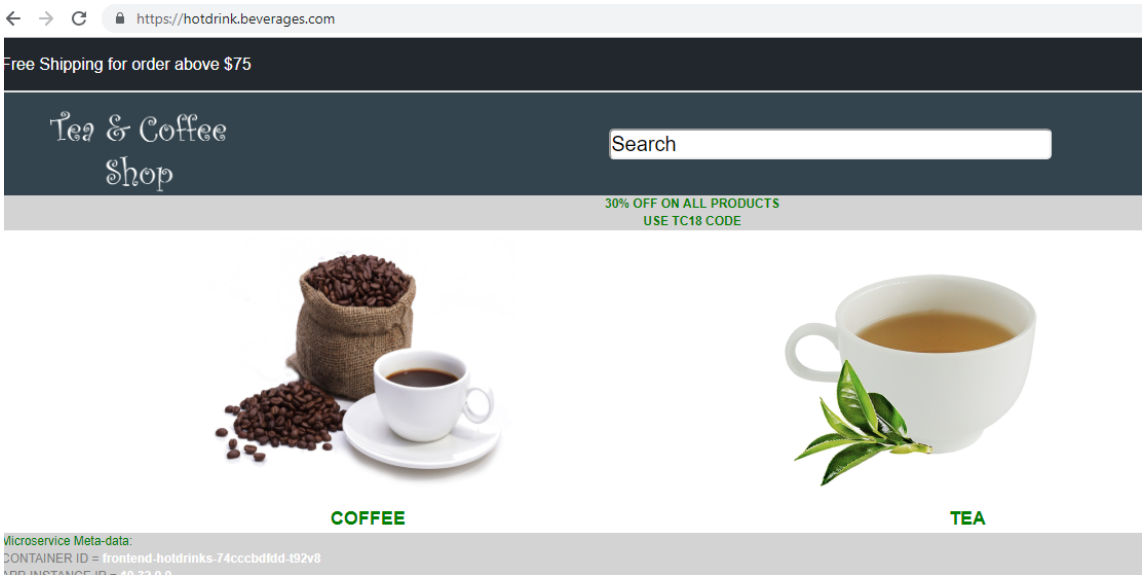
    Pour les clients Windows, accédez à : **C:\Windows\System32\drivers\etc\hosts**

    Pour les clients macOS, dans le Terminal, entrez : **sudo nano /etc/hosts '**

    Ajoutez les entrées suivantes dans le fichier de l'hôte et enregistrez le fichier.

```
1 hotdrink.beverages.com   xxx.xxx.xxx.xxx (static-external-traffic
     -ip-tier1-vpx)
2 colddrink.beverages.com  xxx.xxx.xxx.xxx (static-external-traffic
     -ip-tier1-vpx)
3 guestbook.beverages.com  xxx.xxx.xxx.xxx (static-external-traffic
     -ip-tier1-vpx)
4 grafana.beverages.com    xxx.xxx.xxx.xxx (static-external-traffic
     -ip-tier1-vpx)
5 prometheus.beverages.com xxx.xxx.xxx.xxx (static-external-traffic
     -ip-tier1-vpx)
6 <!--NeedCopy-->
```

12. Maintenant, vous pouvez accéder à chaque application sur Internet. Par exemple, `https://hotdrink.beverages.com`.



Activer les stratégies de réécriture et de répondeur pour l'exemple d'application

Il est maintenant temps de pousser les stratégies de réécriture et de réponse sur VPX via la définition de ressource personnalisée (CRD).

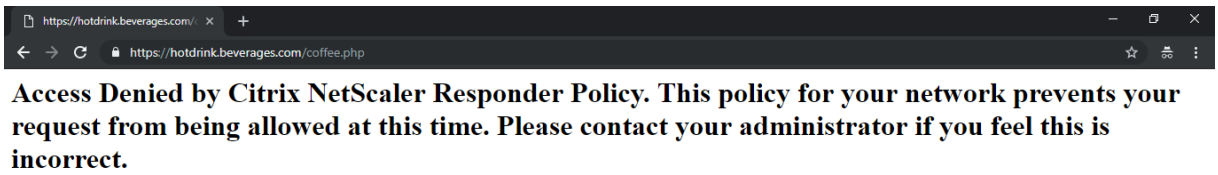
1. Déployez le CRD pour pousser les stratégies de réécriture et de réponse vers le niveau 1-adc dans l'espace de noms par défaut.

```
1    kubectl create -f crd_rewrite_responder.yaml
2    <!--NeedCopy-->
```

1. **URL de liste noire** Configurez la stratégie Responder surhotdrink.beverages.com pour bloquer l'accès à la page café.

```
1    kubectl create -f responderpolicy_hotdrink.yaml -n tier-2-adc
2    <!--NeedCopy-->
```

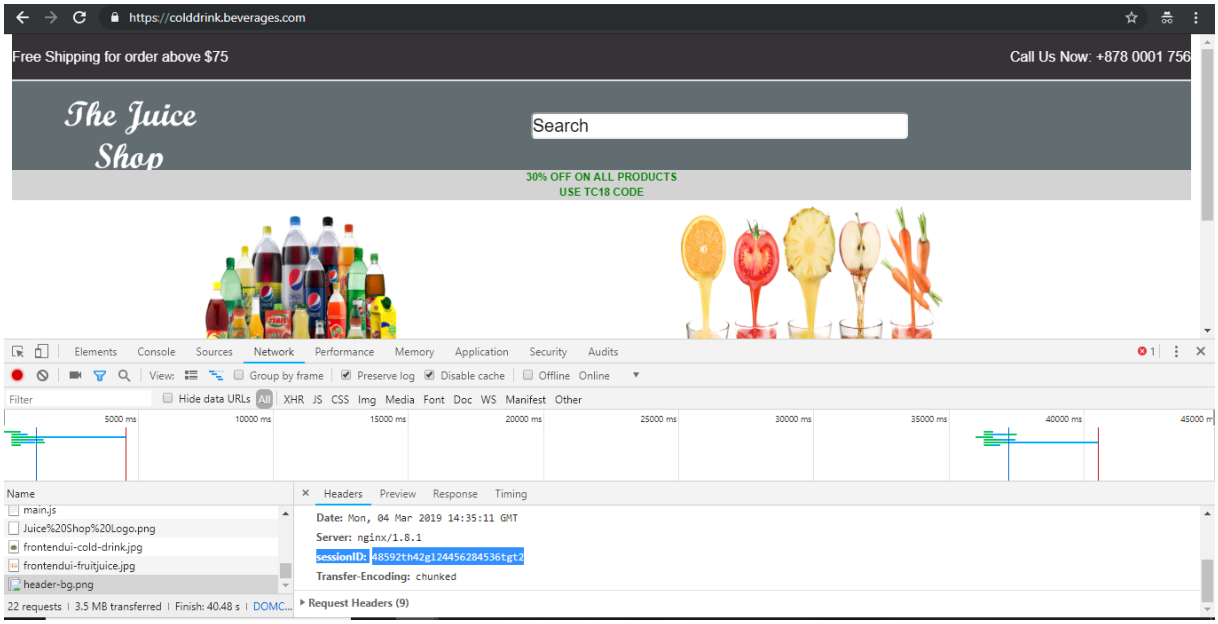
Après avoir déployé la stratégie Responder, accédez à la page café surhotdrink.beverages.com. Ensuite, vous recevez le message suivant.



1. **Insertion d'en-tête** Configurez la stratégie de réécriture surcolddrink.beverages.com pour insérer l'ID de session dans l'en-tête.

```
1    kubectl create -f rewritepolicy_colddrink.yaml -n tier-2-adc
2    <!--NeedCopy-->
```

Après avoir déployé la stratégie de réécriture, accédezcolddrink.beverages.com au mode développeur activé sur le navigateur. Dans Chrome, appuyez sur F12 et conservez le journal dans la catégorie réseau pour afficher l'ID de session, qui est inséré par la stratégie de réécriture sur le niveau 1-adc (VPX).



Jeux d'outils Open Source

1. Déployez les outils de surveillance de la Cloud Native Computing Foundation (CNCF), tels que Prometheus et Grafana, pour collecter les statistiques de proxy ADC.

```
1   kubectl create -f monitoring.yaml -n monitoring
2   kubectl create -f ingress_vpx_monitoring.yaml -n monitoring
3   <!--NeedCopy-->
```

Agrégateur de log Prométhée

1. Connectez-voushttp://grafana.beverages.com et effectuez la configuration unique suivante.

    a) Connectez-vous au portail à l'aide des informations d'identification d'administrateur.

b) Cliquez sur **Ajouter une source de données** et sélectionnez la source de données **Prometheus** .

c) Configurez les paramètres suivants et cliquez sur le bouton **Enregistrer et tester** .

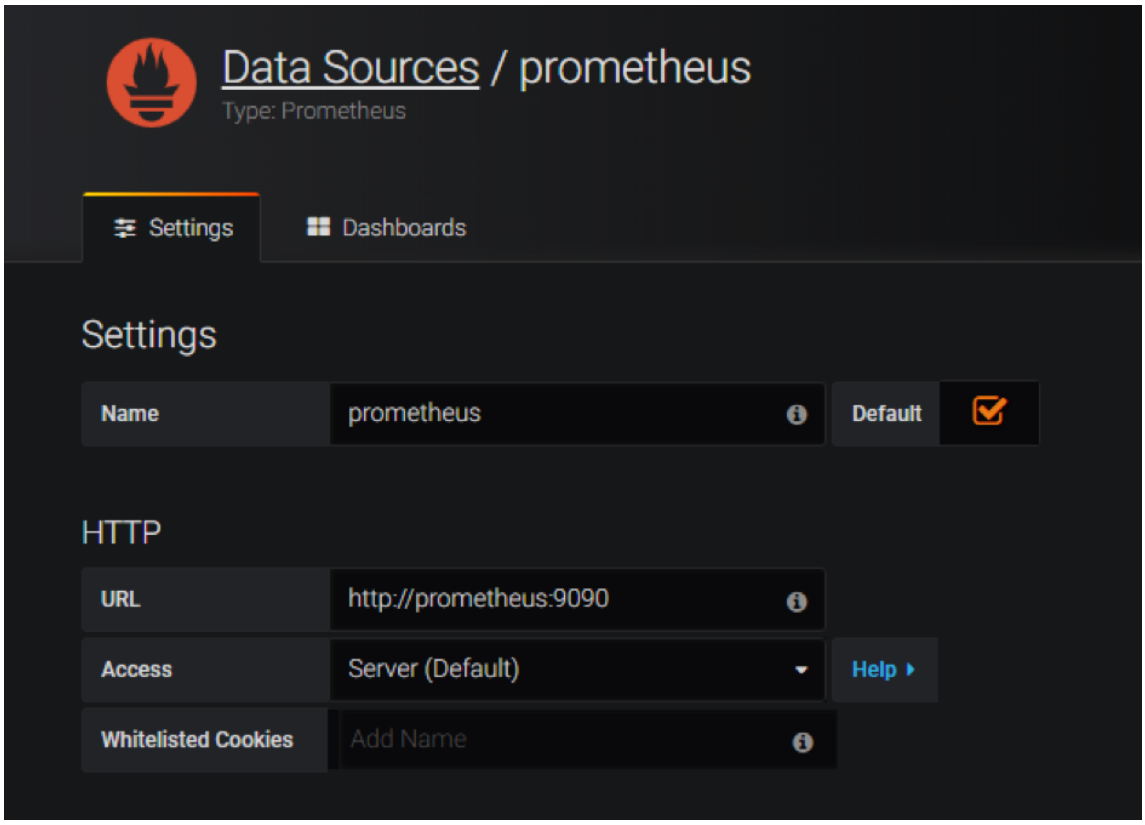
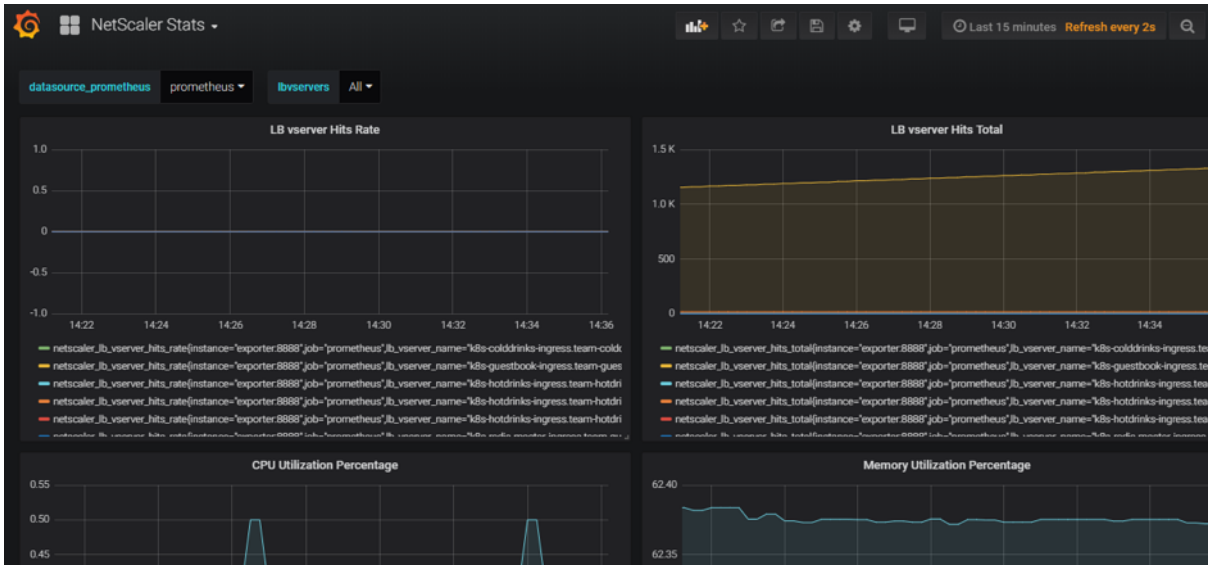


Tableau de bord visuel Grafana

1. Dans le panneau de gauche, sélectionnez l'option **Importer** et téléchargez le`grafana_config.json` fichier fourni dans le`yamlFiles` dossier. Vous pouvez maintenant voir le tableau de bord Grafana avec les statistiques ADC de base répertoriées.

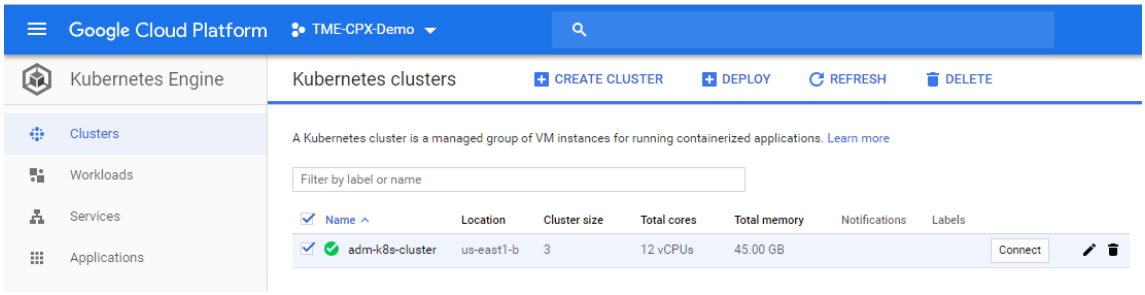


Supprimer un déploiement

1. Pour supprimer le déploiement Citrix VPX (niveau 1-adc), accédez à la console Google SDK CLI pour supprimer l'instance :

```
gcloud deployment-manager deployments delete tier1-vpx
<!--NeedCopy-->
```

2. Pour supprimer le cluster GKE Kubernetes, accédez à la console GCP, sélectionnez le cluster kubernetes et cliquez sur **Supprimer** pour effacer le cluster.



Modèle de conception validé du clustering Citrix ADC

January 8, 2020

Un cluster Citrix ADC est un groupe d'appliances Citrix ADC nCore qui travaillent ensemble sous la forme d'une image système unique. Chaque appliance du cluster est appelée nœud. Un cluster Citrix

ADC peut inclure aussi peu que 2 ou 32 appliances virtuelles Citrix ADC nCore en tant que nœuds.

Le trafic client est distribué entre les nœuds pour fournir une haute disponibilité, un débit élevé et une évolutivité.

Pour créer un cluster, ajoutez les appliances Citrix ADC requises en tant que nœuds de cluster, configurez la communication entre les nœuds, configurez les liens vers les réseaux client et serveur, configurez les appliances Citrix ADC et configurez la distribution du trafic client et serveur.

Fonctionnalités de Citrix ADC prises en charge par un cluster

Le tableau suivant répertorie les fonctionnalités Citrix ADC qui sont entièrement prises en charge sur le cluster, qui ne fonctionnent que sur des nœuds de cluster individuels et qui ne sont pas prises en charge sur le cluster.

Matrice de prise en charge des fonctionnalités de Citrix ADC :

Fonctionnalités prises en charge	Fonctionnalités prises en charge au niveau du nœud	Fonctionnalités non prises en charge
Équilibrage de charge	Protection contre les surtensions	Équilibrage de charge DNS
Persistance de l'équilibrage de charge	Bien sûr Connect	Équilibrage de charge FTP
SIP	File d'attente prioritaire	Équilibrage global de charge serveur (GSLB)
maxClient	Protection HTTP par déni de service (HTTP DoSP)	Citrix ADC Push
Spillover	Mise en cache intégrée	RTSP
Politique de PI SSL	Call Home	Basculement avec état de connexion
Commutation de contenu		Arrêt gracieux
Redirection du cache		Auto Scaling DBS
Contrôle de compression		DSR utilisant TOS
Filtrage de contenu		Spillover basé sur la bande passante
OSPF (IPv4 et IPv6)		Contrôle de démarrage plus précis
RIP (IPv4 et IPv6)		Limitation de taux

Fonctionnalités prises en charge	Fonctionnalités prises en charge au niveau du nœud	Fonctionnalités non prises en charge
BGP (IPv4 et IPv6)		Analyses de flux
Injection HTML		Profil net
Mise en mémoire tampon TCP		Mise en cache DNS
Déni de service distribué (DDoS)		SSL-VPN
Mise en réseau de base (IPv4 et IPv6)		Stratégie CPE SSL
VLAN		Pare-feu d'application
ICMP		AAA
Fragmentation		Cloud Bridging-Tunneling
Transfert basé sur Mac (MBF)		Layer2 Mode
RNAT		FIPS
INAT		XML XSM
KRPC		AAA-TM
ACL		VMAC/VRRP
ACL simple		Équilibrage de la charge de liaison
PBR		Tunneling IP
SNMP GET/SET, Walk		DHCP RA
Traps SNMP		Groupe de ponts
Infrastructure des politiques (PE/PI)		Pont réseau
API NITRO		Interface Web sur Citrix ADC
AppExpert		Surveillance EdgeSight
Réécrire		BR LB
Répondeur		Routage ISIS
Utiliser l'IP source (USIP)		FIS (ensemble d'interfaces de basculement)

Fonctionnalités prises en charge	Fonctionnalités prises en charge au niveau du nœud	Fonctionnalités non prises en charge
Exportateur AppFlow et collecteur Appflow (client) avec graphique en cascade		
DataStream		
MSR		
RNAT basé sur des politiques		
Journalisation Web		
Audit (syslog et nsauditlog)		
Découverte MTU de chemin		
Client Keep-Alive		

Configuration matérielle et logicielle requise

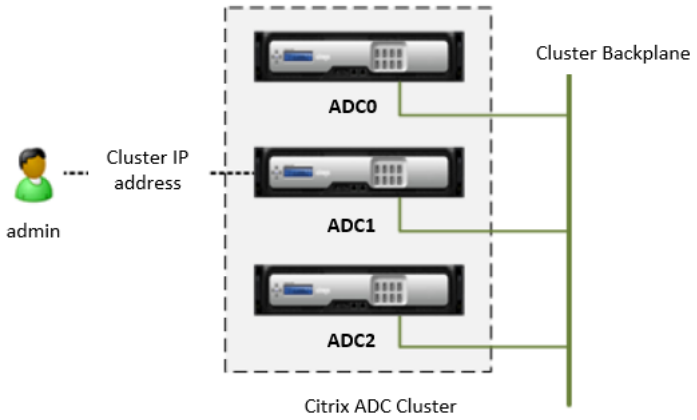
Les appliances que vous ajoutez à un cluster Citrix ADC doivent satisfaire aux exigences suivantes :

- Êtes des appliances Citrix ADC nCore. Le clustering des appliances Citrix ADC Classic n'est pas pris en charge.
- Être du même type de plate-forme (appliance physique ou instance VPX).
- Être du même type de matériel (pour les appareils physiques).
- Être sur le même sous-réseau.
- Avoir le fichier de licence de cluster.
- Avoir les mêmes licences (Standard, Enterprise ou Platinum, et toutes les licences complémentaires).
- Être de la même version du logiciel et construire.
- Être initialement configuré et connecté à un réseau côté client et côté serveur commun.

Fonctionnement du clustering

Un cluster Citrix ADC est formé en regroupant les appliances Citrix ADC qui répondent aux exigences spécifiées dans laConfiguration matérielle et logicielle requise. L'un des nœuds de cluster est désigné en tant que coordinateur de configuration (CCO). Comme son nom l'indique, le CCO coordonne toutes les configurations de cluster via l'adresse IP de gestion du cluster, appelée adresse IP du cluster.

Le cluster doit être configuré en accédant au CCO via l'adresse IP du cluster, comme indiqué dans la figure suivante :



> Remarque :
>
> Vous ne pouvez pas configurer un nœud individuel en y accédant via l'adresse IP ADCIP (Citrix ADC). Les nœuds accessibles via l'adresse ADCIP sont disponibles en mode lecture seule. Cela signifie que vous ne pouvez afficher que les configurations et les statistiques. Cependant, certaines commandes peuvent être exécutées sur des nœuds individuels. Pour plus d'informations, reportez-vous à la section Opérations prises en charge sur des nœuds individuels.

Les adresses VIP que vous définissez sur un cluster sont disponibles sur tous les nœuds du cluster (*adresses répartie*). Vous pouvez définir des adresses SNIP pour être disponibles sur tous les nœuds (adresses par bandes) ou uniquement sur un seul nœud (*adresses ponctuées*). Les détails de la distribution du trafic dans un cluster dépendent de l'algorithme utilisé, mais les mêmes entités logiques traitent le trafic dans chaque cas.

Synchronisation de cluster

Lorsqu'un nœud est ajouté au cluster, les configurations Citrix ADC et les fichiers (par exemple, certificats SSL, licences et DNS) disponibles sur le CCO sont synchronisés sur le nœud de cluster nouvellement ajouté. Cela garantit que les configurations et les fichiers sont toujours synchronisés sur tous les nœuds du cluster.

Lorsqu'un nœud de cluster existant rejoint le cluster (après qu'il a échoué ou a été délibérément désactivé), le cluster vérifie les configurations disponibles sur le nœud. En cas de non-concordance entre les configurations disponibles sur le nœud rattaché et sur le CCO, le nœud est synchronisé à l'aide de l'une des techniques suivantes :

- **Full synchronization.** Si la différence entre les configurations dépasse 255 commandes, toutes les configurations implémentées sur le CCO sont appliquées au nœud qui rejoint le cluster. Le nœud reste opérationnel indisponible pendant la durée de la synchronisation.
- **Synchronisation incrémentielle.** Si la différence entre les configurations est inférieure ou égale à 255 commandes, seules les configurations qui ne sont pas disponibles sont appliquées au nœud qui rejoint le cluster. L'état opérationnel du nœud reste inchangé.

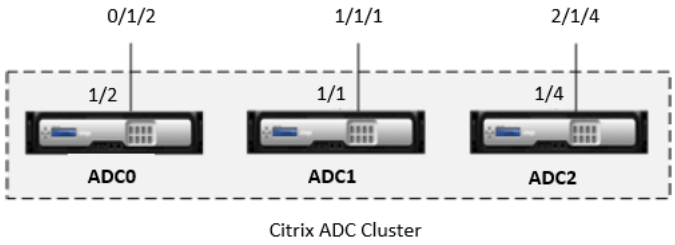
Les configurations effectuées sur le CCO via l'adresse IP du cluster sont automatiquement propagées aux nœuds du cluster. Étant donné que les configurations de cluster sont basées sur un quorum des nœuds disponibles, une commande (exécutée sur l'adresse IP du cluster) peut être propagée aux autres nœuds de cluster uniquement lorsque la majorité des nœuds sont synchronisés. Si la plupart des nœuds ne sont pas synchronisés ou sont en cours de synchronisation, ils ne peuvent pas accepter de nouvelles commandes et, par conséquent, les commandes ne sont pas propagées tant que la synchronisation n'est pas terminée.

Connexions de cluster

Pour identifier le nœud auquel appartient une interface, la convention de dénomination d'interface Citrix ADC standard est préfixée par un ID de nœud. Autrement dit, l'identificateur d'interface **c/u**, où **c**est le numéro du contrôleur et **u**est le numéro d'unité, devient **n/c/u**, où **n**est l'ID du nœud.

Par exemple, dans la figure suivante, l'interface **1/2** du nœud 0 est représentée par **0/1/2** , l'interface **1/1** du nœud 1 est représentée par **1/1/1** et l'interface **1/4** du nœud 2 est représentée par **2/1/4** .

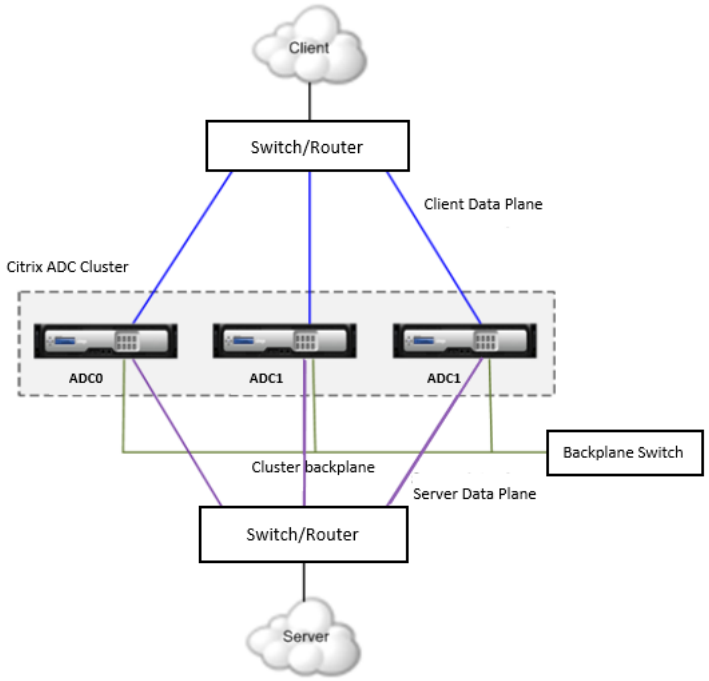
Convention de nom pour les interfaces réseau dans un cluster



Le cluster communique avec le client via les connexions physiques entre le nœud de cluster et le *périphérique de connexion côté client*. Le regroupement logique de ces connexions physiques est appelé plan de données client. De même, le cluster communique avec le serveur via les connexions physiques entre les nœuds de cluster et le périphérique de connexion côté serveur. Le regroupement logique de ces connexions physiques est appelé *plan de données du serveur*.

En plus de communiquer avec le client et le serveur via le plan de données client et le plan de données serveur respectivement, les nœuds de cluster communiquent entre eux à l'aide du *fond de panier du cluster*. Le fond de panier, qui comprend les connexions physiques de chaque nœud de cluster et le commutateur de fond de panier, est l'épine dorsale du système de cluster.

Interfaces de communication en cluster



La figure ci-dessus montre le regroupement logique des connexions physiques pour former le plan de données client, le plan de données serveur et le fond de panier de cluster.

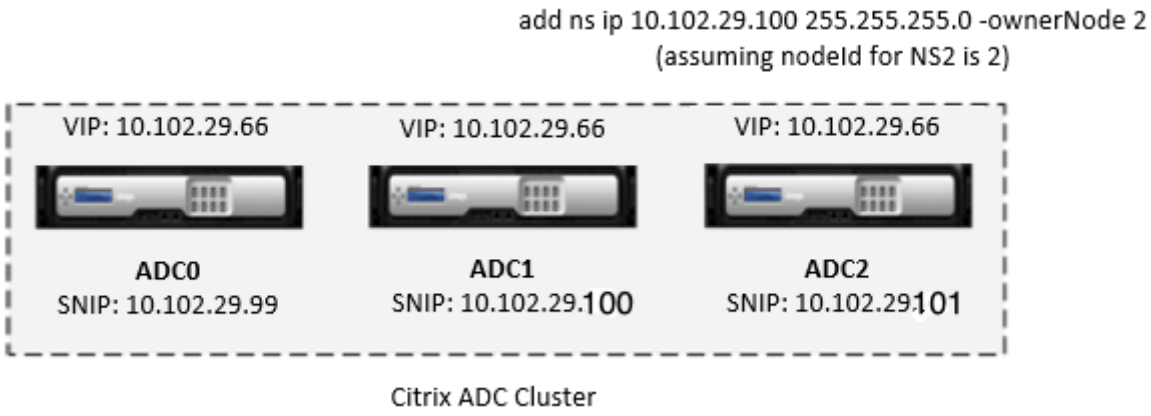
Adresses IP striped et spotted

Dans un déploiement en cluster, les adresses VIP et SNIP peuvent être répartie ou repérées.

- Une *adresse IP ré* partie est active sur tous les nœuds du cluster. Les adresses IP configurées sur le cluster sans spécifier de nœud propriétaire sont actives sur tous les nœuds de cluster.
- Une *adresse IP ponctuée* est active sur et appartient exclusivement à un nœud. Les adresses IP configurées sur le cluster en spécifiant un nœud propriétaire sont actives uniquement sur le nœud spécifié en tant que propriétaire.

La figure suivante montre les adresses IP rayées et repérées dans un cluster à trois nœuds.

Cluster à trois nœuds avec adresses IP striped et spotted



Dans la figure ci-dessus, l'adresse VIP 10.102.29.66 est répartie sur tous les nœuds de cluster, et l'adresse SNIP 10.102.29.99 est répartie sur ADC0 et ADC1. ADC2 a une adresse SNIP repérée.

Le tableau suivant présente les adresses IP appartenant à Citrix ADC qui peuvent être répartie ou repérées :

Adresses IP striped et spotted

Adresses IP appartenant à Citrix ADC	Adresses IP par bandes	Adresses IP repérées
ADCIP	Non	Oui
Adresse IP du cluster	Non	Non
VIP	Oui	Non
SNIP	Oui	Oui (recommandé)

> Remarque :
>
> - L'adresse IP du cluster n'est pas une adresse IP répartie ou ponctuée. Il s'agit d'une adresse IP flottante appartenant à l'OCC, qui n'est pas un nœud fixe.
> - Citrix vous recommande d'utiliser uniquement des adresses IP ponctuées. Vous pouvez utiliser des adresses IP répartie uniquement en cas de pénurie d'adresses IP. L'utilisation d'adresses IP par bandes peut entraîner des problèmes de flux ARP.

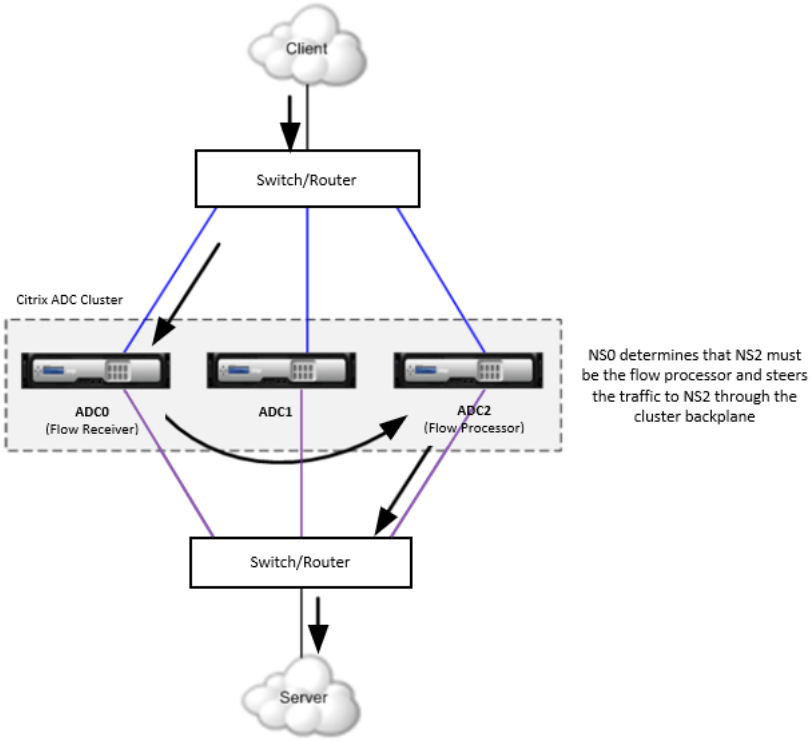
Répartition du trafic

Le cluster Citrix ADC utilise des mécanismes de distribution de trafic ECMP (Equal Cost Multiple-path) ou CLAG (Cluster Link Aggregation Group) pour déterminer le nœud qui reçoit le trafic (le *récepteur de flux*) à partir du périphérique de connexion externe. Chacun de ces mécanismes utilise un algo-

rithme différent pour déterminer le récepteur de débit. Le récepteur de flux utilise ensuite la logique de cluster interne pour déterminer le nœud qui traite le trafic (le *processeur de flux*).

> Remarque :
>
> Le récepteur de débit et le processeur de débit doivent être des nœuds capables de servir le trafic.

Distribution du trafic dans un cluster



La figure ci-dessus montre une demande client passant par le cluster. Le client envoie une requête à une adresse IP virtuelle (VIP) par bandes. Un mécanisme de distribution du trafic configuré sur le plan de données client sélectionne l'un des nœuds de cluster comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le nœud qui doit traiter le trafic et dirige la demande vers ce nœud à travers le fond de panier du cluster (sauf si le récepteur de flux se sélectionne comme processeur de flux).

Le processeur de flux établit une connexion avec le serveur. Le serveur traite la demande et envoie la réponse à l'adresse IP du sous-réseau (SNIP) qui a envoyé la demande au serveur.

- Si l'adresse SNIP est une adresse IP répartie, le mécanisme de distribution du trafic configuré sur le plan de données du serveur sélectionne l'un des nœuds de cluster (qui possède l'adresse SNIP) comme récepteur de flux. Le récepteur de flux reçoit le trafic, détermine le processeur de flux et dirige la demande vers le processeur de flux à travers le backplane du cluster.
- Si l'adresse SNIP est une adresse IP spotted, le nœud qui possède l'adresse SNIP reçoit la réponse du serveur.

Dans une topologie de cluster asymétrique (tous les nœuds de cluster ne sont pas connectés au commutateur externe), vous devez utiliser des *jeux de liens* exclusivement ou combinés avec ECMP ou CLAG. Pour plus d'informations, reportez-vous à la section Utilisation des jeux de liens.

État du cluster et du nœud

La classification des nœuds de cluster comprend trois types d'états : l'état d'administration, l'état opérationnel et l'état d'intégrité.

- **État d'administration**. Un état admin est configuré lorsque vous ajoutez le nœud au cluster. Il indique le but du nœud, qui peut être dans l'un des états suivants :
  - **ACTIF**. Les nœuds dans cet état servent le trafic s'ils sont opérationnels et sains.
  - **PASSIVE**. Les nœuds dans cet état ne servent pas le trafic, mais sont synchronisés avec le cluster. Ces nœuds sont utiles pendant l'activité de maintenance, car ils peuvent être mis à niveau sans supprimer le nœud du cluster.
  - **RECHANGE**. Les nœuds dans cet état ne servent pas le trafic, mais sont synchronisés avec le cluster. Les nœuds de rechange agissent comme des nœuds de sauvegarde pour le cluster. Si l'un des nœuds ACTIVE devient indisponible, l'état opérationnel de l'un des nœuds de secours devient ACTIVE et ce nœud commence à servir le trafic.
- **État opérationnel**. Lorsqu'un nœud fait partie d'un cluster, son état opérationnel peut passer à ACTIVE, INACTIVE ou INCONNU. Il y a plusieurs raisons pour lesquelles un nœud est en état INACTIVE ou INCONNU. Passez en revue les compteurs de`ns.log` fichiers ou d'erreurs pour déterminer la raison exacte.
- **État d'intégrité**. Selon son état d'intégrité, un nœud peut être UP ou NON UP. Pour afficher les raisons pour lesquelles un nœud est dans l'état NOT UP, exécutez la commande **show cluster node** pour ce nœud à partir de l'adresse IP du cluster.

Seuls les nœuds dont l'état administrateur est ACTIVE, l'état opérationnel est ACTIVE et l'état d'intégrité en tant que UP peuvent servir le trafic. Un cluster n'est fonctionnel que lorsqu'un minimum de nœuds (n/2 + 1), où n est le nombre de nœuds de cluster, sont capables de servir le trafic.

Configuration d'un cluster Citrix ADC

Pour configurer un cluster Citrix ADC, commencez par configurer le fond de panier du cluster. Ensuite, vous créez le cluster en ajoutant le premier nœud au cluster, qui devient le coordinateur de configuration initial (CCO), et en affectant une adresse IP de cluster à ce nœud. Une fois que l'adresse IP du cluster est définie sur le CCO, vous pouvez ajouter d'autres nœuds au cluster.

Chaque appliance que vous souhaitez ajouter au cluster doit :

- Êtes des appliances Citrix ADC nCore. Le clustering des appliances Citrix ADC Classic n'est pas pris en charge.
- Être du même type de plate-forme (appliance physique ou instance VPX).
- Être du même type de matériel (pour les appareils physiques).
- Être sur le même sous-réseau.
- Avoir le fichier de licence de cluster.
- Avoir les mêmes licences (Standard, Enterprise ou Platinum, et toutes les licences complémentaires).
- Être de la même version du logiciel et construire.
- Être initialement configuré et connecté à un réseau côté client et côté serveur commun.

Seules les appliances qui satisfont à tous les critères ci-dessus peuvent faire partie d'un cluster Citrix ADC.

Configuration du fond de panier du cluster

Les nœuds d'un cluster communiquent entre eux via le fond de panier du cluster. Le fond de panier est un ensemble de connexions dans lequel une interface de chaque nœud est connectée à un commutateur commun, appelé le commutateur de fond de panier de cluster. Chaque nœud du cluster utilise une adresse MAC spéciale pour communiquer avec d'autres nœuds via le fond de panier du cluster.

> Remarque :
>
> Dans un cluster d'appliances VPX déployées sur un XenServer (avec l'usurpation MAC activée), la carte réseau (XenServer Vswitch) peut supprimer les paquets envoyés sur le fond de panier. Vous devez donc vous assurer que l'usurpation MAC est désactivée sur le XenServer.
> Vous devez vous assurer que le commutateur de fond de panier de cluster prend en charge des paquets de plus de 1 500 octets.

Points à retenir :

- N'utilisez pas l'interface de gestion de l'appliance (0/1) comme interface de fond de panier.
- Les interfaces utilisées pour le fond de panier ne doivent pas être utilisées pour le plan de données client ou le plan de données serveur.
- Les interfaces de fond de panier de tous les nœuds d'un cluster doivent être connectées au même commutateur et liées au même VLAN L2. Par défaut, les interfaces de fond de panier sont présentes sur tous les VLAN L3 configurés sur le cluster.
- Si vous avez plusieurs clusters Citrix ADC avec le même ID d'instance de cluster, assurez-vous que les interfaces de fond de panier de chaque cluster sont liées à un VLAN différent.
- Citrix vous recommande de dédier un commutateur séparé uniquement pour le fond de panier, afin que de grandes quantités de trafic soient gérées de manière transparente.

- L'interface du backplane est toujours surveillée, quels que soient les paramètres de surveillance HA de cette interface.

Pour configurer le fond de panier du cluster, procédez comme suit pour chaque nœud :

1. Identifiez l'interface réseau que vous souhaitez utiliser pour le backplane.
2. Connectez un câble Ethernet ou optique à partir de l'interface réseau sélectionnée au commutateur de backplane de cluster.

Par exemple, pour utiliser l'interface 1/2 comme interface de backplane pour le nœud 4, connectez un câble de l'interface 1/2 du nœud 4 au commutateur de backplane.

> Remarque :
>
> Vous pouvez configurer un canal d'agrégation de liens (LA) pour optimiser le débit du fond de panier du cluster.

Création d'un cluster Citrix ADC

Pour créer un cluster, vous devez créer une instance de cluster et configurer une adresse IP de cluster sur la première solution matérielle-logicielle que vous ajoutez au cluster. Ce nœud est appelé le coordinateur de configuration (CCO). Toutes les configurations de cluster sont effectuées sur ce nœud, en y accédant via l'adresse IP du cluster. Le CCO n'est pas fixé à un nœud de cluster spécifique. Cela peut changer avec le temps. Par exemple, si le CCO tombe en panne, le cluster choisit l'un des autres nœuds comme nouveau CCO, qui possède ensuite l'adresse IP du cluster.

Lorsque vous ajoutez l'instance de cluster, la commande **clear ns config extended** est exécutée en interne sur ce nœud. En outre, les adresses SNIP et toutes les configurations VLAN (à l'exception du VLAN par défaut et de l'ADCVLAN) sont effacées du nœud.

> Remarque :
>
> Avant de créer le cluster, assurez-vous que vous avez configuré l'
> interface de fond de panier pour ce nœud.

Pour créer un cluster à l'aide de la ligne de commande Citrix ADC

> Remarque :
>
> Les commandes suivantes incluent uniquement les paramètres obligatoires. Pour plus d'informations sur les commandes CLI, consultez les pages de **manuel** disponibles pour chaque commande. Tapez `man <command syntax>`. Par exemple, pour obtenir la page de **manuel** de la commande add cluster instance, tapez`man add cluster instance` .

1. Ouvrez une session sur un appliance Citrix ADC (par exemple, une appliance avec l'adresse ADCIP 10.102.29.60) que vous avez l'intention d'ajouter au cluster.

2. Ajoutez une instance de cluster. L'instance de cluster est une entité qui identifie le cluster. Tapez, `add cluster instance <clId>`. Où, **clId** est un numéro unique qui identifie le cluster. Valeur minimale : 1. Valeur maximale : 16.

> Remarque :
>
> Assurez-vous que l'ID d'instance de cluster est unique dans un réseau local.

1. Ajoutez le dispositif Citrix ADC au cluster. Tapez, `add cluster node <nodeId> <IPAddress> [-state <state>] [-backplane <interface_name>]`. où,

   - **NodeID** est un numéro unique qui identifie l'appliance sur le cluster. Chaque nœud doit avoir un ID de nœud différent. Valeur minimale : 0. Valeur maximale : 31.
   - **Adresse IP** est l'adresse IP de l'appliance Citrix ADC. Seules les adresses IPv4 sont prises en charge.
   - **état** est l'état configuré du nœud de cluster. Valeurs possibles : ACTIVE, PASSIVE, SPARE. Par défaut : PASSIVE.

   > Remarque :
   >
   > Si vous souhaitez effectuer des configurations spécifiques au nœud, telles que l'ajout d'adresses IP ponctuées, avant que le nœud ne serve le trafic, définissez l'état sur PASSIVE (état par défaut). Après avoir effectué les configurations spécifiques aux nœuds, changez l'état du nœud en ACTIVE à l'aide de la commande **set cluster node** .

   - **backplane** est l'interface de fond de panier du nœud. Par exemple, si le nœud 0 utilise l'interface 1/1, la valeur de ce paramètre est 0/1/1.

   Par exemple,

   ```
   add cluster node 0 10.102.29.60 -state PASSIVE -backplane 0/1/1
   <!--NeedCopy-->
   ```

2. Ajoutez l'adresse IP du cluster (par exemple, 10.102.29.61) sur ce nœud. Tapez, `add ns ip <IPAddress> <netmask> -type clip`. où,

   - **IPAddress** est l'adresse IP du cluster Citrix ADC. Seules les adresses IPv4 sont prises en charge.
   - **netmask** est le masque de sous-réseau de l'adresse IP du cluster. La valeur doit être 255.255.255.255.

   Par exemple,

   ```
   add ns ip 10.102.29.61 255.255.255.255 -type clip
   <!--NeedCopy-->
   ```

3. Activez l'instance de cluster pour créer le cluster. Tapez, `enable cluster instance <clId>`. Où, **CLID** est le numéro qui identifie l'instance de cluster qui doit être activée.

4. Enregistrez la configuration. Tapez, `save ns config`.
5. Réinitialisez l'appliance à chaud. Tapez, `reboot -warm`.

Vérifiez les configurations de cluster à l'aide de la commande show cluster instance. La sortie de la commande doit afficher l'adresse ADCIP du CCO en tant que nœud du cluster.

Pour créer un cluster à l'aide de l'utilitaire de configuration

1. Ouvrez une session sur un appliance Citrix ADC (par exemple, une appliance avec l'adresse ADCIP 10.102.29.60) que vous avez l'intention d'ajouter au cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Démarrer**, cliquez sur **Gérer le cluster**.
4. Dans la boîte **de dialogue Configuration du cluster** , définissez les paramètres suivants :
   - **ID d'instance de cluster** : numéro unique qui identifie le cluster. Valeur minimale : 1. Valeur maximale : 16.
   - **Adresse IP du cluster** : adresse IP du cluster Citrix ADC. Seules les adresses IPv4 sont prises en charge.
   - **Backplane** - Interface backplane du nœud. Par exemple, si le nœud 0 utilise l'interface 1/1, la valeur de ce paramètre est 1/1.
5. Cliquez sur **Créer**.
6. Dans la boîte de dialogue **Configurer l'instance de cluster** , assurez-vous que la case à cocher **Activer l'instance de cluster** est activée.
7. Dans le volet **Noeuds de cluster** , sélectionnez le nœud et cliquez sur **Ouvrir** .
8. Dans la boîte de dialogue **Configurer le nœud de cluster** , définissez la valeur **tate** .
9. Cliquez sur **OK**, puis sur **Enregistrer**.
10. Réinitialisez l'appliance à chaud.

Ajout d'un nœud au cluster

Vous pouvez facilement redimensionner la taille d'un cluster pour inclure un maximum de 32 nœuds. Lorsqu'une solution matérielle-logicielle est ajoutée au cluster, les licences de ce dispositif sont vérifiées par rapport aux licences disponibles sur le CCO. Si les licences correspondent, la solution matérielle-logicielle est ajoutée au
cluster. Les configurations existantes du nœud sont effacées et les configurations de cluster sont synchronisées avec le nœud. Il peut y avoir une baisse intermittente du trafic pendant que la synchronisation est en cours.

Pour ajouter un nœud à un cluster, vous devez d'abord configurer le nœud sur le cluster (en ajoutant le nœud), puis configurer le cluster sur le nœud (en joignant le cluster).

Si vous utilisez la ligne de commande Citrix ADC, connectez-vous d'abord à l'adresse IP du cluster pour ajouter le nœud. Ensuite, connectez-vous à ce nœud et rejoignez le nœud au cluster. Si vous

utilisez l'utilitaire de configuration, vous devez uniquement vous connecter à l'adresse IP du cluster pour ajouter le nœud. Le nœud nouvellement ajouté est automatiquement joint au cluster. Vous pouvez également ajouter le nœud à partir de la ligne de commande et utiliser l'utilitaire de configuration pour joindre le nœud au cluster.

> Remarque :
>
> - Avant d'ajouter le nœud, assurez-vous que vous avez configuré l'interface de fond de panier pour ce nœud.
> - Lorsque vous ajoutez un nouveau nœud à un cluster qui n'a que des adresses IP repérées, la synchronisation se produit avant que les adresses IP repérées ne soient affectées à ce nœud. Dans de tels cas, les liaisons VLAN L3 et les routes statiques peuvent être perdues. Pour éviter cette perte, ajoutez une adresse IP par bandes ou ajoutez les liaisons VLAN L3 et les routes statiques sur l'ADCIP du nœud nouvellement ajouté.
> - Lorsqu'un dispositif Citrix ADC avec un canal d'agrégation de liens préconfiguré (LA) est ajouté à un cluster, les canaux LA continuent d'exister dans l'environnement de cluster. Le canal LA est renommé de LA/x en NodeId/LA/x, où LA/x est l'identificateur de canal LA.

Pour ajouter un nœud au cluster à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à l'adresse IP du cluster et procédez comme suit :
   - Ajoutez le dispositif Citrix ADC (par exemple, 10.102.29.70) au cluster. Tapez, `add cluster node <nodeId> <IPAddress> [-state <state>] [-backplane <interface_name>]`. où,
     - **NodeID** est un entier unique qui identifie la solution matérielle-logicielle sur le cluster. Chaque nœud doit avoir un ID de nœud différent. Valeur minimale : 0. Valeur maximale : 31.
     - **Adresse IP** est l'adresse IP de l'appliance Citrix ADC. Seules les adresses IPv4 sont prises en charge.
     - **état** est l'état configuré du nœud de cluster. Valeurs possibles : ACTIVE, PASSIVE, SPARE. Par défaut : PASSIVE.

       > Note :
       > Si vous souhaitez effectuer des configurations spécifiques au nœud, telles que l'ajout d'adresses IP ponctuées, avant que le nœud ne serve le trafic, définissez l'état sur PASSIVE (état par défaut). Après avoir effectué les configurations spécifiques au nœud, modifiez l'état du nœud en ACTIVE à l'aide de la commande **set cluster node**.
       > - **nom_interface** est l'interface de fond de panier du nœud. Par exemple, si le nœud 1 utilise l'interface 1/1, la valeur de ce paramètre est 1/1/1.

     Par exemple,

```
1  add cluster node 1 10.102.29.70 -state PASSIVE -backplane
       1/1/1
```



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

- Enregistrez la configuration en entrant `save ns config`.

2. Ouvrez une session sur le nœud nouvellement ajouté (par exemple, 10.102.29.70) et procédez comme suit :
   - Joignez le nœud au cluster. Tapez, `join cluster -clip <ip_addr> -password <password>`. où,
     - **est l'adresse IP du cluster Citrix ADC.** Seules les adresses IPv4 sont prises en charge.
     - **password** est le mot de passe nsroot du CCO.

     Par exemple,

     ```
     join cluster -clip 10.102.29.61 -password nsroot
     <!--NeedCopy-->
     ```

   - Enregistrez la configuration en entrant `save ns config`.
   - Réinitialisez l'appliance à chaud en entrant`reboot -warm`.

Pour ajouter un nœud au cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Démarrer**, cliquez sur **Gérer le cluster**.
4. Cliquez sur **Ajouter** pour ajouter le nouveau nœud (par exemple, 10.102.29.70).
5. Dans la boîte de dialogue **Créer un nœud de cluster** , définissez les paramètres suivants :
   - **Node Id** : entier unique qui identifie la solution matérielle-logicielle sur le cluster. Chaque nœud doit avoir un ID de nœud différent. Valeur minimale : 0. Valeur maximale : 31.
   - **Adresse IP** : adresse IP de l'appliance Citrix ADC. Seules les adresses IPv4 sont prises en charge.
   - **Backplane** - Interface backplane du nœud. Par exemple, si le nœud 1 utilise l'interface 1/1, la valeur de ce paramètre est 1/1.
   - **État** : état configuré du nœud de cluster. Valeurs possibles : ACTIVE, PASSIVE, SPARE. Par défaut : PASSIVE.

     > Remarque :
     > Si vous souhaitez effectuer des configurations spécifiques au nœud, telles que l'ajout d'adresses IP ponctuées, avant que le nœud ne serve le trafic, définissez l'état sur PASSIVE (état par défaut). Après avoir effectué les configurations spécifiques au nœud, changez l'état du nœud sur ACTIVE.

6. **Cliquez sur Créer**. Une boîte de dialogue vous informe que la solution matérielle-logicielle sera redémarré à chaud. Cliquez sur **Oui** pour confirmer.

Pour joindre un nœud précédemment ajouté au cluster à l'aide de l'utilitaire de configuration

Si vous avez utilisé la ligne de commande Citrix ADC pour ajouter un nœud au cluster, mais que vous n'avez pas joint le nœud au cluster, vous pouvez utiliser la procédure suivante pour joindre le nœud au cluster.

1. Connectez-vous au nœud que vous souhaitez joindre au cluster (par exemple, 10.102.29.70).
2. Dans le volet de navigation, développez Système, puis cliquez sur Cluster.
3. Dans le volet d'informations, sous Démarrer, cliquez sur Joindre un cluster.
4. Dans la boîte de dialogue Joindre à un cluster existant, définissez les paramètres suivants :
   - **Cluster IP** - Adresse IP du cluster Citrix ADC. Seules les adresses IPv4 sont prises en charge.
   - **Mot de passe** - L`nsroot` mot de passe du CCO.
5. Cliquez sur **OK**.

Suppression d'un nœud de cluster

La suppression d'un nœud d'un cluster est un processus en deux étapes :

1. Supprimez la référence à l'instance de cluster du nœud. Cette commande exécute en interne la commande **clear ns config extended** sur ce nœud. En outre, les adresses SNIP et toutes les configurations VLAN (à l'exception des VLAN et ADCVLAN par défaut) sont effacées du nœud.
2. Supprimez le nœud du cluster.

> Remarque :
>
> - Lorsque vous supprimez un nœud qui est le CCO, toutes les sessions d'adresse IP de cluster en cours sont invalidées. Un autre nœud de cluster est fait CCO et l'adresse IP du cluster est attribuée à ce nœud. Vous devez démarrer une nouvelle session avec l'adresse IP du cluster.
> - Pour supprimer le cluster (et tous les nœuds), vous devez supprimer chaque nœud individuellement. Lors de la suppression du dernier nœud, les adresses IP du cluster sont supprimées.

Pour supprimer un nœud de cluster à l'aide de la ligne de commande Citrix ADC

1. Ouvrez une session sur le nœud que vous souhaitez supprimer du cluster et procédez comme suit :
   - Supprimez la référence à l'instance de cluster. Tapez, `rm cluster instance <clId>`. Où, **CLID** est l'entier qui identifie le cluster à partir duquel le nœud doit être supprimé.
   - Enregistrez la configuration en entrant `save ns config`.

> Remarque :
>
> Pour supprimer le dernier nœud d'un cluster, vous devez uniquement supprimer l'instance de cluster de ce nœud. Le nœud est automatiquement supprimé du cluster.

2. Connectez-vous à l'adresse IP du cluster et procédez comme suit :
   - Supprimez le nœud à partir duquel vous avez supprimé l'instance de cluster. Tapez, `rm cluster node <nodeId>`. Où, **NodeId** est l'entier qui identifie le nœud que vous supprimez.
   - Enregistrez la configuration en entrant `save ns config`.

> Remarque :
>
> Assurez-vous que vous n'exécutez pas la commande **rm cluster node** à partir du nœud local car cela entraîne des configurations incohérentes entre le CCO et le nœud.

Pour supprimer un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Mise en route**, cliquez sur **Gérer Cluste**r.
4. Sélectionnez le nœud à supprimer du cluster, puis cliquez sur **Supprimer**.
5. Cliquez sur **OK**.

Affichage des détails d'un cluster

Vous pouvez afficher les détails de l'instance de cluster et des nœuds de cluster à partir de l'adresse IP du cluster.

Pour afficher les détails d'une instance de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez : `sh cluster instance <clId>`. Où, **CLID** est l'entier qui identifie l'instance de cluster dont vous souhaitez afficher les détails.

```
1 > show cluster instance 1
2 1)Cluster ID: 1
3   Dead Interval: 3 secs
4   Hello Interval: 200 msecs
5   Preemption: DISABLED
6   Propagation: ENABLED
7   Cluster Status: ENABLED(admin), ENABLED(operational), UP
8   Member Nodes:
9   Node ID    Node IP    Health Admin State Operation State
```



```
10    -------     -------     ------  -----------  ---------------
11 1)   0    10.102.29.60*   UP      ACTIVE      ACTIVE(CCO)
12 2)   1    10.102.29.70    UP      ACTIVE      ACTIVE
13 Done
14 <!--NeedCopy-->
```

> Remarque : L'exécution de cette commande à partir de l'adresse ADCIP d'un nœud non-CCO affiche l'état du cluster sur ce nœud.

Pour afficher les détails d'un nœud de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez `sh cluster node <nodeId>`. Où **NodeId** est l'entier qui identifie le nœud dont vous souhaitez afficher les détails.

```
1 >show cluster node 1
2 Node ID: 1
3 IP: 10.102.29.70
4 Backplane: 1/1/1
5 Health: UP
6 Admin state: ACTIVE
7 Operational State: ACTIVE
8 Sync State: ENABLED
9 <!--NeedCopy-->
```

Pour afficher les détails d'une instance de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Démarrer**, cliquez sur **Gérer le cluster**.
4. Dans la boîte de **dialogue Configurer une instance de cluster** , affichez les détails du cluster.

Pour afficher les détails d'un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, cliquez sur **Cluster**, puis cliquez sur **Noeuds**.
3. Dans la liste **Noeuds de cluster** , affichez les détails du nœud. Pour obtenir une vue plus détaillée du nœud, cliquez sur le nœud.

Répartition du trafic entre les nœuds de cluster

Après avoir créé le cluster Citrix ADC et effectué les configurations requises, vous devez déployer ECMP (equ-cost multi-path) ou le groupe d'agrégation de liens de cluster (CLAG) sur le plan de données client

(pour le trafic client) ou le plan de données serveur (pour le trafic serveur). Ces mécanismes répartissent le trafic externe sur les nœuds de cluster.

Utilisation de chemins multiples à coût égal

Avec le mécanisme multi-chemins Equal-cost, le routeur a des routes à coût égal vers des adresses VIP avec les sauts suivants comme nœuds actifs du cluster. Le routeur utilise un mécanisme basé sur le hachage sans état pour distribuer le trafic sur les routes.

> Remarque :
>
> Les routes sont limitées au nombre maximal de routes ECMP prises en charge par le routeur amont.

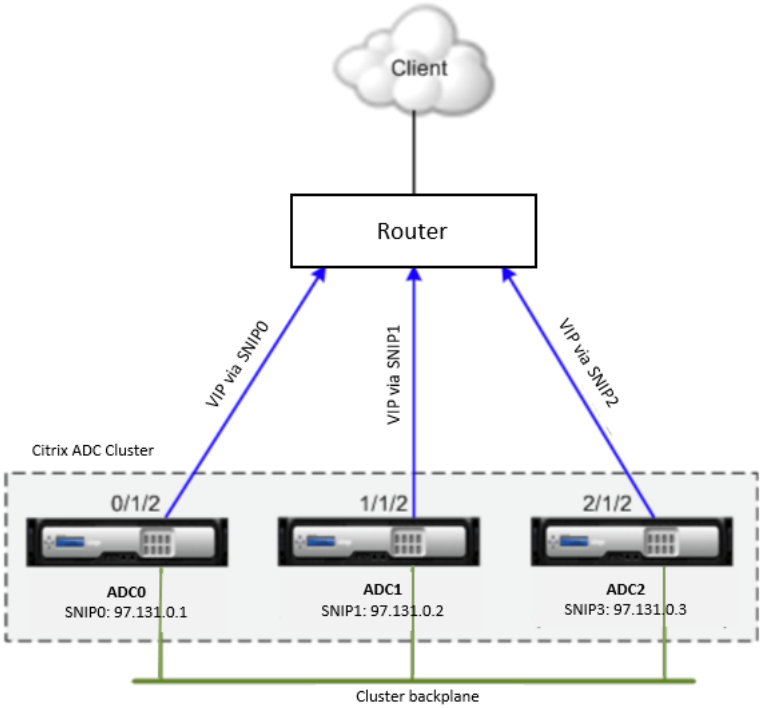
Pour utiliser ECMP, vous devez d'abord activer le protocole de routage requis (OSPF, RIP ou BGP) sur l'adresse IP du cluster. Vous devez lier les interfaces et l'adresse IP ponctuée (avec le routage dynamique activé) à un VLAN. Configurez le protocole de routage sélectionné et redistribuez les routes du noyau sur les ZebOS à l'aide du shell vtysh.

Vous devez effectuer des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe.

Vous devez avoir une connaissance détaillée des protocoles de routage pour utiliser ECMP. Pour plus d'informations, consultez la section **Configuration des routes dynamiques** (/en-us/advanced-concepts/downloads/citrix-Citrix ADC-clustering-guide-v2 copy.pdf).

> Remarque :
>
> Assurez-vous que les licences du cluster prennent en charge le routage dynamique, sinon la distribution du trafic ECMP ne fonctionne pas. La licence Citrix ADC standard, par exemple, ne prend pas en charge le routage dynamique.

Topologie ECMP



Comme vu dans la figure ci-dessus, le routeur ECMP peut atteindre l'adresse VIP via SNIP0, SNIP1 ou SNIP2.

Pour configurer ECMP sur le cluster Citrix ADC à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à l'adresse IP du cluster.
2. Activez le protocole de routage (OSPF, RIP ou BGP).
   enable ns feature <routing protocol>
   Par exemple,

```
1 enable ns feature ospf
2 <!--NeedCopy-->
```

3. Ajoutez un VLAN.
   add vlan <vlan id>
   Par exemple,

```
1 add vlan 97
2 <!--NeedCopy-->
```

4. Liez les interfaces des nœuds de cluster au VLAN.
   bind vlan <vlan id> -ifnum <interface_name>
   Par exemple,


```
bind vlan 97 -ifnum 0/1/2 1/1/2 2/1/2
<!--NeedCopy-->
```

5. Ajoutez une adresse SNIP ponctuée sur chaque nœud et activez le routage dynamique sur celui-ci.
   add ns ip <SNIP> <netmask> -ownerNode <node id‘ > -DynamicRouting ENABLED
   Par exemple,

```
add ns ip 97.131.0.1 255.0.0.0 -ownerNode 0 -dynamicRouting
ENABLED -type SNIP
add ns ip 97.131.0.2 255.0.0.0 -ownerNode 1 -dynamicRouting
ENABLED -type SNIP
add ns ip 97.131.0.3 255.0.0.0 -ownerNode 2 -dynamicRouting
ENABLED -type SNIP
<!--NeedCopy-->
```

6. Liez l’une des adresses SNIP spotted au VLAN. Lorsque vous liez une adresse SNIP spotted à un VLAN, toutes les autres adresses SNIP spotted définies sur le cluster dans ce sous-réseau sont automatiquement liées au VLAN.
   bind vlan <vlan id> -ipAddress <SNIP> <netmask>. Par exemple,

```
bind vlan 97 -ipAddress 97.131.0.1 255.0.0.0
<!--NeedCopy-->
```

> Remarque :
>
> Vous pouvez utiliser les adresses ADCIP des nœuds de cluster au lieu d’ajouter des adresses SNIP. Si c’est le cas, vous n’avez pas à effectuer les étapes 3 à 6.

7. Configurez le protocole de routage sur ZeBos en utilisant vtysh shell. Pour configurer le protocole de routage OSPF sur les ID de nœud 0, 1 et 2.

```
!
interface vlan97
!
router ospf
owner-node 0
ospf router-id 97.131.0.1
exit-owner-node
owner-node 1
ospf router-id 97.131.0.2
exit-owner-node
owner-node 2
ospf router-id 97.131.0.3
```



```
exit-owner-node
redistribute kernel
network 97.0.0.0/8 area 0
!
<!--NeedCopy-->
```

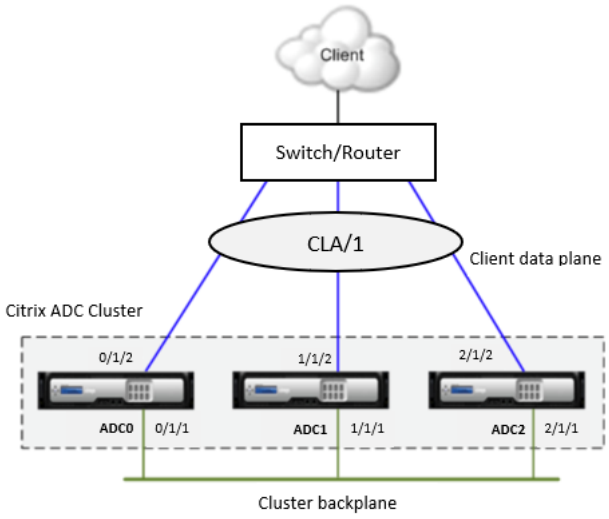
Utilisation du groupe d'agrégation de liens de cluster (CLAG)

Un groupe d'agrégation de liens de cluster, comme son nom l'indique, est un groupe d'interfaces de nœuds de cluster. Il s'agit d'une extension de l'agrégation de liens Citrix ADC. La seule différence est que si l'agrégation de liens nécessite que les interfaces proviennent du même périphérique, dans CLAG, les interfaces proviennent de différents nœuds du cluster.

Pour plus d'informations sur l'agrégation de liens, reportez-vous à la section Configuration de l'agrégation de liens.

CLAG peut être statique ou dynamique. Par exemple, considérez un cluster à trois nœuds où les trois nœuds sont connectés au commutateur en amont. Un canal CLAG (CLA/1) est formé par des interfaces de liaison 0/1/2, 1/1/2 et 2/1/2.

Topologie du groupe d'agrégation de liens de cluster

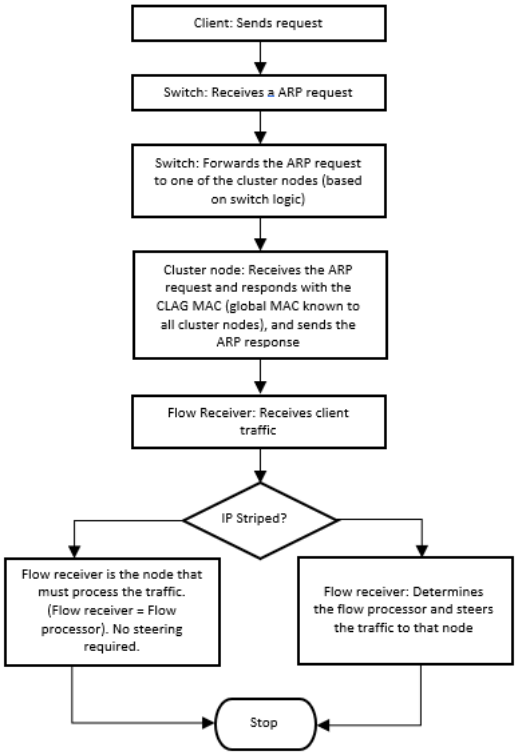


Un canal CLAG possède les attributs suivants :

- Chaque canal a un MAC unique convenu par les nœuds de cluster.
- Le canal peut lier les interfaces des nœuds locaux et distants.
- Un maximum de quatre canaux CLAG sont pris en charge dans un cluster.
- Les interfaces de fond de panier ne peuvent pas faire partie d'un canal CLAG.

- Lorsqu'une interface est liée à un canal CLAG, les paramètres de canal ont priorité sur les paramètres de l'interface réseau. Une interface réseau peut être liée à un seul canal.

Flux de distribution du trafic utilisant CLAG



Groupe d'agrégation de liens de cluster statique

Vous devez configurer un canal CLAG statique sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur amont pour distribuer le trafic en fonction de l'adresse IP ou du port au lieu de l'adresse MAC.

Pour plus d'informations sur la configuration d'un canal AL statique, reportez-vous à laConfiguration manuelle de l'agrégation de lienssection.

Pour configurer un canal CLAG statique à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à l'adresse IP du cluster.

> Remarque :
>
> Assurez-vous de configurer le canal CLAG sur l'adresse IP du cluster avant de configurer CLAG sur le commutateur externe. Sinon, le commutateur transmettra le trafic vers le cluster même si le canal CLAG n'est pas configuré. Cela peut entraîner une perte de trafic.

2. Créez un canal CLAG. Ajouter le canal <clag channel id> -vitesse <speed>, où,

   - <clag channel id> est un numéro unique qui identifie le canal CLAG. Doit être de la forme CLA/x où x peut aller de 1 à 4.
   - <speed> est la vitesse des interfaces membres du CLAG.

   Par exemple,

   ```
   1 add channel CLA/1 -speed 1000
   2 <!--NeedCopy-->
   ```

   > Remarque :
   >
   > Vous ne devez pas spécifier la vitesse commeAUTO. Vous devez spécifier explicitement la vitesse 10, 100, 1000 ou 10000. Seules les interfaces dont la vitesse correspond à l'attribut <speed> dans CLAG sont ajoutées à la liste de distribution active.

3. Liez les interfaces requises au canal CLAG. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster. Lier le canal <clag channel id> <interface_name...>, où,

   - <clag channel id> identifie le canal CLAG auquel vous souhaitez lier les interfaces.
   - <interface_name> spécifie les interfaces à lier au canal CLAG.

   Par exemple,

   ```
   1 bind channel CLA/1 1/1/2 2/1/2 3/1/2
   2 <!--NeedCopy-->
   ```

4. Vérifiez les configurations des canaux CLAG. Afficher la chaîne <clag channel id>.
   Par exemple, les opérations suivantes peuvent être effectuées :

   ```
   1 show channel CLA/1
   2 <!--NeedCopy-->
   ```

   > Remarque :
   >
   > Vous pouvez lier le canal CLAG à un VLAN à l'aide de la commande bind vlan. Les interfaces du canal CLAG sont automatiquement liées au VLAN.

Groupe d'agrégation de liens de cluster dynamique

Dynamic CLAG utilise le protocole LACP (Link Aggregation Control Protocol) .Pour plus d'informations sur la configuration d'un canal LA dynamique, reportez-vous à laConfiguration de l'agrégation de liens à l'aide du protocole de contrôle de l'agrégation de lienssection.

Vous devez effectuer des configurations similaires sur l'adresse IP du cluster et sur le périphérique de connexion externe. Si possible, configurez le commutateur amont pour distribuer le trafic en fonction

de l'adresse IP ou du port au lieu de l'adresse MAC.

Points à retenir :

- Activez LACP (en spécifiant le mode LACP comme ACTIVE ou PASSIVE).

  > Remarque :
  >
  > Assurez-vous que le mode LACP n'est pas défini comme PASSIVE sur le cluster Citrix ADC et sur le périphérique de connexion externe.

- Spécifiez la même clé LACP sur chaque interface que vous souhaitez faire partie du canal. Pour créer un canal CLAG, la clé LACP peut avoir une valeur comprise entre 5 et 8.

  Par exemple, si vous définissez la clé LACP sur les interfaces 1/1/2 et 2/1/2 sur 5, CLA/1 est créé. Les interfaces 1/1/2 et 2/1/2 sont automatiquement liées à CLA/1. De même, si vous définissez la touche LACP sur 6, le canal CLA/2 est créé.

- Spécifiez le type de LAG en tant que Cluster.

Pour configurer un canal CLAG dynamique à l'aide de la ligne de commande Citrix ADC

Sur l'adresse IP du cluster, pour chaque interface que vous souhaitez ajouter au canal CLAG, tapez : **set interface** <`interface id` > -lacpMode <`lacpMode` > -lacpKey <`lacpKey` > -lagType Cluster

Pour configurer un canal CLAG pour 3 interfaces.

```
set interface 0/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
set interface 1/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
set interface 2/1/2 -lacpMode active -lacpKey 5 -lagType Cluster
<!--NeedCopy-->
```

Utilisation des jeux de liens

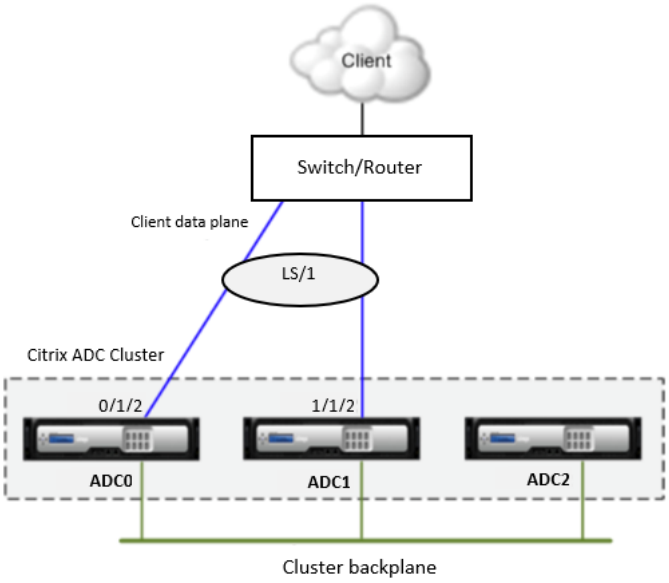
Les jeux de liens doivent être utilisés lorsque certains nœuds de cluster ne sont pas physiquement connectés au réseau externe. Dans une telle topologie de cluster, les nœuds de cluster non connectés utilisent les interfaces spécifiées dans le jeu de liens pour communiquer avec le réseau externe via le backplane du cluster. Les jeux de liens sont généralement utilisés dans des scénarios lorsque les périphériques de connexion ont des ports insuffisants pour connecter les nœuds de cluster.

Les jeux de liens doivent être configurés uniquement sur l'adresse IP du cluster.

Par exemple, considérez un cluster à trois nœuds où le commutateur en amont ne dispose que de deux ports. En utilisant des jeux de liens, vous pouvez connecter deux nœuds au commutateur et laisser le troisième nœud non connecté. Dans la figure suivante, un jeu de liens (LS/1) est formé en liant les interfaces 0/1/2 et 1/1/2. ADC2 est le nœud non connecté du cluster.

> Remarque :
>
> Utilisez des jeux de liens pour améliorer les performances des topologies nécessitant le transfert basé sur Mac (MBF).

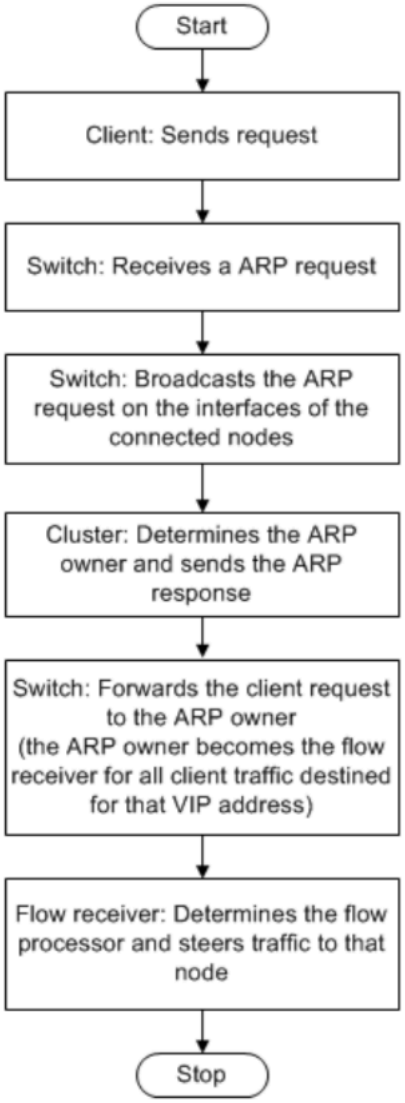
Topologie des jeux de liens



Le jeu de liens informe ADC2 qu'il peut utiliser des interfaces 0/1/2 et 1/1/2 pour communiquer avec les périphériques réseau. Tout le trafic à destination et en provenance de l'ADC2 est désormais acheminé via les interfaces 0/1/2 ou 1/1/2.

Flux de distribution du trafic à l'aide de jeux de liens

Figure 1-10. Traffic distribution flow using linksets



Pour configurer un jeu de liens à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à l'adresse IP du cluster.
2. Créez un jeu de liens. Pour ajouter un jeu de liens, entrez <`linkset id`>. **L'identifiant du jeu de liens** est un identifiant unique du jeu de liens. Il doit être de la forme LS/x. Par exemple,

```
1 add linkset LS/1
2 <!--NeedCopy-->
```

3. Liez les interfaces requises au jeu de liens. Assurez-vous que les interfaces ne sont pas utilisées pour le backplane du cluster. Pour lier le jeu de liens, entrez <`linkset id`> -ifnum

<interface_name...>. **Interface_name** spécifie les interfaces à lier au jeu de liens. Par exemple,

```
bind linkset LS/1 -ifnum 0/1/2 1/1/2
<!--NeedCopy-->
```

4. Vérifiez les configurations du jeu de liens. Pour afficher le jeu de liens, entrez <linkset id >. L'**identifiant du jeu de liens** est un identifiant du jeu de liens que vous voulez vérifier. Par exemple,

```
show linkset LS/1
<!--NeedCopy-->
```

> Remarque :
>
> Vous pouvez lier le jeu de liens à un VLAN en utilisant la commande bind vlan. Les interfaces du jeu de liens sont automatiquement liées au VLAN.

Pour configurer un jeu de liens à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Réseau**, puis cliquez sur **Jeu de liens**.
3. Dans le volet d'informations, cliquez sur **Ajouter**.
4. Dans la boîte de dialogue **Créer un jeu de liens** :
   a) Spécifiez le nom du **jeu de liens** en définissant le paramètre Linkset.
   b) Spécifiez les **interfaces** à ajouter au jeu de liens et cliquez sur **Ajouter** . Répétez cette étape pour chaque interface que vous souhaitez ajouter au jeu de liens.
5. Cliquez sur **Créer**, puis sur **Fermer**.

Gérer le cluster Citrix ADC

Après avoir créé un cluster et configuré le mécanisme de distribution du trafic requis, le cluster peut servir le trafic. Au cours de la durée de vie du cluster, vous pouvez effectuer des tâches de gestion de cluster telles que la désactivation des nœuds d'un cluster, la découverte des appliances Citrix ADC, l'affichage des statistiques, la synchronisation des configurations de cluster, des fichiers de cluster et la durée des nœuds, ainsi que la mise à niveau ou la rétrogradation du logiciel des nœuds de cluster.

Désactiver un nœud de cluster

Vous pouvez supprimer temporairement un nœud d'un cluster en désactivant l'instance de cluster sur ce nœud. Un nœud désactivé n'est pas synchronisé avec les configurations de cluster et ne peut pas servir le trafic.

Pour désactiver un nœud de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC du nœud que vous souhaitez désactiver. Pour désactiver l'instance de cluster, entrez <clId>. **CLID** identifie l'instance de cluster que vous souhaitez désactiver.

> Remarque :
>
> Pour désactiver le cluster, exécutez la commande disable cluster instance sur l'adresse IP du cluster.

Pour désactiver un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous au nœud que vous souhaitez désactiver.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Démarrer**, cliquez sur **Gérer le cluster**.
4. Dans la boîte de dialogue **Configurer l'instance de cluster** , décochez la case **Activer l'instance de cluster** .
5. Cliquez sur **OK**.

> Remarque :
>
> Pour désactiver le cluster, exécutez la commande disable cluster instance sur l'adresse IP du cluster. Pour désactiver l'instance de cluster sur tous les nœuds, connectez-vous au cluster et effectuez la procédure ci-dessus.

Découvrir les appliances Citrix ADC

Vous pouvez découvrir les appliances Citrix ADC présentes dans le même sous-réseau que l'adresse ADCIP du CCO. Les appliances découvertes peuvent ensuite être ajoutées au cluster.

> Remarque :
>
> Cette opération n'est disponible que par l'intermédiaire de l'utilitaire de configuration.

Pour découvrir des solutions matérielles-logicielles à l'aide de l'utilitaire de configuration Citrix ADC

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, cliquez sur **Cluster**, puis cliquez sur Noeuds.
3. Dans le volet d'informations, en bas de la page, cliquez sur **Découvrir les Citrix ADC**.
4. Dans la boîte de dialogue **Discover Citrix ADCs** , définissez les paramètres suivants :
    - **Plage d'adresses IP** : spécifiez la plage d'adresses IP dans laquelle vous souhaitez découvrir les appliances Citrix ADC. Par exemple, vous pouvez rechercher toutes les adresses ADCIP comprises entre 10.102.29.4 et 10.102.29.15 en spécifiant cette option comme 10.102.29.4 - 15.

- **Interface de backplane** : spécifiez les interfaces à utiliser comme interface de backplane. Il s'agit d'un paramètre facultatif. Si vous ne spécifiez pas ce paramètre, vous devez le actualiser après l'ajout du nœud au cluster.

5. Cliquez sur **OK**.
6. Sélectionnez les appliances Citrix ADC que vous souhaitez ajouter au cluster.
7. Cliquez sur **OK**.

Affichage des statistiques d'un cluster

Vous pouvez afficher les statistiques d'une instance de cluster et des nœuds de cluster pour évaluer les performances ou résoudre les problèmes de fonctionnement du cluster.

Pour afficher les statistiques d'une instance de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez :

- **instance de cluster stat** <clId >

```
1  >stat cluster instance
2  Cluster Instance Summary
3  Cluster Size                                    3
4  Cluster Status                              ENABLED
5  Cluster Config Coordinator (CCO)        10.102.29.80
6  Current DFD Sessions                            0
7  Total Steered Packets                           0
8  Done
9  <!--NeedCopy-->
```

Pour afficher les statistiques de l'instance de cluster avec les statistiques d'erreur, à l'invite de commande Citrix ADC de l'adresse IP du cluster, tapez :

- **stat instance de cluster** -detail <clId >

```
1  > stat cluster instance -detail
2  Cluster Statistics
3  Summary
4  Cluster Size                                    3
5  Cluster Status                              ENABLED
6  Cluster Config Coordinator (CCO)        10.102.29.80
7  Current DFD Sessions                            0
8  Total Steered Packets                           0
9  Error Statistics
10 DFD Dropped Packets                             0
```



```
Propagation timeout                                    0
Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'un nœud de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez : `stat cluster node`.

```
> stat cluster node
Cluster Node Summary
NodeID NodeIP       State    Health  Sync State HB Tx HB Rx
0      10.102.29.70 ACTIVE   UP      ENABLED    4489  2247
1      10.102.29.80 ACTIVE   UP      ENABLED    2659  4805
2      10.102.29.60 INACTIVE UNKNOWN UNKNOWN    7145  0
Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'un nœud de cluster individuel, à l'invite de commande Citrix ADC de l'adresse IP du cluster, tapez :`stat cluster node <nodeid>`.

```
> stat cluster node 1
Node ID : 1
Node IP                                  10.102.29.80
Master State                                   ACTIVE
Health                                             UP
Sync State                                    ENABLED
Heartbeats Sent                                  3025
Heartbeats received                              5537
NNM Statistics
NNM current connections                             7
NNM total transmitted messages                     15
NNM total received messages                        18
Error Statistics
NNM Multicast/Broadcast req err                     0
Done
<!--NeedCopy-->
```

Pour afficher les statistiques d'une instance de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, au centre de la page, cliquez sur **Statistiques**.

Pour afficher les statistiques d'un nœud de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, cliquez sur **Cluster**, puis cliquez sur **Noeuds**.
3. Dans le volet d'informations, sélectionnez un nœud et cliquez sur **Statistiques** pour afficher les statistiques du nœud. Pour afficher les statistiques de tous les nœuds, cliquez sur **Statistiques** sans sélectionner un nœud spécifique.

Synchronisation des configurations de cluster

Les configurations Citrix ADC qui sont disponibles sur le CCO sont synchronisées avec les autres nœuds du cluster lorsque :

- Un nœud joint le cluster.
- Un nœud rejoint le cluster.
- Une nouvelle commande est exécutée sur le CCO.

En outre, vous pouvez synchroniser avec force les configurations disponibles sur le CCO (synchronisation complète) vers un nœud de cluster spécifique. Assurez-vous de synchroniser un nœud de cluster à la fois, sinon le cluster peut être affecté.

Pour synchroniser des configurations de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'appliance sur laquelle vous souhaitez synchroniser les configurations CCO, tapez : **force cluster sync**.

Pour synchroniser des configurations de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous à la solution matérielle-logicielle sur laquelle vous souhaitez synchroniser les configurations CCO.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur **Forcer la synchronisation du cluster**.
4. Cliquez sur **OK**.

Synchronisation des fichiers de cluster

Les fichiers disponibles sur le CCO sont appelés fichiers de cluster. Ces fichiers sont automatiquement synchronisés sur les autres nœuds de cluster lorsque le nœud est ajouté au cluster et périodiquement, pendant la durée de vie du cluster. En outre, vous pouvez synchroniser manuellement les fichiers de cluster.

Les répertoires et fichiers du CCO synchronisés sont les suivants :

- /nsconfig/ssl/
- /var/netscaler/ssl/
- /var/vpn/bookmark/
- /nsconfig/dns/
- /nsconfig/htmlinjection/
- /netscaler/htmlinjection/ens/
- /nsconfig/moniteur/
- /nsconfig/nstemplates/
- /nsconfig/ssh/
- /nsconfig/rc.netscaler
- /nsconfig/resolv.conf
- /nsconfig/inetd.conf
- /nsconfig/syslog.conf
- /nsconfig/snmpd.conf
- /nsconfig/ntp.conf
- /nsconfig/httpd.conf
- /nsconfig/sshd_config
- /nsconfig/hosts
- /nsconfig/enckey
- /var/nslw.bin/etc/krb5.conf
- /var/nslw.bin/etc/krb5.keytab
- /var/lib/likewise/db/
- /var/download/
- /var/wi/tomcat/webapps/
- /var/wi/tomcat/conf/Catalina/localhost/
- /var/wi/java_home/lib/security/cacerts
- /var/wi/java_home/jre/lib/security/cacerts
- /nsconfig/license/
- /nsconfig/rc.conf-

Pour synchroniser des fichiers de cluster à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez `sync cluster files <mode>`.

- **mode** spécifie les répertoires ou fichiers à synchroniser. Les valeurs possibles sont : all, signets, ssl, htmlinjection, imports, misc, dns, all_plus_misc. Valeur par défaut : all.

Pour synchroniser des fichiers de cluster à l'aide de l'utilitaire de configuration

1. Connectez-vous au cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.

3. Dans le volet d'informations, sous Utilitaires, cliquez sur **Synchroniser les fichiers de cluster**.
4. Dans la boîte de dialogue **Synchroniser les fichiers de cluster** , sélectionnez les fichiers à synchroniser dans la liste déroulante **Mode** .
5. Cliquez sur **OK**.

Synchronisation de l'heure sur les nœuds de cluster

Le cluster Citrix ADC utilise Precision Time Protocol (PTP) pour synchroniser l'heure entre les nœuds de cluster. PTP utilise des paquets de multidiffusion pour synchroniser l'heure. S'il y a des problèmes dans la synchronisation de l'heure, vous devez désactiver PTP et configurer NTP (Network Time Protocol) sur le cluster.

Pour activer/désactiver PTP à l'aide de la ligne de commande Citrix ADC

À l'invite de commandes Citrix ADC de l'adresse IP du cluster, tapez : `set ptp -state disable`.

Pour activer/désactiver PTP à l'aide de l'utilitaire de configuration

1. Connectez-vous à l'adresse IP du cluster.
2. Dans le volet de navigation, développez **Système**, puis cliquez sur **Cluster**.
3. Dans le volet d'informations, sous **Utilitaires**, cliquez sur **Configurer les paramètres PTP**.
4. Dans la boîte de dialogue **Activer/Désactiver PTP** , indiquez si vous souhaitez activer ou désactiver PTP.
5. Cliquez sur **OK**.

Mise à niveau ou rétrogradation du logiciel du cluster

Tous les nœuds de cluster doivent exécuter la même version logicielle. Pour effectuer la mise à niveau ou la rétrogradation du logiciel d'un cluster, vous devez effectuer une mise à niveau ou une rétrogradation du logiciel sur chaque nœud, un nœud à la fois.

Lorsque le logiciel d'un nœud est mis à niveau ou rétrogradé, le nœud n'est pas supprimé du cluster. Le nœud reste une partie du cluster et sert le trafic client sans interruption, à l'exception du temps d'arrêt lorsque le nœud redémarre après sa mise à niveau ou sa mise à niveau. Toutefois, en raison de la non-concordance des versions logicielles entre les nœuds de cluster, la propagation de la configuration est désactivée et n'est activée qu'une fois que tous les nœuds de cluster sont de la même version.

Étant donné que la propagation de la configuration est désactivée lors de la mise à niveau lors de la rétrogradation d'un cluster, vous ne pouvez pas effectuer de configurations via l'adresse IP du cluster pendant cette période. Toutefois, vous pouvez effectuer des configurations au niveau des nœuds via l'adresse ADCIP de nœuds individuels, mais vous devez vous assurer que vous effectuez les mêmes configurations sur tous les nœuds pour les maintenir en synchronisation.

> Remarque :
>
> Vous ne pouvez pas ajouter de nœuds de cluster lors de la mise à niveau ou de la rétrogradation de la version du logiciel de cluster.

Pour effectuer une mise à niveau ou une rétrogradation du logiciel des nœuds de cluster

1. Assurez-vous que le cluster est stable et que les configurations sont synchronisées sur tous les nœuds.
2. Mettez à niveau ou rétrogradez le logiciel du cluster.
   - Mettez à niveau ou rétrogradez le logiciel d'un nœud de cluster. Pour plus d'informations sur la mise à niveau et la rétrogradation du logiciel d'une appliance, reportez-vous **à la section Mise à niveau ou rétrogradation du logiciel système**.
   - Redémarrez l'appliance.
   - Répétez les deux étapes ci-dessus pour chacun des autres nœuds de cluster.

   > Remarque :
   >
   > Citrix vous recommande d'attendre que le nœud précédent devienne actif avant de procéder à la mise à niveau du nœud suivant.

Cas d'utilisation

Cette rubrique fournit certains cas d'utilisation pour le déploiement d'un cluster Citrix ADC.

- Création d'un cluster à deux nœuds
- Utilisation de la redirection du cache dans un cluster
- Utilisation de CLAG avec des jeux de liens
- Interfaces communes pour le client et le serveur et interfaces dédiées pour le fond de panier
- Commutateur commun pour le client, le serveur et le fond de panier
- Commutateur commun pour le client et le serveur et commutateur dédié pour le fond de panier
- Plusieurs commutateurs pour chaque nœud
- Commutateur différent pour chaque nœud
- Exemples de configurations de cluster

Création d'un cluster à deux nœuds

Un cluster à deux nœuds est une exception à la règle selon laquelle un cluster n'est fonctionnel que lorsqu'un minimum de nœuds (n/2 + 1), où **n** est le nombre de nœuds de cluster, sont capables de servir le trafic. Si cette formule était appliquée à un cluster à deux nœuds, le cluster échouerait si un nœud était en panne (n/2 + 1 = 2).

Un cluster à deux nœuds est fonctionnel même si un seul nœud est capable de servir le trafic. La création d'un cluster à deux nœuds est la même chose que la création d'un autre cluster. Vous devez ajouter un nœud en tant que coordinateur de configuration et l'autre nœud en tant que nœud de cluster.

> Remarque :
>
> La synchronisation incrémentielle de configuration n'est pas prise en charge dans un cluster à deux nœuds. Seule la synchronisation complète est prise en charge.

Migration d'une configuration HA vers une configuration de cluster

Une installation de haute disponibilité (HA) existante peut être migrée vers une configuration de cluster en supprimant les appliances de la configuration HA, puis en créant le cluster Citrix ADC. Par exemple, considérez une configuration HA avec des adresses ADCIP 10.102.97.131 et 10.102.97.132.

Pour convertir une configuration HA en configuration de cluster à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à chaque nœud HA et supprimez-le de la configuration HA. Tapez, `rm HA node <nodeId>`. Par exemple, `rm HA node 1`.
2. Accédez à l'interpréteur de commandes sur l'un des nœuds HA et copiez`ns.conf` le dans un autre`.conf` fichier. Par exemple, `ns_backup.conf`.
3. Modifiez le nouveau fichier de configuration comme suit :
   - Supprimez toutes les fonctionnalités qui ne sont pas prises en charge par un cluster. Pour obtenir la liste des fonctionnalités non prises en charge, reportez-vous à la section Fonctionnalités de Citrix ADC prises en charge par un cluster.
   - Supprimez les configurations qui ont des interfaces ou mettez à jour les noms d'interface de la convention **c/u** vers la convention **n/c/u** .
4. Sur les deux nœuds, identifiez les interfaces réseau à utiliser pour le fond de panier du cluster.
5. Configurez l'un des nœuds (par exemple, 10.102.97.131) en tant que nœud CCO. Pour obtenir des instructions détaillées, reportez-vous à la section Configuration d'un cluster Citrix ADC.
6. Ouvrez une session sur l'adresse IP du cluster et appliquez des configurations à partir du fichier de configuration de sauvegarde. Tapez, `batch -f \<fileName\>`. Par exemple, `batch -f ns_backup.conf`.
7. Enregistrez la configuration. Tapez, `save ns config`.
8. Ajoutez l'autre nœud au cluster. Pour obtenir des instructions détaillées, reportez-vous à la section Ajout d'un nœud au cluster.

Les appliances du programme d'installation HA sont migrées vers une configuration de cluster.

Utilisation de la redirection du cache dans un cluster

La redirection du cache dans un cluster Citrix ADC fonctionne de la même manière que sur un dispositif Citrix ADC autonome. La seule différence est que les configurations sont effectuées sur l'adresse IP du cluster. Pour plus d'informations, consultez la section Redirection du cache.

Points à retenir lors de l'utilisation de la redirection du cache en mode transparent :

- Avant de configurer la redirection du cache, assurez-vous que vous avez connecté tous les nœuds au commutateur externe et que vous avez configuré des jeux de liens. Sinon, les demandes des clients seront supprimées.
- Lorsque le mode MAC est activé sur un serveur virtuel d'équilibrage de charge, assurez-vous que le mode MBF est activé sur le cluster (à l'aide de la`enable ns mode MBF` commande). Sinon, les requêtes sont envoyées directement au serveur d'origine au lieu d'être envoyées au serveur de cache.

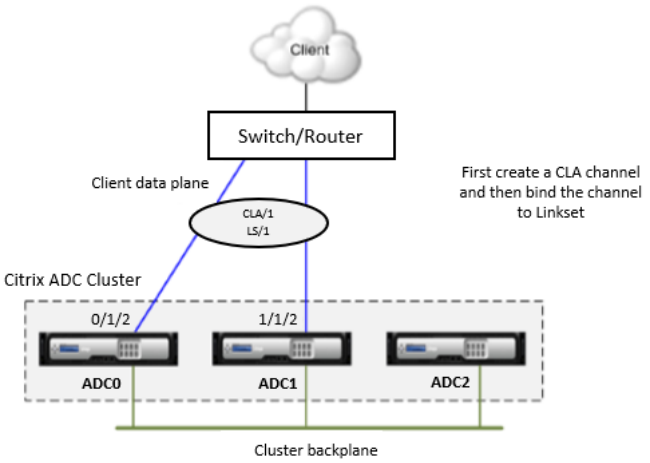
Utilisation de CLAG avec des jeux de liens

Dans une topologie de cluster asymétrique, certains nœuds de cluster ne sont pas connectés au réseau en amont. Dans ce cas, vous devez utiliser des jeux de liens. Pour optimiser les performances, vous pouvez lier les interfaces connectées au commutateur en tant que canal CLA, puis lier le canal CLA à un jeu de liens.

Pour comprendre comment une combinaison de CLAG et de jeux de liens peut être utilisée, considérez un cluster à trois nœuds pour lequel le commutateur en amont ne dispose que de deux ports disponibles. Vous pouvez connecter deux des nœuds de cluster au commutateur et laisser l'autre nœud non connecté.

> Remarque :
>
> De même, vous pouvez également utiliser une combinaison d'ECMP et de jeux de liens dans une topologie asymétrique.

Topologie jeux de liens et CLAG

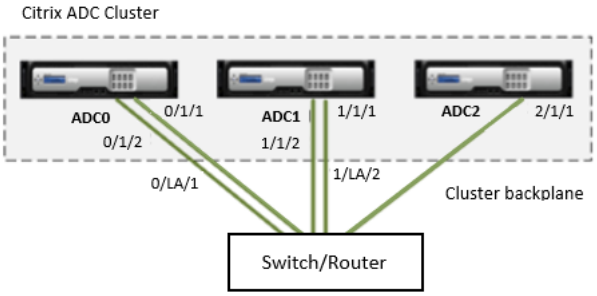


Pour utiliser CLAG et les jeux de liens à l'aide de la ligne de commande Citrix ADC

1. Connectez-vous à l'adresse IP du cluster.
2. Liaison des interfaces connectées à un canal`add channel CLA/1 -ifnum 0/1/2 1/1/2` CLA
3. Liaison du canal CLA à un jeu de liens`add linkset LS/1 -ifnum CLA/1`

Backplane sur LA Channel

Dans ce déploiement, les canaux LA sont utilisés pour le backplane du cluster.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC1 - nodeId: 1, ADCIP: 10.102.29.70

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

Pour déployer un cluster avec les interfaces de backplane en tant que canaux LA

1. Créez un cluster de nœuds ADC0, ADC1 et ADC2.
    - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :


```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

- Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
add cluster node 1 10.102.29.70 -state ACTIVE
add cluster node 2 10.102.29.80 -state ACTIVE
<!--NeedCopy-->
```

- Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

Comme on le voit dans les commandes ci-dessus, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de backplane des trois nœuds de cluster.

2. Connectez-vous à l'adresse IP du cluster et procédez comme suit :
   - Créez les canaux LA pour les nœuds ADC0 et ADC1.

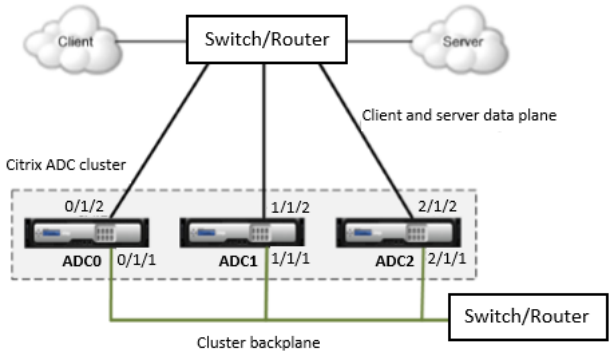
```
add channel 0/LA/1 -ifnum 0/1/1 0/1/2
add channel 1/LA/2 -ifnum 1/1/1 1/1/2
<!--NeedCopy-->
```

   - Configurez le backplane pour les nœuds de cluster.

```
set cluster node 0 -backplane 0/LA/1
set cluster node 1 -backplane 1/LA/2
set cluster node 2 -backplane 2/1/1
<!--NeedCopy-->
```

Interfaces communes pour le client et le serveur et interfaces dédiées pour le backplane

Il s'agit d'un déploiement à un bras du cluster Citrix ADC. Dans ce déploiement, les réseaux client et serveur utilisent les mêmes interfaces pour communiquer avec le cluster. Le backplane du cluster utilise des interfaces dédiées pour la communication entre nœuds.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC1 - nodeId: 1, ADCIP: 10.102.29.70

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

Pour déployer un cluster avec une interface commune pour le client et le serveur et une interface différente pour le backplane du cluster

1. Créez un cluster de nœuds ADC0, ADC1 et ADC2.

   - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

   - Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```


Comme on le voit dans les commandes ci-dessus, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces de backplane et pour les interfaces client et serveur.

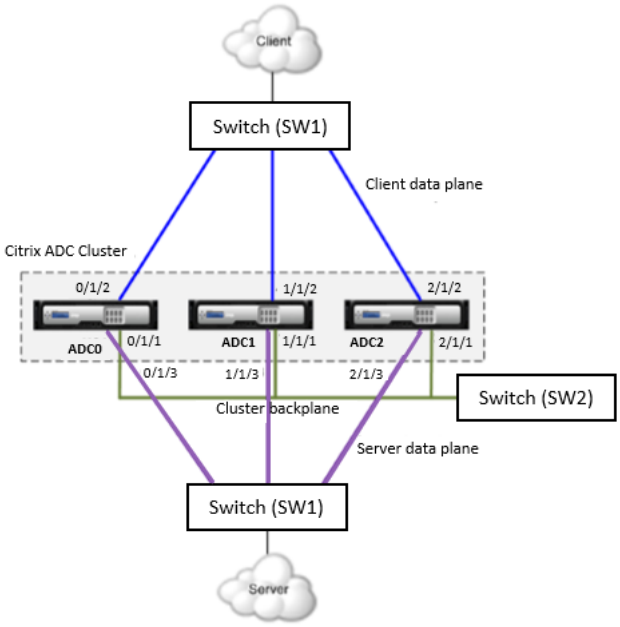
```
1 //For the backplane interfaces
2 add vlan 10
3 bind vlan 10 0/1/1 1/1/1 2/1/1
4 //For the interfaces that are connected to the client and server
     networks
5 add vlan 20
6 bind vlan 20 0/1/2 1/1/2 2/1/2
7 <!--NeedCopy-->
```

3. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configurations suivants sont fournis pour le commutateur SE Cisco C3750 Version 12.2 (40). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
1  //For the backplane interfaces. Repeat for each interface...
2  interface GigabitEthernet1/0/1
3  switchport access vlan 100
4  switchport mode access
5  end
6  //For the interfaces connected to the client and server networks.
      Repeat for each interface...
7  interface GigabitEthernet1/0/3
8  switchport access vlan 200
9  switchport mode access
10 end
11 <!--NeedCopy-->
```

Commutateur commun pour le client, le serveur et le backplane

Dans ce déploiement, le client, le serveur et le backplane utilisent des interfaces dédiées sur le même commutateur pour communiquer avec le cluster Citrix ADC.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC1 - nodeId: 1, ADCIP: 10.102.29.70

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

Pour déployer un cluster avec un commutateur commun pour le client, le serveur et le back-plane

1. Créez un cluster de nœuds ADC0, ADC1 et ADC2.

   - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1 add ns ip 10.102.29.61 255.255.255.255 -
    type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```


- Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

Comme on le voit dans les commandes ci-dessus, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de backplane des trois nœuds de cluster.

2. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces backplane, client et serveur.

```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
//For the client-side interfaces
add vlan 20 bind vlan 20 0/1/2 1/1/2 2/1/2
//For the server-side interfaces
add vlan 30
bind vlan 30 0/1/3 1/1/3 2/1/3
<!--NeedCopy-->
```

3. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configurations suivants sont fournis pour le commutateur SE Cisco C3750 Version 12.2 (40). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

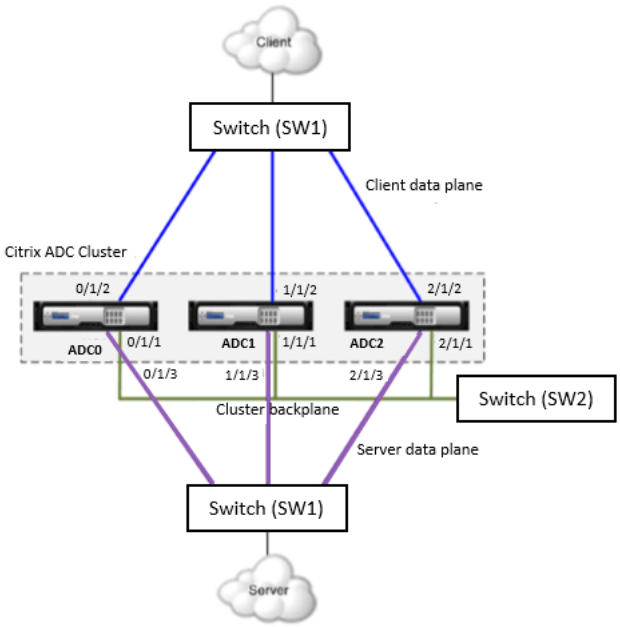
```
//For the backplane interfaces. Repeat for each interface...
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
end
//For the client interfaces. Repeat for each interface...

interface GigabitEthernet1/0/3
switchport access vlan 200
switchport mode access
end
//For the server interfaces. Repeat for each interface...

interface GigabitEthernet1/0/6
switchport access vlan 300
switchport mode access
end
```



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

Commutateur commun pour le client et le serveur et commutateur dédié pour le backplane

Dans ce déploiement, les clients et les serveurs utilisent différentes interfaces sur le même commutateur pour communiquer avec le cluster Citrix ADC. Le backplane du cluster utilise un commutateur dédié pour la communication entre nœuds.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC1 - nodeId: 1, ADCIP: 10.102.29.70

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

Pour déployer un cluster avec le même commutateur pour les clients et les serveurs et un autre commutateur pour le backplane du cluster

1. Créez un cluster de nœuds ADC0, ADC1 et ADC2.
   - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
```



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

- Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

- Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

Comme on le voit dans les commandes ci-dessus, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de fond de panier des trois nœuds de cluster.

2. Sur l'adresse IP du cluster, créez des VLAN pour les interfaces backplane, client et serveur.

```
//For the backplane interfaces
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
//For the client-side interfaces
add vlan 20
bind vlan 20 0/1/2 1/1/2 2/1/2
//For the server-side interfaces
add vlan 30
bind vlan 30 0/1/3 1/1/3 2/1/3
<!--NeedCopy-->
```

1. Sur le commutateur, créez des VLAN pour les interfaces correspondant aux interfaces de backplane et aux interfaces client et serveur. Les exemples de configurations suivants sont fournis pour le commutateur SE Cisco C3750 Version 12.2 (40). Des configurations similaires doivent être effectuées sur d'autres commutateurs.

```
//For the backplane interfaces. Repeat for each interface...
interface GigabitEthernet1/0/1
switchport access vlan 100
switchport mode access
end

//For the client interfaces. Repeat for each interface...
interface GigabitEthernet1/0/3
```

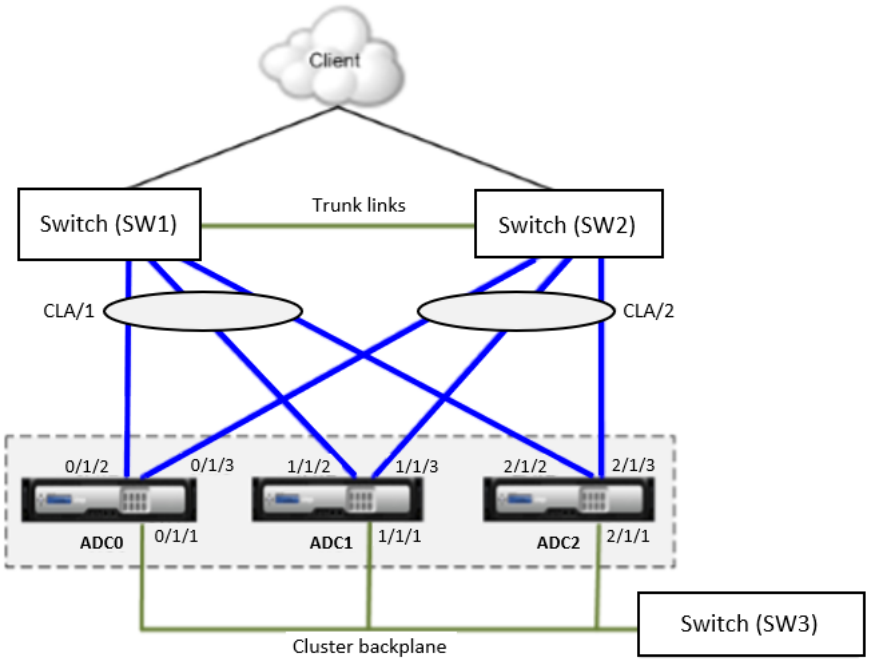


```
switchport access vlan 200
switchport mode access
end

//For the server interfaces. Repeat for each interface...
interface GigabitEthernet1/0/6
switchport access vlan 300
switchport mode access
end
<!--NeedCopy-->
```

Plusieurs commutateurs pour chaque nœud

Dans ce déploiement, nous introduisons deux commutateurs côté client pour assurer la redondance des commutateurs côté client. Les commutateurs sont connectés les uns aux autres par des liaisons de jonction. Une défaillance d'un commutateur n'affectera pas le fonctionnement global du cluster.

> Remarque :
>
> La même stratégie de déploiement peut également être utilisée pour les connexions côté serveur.



ADC0 - nodeId: 0, ADCIP: 10.102.29.60

ADC1 - nodeId: 1, ADCIP: 10.102.29.70

ADC2 - nodeId: 2, ADCIP: 10.102.29.80

> Remarque :
>
> Lors de l'utilisation des liaisons de tronc, il y a possibilité que le trafic circule dans les boucles. Pour éviter cela, vous devez vous assurer que la topologie réseau est configurée pour éviter les boucles.

Pour déployer un cluster avec chaque nœud connecté à deux commutateurs et les commutateurs connectés par des liaisons de jonction

1. Créez un cluster de nœuds ADC0, ADC1 et ADC2.

   - Ouvrez une session sur le premier nœud que vous souhaitez ajouter au cluster et procédez comme suit :

```
create cluster instance 1
add cluster node 0 10.102.29.60 -state ACTIVE -backplane 0/1/1
enable cluster instance 1
add ns ip 10.102.29.61 255.255.255.255 -type CLIP
save ns config
reboot -warm
<!--NeedCopy-->
```

   - Connectez-vous à l'adresse IP du cluster et procédez comme suit :

```
add cluster node 1 10.102.29.70 -state ACTIVE -backplane 1/1/1
add cluster node 2 10.102.29.80 -state ACTIVE -backplane 2/1/1
<!--NeedCopy-->
```

   - Connectez-vous aux nœuds 10.102.29.70 et 10.102.29.80 pour joindre les nœuds au cluster.

```
join cluster -clip 10.102.29.61 -password nsroot
save ns config
reboot -warm
<!--NeedCopy-->
```

   Comme on le voit dans les commandes ci-dessus, les interfaces 0/1/1, 1/1/1 et 2/1/1 sont configurées comme interfaces de backplane des trois nœuds de cluster.

2. Connectez-vous à l'adresse IP du cluster et procédez comme suit :

   - Créez un VLAN pour les interfaces de fond de panier.

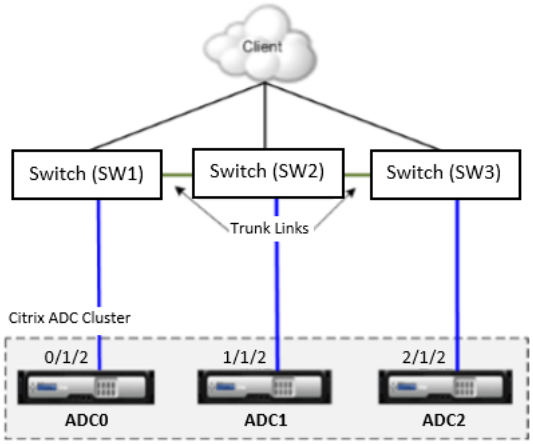
```
add vlan 10
bind vlan 10 0/1/1 1/1/1 2/1/1
<!--NeedCopy-->
```


- Créez un CLAG pour les interfaces côté client avec SW1 et SW2.

```
add channel CLA/1 -ifnum 0/1/2 1/1/2 2/1/2 -speed 1000
add channel CLA/2 -ifnum 0/1/3 1/1/3 2/1/3 -speed 1000
<!--NeedCopy-->
```

Commutateur différent pour chaque nœud

Dans ce déploiement, chaque nœud de cluster est connecté à un commutateur différent et les liaisons de jonction sont configurées entre les commutateurs.



Les configurations de cluster seront les mêmes que les autres scénarios de déploiement. La plupart des configurations côté client seront effectuées sur les commutateurs côté client.

Exemples de configurations de cluster

L'exemple suivant peut être utilisé pour configurer un cluster à quatre nœuds avec ECMP, CLAg ou Jeux de liens.

1. Créez le cluster.

   - Connectez-vous au premier nœud.
   - Ajoutez l'instance de cluster.

```
add cluster instance 1
<!--NeedCopy-->
```

   - Ajoutez le premier nœud au cluster.

```
add cluster node 0 10.102.33.184 -backplane 0/1/1
<!--NeedCopy-->
```


- Activez l'instance de cluster.

```
enable cluster instance 1
<!--NeedCopy-->
```

- Ajoutez l'adresse IP du cluster.

```
add ns ip 10.102.33.185 255.255.255.255 -type CLIP
<!--NeedCopy-->
```

- Enregistrez les configurations.

```
save ns config
<!--NeedCopy-->
```

- Réinitialisez l'appliance à chaud.

```
reboot -warm
<!--NeedCopy-->
```

2. Ajoutez les trois autres nœuds au cluster.
   - Connectez-vous au cluster.
   - Ajoutez le deuxième nœud au cluster.

```
add cluster node 1 10.102.33.187 -backplane 1/1/1
<!--NeedCopy-->
```

   - Ajoutez le troisième nœud au cluster.

```
add cluster node 2 10.102.33.188 -backplane 2/1/1
<!--NeedCopy-->
```

   - Ajoutez le quatrième nœud au cluster.

```
add cluster node 3 10.102.33.189 -backplane 3/1/1
<!--NeedCopy-->
```

3. Joignez les nœuds ajoutés au cluster. Cette étape n'est pas applicable au premier nœud.
   - Connectez-vous à chaque nœud nouvellement ajouté.
   - Joignez le nœud au cluster.

```
join cluster -clip 10.102.33.185 -password nsroot
<!--NeedCopy-->
```


- Enregistrez la configuration.

```
save ns config
<!--NeedCopy-->
```

- Réinitialisez l'appliance à chaud.

```
reboot -warm
<!--NeedCopy-->
```

4. Configurez le cluster Citrix ADC via l'adresse IP du cluster.

```
// Enable load balancing feature enable ns feature lb
// Add a load balancing virtual server add lb vserver
   first_lbvserver http
....
....
<!--NeedCopy-->
```

5. Configurez l'un des mécanismes de distribution de trafic suivants (ECMP, Jeu de liens, CLAG) pour le cluster.

- **ECMP**.
  - Connectez-vous au cluster.
  - Activez le protocole de routage OSPF.

```
enable ns feature ospf
<!--NeedCopy-->
```

  - Ajoutez un VLAN.

```
add vlan 97
<!--NeedCopy-->
```

  - Liez les interfaces des nœuds de cluster au VLAN.

```
bind vlan 97 -ifnum 0/1/4 1/1/4 2/1/4 3/1/4
<!--NeedCopy-->
```

  - Ajoutez un SNIP spotted sur chaque nœud et activez le routage dynamique sur celui-ci.

```
add ns ip 1.1.1.10 255.255.255.0 -ownerNode 0 dynamicRouting
   ENABLED
add ns ip 1.1.1.11 255.255.255.0 -ownerNode 1 dynamicRouting
   ENABLED
```



```
add ns ip 1.1.1.12 255.255.255.0 -ownerNode 2 dynamicRouting
    ENABLED
add ns ip 1.1.1.13 255.255.255.0 -ownerNode 3 dynamicRouting
    ENABLED
<!--NeedCopy-->
```

- Liez l'une des adresses SNIP au VLAN.

```
bind vlan 97 -ipAddress 1.1.1.10 255.255.255.0
<!--NeedCopy-->
```

- Configurez le protocole de routage sur ZeBos à l'aide de vtysh shell.

- **Ensembles de liens**. Supposons que le nœud avecnodeId 3 n'est pas connecté au commutateur. Vous devez configurer un jeu de liens afin que le nœud non connecté puisse utiliser les autres interfaces de nœud pour communiquer avec le commutateur.
  - Connectez-vous au cluster.
  - Ajouter un jeu de liens.

```
add linkset LS/1
<!--NeedCopy-->
```

  - Liez les interfaces connectées au jeu de liens.

```
bind linkset LS/1 -ifnum 0/1/6 1/1/6 2/1/6
<!--NeedCopy-->
```

- **CLAG statique.**
  - Connectez-vous au cluster.
  - Ajouter un canal CLA.

```
add channel CLA/1 -speed 1000
<!--NeedCopy-->
```

  - Liez les interfaces au canal CLA.

```
bind channel CLA/1 0/1/5 1/1/5 2/1/5 3/1/5
<!--NeedCopy-->
```

  - Effectuez une configuration équivalente sur le commutateur.
- **CLAG dynamique.**
  - Connectez-vous au cluster.
  - Ajoutez les interfaces au canal CLA.

```
set interface 0/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
set interface 1/1/5 -lacpmode active -lacpkey 5 -lagtype
    cluster
```



```
3   set interface 2/1/5 -lacpmode active -lacpkey 5 -lagtype
       cluster
4   set interface 3/1/5 -lacpmode active -lacpkey 5 -lagtype
       cluster
5   <!--NeedCopy-->
```

- Effectuez une configuration équivalente sur le commutateur.

6. Mise à jour de l'état des nœuds de cluster vers ACTIVE

```
1 set cluster node 0 -state ACTIVE
2 set cluster node 1 -state ACTIVE
3 set cluster node 2 -state ACTIVE
4 set cluster node 3 -state ACTIVE
5 <!--NeedCopy-->
```

Dépannage du cluster Citrix ADC

Si une défaillance se produit dans un cluster Citrix ADC, la première étape du dépannage consiste à obtenir des informations sur l'instance de cluster et les nœuds de cluster en exécutant les`show cluster instance <clId>` commandes`show cluster node <nodeId>` et respectivement.

Si vous ne parvenez pas à trouver le problème en utilisant les deux approches ci-dessus, vous pouvez utiliser l'une des méthodes suivantes :

- **Isolez la source de l'échec.** Essayez de contourner le cluster pour atteindre le serveur. Si la tentative réussit, le problème est probablement lié à la configuration du cluster.
- **Vérifiez les commandes récemment exécutées.** Exécutez la commande **history** pour vérifier les configurations récentes effectuées sur le cluster. Vous pouvez également consulter le `ns.conf` fichier pour vérifier les configurations qui ont été implémentées.
- **Vérifiez les fichiers ns.log.** Utilisez les fichiers journaux, disponibles dans le `/var/log/` répertoire de chaque nœud, pour identifier les commandes exécutées, l'état des commandes et les changements d'état.
- **Vérifiez les fichiers newnslog.** Utilisez les fichiers newnslog, disponibles dans le `/var/nslog /` répertoire de chaque nœud, pour identifier les événements qui se sont produits sur les nœuds de cluster. Vous pouvez afficher plusieurs fichiers newnslog sous la forme d'un seul fichier, en copiant les fichiers dans un seul répertoire, puis en exécutant la commande suivante :

```
1 nsconmsg -K newnslog-node<id> -K newnslog.node<id> -d current
2 <!--NeedCopy-->
```

Si vous ne pouvez toujours pas résoudre le problème, vous pouvez essayer de tracer les paquets sur le cluster ou utiliser la commande **show tech support scope cluster** pour envoyer le rapport à l'équipe de support technique.

Suivi des paquets d'un cluster Citrix ADC

Le système d'exploitation Citrix ADC fournit un utilitaire appelé nstrace pour obtenir un vidage des paquets reçus et envoyés par une solution matérielle-logicielle. L'utilitaire stocke les paquets dans des fichiers de suivi. Vous pouvez utiliser ces fichiers pour déboguer des problèmes dans le flux de paquets vers les nœuds de cluster. Les fichiers de suivi doivent être affichés avec l'application Wireshark. Pour les traces collectées en mode natif (.cap), il est important d'utiliser la version interne de Wireshark, qui peut comprendre les paquets natifs.

Certains aspects saillants de l'utilitaire nstrace sont :

- Peut être configuré pour tracer les paquets de manière sélective à l'aide d'expressions classiques et d'expressions par défaut.
- Peut capturer la trace dans plusieurs formats : format nstrace (.cap) et format de vidage TCP (.pcap).
- Peut agréger les fichiers de trace de tous les nœuds de cluster sur le CCO.
- Peut fusionner plusieurs fichiers de trace en un seul fichier de trace.

Vous pouvez utiliser l'utilitaire nstrace à partir de la ligne de commande Citrix ADC ou de l'interpréteur de commandes Citrix ADC.

Pour suivre les paquets d'une appliance autonome

Exécutez la commande start nstrace sur l'appliance. La commande crée des fichiers de trace dans le `/var/nstrace/<date-timestamp>` répertoire. Les noms des fichiers de suivi sont au format `nstrace<id>.cap`.

Vous pouvez afficher l'état en exécutant la commande **show nstrace** . Vous pouvez arrêter le suivi des paquets en exécutant la commande **stop nstrace** .

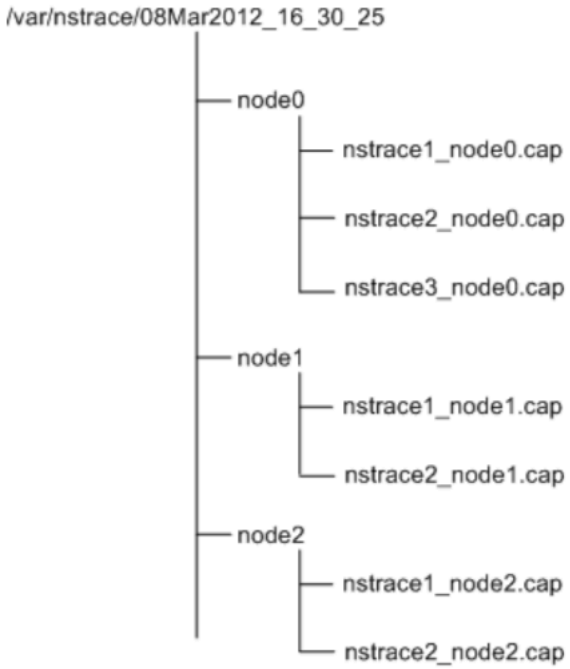
> Remarque :
>
> Vous pouvez également exécuter l'utilitaire nstrace à partir du shell Citrix ADC en exécutant le fichier nstrace.sh. Citrix recommande d'utiliser l'utilitaire nstrace via la ligne de commande Citrix ADC.

Pour suivre les paquets d'un cluster

Vous pouvez suivre les paquets sur tous les nœuds de cluster et obtenir tous les fichiers de trace sur le nœud CCO.

Exécutez la commande **start nstrace** sur l'adresse IP du cluster. La commande est propagée et exécutée sur tous les nœuds de cluster. Les fichiers de suivi sont stockés dans des nœuds de cluster individuels dans le `/var/nstrace/<date-timestamp>` répertoire. Les noms des fichiers de suivi sont au format `nstrace<id>_node<id>.cap`.

Vous pouvez utiliser les fichiers de trace de chaque nœud pour déboguer les opérations des nœuds. Mais si vous souhaitez que les fichiers de trace de tous les nœuds de cluster soient situés à un seul emplacement, vous devez exécuter la commande **stop nstrace** sur l'adresse IP du cluster. Les fichiers de suivi de tous les nœuds sont téléchargés sur le nœud CCO (cluster Configuration Coordinator) du /var/nstrace/<date-timestamp> répertoire comme suit :



Fusionner plusieurs fichiers de trace

Vous pouvez préparer un seul fichier à partir des fichiers de trace obtenus à partir des nœuds de cluster. Les fichiers de trace uniques vous donnent une vue cumulative de la trace des paquets de cluster. Les entrées de suivi dans le fichier de suivi unique sont triées en fonction de l'heure à laquelle les paquets ont été reçus sur le cluster.

Pour fusionner les fichiers de trace, dans le shell Citrix ADC, tapez :`nstracemerge.sh -srcdir <DIR> -dstdir <DIR> -filename <name> -filesize <num>`.

- **srcdir** est le répertoire à partir duquel les fichiers de trace sont fusionnés. Tous les fichiers de suivi de ce répertoire sont fusionnés en un seul fichier.
- **dstdir** est le répertoire dans lequel le fichier de trace fusionné est créé.
- **nomfichier** est le nom du fichier de trace créé.
- **filesize** est la taille du fichier trace.

Voici quelques exemples d'utilisation de l'utilitaire nstrace pour filtrer les paquets.

- Pour suivre les paquets sur les interfaces de backplane de trois nœuds :

- **Utilisation d'expressions classiques :**

```
start nstrace -filter /"INTF == 0/1/1 && INTF == 1/1/1 && INTF==
   2/1/1"
<!--NeedCopy-->
```

- **Utilisation des expressions par défaut :**

```
start nstrace -filter "CONNECTION.INTF.EQ("0/1/1") &&CONNECTION.
   INTF.EQ("1/1/1") && CONNECTION.INTF.EQ("2/1/1")"
<!--NeedCopy-->
```

- Pour suivre les paquets à partir d'une adresse IP source 10.102.34.201 ou d'un système dont le port source est supérieur à 80 et le nom de service n'est pas "s1" :

- **Utilisation d'expressions classiques**

```
start nstrace -filter "SOURCEIP == 10.102.34.201 || (SVCNAME !=
   s1 && SOURCEPORT > 80)"
<!--NeedCopy-->
```

- **Utilisation d'expressions par défaut**

```
start nstrace -filter "CONNECTION.SRCIP.EQ(10.102.34.201) ||(
   CONNECTION.SVCNAME.NE("s1") && CONNECTION.SRCPORT.GT(80))"
<!--NeedCopy-->
```

Résolution des problèmes courants

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : nom/numéro d'interface non valide." Que dois-je faire pour résoudre cette erreur ?

- Cette erreur se produit si vous avez fourni une interface de fond de panier non valide ou incorrecte lors de l'utilisation de la commande **add cluster node** pour ajouter le nœud. Pour résoudre cette erreur, vérifiez l'interface que vous avez fournie lors de l'ajout du nœud. Assurez-vous que vous n'avez pas spécifié l'interface de gestion de l'appliance comme interface de fond de panier et que le bit **NodeID** de l'interface est identique à l'ID du nœud. Par exemple, si la valeur **NodeID** est **3** , l'interface du fond de panier doit être`3/<c>/<u>` .

Lors de la jonction d'un nœud au cluster, je reçois le message suivant : "ERREUR : Le clustering ne peut pas être activé, car le nœud local n'est pas membre du cluster." Que dois-je faire pour résoudre cette erreur ?

- Cette erreur se produit lorsque vous essayez de joindre un nœud sans ajouter l'ADCIP du nœud au cluster. Pour résoudre cette erreur, vous devez d'abord ajouter l'adresse ADCIP du nœud au cluster à l'aide de la commande **add cluster node** , puis exécuter la commande **join cluster** .

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : Connexion refusée." Que dois-je faire pour résoudre cette erreur ?

Cette erreur peut se produire pour les raisons suivantes :

- **Problèmes de connectivité.** Le nœud ne peut pas se connecter à l'adresse IP du cluster. Essayez d'effectuer un ping sur l'adresse IP du cluster à partir du nœud que vous essayez de joindre.
- **Dupliquer l'adresse IP du cluster.** Vérifiez si l'adresse IP du cluster existe sur un nœud non cluster. Si c'est le cas, créez une nouvelle adresse IP de cluster et essayez de rejoindre le cluster.

Lors de la jonction d'un nœud au cluster, je reçois le message suivant, "ERREUR : Licence non concordante entre CCO et nœud local." Que dois-je faire pour résoudre cette erreur ?

- La solution matérielle-logicielle que vous joignez au cluster doit posséder les mêmes licences que le CCO. Cette erreur se produit lorsque les licences sur le nœud que vous rejoignez ne correspondent pas aux licences sur le CCO. Pour résoudre cette erreur, exécutez les commandes suivantes sur les deux nœuds et comparez les sorties.

  À partir de la ligne de commande, exécutez :

  - Afficher ns matériel
  - Afficher la licence ns

  À partir du shell, exécutez :

  - nsconmsg -g feature -d stats
  - ls /nsconfig/license
  - Afficher le contenu du fichier /var/log/license.log

Que dois-je faire lorsque les configurations d'un nœud de cluster ne sont pas synchronisées avec les configurations de cluster ?

- Habituellement, les configurations sont automatiquement synchronisées entre tous les nœuds de cluster. Toutefois, si vous estimez que les configurations ne sont pas synchronisées sur un nœud spécifique, vous devez forcer la synchronisation en exécutant la commande force cluster sync à partir du nœud que vous souhaitez synchroniser. Pour plus d'informations, reportez-vous à la section Synchronisation des configurations de cluster.

Les configurations sur les nœuds de cluster ne sont pas synchronisées. Comment puis-je m'assurer que les configurations sont toujours synchronisées ?

- Pour assurer la synchronisation des configurations de cluster sur les nœuds, exécutez la commande **save ns config** après chaque configuration. Sinon, les configurations peuvent ne pas être disponibles sur les nœuds de cluster lors du redémarrage.

Lors de la configuration d'un nœud de cluster, je reçois le message suivant : "ERREUR : La session est en lecture seule ; connectez-vous à l'adresse IP du cluster pour modifier la configuration."

- Toutes les configurations d'un cluster doivent être effectuées via l'adresse IP du cluster et les configurations sont propagées aux autres nœuds de cluster. Toutes les sessions établies via l'adresse IP Citrix ADC (ADCIP) de nœuds individuels sont en lecture seule.

Pourquoi l'état du nœud affiche-t-il « INACTIVE » lorsque l'état du nœud affiche « UP » ?

- Un nœud sain peut être dans l'état INACTIVE pour un certain nombre de raisons. Une analyse de compteurs`ns.log` ou d'erreurs peut vous aider à déterminer la raison exacte.

Comment puis-je résoudre l'intégrité d'un nœud lorsque son état affiche « Not UP » ?

- L'intégrité du nœud No **t UP** indique qu'il y a des problèmes avec le nœud. Pour connaître la cause première, vous devez exécuter la commande **sh cluster node** . Cette commande affiche les propriétés du nœud et la raison de l'échec du nœud.

Lorsque j'exécute la commande set vserver, j'obtiens le message suivant, "Aucune ressource de ce genre." Que dois-je faire pour résoudre ce problème ?

- La commande **set vserver** n'est pas prise en charge dans le clustering. Les commandes **unset vserver**, **enable vserver**, **disable vserver**et **rm vserver**ne sont pas non plus prises en charge. Toutefois, la commande **show vserver** est prise en charge.

Je ne peux pas configurer le cluster sur une session Telnet. Que dois-je faire ?

- Sur une session telnet, l'adresse IP du cluster est accessible uniquement en mode lecture seule. Par conséquent, vous ne pouvez pas configurer un cluster sur une session telnet.

Je remarque une différence d'heure significative entre les nœuds de cluster. Que dois-je faire pour résoudre ce problème ?

Lorsque des paquets PTP sont abandonnés en raison d'un commutateur de backplane ou si les ressources physiques sont surengagées dans un environnement virtuel, l'heure ne sera pas synchronisée.

Pour synchroniser les heures, vous devez effectuer les opérations suivantes sur l'adresse IP du cluster :

1. Désactivez PTP.

```
set ptp -state disable
<!--NeedCopy-->
```

2. Configurer le protocole NTP (Network Time Protocol) pour le cluster. Pour plus d'informations, consultez la section Configuration de la synchronisation d'horloge à l'aide de l'interface de ligne de commande ou de l'utilitaire de configuration.

Questions fréquentes

Combien d'appliances Citrix ADC puis-je avoir dans un cluster ?

- Un cluster Citrix ADC peut inclure jusqu'à 2 ou jusqu'à 32 appliances matérielles ou virtuelles Citrix ADC nCore.

J'ai plusieurs nœuds autonomes, dont chacun a des configurations différentes. Puis-je les ajouter à un seul cluster ?

- Oui. Vous pouvez ajouter un maximum de 32 nœuds au cluster. Toutefois, les configurations existantes des appliances sont effacées lorsque les nœuds sont ajoutés au cluster. Pour utiliser les configurations de solutions matérielles-logicielles individuelles, vous devez préparer manuellement un `*.conf` fichier unique de toutes les configurations, modifier les configurations pour supprimer les fonctionnalités non prises en charge par le clustering, modifier la convention de nommage des interfaces, puis appliquer la méthode au CCO à l'aide de la commande **batch** .

Puis-je migrer les configurations d'une appliance Citrix ADC autonome ou d'une installation HA vers la configuration en cluster ?

- Non. Lorsqu'un nœud est ajouté à une configuration en cluster, la commande **clear ns config** (avec l'option étendue) est exécutée sur cette appliance. En outre, les adresses SNIP et toutes les configurations VLAN (sauf VLAN et ADCVLAN par défaut) sont effacées. Par conséquent, Citrix recommande de sauvegarder les configurations avant d'ajouter la solution matérielle-logicielle à un cluster.

Puis-je détecter automatiquement les appliances Citrix ADC afin de pouvoir les ajouter à un cluster ?

- Oui. L'utilitaire de configuration vous permet de découvrir les appliances Citrix ADC présentes dans le même sous-réseau que l'adresse ADCIP du CCO. Pour plus d'informations, reportez-vous à la section Découvrir les appliances Citrix.

Le cluster est-il une fonctionnalité sous licence ?

- Oui, le cluster est une fonctionnalité sous licence. Vous devez avoir une copie du fichier de licence de cluster dans le `/nsconfig/license/` répertoire de toutes les appliances que vous souhaitez ajouter au cluster. En outre, toutes les appliances que vous souhaitez ajouter au cluster doivent également disposer des mêmes fichiers de licence disponibles.

Un dispositif Citrix ADC peut-il faire partie de plusieurs clusters ?

- Non. Une solution matérielle-logicielle ne peut appartenir qu'à un seul cluster.

Un nœud qui n'est pas connecté au réseau client ou serveur peut-il encore servir le trafic ?

- Oui. Le cluster Citrix ADC prend en charge un mécanisme de distribution de trafic appelé jeux de liens, qui permet aux nœuds non connectés de servir le trafic à l'aide des interfaces de nœuds connectés. Les nœuds non connectés communiquent avec les nœuds connectés via le backplane du cluster.

Que se passera-t-il si la licence de cluster sur un nœud a expiré ?

- Si la licence de cluster sur un nœud expire lorsque le nœud est en cours d'exécution, le cluster n'est pas affecté. Toutefois, lorsque vous redémarrez ce nœud, le cluster est désactivé opérationnellement sur ce nœud, par conséquent, le nœud ne pourra pas servir le trafic. Pour corriger le problème et rendre le nœud actif, vous devez télécharger une nouvelle licence et redémarrer à chaud la solution matérielle-logicielle.

Pourquoi les interfaces réseau d'un cluster sont-elles représentées en utilisant une notation 3-tuple (n/u/c) au lieu de la notation 2-tuple (u/c) normale ?

- Lorsqu'une solution matérielle-logicielle fait partie d'un cluster, vous devez être en mesure d'identifier le nœud auquel appartient l'interface réseau. Ainsi, la convention de nommage de l'interface réseau pour les nœuds de cluster est modifiée de u/c à n/u/c, où n indique l'ID du nœud.

Qu'est-ce qu'une adresse IP par bandes ?

- Toute adresse IP (VIP ou SNIP) définie sur le cluster est, par défaut, une adresse IP répartie. Les adresses IP par bandes sont actives sur tous les nœuds du cluster.

Qu'est-ce qu'une adresse IP ponctuée ? Puis-je modifier la propriété d'une adresse IP ponctuée au moment de l'exécution ?

- Une adresse IP ponctuée est une adresse IP active et détenue exclusivement par un nœud du cluster. L'adresse IP ponctuée doit être définie via l'adresse IP du cluster, en spécifiant le nœud propriétaire dans la commande **add ns ip** .

Vous ne pouvez pas modifier la propriété d'une adresse IP ponctuée au moment de l'exécution. Pour modifier la propriété, vous devez d'abord supprimer l'adresse IP et l'ajouter à nouveau en spécifiant le nouveau propriétaire.

Qu'est-ce que CCO ?

- CCO est la forme abrégée de *Configuration Coordinator*. Ce nœud possède l'adresse IP du cluster et coordonne toutes les configurations du cluster.

Qu'est-ce qu'une adresse IP de cluster ? Quel est son masque de sous-réseau ?

- L'adresse IP du cluster est l'adresse de gestion d'un cluster Citrix ADC. Toutes les configurations de cluster doivent être effectuées en accédant au cluster via cette adresse. Le masque de sous-réseau de l'adresse IP du cluster est fixé à 255.255.255.255.

Lorsque j'ai ajouté le premier nœud au cluster, c'était le coordinateur de configuration (CCO). Maintenant, un autre nœud est affiché en tant que CCO. Pourquoi ?

- Lorsqu'un cluster est créé, le premier nœud devient le CCO. L'adresse IP du cluster appartient à ce nœud. Cependant, le CCO n'est pas un nœud fixe. Il peut changer au fil du temps pour diverses raisons. Dans ce cas, le cluster choisit un nouveau CCO et attribue l'adresse IP du cluster au nouvel CCO.

Puis-je exécuter des commandes à partir de l'adresse ADCIP d'un nœud de cluster ?

- Non. L'accès aux nœuds de cluster individuels via les adresses IP Citrix ADC (ADCIP) est en lecture seule. Cela signifie que lorsque vous vous connectez à l'adresse ADCIP d'un nœud de cluster, vous ne pouvez afficher que les configurations et les statistiques. Vous ne pouvez pas effectuer de configurations. Toutefois, certaines opérations peuvent être exécutées à partir de l'adresse ADCIP d'un nœud de cluster. Pour plus d'informations, reportez-vous à la section Opérations prises en charge sur des nœuds individuels.

Puis-je désactiver la propagation de la configuration entre les nœuds de cluster ?

- Non, vous ne pouvez pas désactiver explicitement la propagation des configurations de cluster entre les nœuds de cluster. Toutefois, la propagation de la configuration peut être désactivée automatiquement lors de la mise à niveau ou de la rétrogradation du logiciel en raison d'une incompatibilité de version.

Comment puis-je supprimer un cluster et tous les nœuds du cluster ?

- Pour supprimer un cluster et tous les nœuds du cluster, vous devez supprimer chaque nœud individuellement, comme décrit à la sectionSuppression d'un nœud de cluster.

Puis-je modifier l'adresse ADCIP ou l'ADCVLAN d'un dispositif Citrix ADC lorsqu'il fait partie du cluster ?

- Non. Pour effectuer de telles modifications, vous devez d'abord supprimer l'appliance du cluster, effectuer les modifications, puis ajouter l'appliance au cluster.

Le cluster Citrix ADC prend-il en charge les réseaux locaux virtuels (VLAN) L2 et L3 ?

- Oui, un cluster Citrix ADC prend en charge les VLAN entre les nœuds de cluster. Les VLAN doivent être configurés sur l'adresse IP du cluster.
  - **VLAN L2.** Vous pouvez créer un VLAN de couche 2 en liant des interfaces appartenant à différents nœuds du cluster.
  - **VLAN L3.** Vous pouvez créer un VLAN de couche 3 en liant des adresses IP appartenant à différents nœuds du cluster. Les adresses IP doivent appartenir au même sous-réseau. Assurez-vous que l'un des critères suivants est satisfait. Sinon, les liaisons VLAN L3 peuvent échouer :
    * Tous les nœuds ont une adresse IP sur le même sous-réseau que celui lié au VLAN.
    * Le cluster a une adresse IP répartie et le sous-réseau de cette adresse IP est lié au VLAN.

Lorsque vous ajoutez un nouveau nœud à un cluster qui n'a que des adresses IP spotted, la synchronisation se produit avant que les adresses IP spotted ne soient affectées à ce nœud. Dans de tels cas, les liaisons VLAN L3 peuvent être perdues. Pour éviter cette perte, ajoutez une adresse IP répartie ou ajoutez les liaisons VLAN L3 sur l'ADCIP du nœud nouvellement ajouté.

Pourquoi les liaisons VLAN et VLAN sont-elles supprimées lorsqu'une appliance Citrix ADC est ajoutée au cluster ?

- Lorsqu'une appliance Citrix ADC est ajoutée à une installation en cluster, la commande clear ns config (avec l'option étendue) est exécutée sur cette appliance. En outre, les adresses SNIP et toutes les configurations VLAN (à l'exception des VLAN et ADCVLAN par défaut) sont effacées.

Comment puis-je configurer SNMP sur un cluster Citrix ADC ?

- SNMP surveille le cluster et tous les nœuds du cluster, de la même manière qu'un dispositif Citrix ADC autonome. La seule différence est que SNMP sur un cluster doit être configuré via l'adresse IP du cluster. Lors de la génération d'interruptions spécifiques au matériel, deux varbinds supplémentaires sont inclus pour identifier le nœud du cluster : l'ID du nœud et l'ADCIP du nœud.

Pour plus d'informations sur la configuration de SNMP, reportez-vous à la SNMP section.

Quels détails dois-je disposer lorsque je contacte le support technique pour des problèmes liés au cluster ?

- Citrix ADC fournit une commande **show techsupport -scope cluster** qui extrait les données de configuration, les informations statistiques et les journaux de tous les nœuds de cluster. Vous devez exécuter cette commande sur l'adresse IP du cluster.

La sortie de cette commande est enregistrée dans un fichier nommé `collector_cluster_<nsip_CCO>_P_<date-timestamp>.tar.gz`, qui est disponible dans le `/var/tmp/support/cluster/` répertoire du CCO. Envoyez cette archive à l'équipe de support technique pour déboguer le problème.

Opérations prises en charge sur des nœuds individuels

Toutes les configurations de cluster sont effectuées sur le CCO via l'adresse IP du cluster et ces configurations sont propagées aux nœuds du cluster. Toutefois, certaines opérations peuvent être effectuées sur des nœuds de cluster individuels en y accédant via leurs adresses IP ADCIP (Citrix ADC).

- activer l'instance de cluster w désactiver l'instance de cluster
- set cluster instance
- rm cluster instance
- set cluster node
- rm cluster node
- force cluster sync
- sync cluster files
- send arp all
- start nstrace
- stop nstrace

- show nstrace
- set interface
- enable interface w disable interface w save ns config
- redémarrez

> Remarque :
>
> Toutes les commandes show et stat sont autorisées car elles n'impliquent aucun changement de configuration.

Conception de référence validée de capacité groupée Citrix ADC

March 10, 2020

La capacité mise en commun de Citrix ADC est un cadre de licences composé d'un pool de bande passante et d'un pool d'instances virtuelles hébergé sur Citrix Application Delivery Management (ADM) et desservi par Citrix Application Delivery Management (ADM). À partir de ce pool commun, chaque Citrix ADC dans un centre de données, vérifie une licence d'instance virtuelle et seulement autant de bande passante que nécessaire. Il le fait indépendamment de la plate-forme ou du facteur de forme (sauf pour le MPX-Z, qui ne vérifie qu'une licence de bande passante). Le fichier de licence et la bande passante ne sont pas liés à Citrix ADC. Lorsque Citrix ADC n'a plus besoin de ces ressources, il les réintègre dans le pool commun, ce qui rend les ressources disponibles pour les autres ADC qui en ont besoin.

Ce cadre de licences maximise l'utilisation de la bande passante en veillant à ce que les ADC n'allouent pas de bande passante inutilisée excédentaire. La capacité de Citrix ADC à vérifier les licences et la bande passante dans et hors d'un pool commun permet aux utilisateurs et aux administrateurs d'automatiser le provisioning des instances. Les utilisateurs et les administrateurs peuvent augmenter ou diminuer la bande passante allouée à une instance au moment de l'exécution sans affecter le trafic. De plus, les licences Citrix ADC dans le pool peuvent également être transférées d'une instance à une autre, et ces licences peuvent être partagées par tous les facteurs de forme (MPX, SDX, VPX et CPX).

Composants

La capacité groupée découple le logiciel du matériel sous-jacent. Cette approche permet un modèle de licence transférable des plateformes existantes vers de nouvelles plateformes. La capacité groupée se compose de quatre éléments :

1. Matériel à capacité nulle qui n'a aucune bande passante, aucune instance et aucune fonctionnalité.

2. Un pool de bande passante avec l'édition logicielle (standard, avancé et premium) qui peut être partagé entre tous les facteurs de forme Citrix ADC, y compris MPX, SDX, VPX et CPX.
3. Pool d'instances, qui est un pool d'instances partagé entre des facteurs de forme logiciels/virtuels Citrix ADC, y compris VPX s'exécutant sur SDX, VPX autonome et CPX.
4. Citrix ADM, qui est utilisé pour gérer la bande passante et les licences d'instance. Cette fonction de Citrix ADM est gratuite pour le client.

Les composants de la capacité groupée sont discutés plus en détail plus loin dans cet article.

Licences perpétuelles

Une licence perpétuelle est une licence qui n'expire pas. Avec une licence perpétuelle, un utilisateur paie des frais uniques et a le droit d'utiliser la licence pour toujours. Voici quelques points à considérer :

- Il y a souvent des restrictions sur une licence perpétuelle, telles que les coûts récurrents de soutien à la maintenance.
- La licence est liée à une plate-forme matérielle spécifique et ne peut généralement pas être déplacée.
- La licence peut devenir obsolète à mesure que la technologie évolue.
- Les fonctionnalités spécifiques sont activées avec un droit de licence perpétuel qui sont spécifiques à l'édition, comme la bande passante. Pour Citrix ADC, les licences spécifiques à ces éditions sont les éditions Standard, Avancé et Premium.

En revanche, une licence de capacité groupée n'est pas liée à une plate-forme matérielle spécifique, et elle est transférable des plates-formes existantes vers de nouvelles plates-formes.

Avantages de la capacité mise en commun

Cas d'utilisation 1 : Déplacement vers le cloud

La capacité mise en commun facilite l'adoption du cloud hybride en assurant une protection de l'investissement sur l'infrastructure existante. Les clients peuvent choisir de déplacer une partie de leur capacité des déploiements sur site vers le cloud, réduisant ainsi le coût des appliances Citrix ADC.

Cas d'utilisation 2 : Cycles de rafraîchissement du matériel

Les clients qui ont déjà déployé Citrix ADC dans un déploiement traditionnel doivent désormais tout racheter lorsqu'ils actualisent leur environnement. Avec les licences Citrix ADC groupées, un cycle d'actualisation nécessite uniquement l'actualisation du matériel pendant la conservation du logiciel.

Lorsque le matériel est actualisé, les licences logicielles peuvent être facilement transférées des appliances héritées vers les nouvelles appliances matérielles/logicielles. Cela réduit considérablement le coût des cycles de rafraîchissement et permet aux clients d'examiner les cycles de rafraîchissement plus tôt que l'intervalle traditionnel de 5 ans.

Cas d'utilisation 3 : déploiement de DevOps (VPX/CPX)

Les clients qui ont investi dans des appliances à capacité nulle peuvent acheter des appliances CPX et transférer une partie de leur capacité dans un environnement de microservices. Ils peuvent également acheter des capacités supplémentaires pour prendre en charge une nouvelle architecture. Dans l'ensemble, il s'agit d'une transition beaucoup plus rentable de l'architecture sur site ou matérielle à l'architecture microservices ou logicielle.

Fonctionnement de la capacité groupée

Description

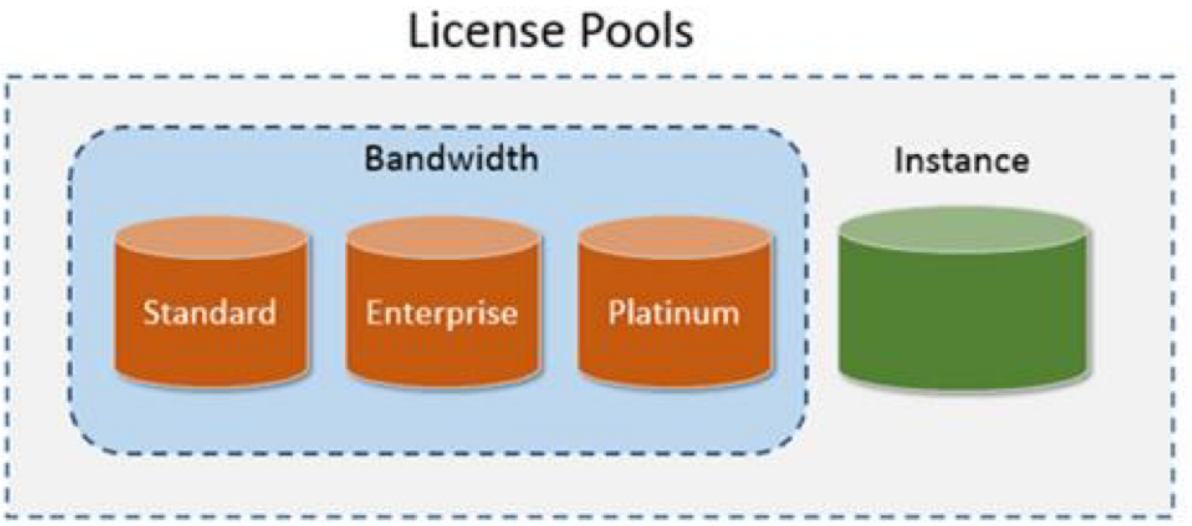
La capacité groupée est un cadre de licence qui découple le logiciel du matériel sous-jacent. Cette approche permet un modèle de licence transférable des plates-formes existantes vers de nouvelles plates-formes, et elle maximise l'utilisation de la bande passante en veillant à ce que les ADC ne reçoivent pas une bande passante supérieure à leurs besoins. La capacité des Citrix ADC à vérifier les licences et la bande passante dans et hors d'un pool commun permet également aux utilisateurs d'automatiser le provisioning des instances.

Les utilisateurs peuvent augmenter ou diminuer la bande passante allouée à Citrix ADC au moment de l'exécution sans affecter le trafic. Les utilisateurs peuvent également transférer les licences Citrix ADC dans le pool d'un Citrix ADC à un autre.

Flux de licences

Les clients achètent des licences de capacité groupée Citrix ADC et les téléchargent à partir dePage de connexion Mon compte.

Ensuite, ces licences sont importées dans Citrix ADM.



Matériel à capacité nulle

Lorsqu'elles sont gérées via une capacité groupée Citrix ADC, les instances SDX sont appelées « matériel à capacité nulle » car ces instances ne peuvent pas fonctionner tant qu'elles n'ont pas réussi à extraire les ressources de la bande passante et des pools d'instances. Par conséquent, ces plates-formes sont appelées appliances SDX-Z.

De même, les appliances MPX sont également appelées « matériel à capacité nulle » lorsqu'elles sont gérées via une capacité groupée Citrix ADC, car elles ne peuvent pas fonctionner tant qu'elles n'ont pas vérifié les ressources du pool de bande passante. Par conséquent, ces plates-formes sont appelées appliances MPX-Z.

Les appliances matérielles à capacité nulle nécessitent une licence de plate-forme pour récupérer la bande passante et/ou une licence d'instance du pool commun. Les utilisateurs doivent d'abord installer une licence de plate-forme manuellement à l'aide du numéro de série du matériel ou du code d'accès à la licence.

Actuellement, les plates-formes à capacité zéro suivantes, exécutant le logiciel Citrix ADC version 11.1 ou ultérieure, prennent en charge la capacité groupée Citrix ADC pour les nouveaux achats et mises à niveau :

- MPX-14000Z
- MPX-14000Z-40G
- MPX-15000Z
- MPX-15000Z-50G
- MPX-25000Z-40G
- MPX-26000Z

- MPX-26000Z-100G
- SDX-14000Z
- SDX-14000Z-40G
- SDX-15000Z-50G
- SDX-25000Z-40G
- SDX-26000Z-100G

Actuellement, les plates-formes à capacité zéro suivantes, exécutant le logiciel Citrix ADC version 12.0 ou ultérieure (MPX) et 11.1 ou version ultérieure (SDX), prennent en charge la capacité groupée Citrix ADC pour les nouveaux achats et mises à niveau :

- MPX-14000Z-40S
- MPX-14000Z-40C
- MPX-14000 FIPS
- MPX-25000ZA
- MPX-26000Z-50S
- SDX-14000Z-40S
- SDX-14000Z-40C
- SDX-14000 FIPS
- SDX-25000ZA

Actuellement, les plates-formes à capacité zéro suivantes, exécutant le logiciel Citrix ADC version 12.0 ou ultérieure, prennent en charge la capacité groupée Citrix ADC pour les nouveaux achats et mises à niveau :

- MPX-8900Z
- SDX-8900Z

Actuellement, les plates-formes à capacité zéro suivantes, exécutant le logiciel Citrix ADC version 12.0 ou ultérieure (MPX) et 11.1 ou version ultérieure (SDX), prennent en charge la capacité groupée Citrix ADC pour la mise à niveau uniquement :

- MPX-115xx (11515 - 11542)
- MPX-89xx/80xx
- MPX-22xxx
- MPX-24xxx
- SDX-115xx (11515 - 11542)

- SDX-89xx/80xx
- SDX-22xxx
- SDX-24xxx

Actuellement, les plates-formes à capacité zéro suivantes, exécutant le logiciel Citrix ADC version 11.1 ou ultérieure, prennent en charge la capacité groupée Citrix ADC uniquement pour les nouveaux achats :

- VPX
- CPX

Instances Citrix ADC VPX autonomes

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 11.1 ou ultérieure sur les hyperviseurs suivants prennent en charge la capacité groupée :

- VMware ESX 6.0
- Citrix XenServer
- KVM Linux

Les instances Citrix ADC VPX exécutant le logiciel Citrix ADC version 12.0 ou ultérieure sur les hyperviseurs et plates-formes cloud suivants prennent en charge la capacité groupée :

- Microsoft Hyper-V
- Amazon AWS
- Microsoft Azure

> Remarque :
>
> Pour activer la communication entre Citrix ADM et Microsoft Azure ou AWS, un tunnel IPSEC doit être configuré. Pour plus d'informations, reportez-vous à la section Ajouter des instances NetScaler VPX déployées dans le cloud à NetScaler MAS.

Instances Citrix ADC CPX autonomes

Les instances CPX Citrix ADC déployées sur un hôte Docker prennent en charge la capacité groupée. Contrairement au matériel à capacité nulle, CPX ne nécessite pas de licence de plate-forme. Pour traiter le trafic, il doit extraire une licence d'instance du pool.

Pool de bande passante

Le pool de bande passante est la bande passante totale qui peut être partagée par Citrix ADC, tant physique que virtuelle. Le pool de bande passante comprend des pools distincts pour chaque édition logicielle (Standard, Avancé et Premium). Un Citrix ADC donné ne peut pas avoir la bande passante provenant de différents pools récupérée simultanément. Le pool de bande passante à partir duquel un Citrix ADC peut extraire la bande passante dépend de son édition logicielle pour laquelle il est sous licence. Lorsqu'elle est retirée du pool, une licence déverrouille des ressources telles que les CPU/PE, les cœurs SSL, les paquets par seconde et la bande passante.

Pool d'instances

Le pool d'instances définit le nombre d'instances VPX ou CPX qui peuvent être gérées via la capacité groupée Citrix ADC ou le nombre d'instances VPX dans un SDX-Z.

> Remarque :
>
> Le service de gestion d'un SDX-Z ne consomme pas d'instance.

Citrix ADM

La capacité groupée Citrix ADC utilise Citrix ADM pour gérer les licences de capacité groupée : licences de pool de bande passante et licences de pool d'instances. Les utilisateurs peuvent utiliser Citrix ADM pour gérer les licences de capacité groupée sans licence ADM.

Lors de l'extraction de licences à partir d'une bande passante et/ou d'un pool d'instances, le facteur de forme Citrix ADC et le numéro de modèle matériel sur une plate-forme matérielle à capacité nulle déterminent :

- La bande passante minimale et le nombre d'instances qu'un Citrix ADC doit extraire avant d'être fonctionnel.
- Bande passante maximale et nombre d'instances qu'un Citrix ADC peut extraire.
- Unité de bande passante minimale pour chaque extraction de bande passante. L'unité de bande passante minimale est la plus petite unité de bande passante qu'un Citrix ADC doit extraire d'un pool. Toute extraction doit être un multiple entier de l'unité de bande passante minimale. Par exemple, si l'unité de bande passante minimale d'un Citrix ADC est de 1 Gbit/s, 100 Gbit/s peuvent être récupérés, mais 200 Mbit/s ou 150,5 Gbit/s ne peuvent pas être récupérés. L'unité de bande passante minimale est différente de la bande passante minimale requise. Un Citrix ADC ne peut fonctionner qu'après avoir obtenu une licence avec au moins la bande passante minimale. Une fois la bande passante minimale atteinte, l'instance peut récupérer la bande passante supplémentaire avec l'unité de bande passante minimale.

Les tableaux suivants récapitule la bande passante/instances maximale, la bande passante/instances minimale et l'unité de bande passante minimale pour toutes les plates-formes Citrix ADC prises en charge :

Pour les modèles Citrix ADC MPX

Unité de bande passante/de bande passante d'instance	MPX-8900Z	MPX-14000Z	MPX-14000Z-40G	MPX-15000Z	MPX-15000Z-50G	MPX-25000Z-40G	MPX-26000Z	MPX-26000Z-50S	MPX-26000Z-100G
Bande passante maximale (Gbit/s)	33	100	100	100	100	200	200	200	200
Bande passante minimale (Gbit/s)	5	20	20	20	20	100	100	100	100
Instance minimales	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.
Nombre maximal d'instances	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.	S.O.

Unité de bande pas-sante/de bande pas-sante d'instance	MPX-8900Z	MPX-14000Z	MPX-14000Z-40G	MPX-15000Z	MPX-15000Z-50G	MPX-25000Z-40G	MPX-26000Z	MPX-26000Z-50S	MPX-26000Z-100G
Unité de bande pas-sante mini-male	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s	1 Gbit/s

Pour les modèles Citrix ADC SDX

Unité de bande pas-sante/de bande passante d'instance	SDX-8900Z	SDX-14000Z	SDX-14000Z-40G	SDX-15000Z-50G	SDX-25000Z-40G	SDX-26000Z-100G
Bande passante maximale (Gbit/s)	33	100	100	100	200	200
Bande passante minimale (Gbit/s)	5	20	20	20	100	100
Instances minimales	2.	5	5	5	20	20

Unité de bande pas-sante/de bande passante d'instance	SDX-8900Z	SDX-14000Z	SDX-14000Z-40G	SDX-15000Z-50G	SDX-25000Z-40G	SDX-26000Z-100G
Nombre maximal d'instances	7	25	25	25	115	115
Unité de bande passante minimale	1 Gbit/s	1 Gbit/s	1 Gbit/s			1 Gbit/s

Pour les modèles Citrix ADC CPX

Unité de bande passante/de bande passante d'instance	CPX
Bande passante maximale (Gbit/s)	1
Bande passante minimale (Gbit/s)	S.O.
Instances minimales	1
Nombre maximal d'instances	S.O.
Unité de bande passante minimale	S.O.

Pour Citrix ADC VPX sur les hyperviseurs et les services cloud

Unité de bande pas-sante/de bande passante d'instance	Citrix XenServer	VMware ESXi	KVM Linux	Microsoft Hyper-V	AWS	AZURE
Bande passante maximale (Gbit/s)	40 Gbit/s	100 Gbit/s	100 Gbit/s	3 Gbit/s	5 Gbit/s	3 Gbit/s
Bande passante minimale (Gbit/s)	10 Mbit/s	10 Mbit/s	10 Mbit/s	10 Mbit/s	10 Mbit/s	10 Mbit/s
Instances minimales	1	1	1	1	1	1
Nombre maximal d'instances	1	1	1	1	1	1
Unité de bande passante minimale	10 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s	10 Gbit/s

L'exigence de licence pour différents facteurs de forme

Exigence de licence	MPX	SDX	VPX	CPX
Achat de matériel à capacité nulle	X	X		
Abonnement à la bande passante et à l'édition	X	X	X	
Abonnement à l'instance		X	X	X

Pour plus d'informations sur les plates-formes prises en charge, la bande passante/instances minimale prise en charge, la bande passante/instances maximale prise en charge et l'unité de bande passante minimale pour les plates-formes prises en charge, reportez-vous à la section Bande passante et informations d'instance pour MPX/CPX/VPX.

Configuration de la capacité groupée Citrix ADC

La capacité groupée permet aux utilisateurs de :

- Allocation des licences dans le pool de licences à Citrix ADC à la demande.
- Téléchargez les fichiers de licence de capacité regroupés (Pool de bande passante ou Pool d'instance) vers ADM.
- Allocation des licences de Citrix ADM en fonction de la capacité minimale et maximale de l'instance.

Citrix Application Delivery Management (ADM)

Les utilisateurs peuvent configurer Citrix ADM en tant que serveur de licences pour la capacité groupée Citrix ADC. Il existe deux façons pour une instance Citrix ADC d'obtenir des licences de bande passante et/ou d'instance :

- La première demande d'extraction de licence doit être lancée à partir de Citrix ADC (SDX/MPX/VPX) pour obtenir sa bande passante et/ou ses licences d'instance.
- Les utilisateurs peuvent initier la récupération de licence à partir de Citrix ADC ou Citrix ADM ultérieurement.

> Remarque :
>
> La capacité groupée est affichée sur Citrix ADM uniquement si des licences groupées sont ajoutées à Citrix ADM.

État du pool de licences Citrix ADM

- **Attribué :** l'état de la licence est correct.
- **Grace :**l'instance de Citrix ADC est dans la période de grâce de licence pendant 30 jours.
- **Synchronisation en cours :** Citrix ADM récupère les informations de Citrix ADC à intervalles de 2 minutes.
- **Synchronisation en cours :** la synchronisation des licences entre Citrix ADM et Citrix ADC peut prendre jusqu'à 15 minutes. Citrix ADM peut avoir redémarré ou le basculement ADM HAS est déclenché.

- **Partiellement alloué :** Citrix ADC ne peut pas accepter la capacité allouée car elle peut être exécutée à son allocation maximale. Par exemple, Citrix ADC fonctionne avec une capacité de pool de licences de 10 Gbit/s. Lorsque l'ADC redémarre, les 10 Gbit/s sont consignés sur le serveur de licences ADM. Lorsque Citrix ADC revient en ligne, il essaie de récupérer automatiquement les 10 Gbit/s alloués précédemment. Pendant ce temps, d'autres ADC peuvent avoir extrait cette bande passante. **Partiellement alloué** apparaît si le pool de licences ne dispose pas d'une capacité suffisante pour allouer 10 Gbit/s ou même une capacité partielle à cet ADC.
- **Non géré :** Citrix ADC n'est pas ajouté à ADM pour faciliter la gestion. Cela n'a pas d'impact sur les licences Citrix ADC, mais cela peut avoir un impact sur la surveillance des licences d'ADM.
- **Connexion perdue :** Citrix ADC n'est pas accessible à partir d'ADM pour la gestion. Par exemple, il existe des problèmes de connectivité réseau, NITRO ne fonctionne pas ou des incohérences de mot de passe Citrix ADC. Si NITRO ne fonctionne pas ou si le mot de passe de Citrix ADC ne correspond pas, cela n'a pas d'impact sur les licences Citrix ADC. Cependant, cela peut avoir un impact sur la surveillance des licences d'ADM.
- **Alloué : non appliqué sur l'ADC :** Citrix ADC peut nécessiter un redémarrage si la licence est récupérée ou archivée à partir de l'ADC, mais Citrix ADC n'a pas encore redémarré.
- **Non alloué :**la licence n'est pas allouée dans l'instance de l'ADC.

Pool de licences Citrix ADM : Problèmes courants

- ADC affiche le serveur de licences comme **inaccessible** :
  - La connexion au serveur de licences (ADM ou ADM Service Agent) a été interrompue pendant plus de 15 minutes.
  - L'ADC est en mode Grace.
- ADC affiche l'état du serveur de licences comme étant **accessible** , mais la tentative de l'utilisateur de modifier l'allocation n'a aucun effet :
  - La connexion au serveur de licences a récemment cessé, mais ADC n'a toujours pas manqué le second rythme cardiaque. Par conséquent, il n'est pas dans Grace (encore).
  - Appuyez sur « Modifier l'allocation » renvoie 0 0, cela peut faire apparaître que la capacité configurée a été perdue.
- ADC affiche le nombre de capacités/instances mais le serveur de licences est **accessible ou inaccessible** :
  - La connexion au serveur de licences a été restaurée, mais ADC manque toujours le deuxième battement de cœur/ou envoyer la sonde Re-Connect.
  - Appuyez sur **Modifier l'allocation** renvoie certains nombres mais ne tient pas compte de la capacité configurée.

- ADC indique **Impossible de se connecter au serveur de licences** lors de la configuration des licences groupées avec le service ADM :
  - Vérifiez les règles de pare-feu : 27000 et 7279.
  - L'agent n'est pas enregistré ou ADM Service n'a pas de fichiers de licence téléchargés (ou il a les mauvais fichiers).

Cas d'utilisation : rapport d'utilisation du pool de licences Citrix ADM

Les rapports d'utilisation du pool de licences Citrix ADM identifient les pics mensuels pour lesquels les clients peuvent planifier l'augmentation de l'utilisation des licences et planifier le prochain achat du pool de licences.

- Sondage :
  - Les données de licence sont interrogées à partir d'ADC toutes les 15 minutes.
- Maintenir uniquement les pics par heure :
  - Les exigences maximales d'utilisation de la licence en une heure seront stockées par appareil.
- Rapports :
  - Les rapports d'interface graphique à générer indiquent l'utilisation par périphérique pour une plage de temps spécifiée.
- Exporter :
  - Possibilité d'exporter les données de mesure au format CSV ou XLS pour une plage de temps spécifiée.
- Purger :
  - Les tâches de purge seront exécutées le 1er de chaque mois à 12 h 10.
  - La période de purge est configurable (la période par défaut est de 2 mois).

Pour installer des fichiers de licence sur Citrix Application Delivery Management (ADM)

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM. Par exemple, `http://192.168.100.1` .
2. Dans le champ **Nom d'utilisateur et Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration** , accédez à **Réseaux > Licences > Paramètres** , puis cliquez sur **Ajouter une nouvelle licence** .

4. Dans la section **Fichiers de licence**, sélectionnez l'une des options suivantes :

   - Télécharger des fichiers de licence à partir d'un ordinateur local - Si un fichier de licence est déjà présent sur l'ordinateur local de l'utilisateur, l'utilisateur peut le télécharger sur Citrix ADM. Pour ajouter des fichiers de licence, l'utilisateur peut cliquer sur **Parcourir** pour sélectionner le fichier de licence (.lic). Cliquez ensuite sur **Terminé**.

     > Remarque :
     >
     > Si les fichiers de licence téléchargés n'ajoutent pas les licences dans la capacité Citrix ADC Pooled, vous pouvez sélectionner les fichiers de licence et cliquer sur **Appliquer les licences** pour ajouter les licences au pool.

   - Utiliser le code d'accès de licence - Citrix envoie par e-mail le code d'accès de licence (LAC) pour les licences achetées par les clients. Pour ajouter des fichiers de licence, entrez le **LAC** dans la zone de texte, puis cliquez sur **Obtenir des licences** .

     > Remarque :
     >
     > À tout moment, les utilisateurs peuvent ajouter d'autres licences à Citrix ADM à partir des paramètres de licence.

Pour allouer des licences de capacité groupée Citrix ADC à partir de Citrix ADM

Prérequis : Avant que les utilisateurs puissent gérer leurs licences de pool d'instances via Citrix ADM, ils doivent enregistrer l'instance de Citrix ADC auprès de Citrix ADM. Dans l'interface graphique de Citrix ADC, accédez à **Système > Licences > Gérer les licences** et activez la case à cocher **Enregistrer auprès de Citrix ADM pour la gérabilité** lors de l'ajout de Citrix ADM IP.

> Remarque :
>
> Si les utilisateurs n'ont pas enregistré l'instance de Citrix ADC auprès de Citrix ADM, ils peuvent extraire des licences de Citrix ADM. Toutefois, ils ne peuvent pas allouer à partir de Citrix ADM à l'instance Citrix ADC avec capacité mise en commun.
>
> Dans les champs **Nom d'utilisateur et Mot de passe** , entrez les informations d'identification Citrix ADM.
>
> Cette option ne fonctionne pas si le mot de passe Citrix ADC (SDX/MPX/VPX) n'est pas par défaut.

Une fois l'instance enregistrée auprès du serveur de licences, allouez les licences comme suit

1. Dans un navigateur Web, tapez l'adresse IP de Citrix ADM. Par exemple, `http://192.168.100.1` .
2. Dans le champ **Nom d'utilisateur et Mot de passe**, entrez les informations d'identification de l'administrateur.

3. Sous l'onglet **Configuration** , accédez à **Réseaux > Licences > Capacité groupée** .
4. Cliquez sur le pool de licences à gérer.
5. Sélectionnez une instance Citrix ADC dans la liste des instances disponibles en cliquant sur le bouton **>** .
6. Si les utilisateurs souhaitent modifier ou libérer une allocation de licence, cliquez sur **Modifier l'allocation** ou **Release allocation** .
7. Si les utilisateurs cliquent sur **Modifier l'allocation**, une fenêtre contextuelle contenant les licences disponibles dans le serveur de licences apparaît.
8. Les utilisateurs peuvent choisir la bande passante ou l'allocation d'instance pour l'instance Citrix ADC en définissant les options déroulantes **Allocation** . Après avoir effectué les sélections souhaitées, cliquez sur **Allouer**.
9. Les utilisateurs peuvent également modifier l'édition de la licence allouée à partir des options déroulantes de la fenêtre **Modifier l'allocation de licence** .

Citrix ADM avec pool de licences Haute disponibilité (HA)

Auparavant, les licences de pool de licences étaient verrouillées par nœud et associées à l'ID d'hôte du nœud principal ADM. Chaque fois que le basculement se produisait sur le nœud secondaire, Citrix ADC passait en une période de grâce de 30 jours pour éviter toute interruption due à un événement ADM inaccessible. Cela a permis à Citrix ADC de s'exécuter pendant 30 jours même si Citrix ADM n'était pas accessible. Toutefois, les nouvelles instances de Citrix ADC ne seraient pas en mesure d'extraire des licences du serveur de licences ADM si elle n'était pas accessible, ce qui signifie qu'il n'y a pas eu de nouvelles sorties de licence pendant la période de grâce de 30 jours. Les clients devaient générer un réplica du fichier de licence à partir du système de licences Citrix pour que cette licence fonctionne si le nœud principal ne revenait pas et que 30 jours étaient passés, ce qui signifiait qu'ils généraient de nouveaux fichiers de licence.

Solution

Avec la solution HA Pool de licences, les clients n'ont pas à générer de nouveaux fichiers de licence avec basculement ADM vers le nœud secondaire si le nœud principal ne revient pas. La nouvelle récupération de licence continue de fonctionner après basculement. Les licences de pool de licences et les licences ADM sont désormais associées à un identifiant d'hôte virtuel partagé entre les nœuds principaux et secondaires Citrix ADM.

ID d'hôte virtuel

Les nœuds principaux et secondaires Citrix ADM partagent le même identifiant d'hôte virtuel. L'identifiant d'hôte réel du nœud principal ou du premier serveur Citrix ADM dans le déploiement HA est utilisé comme identifiant d'hôte virtuel. L'ID d'hôte virtuel est généré automatiquement dans le déploiement d'ADM, et il est stocké dans la base de données ADM au format chiffré et ne peut pas être modifié par le client. L'identifiant d'hôte virtuel a la préférence sur l'identifiant d'hôte réel. Les fichiers de licence sont synchronisés à partir du nœud principal ADM vers le nœud secondaire. Citrix ADC vérifie les licences à l'aide de l'adresse IP flottante ADM. Lors du basculement entre le nœud principal et le nœud secondaire, les fichiers de licence et l'identifiant d'hôte virtuel sont synchronisés du nœud principal vers le nœud secondaire avec l'adresse IP flottante.

Comportement de rupture de HA

Si les clients lancent l'action HA de rupture ADM, les deux nœuds ADM conservent l'ID d'hôte virtuel, puis lancent le workflow HA de rupture. Le nœud 1 et le nœud 2 peuvent continuer à extraire les licences. Citrix ADC existant entre dans un délai de grâce de 30 jours puisque l'adresse IP flottante est supprimée de l'ADM.

Split Brain

Citrix ADM surveille la disponibilité des nœuds ADM HA en envoyant des battements cardiaques à intervalles réguliers. Si les battements cardiaques n'atteignent pas l'autre nœud en raison de problèmes de réseau, les deux nœuds ADM se promènent en tant que principal ADM. Le serveur de licences s'exécute sur les deux nœuds dans ce scénario. Citrix ADC peut extraire les licences des deux nœuds à l'aide de l'IP du nœud de serveur ADM puisque les deux partagent le même identifiant d'hôte virtuel. Le nœud 1 et le nœud 2 sont promus en tant que principal ADM. Le serveur de licences s'exécute sur les deux serveurs avec le même identifiant d'hôte virtuel. La capacité de licence est doublée. Les événements liés au Split Brain Citrix ADM et les événements liés à la période de grâce ADM HA sont générés.

Récupération à partir d'un Split Brain

Citrix ADM peut récupérer à partir d'une situation de Split Brain une fois que l'administrateur du client trouve et résout les problèmes réseau. Le flux de travail pour la récupération à partir d'un Split Brain ADM est le suivant. Une fois le réseau restauré, Citrix ADM détecte automatiquement le nœud ADM 1 en tant que principal ADM. Citrix ADM lance le workflow HA de jointure à partir du nœud ADM 2. Citrix ADM Node 1 Real Host-ID est sélectionné comme identifiant d'hôte virtuel. Citrix ADM est restauré dans le scénario HA normal, et les fichiers de licence et l'ID d'hôte virtuel sont synchronisés avec le nœud ADM 2.

Configuration de la capacité groupée sur MPX-Z

MPX-Z est l'appliance Citrix ADC MPX compatible avec la capacité groupée Citrix ADC MPX. MPX-Z prend en charge le regroupement de bande passante pour les licences Premium, Advanced ou Standard Edition. MPX-Z requiert ses licences de plate-forme avant de pouvoir se connecter au serveur de licences. Les utilisateurs peuvent installer la licence de plate-forme MPX-Z en téléchargeant le fichier de licence à partir d'un ordinateur local ou en utilisant le numéro de série matériel de l'instance, ou le code d'accès de licence de la section **Système > Licences** de l'interface graphique de l'instance Citrix ADC. Si les utilisateurs suppriment la licence de plate-forme MPX-Z, la fonctionnalité de capacité groupée est désactivée et toutes les licences retirées sont archivées sur le serveur de licences.

Les utilisateurs peuvent modifier dynamiquement la bande passante de l'ADC MPX-Z sans redémarrer. Un redémarrage n'est requis que si les utilisateurs souhaitent modifier l'édition de la licence.

> Remarque :
>
> Lorsque les utilisateurs redémarrent Citrix ADC, il vérifie automatiquement les licences groupées requises pour sa capacité configurée.

Configuration de la capacité groupée sur une instance VPX

Une instance Citrix ADC VPX compatible avec la capacité mise en commun peut extraire les licences d'un pool de bande passante (éditions Premium/Advanced/Standard). Les utilisateurs peuvent utiliser l'interface graphique de Citrix ADC pour extraire les licences du serveur de licences.

Les utilisateurs peuvent modifier dynamiquement la bande passante d'une instance VPX sans redémarrer. Un redémarrage n'est requis que si les utilisateurs souhaitent modifier l'édition de la licence.

> Remarque :
>
> Lorsque les utilisateurs redémarrent l'instance, l'instance vérifie automatiquement les licences groupées requises pour sa capacité configurée.

Allocation de licences de pool à l'instance MPX-Z ou VPX

Pour allouer des licences :

1. Dans un navigateur Web, tapez l'adresse IP de l'instance Citrix ADC. Par exemple, `http://192.168.100.1`.
2. Dans les champs **Nom d'utilisateur et Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration** , accédez à **Système > Licences > Gérer les licences** , cliquez sur **Ajouter une nouvelle licence** , puis sélectionnez **Utiliser les licences groupées** .
4. Entrez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.

5. Si les utilisateurs souhaitent gérer les licences de pool de leur instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM pour la gérabilité** et entrez les informations d'identification Citrix ADM.
6. Sélectionnez l'édition de la licence et la bande passante requise, puis cliquez sur **Obtenir les licences**.
7. Les utilisateurs peuvent modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Release allocation**.
8. Si les utilisateurs cliquent sur **Modifier l'allocation**, une fenêtre contextuelle affiche les licences disponibles sur le serveur de licences.

   > Remarque :
   >
   > Un redémarrage n'est pas requis si les utilisateurs modifient l'allocation de bande passante, mais un redémarrage à chaud est requis si les utilisateurs modifient l'édition de la licence.

9. Les utilisateurs peuvent allouer de la bande passante ou des instances à l'instance Citrix ADC à partir de la liste déroulante **Allocation** . Cliquez ensuite sur **Obtenir des licences**.
10. Les utilisateurs peuvent choisir l'édition de licence et la bande passante requise dans les listes déroulantes de la fenêtre contextuelle.

    > Remarque :
    >
    > L'allocation de bande passante doit être un multiple de l'unité de bande passante minimale.

Configuration de la capacité groupée sur SDX-Z

Une instance SDX-Z est une instance mise en commun de Citrix ADC SDX. SDX-Z prend en charge le regroupement de bande passante pour les éditions Premium, Advanced et Standard, ainsi que le regroupement d'instances. Une fois que les utilisateurs ont appliqué la licence de plate-forme SDX-Z, le service de gestion fournit des options pour récupérer les licences depuis et vers le serveur de licences, et pour allouer la capacité de bande passante aux instances Citrix ADC exécutées sur la plate-forme SDX-Z.

> Remarque :
>
> Les instances Citrix ADC VPX exécutées sur SDX-Z ne peuvent pas extraire directement les licences depuis ou vers le serveur de licences. Cela peut être fait par le service de gestion dans SDX.

Les utilisateurs peuvent installer la licence de plate-forme SDX-Z soit en téléchargeant le fichier de licence à partir d'un ordinateur local, soit en utilisant le numéro de série matériel de l'instance ou le code d'accès de licence.

Si les utilisateurs suppriment la licence de plate-forme SDX-Z, la fonctionnalité de capacité groupée est désactivée et toutes les licences sont récupérées dans le serveur de licences.

> Remarque :
>
> Si les utilisateurs redémarrent l'instance, l'instance vérifie les licences groupées requises pour sa capacité configurée.

Capacité mise en commun sur SDX

Pool d'instances

Un dispositif SDX peut provisionner le même nombre d'instances disponibles dans le pool d'instances du dispositif SDX.

Pool de bande passante

Pendant le provisioning d'instance Citrix ADC, la bande passante est allouée à l'instance. Les utilisateurs peuvent sélectionner l'édition et la bande passante requise pour provisionner une instance Virtual Citrix ADC. Le service de gestion permet de continuer le provisioning uniquement si l'instance dispose d'une bande passante suffisante pour l'édition demandée. Les utilisateurs sont avertis si la bande passante est insuffisante.

> Remarque :
>
> La modification de la bande passante ne nécessite pas le redémarrage d'une instance.

Allocation de licences de pool à l'instance SDX-Z

Pour allouer des licences :

1. Dans un navigateur Web, tapez l'adresse IP de l'instance Citrix ADC SDX-Z. Par exemple, `http://192.168.100.1`.
2. Dans les champs **Nom d'utilisateur et Mot de passe**, entrez les informations d'identification de l'administrateur.
3. Sous l'onglet **Configuration** , accédez à **Système > Licences** et accédez à **Capacité groupée** .
4. Entrez les détails du serveur de licences dans le champ **Nom du serveur/Adresse IP**.
5. Si les utilisateurs souhaitent gérer les licences de pool de leur instance via Citrix ADM, activez la case à cocher **Enregistrer auprès de Citrix ADM pour la gérabilité** et entrez les informations d'identification Citrix ADM.
6. Les utilisateurs peuvent modifier ou libérer l'allocation de licence en sélectionnant **Modifier l'allocation** ou **Release allocation**.

> Remarque :
>
> Les licences récupérées sont stockées dans un pool séparé par le service de gestion.

7. Pour modifier l'allocation de licence pour une instance VPX spécifique dans l'instance SDX-Z, sélectionnez l'instance dans la section **Instances** , puis cliquez sur **Modifier l'allocation** . Une nouvelle fenêtre affiche les licences disponibles.
8. Les utilisateurs peuvent modifier l'édition de bande passante de l'instance à partir de la liste déroulante **Licence de fonctionnalité** et la bande passante requise dans le champ **Débit (mbps)** . Cliquez ensuite sur **Terminé**.

> Remarque :
>
> L'allocation de bande passante doit être un multiple entier de l'unité de bande passante minimale du facteur de forme correspondant.

Configuration de la capacité groupée sur une instance CPX

Lors du provisioning de l'instance Citrix ADC CPX, les utilisateurs peuvent configurer l'instance Citrix ADC CPX pour utiliser Citrix ADC Pooled Capacity. Dans le docker, les utilisateurs doivent fournir les détails Citrix ADC Licensing Server (Citrix ADM). L'instance CPX de Citrix ADC extraire les licences du pool d'instances.

> Remarque :
>
> Par défaut, l'instance Citrix ADC CPX extraire une licence d'instance du pool d'instances et le débit est automatiquement défini sur 1 000 Mbps. Les utilisateurs ne peuvent pas modifier la bande passante de 1 000 Mbps allouée à l'instance.

Les utilisateurs peuvent télécharger Citrix ADC CPX à partir de l'App Store Docker. Sur l'hôte Docker, pour télécharger Citrix ADC CPX, exécutez la commande suivante :

```
docker pull store/citrix/netscalercpx:[version number]
```

Pour configurer la capacité groupée lors du provisioning de l'instance CPX Citrix ADC :

Lors du provisioning d'une instance Citrix ADC CPX, définissez Citrix ADC Licensing Server (Citrix ADM) en tant que variable d'environnement dans l'hôte docker, puis exécutez la commande comme indiqué ci-dessous :

```
docker run -dt -P -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT> --name <
container_name> --ulimit core=-1 -e EULA=yes -v <host_dir>:/cpx --cap-add=
NET_ADMIN >REPOSITORY<:>TAG<
```

Où :

- <LS_IPADDRESS> est l'adresse IP du serveur de licences Citrix ADC (Citrix ADM).

- <LS_PORT> est le port du serveur de licences Citrix ADC. Par défaut, le port est 27000.

Meilleures pratiques, cas de coin et FAQ

Mise à niveau de la licence SDX - perpétuelle vers mise en commun

Lorsque la licence sur un SDX est mise à niveau de licence perpétuelle vers une licence groupée, le SDX ne nécessite pas de redémarrage. Ni le SDX ni le VPX ne nécessitent un redémarrage pour passer à une licence groupée. La SVM fait automatiquement la transition d'un ou de plusieurs VPX vers des licences groupées.

Pour une transition en douceur, les utilisateurs doivent veiller à ce que les éléments suivants soient les suivants :

- Assurez-vous que le SDX possède la licence de capacité nulle appropriée.
- Assurez-vous que le serveur Citrix ADM dispose d'une capacité suffisante pour les éditions de licence utilisées dans les instances VPX du SDX.
- Assurez-vous que la capacité de bande passante suffisante est retirée de l'ADM dans la SVM pour toutes les instances VPX.
  - Par exemple : si le SDX a 10 instances VPX et qu'ensemble ils consomment 40 Gbit/s Premium et 20 Gbit/s Advanced, assurez-vous que cette option est retirée d'abord via SVM afin que les instances VPX puissent obtenir ces licences.

Opération d'instance de Citrix ADC au cours d'une période de grâce de 30 jours

Si une instance Citrix ADC est déconnectée de Citrix ADM après avoir reçu une licence du pool, elle est autorisée à continuer à fonctionner dans une période de grâce de 30 jours pendant qu'elle tente de rétablir une connexion avec le serveur de licences. Même si le Citrix ADC redémarre, la licence reste dans la période de grâce de 30 jours et l'instance continue de fonctionner.

Enregistrement initié côté client (randomisé) : Scénarios dans lesquels Citrix ADM initie la connexion

Pour l'archivage initié côté client (randomisé), existe-t-il des scénarios dans lesquels Citrix ADM lancerait cette connexion ?

Citrix ADM (serveur de licences) et Citrix ADC (client de licence) échangent des paquets de rythme cardiaque pour surveiller l'intégrité de la connexion établie entre le client et le serveur. Cette période est aléatoire pour éviter que tous les clients Citrix ADC n'envoient des demandes au serveur de licences Citrix ADM en même temps.

En cas de problème avec la connexion de licence entre le client et le serveur, les actions suivantes sont effectuées :

- Si Citrix ADM ne reçoit pas de paquet cardiaque d'un client Citrix ADC, le serveur Citrix ADM revendique les licences allouées à ce serveur Citrix ADC spécifique.
- Si Citrix ADC ne reçoit pas le paquet cardiaque, Citrix ADC passe à une période de grâce de licence de 30 jours.
- Si Citrix ADC reçoit un signal établi de connexion au serveur de licences avec le serveur de licences Citrix ADM, Citrix ADC retire à nouveau la licence de Citrix ADM.

Allocation de bande passante groupée pendant le redémarrage de Citrix ADC

Si la bande passante a été allouée lors d'un redémarrage de Citrix ADC, la licence de bande passante groupée serait-elle partiellement distribuée (jusqu'à la bande passante disponible dans le pool) ou aucune licence ne serait-elle distribuée ?

Citrix ADC tente d'abord de récupérer la capacité groupée configurée par l'utilisateur. Si cette tentative échoue, Citrix ADC tente de récupérer la capacité mise en commun disponible dans Citrix ADM.

> Remarque :
>
> Cette fonctionnalité est uniquement disponible pour MPX et VPX. SDX tente de retirer une licence partielle si Citrix ADM ne dispose pas d'une capacité suffisante.

Alerte de non-concordance de licence (Citrix ADC reçoit une licence partielle ou aucune licence)

En cas d'inadéquation (par exemple, Citrix ADC n'a pas reçu de licence ou n'a reçu qu'une licence partielle), Citrix ADM est-il en mesure d'indiquer cette situation pour la réconciliation ?

En cas de non-concordance de licence où Citrix ADC ne reçoit aucune licence ou une licence partielle, Citrix ADM doit signaler cette situation pour réconciliation. Une inadéquation de licence peut se produire dans les scénarios suivants :

- Si Citrix ADC redémarre, Citrix ADC vérifie à nouveau la licence après le redémarrage. Cela efface l'événement de non-concordance de capacité mise en commun.
- Si Citrix ADM redémarre, Citrix ADC et Citrix ADM synchronisent les informations de licence dans un intervalle de battements cardiaques et cet événement est effacé.
- Si la récupération de Citrix ADC échoue après redémarrage/reconnexion du serveur de licences, il n'y a pas de récupération automatique. L'utilisateur doit récupérer manuellement une licence du pool à nouveau.

Basculement haute disponibilité (HA) de Citrix ADM

Lors du basculement HA de Citrix ADM, comment le fichier de licences se synchronise-t-il et quelles échecs pourraient se produire (comme le certificat SSL sur Citrix ADC ne sont parfois pas copiés vers un nœud secondaire lors de la mise à jour sur le nœud principal) ?

La prise en charge de Citrix ADM High Availability (HA) pour les licences groupées est disponible à partir de la version 12.1-50.x du logiciel. Citrix ADM synchronise périodiquement les fichiers téléchargés dans le Citrix ADM principal vers le Citrix ADM secondaire. Par conséquent, une synchronisation de fichiers est effectuée avant que l'événement de basculement HA ne se produise. Par conséquent, les échecs de synchronisation des fichiers ne sont pas susceptibles de se produire. Par exemple, le certificat SSL sur Citrix ADC qui a été mis à jour sur le Citrix ADM principal et qui n'a pas été copié dans le Citrix ADM secondaire.

Vérifications de l'état d'intégrité de la base de données Citrix ADM secondaire

Y a-t-il des vérifications de l'état d'intégrité en place pour les problèmes de base de données secondaires ? Le Citrix ADM secondaire vérifie-t-il que les informations partagées sont saines pour éviter de répliquer des informations malsaines ?

Les informations de licence sont conservées dans la mémoire du serveur de licences (dans Citrix ADM). Ces informations ne sont pas synchronisées avec Citrix ADM secondaire. Toutes les extractions de licences sont effectuées par rapport aux informations en mémoire du serveur de licences. La base de données Citrix ADM est utilisée uniquement pour stocker les rapports collectés à partir du serveur de licences (dans Citrix ADM) et de l'instance Citrix ADC.

Citrix ADM synchronise uniquement les fichiers de licence de Citrix ADM principal vers secondaire (à partir de la version 12.1-50.x du logiciel).

Pendant le basculement de Citrix ADM HA, Citrix ADC vérifie les licences d'ADM après que l'intervalle de battement de cœur et que la mémoire du serveur de licences est mise à jour après l'intervalle de battement de cœur.

Délai de grâce inversé pour indisponibilité de licence

Existe-t-il un délai de grâce inversé pour l'indisponibilité de la licence qui permettrait à l'instance de rester sous licence pendant une période de grâce plutôt qu'une fermeture immédiate ? Par exemple, Citrix ADC tente d'archiver et Citrix ADM indique qu'aucune licence valide n'est disponible.

Une solution à ce problème particulier est en cours d'étude. Nous informerons les utilisateurs lorsque nous aurons une solution proposée à ce problème.

ID système configurable pour les licences sur Citrix ADM

Existe-t-il une prise en charge d'un ID système configurable (par opposition à un système basé sur l'adresse MAC) à utiliser pour les licences sur Citrix ADM ?

La prise en charge d'un ID système configurable pour les licences n'est pas actuellement prévue.

Contrôles ou mécanismes de cohérence des fichiers

Pour les fichiers, y compris les licences qui sont répliquées de Citrix ADM principal vers secondaire, existe-t-il des vérifications de cohérence/corruption ou des mécanismes en place pour s'assurer que la corruption DB principale ne réplique pas le problème vers le secondaire ?

Citrix ADM gère les fichiers de licence dans le système de fichiers et synchronisés à l'aide de l'utilitaire RSYNC. Par conséquent, les problèmes de base de données n'ont pas d'impact sur les fichiers de licence.

Utilisation de l'agent Citrix ADM pour l'archivage/retrait des licences

> Remarque :
>
> Actuellement, un seul agent par locataire donné est pris en charge pour la capacité groupée dans les clouds publics.

Licences en rafale

La licence d'éclatement est une amélioration de la capacité mise en commun en y ajoutant un élément de consommation. Il se peut que les clients ne soient pas en mesure de prévoir leurs besoins en bande passante avec précision. Cela peut se produire pour diverses raisons ou circonstances particulières, comme une fusion ou une acquisition ou des événements spéciaux tels que les ventes Black Friday, qui peuvent entraîner une augmentation du trafic et dépasser la capacité actuelle d'un client. En général, l'industrie s'oriente vers un modèle de consommation (payant à ce que vous utilisez) basé sur de nombreuses offres cloud.

La licence d'éclatement pour la capacité groupée permet aux clients d'acheter la capacité groupée en tant qu'abonnement de base et d'avoir la possibilité de surpasser la capacité groupée achetée en cas de besoin. Pour le pool d'abonnement de base, les clients doivent payer à l'avance pour la durée de la période d'abonnement (1, 3 ou 5 ans). Pour la piscine de rafale, les clients peuvent consommer sans payer à l'avance et seront facturés en fonction de l'utilisation réelle chaque année après la consommation.

Avec la licence de rafale, Citrix ADC verra un pool, une vue combinée du pool de base et du pool de rafale. Si Citrix ADC ne parvient pas à quitter le pool de base, il essaiera de quitter le pool de rafale.

Rapport de licence de rafale dans ADM

Des rapports d'utilisation des licences seront générés pour la base et le pool de rafale. Des rapports mensuels sur l'utilisation des licences seront générés pour indiquer l'utilisation maximale des licences par heure dans un pool de licences. L'intervalle de purge pour ces rapports mensuels est une limite maximale de trois ans. Des rapports annuels sur l'utilisation des licences seront générés pour indiquer l'utilisation maximale des licences par mois dans un pool de licences. L'intervalle de purge pour ces rapports annuels est une limite maximale de six ans. Les clients auront la possibilité d'exporter des données de mesure au format CSV, XLS et PDF pour une plage de temps spécifiée.

Licences groupées BLX

BLX utilise le même pool de licences que Citrix ADC VPX.

Vue d'ensemble de la licence de CPU virtuelle

Les datacenters optent pour des technologies plus récentes qui simplifient les fonctions du réseau tout en offrant des coûts réduits et une plus grande évolutivité. Une architecture de datacenter plus récente doit au moins inclure les fonctionnalités suivantes :

- Mise en réseau définie par logiciel (SDN).
- Virtualisation des fonctions réseau (NFV).
- Virtualisation réseau (NV).
- Micro-services.

Un tel mouvement exige également que les exigences logicielles soient dynamiques, flexibles et agiles pour répondre aux besoins de l'entreprise en constante évolution. Les licences devraient également être gérées par un outil de gestion centralisé offrant une visibilité complète de l'utilisation.

Auparavant, les licences Citrix SW ADC étaient allouées en fonction de la consommation de bande passante par les instances. Un Citrix SW ADC a été limité à utiliser une bande passante spécifique et d'autres mesures de performances basées sur l'édition de licence (Standard, Advanced ou Premium) à laquelle il était lié. Pour augmenter la bande passante disponible, les utilisateurs ont dû effectuer une mise à niveau vers une édition de licence offrant plus de bande passante. Dans certains scénarios, l'exigence de bande passante peut être moindre, mais l'exigence était plus importante pour d'autres performances L7 telles que SSL TPS, débit de compression, etc. La mise à niveau de la licence Citrix SW ADC peut ne pas convenir dans de tels cas. Toutefois, les utilisateurs peuvent avoir à acheter une licence avec une large bande passante pour déverrouiller les ressources système requises pour un traitement intensif en CPU. Citrix SW ADM prend désormais en charge l'allocation de licences en fonction du nombre de CPU virtuel (vCPU).

Avec la fonctionnalité de licence basée sur VCPU, la licence spécifie le nombre de vCPU auxquels un Citrix SW ADC VPX particulier a droit. Le Citrix SW ADC VPX peut retirer des licences dynamiquement à par-

tir du serveur de licences uniquement pour le nombre de vCPU sur lesquels le SW ADC peut s'exécuter. Les licences vCPU prennent en charge tous les facteurs de forme SW ADC, y compris VPX, CPX et BLX.

À l'instar de la capacité de licence groupée et des fonctionnalités de licence CICO (Check-in, Check-out), le serveur de licences Citrix SW ADM gère un ensemble distinct de licences vCPU. Ici aussi, les trois éditions gérées pour les licences vCPU sont standard, avancées et premium. Ces éditions déverrouillent les mêmes ensembles de fonctionnalités que celles déverrouillées par les éditions pour les licences de bande passante.

Il peut y avoir un changement dans le nombre de vCPU ou lorsqu'il y a un changement dans l'édition de la licence. Dans ce cas, les utilisateurs doivent toujours arrêter l'instance avant de lancer une demande pour un nouvel ensemble de licences. Les utilisateurs doivent redémarrer le Citrix SW ADC après avoir vérifié les licences.

Configurer le serveur de licences dans Citrix SW ADC VPX à l'aide de l'interface graphique :

1. Dans Citrix SW ADC VPX, accédez à **Système** > **Licences** et cliquez sur **Gérer les licences** .
2. Sur la page Licence, cliquez sur **Ajouter une nouvelle licence**.
3. Dans la page Licences, sélectionnez l'option **Utiliser les licences à distance** .
4. Sélectionnez **Licences CPU** dans la liste Mode de licence à distance.
5. Tapez l'adresse IP du serveur de licences et le numéro de port.
6. Cliquez sur **Continuer**.

   > **Remarque :** les utilisateurs doivent toujours enregistrer les instances Citrix SW ADC VPX avec Citrix SW ADM. Si ce n'est pas déjà fait, activez Enregistrer auprès de Citrix SW ADM et tapez les informations d'identification de connexion Citrix ADM.

7. Dans la fenêtre Allouer des licences, sélectionnez le type de licence. La fenêtre affiche le total et les vCPU disponibles ainsi que les CPU pouvant être alloués. Cliquez sur **Obtenir les licences**.
8. Cliquez sur **Redémarrer** sur la page suivante pour demander les licences.

> **Remarque :** Les utilisateurs peuvent également libérer la licence actuelle et vérifier à partir d'une autre édition. Par exemple, les utilisateurs exécutent déjà une licence d'édition Standard sur leur instance. Ils peuvent libérer cette licence, puis vérifier à partir de Advanced Edition.
> **Remarque :** Les utilisateurs doivent s'assurer que la quantité de mémoire correcte (2 Go) est attribuée par vCPU. Vérifiez la mémoire par allocation vCPU. Si elles ne sont pas correctes, augmentez la mémoire et redémarrez l'instance Citrix SW ADC VPX.

Configurer le serveur de licences dans Citrix SW ADC VPX à l'aide de l'interface de ligne de commande :

Dans la console Citrix SW ADC VPX, tapez les commandes suivantes pour les deux tâches suivantes :

1. Pour ajouter le serveur de licences à Citrix SW ADC VPX :
   - Tapez l'adresse IP du serveur de licences. Par exemple, http://192.168.100.1.
2. Pour demander les licences :
   - set capacity -vcpu - edition platinum
   - Lorsque vous y êtes invité, redémarrez l'instance en tapant la commande suivante : **reboot -w**

Gestion des licences vCPU sur Citrix SW ADM

1. Dans Citrix SW ADM, accédez à **Réseaux** > **Licences > LicencesCPU virtuelles** .
2. La page affiche les licences allouées pour chaque type d'édition de licence.
3. Cliquez sur le numéro de chaque donut (Standard, Advanced, Premium) pour afficher les instances de Citrix SW ADC qui utilisent cette licence.

Licences vCPU pour Citrix SW ADC CPX

Lors du Provisioning de l'instance Citrix SW ADC CPX, les utilisateurs peuvent configurer l'instance Citrix SW ADC CPX pour récupérer les licences du serveur de licences en fonction de l'utilisation du processeur dans l'instance.

Citrix SW ADC CPX s'appuie sur le serveur de licences, exécuté sur Citrix SW ADM, pour gérer les licences. Citrix SW ADC CPX vérifie les licences du serveur de licences lors du démarrage. Les licences sont réarchivées sur le serveur de licences lorsque Citrix SW ADC CPX s'arrête.

Les utilisateurs peuvent télécharger Citrix SW ADC CPX depuis le Docker App Store. Sur l'hôte Docker, pour télécharger Citrix SW ADC CPX, exécutez la commande suivante :

- `docker pull store/citrix/netscalercpx:[version number]`

Il existe trois types de licences disponibles pour les licences CPX :

1. Licences d'abonnement CPU virtuelles prises en charge pour CPX et VPX
2. Licences de capacité groupée
3. Licences CP1000 qui prennent en charge des vCPU uniques à multiples pour CPX uniquement

Pour configurer les licences d'abonnement vCPU lors du Provisioning de l'instance CPX SW ADC Citrix :

Les utilisateurs doivent spécifier le nombre de licences vCPU utilisées par l'instance Citrix ADC CPX.

- Cette valeur est entrée en tant que variable d'environnement via Docker, Kubernetes ou Mesos/-Marathon.
- La variable cible est **« CPX_CORES »** Le CPX peut prendre en charge de 1 à 7 cœurs.

Pour spécifier 2 cœurs, les utilisateurs peuvent exécuter la commande docker run comme suit :

- `docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2`

Lors du Provisioning d'une instance Citrix ADC CPX, définissez Citrix SW ADC Licensing Server en tant que variable d'environnement dans la commande docker run, comme indiqué ci-dessous :

- `docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT > cpx:11.1`

où,

- <LS_IP_ADDRESS>est l'adresse IP du serveur Citrix ADC Licensing Server.
- <LS_PORT> est le port du serveur de licences Citrix ADC. Par défaut, le port est 27000.

> **Remarque :** Par défaut, l'instance Citrix SW ADC CPX vérifie la licence du pool d'abonnement vCPU. L'instance CPX vérifie le nombre « n » de licences si l'instance est exécutée avec « n » processeurs.

Pour configurer Citrix SW ADC Pooled Capacity ou des licences CP1000 lors du provisioning de l'instance Citrix SW ADC CPX :

Si les utilisateurs souhaitent récupérer des licences pour l'instance CPX à l'aide de la licence groupée (basée sur la bande passante) ou du pool privé CPX (CP1000 ou sur le pool privé), les utilisateurs doivent fournir les variables d'environnement en conséquence.

Par exemple,

- `docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT > -e PLATFORM=CP1000 cpx:11.1`

CP1000. Cette commande déclenche l'extraction à partir du pool CP1000 (pool privé CPX). L'instance CPX de Citrix SW ADC récupère alors le nombre « n » d'instances pour le nombre « n » de cœurs spécifié pour CPX_CORES. Le cas d'utilisation le plus courant est de spécifier n = 1 pour une extraction d'une instance unique. Les cas d'utilisation CPX multicœur vérifient les vCPU « n » (où « n » est de 1 à 7).

- `docker run -dt -P --privileged=true --ulimit core=-1 -v<host_dir>:/cpx -e EULA=yes -e CPX_CORES=2 -e LS_IP=<LS_IP_ADDRESS> -e LS_PORT=<LS_PORT > -e BANDWIDTH=2000 cpx:11.1`

Capacité mise en commun. Cette commande vérifie une licence du pool d'instances et consomme 1000 Mbit/s de bande passante du pool de bande passante platine tout en permettant à CPX de s'exécuter jusqu'à 2000 Mbit/s. Dans les licences groupées, les 1000 premiers Mbps ne sont pas facturés.

> **Remarque :** indiquez le nombre de vCPU correspondant à la bande passante cible souhaitée lors de l'extraction du pool de bande passante, comme indiqué dans le tableau suivant :

Nombre de cœurs (vCPU)	Bande passante maximale
1	1000 Mbit/s
2.	2000 Mbit/s
3	3500 Mbit/s
4	5000 Mbit/s
5	6500 Mbit/s
6	8000 Mbit/s
7	9300 Mbit/s

Présentation de Citrix ADM Service Pooled Licensing

Les licences groupées Citrix ADM Service sont une fonctionnalité de Citrix ADM Service. Les licences groupées Citrix ADM Service permettent aux clients d'utiliser des licences groupées avec ADM Service. Avec les licences groupées d'ADM Service, les utilisateurs sont en mesure de gérer les allocations de licences sur plusieurs ADC répartis sur plusieurs centres de données. Les licences groupées Citrix ADM Service prennent en charge plusieurs agents par centre de données. Les licences sont gérées par le Service des SMA dans son ensemble et non par un seul agent. Ainsi, les utilisateurs devraient considérer un agent comme un proxy réseau vers un serveur de licences basé sur le cloud. Les licences groupées Citrix ADM Service prennent également en charge les codes d'accès aux licences pour récupérer les licences à partir du portail Citrix. Citrix ADM Service fournit un tableau de bord qui aide les utilisateurs à gérer l'allocation de capacité et à afficher l'utilisation des licences.

Les licences téléchargées sur le service ADM doivent être du type de licence groupée et être verrouillées sur l'ID d'hôte virtuel du nuage. Les ports entrants 27000 et 7279 de l'agent doivent être ouverts. Si un agent tombe en panne, les ADC qui y sont connectés passent en mode de grâce. Si un agent tombe en panne, les ADC non connectés ne refléteront aucune modification de configuration pendant environ vingt minutes. Ils continueront à fonctionner normalement. La modification du type de licence sur un ADC (ou l'édition de licence) nécessite un redémarrage à chaud. Un changement de capacité pour une licence ne nécessite pas de redémarrage.

Les agents et les ADC doivent être mis à la disposition du service Citrix ADM au moyen d'un processus d'inscription/ajout avant d'utiliser une fonctionnalité du service ADM. Voici le processus d'inscription et d'ajout du service SMA :

> **Remarque :** Les trois premières étapes se rapportent au contexte du SMA.

1. Inscrire les agents auprès du service ADM.
2. Ajoutez des instances ADC à ces agents (sur le service ADM).
3. Chargez des licences sur le service ADM.

   > **Remarque :** Les trois étapes suivantes se rapportent au contexte ADC.

4. Choisissez une licence à distance dans l'interface graphique ADC.
5. Entrez l'adresse IP de l'agent auquel l'ADC est enregistré.
6. Allouer (sur ADC)

> **Remarque :** le service ADM peut désormais être utilisé pour surveiller les licences groupées sur tous les ADC et aussi pour modifier l'allocation.

Citrix ADC CPX dans Kubernetes avec modèle de conception validé Diamanti et Nirmata

March 10, 2020

Caractéristiques et fonctions à tester

Cas d'essai : CPX en tant que contrôleur d'entrée et dispositif pour North-South et Hairpin East-West :

Configuration pour tous les cas de test à l'exception de VPX en tant que North-South :

- Deux CPX dans un cluster (CPX-1, CPX-2)
- ADM en tant que serveur de licences
- Conteneur exportateur Prometheus dans un cluster
- Serveur Prometheus et Grafana (soit en tant que pods dans Kubernetes ou externes au serveur Kubernetes)
- Plusieurs applications frontales
- Plusieurs applications principales

I. VPX en tant que North-South

1. VPX sur une plate-forme frontale SDX Diamanti

    - Tester le déchargement SSL et re-chiffrer avec l'insertion de X-Forward pour chaque connexion SSL
    - Insertion de X-Forward sur les sessions SSL

II. CPX comme dispositif North-South

1. CPX-1. Configurez l'entrée HTTPS avec la prise en charge de deux ou trois applications HTTPS avec une classe d'entrée spécifiée :

    - Démontrer la création de plusieurs stratégies de commutation de contenu : une par application frontale.
    - Démontrer plusieurs certificats génériques par CPX : un certificat générique par application.
    - Démontrer le déchargement CPX et le recryptage du trafic vers les applications frontales.
    - Démontrer un algorithme d'équilibrage de charge différent.
    - Démontrer la persistance d'une capsule.

2. CPX-1. Configurer l'entrée TCP séparée avec la classe d'entrée spécifiée :

    - Insérez l'application TCP comme MongoDB.
    - Afficher la création VIP TCP.
    - Afficher le trafic client TCP qui touche le conteneur MongoDB.
    - Afficher la vérification de l'état de l'application TCP par défaut.

3. CPX-1. Configurer l'entrée TCP-SSL séparée avec la classe d'entrée spécifiée :

    - Démontrer le déchargement SSL et le rechiffrement pour TCP-SSL VIP.
    - Répéter le cas 2.

4. CPX par application. Utilisation d'une classe d'entrée séparée :

    - Répétez les cas de test 1 à 3 en utilisant CPX-2 prenant en charge une seule application.

5. CPX par équipe. Utilisation de la classe d'entrée :

    - Attribuez différentes classes d'entrée pour 2 équipes.
    - Démontrer le cas de test 1 comme preuve que CPX peut configurer des règles d'entrée pour des équipes individuelles.

6. Mise à l'échelle automatique des modules Front End :

    - Augmentez le trafic vers les modules Front End et assurez-vous que les modules s'adaptent automatiquement.
    - Afficher que CPX-1 ajoute de nouveaux modules au groupe de services.

- Démontrer pour VIP d'entrée HTTPS.

7. Prise en charge de 4 à 7 vCPU :
    - Configurez CPX-1 avec 4 ou 7 vCPU.
    - Afficher le test de performance de HTTPS TPS, BW cryptée tout au long.

III. CPX comme dispositif Hairpin East-West

1. CPX-1. Créer une entrée HTTPS pour le trafic North-South comme décrit dans la section I.1 :
    - Exposer l'application dorsale à l'application frontale.
    - Afficher le trafic entre les deux applications.
    - Exposer l'application principale à une autre application principale.
    - Afficher le trafic entre les applications.
2. CPX-1. Suivez les instructions de l'étape 1. Affichez également le chiffrement de bout en bout :
    - Application principale vers application principale cryptée avec CPX-1 effectuant le déchargement et le rechiffrement.
3. Modules principaux Autoscale :
    - Démonstration CPX-1 en ajoutant des modules principaux Autoscale au groupe de services.

IV. Intégration CPX avec Prometheus et Grafana

1. Insérer le conteneur Prometheus dans le cluster Kubernetes :
    - Configurez le conteneur avec des compteurs recommandés pour l'exportation pour chaque application.
    - Démontrer l'envoi de données de compteur au serveur Prometheus par conteneur exportateur.
    - Afficher le tableau de bord Grafana illustrant les données du serveur Prometheus provenant de CPX.
    - L'objectif est de montrer que les développeurs peuvent utiliser des outils natifs dans le cloud qui sont couramment utilisés pour DevOps.
2. Démontrer l'intégration déploiement continu Kubernetes :
    - Insérer une nouvelle version de l'application dans Nirmata.
    - Afficher Kubernetes déployant une nouvelle version de l'application dans le cluster.
    - Démontrez que CPX répond aux commandes déployées de Kubernetes afin de prendre 100 % du trafic de l'ancienne version de l'application vers la nouvelle version de l'application.

Solution Citrix pour le déploiement Citrix ADC CPX

1. **Protocoles personnalisés :** Par défaut, CITRIX INGRESS CONTROLLER automatise la configuration avec les protocoles par défaut (HTTP/SSL). CITRIX INGRESS CONTROLLER prend en charge la configuration de protocoles personnalisés (TCP/SSL -TCP/UDP) en utilisant des annotations.

   Annotations :

   `ingress.citrix.com/insecure-service-type: "tcp"` [Annotation au protocole LB de sélection]

   `ingress.citrix.com/insecure-port: "53"` [Annotation pour prendre en charge le port personnalisé]

2. **Réglage fin des paramètres CS/LB/ServiceGroup :** Par défaut, CITRIX INGRESS CONTROLLER configure ADC avec les paramètres par défaut. Les paramètres peuvent être affiner à l'aide des annotations NetScaler ADC entity-parameter (**lb/servicegroup**).

   Annotations :

   Méthode LB :`ingress.citrix.com/lbvserver: '{ "app-1":{ "lbmethod":" ROUNDROBIN" } } '`

   Persistance :`ingress.citrix.com/lbvserver: '{ "app-1":{ "persistencetype ":"sourceip" } } '`

   API NITRO

3. **Chiffrement SSL par application :** CITRIX INGRESS CONTROLLER peut activer sélectivement le chiffrement SSL pour les applications à l'aide d'annotations intelligentes.

   Annotations :

   `ingress.citrix.com/secure_backend: '{ "web-backend": "True" }` [Annotation permettant d'activer sélectivement le chiffrement par application]

4. **Default cert for ingress :** CITRIX INGRESS CONTROLLER peut prendre le certificat par défaut comme argument. Si la définition d'entrée n'a pas le secret, alors le certificat par défaut est pris. Le secret doit être créé une fois dans l'espace de noms, puis toutes les entrées qui se trouvent dans l'espace de noms peuvent l'utiliser.

5. **Citrix multiple ingress class support :** Par défaut, CITRIX INGRESS CONTROLLER écoute tous les objets d'entrée dans le cluster k8s. Nous pouvons contrôler la configuration de l'ADC (Tier-1 MPX/VPX & Tier-2 CPX) à l'aide d'annotations de classe d'entrée. Cela permet à chaque équipe de gérer indépendamment les configurations de leur ADC. La classe Ingress peut aider à déployer

des solutions pour configurer l'ADC pour un espace de noms particulier ainsi qu'un groupe d'espaces de noms. Le support est plus générique que celui fourni par d'autres fournisseurs.

Annotations :

`kubernetes.io/ingress.class: "citrix"` [Notifier CITRIX INGRESS CONTROLLER de configurer uniquement l'entrée appartenant à une classe particulière]

6. **Visibilité :** la `k8s` solution Citrix est intégrée à des outils de `cncf` visibilité tels que Prometheous/Grafana pour la collecte de métriques afin de mieux prendre en charge le débogage et l'analyse. Citrix prometheus exportateur peut rendre les mesures disponibles à Prometheus pour une visibilité avec Grafana comme graphiques de séries chronologiques.

Pour plus d'informations sur l'utilisation de l'architecture des microservices, consultez leREADME.mdfichier dans GitHub. Vous pouvez trouver les `.yaml` fichiers dans leConfig dossier.

Scénario POC

Trois équipes exécutent leurs applications sur le cluster kubernetes. La configuration de chaque équipe est gérée indépendamment sur différents CPX à l'aide de la classe d'infiltration citrix.

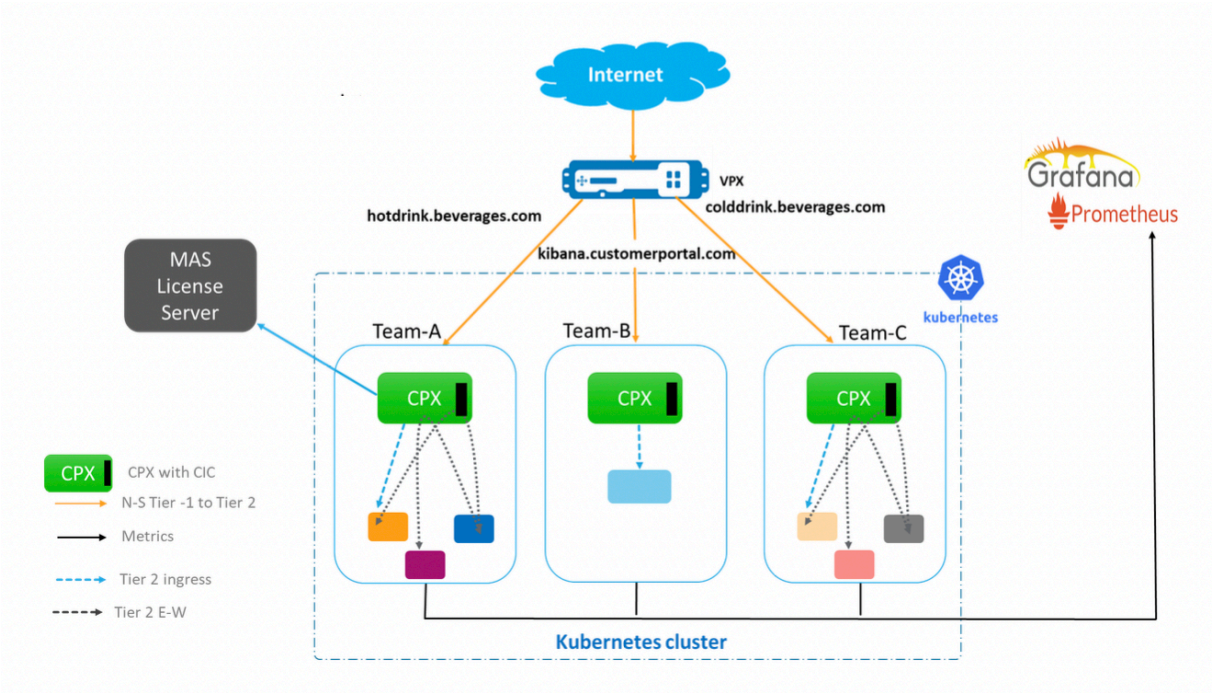
Les applications de chaque équipe sont exécutées dans des espaces de noms distincts (team-hotdrink, team-colddrink et team-redis) et tous les CPX s'exécutent dans l'espace de noms CPX.

`team-hotdrink`: SSL/HTTP Ingress, persistency, lbmethod, encryption/dycription per application, default-cert.

`team-colddrink`: Infiltration SSL-TCP

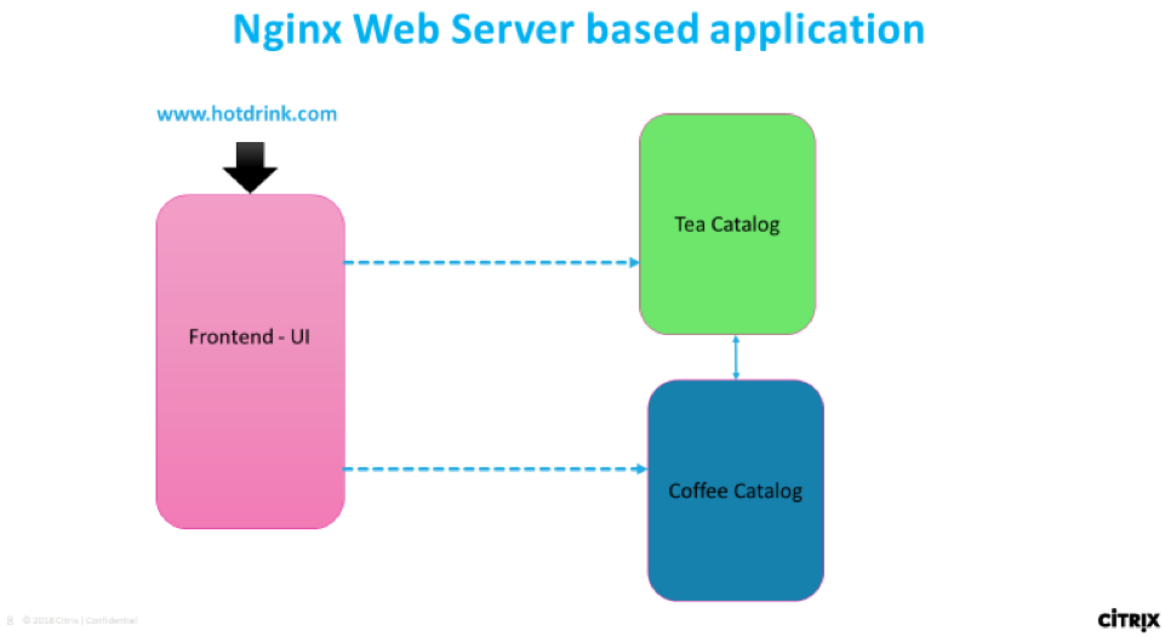
team-redis**":**Infiltration TCP

Configuration du POC

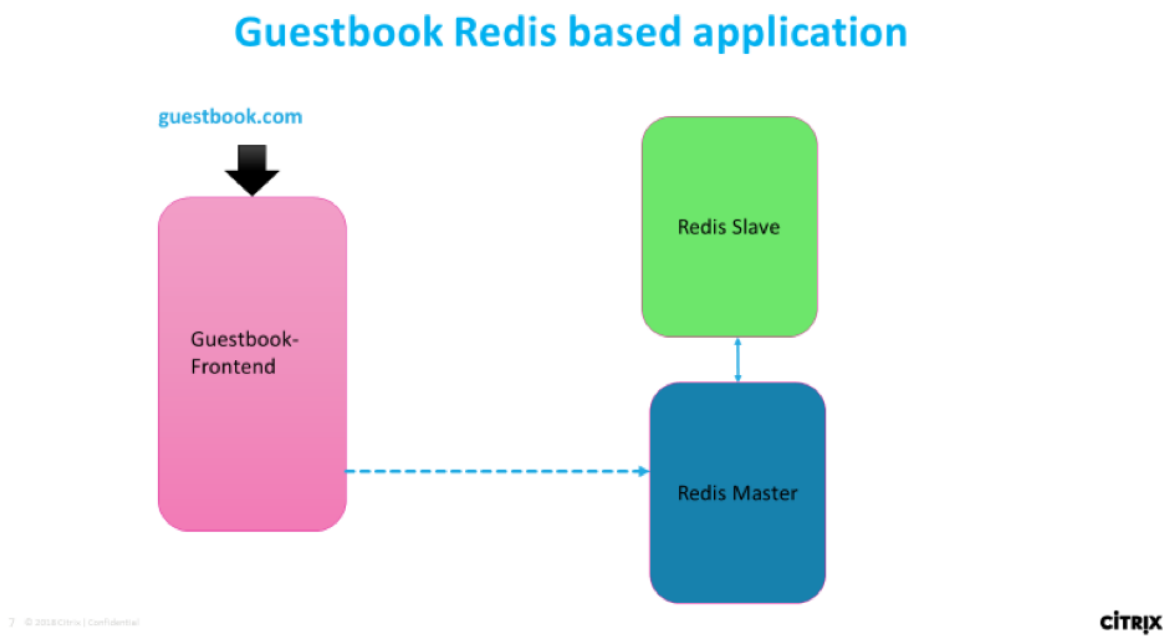


Flux d’application

Cas d’utilisation HTTP/SSL/SSL -TCP :



Cas d’utilisation TCP :



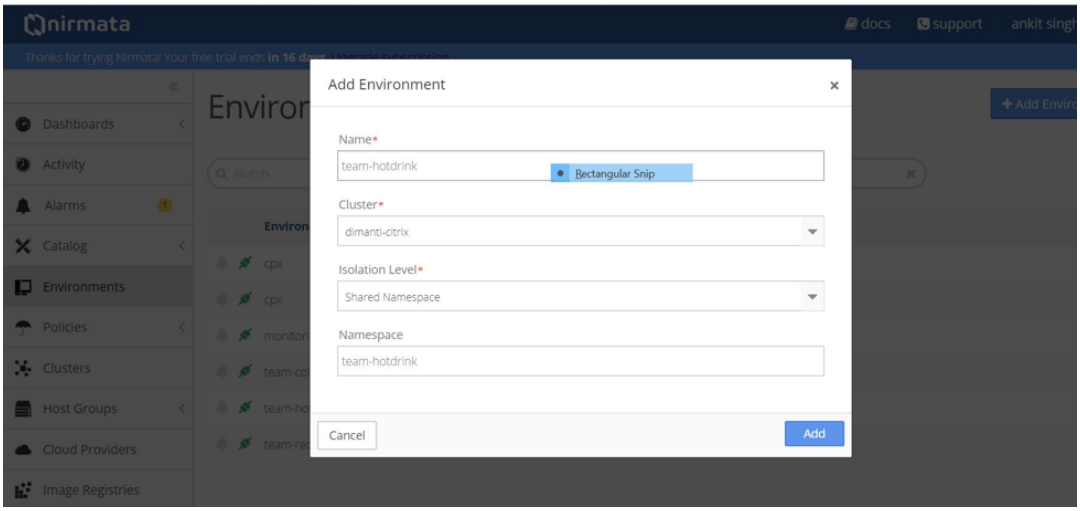
Obtention des images docker

Les commandes YAML fournies sont en train de récupérer les images à partir du dépôt quay.

Les images peuvent également être extraites et stockées dans le dépôt local. Vous pouvez les utiliser en modifiant le paramètre **Image** dans YAML.

Application étape par étape et déploiement CPX à l'aide de Nirmata

1. Téléchargez les rôles de cluster et les rolebindings de cluster dans YAML et appliquez-les dans le cluster à l'aide de Nirmata (rbac.yaml).
    a) Accédez à l'onglet **Clusters** .
    b) Sélectionnez le cluster.
    c) Dans les paramètres, appliquez YAML à partir de l'option **Appliquer YAML** .
2. Créez l'environnement pour exécuter CPX et les applications.
    a) Accédez à l'onglet **Environnement**.
    b) Cliquez sur **l'onglet Ajouter un environnement** .
        - Sélectionnez le cluster et créez un environnement dans l'espace de noms partagé.



c) Créez les environnements suivants pour exécuter Prometheus, CPX et des applications pour différentes équipes.

- Créer un environnement : cpx
- Créer un environnement : team-hotdrink
- Créer un environnement : team-colddrink
- Créer un environnement : team-redis

3. Téléchargez l'`.yaml` application en utilisant Nirmata.

a) Accédez à l'onglet **Catalogue**.

b) Cliquez sur **Ajouter une application**.

c) Cliquez sur **Ajouter** pour ajouter les applications.

Ajouter une application : team-hotdrink (team_hotdrink.yaml). Nom de l'application : `team-hotdrink`.

Ajouter une application : team-colddrink (team_coldrink.yaml). Nom de l'application : `team-colddrink`.

Ajouter une application : team-redis (team_redis.yaml). Nom de l'application : `team-redis`.

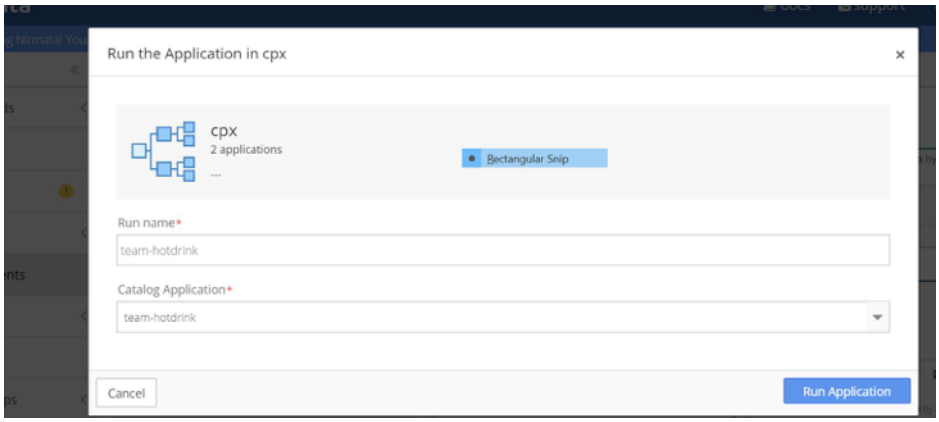
Ajouter une application : cpx-svcacct (cpx_svcacct.yaml). Nom de l'application : cpx-svcacct.

> Remarque :
>
> CPX avec CITRIX INGRESS CONTROLLER intégré nécessite un compte de service dans l'espace de noms où il est exécuté. Pour la version actuelle dans Nirmata, créez ceci`cpx_svcacct.yaml` en utilisant l'environnement cpx.

Ajouter l'application : cpx (cpx_wo_sa.yaml). Nom de l'application : cpx.

4. Exécutez le CPX en utilisant Nirmata.

   a) Accédez à l'onglet **Environnement** et sélectionnez l'environnement approprié.
   b) Cliquez sur **Exécuter l'application** pour exécuter l'application.
   c) Dans l'environnement cpx, exécutez l'`cpx-svcacct` application. Sélectionnez`cpx-svcacct` avec le nom d'exécution dans l' **application`cpx-svcacct` de catalogue** .
   d) Dans l'environnement cpx, exécutez l'application cpx. Sélectionnez cpx dans l' **application de catalogue**.



> Remarque :
>
> Il y a quelques petites solutions de contournement nécessaires pour le déploiement CPX, car l'installation utilise une version antérieure de Nirmata.
>
> a) Lors de la création des déploiements CPX, ne définissez pas le`serviceAccountName` . Le`serviceAccountName` peut être ajouté plus tard. Pour contourner le problème, redéployez automatiquement les pods.
> b) Importez le secret TLS pour l'entrée directement dans l'environnement. Cela garantit que le champ de type est préservé.

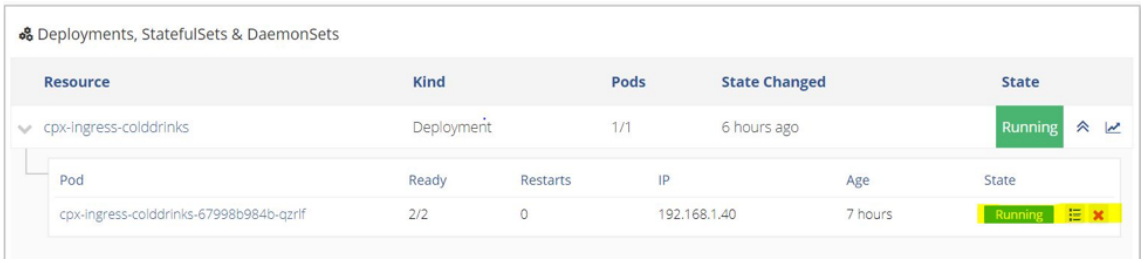
   a) Après avoir exécuté l'application, accédez à l'application **CPX** .
   b) Sous l'onglet **Déploiements > StatefulSets & Daemonsets** , cliquez sur le`cpx-ingress-colddrinks` déploiement.
   c) Sur la page suivante, modifiez le **modèle Pod**. Saisissez **CPX** dans le **compte de service**.
   d) Retournez à l'application **CPX** .
   e) Répétez la même procédure pour le`cpx-ingress-hotdrinks` déploiement`cpx-ingress-redis` et.

L'application du compte de service permet de redéployer les pods. Attendez que les pods arrivent et confirmez si le compte de service a été appliqué.

La même chose peut être vérifiée à l'aide des commandes suivantes dans le cluster Diamanti.


```
[diamanti@diamanti-250 ~]$ kubectl get deployment -n cpx -o yaml |
    grep -i account
        serviceAccount: cpx
        serviceAccountName: cpx
        serviceAccount: cpx
<!--NeedCopy-->
```

> **Remarque :** Si le n'`serviceAccount` est pas appliqué, annulez les pods CPX. Le déploiement qui le recrée, vient avec`serviceAccount`.



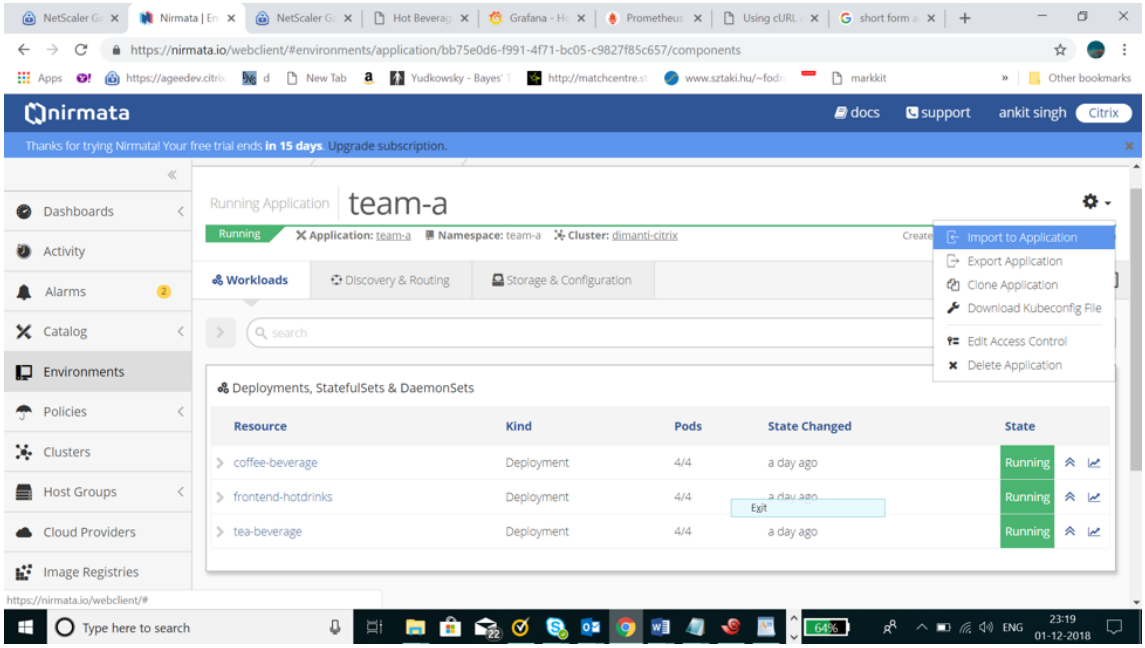
5. Exécutez les applications à l'aide de Nirmata.

   application team-hotdrink :

   a) Accédez à l'onglet **Environnement** et sélectionnez l'environnement approprié : `team-hotdrink`.

   b) Dans l'environnement `team-hotdrink`, exécutez l'application `team-hotddrink` avec le nom d'exécution `team-hotdrink`. Sélectionnez `team-hotdrink` dans l'**application de catalogue**.

   c) Allez à l'application `team-hotdrink`. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres** et sélectionnez **Importer dans l'application** . Charger `hotdrink-secret.yaml`.



application team-colddrink :

a) Accédez à l'onglet **Environnement** et sélectionnez l'environnement approprié : `team-colddrink`.

b) Dans l'environnement `team-colddrink`, exécutez l'application `team-coldddrink` avec le nom d'exécution `team-colddrink`. Sélectionnez `team-hotdrink` dans l'**application de catalogue**.

c) Allez à l'application `team-colddrink`. Dans le coin supérieur droit de l'écran, cliquez sur **Paramètres** et sélectionnez **Importer dans l'application** . Charger `colddrink-secret.yaml`.

application team-redis :

a) Accédez à l'onglet **Environnement** et sélectionnez l'environnement approprié : `team-redis`.

b) Dans l'environnement `team-colddrink`, exécutez une application avec le nom d'exécution `team-redis`. Sélectionnez `team-redis` dans l'**application de catalogue**.

- Dans l'environnement `team-redis`, exécutez une application avec le nom d'exécution `team-redis`.

Commandes sur VPX pour exposer le CPX de niveau 2

Le VPX de niveau 1 devrait effectuer le chiffrement ssl et le décryptage et insérer l'en-tête X-forward lors de l'envoi au CPX de niveau 2. La configuration de niveau 1 doit être effectuée manuellement. L'en-tête X-Forward peut être inséré à l'aide de -cip ENABLED dans servicegroup. Ouvre`config.txt`.

Créer un csverver :

Téléchargez lecertkey dans Citrix ADC :wild.com-key.pem, wild.com-cert.pem

```
add cs vserver frontent_grafana HTTP <CS_VSERVER_IP> 80 -cltTimeout 180
<!--NeedCopy-->
```

Exposez www.hotdrinks.com, www.colddrinks.com, www.guestbook.com sur Tier-1 VPX :

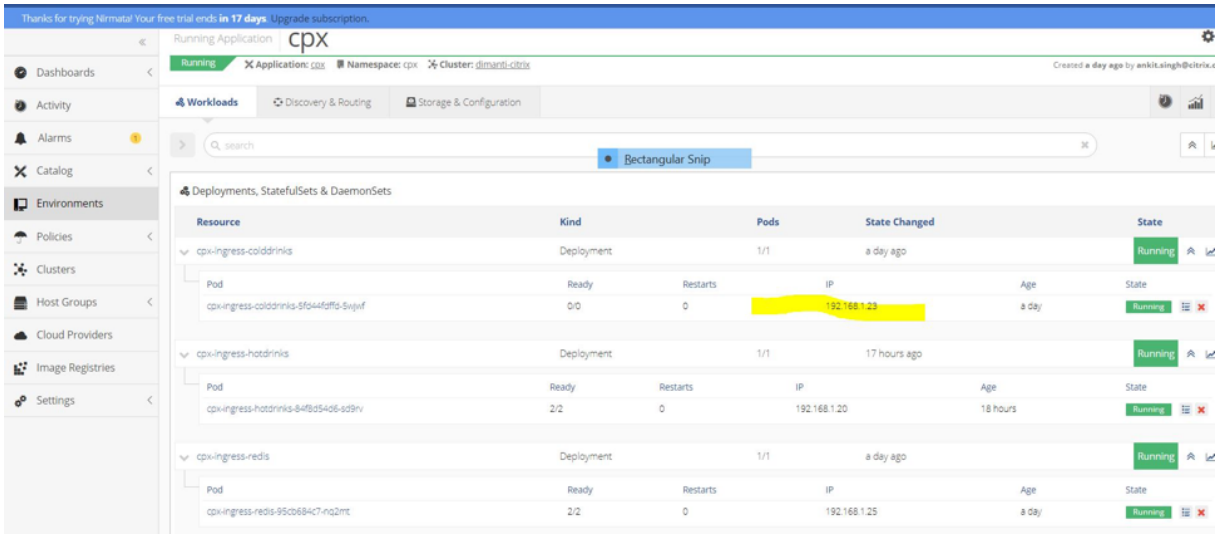
```
add serviceGroup team_hotdrink_cpx SSL -cip ENABLED
add serviceGroup team_colddrink_cpx SSL -cip ENABLED
add serviceGroup team_redis_cpx HTTP
add ssl certKey cert -cert "wild-hotdrink.com-cert.pem" -key "wild-
    hotdrink.com-key.pem"
add lb vserver team_hotdrink_cpx HTTP 0.0.0.0 0
add lb vserver team_colddrink_cpx HTTP 0.0.0.0 0
add lb vserver team_redis_cpx HTTP 0.0.0.0 0
add cs vserver frontent SSL 10.106.73.218 443
add cs action team_hotdrink_cpx -targetLBVserver team_hotdrink_cpx
add cs action team_colddrink_cpx -targetLBVserver team_colddrink_cpx
add cs action team_redis_cpx -targetLBVserver team_redis_cpx
add cs policy team_hotdrink_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www
    .hotdrinks.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_hotdrink_cpx
add cs policy team_colddrink_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("
    www.colddrinks.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_colddrink_cpx
add cs policy team_redis_cpx -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.
    guestbook.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    team_redis_cpx
bind lb vserver team_hotdrink_cpx team_hotdrink_cpx
bind lb vserver team_colddrink_cpx team_colddrink_cpx
bind lb vserver team_redis_cpx team_redis_cpx
bind cs vserver frontent -policyName team_hotdrink_cpx -priority 10
bind cs vserver frontent -policyName team_colddrink_cpx -priority 20
bind cs vserver frontent -policyName team_redis_cpx -priority 30
bind serviceGroup team_hotdrink_cpx 10.1.3.8 443
bind serviceGroup team_colddrink_cpx 10.1.2.52 443
bind serviceGroup team_redis_cpx 10.1.2.53 80
bind ssl vserver frontent -certkeyName cert
<!--NeedCopy-->
```

Mettez à jour l'adresse IP vers les adresses IP du pod CPX pour servicegroup :

```
root@ubuntu-211:~/demo-nimata/final/final-v1# kubectl get pods -n cpx -
    o wide
```



```
NAME                                          READY     STATUS    RESTARTS
      AGE       IP              NODE
cpx-ingress-colddrinks-5bd94bff8b-7prdl   1/1       Running   0
              2h        10.1.3.8    ubuntu-221
cpx-ingress-hotdrinks-7c99b59f88-5kclv    1/1       Running   0
              2h        10.1.2.52   ubuntu-213
cpx-ingress-redis-7bd6789d7f-szbv7        1/1       Running   0
              2h        10.1.2.53   ubuntu-213
<!--NeedCopy-->
```



- Pour accéder à **www.hotdrinks.com, www.colddrinks.com, www.guestbook.com**, le fichier hosts (de la machine à partir de laquelle les pages sont accessibles) doit être ajouté avec les valeurs suivantes :

```
<CS_VSERVER_IP>      www.hotdrinks.com

<CS_VSERVER_IP>      www.colddrinks.com

<CS_VSERVER_IP>      www.guestbook.com
```

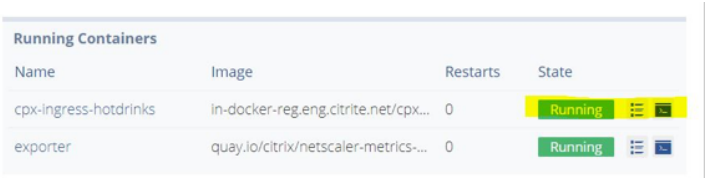
  Après cela, vous pouvez accéder aux applications en visitant : **www.hotdrinks.com, www.colddrinks.com, www.guestbook.com**

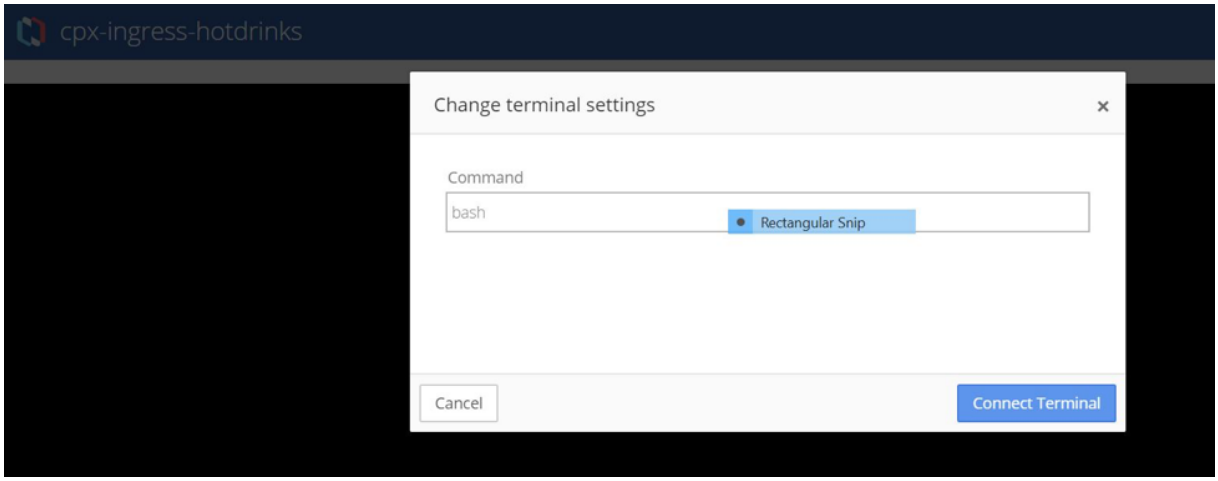
Validation de la configuration CPX de niveau 2

Pour valider la configuration CPX, accédez à l'environnement CPX. Sélectionnez l'application CPX en cours d'exécution.

Sélectionnez le`cpx-ingress-hotdrinks` déploiement, puis cliquez sur le`cpx-ingress-hotdrinks-xxxx-xxxx` module.

Sur la page suivante, allez dans le conteneur en cours d'exécution et lancez le terminal pour `cpx-ingress-hotdrinks` en tapant la commande « bash ».





Lorsque le terminal est connecté, validez la configuration à l'aide de la commande NetScaler standard via`cli_script.sh`.

- cli_script.sh "sh cs vs"
- cli_script.sh "sh lb vs"
- cli_script.sh "sh servicegroup"

La validation peut être effectuée pour d'autres déploiements CPX pour`team-colddrink` et`team-mongodb` de la même manière.

Effectuer une mise à l'échelle haut/descendante

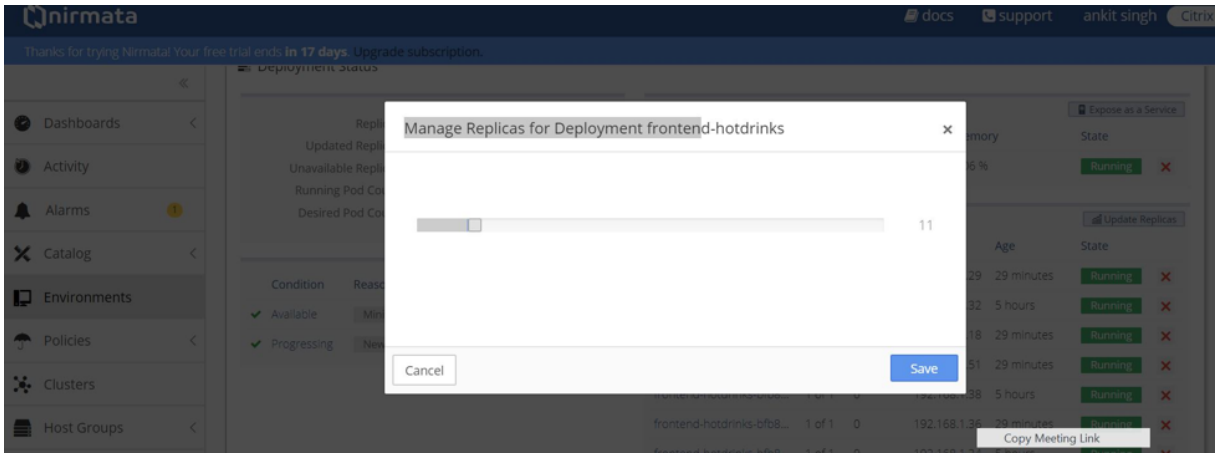
Pour effectuer une mise à l'échelle haut/descendante :

1. Allez dans l'environnement `team-hotdrink`. Sélectionnez l'application `team-hotdrink` en cours d'exécution.
2. Cliquez sur le déploiement `frontend-hotdrinks`.
3. Sur la page suivante, cliquez sur **Mise à jour des réplicas**. Augmentez-le à 10.

Reportez-vous à : Validation de la configuration CPX de niveau 2 pour vérifier la configuration dans CPX (déploiement : cpx-ingress-hotdrinks).

1. Accédez à l'environnement CPX. Sélectionnez une application CPX en cours d'exécution.
2. Cliquez sur le déploiement `cpx-ingress-hotdrinks`.
3. Cliquez sur le`cpx-ingress-hotdrinks-xxxx-xxxx` module.

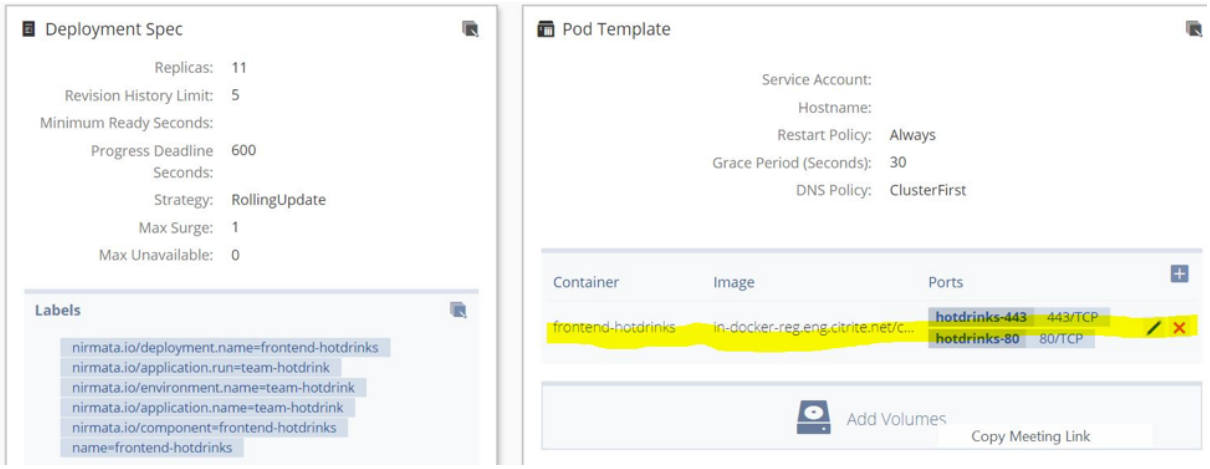
4. Sur la page suivante, allez dans le conteneur en cours d'exécution et lancez le terminal pour `cpx-ingress-hotdrinks` en tapant la commande « bash ».
5. `cli_script.sh "sh servicegroup < servicegroup name >"`.



Mise à jour continue

Pour effectuer une mise à jour continue :

1. Allez dans l'environnement `team-hotdrink`. Sélectionnez l'application `team-hotdrink` en cours d'exécution.
2. Déployer les boissons chaudes avant.
3. Sur la page suivante, accédez au modèle **Pod** .
4. Mettez à jour l'image pour : *quay.io/citrix/hotdrinks -v2 : latest*.
5. Laissez la mise à jour se terminer.
6. Accédez à nouveau à l'application. La nouvelle page devrait être accompagnée d'une image mise à jour après avoir effectué la mise à jour.



Déploiement de Prometheus

NetScaler Metrics Exporter, Prometheus et Grafana sont utilisés pour détecter et collecter automatiquement des mesures à partir du CPX d'entrée.

Étapes à suivre pour déployer Prometheus :

Créez les environnements pour exécuter CPX et les applications :

1. Accédez à l'onglet **Environnement**.
2. Cliquez sur **Ajouter un environnement**.
3. Créez les environnements pour exécuter Exporter, Prometheus et Grafana.
    - Créer l'environnement : **surveillance**.

Téléchargez le `.yaml` fichier en utilisant Nirmata :

1. Accédez à l'onglet **Catalogue**.
2. Cliquez sur **Ajouter une application**.
3. Cliquez sur **Ajouter** pour ajouter les applications.
    - Ajouter application : monitoring (monitoring.yaml).

Exécution de l'application Prometheus :

1. Allez dans l'onglet **Environnement** et sélectionnez l'environnement approprié : **surveillance** .
2. Cliquez sur **Exécuter l'application** à l'aide de la **surveillance des** noms.
3. Cette opération déploie les pods Exportateur, Prométhée et Grafana et commence à collecter des mesures.
4. Maintenant Prométhée et Grafana doivent être exposés à travers le VPX.

Commandes sur le VPX pour exposer Prometheus et Grafana :

Créer un serveur csvserver :

```
add cs vserver frontent_grafana HTTP <CS_VSERVER_IP> 80 -cltTimeout 180
<!--NeedCopy-->
```

Exposer Prométhée :

```
add serviceGroup prometheus HTTP
add lb vserver prometheus HTTP 0.0.0.0 0
add cs action prometheus -targetLBVserver prometheus
add cs policy prometheus -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.
    prometheus.com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action
    prometheus
bind lb vserver prometheus prometheus
bind cs vserver frontent_grafana -policyName prometheus -priority 20
bind serviceGroup prometheus <PROMETHEUS_POD_IP> 9090
<!--NeedCopy-->
```


> Remarque :
>
> Obtenez l'IP du pod prometheus-k8s-0 en utilisant « kubectl get pods -n monitoring -o wide »

Exposer Grafana :

```
add serviceGroup grafana HTTP
add lb vserver grafana HTTP 0.0.0.0 0
add cs action grafana -targetLBVserver grafana
add cs policy grafana -rule "HTTP.REQ.HOSTNAME.SERVER.EQ("www.grafana.
    com") && HTTP.REQ.URL.PATH.STARTSWITH("/")" -action grafana
bind lb vserver grafana grafana
bind cs vserver frontent_grafana -policyName grafana -priority 10
bind serviceGroup grafana <GRAFANA_POD_IP>  3000
<!--NeedCopy-->
```

> Remarque :
>
> Obtenez l'adresse IP du pod grafana-xxxx-xxx en utilisant `kubectl get pods -n monitoring -o wide`

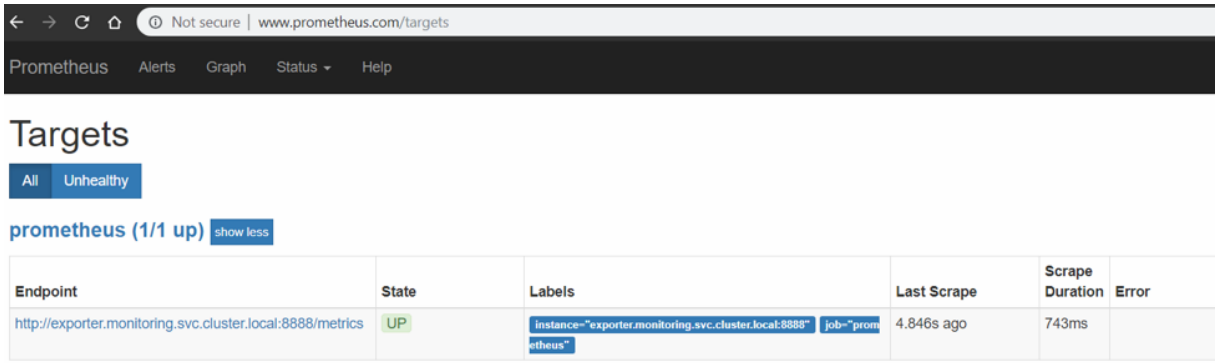
- Maintenant, les pages Prometheus et Grafana ont été exposées pour accès via le serveur cs du VPX.
- Pour accéder à Prometheus et Grafana, le fichier hosts (de la machine à partir de laquelle les pages sont accessibles) doit être ajouté avec les valeurs suivantes :

```
<CS_VSERVER_IP>       www.grafana.com
<CS_VSERVER_IP>       www.prometheus.com
```

- Lorsque cela est fait, accédez à Prometheus en visitant **www.prometheus.com**. Accédez à Grafana en visitant **www.grafana.com**.

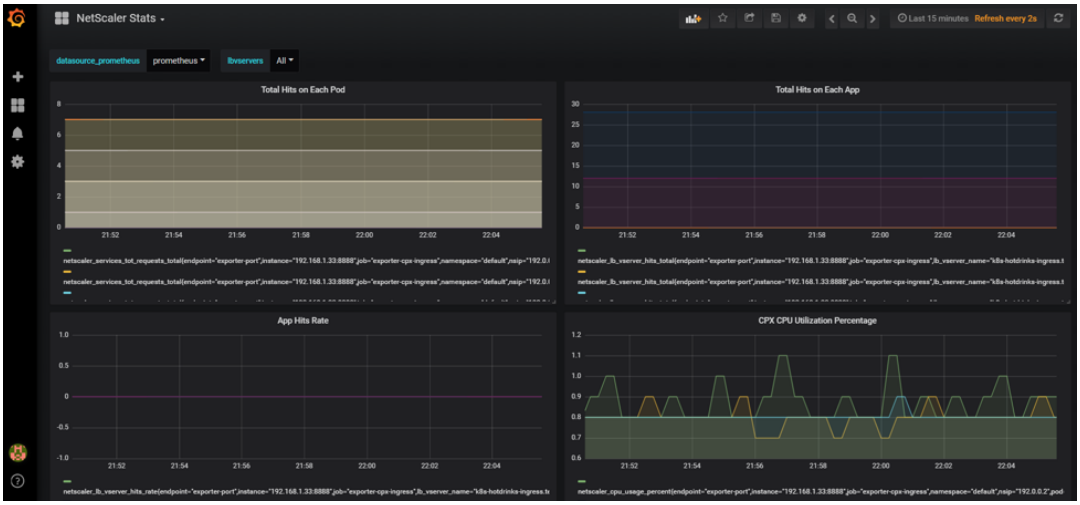
Visualisez les mesures :

- Pour vous assurer que Prometheus a détecté l'exportateur, visitez le **site www.prometheus.com/targets**. Il devrait contenir une liste de tous les exportateurs qui surveillent les périphériques CPX et VPX. Assurez-vous que tous les exportateurs sont dans l'état **UP** . Voir l'exemple suivant :



- Vous pouvez maintenant utiliser Grafana pour tracer les valeurs qui sont collectées. Pour ce faire :

  1. Rendez-vous **sur www.grafana.com**. Assurez-vous qu'une entrée appropriée est ajoutée dans le fichier hôte.
  2. Connectez-vous en utilisant le nom d'utilisateur **admin** et mot de passe **admin** par défaut.
  3. Une fois connecté, cliquez sur **Ajouter une source de données** dans le tableau de bord d'accueil.
  4. Sélectionnez l'option **Prometheus** .
  5. Fournisseur/modifiez les détails suivants :
     - Nom : prometheus (minuscules).
     - URL :`http://prometheus:9090`.
     - Laissez les entrées restantes avec les valeurs par défaut.
  6. Cliquez sur **Enregistrer et tester**. Attendez quelques secondes jusqu'à ce que le message **de la source de données fonctionne** apparaît en bas de l'écran.
  7. Importez un modèle Grafana préconçu en cliquant sur l'+ icône sur le panneau de gauche. Choisissez **Importer**.
  8. Cliquez sur le bouton **Télécharger json** et sélectionnez le fichier **sample_grafana_dashboard.json** (Laisser le **nom** , **le dossier** et l' **identificateur unique** inchangés).
  9. Choisissez **Prometheus** dans le menu déroulant Prometheus, puis cliquez sur **Importer** .
  10. Ceci télécharge un tableau de bord similaire à l'image suivante :



Licences et tests de performance

Exécution de CPX pour perf et licence.

Le nombre de cœurs CPX et les détails du serveur de licences sont donnés dans les variables d'environnement suivantes.

Variable d'environnement pour sélectionner le nombre de cœurs

- **nom : "CPX_CORES"**
- **valeur : "3"**

Variable d'environnement pour sélectionner le serveur de licences

- **nom : "LS_IP"**
- **valeur : "X.X.X.X"**

  Annotations Diamanti :
  `diamanti.com/endpoint0: '{ "network":"lab-network","perfTier":"high" }`

  Pointez pour corriger le serveur de licences en définissant l'adresse IP correcte ci-dessus.

  1. Ajoutez les variables d'environnement mentionnées ci-dessus ainsi que les annotations spécifiques Diamanti dans le`cpx-perf.yaml` fichier.
  2. Accédez à l'onglet **Environnement** et créez l'environnement `cpx-perf`.

  Téléchargez l'application YAML en utilisant Nirmata.

  1. Accédez à l'onglet **Catalogue**.
  2. Cliquez sur **Ajouter une application**.

3. Cliquez sur **Ajouter** pour ajouter une application : `cpx-perf.yaml`. Nom de l'application : `cpx-perf`.

Exécution de CPX :

1. Accédez à l'onglet **Environnement** et sélectionnez l'`cpx-perf` environnement.
2. Dans l'environnement `cpx-perf`, exécutez l'application `cpx-svcacct`.
3. Dans l'environnement `cpx-perf`, exécutez l'application `cpx-perf`.
4. Après avoir exécuté l'application, accédez à l'`cpx-perf` application.
5. Sous **Déploiements > onglet StatefulSets & DaemonSets** , cliquez sur le`cpx-ingress-perf` déploiement. Sur la page suivante, modifiez le modèle Pod. Saisissez **CPX** dans le **compte de service**.
6. Valider que la licence fonctionne et que la récupération de licence a lieu dans Citrix ADM.
   - Pour valider sur le CPX, effectuez les opérations suivantes :
     * `kubectl get pods -n cpx`
     * `kubectl exec -it <CPX_POD_NAME> -n cpx bash`
     * `cli_script.sh 'sh licenseserver'`
     * `cli_script.sh 'sh capacity'`
   - Afficher une sortie similaire :

```
root@cpx-ingress-colddrinks-66f4d75f76-kzf8w:/# cli_script.sh
    'sh licenseserver'
exec: sh licenseserver
1)  ServerName:  10.217.212.228Port:  27000           Status:
     1             Grace:  0              Gptimeleft:  0
Done
root@cpx-ingress-colddrinks-66f4d75f76-kzf8w:/# cli_script.sh
    'sh capacity'
exec: sh capacity
    Actualbandwidth:  10000 VcpuCount:  3          Edition:
       Platinum      Unit:  Mbps            Maxbandwidth:
       10000    Minbandwidth:  20       Instancecount:  0
Done
<!--NeedCopy-->
```

   - Pour valider sur l'ADM, accédez au serveur de licences et accédez à **Réseaux > Licences > Licences CPU virtuelles**.
   - Ici, vous devriez voir le CPX sous licence avec le nombre de cœurs.

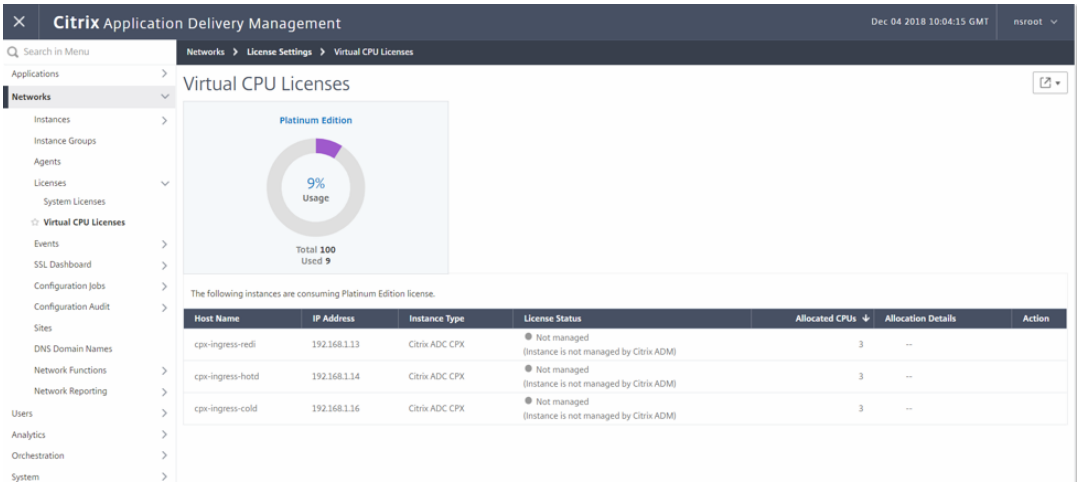


Tableau des annotations

Annotation	Valeur possible	Description	Par défaut (le cas échéant)
kubernetes.io/ingress.c	nom de classe d'entrée	C'est un moyen d'associer une ressource d'entrée particulière à un contrôleur d'entrée. Par exemple, les opérations suivantes peuvent être effectuées : `kubernetes.io/ingress.class:"Citrix"`	Configure toutes les incursions

Annotation	Valeur possible	Description	Par défaut (le cas échéant)
ingress.citrix.com/secure_backend	À l'aide du format .json, lister les services pour le backend sécurisé	Utilisez **True**, si vous souhaitez que Citrix ADC connecte votre application à la connexion HTTPS sécurisée. Utilisez **False**si vous souhaitez que Citrix ADC connecte votre application avec une connexion HTTP non sécurisée. Par exemple, les opérations suivantes peuvent être effectuées : `ingress.citrix.com/secure_backend: { 'app1' :"True", 'app2' :"False", 'app3' :"True"}`	« Faux »

Annotation	Valeur possible	Description	Par défaut (le cas échéant)
ingress.citrix.com/lbvse	Dans le formulaire JSON, les paramètres pour lbvserver	Il fournit une fonctionnalité d'annotation intelligente. Grâce à cela, un utilisateur avancé (qui connaît les options de serveur NetScaler LB et de groupe de services) peut les appliquer directement. Les valeurs doivent être au format .json. Pour chaque application principale dans l'entrée, fournissez une paire de valeurs clés. Le nom de la clé doit correspondre au nom de l'interface de ligne de commande correspondante. Par exemple, les opérations suivantes peuvent être effectuées : `ingress.citrix.com/lbvserver: '{ "app-1":{ "lbmethod":"ROUNDROBIN" } }'`	Valeurs par défaut

Modèle de conception validé des profils SSL de Citrix ADC

January 8, 2020

Généralités

Récapitulatif de Citrix ADC

Citrix ADC est un contrôleur de mise à disposition d'applications tout-en-un qui permet d'exécuter les applications jusqu'à cinq fois mieux, réduit les coûts de propriété des applications, optimise l'expérience utilisateur et garantit que les applications sont toujours disponibles à l'aide de :

- Équilibrage de charge avancé L4-7 et gestion du trafic
- Accélération éprouvée des applications comme la compression HTTP et la mise en cache
- Un pare-feu intégré pour la sécurité des applications
- Déchargement des serveurs pour réduire considérablement les coûts et consolider les serveurs

En tant que leader incontesté de la fourniture de services et d'applications, Citrix ADC est déployé sur des milliers de réseaux à travers le monde pour optimiser, sécuriser et contrôler la fourniture de tous les services d'entreprise et de cloud. Déployé directement devant les serveurs Web et de base de données, Citrix ADC combine l'équilibrage de charge et la commutation de contenu à grande vitesse, la compression http, la mise en cache du contenu, l'accélération SSL, la visibilité du flux d'applications et un pare-feu d'application puissant dans une plate-forme intégrée et facile à utiliser. Il est beaucoup plus simple de respecter les SLA grâce à une surveillance de bout en bout qui transforme les données réseau en Business Intelligence exploitable. Citrix ADC permet de définir et de gérer les stratégies à l'aide d'un moteur de stratégie déclarative simple sans expertise en programmation requise.

Présentation des profils SSL Citrix ADC

Vous pouvez utiliser un profil SSL pour spécifier comment un Citrix ADC traite le trafic SSL. Le profil est un ensemble de paramètres SSL pour les entités SSL, telles que les serveurs virtuels, les services et les groupes de services, et offre une configuration facile et une flexibilité. Vous n'êtes pas limité à la configuration d'un seul ensemble de paramètres globaux. Vous pouvez créer plusieurs ensembles (profils) de paramètres globaux et affecter différents ensembles à différentes entités SSL. Les profils SSL sont classés en deux catégories :

- Profils frontaux contenant les paramètres applicables à l'entité frontale. Autrement dit, ils s'appliquent à l'entité qui reçoit des demandes d'un client.
- Profils principaux contenant les paramètres applicables à l'entité principale. Autrement dit, ils s'appliquent à l'entité qui envoie des demandes client à un serveur.

Contrairement à un profil TCP ou HTTP, un profil SSL est facultatif. Une fois que les profils SSL (paramètre global) sont activés, tous les points de terminaison SSL héritent des profils par défaut. Le même profil peut être réutilisé sur plusieurs entités. Si aucun profil n'est attaché à une entité, les valeurs définies au niveau global s'appliquent. Pour les services apprises de manière dynamique, les valeurs globales actuelles s'appliquent.

Par rapport à la méthode alternative qui nécessite la configuration des paramètres SSL, des chiffrements et des courbes ECC sur des points de terminaison SSL individuels, les profils SSL sur Citrix ADC simplifient la gestion de la configuration en agissant comme un point unique de configuration SSL pour tous les points de terminaison associés. En outre, les problèmes de configuration tels que la réorganisation du chiffrement et les temps d'arrêt lorsque les chiffrements sont réorganisés sont résolus avec l'utilisation de profils SSL.

Les profils SSL aident à définir les paramètres SSL requis et les liaisons de chiffrement sur les points de terminaison SSL sur lesquels on ne pouvait traditionnellement pas définir ces paramètres et liaisons. Les profils SSL peuvent également être configurés sur des moniteurs sécurisés.

Le tableau suivant répertorie les paramètres qui font partie de chaque profil :

Profil frontal	Profil principal
cipherRedirect, cipherURL	denySSLReneg
clearTextPort*	encryptTriggerPktCount
clientAuth, clientCert	nonFipsCiphers
denySSLReneg	pushEncTrigger
dh, dhFile, dhCount	PushencTriggerTimeout
dropReqWithNoHostHeader	pushFlag
encryptTriggerPktCount	quantumSize
eRSA, eRSACount	serverAuth
insertionEncoding	commonName
nonFipsCiphers	sessReuse, sessTimeout
pushEncTrigger	SNIEnable
PushencTriggerTimeout	ssl3
pushFlag	sslTriggerTimeout
quantumSize	strictCAChecks
redirectPortRewrite	TLS 1.0, TLS 1.1, TLS 1.2
sendCloseNotify	

Profil frontal	Profil principal
sessReuse, sessTimeout	
SNIEnable	
ssl3	
sslRedirect	
sslTriggerTimeout	
strictCAChecks	
tls1, tls11, tls12	

* Le paramètre ClearTextPort s'applique uniquement à un serveur virtuel SSL.

Un message d'erreur s'affiche si vous essayez de définir un paramètre qui ne fait pas partie du profil (par exemple, si vous essayez de définir le paramètre ClientAuth dans un profil principal).

Certains paramètres SSL, tels que la taille de la mémoire CRL, la taille du cache OCSP, le contrôle UndefAction et les données UndefAction, ne font partie d'aucun des profils ci-dessus, car ces paramètres sont indépendants des entités. Ces paramètres sont présents dans **Gestion du trafic > SSL > Paramètres SSL avancés**.

Un profil SSL prend en charge les opérations suivantes :

- Ajouter : crée un profil SSL sur Citrix ADC. Spécifiez si le profil est frontal ou principal. Frontal est la valeur par défaut.
- Set : modifie les paramètres d'un profil existant.
- Unset : définit les paramètres spécifiés sur leurs valeurs par défaut. Si vous ne spécifiez aucun paramètre, un message d'erreur s'affiche. Si vous désactivez un profil sur une entité, le profil est indépendant de l'entité.
- Supprimer (Remove) : supprime un profil. Un profil utilisé par une entité ne peut pas être supprimé. La suppression de la configuration supprime toutes les entités. Par conséquent, les profils sont également supprimés.
- Bind : lie un profil à un serveur virtuel.
- Unbind : délie un profil d'un serveur virtuel.
- Afficher : affiche tous les profils disponibles sur Citrix ADC. Si un nom de profil est spécifié, les détails de ce profil sont affichés. Si une entité est spécifiée, les profils associés à cette entité sont affichés.

Cas d'utilisation des profils SSL

Profils par défaut SSL

Les appliances Citrix ADC sont livrés avec deux profils par défaut intégrés :

1. ns_default_ssl_profile_frontend — profil frontal par défaut pour tous les serveurs virtuels de type SSL et les services internes.
2. ns_default_ssl_profile_backend — profil principal par défaut pour les services de type SSL, les groupes de services et les moniteurs sécurisés.

Tout nouveau point de terminaison créé obtient le profil SSL par défaut correspondant lié.

Il est possible de modifier les paramètres SSL et les chiffrements des profils SSL par défaut. Cela garantit que les clients peuvent modifier les paramètres et les liaisons à un point qui est référencé par les points de terminaison correspondants.

> **Important :**
>
> enregistrez votre configuration avant de procéder à la mise à niveau du logiciel et activez les profils par défaut.
>
> Mettez à niveau le logiciel vers une version prenant en charge l'infrastructure de profil améliorée, puis activez les profils par défaut. Vous pouvez adopter l'une des deux approches en fonction de votre déploiement spécifique. Si votre déploiement a une configuration SSL commune à travers les points d'extrémité, reportez-vous au cas d'utilisation 1. Si votre déploiement a une configuration SSL importante et que les paramètres SSL et les chiffrements ne sont pas courants entre les points de terminale, reportez-vous au cas d'utilisation 2.
>
> Après la mise à niveau du logiciel, si vous activez le profil, vous ne pouvez pas inverser les modifications. Autrement dit, le profil ne peut pas être désactivé. Par conséquent, la seule façon d'inverser la modification est de redémarrer en utilisant l'ancienne configuration.
>
> **Remarque :** Une seule opération (Activer le profil par défaut ou définir le paramètre ssl -defaultProfile ENABLED) active (lie) à la fois le profil frontal par défaut et le profil principal par défaut.
>
> **Remarque :** les profils SSL par défaut sont désormais disponibles pour le clustering à partir de la version 11.1

Pour enregistrer la configuration à l'aide de la ligne de commande Citrix ADC, à l'invite de commandes, tapez :

```
>save config

>shell

root@ns# cd /nsconfig
```

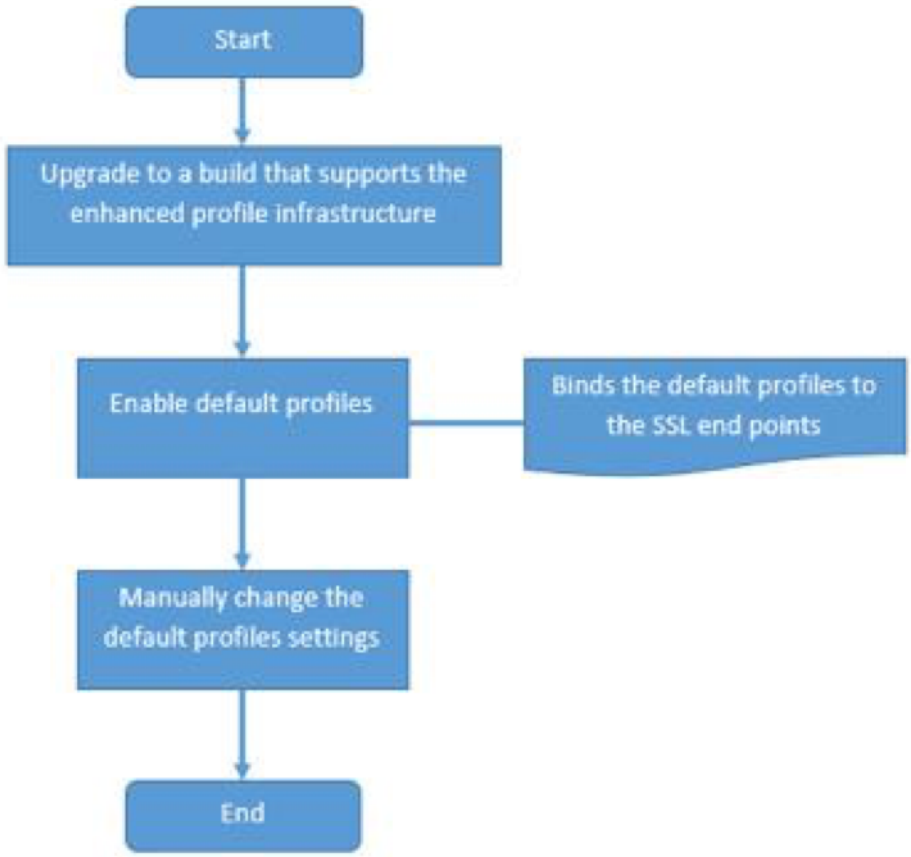


```
6
7 root@ns# cp ns.conf ns.conf.NS<currentreleasenumber><currentbuildnumber
     >
8 <!--NeedCopy-->
```

Cas d'utilisation 1

Après avoir activé les profils par défaut, ils sont liés à tous les points d'extrémité SSL. Les profils par défaut sont modifiables. Si votre déploiement utilise la plupart des paramètres par défaut et ne modifie que quelques paramètres, vous pouvez modifier les profils par défaut. Les changements sont immédiatement répercutés sur tous les points de fin.

L'organigramme suivant explique les étapes que vous devez effectuer :



1. Pour plus d'informations sur la mise à niveau du logiciel, reportez-vous à la section Mise à niveau du logiciel système.
2. Activez les profils par défaut à l'aide de la ligne de commande ou de l'interface graphique de Citrix ADC.

- Sur la ligne de commande, tapez : set ssl paramètre -DefaultProfile ENABLED
- Si vous préférez utiliser l'interface graphique, accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**, faites défiler vers le bas et sélectionnez **Activer le profil par défaut**.

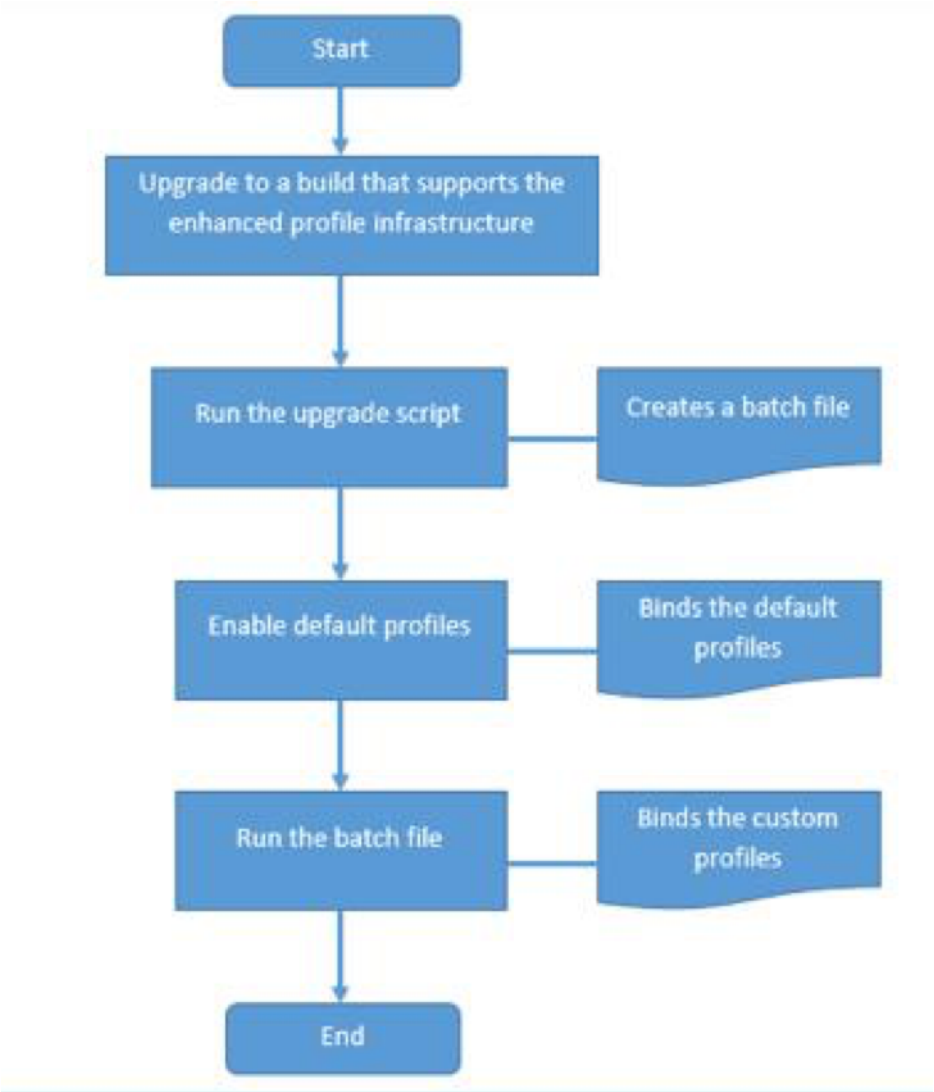
3. (Facultatif) Modifiez manuellement les paramètres du profil par défaut.

   - Sur la ligne de commande, tapez :`set ssl profile <name>` suivi des paramètres à modifier.
   - Si vous préférez utiliser l'interface graphique, accédez à **Système > Profils**. Dans Profils SSL, sélectionnez un profil et cliquez sur **Modifier**.

Cas d'utilisation 2

Si votre déploiement utilise des paramètres spécifiques pour la plupart des entités SSL, vous pouvez exécuter un script qui crée automatiquement des profils personnalisés pour chaque point final et les lie au point final. Utilisez la procédure décrite dans cette section pour conserver les paramètres SSL pour tous les points d'extrémité SSL de votre déploiement. Après la mise à niveau du logiciel, téléchargez et exécutez un script de migration pour capturer les modifications spécifiques à SSL. La sortie de l'exécution de ce script est un fichier batch. Activez les profils par défaut, puis appliquez les commandes dans le fichier de commandes. Voir l'annexe pour un exemple de migration de la configuration SSL après la mise à niveau.

L'organigramme suivant explique les étapes que vous devez effectuer :



1. Pour plus d'informations sur la mise à niveau du logiciel, reportez-vous à la section Mise à niveau du logiciel système.
2. Téléchargez et exécutez un script pour capturer les modifications spécifiques à SSL. Outre d'autres activités de migration, le script analyse l'ancien fichier ns.conf et déplace tous les paramètres spéciaux (autres que la valeur par défaut) d'une configuration de point d'extrémité SSL vers un profil personnalisé. Vous devez activer les profils par défaut après la mise à niveau pour que les modifications de configuration s'appliquent.

   Pour télécharger le script, connectez-vous àhttps://www.citrix.com/. Sous l'onglet **Téléchargements** , sélectionnez Citrix ADC, puis sélectionnez la version (par exemple, version 12.0). Dans la version, dans Firmware, sélectionnez une version. Le script de profil par défaut SSL est disponible dans les composants supplémentaires.

> **Remarque :** Lorsque vous exécutez le script de migration, vous pouvez choisir de générer automatiquement les noms de profil ou vous pouvez inviter l'utilisateur à entrer les noms de profil de manière interactive. Le script de migration vérifie ce qui suit et crée des fichiers pro en conséquence.
>
> - Points de fin avec les paramètres par défaut et les paramètres de chiffrement et de groupe de chiffrement similaires : Le script crée un profil.
> - Points de terminaison avec les paramètres par défaut et avec différents groupes de chiffrement ou priorités pour les groupes de chiffres/chiffrement : dans chaque cas, le script crée un groupe de chiffrement défini par l'utilisateur, le lie à un profil et lie chaque profil aux points d'extrémité appropriés.
> - Points de terminaison avec les paramètres par défaut et les chiffrements par défaut : un profil par défaut est lié au point de fin.

```
Pour exécuter le script, à l'invite de commandes, tapez :
```

```
./default_profile_script /nsconfig/ns.conf -b > <output file name
   >`
<!--NeedCopy-->
```

```
Vous devez exécuter cette commande à partir du dossier dans lequel
    vous stockez le script.
```

3. Activez les profils par défaut à l'aide de la ligne de commande ou de l'interface graphique de Citrix ADC.
   - Sur la ligne de commande, tapez : `set ssl parameter -defaultProfile ENABLED`
   - Si vous préférez utiliser l'interface graphique, accédez à **Gestion du trafic > SSL > Modifier les paramètres SSL avancés**, faites défiler vers le bas et sélectionnez **Activer le profil par défaut**.

Profils SSL personnalisés

Outre les profils SSL par défaut, les clients peuvent créer des profils SSL frontaux et principaux personnalisés pour des cas d'utilisation spécifiques. Il peut y avoir des scénarios où différentes applications nécessitent différents chiffrements et paramètres SSL. Dans ce cas, les clients peuvent créer de nouveaux profils et les lier aux points de terminaison.

Il n'y a pas de limite supérieure sur le nombre de profils personnalisés qui peuvent être créés dans un système.

Consultez la documentation Profils SSL pour plus d'informations sur l'activation des profils SSL et plus encore.

Profils frontaux SSL

Les profils SSL frontaux sont liés aux serveurs virtuels de type SSL et aux services internes. Les profils frontaux sont applicables à tous les serveurs virtuels de type SSL dans les catégories serveur virtuel d'équilibrage de charge, serveur virtuel de commutation de contenu, serveur virtuel AAA-TM et serveur virtuel Gateway VPN.

Les types de serveurs virtuels suivants prennent en charge les profils frontaux : SSL, SSL_TCP, SIP_SSL, SSL_FIX et SSL_DIAMETER.

Tous les services internes prennent en charge les profils frontaux.

Profils principaux SSL

Les profils principaux sont liés aux services de type SSL, aux groupes de services et aux moniteurs sécurisés. Les services et les groupes de services suivants prennent en charge les profils principaux : SSL, SSL_TCP, SIP_SSL, SSL_FIX, SSL_DIAMETER.

Certains moniteurs peuvent être configurés pour vérifier l'intégrité des serveurs principaux sur des connexions sécurisées. Les profils SSL peuvent être liés à de tels moniteurs pour configurer les paramètres SSL et les chiffrements. Ces moniteurs sont HTTP, HTTP-ECV, HTTP-INLINE, TCP et TCP-ECV.

Modèle de conception validé Citrix ADC et Amazon Web Services

January 8, 2020

Vue d'ensemble Citrix Networking VPX

Citrix ADC est un contrôleur de mise à disposition d'applications tout-en-un qui permet d'exécuter les applications jusqu'à cinq fois mieux, réduit les coûts de propriété des applications, optimise l'expérience utilisateur et garantit que les applications sont toujours disponibles à l'aide de :

- Services d'équilibrage de charge et gestion du trafic avancés de couche 4-7
- Accélération éprouvée des applications comme la compression HTTP et la mise en cache

- Un pare-feu intégré pour la sécurité des applications
- Déchargement des serveurs pour réduire considérablement les coûts et consolider les serveurs

En tant que leader incontesté de la fourniture de services et d'applications, Citrix ADC est déployé sur des milliers de réseaux à travers le monde pour optimiser, sécuriser et contrôler la fourniture de tous les services d'entreprise et de cloud. Déployé directement devant les serveurs Web et de base de données, Citrix ADC combine l'équilibrage de charge et la commutation de contenu à haute vitesse, la compression HTTP, la mise en cache de contenu, l'accélération SSL, la visibilité du flux d'applications et un puissant pare-feu applicatif dans une plate-forme intégrée et facile à utiliser. Il est beaucoup plus simple de respecter les SLA grâce à une surveillance de bout en bout qui transforme les données réseau en Business Intelligence exploitable. Citrix ADC permet de définir et de gérer les stratégies à l'aide d'un moteur de stratégie déclarative simple sans expertise en programmation requise.

Vue d'ensemble Citrix ADC dans Amazon Web Services

La prise en charge de Citrix Networking VPX dans Amazon Web Services (AWS) est disponible à partir de la version 10.5 — 61.11. Citrix Networking VPX est disponible en tant qu'Amazon Machine Image (AMI) sur AWS Marketplace. Citrix Networking VPX on AWS permet aux clients de tirer parti des capacités de cloud computing AWS et d'utiliser les fonctionnalités d'équilibrage de charge et de gestion du trafic de Citrix ADC pour leurs besoins professionnels. Citrix ADC sur AWS prend en charge toutes les fonctionnalités de gestion du trafic d'une appliance Citrix ADC physique. Les instances Citrix ADC exécutées dans AWS peuvent être déployées en tant qu'instances autonomes ou en tant que paires HA.

L'AMI Citrix Networking VPX est empaquetée en tant qu'instance EC2 lancée dans un VPC AWS. L'instance AMI VPX nécessite au moins 2 processeurs virtuels et 2 Go de mémoire. Une instance EC2 lancée dans un VPC AWS peut également fournir plusieurs interfaces, plusieurs adresses IP par interface et des adresses IP publiques et privées nécessaires à la configuration VPX. Actuellement, sur AWS, VPX ne peut être lancé que dans un VPC, car chaque instance VPX nécessite au moins trois adresses IP. (Bien que VPX sur AWS puisse être implémenté avec une ou deux interfaces réseau élastiques, Citrix recommande trois interfaces réseau pour une installation VPX standard sur AWS.) AWS rend actuellement la fonctionnalité multi-IP disponible uniquement pour les instances exécutées au sein d'un VPC AWS. Une instance VPX dans un VPC peut être utilisée pour équilibrer la charge des serveurs exécutant dans des instances EC2.

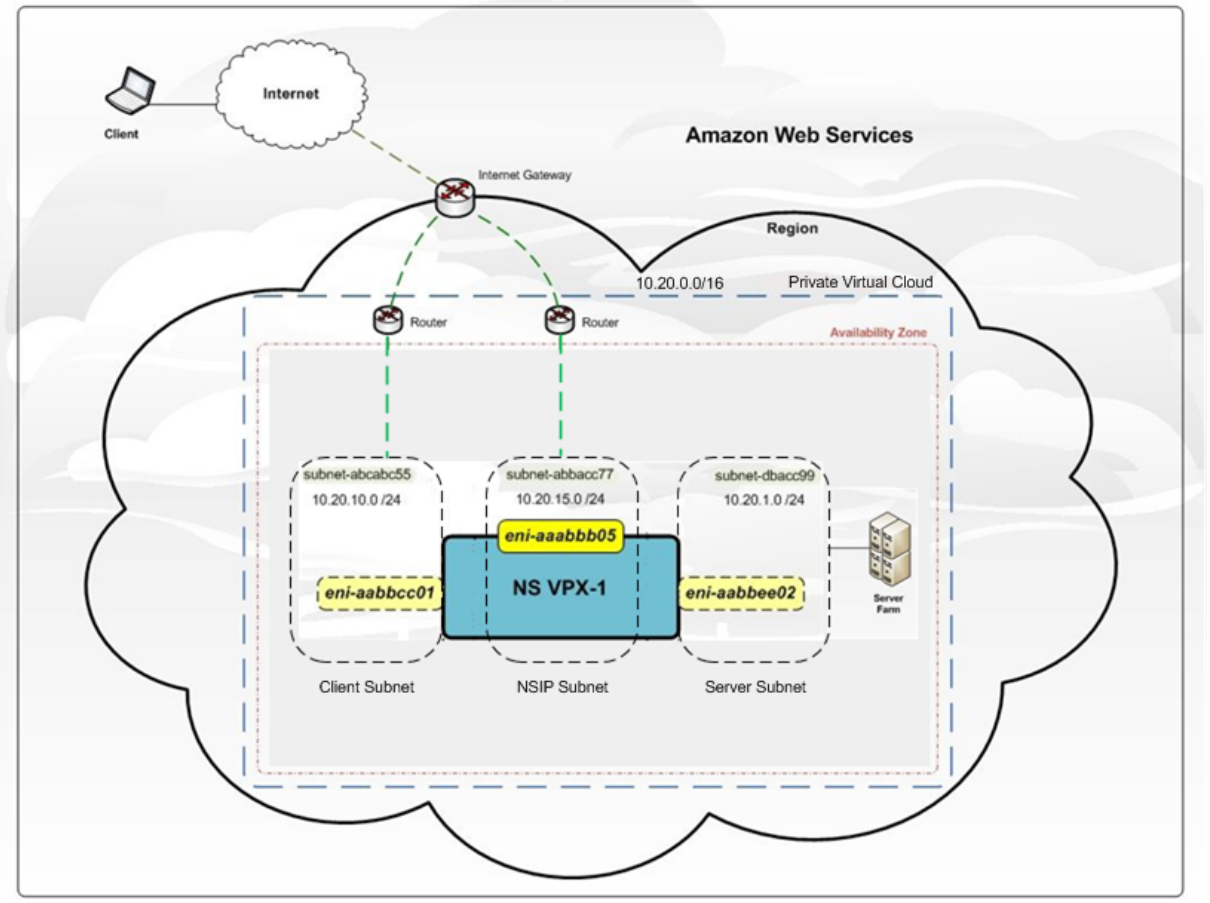
Un VPC Amazon vous permet de créer et de contrôler un environnement de réseau virtuel, y compris votre propre plage d'adresses IP, sous-réseaux, tables de routage et passerelles réseau.

> Remarque :
>
> Par défaut, vous pouvez créer jusqu'à 5 instances VPC par région AWS pour chaque compte AWS. Vous pouvez demander des limites de VPC plus élevées en soumettant

> Formulaire de demande d'Amazon.

Une instance EC2 de Citrix Networking VPX (image AMI) est lancée dans le VPC AWS.

La figure suivante montre un VPX typique sur le déploiement AWS.



La figure présente une topologie simple d'un VPC AWS avec un déploiement Citrix Networking VPX. Le VPC AWS dispose de :

1. Une passerelle Internet unique pour acheminer le trafic entrant et sortant du VPC.
2. Connectivité réseau entre la passerelle Internet et Internet.
3. Trois sous-réseaux, un pour la gestion, le client et le serveur.
4. Connectivité réseau entre la passerelle Internet et les deux sous-réseaux (gestion et client).
5. Citrix Networking VPX unique déployé dans le VPC. L'instance VPX dispose de trois interfaces réseau élastiques (ENI), une attachée à chaque sous-réseau.

Limitations et directives d'utilisation

- La fonctionnalité de clustering n'est pas prise en charge pour VPX.

- Pour que HA fonctionne comme prévu, associez un périphérique NAT dédié à l'interface de gestion ou associez EIP à NSIP. Pour plus d'informations sur NAT, consultez la documentation AWS Instances NAT.
- Le trafic de données et le trafic de gestion doivent être séparés en utilisant des ENI appartenant à différents sous-réseaux.
- Seule l'adresse du NSIP doit figurer sur l'IEN de gestion.
- Si une instance NAT est utilisée pour la sécurité au lieu d'affecter un EIP au NSIP, des modifications appropriées de routage au niveau du VPC sont requises. Pour obtenir des instructions sur les modifications de routage au niveau du VPC, consultez la documentation AWSScénario 2 : VPC avec sous-réseaux publics et privés.
- Une instance VPX peut être déplacée d'un type d'instance EC2 à un autre (par exemple, de m3.large à m3.xlarge).
- Pour les options de stockage pour VPX sur AWS, Citrix recommande EBS, car il est durable et les données sont disponibles même après avoir été détachées de l'instance.
- L'ajout dynamique d'ENI à VPX n'est pas pris en charge. Vous devez redémarrer l'instance VPX pour appliquer la mise à jour. Citrix vous recommande d'arrêter l'instance autonome ou HA, d'attacher la nouvelle ENI, puis de redémarrer l'instance.
- Vous pouvez attribuer plusieurs adresses IP à un ENI. Le nombre maximal d'adresses IP par ENI est déterminé par le type d'instance EC2, reportez-vous à la section Prise en charge EC2 des adresses ENI et IP.
- Citrix vous recommande d'éviter d'utiliser les commandes d'activation et de désactivation de l'interface sur les interfaces Citrix Networking VPX.

En raison des limitations AWS, ces fonctionnalités ne sont pas prises en charge :

Limites de la couche 3 :

- Routage dynamique
- IPV6

Limitations de la couche 2 :

- Gratuitous ARP (GARP)
- Mode L2
- VLAN taggé
- MAC virtuel (VMAC)

Instances EC2 prises en charge

L'AMI Citrix ADC peut être lancée sur l'un des types d'instance EC2 suivants :

- m4.large
- m4.xlarge
- m4.2xlarge

- m4.4xlarge
- m4.10xlarge
- m3.large
- m3.xlarge
- m3.2xlarge

Pour de plus amples informations, consultez Instances Amazon EC2

Prise en charge de l'ENI

Le tableau suivant répertorie les types d'instance EC2 et le nombre correspondant d'ENI pris en charge et le nombre d'adresses IP privées par ENI.

Nom de l'instance	Nombre d'ENIs	Adresses IP privées par ENI
m4.large	2.	10
m4.xlarge	4	15
m4.2xlarge	4	15
m4.4xlarge	8	30
m4.10xlarge	8	30
m3.large	3	10
m3.xlarge	4	15
m3.2xlarge	4	30

Cas d'utilisation

Comparé aux solutions alternatives qui nécessitent le déploiement de chaque service en tant qu'appliance virtuelle distincte, Citrix ADC sur AWS combine l'équilibrage de charge L4, la gestion du trafic L7, le déchargement du serveur, l'accélération des applications, la sécurité des applications et d'autres fonctionnalités essentielles de livraison d'applications dans un seul VPX , facilement disponible via AWS Marketplace. En outre, tout est régi par un cadre de stratégie unique et géré avec le même ensemble puissant d'outils utilisés pour administrer les déploiements Citrix ADC locaux. Le résultat net est que Citrix ADC sur AWS permet plusieurs cas d'utilisation convaincants qui prennent en charge non seulement les besoins immédiats des entreprises d'aujourd'hui, mais aussi l'évolution continue des infrastructures informatiques héritées aux centres de données cloud d'entreprise.

Livraison de production pour les applications Web et virtuelles et les applications de bureau

Les entreprises qui adoptent activement AWS comme une offre d'infrastructure en tant que service (IaaS) pour la livraison de production d'applications peuvent désormais être en première ligne de ces applications avec la même plate-forme de mise en réseau cloud utilisée par les plus grands sites Web et fournisseurs de services cloud au monde. Les capacités étendues de déchargement, d'accélération et de sécurité peuvent être exploitées pour améliorer les performances et réduire les coûts.

XenDesktop 7.5 et XenApp 7.5 ont été redessinés en tant que solutions compatibles avec le cloud pour fournir n'importe quelle application Windows ou bureau dans un service cloud fourni sur n'importe quel réseau, sur n'importe quel appareil. En déployant aujourd'hui cette plateforme étendue d'applications et de postes de travail, vous vous positionnez pour tirer parti de toute infrastructure virtuelle ou plate-forme de gestion du cloud. Cela vous donne la possibilité de tirer parti des capacités d'automatisation et d'orchestration du cloud computing.

Conceptions cloud hybrides

Les organisations informatiques d'entreprise qui suivent une stratégie de cloud hybride obtiennent le meilleur des deux mondes en sélectionnant les applications et les scénarios d'utilisation les mieux adaptés à leur cloud privé et ceux qui s'intègrent le mieux dans un cloud public, ce qui leur permet de s'adapter, de grandir et de se transformer pour répondre aux exigences du milieu de travail moderne.

Avec Citrix ADC sur AWS, les clouds hybrides qui couvrent les centres de données d'entreprise et s'étendent à AWS peuvent bénéficier de la même plate-forme de mise en réseau cloud. Citrix ADC facilite considérablement la transition des applications et des charges de travail entre un centre de données privé et AWS. La suite complète de fonctionnalités, allant de l'équilibrage intelligent de charge de base de données avec DataStream à la visibilité sans précédent des applications avec AppFlow®, en passant par la surveillance et la réponse en temps réel avec Action Analytics, peut être exploitée avec Citrix ADC sur AWS.

Continuité des activités

Les entreprises souhaitant utiliser AWS dans le cadre de leurs plans de reprise après sinistre et de continuité d'activité peuvent compter sur l'équilibrage global de la charge du serveur Citrix ADC exécutant tant tant sur site qu'au sein d'AWS pour surveiller en permanence la disponibilité et les performances des centres de données d'entreprise et des environnements AWS, garantissant ainsi aux utilisateurs sont toujours envoyés à l'emplacement optimal.

Lorsque vous configurez GSLB sur les appliances Citrix ADC et activez Metric Exchange Protocol (MEP), les solutions matérielles-logicielles utilisent l'infrastructure DNS pour connecter le client au centre de données qui répond le mieux aux critères que vous définissez. Les critères peuvent désigner le centre de données le moins chargé, le centre de données le plus proche, le centre de données qui répond

le plus rapidement aux demandes de l'emplacement du client, une combinaison de ces mesures et des mesures SNMP. Une solution matérielle-logicielle assure le suivi de l'emplacement, des performances, de la charge et de la disponibilité de chaque centre de données et utilise ces facteurs pour sélectionner le centre de données auquel envoyer une demande client. Une configuration GSLB consiste en un groupe d'entités GSLB sur chaque appliance de la configuration. Ces entités comprennent les sites GSLB, les services GSLB, les serveurs virtuels GSLB, les serveurs d'équilibrage de charge et/ou de commutation de contenu, et les services ADNS.

Développement et test

Les entreprises exécutent des livraisons de production sur site, mais l'utilisation d'AWS pour le développement et les tests peut désormais inclure Citrix ADC dans leurs environnements de test AWS, accélérant ainsi les délais de production grâce à une meilleure mise en œuvre de la production dans leurs environnements de test.

Dans chaque cas d'utilisation, les architectes réseau peuvent également tirer parti de Citrix CloudBridge, configuré en tant qu'instance autonome ou en tant que fonctionnalité d'une instance Citrix ADC Platinum Edition, pour sécuriser et optimiser la connexion entre un ou plusieurs centres de données d'entreprise et le cloud AWS, ce qui accélère le transfert de données/ la synchronisation et la réduction des coûts réseau.

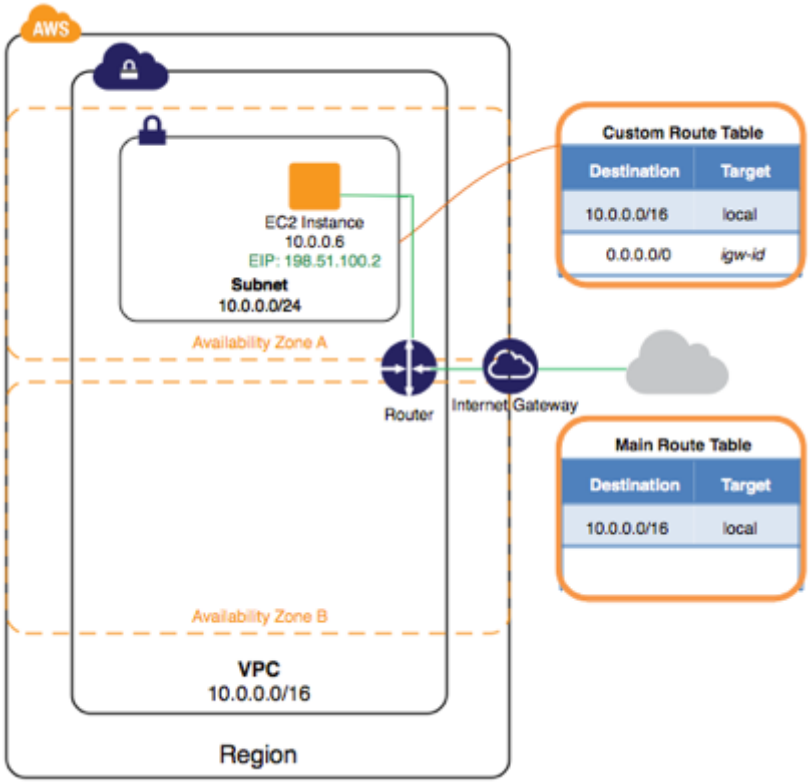
Architecture réseau AWS — ENI et EIP

Les instances Citrix ADC lancées dans un VPC peuvent avoir jusqu'à huit interfaces réseau élastiques (ENI). À son tour, chaque ENI peut se voir attribuer une ou plusieurs adresses IP privées, chacune de ces adresses étant éventuellement mappée à une adresse IP élastique qui est publiquement routable.

Ce qui rend les interfaces réseau et les adresses IP « élastiques » dans ce cas, c'est la possibilité de les remapper par programmation à d'autres instances, une fonctionnalité qui permet la récupération à partir de défaillances d'instance ou de zone de disponibilité sans avoir à attendre les remplacements matériels ou que les modifications DNS se propagent complètement à tous vos clients.

Les autres détails à prendre en compte sont les suivants :

- Une instance peut avoir des ENI différentes dans différents sous-réseaux (mais pas dans différentes zones de disponibilité).
- Chaque ENI doit avoir au moins une adresse IP qui lui est attribuée et doit être attribuée à un groupe de sécurité (voir ci-dessous).
- Les adresses 1 à 4 pour chaque sous-réseau (c'est-à-dire 10.x.1-4) sont réservées à l'utilisation par Amazon.
- Citrix ADC connaît uniquement les adresses IP privées. Les EIP qui sont affectés ne s'affichent pas dans l'interface de ligne de commande Citrix ADC ou dans les outils de gestion associés.



EC2 versus VPC

AWS englobe plusieurs services différents, tels qu'Amazon Simple Storage Services (S3), Amazon Elastic Compute Cloud (EC2) et Amazon Virtual Private Cloud (VPC). La distinction entre ces deux derniers est importante en l'espèce. En particulier, avec EC2, les instances de machine virtuelle sont limitées à une seule interface réseau et une seule adresse IP. En outre, il y a un minimum de fonctionnalités et de contrôles de mise en réseau. Cela exclut l'utilisation d'EC2 pour Citrix ADC - qui nécessite au moins trois adresses IP - et c'est pourquoi les instances de Citrix ADC ne peuvent être lancées que dans un VPC AWS.

Les VPC prennent en charge non seulement les machines virtuelles avec plusieurs interfaces et plusieurs adresses IP privées et publiques, mais vous permettent également de créer et de contrôler un environnement de réseau virtuel isolé, avec sa propre plage d'adresses IP, ses sous-réseaux, ses tables de routage et ses passerelles réseau.

Régions et zones de disponibilité

Dans le cloud AWS, les régions font référence à un emplacement géographique spécifique, tel que USA Est. Dans chaque région, il existe au moins deux zones de disponibilité, chacune pouvant être considérée comme un centre de données cloud indépendant conçu pour être isolé des pannes dans

d'autres zones de disponibilité et pour fournir une connectivité réseau peu coûteuse et à faible latence à d'autres zones de disponibilité dans le même région.

En implémentant des instances dans des zones de disponibilité distinctes, vous pouvez protéger vos applications contre les défaillances qui affectent un seul emplacement.

Les limitations et les dépendances dont les architectes de réseau doivent tenir compte à ce niveau sont les suivantes :

- Bien qu'un cloud privé virtuel puisse couvrir plusieurs zones de disponibilité, il ne peut pas couvrir plusieurs régions.
- Les sous-réseaux individuels d'un VPC ne peuvent pas couvrir plusieurs zones de disponibilité.
- Tout le trafic entrant ou sortant d'un VPC doit être acheminé via une passerelle Internet par défaut correspondante

---

Configurer VPX sur AWS

Dans cet exercice, vous allez créer un VPC et un sous-réseau et lancer une instance orientée vers le public dans votre sous-réseau. Votre instance sera en mesure de communiquer avec Internet et vous pourrez accéder à votre instance depuis votre ordinateur local en utilisant SSH (s'il s'agit d'une instance Linux) ou Bureau à distance (s'il s'agit d'une instance Windows). Dans votre environnement réel, vous pouvez utiliser ce scénario pour créer un serveur Web public, par exemple pour héberger un blog.

> Remarque :
>
> Cet exercice est destiné à vous aider à configurer rapidement votre propre VPC non par défaut. Si vous avez déjà un VPC par défaut et que vous voulez commencer à lancer des instances dedans (et non pas créer ou configurer un nouveau VPC), reportez-vous à la section Lancement d'une instance EC2 dans votre VPC par défaut.

Pour terminer cet exercice, procédez comme suit :

- Créez un VPC autre que par défaut avec un seul sous-réseau public. Les sous-réseaux vous permettent de regrouper les instances en fonction de vos besoins opérationnels et de sécurité. Un sous-réseau public est un sous-réseau qui a accès à Internet via une passerelle Internet.
- Créez un groupe de sécurité pour votre instance qui autorise le trafic uniquement via des ports spécifiques.
- Lancez une instance Amazon EC2 dans votre sous-réseau.
- Associez une adresse IP Elastic à votre instance. Cela permet à votre instance d'accéder à Internet.

Avant de pouvoir utiliser Amazon VPC pour la première fois, vous devez vous inscrire à AWS. Lorsque vous vous inscrivez, votre compte AWS est automatiquement inscrit pour tous les services d'AWS, y

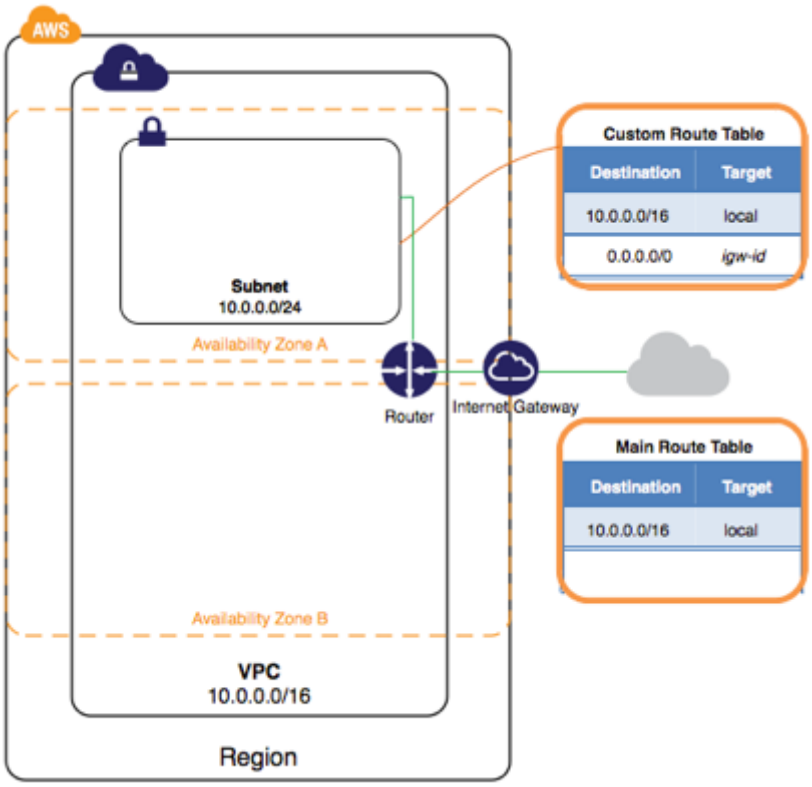
compris Amazon VPC. Si vous n'avez pas encore créé de compte AWS, accédez àhttp://aws.amazon.com, puis choisissez **Créer un compte gratuit**.

Étape 1 : Créer le VPC

Dans cette étape, vous allez utiliser l'assistant Amazon VPC dans la console Amazon VPC pour créer un VPC. L'Assistant effectue les étapes suivantes pour vous :

- Crée un VPC avec un bloc CIDR /16 (un réseau avec 65 536 adresses IP privées). Pour plus d'informations sur la notation CIDR et le dimensionnement d'un VPC, consultez Votre VPC.
- Attache une passerelle Internet au VPC. Pour plus d'informations sur les passerelles Internet, reportez-vous à la section Passerelles Internet.
- Crée un sous-réseau de taille /24 (une plage de 256 adresses IP privées) dans le VPC.
- Crée une table de routage personnalisée et l'associe à votre sous-réseau afin que le trafic puisse circuler entre le sous-réseau et la passerelle Internet. Pour plus d'informations sur les tables de routage, reportez-vous à la section Tables de routage.

Le diagramme suivant représente l'architecture de votre VPC une fois cette étape terminée.

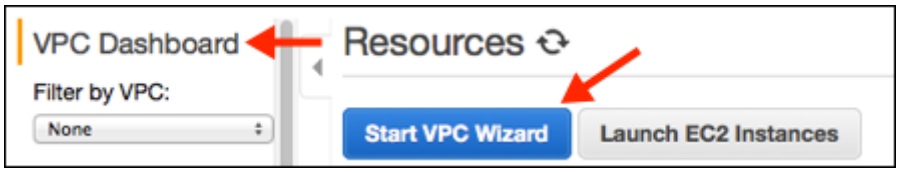


Créer un VPC à l'aide de l'Assistant Amazon VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.

2. Dans la barre de navigation, en haut à droite, prenez note de la région dans laquelle vous allez créer le VPC. Assurez-vous de continuer à travailler dans la même région pour le reste de cet exercice, car vous ne pouvez pas lancer une instance dans votre VPC à partir d'une autre région. Pour plus d'informations sur les régions, reportez-vous à la section Régions et zones de disponibilité.

3. Dans le volet de navigation, choisissez Tableau de **bord VPC**, puis choisissez **Démarrer VPC Wizard**.



> Remarque :
>
> Ne sélectionnez pas Vos VPC dans le volet de navigation ; vous ne pouvez pas accéder à l'assistant VPC à partir de cette page.

4. Choisissez la première option, **VPC avec un sous-réseau public unique**, puis sélectionnez **Sélectionner**.

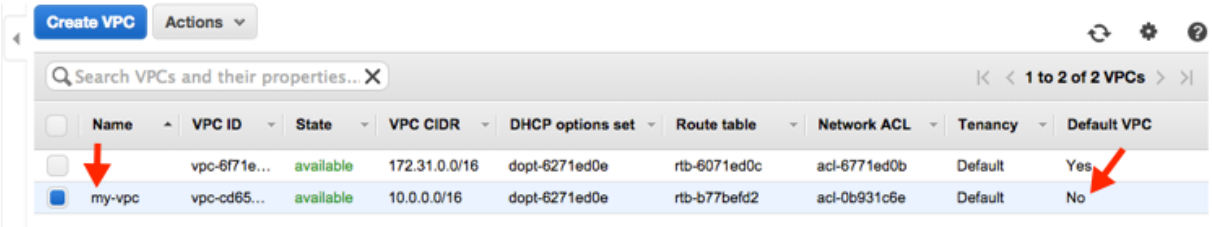
5. Sur la page de configuration, entrez un nom pour votre VPC dans le champ Nom du VPC ; par exemple, my-vpc, puis entrez un nom pour votre sous-réseau dans le champ Nom du **sous-réseau** . Cela vous aide à identifier le VPC et le sous-réseau dans la console Amazon VPC après les avoir créés. Pour cet exercice, vous pouvez laisser le reste des paramètres de configuration sur la page et choisir **Créer un VPC**.

   (Facultatif) Si vous préférez, vous pouvez modifier les paramètres de configuration comme suit, puis choisir **Créer un VPC**.

   - Le bloc CIDR IP affiche la plage d'adresses IP que vous utiliserez pour votre VPC (10.0.0.0/16) et le champ Sous-réseau public affiche la plage d'adresses IP que vous utiliserez pour le sous-réseau (10.0.0.0/24). Si vous ne souhaitez pas utiliser les plages CIDR par défaut, vous pouvez spécifier les vôtres. Pour plus d'informations, reportez-vous à la section Dimensionnement du VPC et du sous-réseau.
   - La liste Zone de disponibilité vous permet de sélectionner la zone de disponibilité dans laquelle créer le sous-réseau. Vous pouvez laisser Aucune préférence pour laisser AWS choisir une zone de disponibilité pour vous. Pour plus d'informations, reportez-vous à la section Régions et zones de disponibilité.
   - Dans la section Ajouter des points de terminaison pour S3 à vos sous-réseaux, vous pouvez sélectionner un sous-réseau dans lequel créer un point de terminaison VPC vers Amazon S3 dans la même région. Pour plus d'informations, reportez-vous à la section Points de terminaison VPC.

- L'`Enable DNS hostnames` option, lorsqu'elle est définie sur Oui, garantit que les instances qui sont lancées dans votre VPC reçoivent un nom d'hôte DNS. Pour plus d'informations, reportez-vous à la section Utilisation de DNS avec votre VPC.
- L'option de location de matériel vous permet de déterminer si les instances lancées dans votre VPC sont exécutées sur du matériel partagé ou dédié. La sélection d'une location dédiée entraîne des coûts supplémentaires. Pour plus d'informations sur la location de matériel, reportez-vous à la section Instances dédiées.

6. Une fenêtre d'état affiche le travail en cours. Lorsque le travail est terminé, cliquez **sur OK** pour fermer la fenêtre d'état.
7. Le`Your VPCs page` affiche votre VPC par défaut et le VPC que vous venez de créer. Le VPC que vous avez créé n'est pas un VPC par défaut. Par conséquent, la colonne **VPC par défaut** affiche Non.



Afficher les informations sur votre VPC

Après avoir créé le VPC, vous pouvez afficher des informations sur le sous-réseau, la passerelle Internet et les tables de routage. Le VPC que vous avez créé possède deux tables de routage : une table de routage principale que tous les VPC possèdent par défaut et une table de routage personnalisée créée par l'Assistant. La table de routage personnalisée est associée à votre sous-réseau, ce qui signifie que les itinéraires de cette table déterminent le flux du trafic pour le sous-réseau. Si vous ajoutez un nouveau sous-réseau à votre VPC, il utilise la table de routage principale par défaut.

Pour afficher des informations sur votre VPC

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez **Vos VPC**. Prenez note du nom et de l'ID du VPC que vous avez créé (regardez dans les colonnes Nom et ID de VPC). Vous utiliserez ces informations pour identifier les composants associés à votre VPC.
3. Dans le volet de navigation, choisissez **Sous-réseaux**. La console affiche le sous-réseau créé lors de la création de votre VPC. Vous pouvez identifier le sous-réseau par son nom dans la colonne **Nom** , ou vous pouvez utiliser les informations VPC que vous avez obtenues à l'étape précédente et regarder dans la colonne VPC.
4. Dans le volet de navigation, choisissez **Gateways Internet**. Vous pouvez trouver la passerelle Internet associée à votre VPC en regardant la colonne VPC, qui affiche l'ID et le nom (le cas

échéant) du VPC.

5. Dans le volet de navigation, choisissez **Tables de routage**. Deux tables de routage sont associées au VPC. Sélectionnez la table de routage personnalisée (la colonne Principal affiche Non), puis choisissez l'onglet Itinéraires pour afficher les informations de routage dans le volet d'informations :
   - La première ligne de la table est la route locale, qui permet aux instances du VPC de communiquer. Cette route est présente dans chaque table de routage par défaut, et vous ne pouvez pas la supprimer.
   - La deuxième ligne indique l'itinéraire que l'assistant Amazon VPC a ajouté pour permettre au trafic destiné à une adresse IP en dehors du VPC (0.0.0.0/0) de passer du sous-réseau à la passerelle Internet.
6. Sélectionnez la table de routage principale. La table de routage principale a un itinéraire local, mais pas d'autres itinéraires.

Étape 2 : Créer un groupe de sécurité 12

Un groupe de sécurité agit comme un pare-feu virtuel pour contrôler le trafic de ses instances associées. Pour utiliser un groupe de sécurité, vous ajoutez les règles entrantes pour contrôler le trafic entrant vers l'instance, et les règles sortantes pour contrôler le trafic sortant de votre instance. Pour associer un groupe de sécurité à une instance, vous spécifiez le groupe de sécurité lorsque vous lancez l'instance. Si vous ajoutez et supprimez des règles du groupe de sécurité, nous appliquons automatiquement ces modifications aux instances associées au groupe de sécurité.

Votre VPC est livré avec un groupe de sécurité par défaut. Toute instance non associée à un autre groupe de sécurité lors du lancement est associée au groupe de sécurité par défaut. Dans cet exercice, vous allez créer un nouveau groupe de sécurité, WebServerSG, et spécifier ce groupe de sécurité lorsque vous lancez une instance dans votre VPC.

Sujets

- Création de votre groupe de sécurité WebServerSG
- Règles pour le groupe de sécurité WebServerSG

Création de votre groupe de sécurité WebServerSG

Vous pouvez créer votre groupe de sécurité à l'aide de la console Amazon VPC.

Règles pour le groupe de sécurité WebServerSG

Le tableau suivant décrit les règles entrantes et sortantes pour le groupe de sécurité WebServerSG. Vous allez ajouter les règles entrantes vous-même. La règle sortante est une règle par défaut qui autorise toutes les communications sortantes vers n'importe où. Vous n'avez pas besoin d'ajouter cette règle vous-même.

Entrant			
IP source	Protocole	Portée des ports	Commentaires
0.0.0.0/0	TCP	80	Permet l'accès HTTP entrant de n'importe où.
0.0.0.0/0	TCP	443	Permet l'accès HTTPS entrant de n'importe où.
Plage d'adresses IP publique de votre réseau domestique	TCP	22	Permet l'accès SSH entrant de votre réseau domestique à une instance Linux/UNIX.
Plage d'adresses IP publique de votre réseau domestique	TCP	3389	Permet l'accès RDP entrant de votre réseau domestique à une instance Windows.

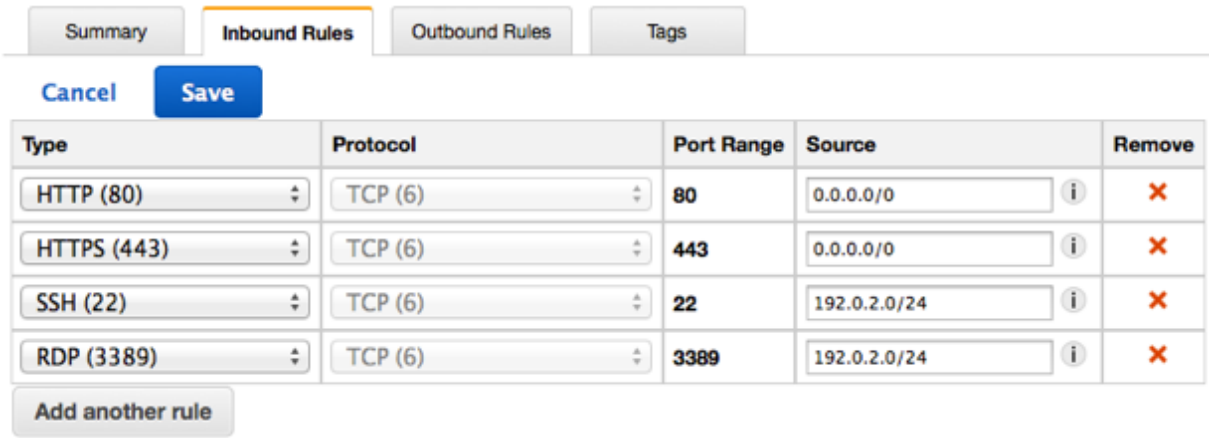
Sortant			
IP de destination	Protocole	Portée des ports	Commentaires
0.0.0.0/0	Tous	Tous	Règle de sortie de stock par défaut qui autorise toutes les communications sortantes.

Pour créer le groupe de sécurité WebServersG et ajouter des règles

1. Ouvrez la console Amazon VPC à l'adresse https://aws.amazon.com/console/.
2. Dans le volet de navigation, choisissez **Groupes de sécurité**.
3. Choisissez **Créer un groupe de sécurité**.
4. Dans le champ Nom du groupe, entrez WebServersG comme nom du groupe de sécurité et fournissez une description. Vous pouvez éventuellement utiliser le champ Nom balise pour créer une balise pour le groupe de sécurité avec une clé Nom et une valeur que vous spécifiez.
5. Sélectionnez l' **ID de votre VPC** dans le menu VPC, puis choisissez **Yes** , **Create** .

6. Sélectionnez le **groupe de sécurité WebServersG** que vous venez de créer (vous pouvez afficher son nom dans la colonne Nom du groupe).
7. Sous l' **onglet Règles d'entrée en stock**, choisissez **Modifier**et ajouter des règles pour le trafic entrant comme suit, puis choisissez **Enregistrer**lorsque vous avez terminé :
    - Sélectionnez **HTTP** dans la liste Type et entrez **0.0.0.0/0** dans le champ **Source** .
    - Choisissez **Ajouter une autre règle**, puis sélectionnez **HTTPS**dans la liste Type et entrez **0.0.0.0/0**dans le champ **Source**.
    - Choisissez **Ajouter une autre règle**. Si vous lancez une instance Linux, sélectionnez **SSH** dans la liste Type ou si vous lancez une instance Windows, sélectionnez **RDP** dans la liste Type. Entrez la plage d'adresses IP publiques de votre réseau dans le champ **Source** . Si vous ne connaissez pas cette plage d'adresses, vous pouvez utiliser 0.0.0.0/0 pour cet exercice.

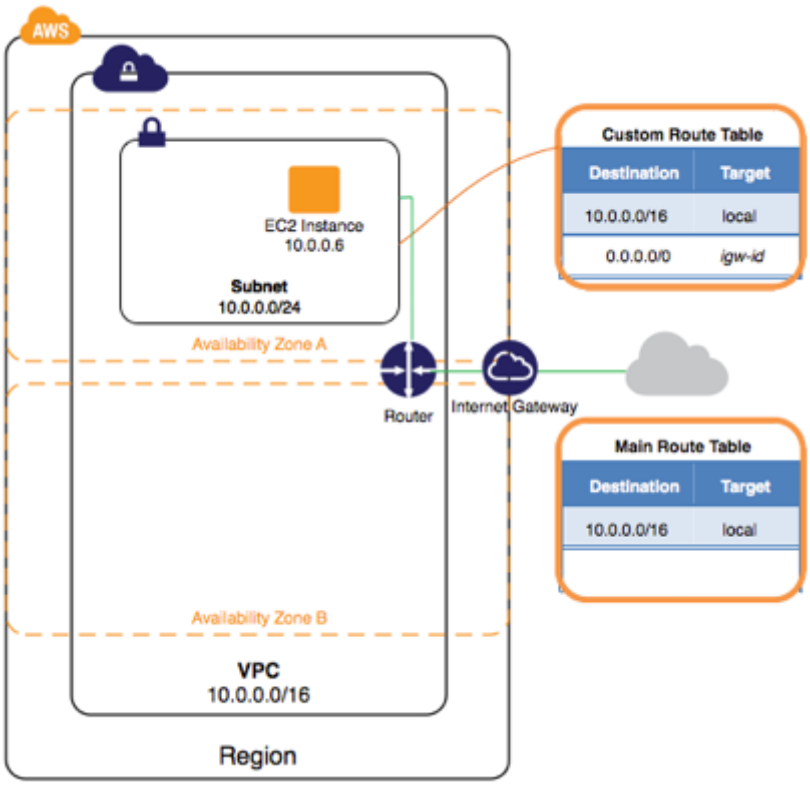
> Attention :
>
> Si vous utilisez 0.0.0.0/0, vous activez toutes les adresses IP pour accéder à votre instance à l'aide de SSH ou RDP. Ceci est acceptable pour l'exercice court, mais ce n'est pas sûr pour les environnements de production. En production, vous n'autorisez qu'une adresse IP spécifique ou une plage d'adresses à accéder à votre instance.



Étape 3 : Lancez une instance dans votre VPC 14

Lorsque vous lancez une instance EC2 dans un VPC, vous devez spécifier le sous-réseau dans lequel lancer l'instance. Dans ce cas, vous lancerez une instance dans le sous-réseau public du VPC que vous avez créé. Vous allez utiliser l'assistant de lancement d'Amazon EC2 dans la console Amazon EC2 pour lancer votre instance.

Le diagramme suivant représente l'architecture de votre VPC une fois cette étape terminée.



Pour lancer une instance EC2 dans un VPC

1. Ouvrez leConsole Amazon EC2.
2. Dans la barre de navigation, en haut à droite, assurez-vous de sélectionner la même région dans laquelle vous avez créé votre VPC et votre groupe de sécurité.
3. Dans le tableau de bord, choisissez **Launch Instance**.
4. Sur la première page de l'Assistant, choisissez l'AMI que vous souhaitez utiliser. Pour cet exercice, nous vous recommandons de choisir une **AMI Amazon Linux** ou une **AMI Windows** .
5. Sur la page **Choisir un type d'instance** , vous pouvez sélectionner la configuration matérielle et la taille de l'instance à lancer. Par défaut, l'Assistant sélectionne le premier type d'instance disponible en fonction de l'AMI que vous avez sélectionnée. Vous pouvez laisser la sélection par défaut, puis choisir **Suivant : Configurer les détails de l'instance**.
6. Dans la page **Configurer les détails de l'instance** , sélectionnez le **VPC** que vous avez créé dans la liste Réseau et le sous-réseau dans la liste **Sous-réseau** . Laissez le reste des paramètres par défaut et passez par les pages suivantes de l'Assistant jusqu'à ce que vous arriviez à la page Instance de balise.
7. Sur la page **Tag Instance** , vous pouvez marquer votre instance avec une balise Name ; par exemple, Name = MyWebServer. Cela vous aide à identifier votre instance dans la console Amazon EC2 après l'avoir lancée. Choisissez **Suivant : Configurer le groupe de sécurité** lorsque vous avez terminé.
8. Sur la page **Configurer un groupe de sécurité** , l'Assistant définit automatiquement le groupe

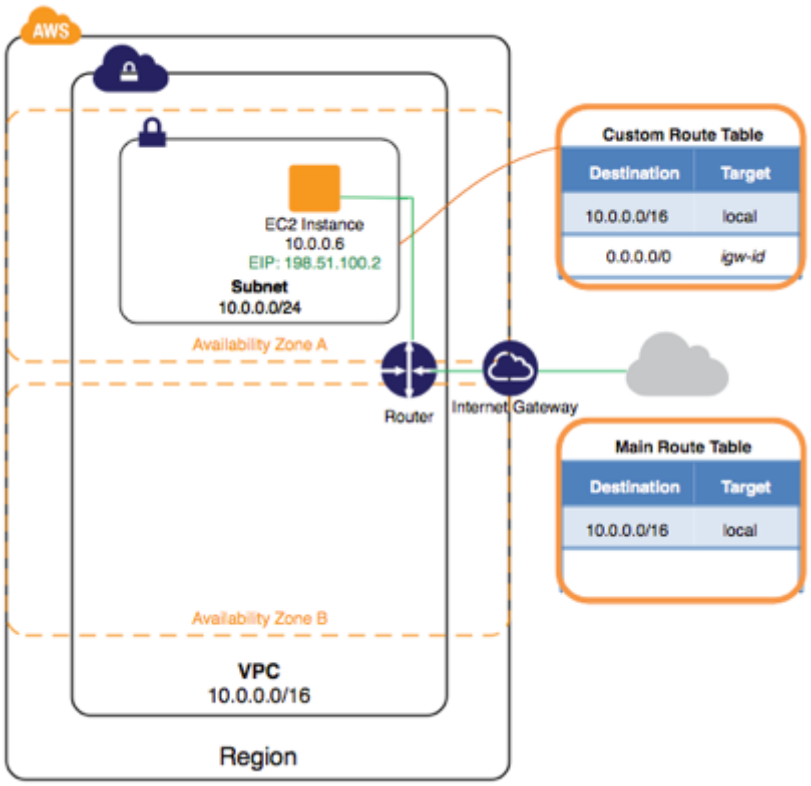
de sécurité launch-wizard-x pour vous permettre de vous connecter à votre instance. Choisissez plutôt l'option Sélectionner un groupe de sécurité existant, sélectionnez le groupe WebServersG que vous avez créé précédemment, puis choisissez **Réviser et Lancer**.

9. Sur la page **Vérifier le lancement de l'instance** , vérifiez les détails de votre instance, puis choisissez **Lancer** .
10. Dans la boîte de dialogue **Sélectionner une paire de clés existanteou créer une paire** de clés, vous pouvez choisir une paire de clés existante ou en créer une nouvelle. Si vous créez une nouvelle paire de clés, assurez-vous de télécharger le fichier et de le stocker dans un emplacement sécurisé. Vous aurez besoin du contenu de la clé privée pour vous connecter à votre instance après son lancement. Pour lancer votre instance, activez la case à cocher Accusé de réception, puis choisissez **Lancer les instances**.
11. Sur la page de confirmation, choisissez **Afficher les instances** pour afficher votre instance sur la page **Instances** . Sélectionnez votre instance et affichez ses détails dans l'onglet **Description** . Le champ IP privé affiche l'adresse IP privée attribuée à votre instance à partir de la plage d'adresses IP de votre sous-réseau.

Étape 4 : Attribuer une adresse IP élastique à votre instance

À l'étape précédente, vous avez lancé votre instance dans un sous-réseau public - un sous-réseau qui a un itinéraire vers une passerelle Internet. Toutefois, l'instance de votre sous-réseau a également besoin d'une adresse IP publique pour pouvoir communiquer avec Internet. Par défaut, une instance d'un VPC autre que par défaut n'est pas affectée d'adresse IP publique. Dans cette étape, vous allez allouer une adresse IP Elastic à votre compte, puis l'associer à votre instance. Pour plus d'informations sur les adresses IP Elastic, reportez-vous à la section Adresses IP élastiques.

Le diagramme suivant représente l'architecture de votre VPC une fois cette étape terminée.



Pour allouer et affecter une adresse IP Elastic

1. Ouvrez la console Amazon VPC à l'adresse https://console.aws.amazon.com/vpc/.
2. Dans le volet de navigation, choisissez **Elastic IP**.
3. Choisissez **Allouer une nouvelle adresse**, puis **Oui**, Allouer.

   > Remarque :
   >
   > Si votre compte prend en charge EC2-Classic, sélectionnez d'abord **EC2-VPC** dans la liste Plateforme réseau.

4. Sélectionnez l' **adresse IP élastique** dans la liste, choisissez **Actions** , puis **Associer Address** .
5. Dans la boîte de dialogue, choisissez **Instance** dans la **liste Associer avec** , puis sélectionnez votre **instance dans la liste Instance** . Sélectionnez **Oui**, Associer lorsque vous avez terminé.

Votre instance est désormais accessible depuis Internet. Vous pouvez vous connecter à votre instance via son adresse IP Elastic en utilisant SSH ou Remote Desktop à partir de votre réseau domestique. Pour plus d'informations sur la connexion à une instance Linux, reportez-vousConnexion à votre instance Linuxau manuel Amazon EC2 User Guide for Linux Instances. Pour plus d'informations sur la connexion à une instance Windows, reportez-vousSe connecter à votre instance Windows à l'aide de RDPau manuel Amazon EC2 User Guide for Windows Instances.

Ceci termine l'exercice ; vous pouvez choisir de continuer à utiliser votre instance dans votre VPC, ou si vous n'en avez pas besoin, vous pouvez la résilier et libérer son adresse IP Elastic pour éviter d'engager

des frais pour eux. Vous pouvez également supprimer votre VPC — notez que vous n'êtes pas facturé pour les composants VPC et VPC créés dans cet exercice (tels que les sous-réseaux et les tables de routage).

Configurer Unified Gateway pour Citrix Virtual Apps and Desktops

Accédez à la console d'administration de votre Citrix ADC.

Connectez-vous à Citrix ADC à l'aide de nsroot et de l'ID d'instance attribué par AWS au cours du processus de génération.

Installer le certificat SSL :

1. Accédez à **Gestion du trafic — SSL**. Cliquez avec le bouton droit de la souris et activez cette fonctionnalité.
2. Importer un certificat SSL une paire de clés.

Installer le certificat SSL :

1. Développez Citrix Gateway et sélectionnez **Serveurs virtuels**.
2. Cliquez sur **Ajouter**.

   Entrez un nom pour la passerelle et l'adresse IP qui se trouvent dans le sous-réseau public que vous avez attribué au cours du processus de génération Citrix ADC.

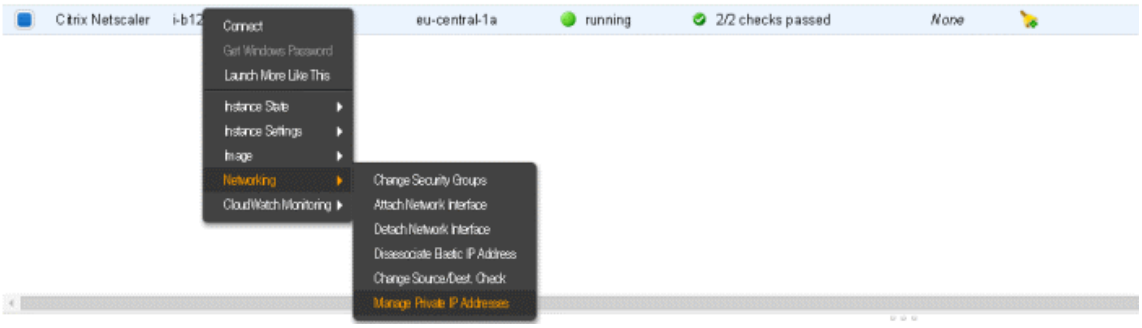
   > NOTE :
   >
   > Notez cette adresse IP comme nous en avons besoin lors de l'allocation des adresses IP élastiques plus tard.

3. Cliquez sur **OK**, puis sur **Aucun certificat de serveur**, puis sélectionnez le certificat que vous avez importé précédemment. Cliquez sur **Liaison**.
4. Cliquez sur **OK** et **Terminé** , et à ce stade, vous devriez afficher un Citrix Gateway dans un état « Up ».

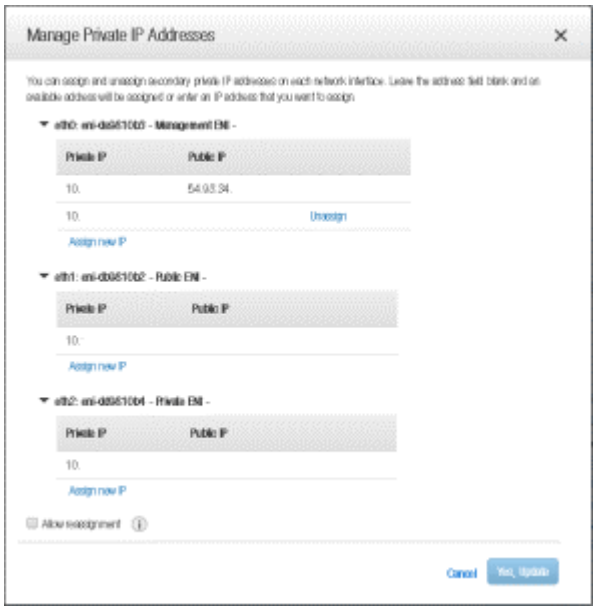
Pour configurer Unified Gateway, reportez-vous à la section https://support.citrix.com/article/CTX205485.

Fournir un accès externe à l'instance Unified Gateway :

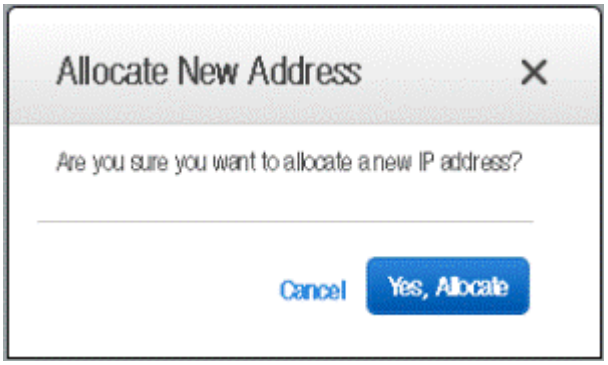
1. Connectez-vous à votre portail AWS sur aws.amazon.com et accédez à vos instances.
2. Cliquez avec le bouton droit sur votre Citrix ADC, sélectionnez **Mise en réseau** , puis **Gérer les adresses IP privées** .



3. Cliquez sur **Affecter une nouvelle adresse IP** sur l'interface sur laquelle vous souhaitez exécuter Citrix ADC Gateway.
4. Affectez l'adresse IP, assurez-vous d'utiliser la même adresse que vous avez attribuée à votre Citrix ADC Gateway.



5. Cliquez sur **Oui Mettre à jour**. Cela affectera la nouvelle adresse IP à l'instance au niveau AWS. Vous pouvez maintenant attribuer une nouvelle adresse IP Elastic à cette adresse IP privée.
6. Accédez à Network and Security et Elastic IP.
7. Cliquez sur **Allouer une nouvelle adresse**, lorsque vous y êtes invité : sélectionnez **Oui**pour obtenir une nouvelle adresse IP.



8. Sélectionnez l'adresse dans la liste et sélectionnez **Adresse associée**.

9. Sélectionnez l'instance **Citrix ADC** que vous avez créée précédemment dans la liste des instances. Une fois cette option sélectionnée, vous pourrez sélectionner l'adresse IP que vous avez affectée statiquement à l'instance (la même adresse que votre Citrix Gateway) et sélectionner **Associer**.

10. Pointez votre enregistrement de nom DNS sur l'adresse IP élastique que vous a attribuée Amazon.
11. Connectez-vous à votre Citrix Gateway.

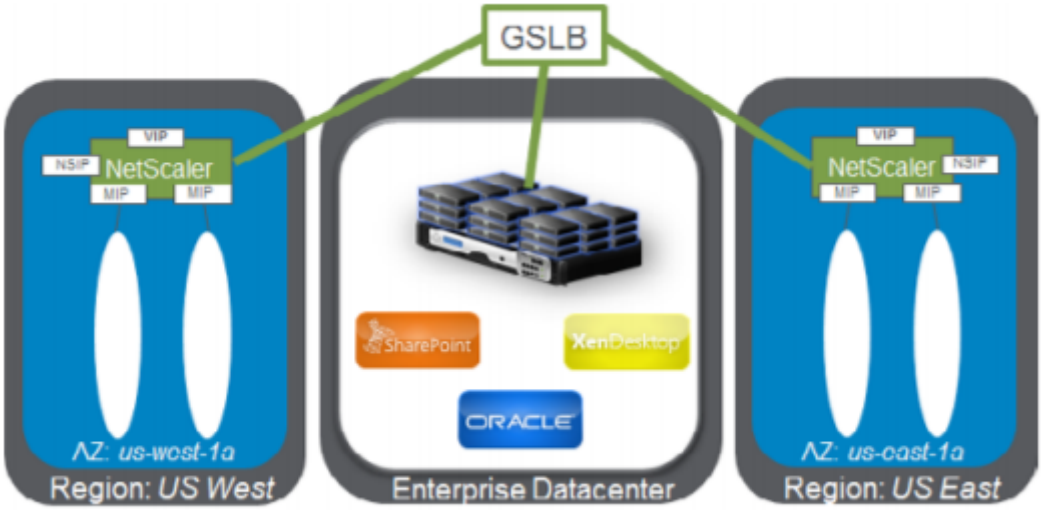
Équilibrage de charge haute disponibilité pour StoreFront

S'il vous plaît voirEtapes de configuration de Citrix.

Configurer GSLB dans deux emplacements AWS

La configuration de GSLB pour Citrix ADC sur AWS consiste en grande partie à configurer Citrix ADC pour équilibrer la charge du trafic vers les serveurs situés en dehors du VPC auquel appartient Cit-

rix ADC, par exemple dans un autre VPC dans une région de disponibilité différente ou un centre de données local, etc.



Services basés sur le nom de domaine (GSLB DBS) avec équilibreurs de charge cloud

Vue d'ensemble GSLB et DBS

La prise en charge de Citrix ADC GSLB à l'aide de DBS (Domain Based Services) pour les équilibreurs de charge cloud permet la découverte automatique des services cloud dynamiques à l'aide d'une solution d'équilibrage de charge cloud. Cette configuration permet à Citrix ADC d'implémenter les services GSLB (Global Server Load Balancing Domain-Name Based Services) dans un environnement Active-Active. DBS permet la mise à l'échelle des ressources back-end dans les environnements AWS et Microsoft Azure à partir de la découverte DNS.

Cette section couvre les intégrations entre Citrix ADC dans les environnements AWS et Azure Auto Scaling. La dernière section du document décrit en détail la possibilité de configurer une paire HA de Citrix ADC couvrant deux zones de disponibilité (AZs) différentes spécifiques à une région AWS.

Conditions préalables

Les conditions requises pour les groupes de services Citrix ADC GSLB comprennent un environnement AWS et Microsoft Azure fonctionnel qui possède les connaissances et la capacité de configurer des groupes de sécurité, des serveurs Web Linux, des Citrix ADC au sein d'AWS, des IP Elastic et des équilibreurs de charge Elastic.

L'intégration du service GSLB DBS nécessite Citrix ADC version 12.0.57 pour les instances d'équilibrage de charge AWS ELB et Microsoft Azure ALB.

Améliorations des fonctionnalités du groupe de services Citrix ADC GSLB

Entité Groupe de services GSLB : Citrix ADC version 12.0.57

GSLB Service Group prend en charge Autoscale à l'aide de la découverte dynamique BDS.

Les composants de fonctionnalités DBS (service basé sur le domaine) doivent être liés au groupe de services GSLB

Exemple :

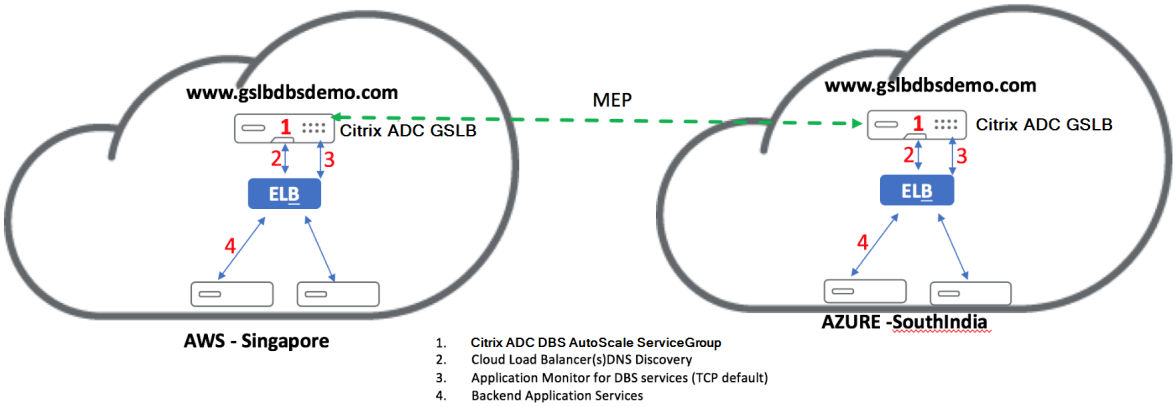
```
> add server sydney_server LB-Sydney-xxxxxxxxxx.ap-southeast-2.elb.
   amazonaws.com
> add gslb serviceGroup sydney_sg HTTP -autoScale DNS -siteName sydney
> bind gslb serviceGroup sydney_sg sydney_server 80
<!--NeedCopy-->
```

Services basés sur les noms de domaine — AWS ELB

GLSB DBS utilise le nom de domaine complet de votre Elastic Load Balancer pour actualiser dynamiquement les groupes de services GSLB afin d'inclure les serveurs principaux créés et supprimés dans AWS. Les serveurs et instances principaux d'AWS peuvent être configurés pour évoluer en fonction de la demande du réseau ou de l'utilisation du processeur. Pour configurer cette fonctionnalité, nous pointons le Citrix ADC vers notre Elastic Load Balancer pour acheminer dynamiquement vers différents serveurs dans AWS sans avoir à actualiser manuellement le Citrix ADC chaque fois qu'une instance est créée et supprimée dans AWS. La fonctionnalité DBS Citrix ADC pour les groupes de services GSLB utilise la découverte de service prenant en charge DNS pour déterminer les ressources de service membre de l'espace de noms DBS identifié dans le groupe AutoScaler.

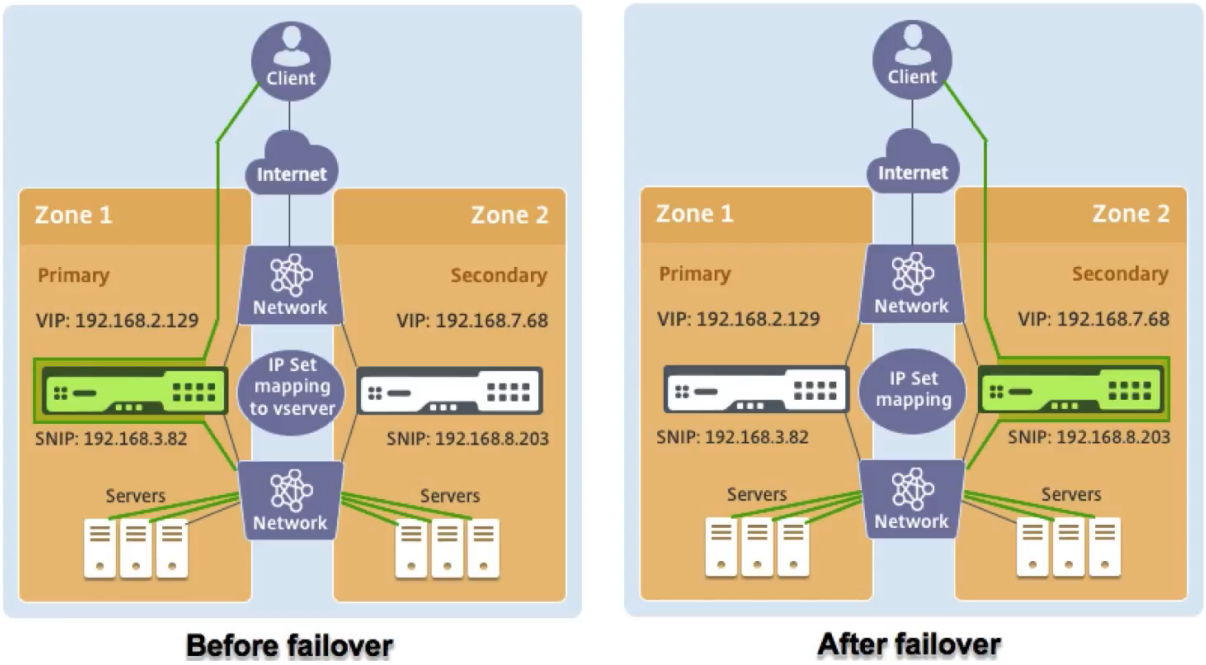
Diagramme :

Composants AutoScale DBA Citrix ADC GSLB avec équilibreurs de charge cloud



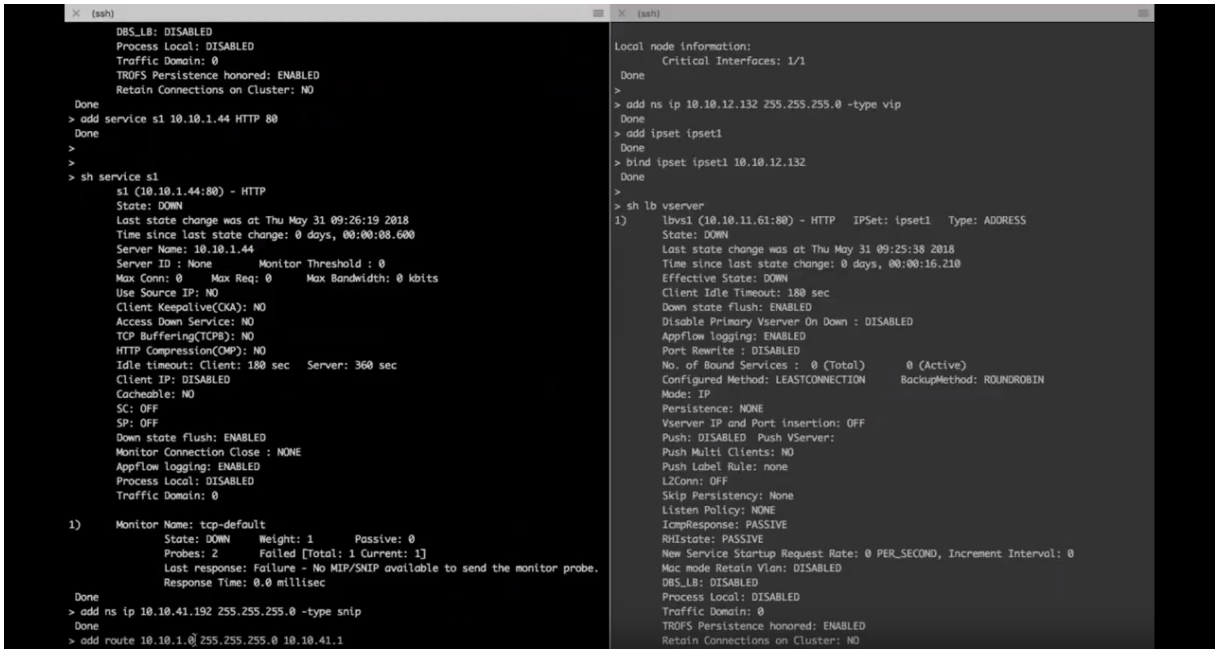
Utiliser Citrix ADC HA dans AWS dans plusieurs zones de disponibilité

Le déploiement de Citrix ADC dans AWS dans différentes zones de disponibilité est une nouvelle fonctionnalité publiée pour Citrix ADC 12.1. Ceci est fait en attachant le Citrix ADC à une adresse IP de réseau Elastic (ENI).

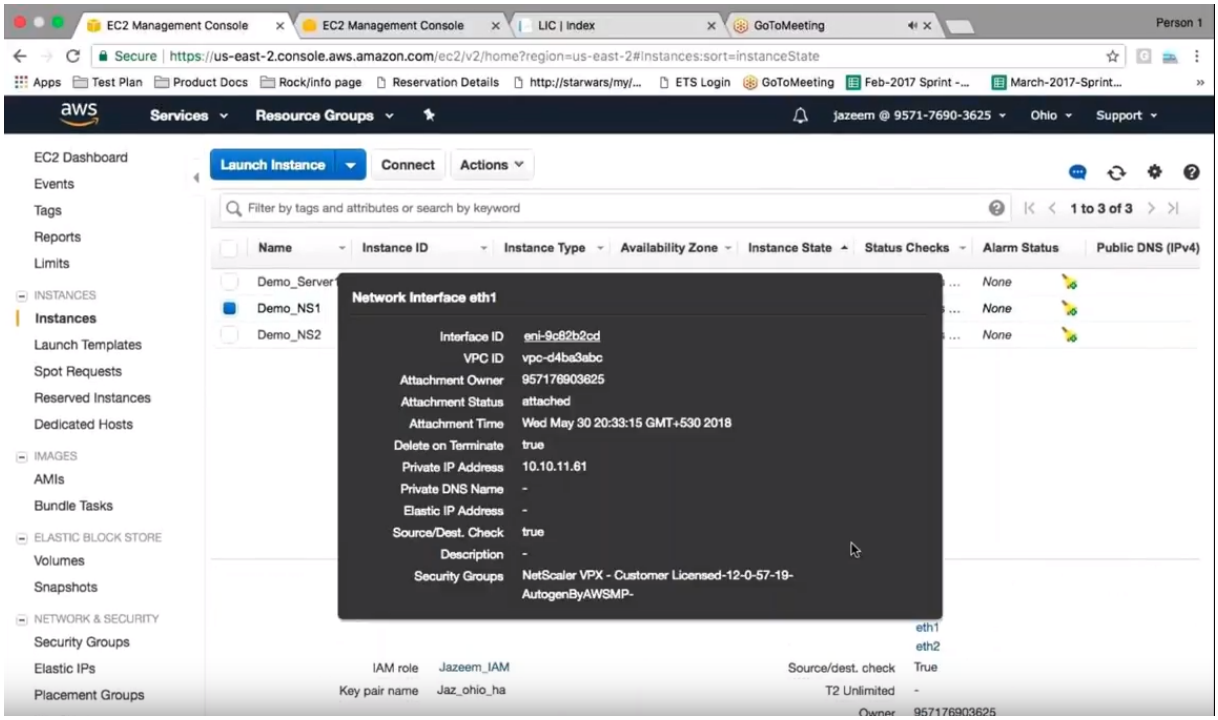


La façon dont la solution fonctionne est légèrement différente des autres, car elle nécessite la configuration de l'HA sur le VPX et une configuration réseau indépendante. Cette solution utilise une nouvelle fonctionnalité de l'ensemble d'adresses IP pour le serveur virtuel de maintenir le basculement sur incident.

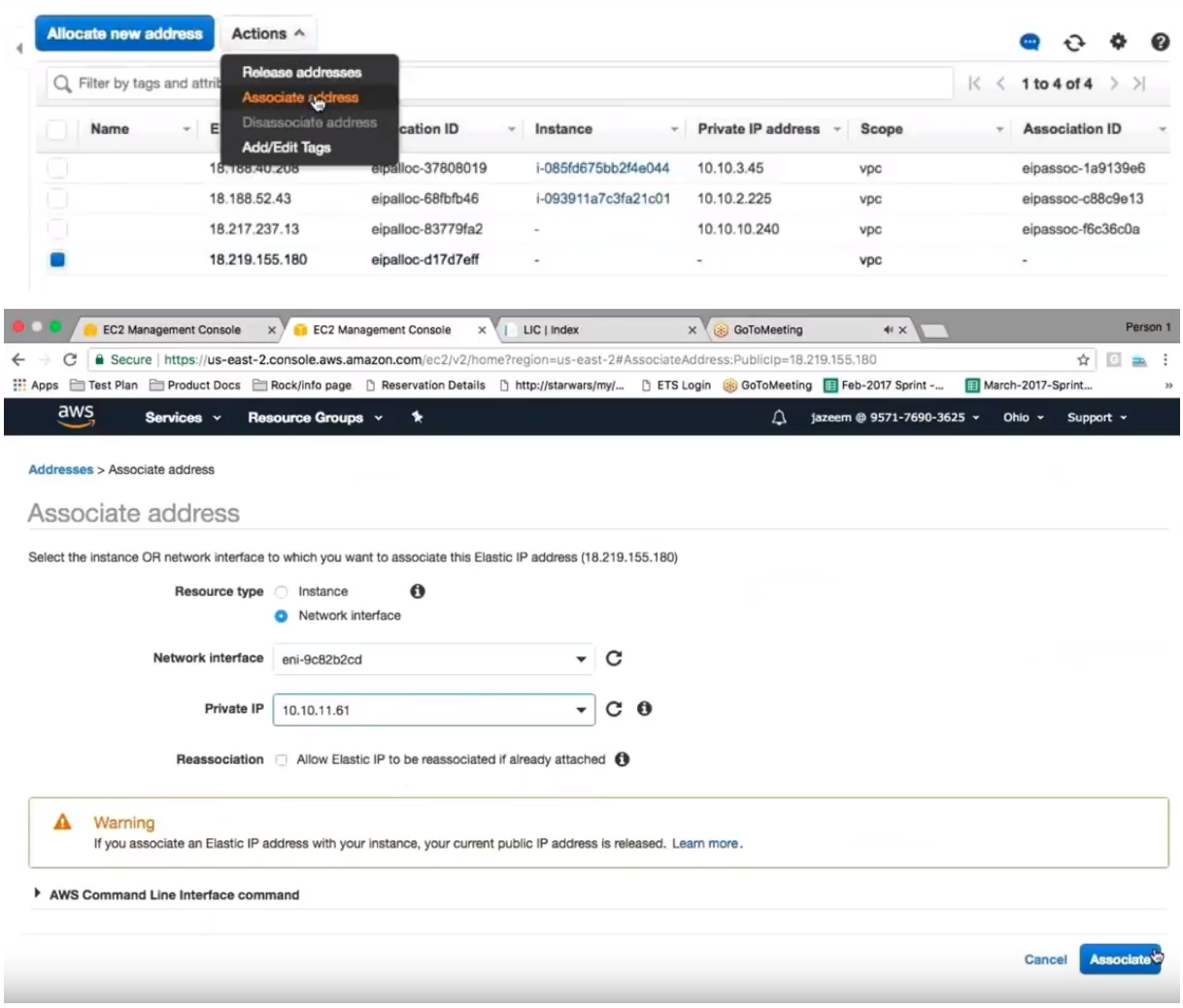
Pour commencer, vous devez vous connecter à Citrix ADC et définir ou gérer une adresse réseau côté serveur, une adresse côté client, ainsi que le routage vers les deux.



Dans la console AWS, le premier VPX a été configuré avec une adresse IP élastique.

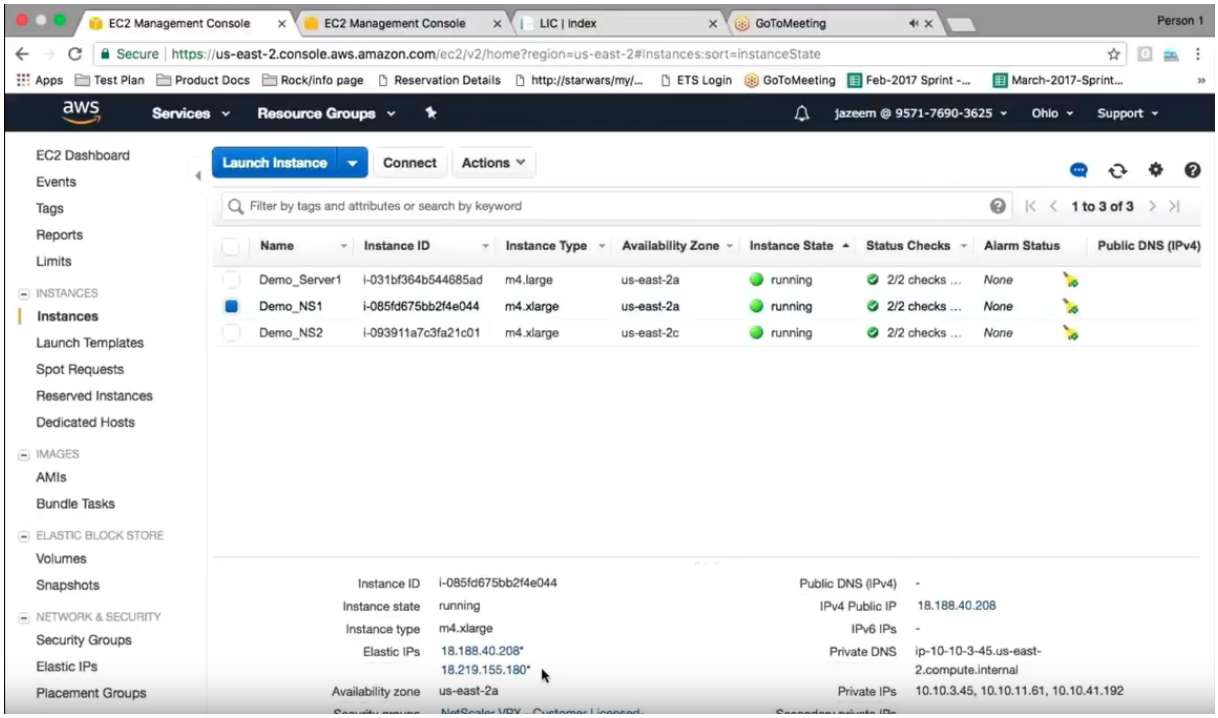


En entrant dans l'interface élastique, la première chose à faire fonctionner la solution est d'associer cette IP élastique à l'adresse privée existante sur cette interface.

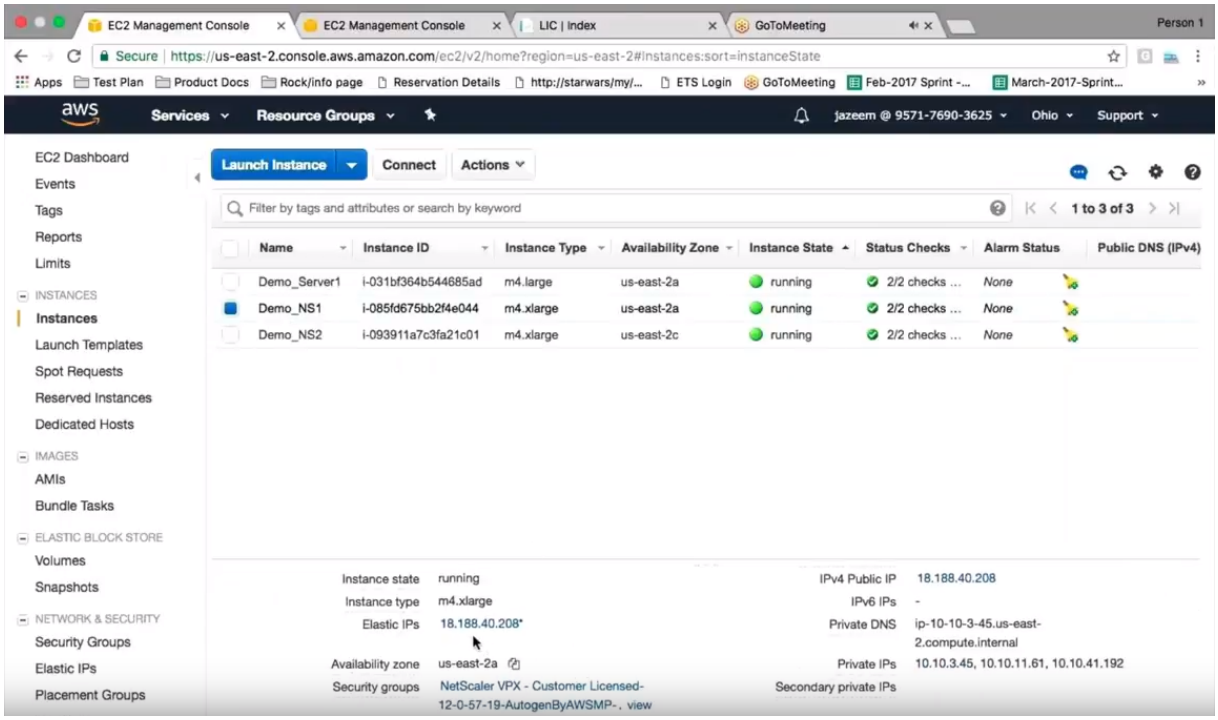


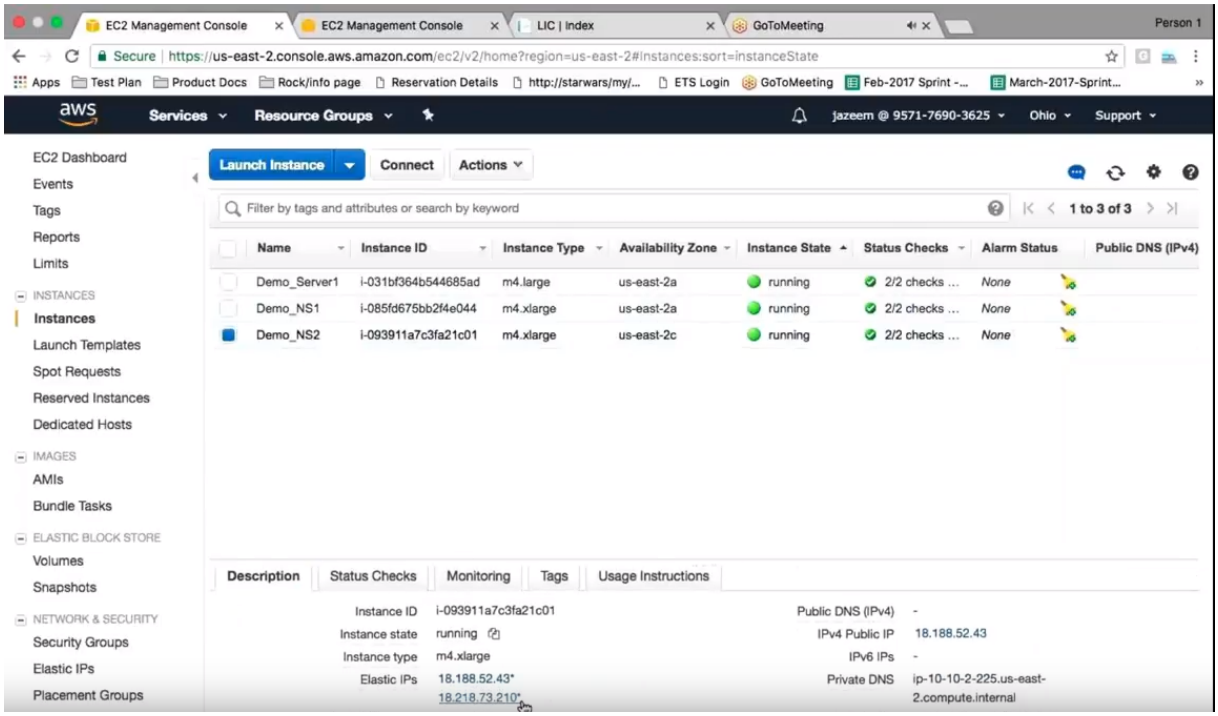
Une fois cette association effectuée, vous êtes prêt à effectuer le basculement.

En bas, il devrait y avoir une deuxième IP élastique maintenant sur le VPX.

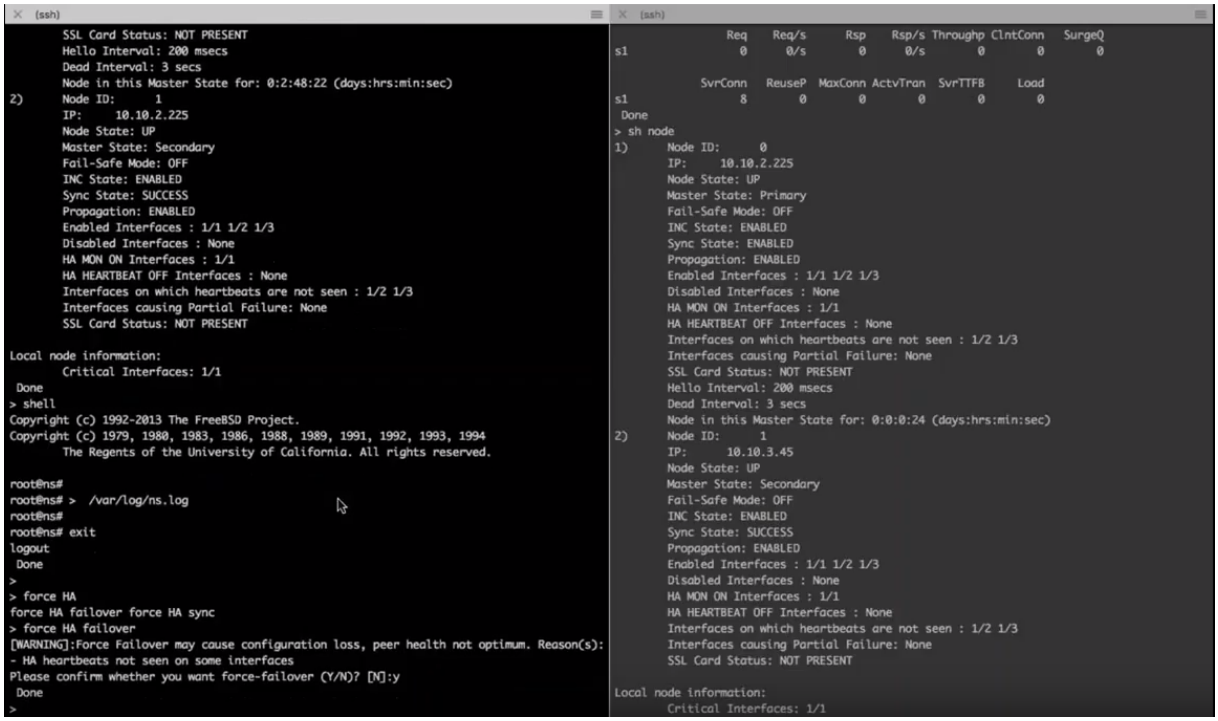


Rendez-vous donc sur le VPX pour lancer un basculement et revenez dans la console AWS. Cette fois, en regardant les adresses IP élastiques appartenant au premier Citrix ADC, remarquez que le nouvel EIP n'est pas là, car il a maintenant été déplacé vers le deuxième Citrix ADC.

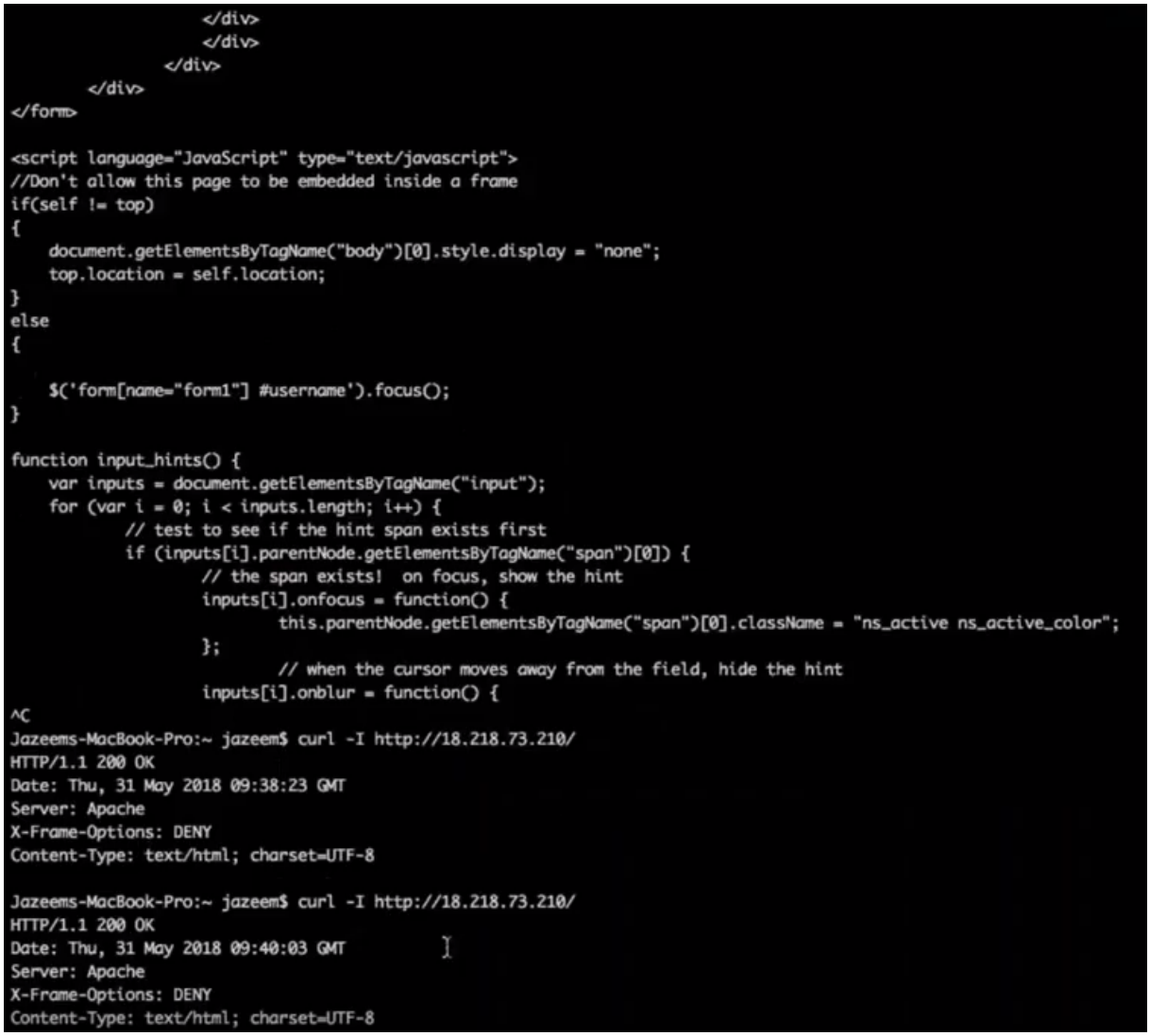




Pour vérifier cela, entrez une commande **show node** sur le premier et le deuxième Citrix ADC pour voir que le second Citrix ADC est maintenant configuré dans un état **principal** comme avant il était en **veille** .

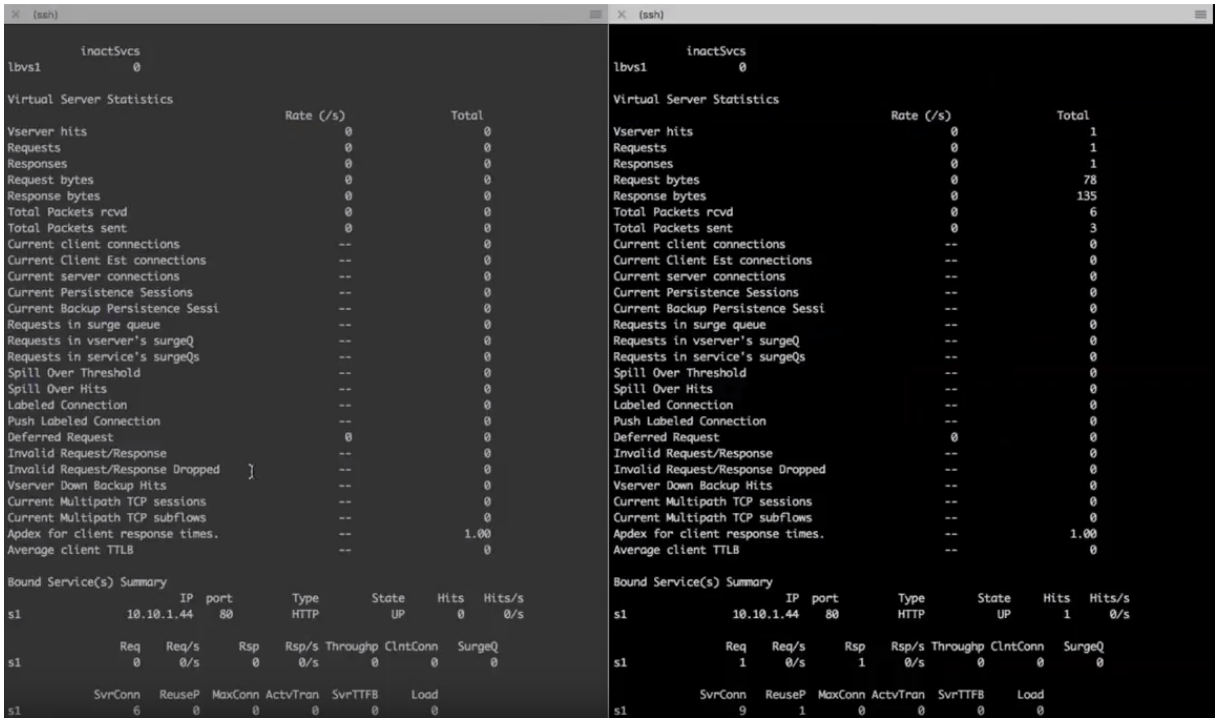


Maintenant, vous pouvez regarder le flux de trafic en temps réel.

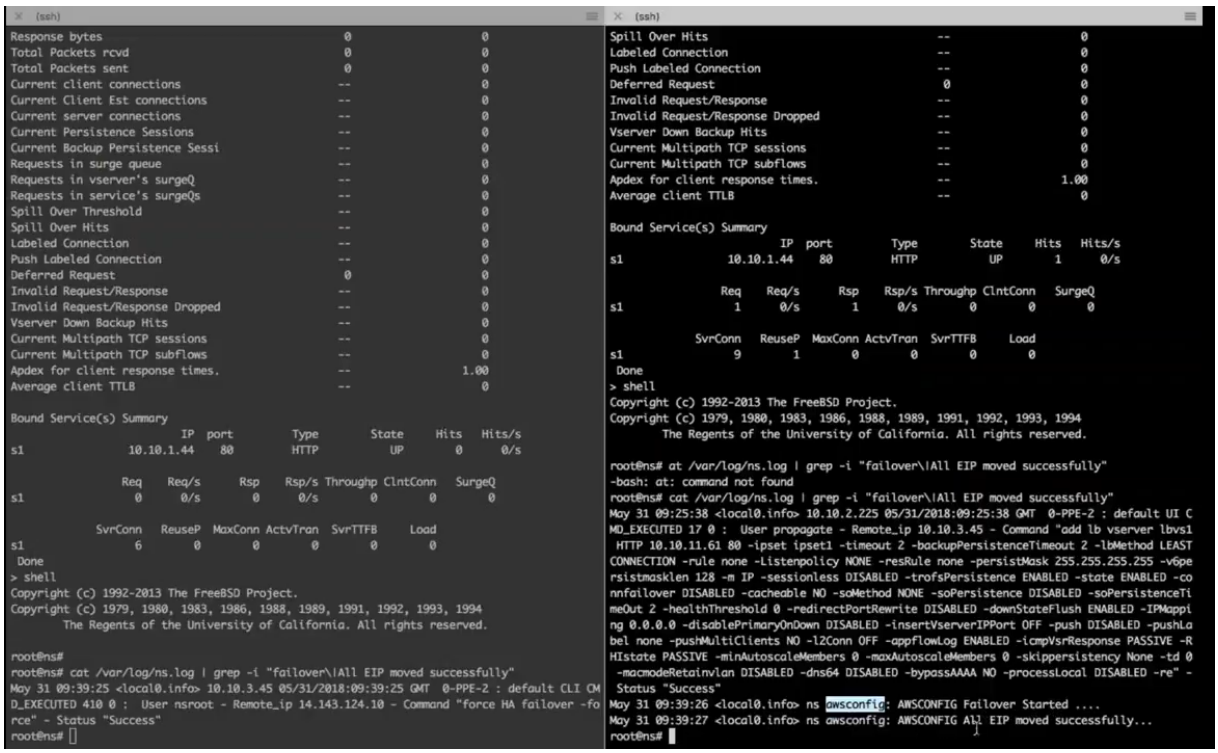


```
                    </div>
                    </div>
                </div>
        </div>
</form>

<script language="JavaScript" type="text/javascript">
//Don't allow this page to be embedded inside a frame
if(self != top)
{
    document.getElementsByTagName("body")[0].style.display = "none";
    top.location = self.location;
}
else
{

    $('form[name="form1"] #username').focus();
}

function input_hints() {
    var inputs = document.getElementsByTagName("input");
    for (var i = 0; i < inputs.length; i++) {
            // test to see if the hint span exists first
            if (inputs[i].parentNode.getElementsByTagName("span")[0]) {
                    // the span exists!  on focus, show the hint
                    inputs[i].onfocus = function() {
                            this.parentNode.getElementsByTagName("span")[0].className = "ns_active ns_active_color";
                    };
                            // when the cursor moves away from the field, hide the hint
                    inputs[i].onblur = function() {
^C
Jazeems-MacBook-Pro:~ jazeem$ curl -I http://18.218.73.210/
HTTP/1.1 200 OK
Date: Thu, 31 May 2018 09:38:23 GMT
Server: Apache
X-Frame-Options: DENY
Content-Type: text/html; charset=UTF-8

Jazeems-MacBook-Pro:~ jazeem$ curl -I http://18.218.73.210/
HTTP/1.1 200 OK
Date: Thu, 31 May 2018 09:40:03 GMT
Server: Apache
X-Frame-Options: DENY
Content-Type: text/html; charset=UTF-8
```

Vous pouvez envoyer une demande au VIP après le basculement. Si vous effectuez une statistique sur le serveur virtuel LB sur le Citrix ADC qui a été actif pour la première fois, remarquez qu'aucune requête n'est touchée. Si vous exécutez la même commande sur l'ancienne instance de secours, maintenant active Citrix ADC, vous pouvez voir qu'il y a un accès sur le serveur virtuel. Après la transition HA, le trafic est allé au nouveau Citrix ADC.



Maintenant, si vous voulez faire un débogage ou voir quel est l'état actuel, vous pouvez passer à l'interpréteur de commandes et rechercher les enregistrements pour vous montrer quand le basculement HA s'est produit, ainsi que lorsque l'appel de configuration ou d'API AWS a été effectué pour balancer tous les EIP du principal serveur Citrix ADC au secondaire.



Configurer les composants AWS

Groupes de sécurité

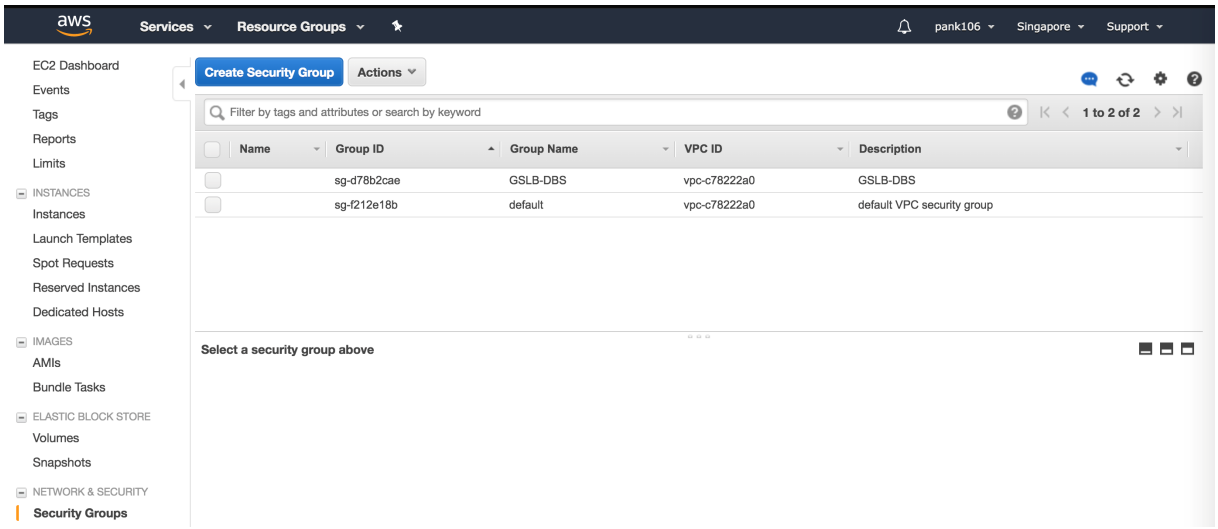
> Remarque :
>
> La recommandation devrait être de créer différents groupes de sécurité pour ELB, Citrix ADC GSLB Instance et Linux, car l'ensemble de règles requis pour chacune de ces entités sera différent. Cet exemple comporte une configuration consolidée du groupe de sécurité par souci de brièveté.

Consultez la documentation AWS Security Group pour garantir la configuration correcte du pare-feu virtuel :

https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html#VPCSecurityGroups

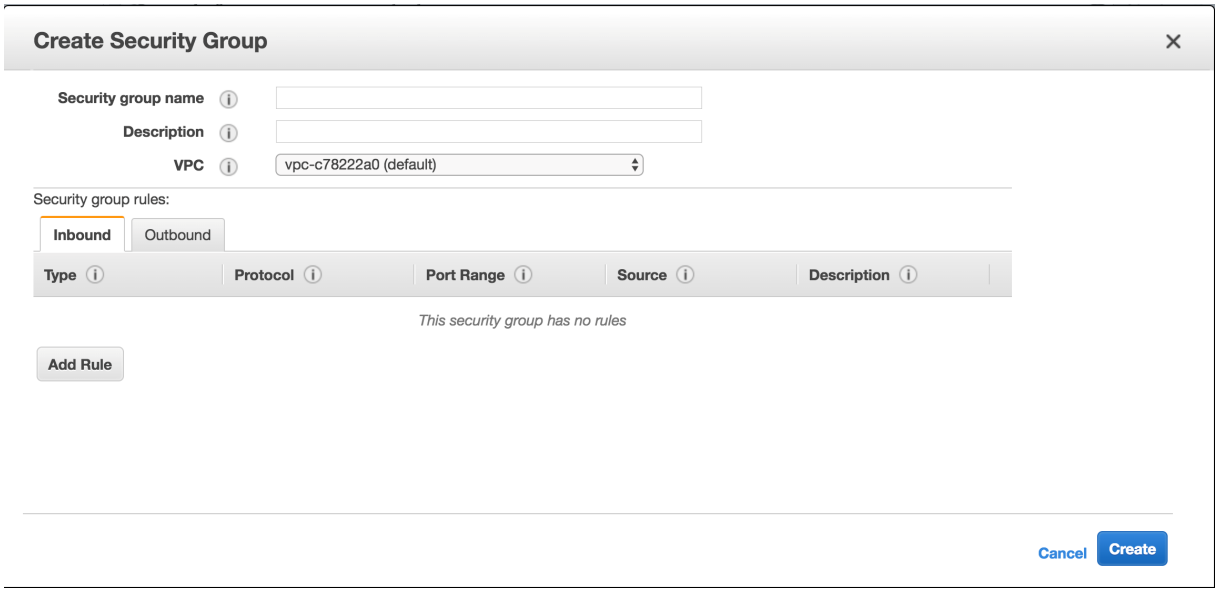
Étape 1 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **NETWORK & SECURITY > Groupes de sécurité**.



Étape 2 :

Cliquez sur **Créer un groupe de sécurité** et fournissez un nom et une description. Ce groupe de sécurité comprend les serveurs Web principaux Citrix ADC et Linux.



Étape 3 :

Ajoutez les règles de port entrant à partir de la capture d'écran ci-dessous.

> Remarque :
>
> La limitation de l'accès IP source est recommandée pour le durcissement granulaire.

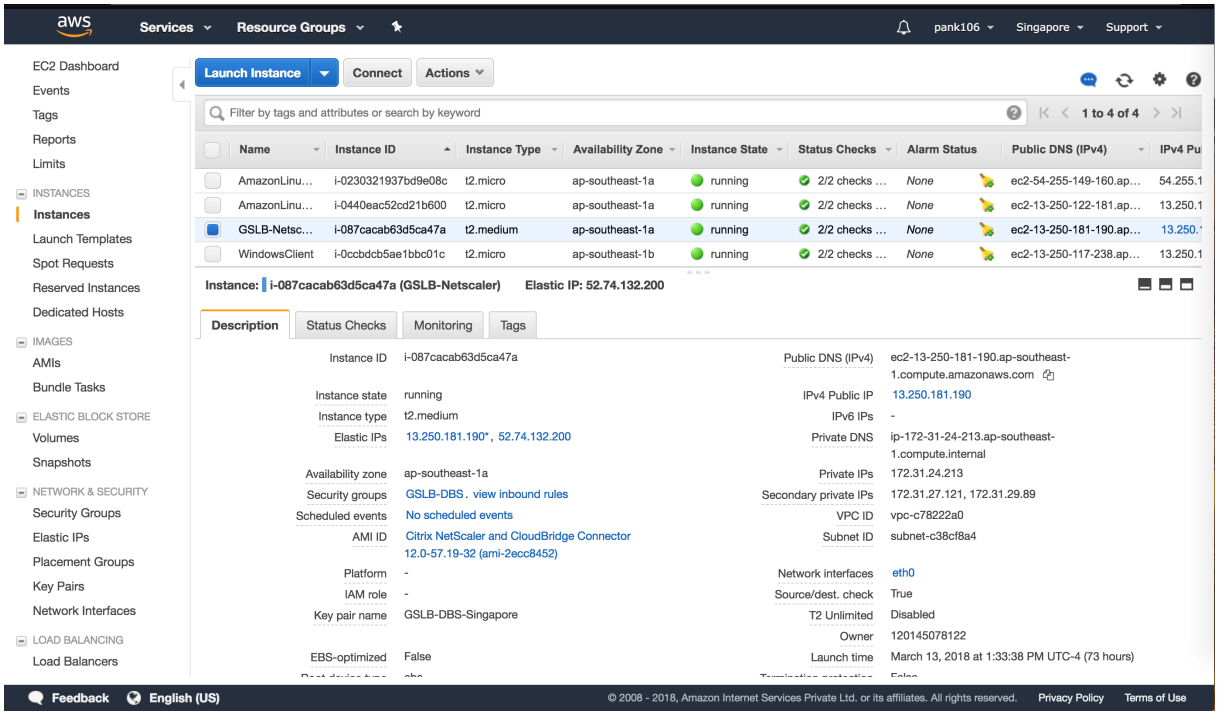
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/security-group-rules-reference.html#sg-rules-web-server

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	
HTTP	TCP	80	::/0	
SSH	TCP	22	0.0.0.0/0	
DNS (UDP)	UDP	53	0.0.0.0/0	
DNS (UDP)	UDP	53	::/0	
Custom TCP Rule	TCP	3389	0.0.0.0/0	
Custom TCP Rule	TCP	3389	::/0	
All ICMP - IPv4	All	N/A	0.0.0.0/0	
All ICMP - IPv4	All	N/A	::/0	
Custom TCP Rule	TCP	5985	0.0.0.0/0	
Custom TCP Rule	TCP	5985	::/0	
Custom TCP Rule	TCP	3008 - 3011	0.0.0.0/0	
Custom TCP Rule	TCP	3008 - 3011	::/0	

Services Web back-end Amazon Linux

Étape 4 :

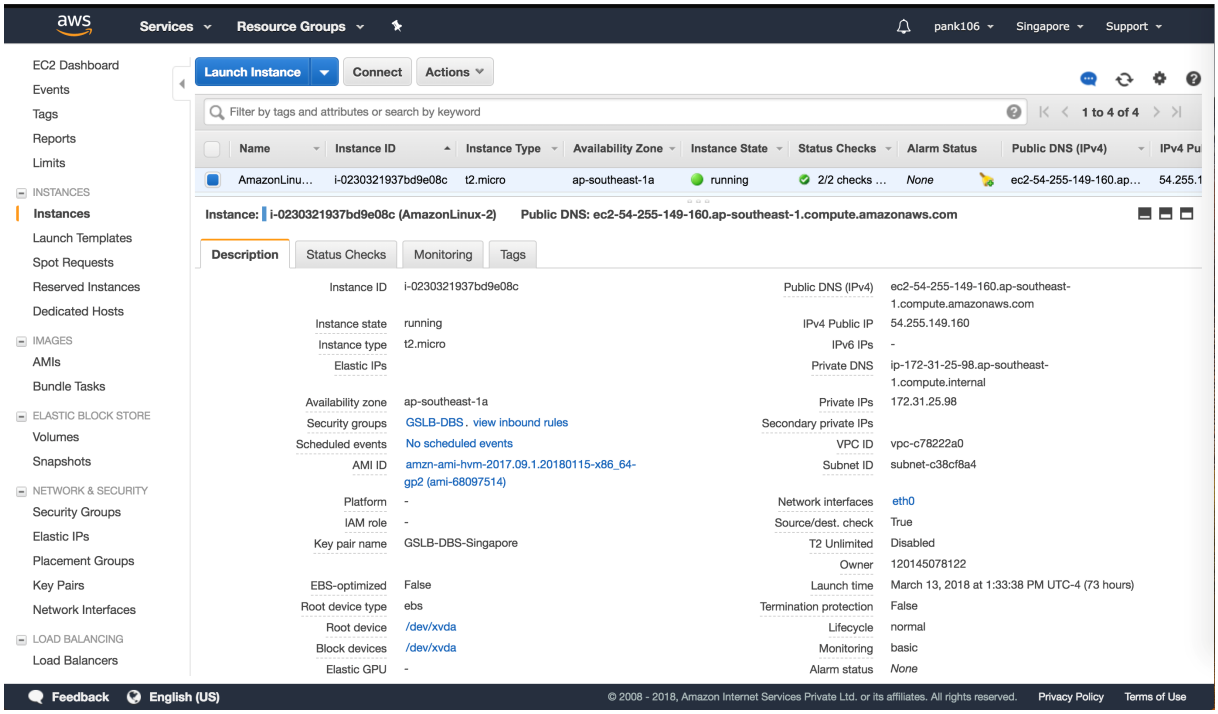
Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **Instances**.



Étape 5 :

Cliquez sur **Lancer l'instance** en utilisant les détails ci-dessous, configurez l'instance **Amazon Linux** .

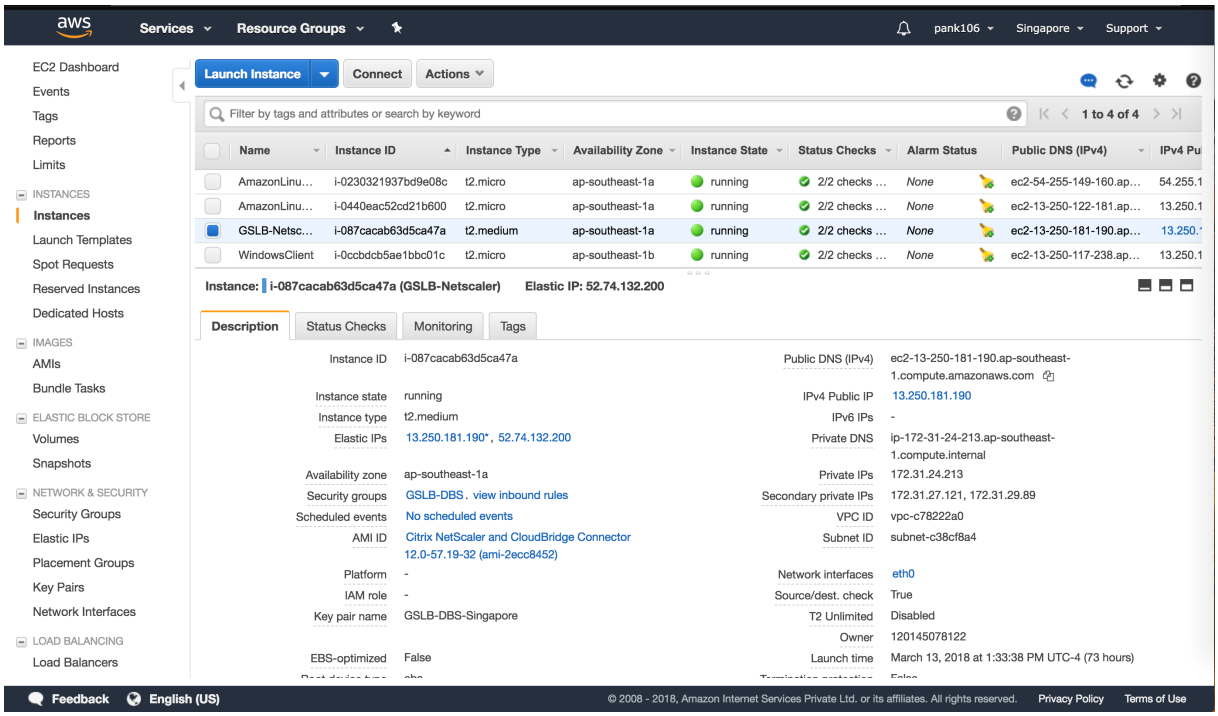
Renseignez les détails sur la configuration d'un serveur Web ou d'un service principal sur cette instance.



Configuration de Citrix ADC

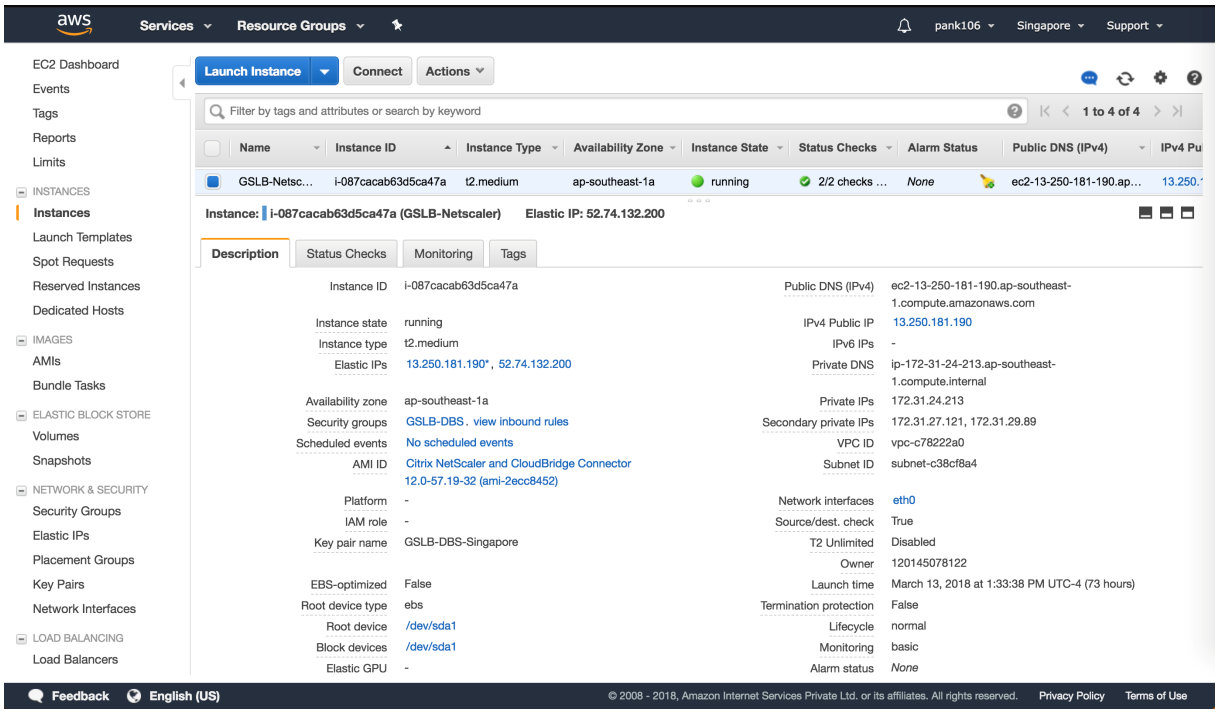
Étape 6 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **Instances**.



Étape 7 :

Cliquez sur **Lancer l'instance** en utilisant les détails ci-dessous, configurez l'instance **Amazon AMI** .



Configuration IP élastique

> Remarque :
>
> Citrix ADC peut également être exécuté avec une seule IP élastique si nécessaire pour réduire les coûts, en n'ayant pas d'IP publique pour le NSIP. Au lieu de cela attacher une IP élastique à SNIP qui peut couvrir pour l'accès de gestion à la boîte, ainsi que l'IP du site GSLB et l'IP ADNS.

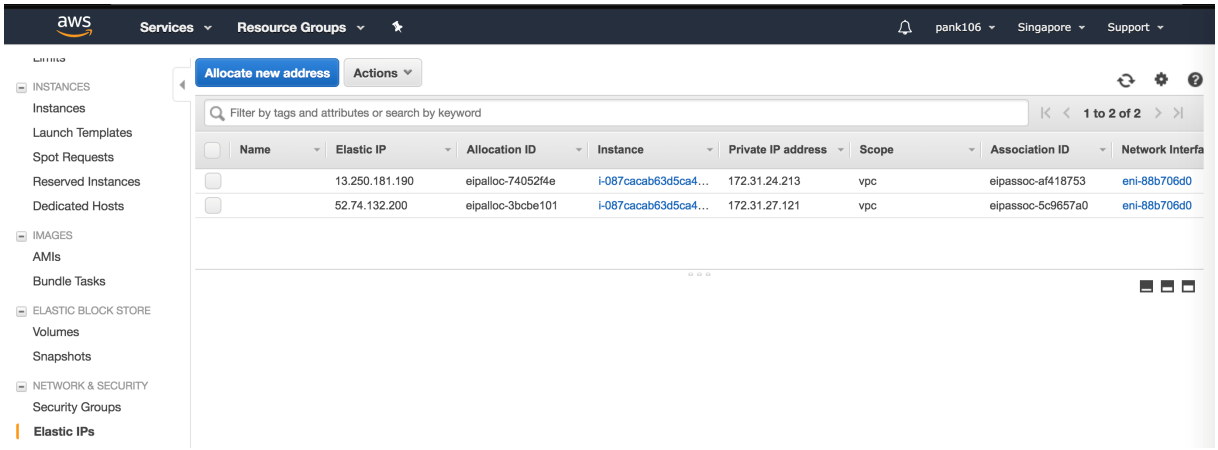
Étape 8 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **NETWORK & SECURITY** , puis configurez **les adresses IP Elastic** .

Cliquez sur **Allouer une nouvelle adresse** pour créer une adresse IP élastique.

Configurez l'adresse IP Elastic pour pointer vers votre instance Citrix ADC en cours d'exécution au sein d'AWS.

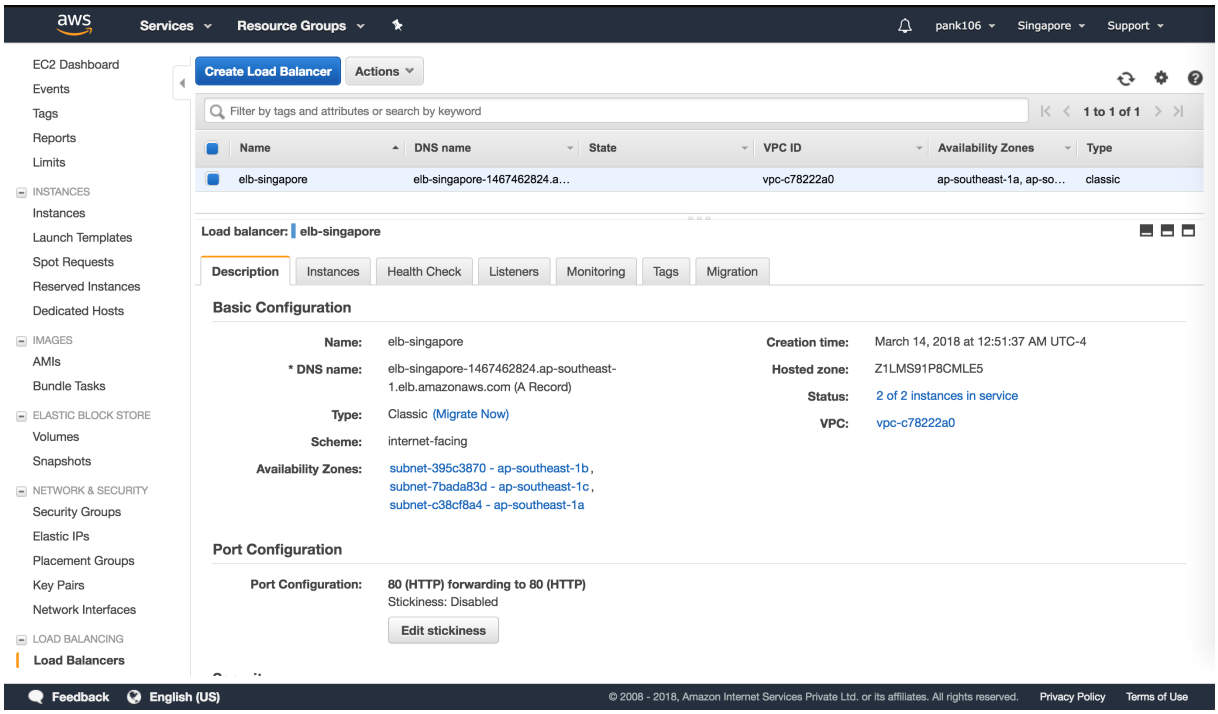
Configurez une deuxième IP Elastic et pointez-la de nouveau vers votre instance Citrix ADC en cours d'exécution.



Équilibreur de charge élastique

Étape 9 :

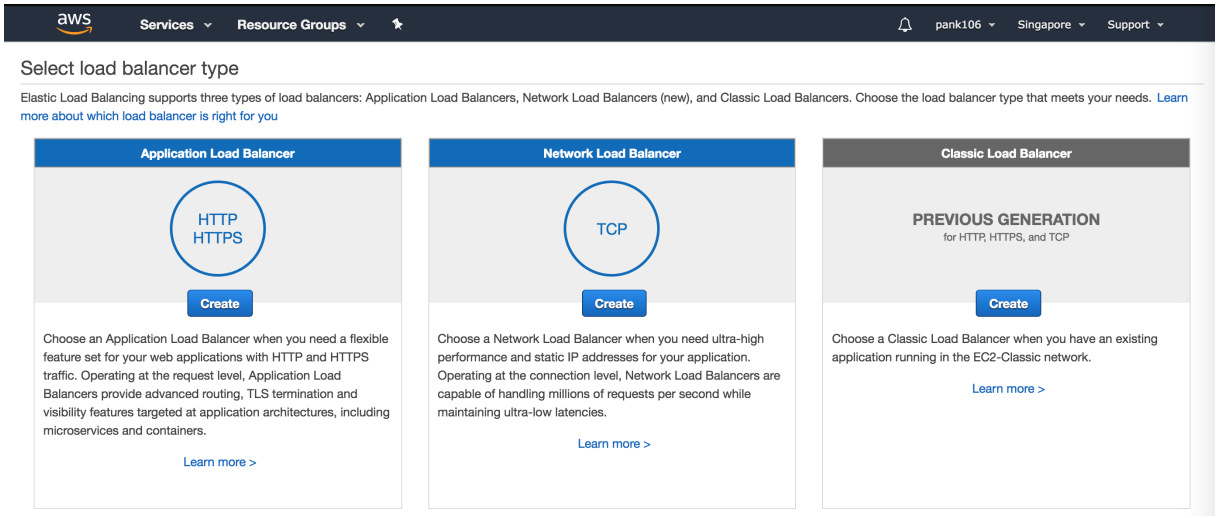
Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à LOAD BALANCING, puis Load Balancers.



Étape 10 :

Cliquez sur **Créer un équilibreur de charge** pour configurer un équilibreur de charge classique

Vos équilibreurs de charge élastiques vous permettent d'équilibrer la charge de vos instances Amazon Linux principales tout en étant en mesure d'équilibrer la charge des instances supplémentaires qui sont réorientées en fonction de la demande.



Configuration des services basés sur le nom de domaine de l'équilibrage de charge serveur global

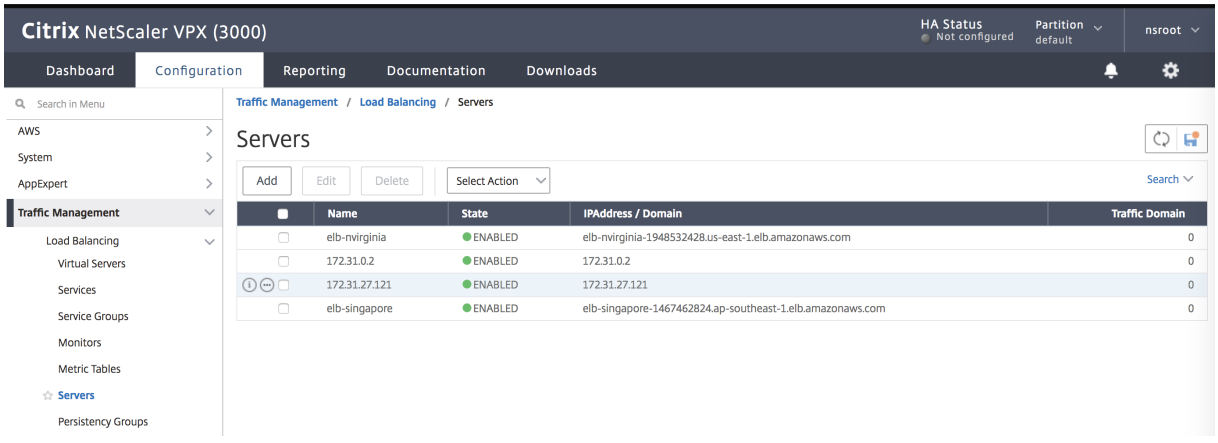
Configurations de gestion du trafic

> Remarque :
>
> Il est nécessaire de configurer Citrix ADC avec un serveur de noms ou un serveur virtuel DNS via lequel les domaines ELB/ALB seront résolus pour les groupes de services DBS.

https://developer-docs.citrix.com/projects/netscaler-command-reference/en/12.0/dns/dns-nameserver/dns-nameserver/

Étape 1 :

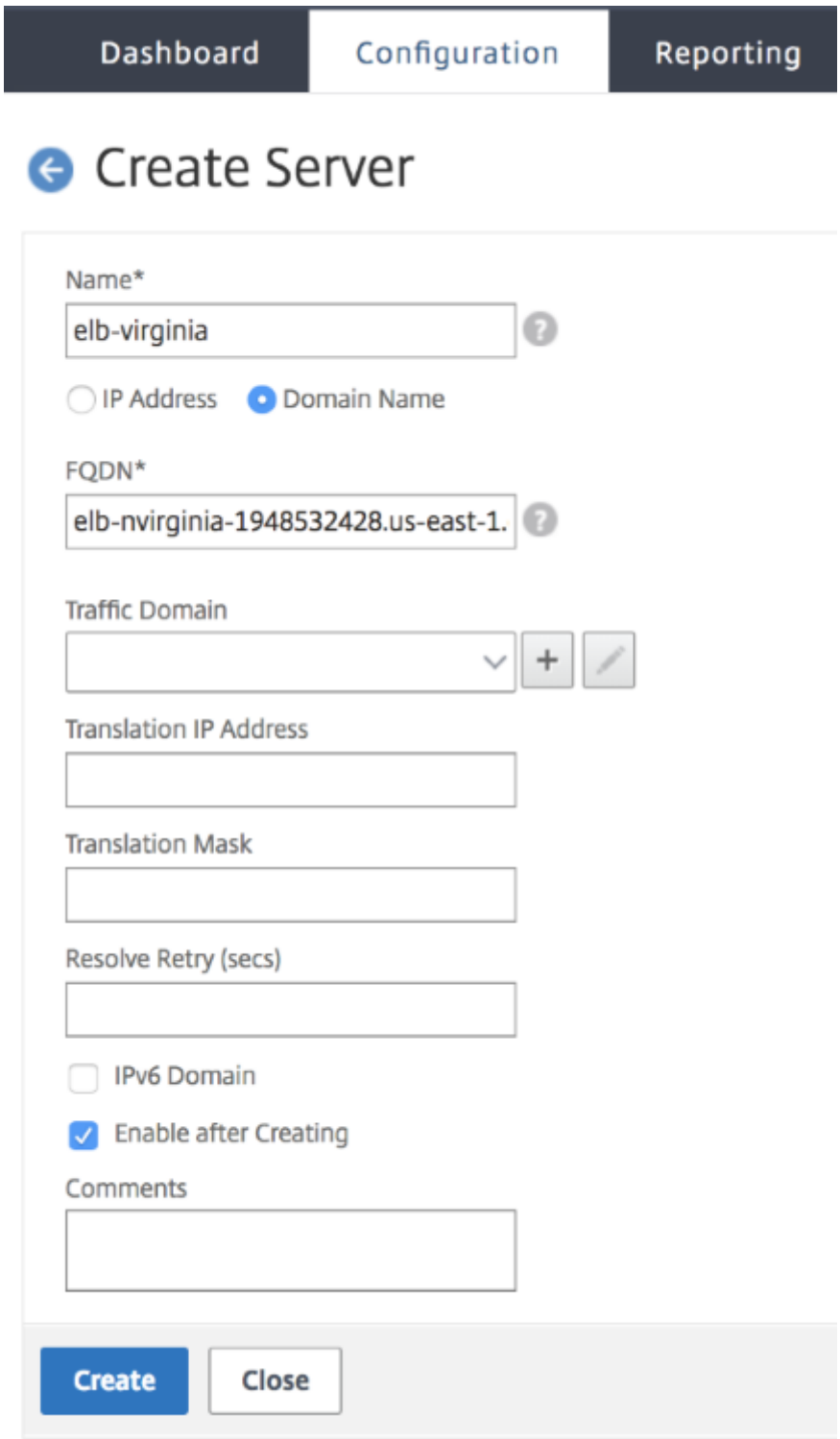
Accédez à **Gestion du trafic > Équilibrage de charge > Serveurs**.



Étape 2 :

Cliquez sur **Ajouter** pour créer un serveur, fournissez un nom et un nom de domaine complet correspondant à l'enregistrement A (nom de domaine) dans AWS pour Elastic Load Balancer (ELB).

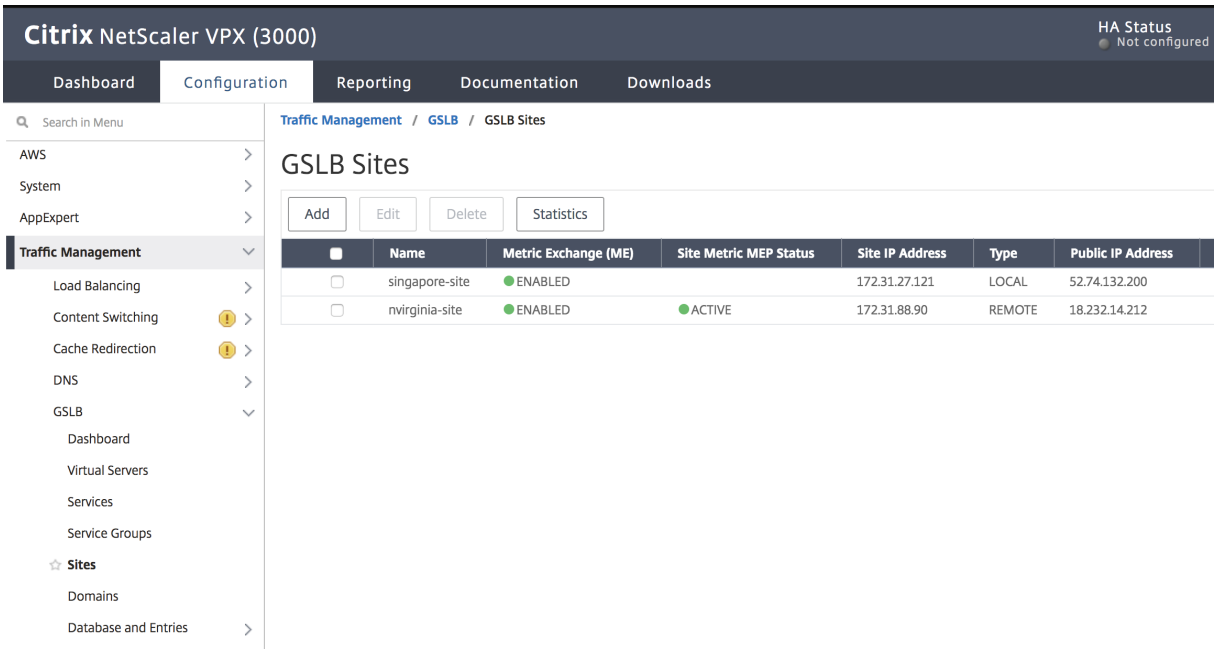
Répétez l'étape 2 pour ajouter le deuxième ELB à partir du deuxième emplacement de ressource dans AWS.



Configurations GSLB

Étape 1 :

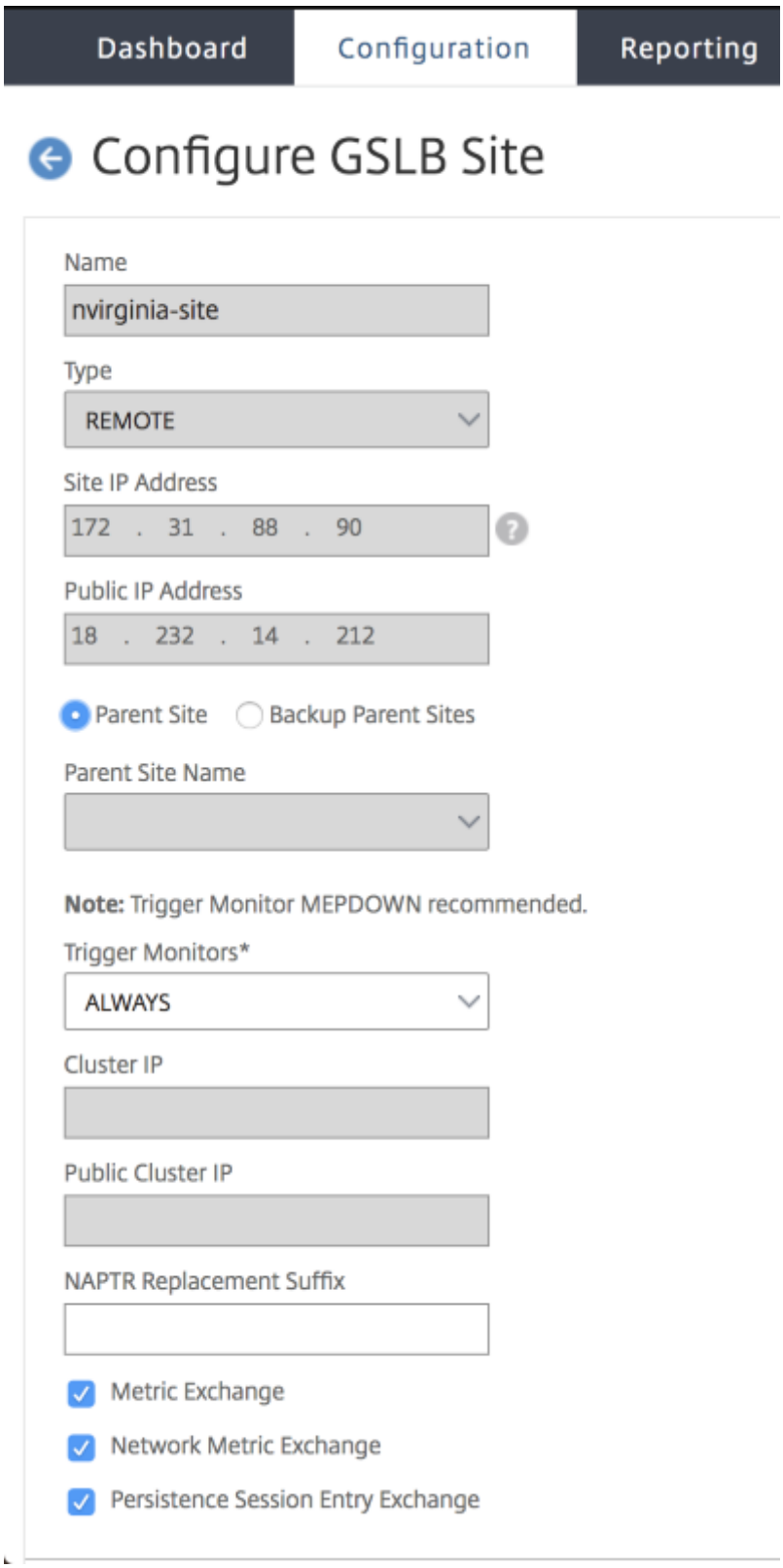
Accédez à **Gestion du trafic > GSLB > Sites**.



Étape 3 :

Cliquez sur le bouton **Ajouter** pour configurer un site GSLB.

Nommez le site. Le type est configuré comme Remote ou Local en fonction de quel Citrix ADC vous configurez le site. L'adresse IP du site est l'adresse IP du site GSLB. Le site GSLB utilise cette adresse IP pour communiquer avec les autres sites GSLB. L'adresse IP publique est requise lors de l'utilisation d'un service cloud où une adresse IP particulière est hébergée sur un pare-feu externe ou un périphérique NAT. Le site doit être configuré en tant que site parent. Assurez-vous que les moniteurs de déclenchement sont réglés sur ALWAYS et veillez à cocher les trois cases en bas pour l'échange de métriques, l'échange de métriques réseau et l'échange d'entrées de session de persistance.

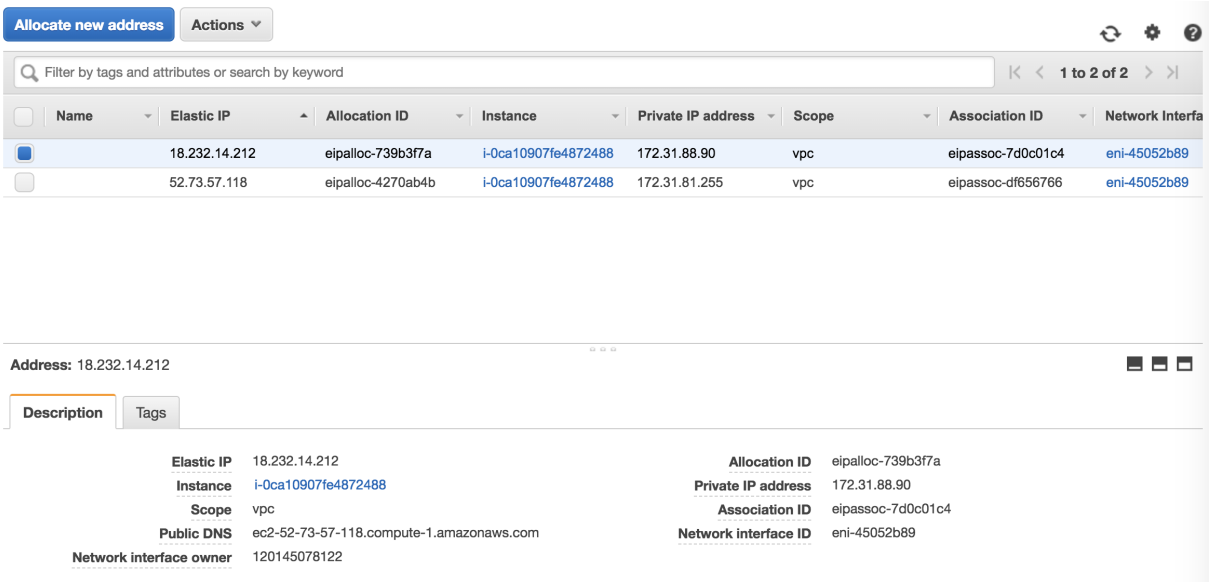


La recommandation consiste à définir le paramètre du moniteur Trigger sur MEPDOWN. Pour plus d'informations, reportez-vous à la section Configurer un groupe de services GSLB.

Étape 4 :

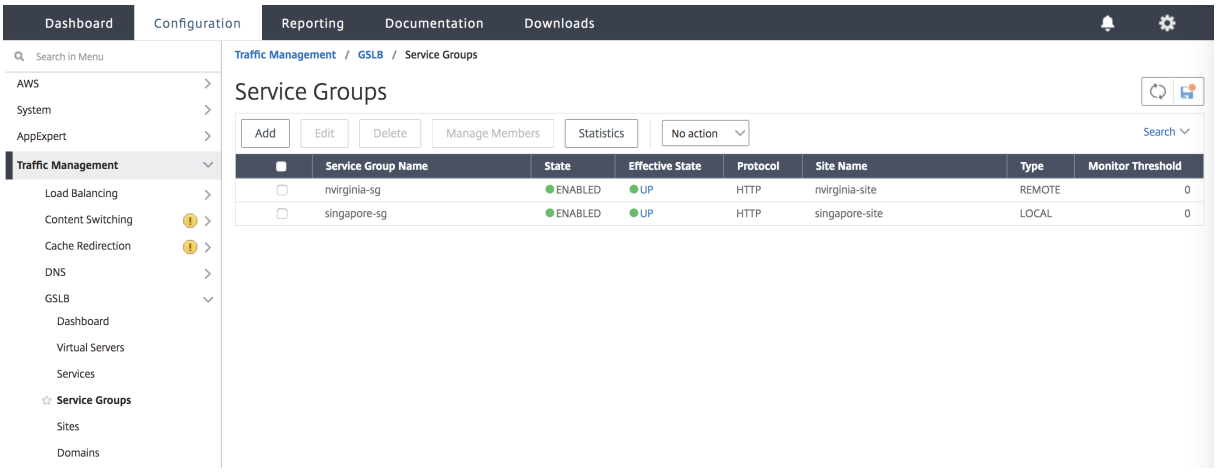
Vous trouverez ci-dessous une capture d'écran de nos configurations AWS, montrant où vous pouvez trouver l'adresse IP du site et l'adresse IP publique. Ils se trouvent sous **Network & Security > Elastic IPs**.

Cliquez sur **Créer**, répétez les étapes 3 et 4 pour configurer le site GSLB pour l'autre emplacement de ressource dans Azure (cela peut être configuré sur le même Citrix ADC)



Étape 5 :

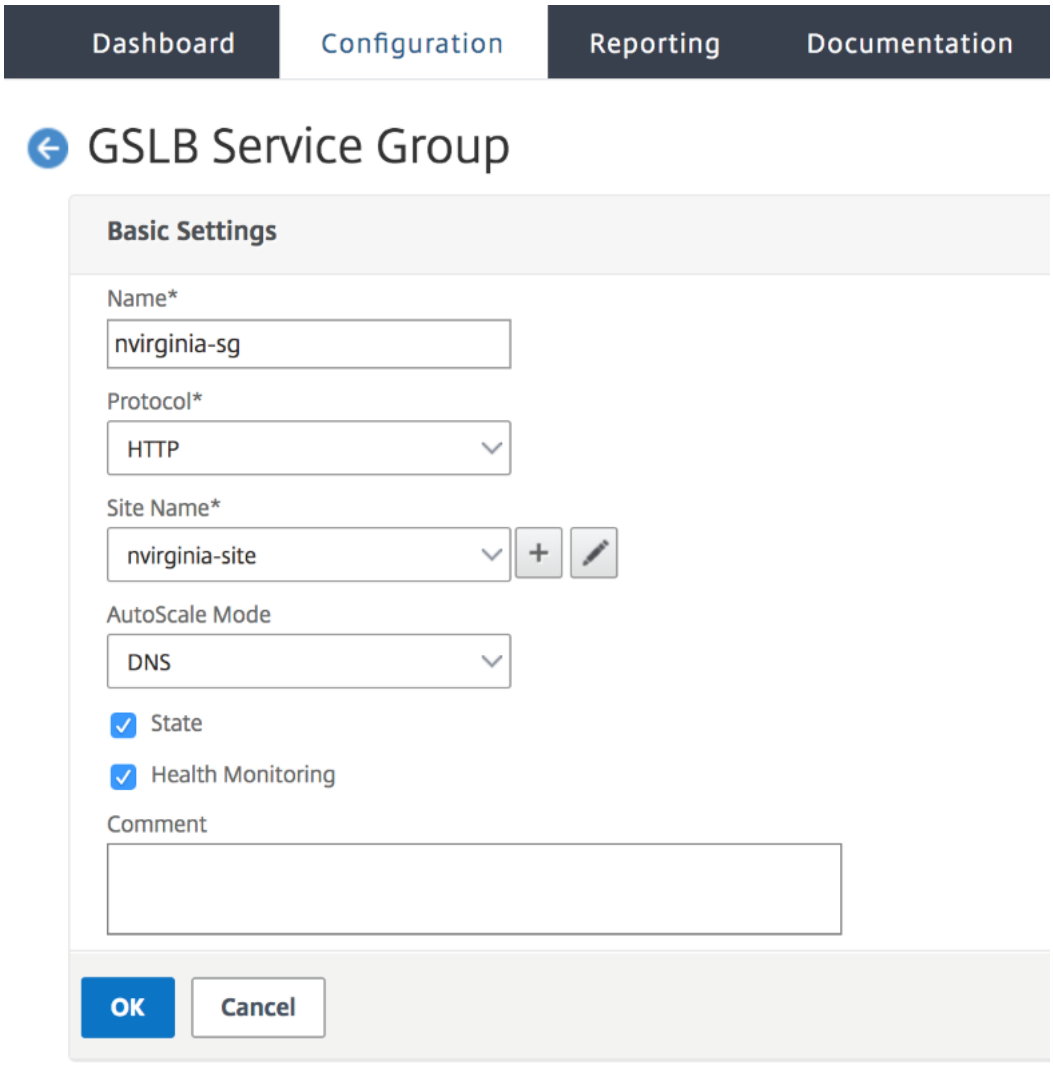
Accédez à **Gestion du trafic > GSLB > Groupes de services**.



Étape 6 :

Cliquez sur **Ajouter** pour ajouter un nouveau groupe de services. Nommez le groupe de services, utilisez le protocole HTTP, puis sous Nom du site, choisissez le site correspondant qui a été créé lors des étapes précédentes. Assurez-vous de configurer le mode AutoScale en tant que DNS et cochez les cases État et Contrôle de l'intégrité.

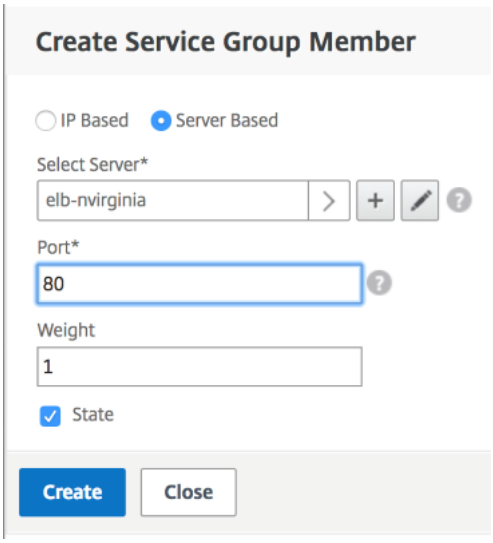
Cliquez sur **OK** pour créer le groupe de services.



Étape 7 :

Cliquez sur **Membres du groupe de services** et sélectionnez **Basé sur serveur**. Sélectionnez le service Elastic Load Balancing Serve correspondant qui a été configuré au début du guide d'exécution. Configurez le trafic pour passer par le port 80.

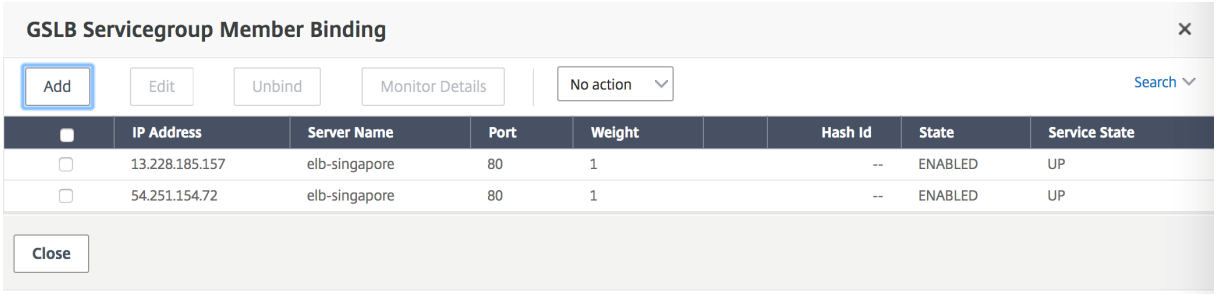
Cliquez sur **Créer**.



Étape 8 :

La liaison de membre du groupe de services doit être remplie avec deux instances qu'il reçoit de l'Elastic Load Balancer.

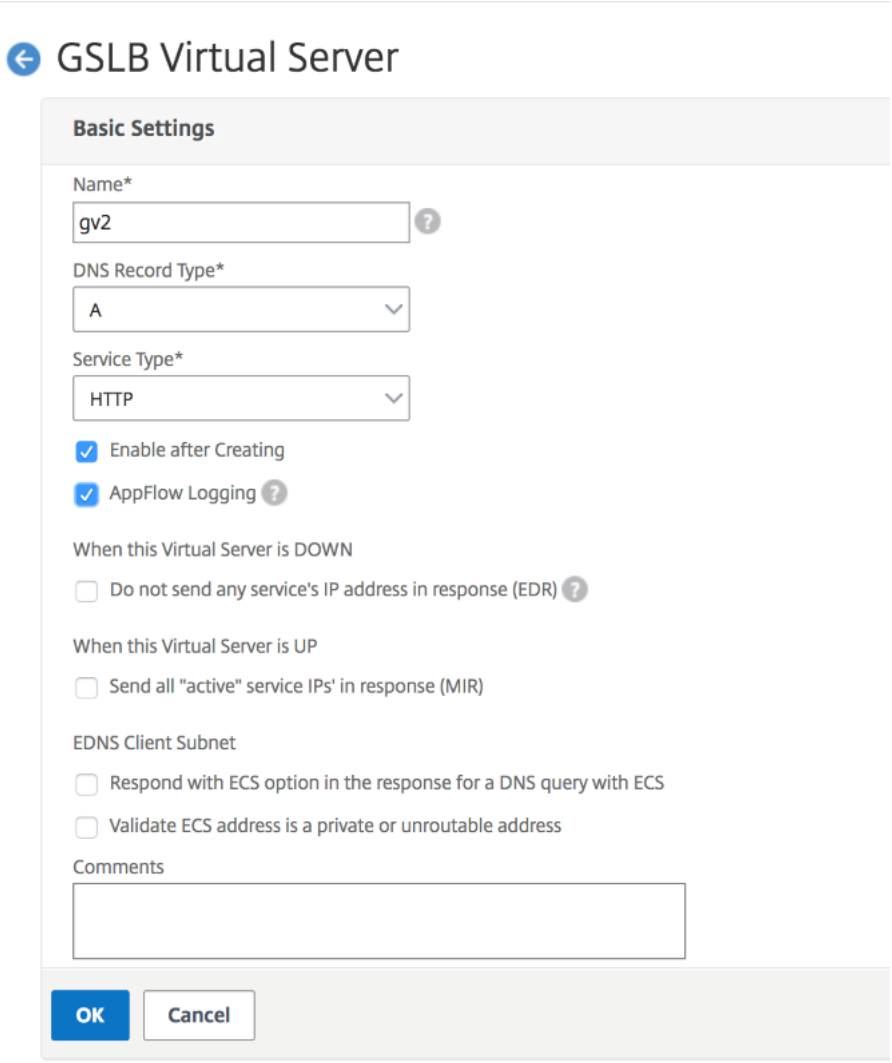
Répétez les étapes pour configurer le groupe de services pour le deuxième emplacement de ressource dans AWS. (Cela peut être fait à partir du même emplacement).



Étape 9 :

Accédez à **Gestion du trafic > GSLB > Serveurs virtuels**.

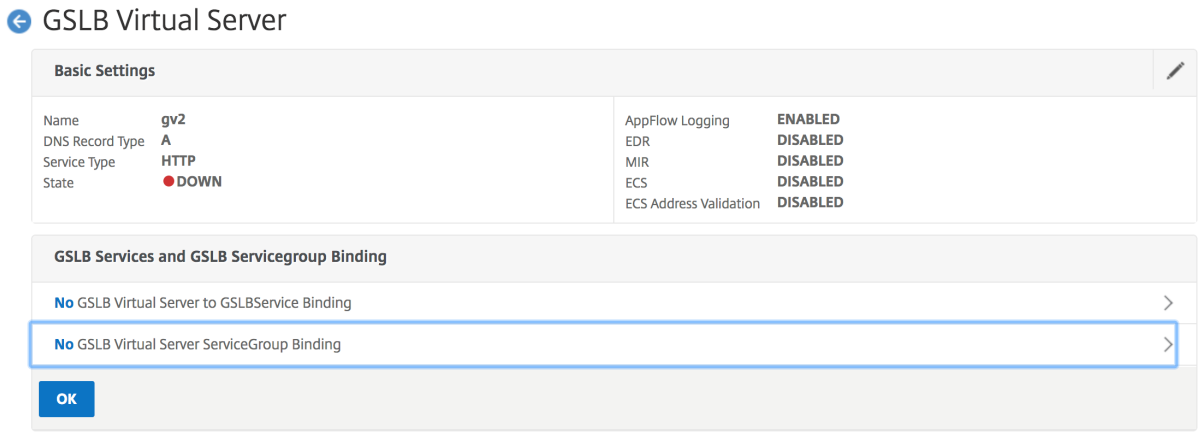
Cliquez sur **Ajouter** pour créer le serveur virtuel. Nommez le serveur, le type d'enregistrement DNS est défini comme A, le type de service est défini comme HTTP et cochez les cases Activer après la création et la journalisation AppFlow. Cliquez sur **OK** pour créer le serveur virtuel GSLB. (interface graphique de Citrix ADC)



Étape 10 :

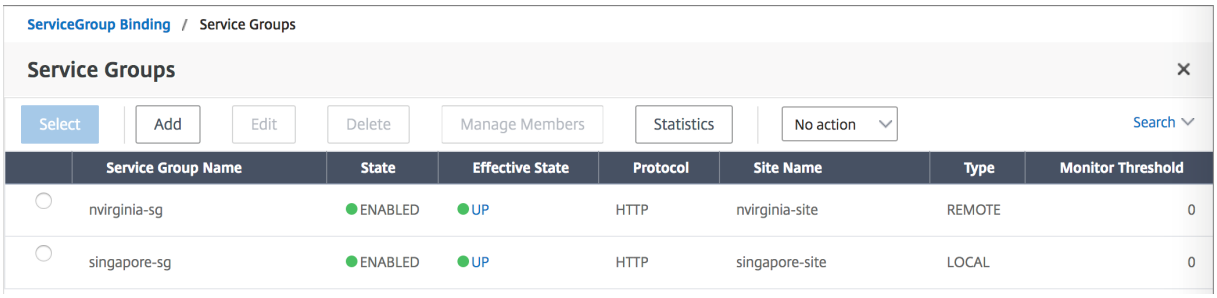
Lorsque le serveur virtuel GSLB est créé, cliquez sur **Aucune liaison GSLB ServiceGroup Service-Group**.

Cliquez sur **Ajouter** pour créer le serveur virtuel. Nommez le serveur, le type d'enregistrement DNS est défini comme A, le type de service est défini comme HTTP et cochez les cases Activer après la création et la journalisation AppFlow. Cliquez sur **OK** pour créer le serveur virtuel GSLB. (interface graphique de Citrix ADC)



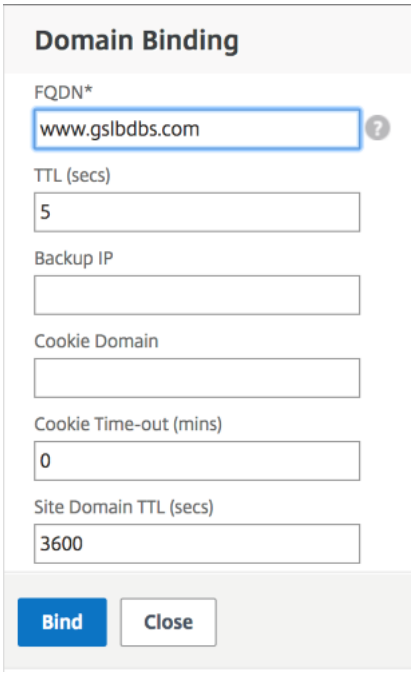
Étape 11 :

Sous Liaison ServiceGroup, utilisez **Sélectionner le nom du groupe** de services pour sélectionner et ajouter les groupes de services créés lors des étapes précédentes.



Étape 12 :

Configurez ensuite la liaison de domaine de serveur virtuel GSLB en cliquant sur **Aucune liaison de domaine de serveur virtuel GSLB**. Configurez le nom de domaine complet et la liaison, les autres paramètres peuvent être laissés comme valeurs par défaut.

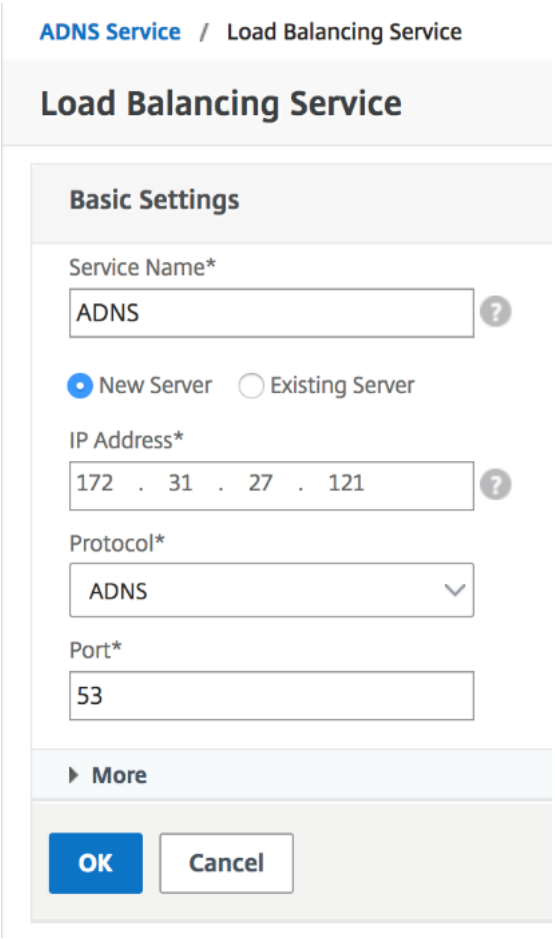


Étape 13 :

Configurez le service ADNS en cliquant sur **Aucun service**. Ajoutez un nom de service, cliquez sur **Nouveau serveur** et entrez l'adresse IP du serveur ADNS.

En outre, si votre ADN est déjà configuré, vous pouvez sélectionner **Serveur existant** , puis choisir votre ADNS dans le menu. Assurez-vous que le protocole est ADNS et que le trafic est sur le port 53.

Configurer la méthode comme LEASTCONNECTION et la méthode de sauvegarde comme ROUNDROBIN



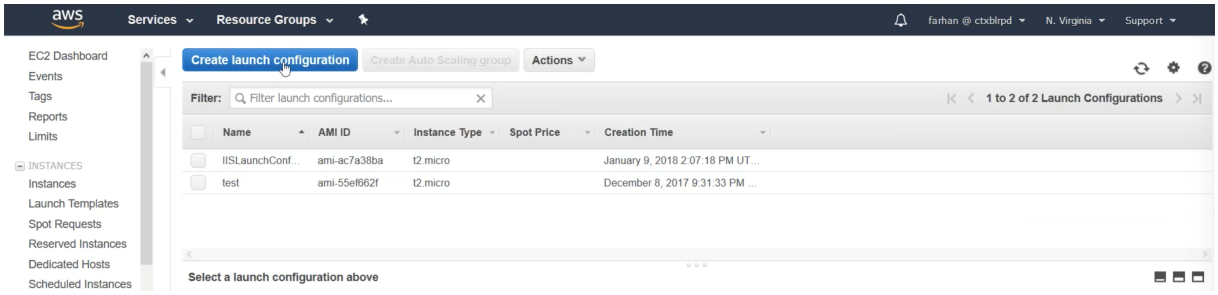
Mise à l'échelle automatique du back-end Citrix ADC avec AWS

AWS inclut une fonctionnalité appelée Auto Scaling qui active des instances supplémentaires exécutées dans AWS en fonction des règles définies par l'administrateur. Ces règles sont définies par l'utilisation du processeur et tournent autour de la création et de la suppression d'instances à la demande. Citrix ADC s'intègre directement à la solution AWS Auto Scaling, ce qui rend Citrix ADC conscient de tous les serveurs back-end disponibles qu'il peut équilibrer la charge. La limitation de cette fonctionnalité est qu'elle ne fonctionne actuellement qu'au sein d'un seul AZ dans AWS.

Configurer les composants AWS

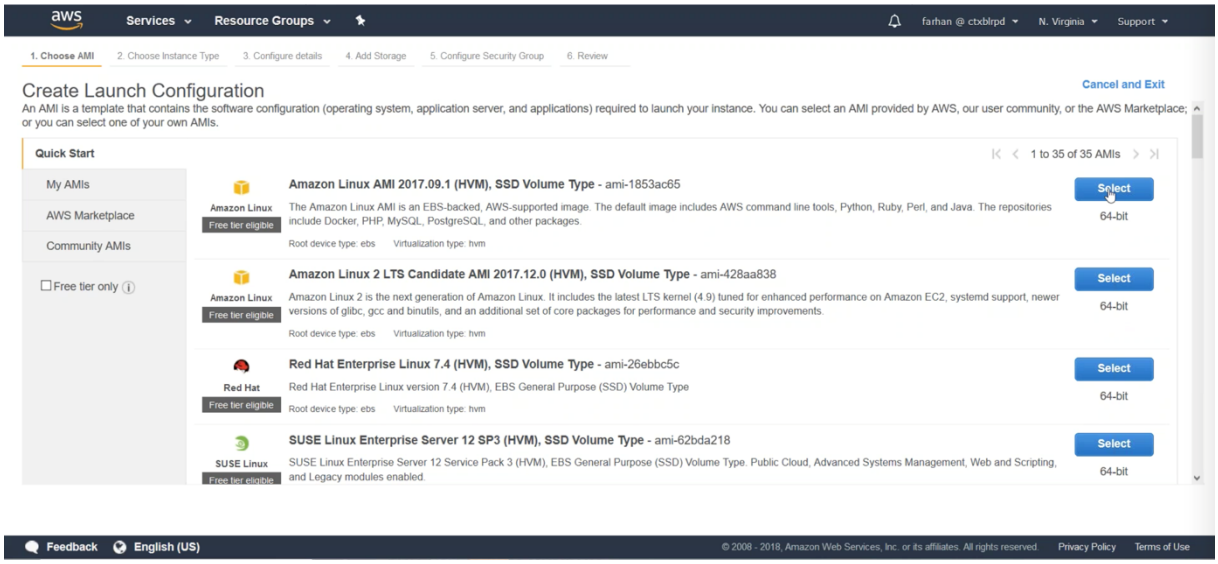
Étape 1 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **AUTO SCALING > Lancer la configuration**. Cliquez sur **Créer une configuration de lancement**.



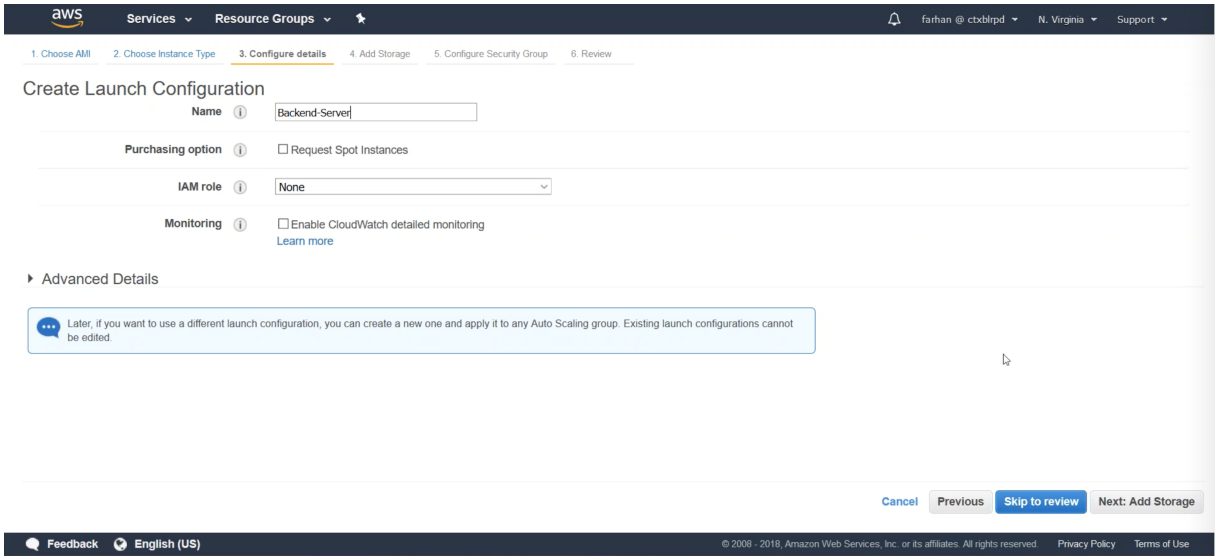
Étape 2 :

À partir de cette étape, vous pouvez choisir le type de serveur de votre choix. C'est là que vous configurez les machines virtuelles que vous souhaitez effectuer une mise à l'échelle automatique. Pour cet exemple, nous devons choisir **Amazon Linux AMI**.



Étape 3 :

Choisissez le type d'instance dont vous avez besoin en sélectionnant une variance potentielle pour les ressources back-end. Nommez votre instance pour le reste du runguide. Le nom de l'instance est connu sous le nom de serveur principal. Configurez le stockage pour l'instance et ajoutez-le à un groupe de sécurité, ou créez un nouveau groupe de sécurité qui englobe tous les composants AWS créés dans ce guide d'exécution.



Étape 4 :

Une note supplémentaire pour votre groupe de sécurité. Pour ce runguide, les ports ouverts suivants :

Type	Protocol	Port Range	Source
All traffic	All	All	0.0.0.0/0
SSH	TCP	22	185.25.64.249/32
SSH	TCP	22	125.16.224.135/32

Groupes et stratégies de mise à l'échelle automatique du back-end Citrix ADC

Configurer Citrix ADC frontal Auto Scaling dans AWS :

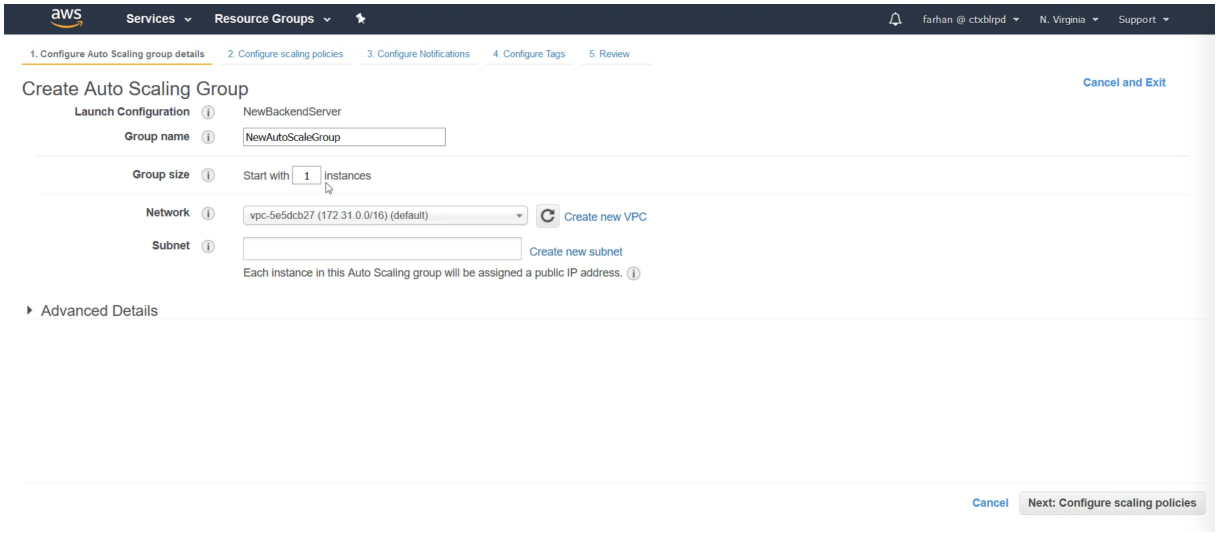
Étape 1 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **AUTO SCALING > Auto Scaling Group**.

Cliquez sur le bouton **Radio** pour créer un groupe Auto Scaling à partir d'une configuration de lancement existante. Assurez-vous de sélectionner le BackEndServer que nous avons créé à l'étape précédente du guide de laboratoire.

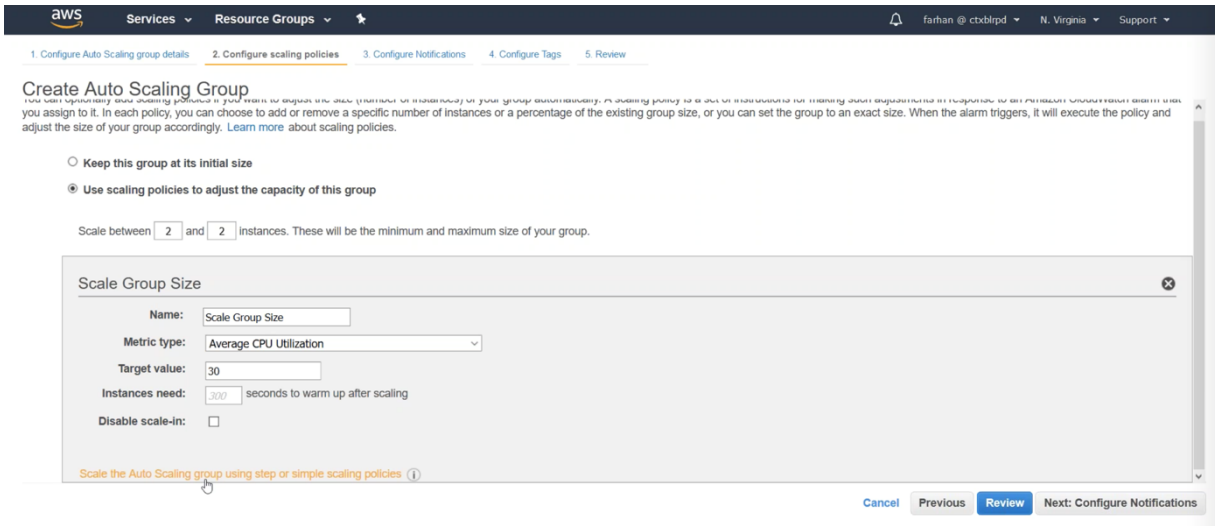
Sous **Créer un groupe Auto Scaling** , ajoutez le nom du groupe, choisissez la taille initiale du groupe, choisissez **Réseau et sous-réseau** ,
puis cliquez sur **Suivant** .

> Remarque :
>
> Le sous-réseau doit être accessible à partir de l'adresse IP du sous-réseau (SNIP) de Citrix ADC.



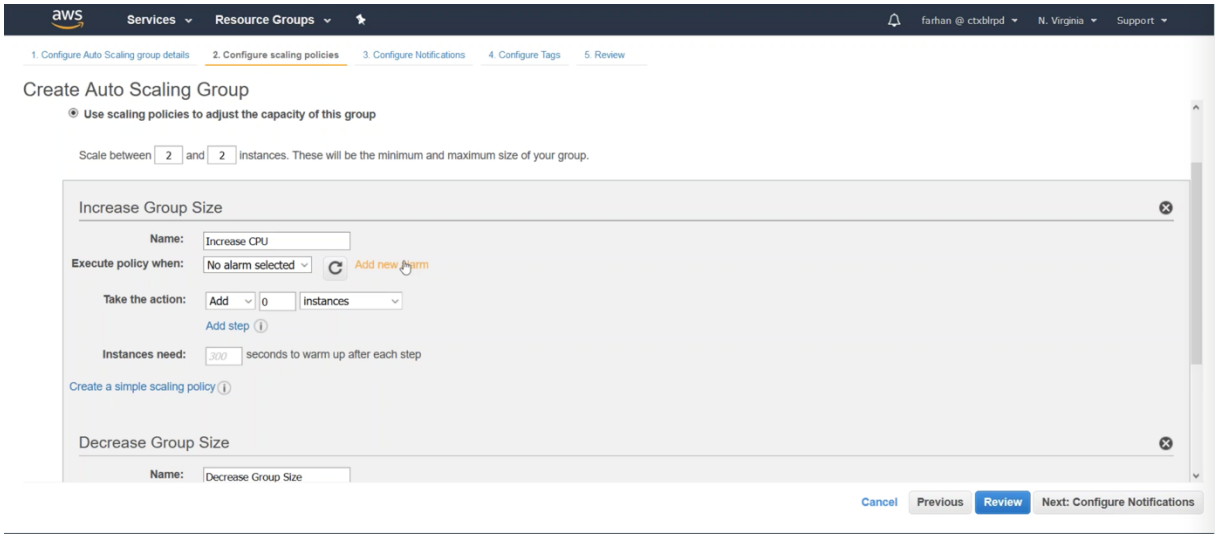
Étape 2 :

Sur la page de configuration **Créer un groupe Auto Scaling**, configurez vos stratégies de mise à l'échelle. Pour ce faire, cliquez sur le bouton radio permettant d'utiliser les stratégies de mise à l'échelle pour ajuster la capacité de ce groupe. Ensuite, cliquez sur **Mise à l'échelle du groupe Auto Scaling** à l'aide de stratégies de mise à l'échelle simple ou étape.



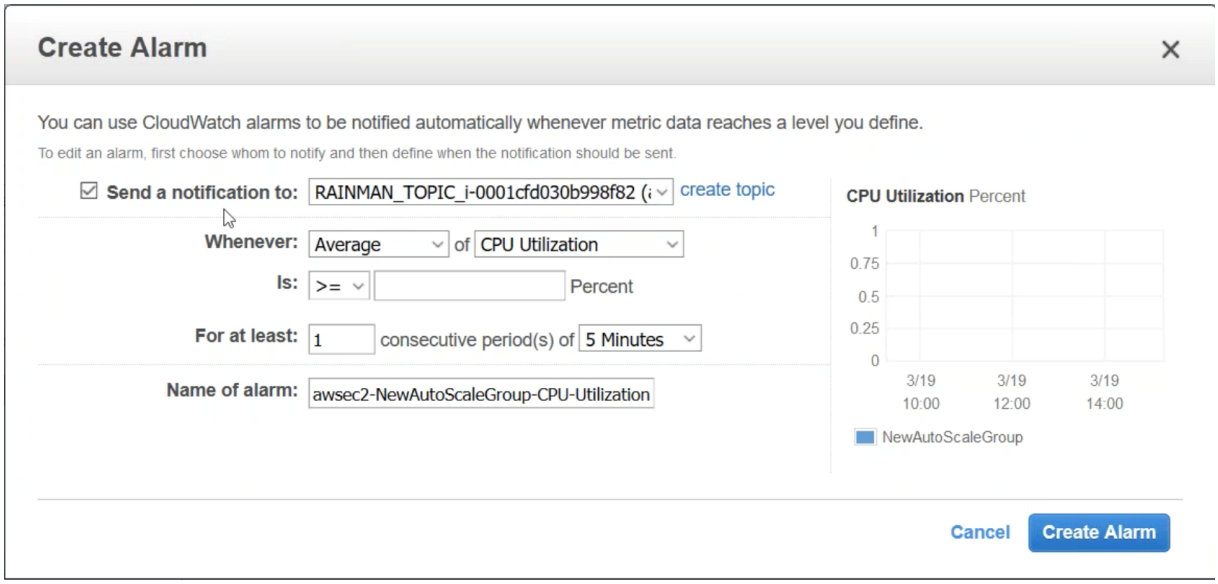
Étape 3 :

Sélectionnez **Ajouter une nouvelle alarme**.



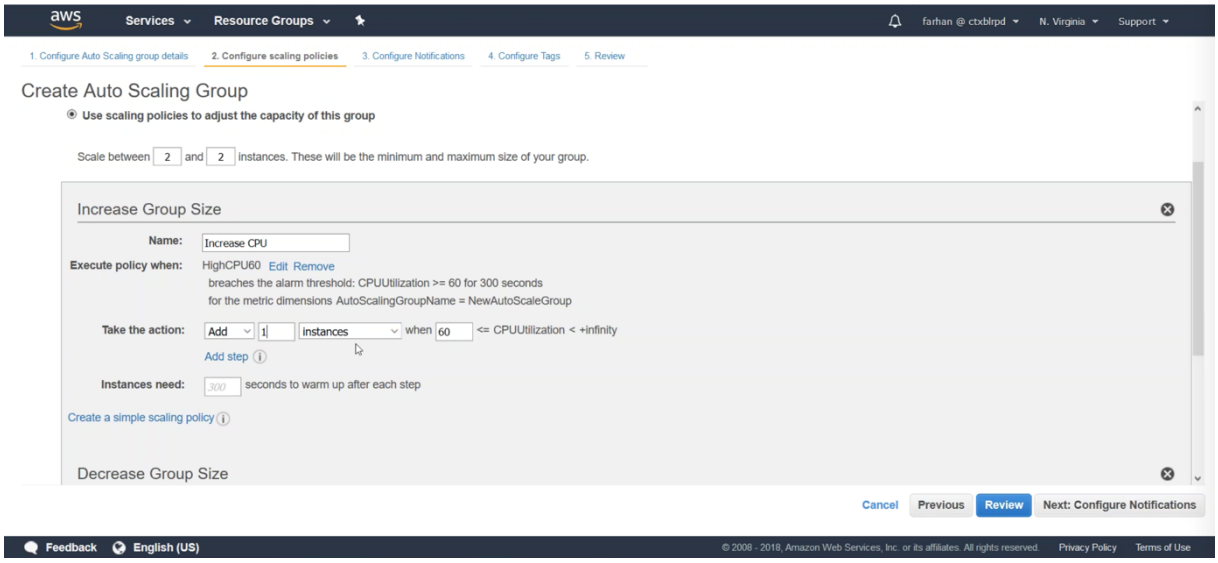
Étape 4 :

Pendant que vous créez l'alarme, configurez pour envoyer une notification à votre Citrix ADC. Configurez l'alarme de sorte que la moyenne d'utilisation du processeur soit > = 70 pendant au moins une période consécutive de 5 minutes. Appliquez la stratégie.



Étape 5 :

Configurez dans votre groupe Auto Scaling pour ajouter une instance lorsque la stratégie est déclenchée.



Étape 6 :

Configurez la même alarme et la même stratégie, mais cette fois pour supprimer un serveur principal lorsque le processeur moyenne est < = 30 pendant 5 minutes. Définissez la réduction de la taille du groupe sur Supprimer une instance lorsque la stratégie de diminution est déclenchée.

> Remarque :
>
> Pour la suppression de serveurs, nous informons Citrix ADC de ne pas envoyer de trafic à un serveur principal marqué pour suppression.

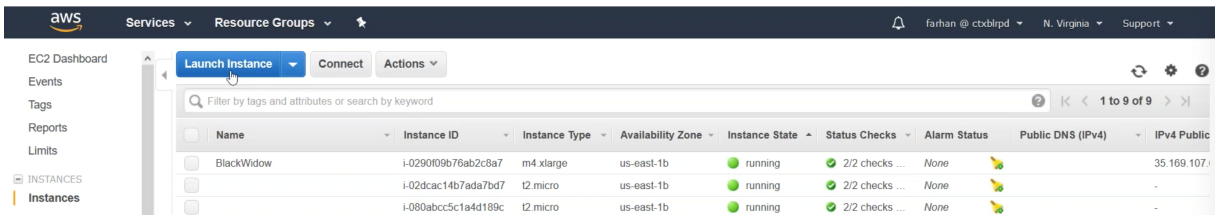
Cliquez sur Configurer les notifications et Configurer les balises pour consulter et créer le groupe Auto Scaling.

> Remarque :
>
> Les variables Min et Max peuvent être configurées pour définir le nombre le plus faible et le plus élevé d'instances qui seront créées et exécutées au sein du groupe Auto Scaling. Actuellement, AWS prend en charge la rotation d'instances supplémentaires avec une seule interface réseau.

Créer un Citrix ADC dans AWS

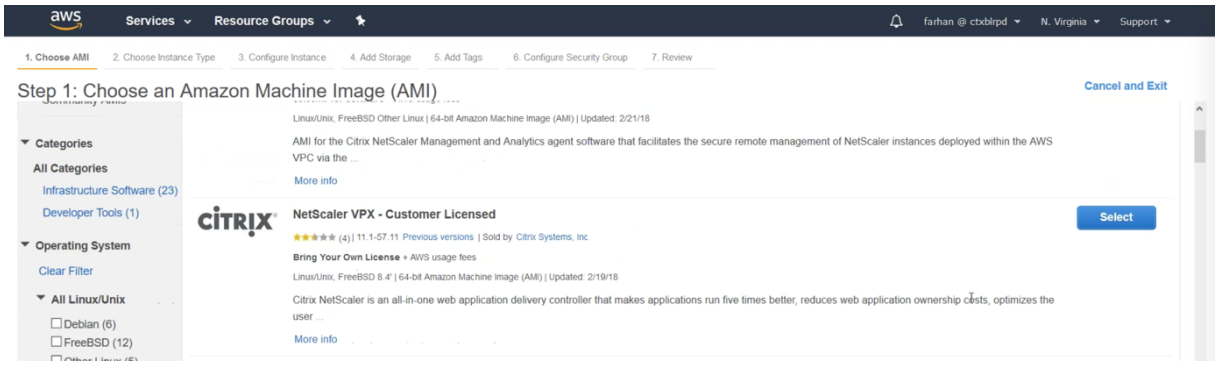
Étape 1 :

Connectez-vous à votre **groupe de ressources AWS** et accédez à **EC2**. Dans EC2, accédez à **Instances > Instances**.



Étape 2 :

Accédez à AWS Marketplace sur la gauche, puis recherchez Citrix ADC. Choisissez **Citrix Networking VPX — Licence client**. Assurez-vous que votre numéro de version est 12.0.51.x pour utiliser Auto Scaling. Vous pouvez sélectionner les versions précédentes pour choisir une version de Citrix ADC prenant en charge Auto Scaling.



Étape 3 :

Accédez à AWS Marketplace sur la gauche, puis recherchez Citrix ADC. Choisissez **Citrix Networking VPX — Licence client**. Assurez-vous que votre numéro de version est 12.0.51.x pour utiliser Auto Scaling. Vous pouvez sélectionner les versions précédentes pour choisir une version de Citrix ADC prenant en charge Auto Scaling.

Choisissez le type d'instance, par exemple General Purpose m4.xlarge 4vCPU et 16gb RAM. Cliquez sur **Suivant**.

Étape 4 :

Sous l'onglet **Configurer les détails de l'instance** , sélectionnez le **sous-réseau** (trois sous-réseaux doivent éventuellement être configurés pour NSIP, SNIP et VIP/passerelle). En outre, vous devez ajouter un rôle IAM. Cliquez pour créer un nouveau rôle IAM. Ajoutez les rôles IAM qui se trouvent à l'étape suivante. Une fois ce rôle créé, vous devez l'ajouter à votre profil Cloud sur votre Citrix ADC.

Étape 5 :

Les configurations pour le profil Cloud sont les suivantes :

Par défaut, le modèle CloudFormation crée et joint le rôle IAM ci-dessous

```
"Version": "2012-10-17",
"Statement": [
   {

       "Action": [
       "ec2:DescribeInstances",
       "ec2:DescribeNetworkInterfaces",
       "ec2:DetachNetworkInterface",
```



```
            "ec2:AttachNetworkInterface",
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:RebootInstances",
            "autoscaling:\*",
            "sns:\*",
            "sqs:\*"
            "iam: SimulatePrincipalPolicy"
            "iam: GetRole"
            ],
            "Resource": "\*",
            "Effect": "Allow"
        }

    ]
    }

<!--NeedCopy-->
```

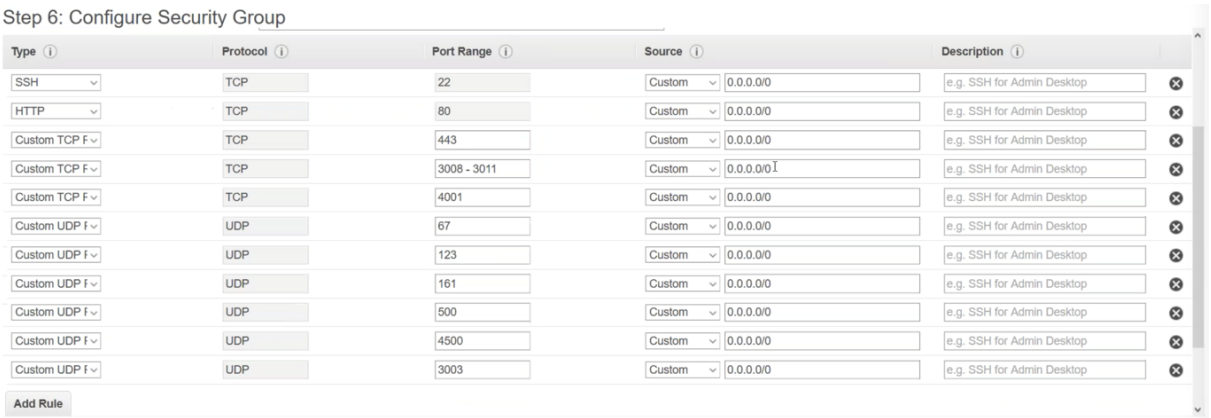
Étape 6 :

Cliquez sur l'option **Ajouter un stockage** . Sous l'onglet **Ajouter des balises** , définissez la valeur de clé comme Nom et la valeur comme Citrix ADC-AutoScale pour marquer ces ressources EC2.

Étape 7 :

Sous l'onglet **Configurer le groupe de sécurité** , créez un nouveau groupe de sécurité avec les ports requis suivants :

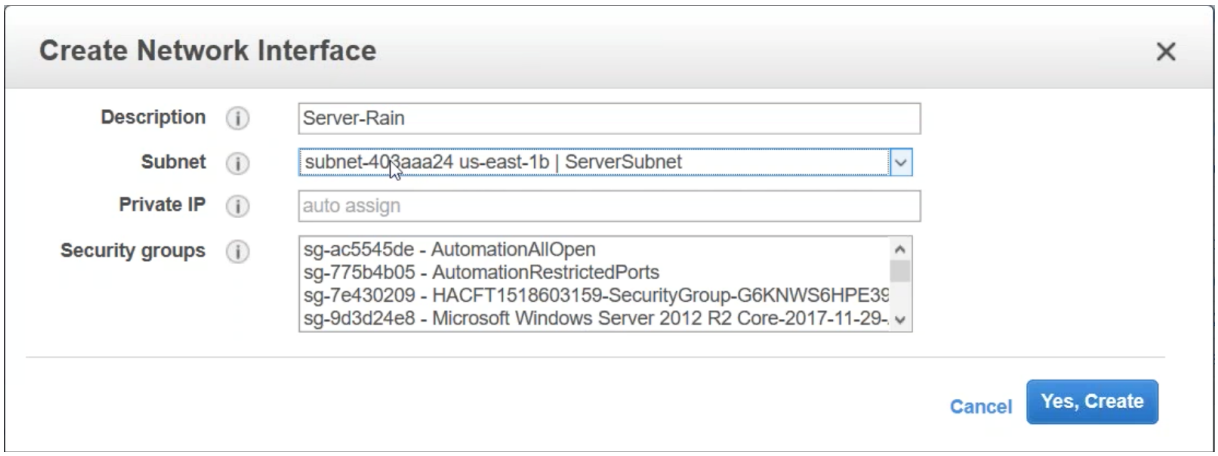
Vérifiez et lancez l'instance.



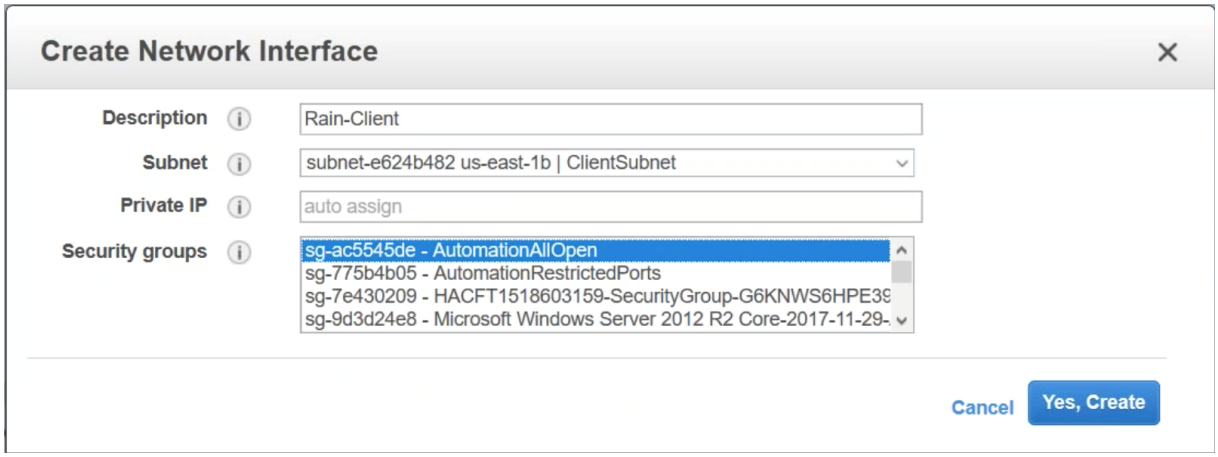
Étape 8 :

Accédez à **NETWORK & SECURITY > Interfaces réseau** , puis cliquez sur **Créer une interface réseau** .

Ajoutez une description, puis sélectionnez un sous-réseau. Ce sous-réseau est utilisé pour votre SNIP, il doit donc être placé sur un sous-réseau du réseau interne. En outre, choisissez le groupe de sécurité créé à l'étape précédente. Cliquez sur **Oui, Créer**.



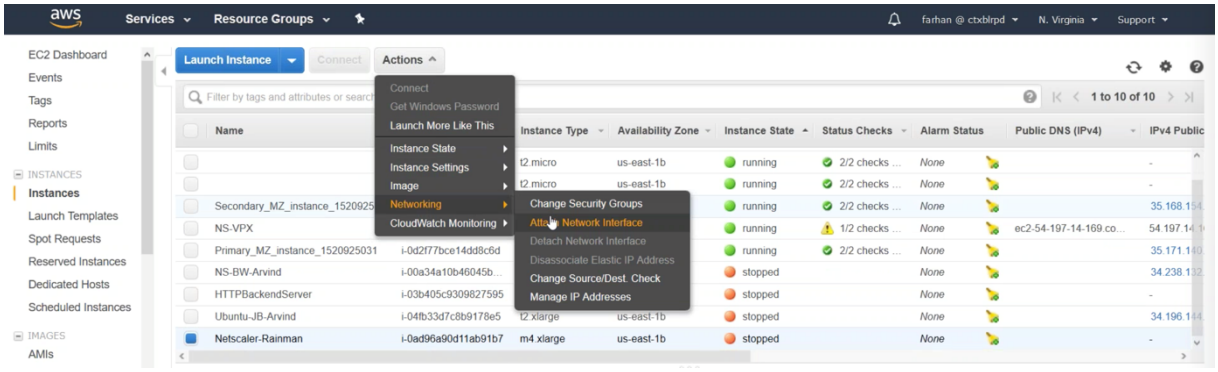
Ajoutez une interface réseau supplémentaire. Il s'agit d'un sous-réseau public pour votre Gateway/LB VIP. Créez une description et choisissez le groupe de sécurité configuré ci-dessus.



Étape 9 :

Revenez à **Instances** et sélectionnez votre Citrix ADC. Pour ajouter les interfaces réseau à Citrix ADC, l'instance doit être arrêtée. Dans la liste **Actions** , sélectionnez **État de l'instance** , puis cliquez sur **Arrêter** .

Cliquez de nouveau sur le bouton **Actions** et accédez à **Mise en réseau et connexion de l'interface réseau** .



L'interface NSIP est déjà attachée à la machine virtuelle, l'interface suivante à ajouter doit être la LB-VIP, suivie de l'ajout de l'interface serveur/interne pour le SNIP. Une fois les interfaces réseau attachées, l'instance peut être démarrée.

Configurez une nouvelle IP Elastic et associez-la à votre interface NSIP.

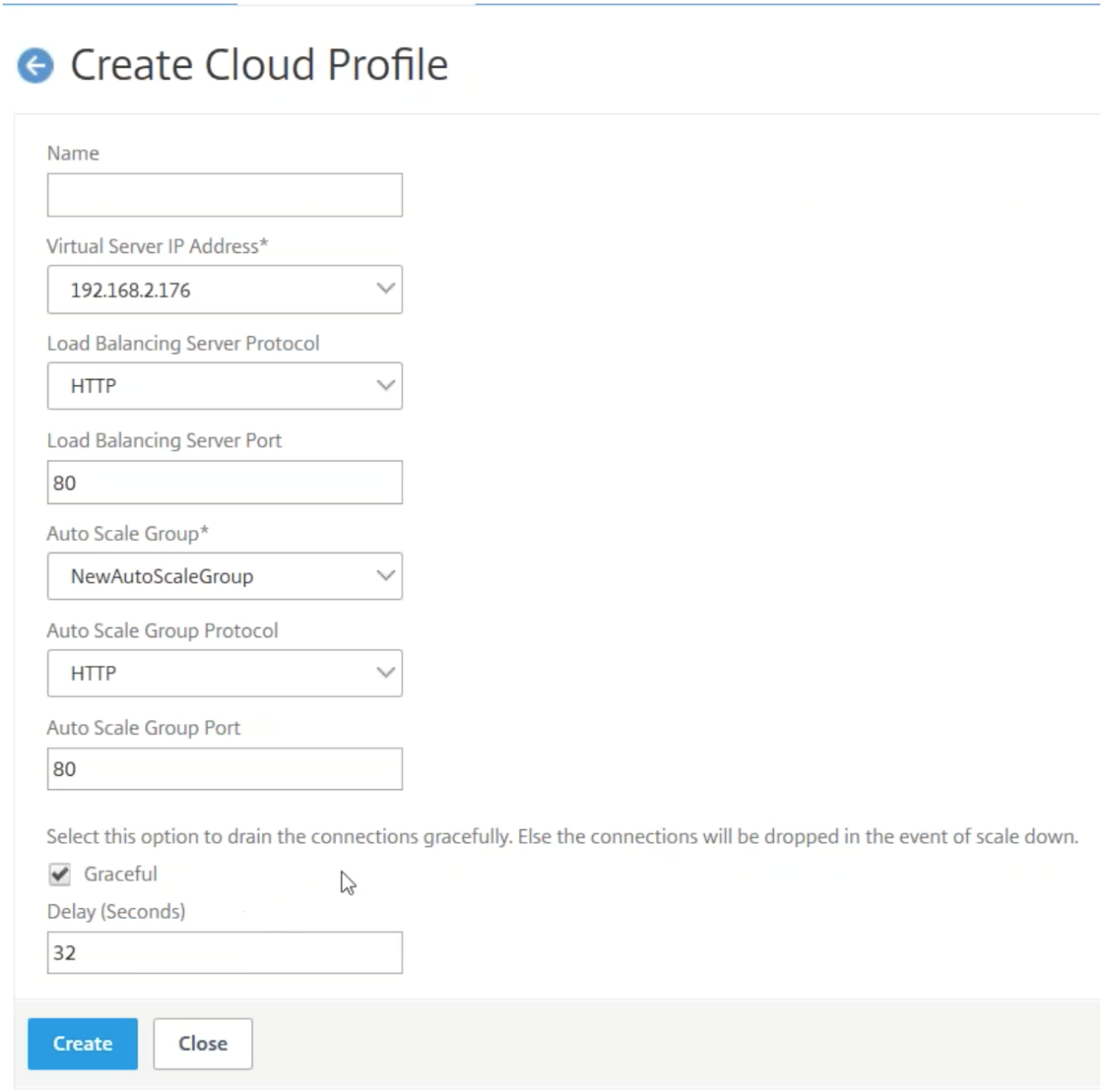
Configurer Citrix ADC pour qu'il s'intègre à AWS Auto Scaling

Étape 1 :

Accédez à l'adresse IP Elastic que vous avez associée au NSIP à l'étape précédente de ce guide de laboratoire pour accéder à la console Citrix ADC Management.

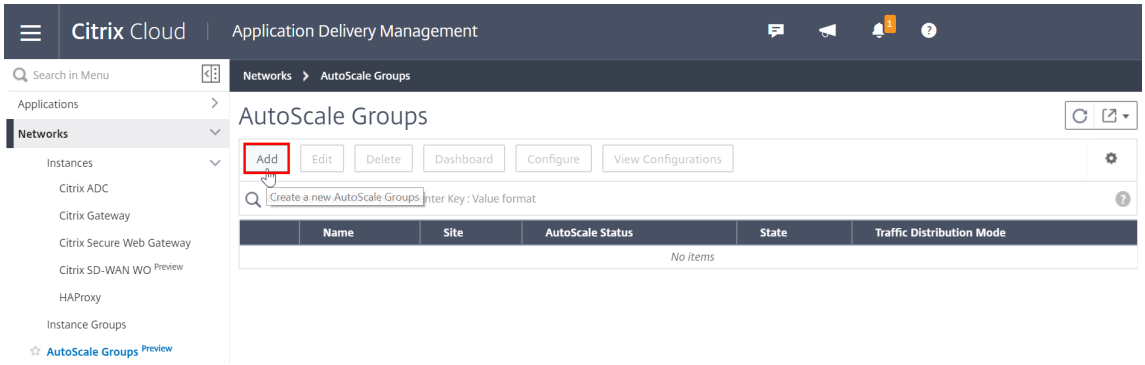
La première étape de configuration de Citrix ADC consiste à attacher un profil Cloud. Cliquez sur **AWS** , puis sur **Cloud Profile** . Cliquez ensuite sur **Ajouter** pour créer un profil Cloud.

Indiquez un nom pour le profil cloud. L'adresse IP du serveur virtuel doit être renseignée et corrélée avec une adresse IP interne sur votre serveur Citrix ADC. Le groupe Auto Scale est celui que vous avez créé lors des étapes précédentes de ce guide de laboratoire. Sélectionnez **Graceful**, cela permet de supprimer un délai d'attente pour les instances back-end, ce qui permet à tous les transferts de paquets de se terminer et de ne pas interrompre les sessions pendant la période de grâce. Le délai de la période de grâce peut être ajusté.

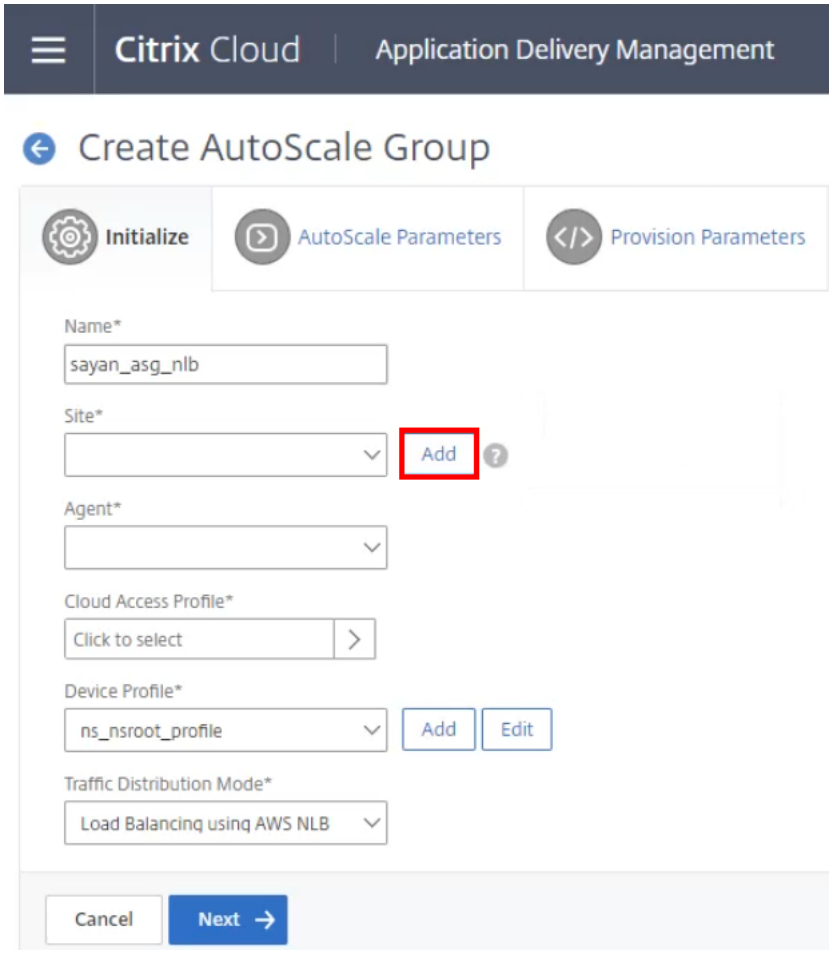


Configurer Citrix ADC frontal Auto Scaling dans AWS

1. Pour créer le groupe Auto Scaling, connectez-vous à Citrix ADM.
2. Accédez à **Networks > AutoScale Groups**, puis cliquez sur **Add**pour créer le nom du groupe.

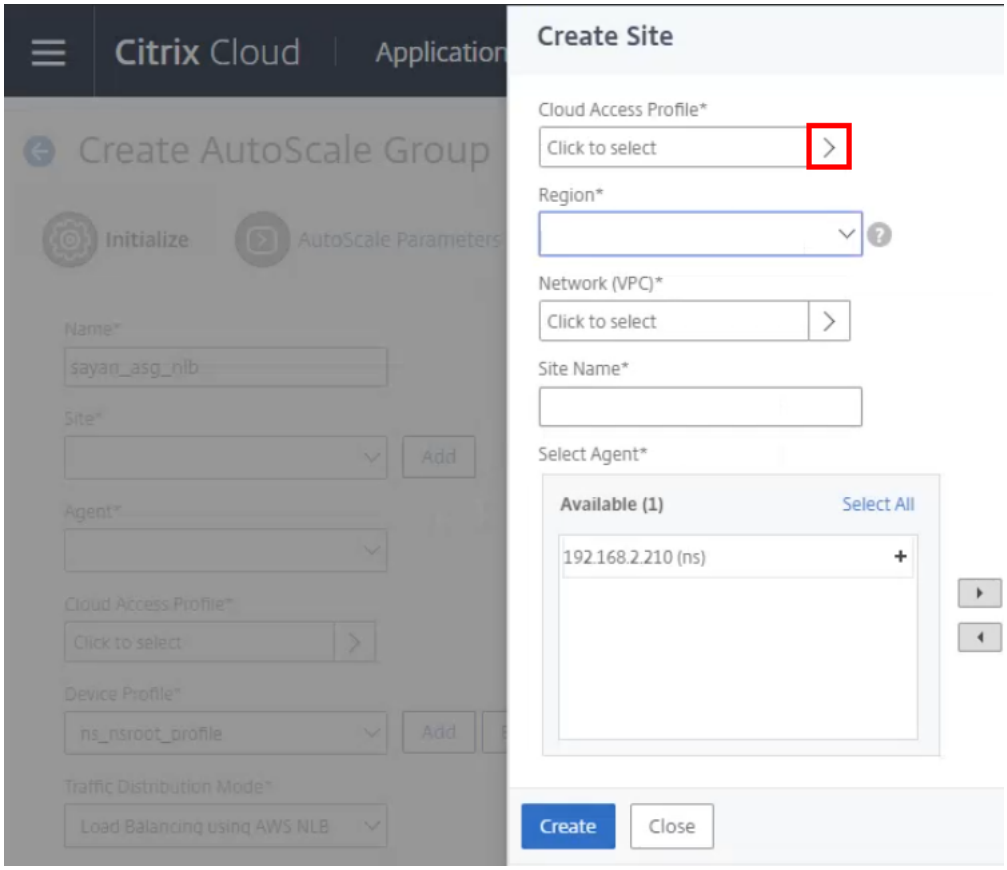


3. Dans le paramètre **Site** , cliquez sur **Ajouter** .

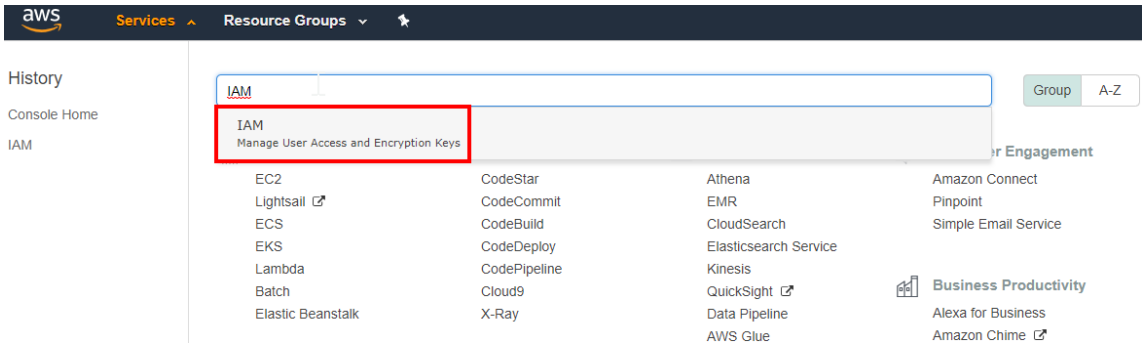


Créer un profil d’accès au cloud

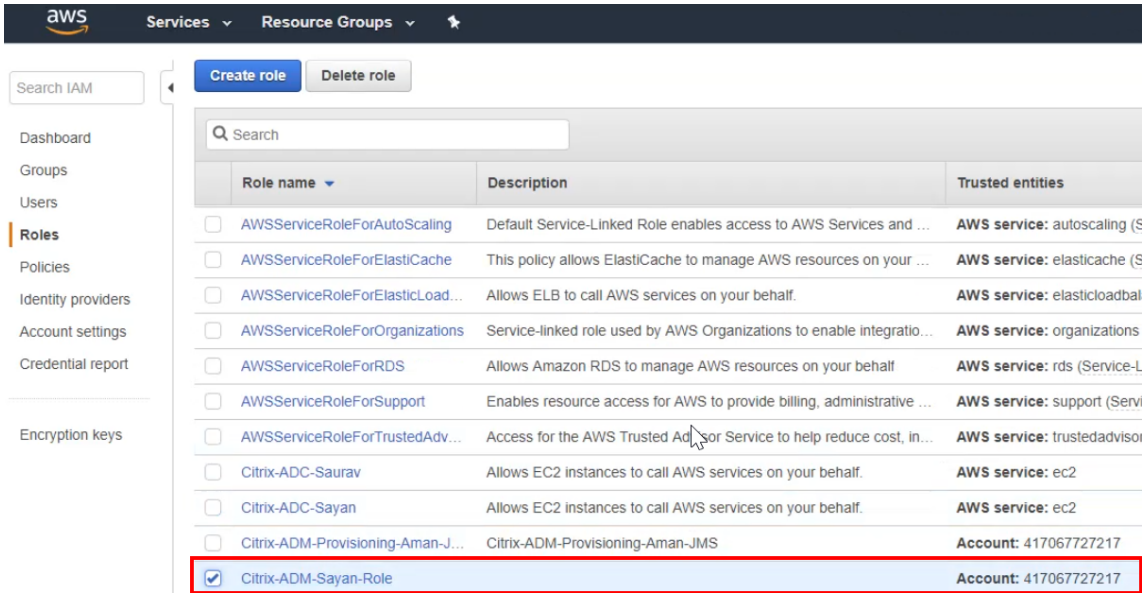
1. Lors de la création d’un site, ajoutez **AWS**dans le **profil d’accès au cloud**.



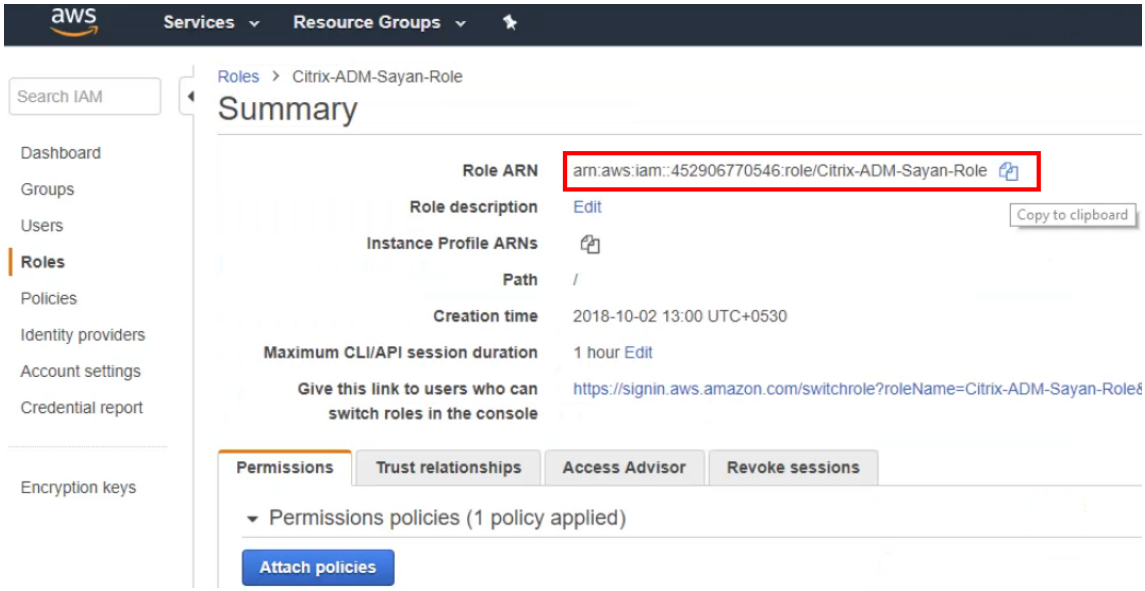
2. Nommez le profil et connectez-vous à votre portail AWS. Recherchez le service de **gestion des identités et des accès (IAM)** pour gérer les clés d'accès utilisateur et de chiffrement.



3. Dans le tableau de **bord IAM**, sélectionnez **Rôles**dans le panneau de gauche et recherchez le rôle Citrix ADM correspondant.

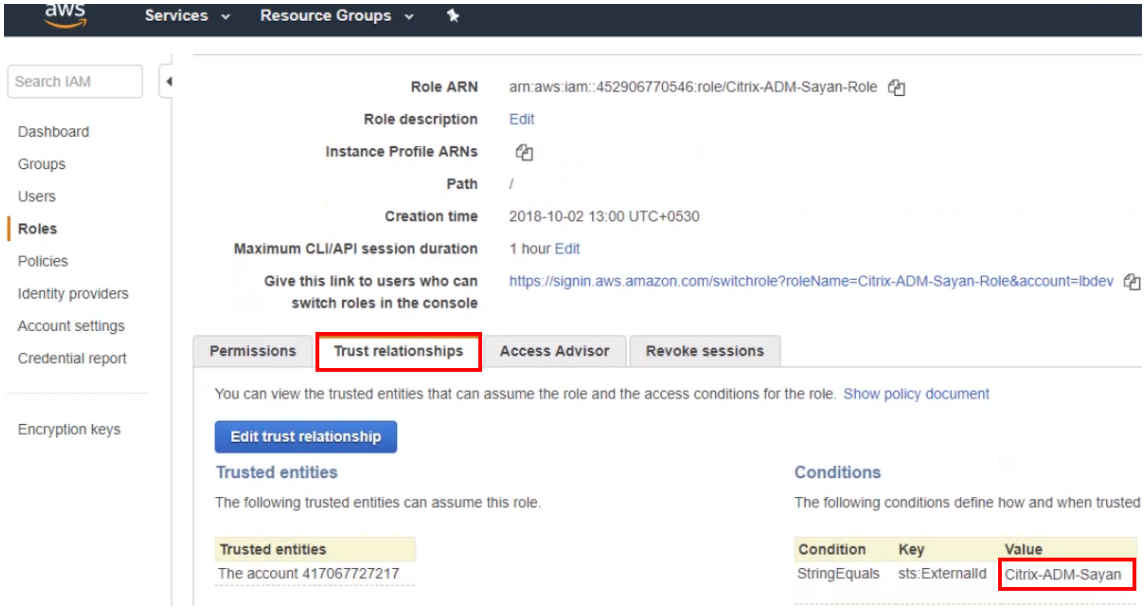


4. Copiez l' **ARN de rôle dans** le Presse-papiers.

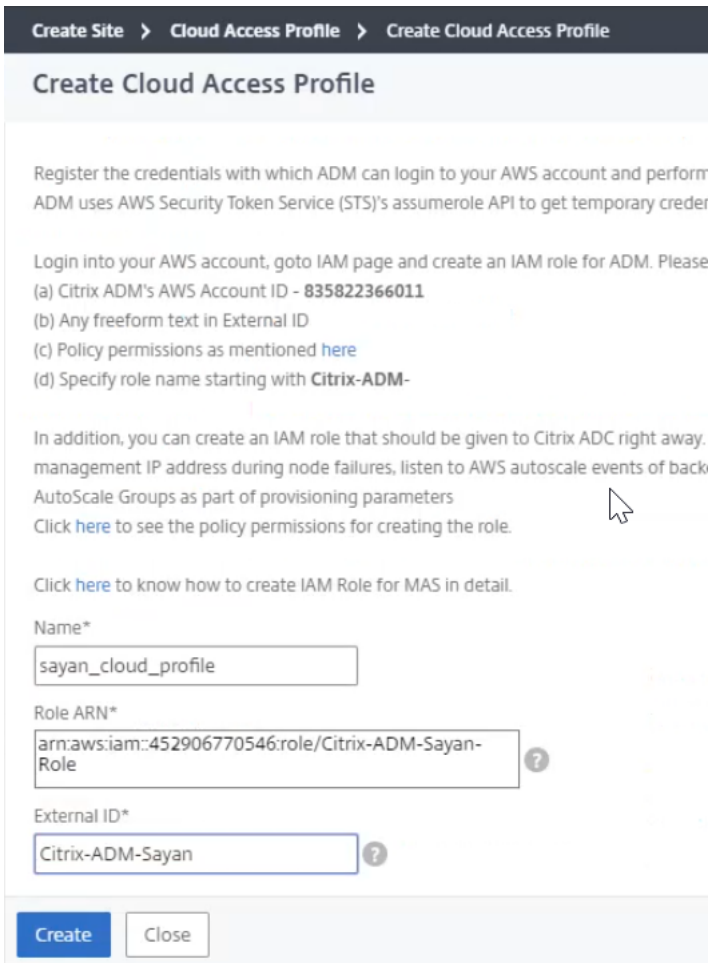


5. Après avoir copié le nom, revenez à la console Citrix ADM et collez le nom dans le champ de texte **ARN de rôle** .

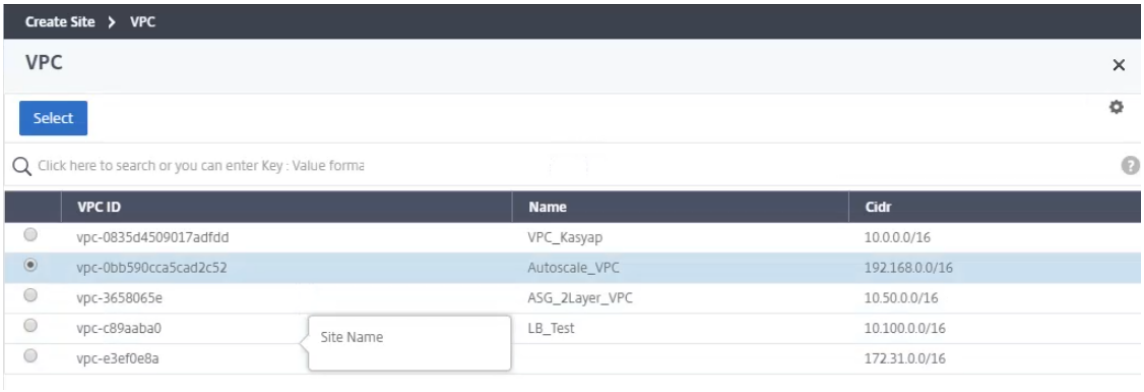
6. Pour obtenir l'ID externe, revenez au tableau de bord **Rôles** AWS, accédez à l'onglet **Relations d'approbation** et copiez la valeur à partir des **Conditions** .



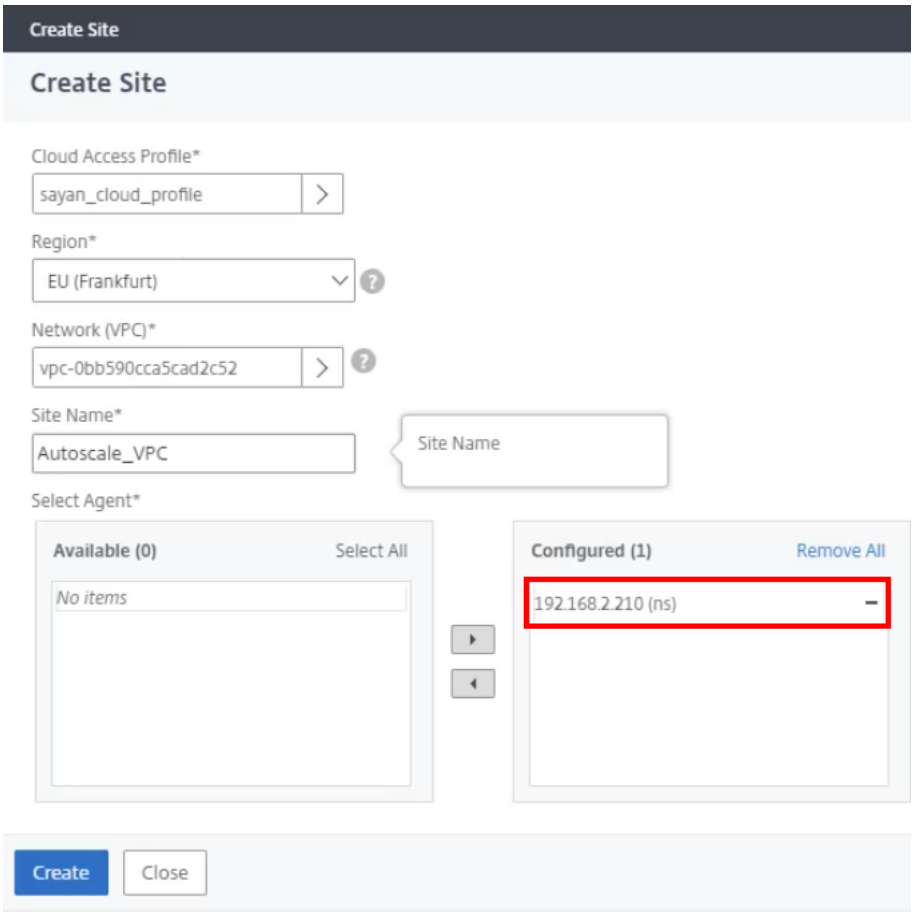
7. Dans la console Citrix ADM, collez la valeur dans le champ **ID externe** et cliquez sur **Créer** .



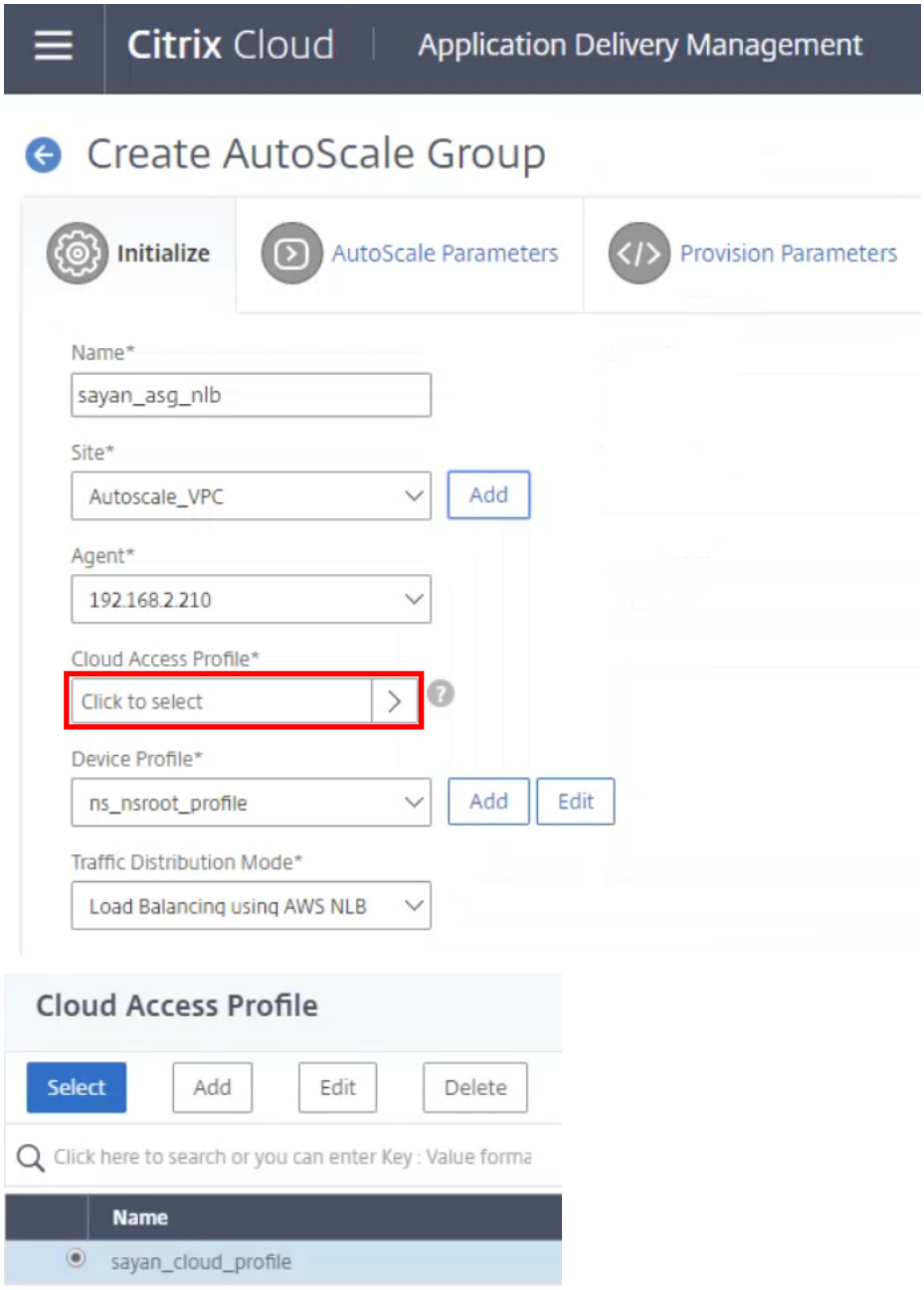
8. Sélectionnez la région, puis choisissez le réseau VPC approprié.



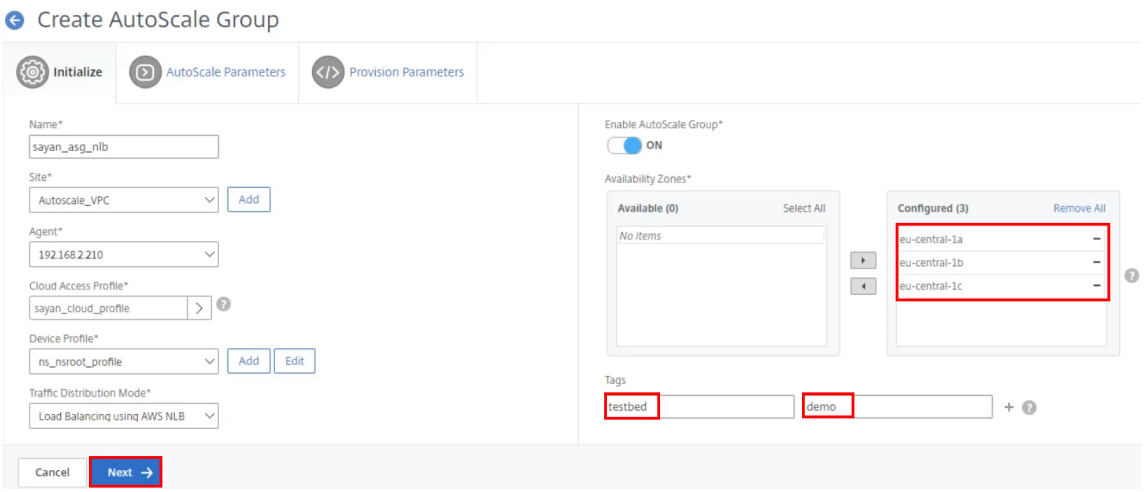
9. Déplacez l'agent de **Disponible** à **Configuré** .



10. Sélectionnez le **profil d'accès Cloud**correspondant.

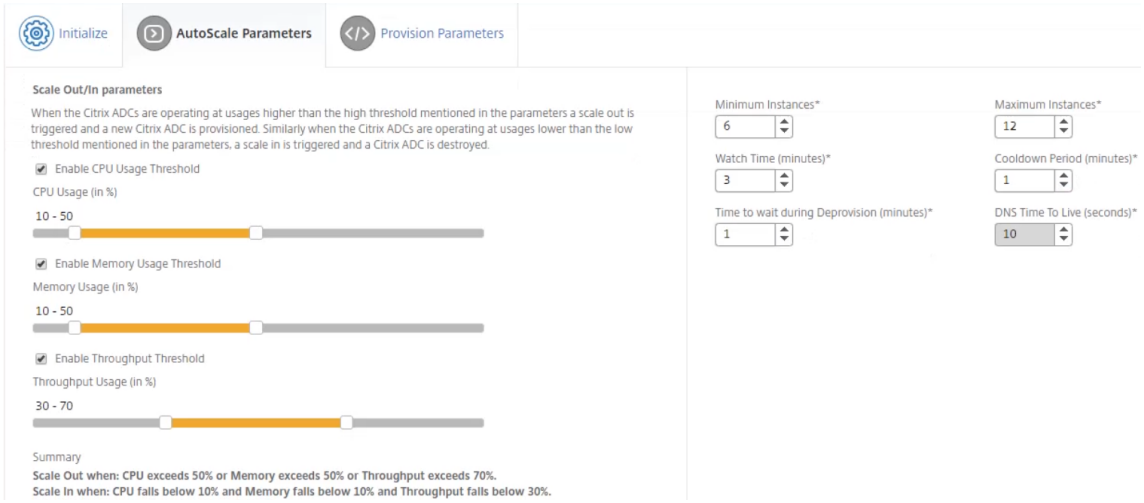


11. Une fois chargées, déplacez les zones de disponibilité de **Disponible** à **Configuré** et ajoutez les balises correspondantes au **groupe AutoScale** . Sélectionnez **Suivant** pour commencer à définir les paramètres **Autoscale**.

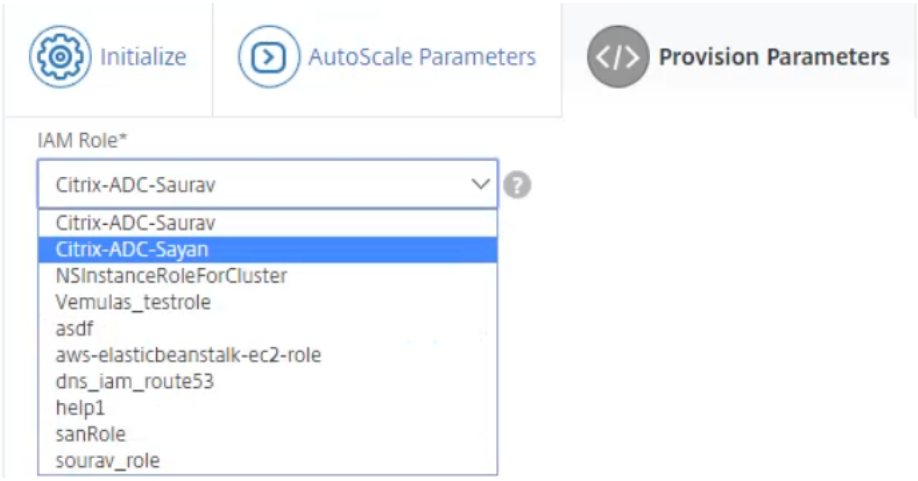


Définir les paramètres AutoScale

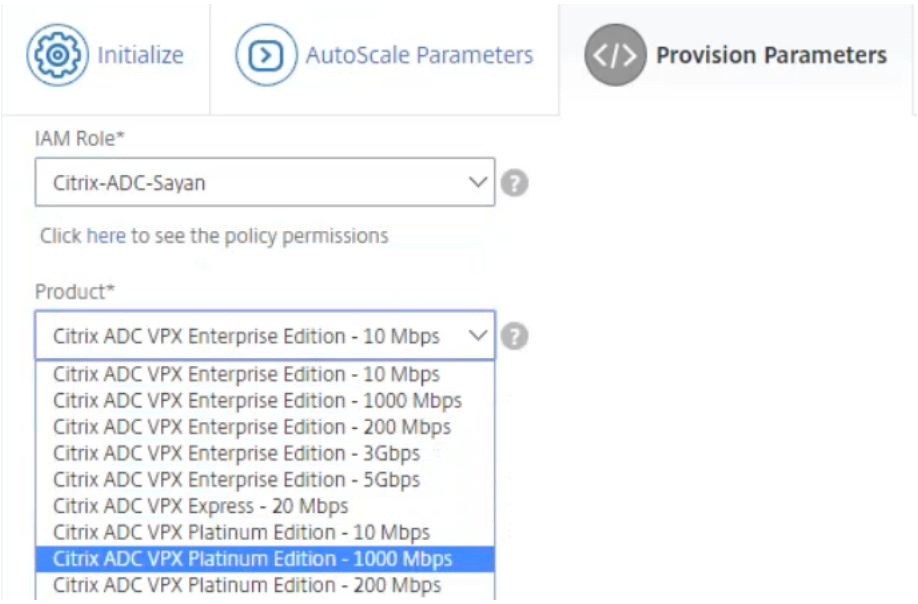
1. Lorsque vous définissez les paramètres AutoScale, ajustez les **seuils** et **paramètres** aux paramètres souhaités. Cliquez ensuite sur **Suivant** pour commencer à configurer les **paramètres Paramètres de provisioning** .



2. Dans la section **Paramètres de mise à disposition**, sélectionnez le rôle dans le champ **Rôle IAM**.

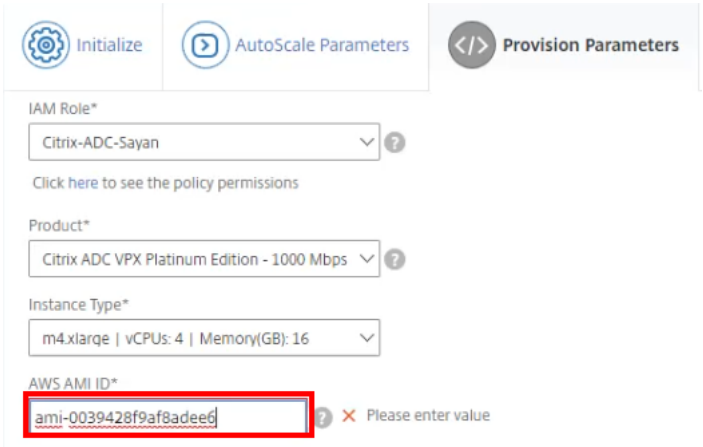


3. Sélectionnez le produit et l'édition Citrix ADC appropriés.

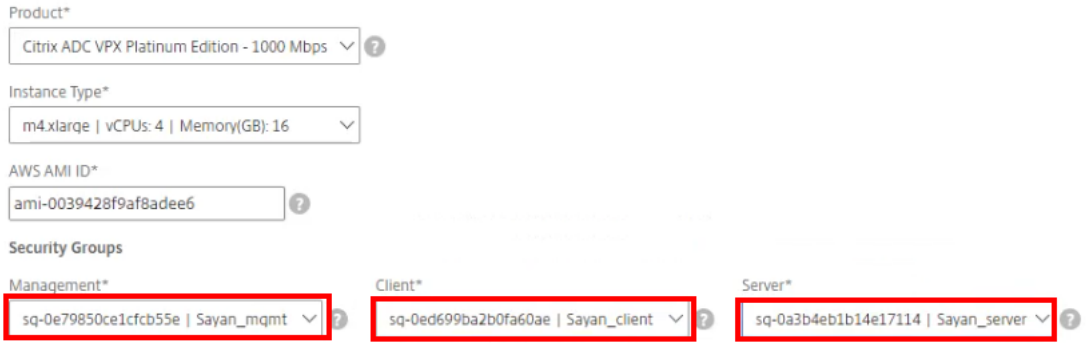


4. Rassemblez l'ID Amazon Machine Image (AMI) à partir des instances spécifiques d'AWS. Saisissez cet ID dans le champ **ID de l'AMI AWS** .

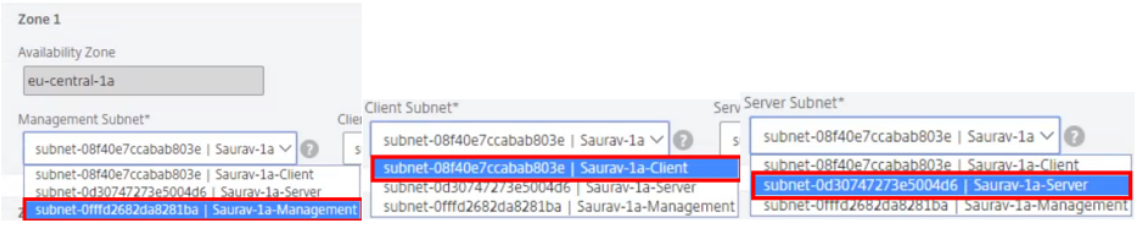
```
AMI ID:
--------------
ami-0039428f9af8adee6
```

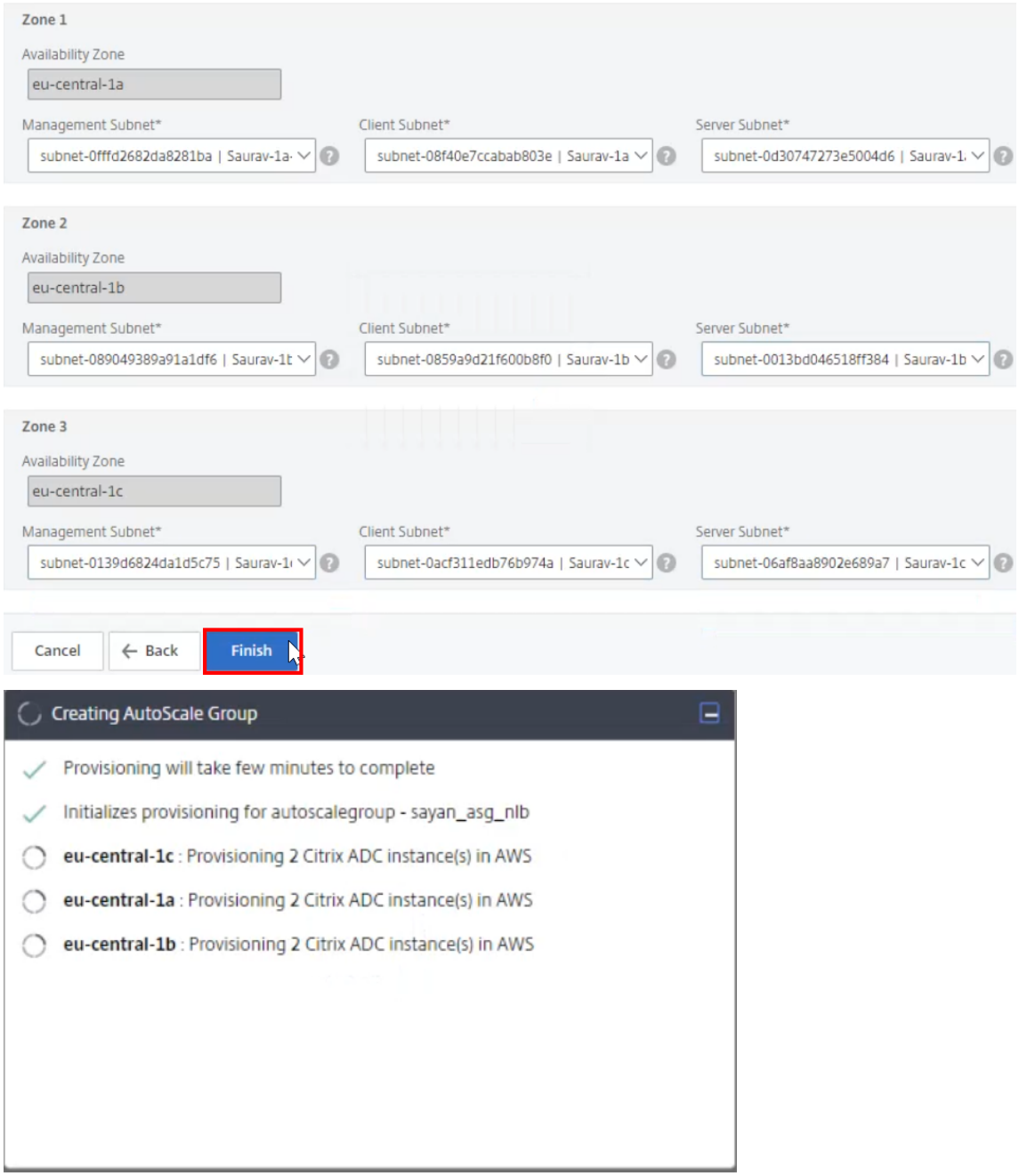
5. Après avoir ajouté l' **ID AMI**, mettez à jour les **groupes de sécurité**avec les groupes appropriés.



6. Pour démarrer les configurations des zones 1, 2 et 3, affectez les sous-réseaux de gestion, client et serveur correspondants.

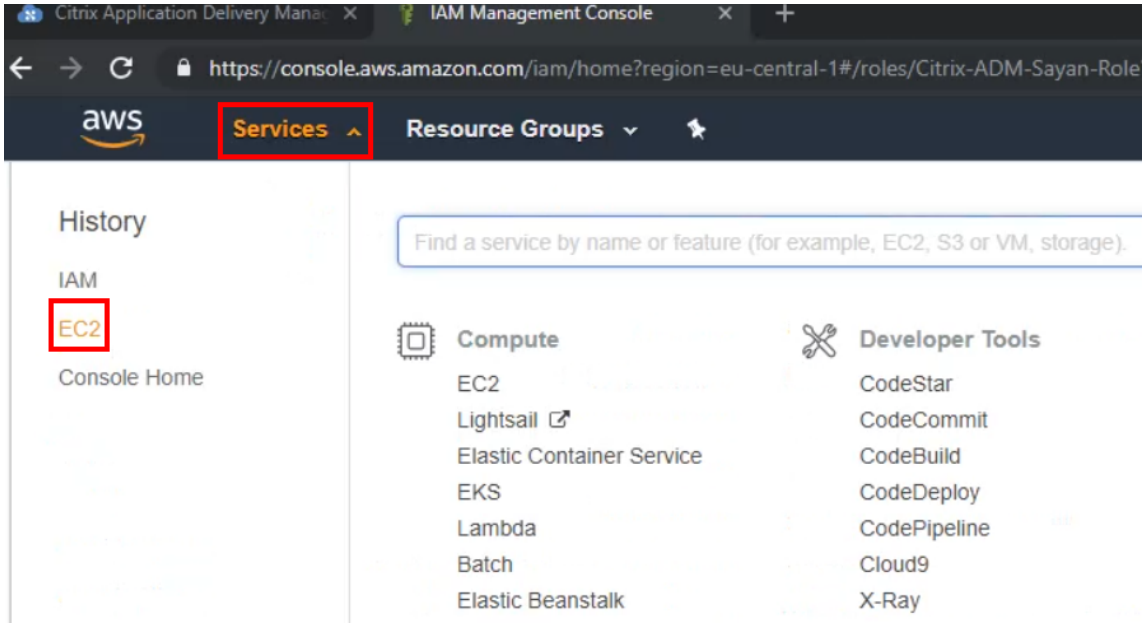


7. Cliquez sur **Terminer** pour créer la configuration de ce groupe Auto Scaling. Le processus de création peut prendre jusqu'à 10-20 minutes.

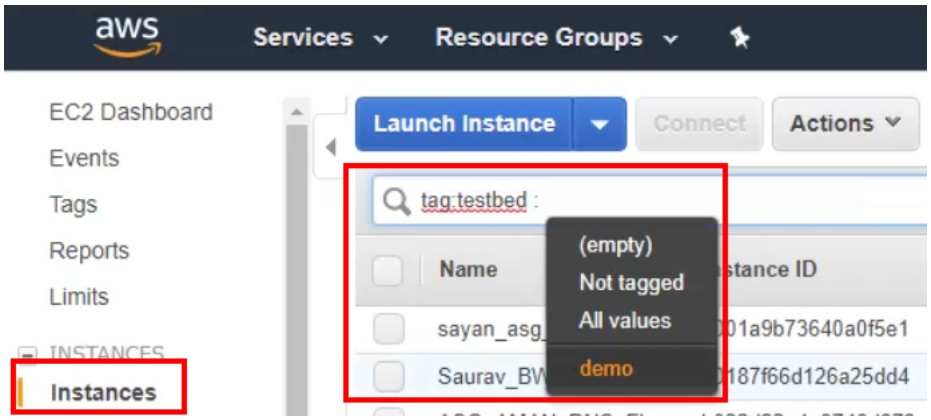


Initialiser les instances dans AWS

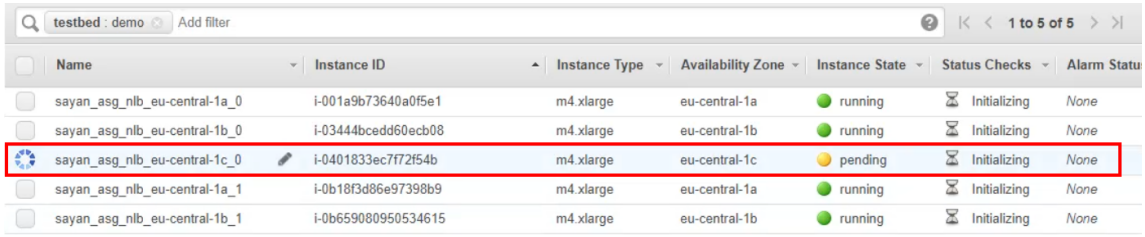
1. Pendant la création du groupe Auto Scaling, ouvrez votre console AWS et accédez à l'onglet **Services** . Sélectionnez le **service Amazon Elastic Compute Cloud (EC2)** .



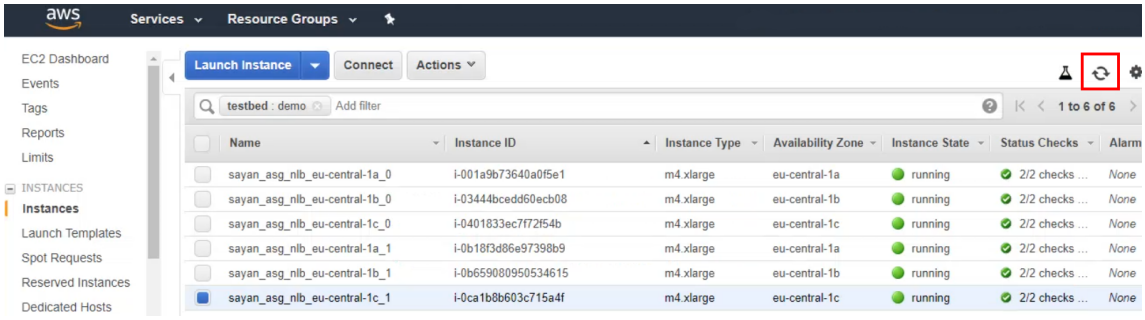
2. Dans le tableau de bord EC2, sélectionnez l'onglet **Instances** et filtrez à l'aide des balises définies dans la section **Groupe AutoScale**.



3. Une fois filtré, vous pouvez voir l'instance en attente qui est toujours en cours d'initialisation.

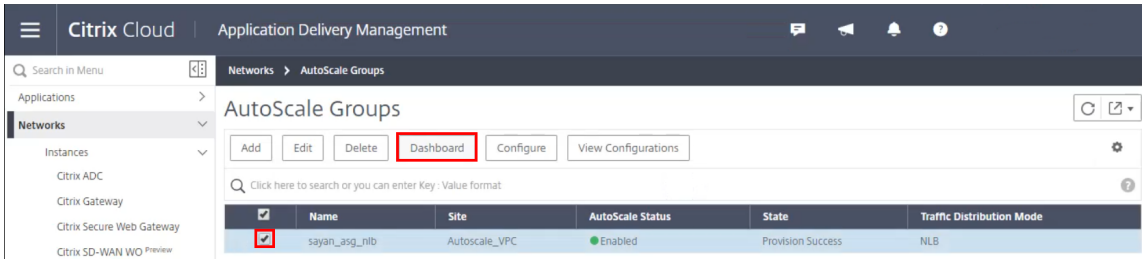


4. Les instances doivent terminer leur initialisation après leur création.

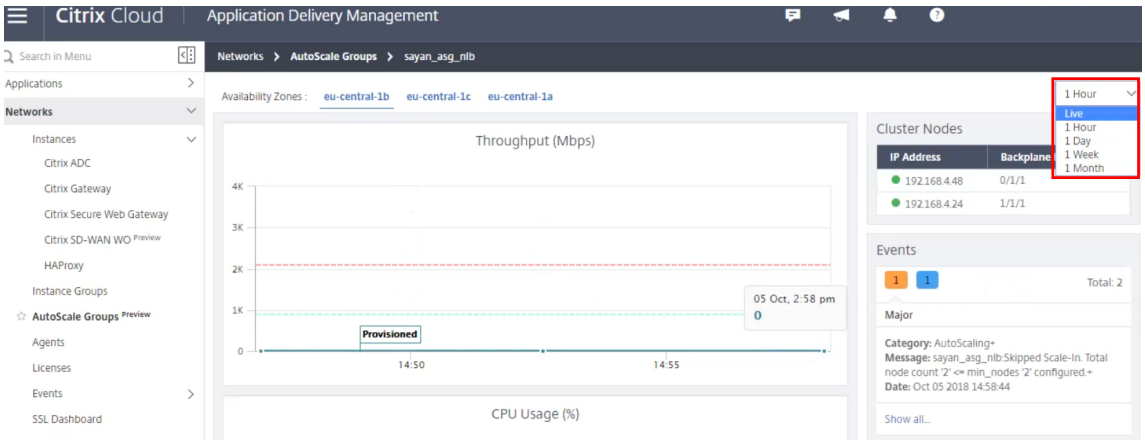


Surveiller les événements du groupe Auto Scaling

1. Après avoir créé le groupe Auto Scaling, sélectionnez votre groupe et passez au tableau de bord **Groupe AutoScale** .

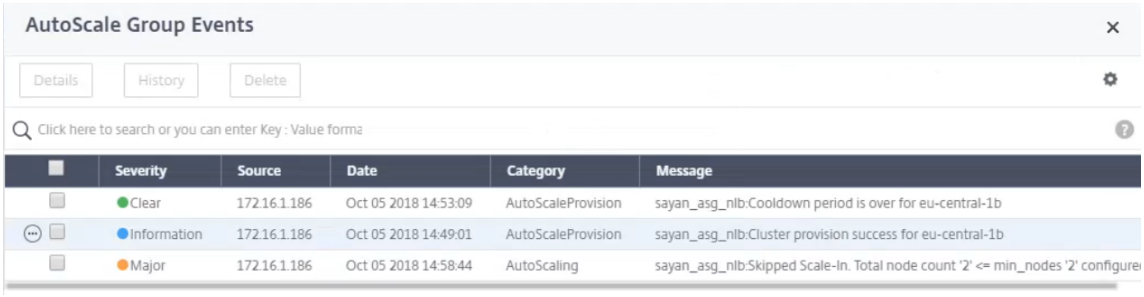


2. Filtrez des périodes spécifiques pour surveiller le groupe Auto Scaling. Pour obtenir des informations en temps réel, modifiez la période de surveillance en **direct**.



3. Cliquez sur le point de données suivant présenté dans le graphique pour afficher les événements de groupe.

4. Lorsque vous affichez les événements en direct spécifiques, vous pouvez surveiller les événements spécifiques du groupe Auto Scaling correspondant.



Provisionner des instances Citrix ADC VPX à l'aide du service Citrix ADM

Le service Citrix ADM est une solution basée sur le cloud qui permet de surveiller les instances de Citrix ADC et d'obtenir une visibilité sur l'intégrité, les performances et la sécurité des applications. En outre, en tirant parti de l'outil de Provisioning pour créer automatiquement des instances dans des clouds publics, tels qu'AWS, il simplifie également la gestion des instances ADC dans plusieurs emplacements, qu'elles soient sur site ou dans le cloud.

Conditions préalables

Le provisionnement d'instances Citrix ADC sur AWS à l'aide du service Citrix ADM nécessite certaines étapes qui sont résumées dans la documentation requise. Pour plus d'informations, reportez-vous à la section Provisionnement d'instances Citrix ADC VPX sur AWS.

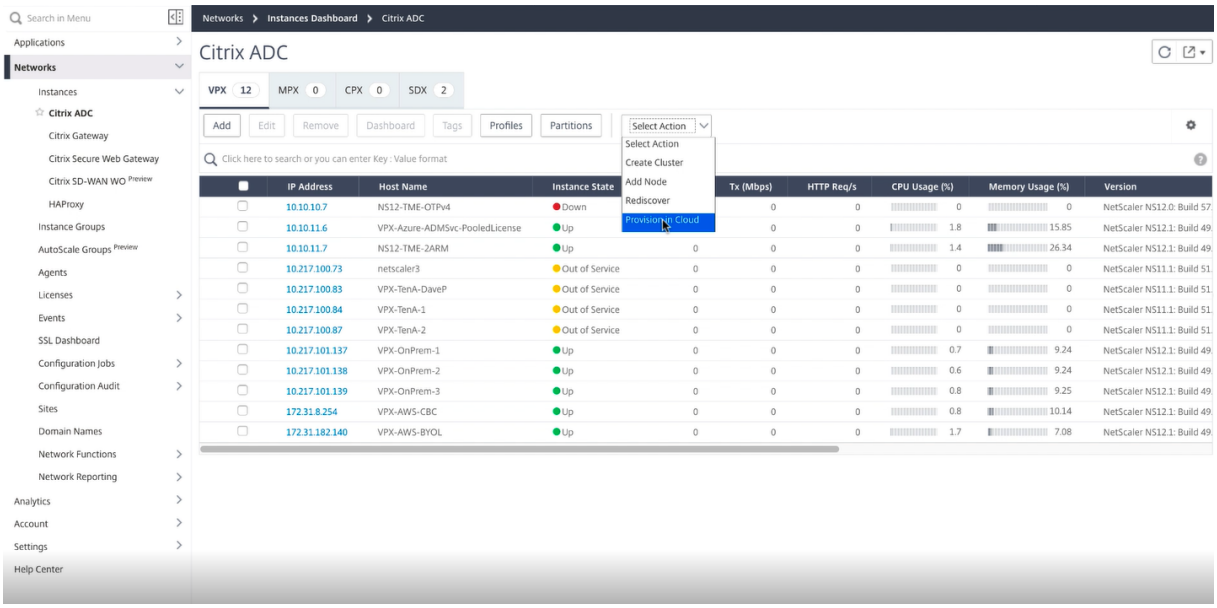
Ces étapes incluent l'exécution des tâches suivantes sur AWS avant de provisionner des instances Citrix ADC VPX dans Citrix ADM :

- Créer des sous-réseaux
- Créer des groupes de sécurité
- Créer un rôle IAM et définir une stratégie

Le rôle IAM doit être configuré avec des autorisations permettant au service Citrix ADM d'accéder au compte AWS. Après avoir tout configuré, vous pouvez tirer parti du service Citrix ADM pour provisionner les instances VPX sur AWS.

Provisionner des instances Citrix ADC VPX à l'aide du service Citrix ADM

Connectez-vous au service Citrix Cloud ADM et accédez à **Réseaux > Instances > Citrix ADC**. Ensuite, sous l'onglet **Sélectionner une action** , cliquez sur **Provisionner dans le Cloud** .



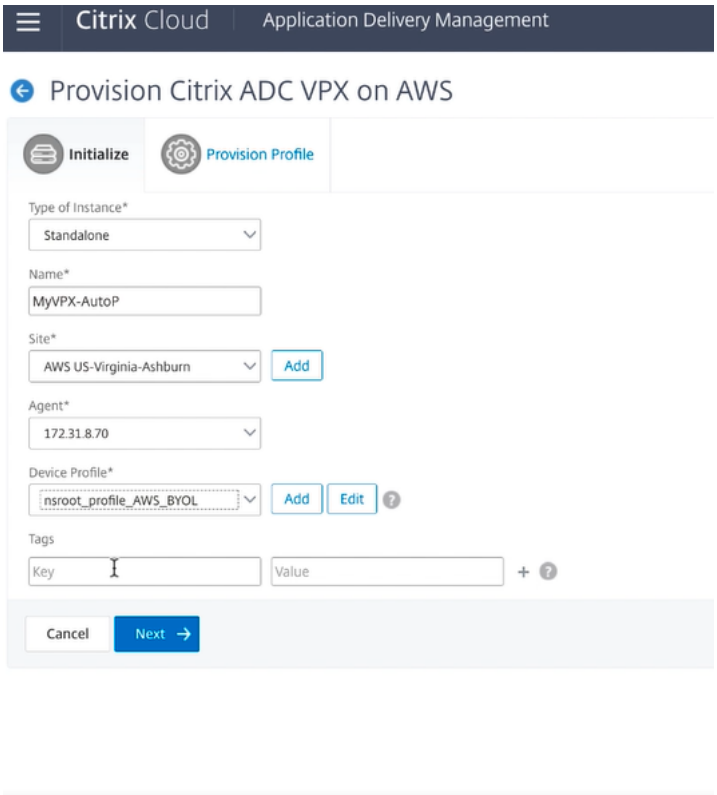
Cela vous invite à définir des informations sur l'instance que vous souhaitez mettre en service.

Plus précisément, vous devez définir ce qui suit :

- **Type d'instance :** L'instance autonome est sélectionnée ici.
- **Nom :** nom que vous souhaitez que l'instance adopte lorsqu'elle est provisionnée.
- **Site :** Le site définit la zone ou la région dans laquelle vous allez effectuer le déploiement.
- **Agent :** l'agent détermine quel agent ADM sera disponible sur le site. Cela devra être configuré avant de procéder à l'auto-provisioning. Vous devrez créer à la fois un site et un agent appartenant à ce site avant de commencer cet exercice.
- **Profil de périphérique :** Profil de périphérique dont le nom d'utilisateur et le mot de passe sont « nsroot ». Une fois que Citrix ADC est provisionné par Citrix ADM, le mot de passe de l'utilisateur

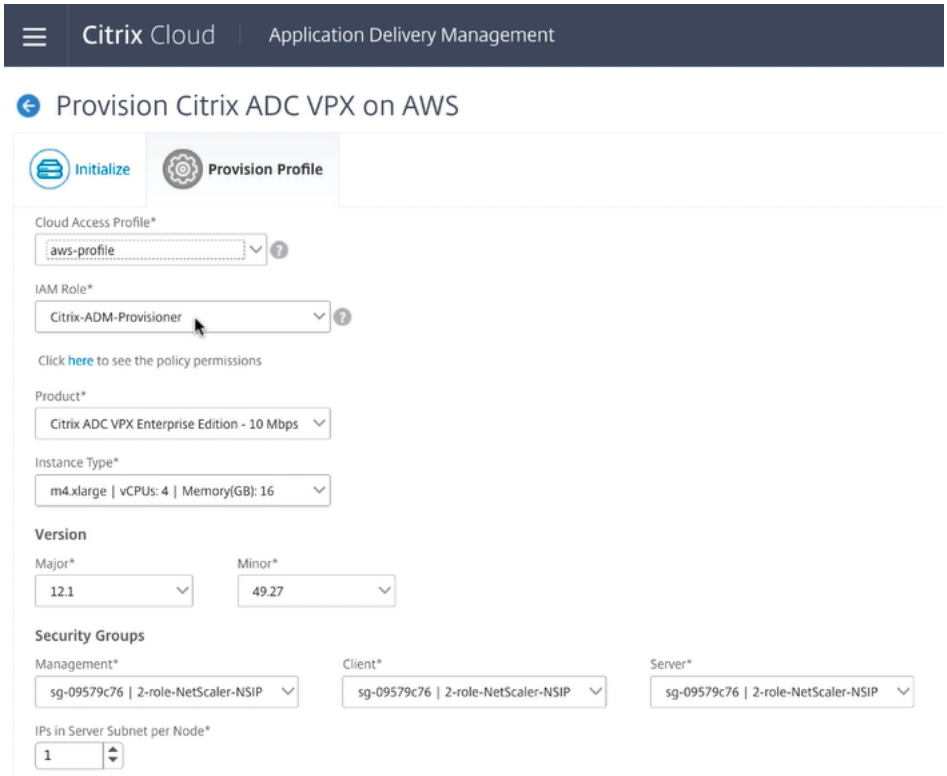
nsroot de l'ADC sera défini sur le mot de passe mentionné dans le profil. Plus loin, ce profil sera utilisé par Citrix ADM chaque fois qu'il doit se connecter à l'instance.

- **Tags :** Balise facultative pour les instances ou le groupe d'instances.



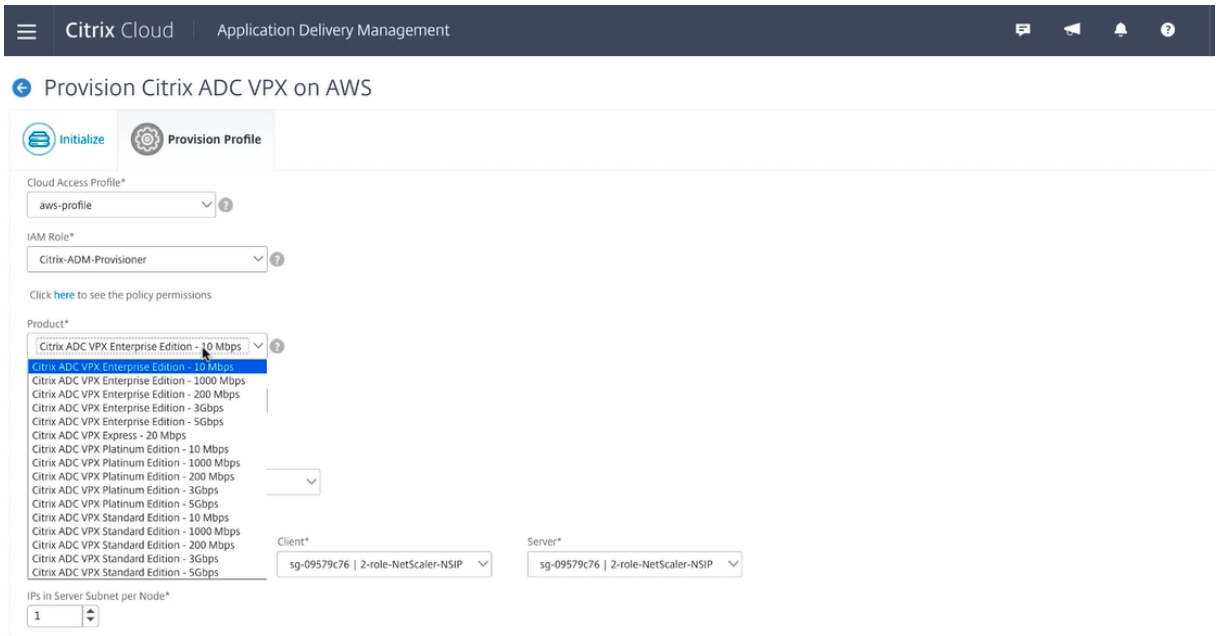
Sélectionnez ensuite le **profil d'accès au cloud** de votre compte AWS. Il s'agit du profil que Citrix ADM utilise pour se connecter à votre compte AWS pour récupérer des entités et effectuer des opérations telles que le Provisioning et le désapprovisionnement. À l'aide de ce profil, le service Citrix ADM remplit le reste des champs avec des objets liés à votre compte.

Dans ce scénario, il existe un rôle IAM prédéfini qui est utilisé par le service Citrix ADM pour provisionner les instances VPX, mais vous pouvez créer d'autres rôles.



Vous devez ensuite sélectionner l'édition de produit de l'instance VPX que vous souhaitez déployer en fonction du débit souhaité.

> **Remarque :**
>
> VPX Express est inclus pour que vous puissiez déployer une instance VPX sans licence.



Version

Déterminez quelle version de logiciel vous souhaitez exécuter en sélectionnant la version principale et la version mineure.

Groupes de sécurité

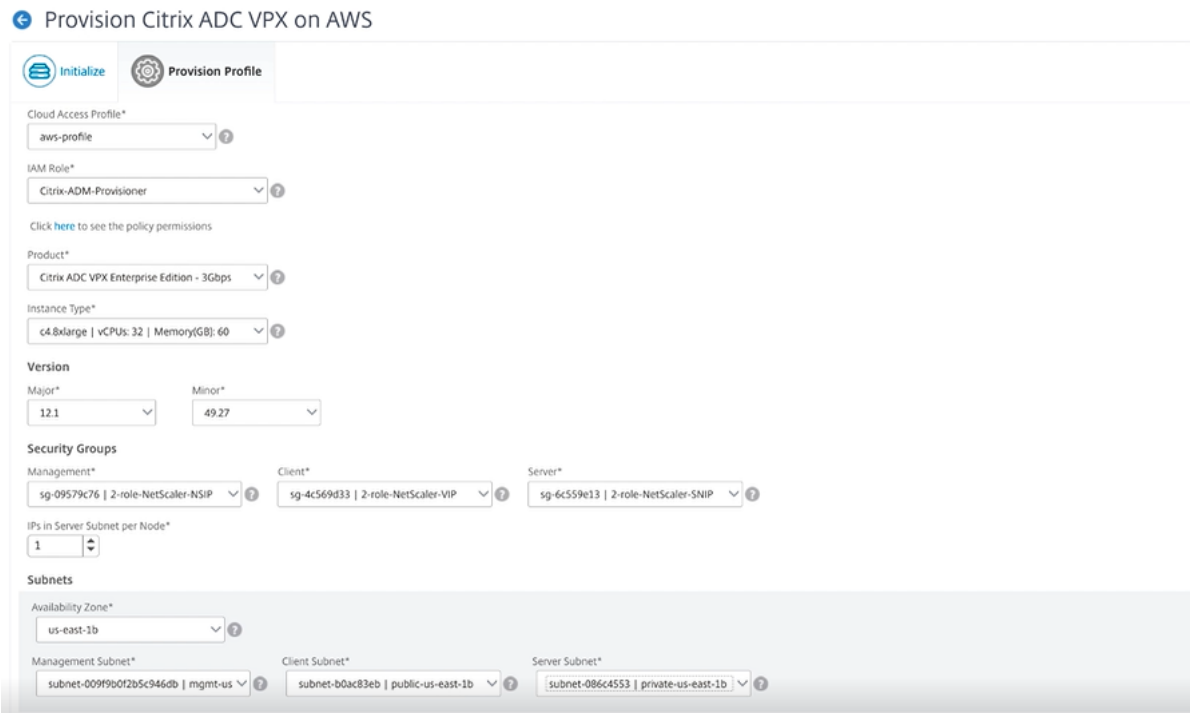
Les groupes de sécurité doivent disposer d'autorisations prédéfinies pour accéder à différents Clouds privés virtuels (VPC). Étant donné que chaque instance nécessite trois interfaces réseau ou VNIC, vous devez appliquer trois groupes de sécurité différents au service que vous déployez, notamment :

- Un pour la gestion à distance (rôle NSIP)
- Un pour l'accès côté client (rôle VIP)
- Un pour la communication côté serveur (rôle SNIP)

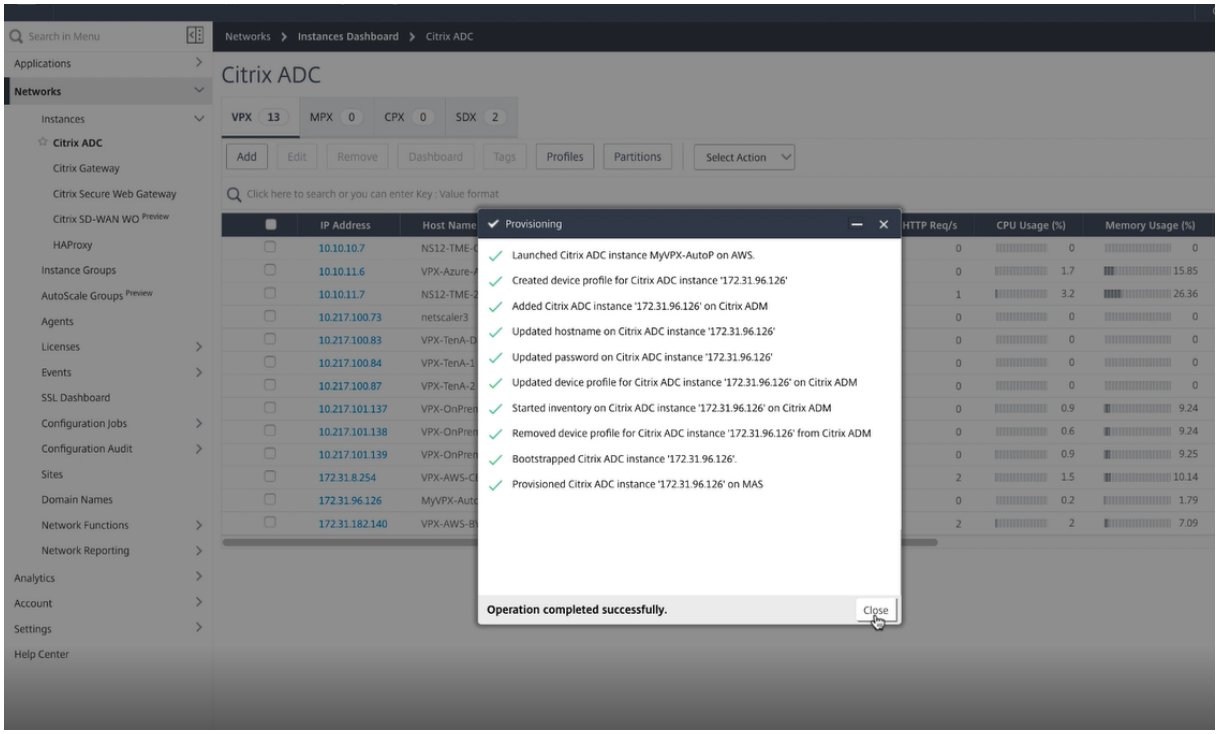
En outre, vous devez sélectionner le nombre nécessaire d'adresses IP requises pour l'évolutivité de cette solution.

Enfin, vous devez choisir la zone de disponibilité dans laquelle vous souhaitez que le déploiement se trouve et définir les informations de sous-réseau du VPC coïncident pour chaque sous-réseau :

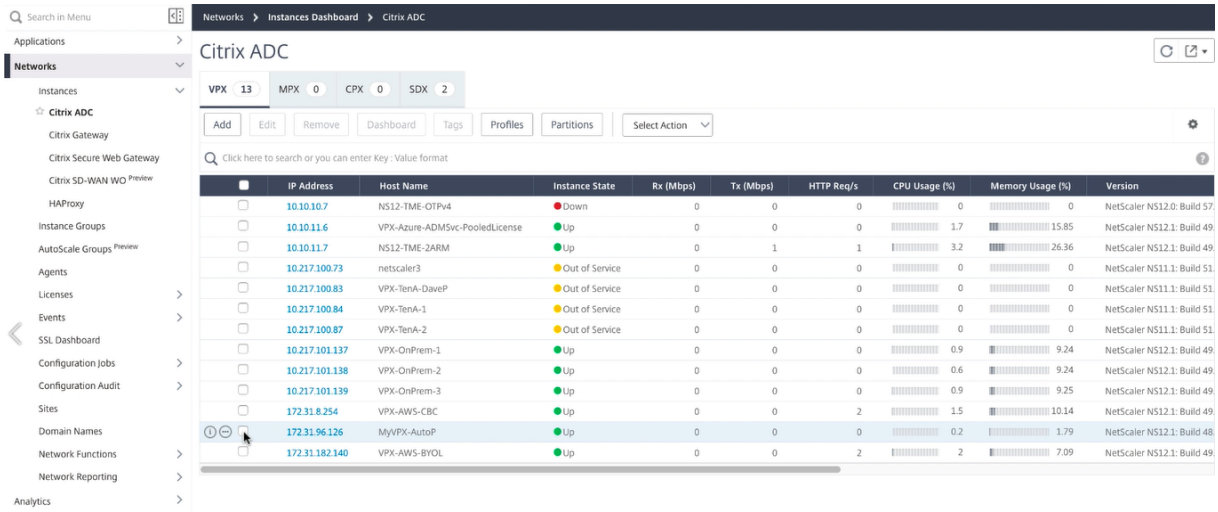
- Un pour l'interface de gestion (NSIP)
- Un pour les clients d'accéder (VIP)
- Un pour SNIP pour accéder aux serveurs back-end (SNIP)



Après avoir cliqué sur **Terminer**, le déploiement commence. Une fois le déploiement terminé, vous recevez une notification indiquant que votre VPX est déployé.

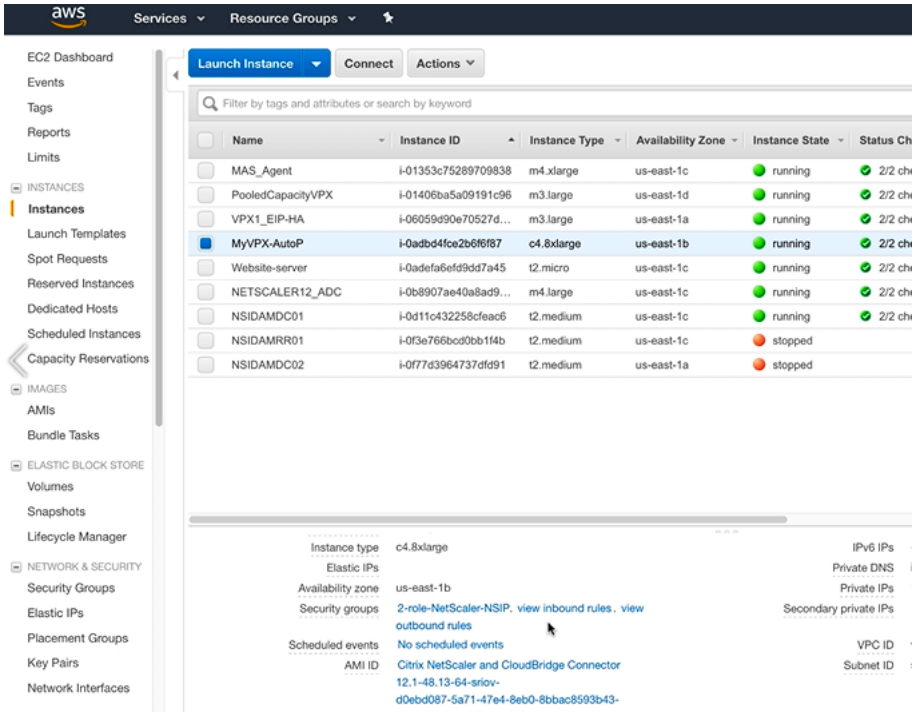


Une fois le déploiement terminé, vous pouvez voir les instances Citrix ADC VPX dans Citrix ADM à toutes fins de gestion et de déploiement.



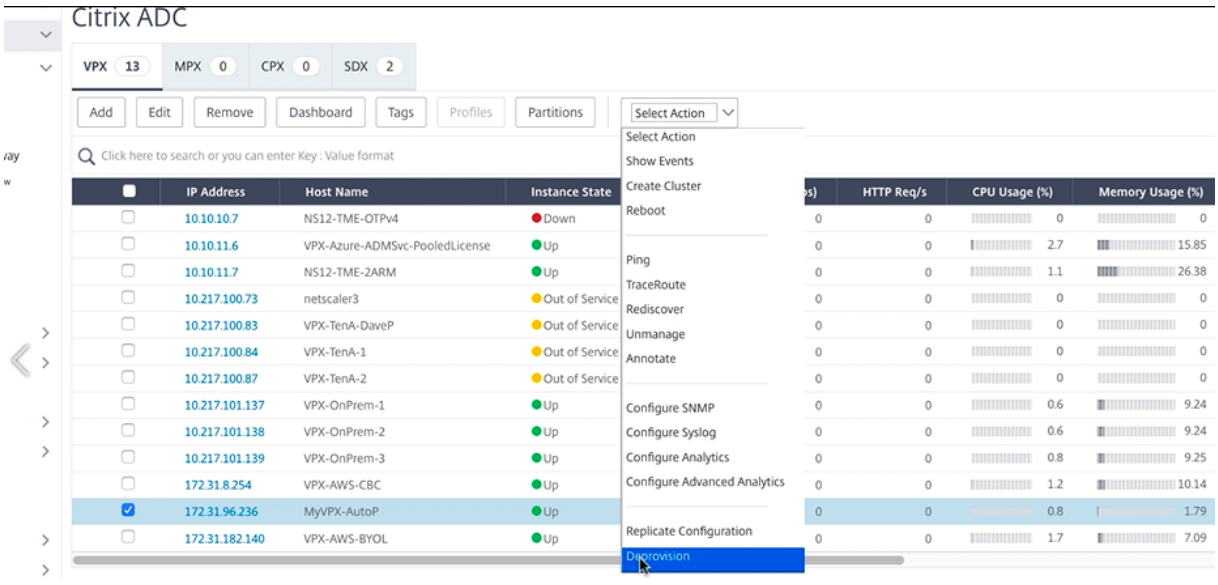
Vous pouvez ensuite accéder à la console EC2 pour voir la nouvelle instance créée avec le nom que nous avons établi dans les paramètres Citrix ADM. Il est synchronisé pour la gestion dans Citrix ADM et prêt pour le déploiement de vos applications sur Citrix ADC.

Déploiement AWS

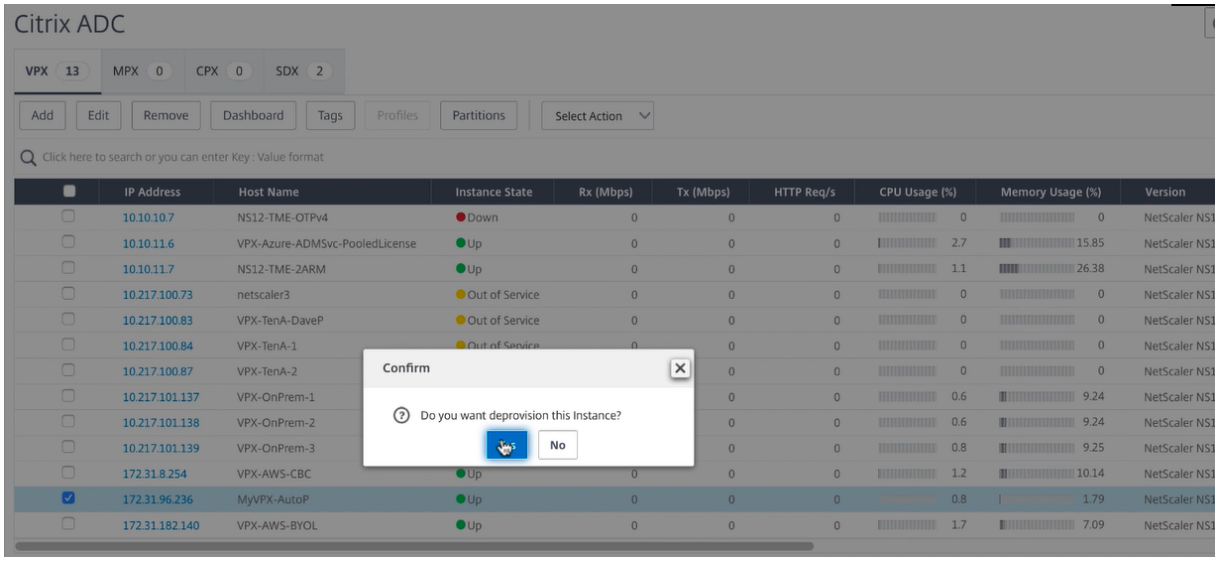


Pour déprovisionner ces instances, accédez au service Citrix Cloud ADM et accédez à **Réseaux > Instances > Citrix ADC**. Sous l'onglet **Sélectionner une action** , cliquez sur **Déprovisionner** .

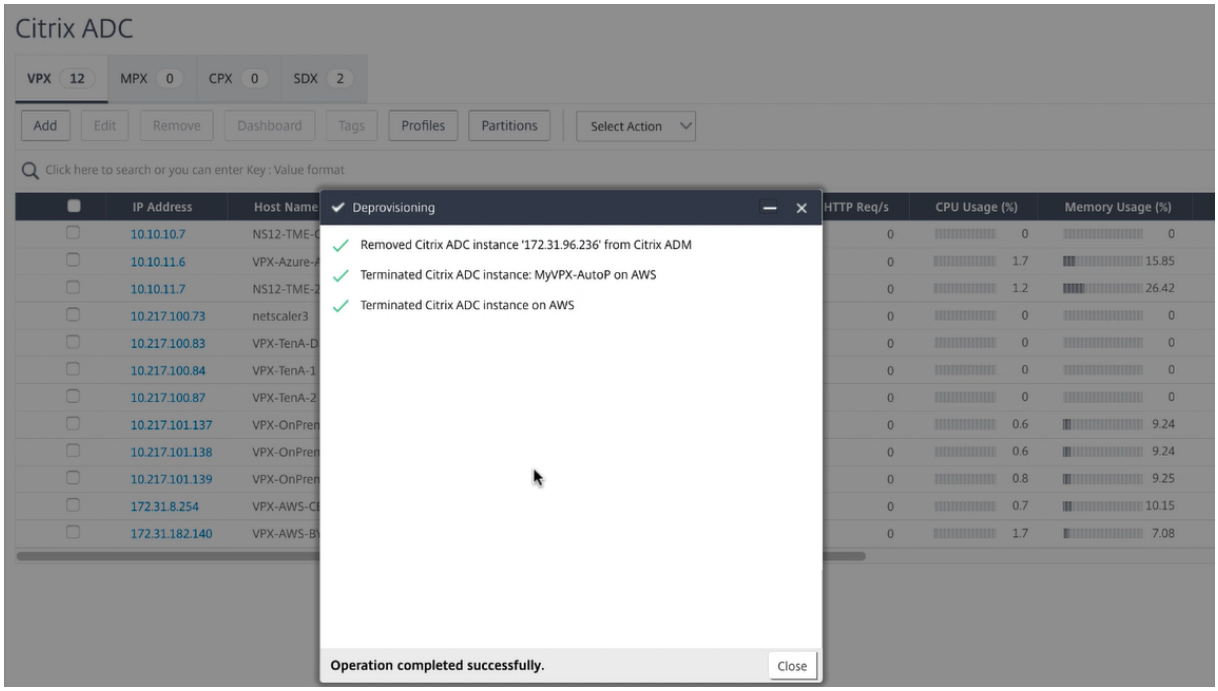
Déprovisionnement AWS

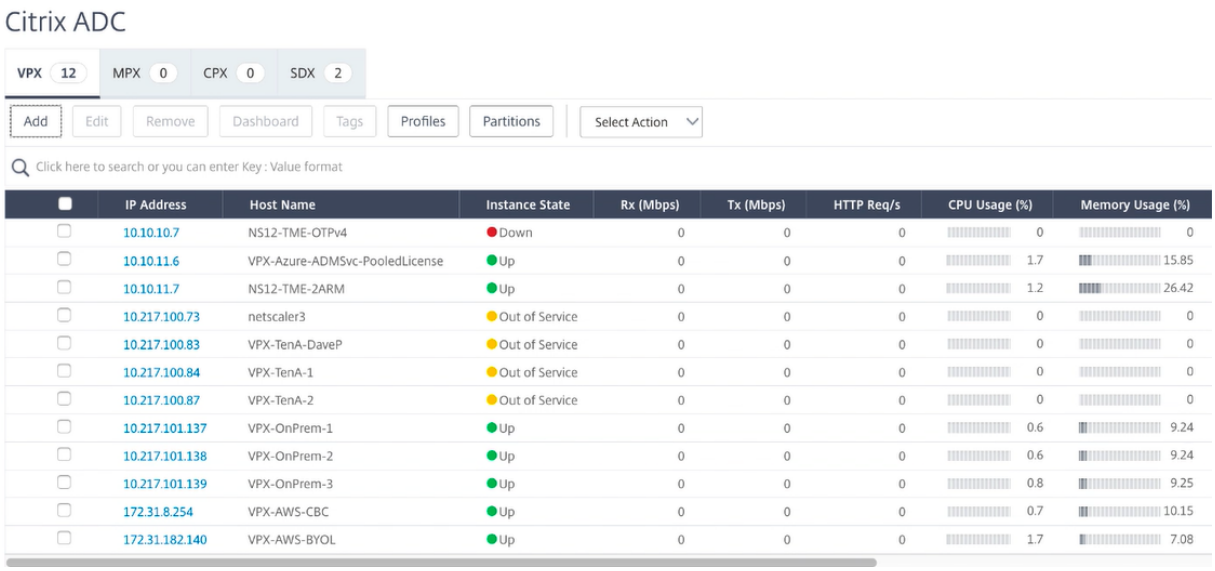


Vous êtes invité à confirmer votre action. Pour continuer, sélectionnez **Oui** , puis tout le Provisioning est inversé.



Après avoir reçu une confirmation que l'instance VPX a été désapprovisionnée, vous ne voyez plus le périphérique dans la console Citrix ADM.





Plus d'informations

- Guide d'implémentation : Citrix XenDesktop dans AWS
- Comment configurer Unified Gateway pour les applications d'entreprise courantes
- Accélérez votre activité en exécutant des solutions Citrix sur Amazon Web Services (AWS)
- Solutions de mise en réseau cloud et de virtualisation des postes de travail pour AWS
- Utilisation de Citrix ADC HA dans AWS dans plusieurs zones de disponibilité
- Intégration NetScaler VPX et AWS AutoScale

Conception de référence validée des partitions Admin Citrix ADC

January 8, 2020

Vue d'ensemble des fonctionnalités

Citrix ADC Admin Partitions permet la multi-location au niveau logiciel dans une seule instance Citrix ADC. Chaque partition a son propre plan de contrôle et plan réseau.

Les principaux avantages des partitions d'administration sont :

1. Plane de commande : configuration et gestion isolées
2. Data Plane : données et fichiers de partition clés étroitement contrôlés dans les limites de la partition
3. Plan réseau : le trafic est isolé avec sa propre configuration réseau. Deux partitions sur le même Citrix ADC ne voient pas le même trafic passant par chaque partition

Ce document décrit en détail les cas d'utilisation habituels qui sont activés par les partitions d'administration et les directives relatives à l'utilisation des partitions d'administration dans l'environnement client.

Cas d'utilisation des partitions d'administration

Cas d'utilisation Enterprise pour les partitions d'administration

Les administrateurs Citrix ADC peuvent partitionner un Citrix ADC en plusieurs ADC et affecter les partitions à différents administrateurs d'applications, tels que Microsoft SharePoint et Microsoft Lync. Chaque administrateur/propriétaire d'application peut apporter ses propres modifications de configuration.

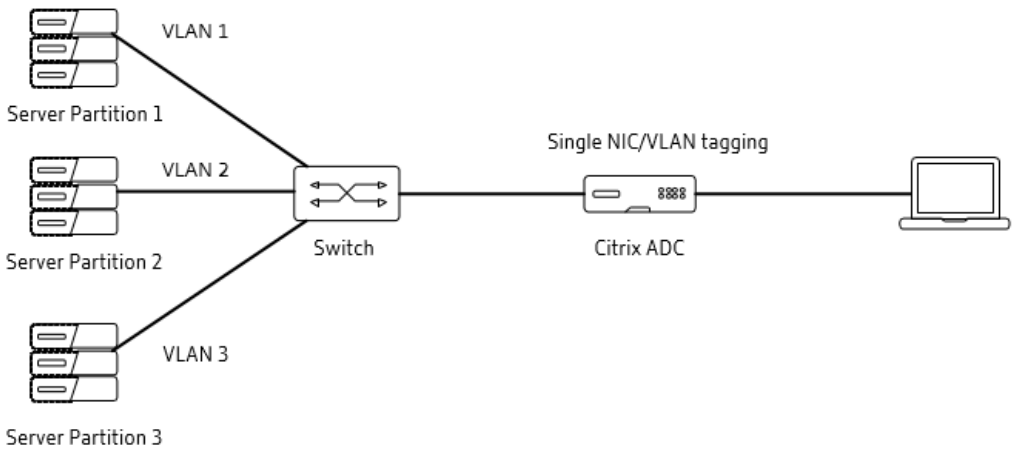
Superposition IP : Le principal avantage du chevauchement IP est que la même plage IP peut être utilisée sur différentes partitions d'administration sans aucun conflit IP. Pour les serveurs principaux, vous pouvez utiliser le même ensemble d'adresses IP privées. Dans un scénario de chevauchement IP, les VLAN ne peuvent pas être partagés.

Routage virtuel : la configuration de routage est unique à chaque partition et chaque propriétaire de partition peut configurer ses propres protocoles de routage.

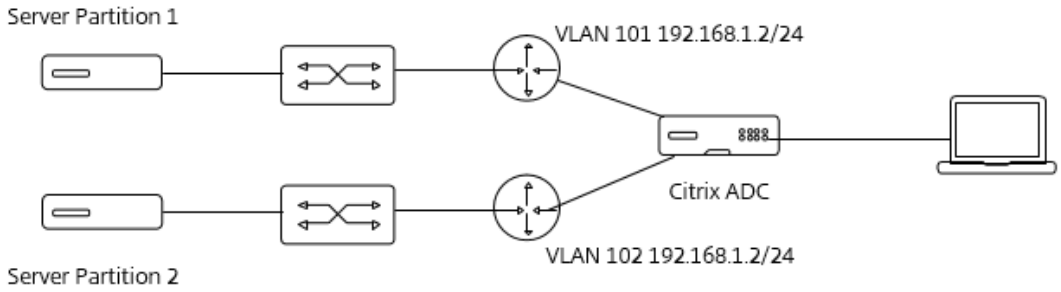
Isolation de l'espace de noms : les noms d'entités sont uniques sur différentes partitions, de sorte que vous pouvez utiliser les mêmes noms sur différentes partitions d'administration.

Diagramme de référence :

Carte réseau unique — VLAN multiples



chevauchement des IP :



Cas d'utilisation du fournisseur de services pour les partitions d'administration

Les fournisseurs de services peuvent partitionner un Citrix ADC et l'affecter à des clients individuels en fonction de leurs besoins en bande passante et du nombre de connexions simultanées.

Les fournisseurs de services peuvent développer des outils d'orchestration à l'aide des API NITRO pour obtenir des commentaires de leurs clients individuels sur leurs besoins en bande passante et leurs connexions simultanées, créer des partitions et les affecter à leurs clients.

Voici un ensemble d'isolations qui aident les fournisseurs de services :

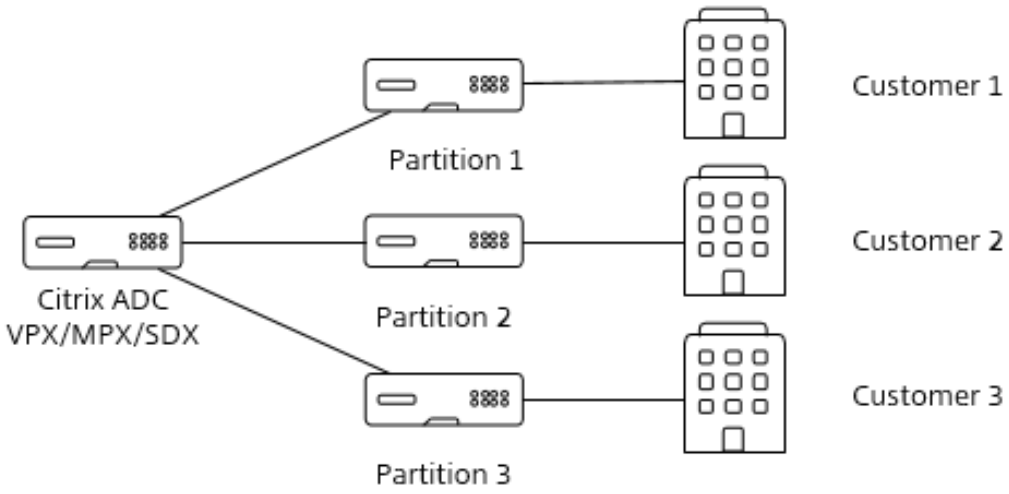
Système de fichiers : chaque partition se voit attribuer une partie d'un système de fichiers et les fichiers stockés dans cet espace de partition respectif ne sont pas visibles par les autres partitions. Les certificats et clés SSL sont stockés dans cette partition et ne sont pas visibles par les autres propriétaires de partition, ce qui rend chaque partition sécurisée.

VLAN partagé : dans un fournisseur de services type avec un déploiement multi-locataire, les clients finaux peuvent ne pas avoir de VLAN indépendants pour le trafic entrant. La fonctionnalité VLAN partagé partage le VLAN lorsqu'il n'est pas possible d'avoir un VLAN dédié.

Balisage VLAN : Une interface unique peut être partagée entre plusieurs partitions d'administration et isolée à l'aide d'un VLAN balisé. Pour un VLAN non balisé, utilisez un VLAN partagé.

Dépannage et débogage : les administrateurs peuvent voir les statistiques de trafic de chaque partition indépendamment et séparer les journaux en les filtrant par l'ID de partition. La fonction de suivi assure l'indépendance de la partition puisque la trace tirée d'une partition ne verra jamais les paquets d'une autre partition.

Diagramme de référence



Instructions pour la mise en œuvre des partitions d'administration

Les partitions d'administration permettent le partage de ressources, y compris la bande passante, la mémoire et les connexions simultanées, et assurent l'isolation au niveau du réseau, des données et du plan de gestion.

Partage des ressources

Les administrateurs ADC ont besoin des détails suivants pour configurer la partition d'administration :

1. Connexions : (Nombre de connexions TCP)
2. Mémoire
3. Besoins en bande passante

Le nombre de connexions et les exigences en bande passante dépendent de l'application et du trafic géré par la partition respective. L'administrateur ADC, en consultation avec l'administrateur de l'application, obtiendra les connexions/bande passante pour une partition.

Directives d'allocation de mémoire

La quantité de mémoire allouée à une partition par défaut doit représenter au moins 50 % de la mémoire totale disponible pour les raisons suivantes :

1. Fournir une flexibilité au client à l'avenir pour augmenter la mémoire des autres partitions dans le cas où la limite est atteinte.

2. La mémoire de mise en cache intégrée pour toutes les partitions est tirée de la partition par défaut.

La mémoire totale pouvant être consommée par un PE est de 4 Go. Donc, total de 2 Go peut être alloué à toutes les partitions à l'exclusion de la partition admin.

La mémoire affectée à la partition admin est utilisée à deux fins :

1. Stockage d'objets statiques (configuration, clés SSL)
2. Objets dynamiques : en fonction de la liste des entités activées et du nombre de connexions, la mémoire allouée aux objets dynamiques varie

L'administrateur ADC utilise les connexions et la bande passante requises par le propriétaire de l'application et les instructions ci-dessous pour obtenir l'estimation de la mémoire.

Instructions pour l'allocation de mémoire statique pour la configuration

Le tableau 1 répertorie les configurations couramment utilisées et la mémoire requise.

Tableau 1

Type de configuration	Mémoire allouée en Ko par moteur de paquets
Ajouter SNIP	255
Ajouter un serveur IPv4	0.384
Ajouter un service	5.253
Ajouter un vServer avec un service	11.157
lier vlan à la partition	0.116
ajouter un itinéraire à la partition	0.564
ajouter acl	0.5
ajouter un moniteur	4.34
ajouter des groupes de services	4.625
lier le serveur au groupe de services	5.817
ajouter une action cs	4.532
add cs policy	2.548
add cs vserver	11.589
lier la politique cs à cs vServer	7.348

Les configurations sont répliquées entre les PE, de sorte que l'exigence ci-dessus doit être multipliée par le nombre de PE.

Directives pour la mémoire dynamique

Tableau 2

Fonctionnalité	Exigences en mémoire
Connexions (Applicable uniquement si la version de Citrix ADC est 12.0 et supérieure)	2,4 Mo par 1 K connexions
Sessions persistantes	600 Ko par 1 Ko de sessions
Sessions persistantes GSLB	6 Mo par 1 K sessions
SSL	6 Mo pour 1000 connections/sessions SSL dans le déchargement SSL et 9 Mo pour 1000 connections/sessions SSL en fin de session SSL
AAA — Selon le nombre d'utilisateurs	Nombre d'utilisateurs * 2 Ko
Réécriture : récupère la longueur maximale qui sera analysée par la stratégie de réécriture	Nombre de connexions * Longueur maximale
Responder — Récupère la longueur maximale qui sera analysée par la stratégie Responder	Nombre de connexions * Longueur maximale
Mise en mémoire tampon TCP	20 % des connexions * taille du tampon TCP configuré

Mémoire dynamique = somme de la mémoire calculée à partir de chacune des lignes ci-dessus dans le tableau ci-dessus.

Ajoutez un tampon de 10 à 20 % à la mémoire totale calculée.

Les exigences en mémoire pour certaines fonctionnalités comme AppQoE ne sont pas fournies car la mémoire consommée à partir de la mémoire de partition est négligeable pour ces fonctionnalités et le tampon de 10 à 20 % est suffisant pour les gérer.

Mémoire totale = Mémoire statique x Nombre de PE + Mémoire dynamique

Supposons que nous arrivons à une conclusion que la mémoire requise est de 1 Go et que le nombre de moteurs de paquets est de 4. Ensuite, pour cette partition particulière, la quantité de mémoire nécessaire est dérivée par la formule ci-dessous :

Configuration de la mémoire de partition d'administration = (Quantité de mémoire requise/Nombre de moteurs de paquets)

Mémoire de partition d'administration = 1 Go/4 = 250 Mo

Comportements lorsque la limite de ressources est atteinte

1. Connexions : les nouvelles connexions seront supprimées
2. Bande passante : le nouveau trafic sera supprimé
3. Mémoire — le nouveau trafic sera abandonné

Vous pouvez configurer les alertes SNMP qui sont déclenchées si les ressources de la partition particulière sont épuisées. La liste des interruptions SNMP est donnée dans la section Ressources supplémentaires.

Plan réseau

VLAN : configurez et affectez différents VLAN aux partitions d'administration pour maintenir l'isolement au niveau du réseau.

Routage : la configuration de routage est unique par partition.

L'administrateur ADC, en consultation avec l'administrateur réseau (avec l'entrée de l'administrateur de l'application), définit les configurations VLAN et de routage en fonction de la topologie du réseau.

Paramètres L3 : Peut être spécifique à la partition. Certains des paramètres L3 sont Drop DF Packets, ICMP err threshold, overridernat, etc., et l'entrée devrait provenir du réseau ou ADC admin.

Plan de contrôle : Expérience utilisateur

Les partitions d'administration fournissent une isolation à différents niveaux permettant à l'utilisateur de gérer en toute sécurité une instance ADC isolée.

Différents niveaux d'isolement comprennent :

1. Page UI — Configuration, statistiques affichées uniquement pour la partition
2. Diagnostics : isolement de trace. Trace ne capturera pas le trafic d'autres partitions
3. Alertes SNMP - configurées au niveau de la partition
4. Isolation au niveau du journal

L'isolation de niveau UI-peut être configurée à l'aide de la méthode suivante :

1. Dans la partition respective, activez l'accès mgmt. pour un SNIP et utilisez ce SNIP pour accéder à l'interface graphique. Cela fournira une isolation et une visibilité au niveau UI-niveau uniquement dans cette partition.

Tableau 3

Type de journal	Partition spécifique
Journal Web	Oui
Offre groupée Techsupport	Oui
Journaux d'audit	Non
/var/log	Non

Partition d'administration pour cas d'utilisation en entreprise

Cette section décrit un cas d'utilisation client d'entreprise avec quatre applications utilisant des partitions d'administration.

Exigences du client

- Nécessités d'héberger 4 applications
- Chaque application a son propre administrateur et un ensemble différent de configuration ADC. Le tableau ci-dessous répertorie les applications et leurs exigences particulières.

Tableau 4

Application	Caractéristiques	Exigence/Caractéristiques
SharePoint	Partage de fichiers, audio, fichiers etc.	Mise en cache, compression, authentification, déchargement SSL, profils SSL
Database	Règles SQL personnalisées, authentification, répartition entre lecture et écriture pour de meilleures performances	Switch de contenu, Policy Infra pour les mots-clés liés à SQL
Site Web Enterprise	Accès public - sujet aux attaques, pare-feu d'application	Profils DDoS, AppQoE, AppFW, SSL
Outlook	Intégré à AD, SSO, meilleures performances dans HTTP	Authentification SSO, Déchargement SSL

À partir du tableau des exigences ci-dessus, il est clair que chacune des applications a besoin d'un ensemble différent de configurations pour profiter pleinement des avantages de Citrix ADC. Il est recommandé de partitionner le Citrix ADC et d'attribuer ces partitions aux propriétaires d'applications respectifs.

Estimation de la bande passante et des connexions

Outlook et SharePoint

La bande passante pour les applications d'entreprise telles que SharePoint, Exchange et Lync dépend des éléments suivants :

1. Nombre d'utilisateurs simultanés
2. Type d'utilisation
    a) Échange : taille moyenne et nombre de messages
    b) SharePoint : type de fichiers, rapport entre lecture et écriture

L'administrateur de l'application calcule les exigences en matière de bande passante à l'aide des deux facteurs ci-dessus et fournit les informations à l'administrateur Citrix ADC pour la configuration de la partition d'administration. Des lignes directrices générales sur la façon de calculer la bande passante sont fournies dansTechnique MicrosoftetBlogs MSDN.

Exemples :

Bande passante pour Outlook 2010 : Types d'utilisateurs (légers, moyens, lourds, etc.). Pour les utilisateurs de taille moyenne, envoyez 10 courriels, recevez 40 courriels, moyenne msg. taille 50 kb = 2,15 Kbps. Pour 1 000 utilisateurs, la bande passante requise est de 2 150 Kbit/s.

Bande passante pour SharePoint : nombre d'utilisateurs = 1 000. En supposant que 20 % des utilisateurs soient actifs à tout moment et que la taille moyenne de chargement des pages est de 100 Ko et qu'ils accèdent à une dizaine de pages pendant une période d'une heure :

= 100 Ko⋆ 200⋆ 10 par heure = 200000 kB/h = 200000 * 8 (8 bits par octet) / 3600 (pas de secondes)

= 444 Kbits/s

Connexions par seconde = Nombre d'utilisateurs actifs⋆ 10

MSSQL

En fonction du taux de requêtes et de la taille de la réponse, dériver la bande passante et les connexions.

Site Web Enterprise

Exigences en bande passante : taille moyenne de la page Nombre⋆ maximum d'utilisateurs à tout moment⋆ 2

Connexions : nombre maximal d'utilisateurs * nombre de connexions par utilisateur

Exemple :

Bande passante : 4 Ko*1000*2 = 48000 Kbps

Nombre maximum d'utilisateurs = 1000 et nombre de connexions par utilisateur = 10. Les connexions = 10K

Si la plupart des utilisateurs proviennent de HTTP/1.1, alors le nombre de connexions par utilisateur serait de 2 à 3, mais si le mélange est incliné plus vers HTTP/1 .0, alors le nombre de connexions serait de 10 à 15. Le nombre multiplicatif de connexions par utilisateur varie de 3 à 15 en fonction de la composition du trafic et du client.

La mémoire à configurer dépend de :

1. Liste des configs dans la partition d'administration respective — mémoire statique. Voir le tableau 1 pour plus de détails.
2. Mémoire dynamique : nombre de connexions et type de connexions (HTTP vs SSL) — Veuillez vous référer au tableau 2 pour plus de détails.
3. Nombre de moteurs de paquets. Mémoire = (mémoire statique + mémoire dynamique) / (nombre de moteurs de paquets)

Étapes pour ADC admin

1. Collecter la bande passante et les connexions pour chaque application
2. Créez trois partitions pour SharePoint, Base de données et Outlook respectivement. Utilisez la bande passante et les connexions de l'étape précédente et affectez-la à la partition respective. Le site Web de l'entreprise peut être hébergé sur la partition par défaut si le client a besoin d'AppFW car AppFW n'est pris en charge que sur les partitions par défaut.
3. Créez des utilisateurs pour chacune des partitions et partagez les informations d'identification.
4. Activez la mise en cache intégrée et définissez la mémoire cache. La mémoire cache provient de la mémoire cache configurée dans la partition par défaut. Pour obtenir des renseignements détaillés sur la répartition, veuillez consulter la section de l'annexe de IC.
    a) Attribuez de la mémoire cache après consultation avec l'administrateur ADC. Essayez d'allouer 30 à 40 % de la mémoire cache totale dans le système. Si le total alloué est de 10 Go, allouez environ 3 à 4 Go pour le cache dans la partition SharePoint.
    b) Les propriétaires d'applications doivent d'abord surveiller les statistiques de mise en cache pour vérifier le niveau des avantages.

c) Vérifiez le taux d'accès des objets de mise en cache et, si un grand nombre d'objets de cache ont un impact élevé, augmentez la taille de la mémoire IC pour cette partition particulière.

5. Activer la compression

a) SharePoint publiera des fichiers de différents types (Excel, PowerPoint, Word) et les mêmes fichiers, s'ils sont compressés et remis aux clients, réduiront l'utilisation de la bande passante.

Utilisateur de base de données

1. Configurez les serveurs CS, VIP et principaux.
2. Utilisez le commutateur de contenu pour fractionner les demandes de lecture/écriture et rediriger vers l'ensemble de serveurs respectif.

Site Web Enterprise

1. Configurez les serveurs VIP et principaux.
2. Activer la mise en cache intégrée.

a) Le site Web Enterprise se trouve dans la partition par défaut, de sorte que la mémoire cache inutilisée des autres partitions est disponible pour le site Web Enterprise. Donc, en supposant que SharePoint et Outlook consomment chacun 35 %, alors le total consommé serait de 70 %, laissant les 30 % restants à la partition par défaut (site Web d'entreprise). Si la mémoire cache totale est de 10 Go, la partition par défaut aura 3 Go de mémoire cache.
b) Les propriétaires d'applications doivent d'abord surveiller les statistiques de mise en cache pour vérifier le niveau des avantages.
c) Vérifiez le taux d'accès des objets de mise en cache, et si un grand nombre d'objets de cache ont un impact élevé, augmentez la taille de la mémoire IC pour cette partition particulière.

3. Activez l'optimisation frontale.
4. Activer AppFW.

Cas d'utilisation des partitions d'administration du fournisseur de services

Le fournisseur de services héberge les applications Microsoft et fournit les applications IIS, SharePoint et MSSQL en tant que service. Leurs clients ont généralement les exigences suivantes :

Exigences du client

- Client 1 : Accède au serveur de base de données et son partage en lecture/écriture est 90:10 et le client final souhaite configurer des filtres SQL personnalisés
- Client 2 : Accède à l'application web via SSL et le client final veut contrôler ses certificats SSL
- Client 3 : Accès à SharePoint hébergé à partir du fournisseur de services

Le fournisseur de services héberge un portail permettant à son client de :

1. Sélectionnez l'application qu'il souhaite héberger
2. Besoins en bande passante

Le fournisseur de services héberge un portail permettant à son client de :

1. Sélectionnez l'application qu'il souhaite héberger
2. Besoins en bande passante
3. Connexions

En fonction de la sélection, le fournisseur de services peut configurer les partitions appropriées avec des configurations liées à des applications spécifiques dans le back-end à l'aide des API NITRO.

En fonction de l'application sélectionnée par le client, choisissez l'option appropriée.

1. Application Web utilisant SSL
    a) Option de certificat SSL à être lié à VIP
    b) Redirection HTTP vers HTTPS
    c) Paramètres liés au profil SSL
2. SQL
    a) Filtres liés à SQL que le client souhaite configurer
3. SharePoint
    a) Limite de mémoire cache et règles
    b) Stratégies de compression

Le fournisseur de services suit l'une des deux options pour implémenter les exigences exactes après la création de partitions d'administration.

Option de configuration 1 :

Le fournisseur de services recueille les demandes du client et les exécute sur la partition correspondante.

Option de configuration 2 :

Automatisez les partitions d'administration à l'aide des API NITRO. Les entrées peuvent être collectées à partir du portail frontal et dans le back-end les API NITRO peuvent être exécutées pour configurer les partitions.

Considérations relatives aux fonctionnalités

Prise en charge des fonctionnalités : La partition d'administration est prise en charge pour la plupart des fonctionnalités et n'est pas prise en charge pour quelques fonctionnalités. Pour la liste exacte, reportez-vous àDocuments Citrixla version du logiciel en question et vérifiez. Il contiendra une table qui répertorie la matrice de compatibilité.

Limites de configuration. Les partitions d'administration n'est pas prise en charge dans :

1. Clustering
2. Appareil MPX-FIPS

Conclusion

Le principal avantage des partitions d'administration est de permettre la séparation de l'ADC au niveau logiciel et de fournir une expérience utilisateur sécurisée et isolée à chaque propriétaire de partition.

Ressources supplémentaires

Outils de dépannage

Problèmes courants dans la partition d'administration :

Partition d'administration sur VPX sur ESX :

- Partition non par défaut non accessible lorsque l'adresse MAC personnalisée est configurée.
- Solution : le mode promiscuous doit être activé sur ESX pour que la partition autre que par défaut fonctionne.

Échec de configuration :

- La configuration peut échouer à lancer l'erreur Fichiers d'entrée non présents.
- Le chemin relatif doit être utilisé et non le chemin absolu.

Configuration VLAN :

- Le VLAN de partition d'administration prend en charge le VLAN balisé, donc lorsque le VLAN est balisé, le commutateur auquel l'interface Citrix ADC est connectée doit être configuré avec le VLAN approprié. Pour un VLAN non balisé, utilisez la configuration de VLAN partagé

Allocation de mémoire cache intégrée

Pour configurer la mise en cache intégrée (IC) sur un Citrix ADC partitionné, après avoir défini la mémoire IC sur la partition par défaut, le super-utilisateur peut configurer la mémoire IC sur chaque partition d'administration de telle sorte que la mémoire CI totale allouée à toutes les partitions

d'administration ne dépasse pas la mémoire IC définie sur la partition par défaut . La mémoire qui n'est pas configurée pour les partitions d'administration reste disponible pour la partition par défaut.

Par exemple, si une appliance Citrix ADC avec deux partitions d'administration dispose de 10 Go de mémoire CI allouée à la partition par défaut et que l'allocation de mémoire IC pour les deux partitions d'administration est la suivante :

- Partition1 : 4 Go
- Partition2 : 3 Go

Ensuite, la partition par défaut a 10 - (4 + 3) = 3 Go de mémoire IC disponible pour l'utilisation.

> **Remarque** :
>
> Si toute la mémoire CI est utilisée par les partitions d'administration, aucune mémoire CI n'est disponible pour la partition par défaut.

Commandes pour vérifier l'utilisation de la mémoire

- La mémoire système de Stat dans la partition affiche l'allocation de mémoire agrégée au niveau système pour la partition et le nom de la partition de stat indique le pourcentage de mémoire utilisée dans la partition.

```
>add partition p1
Done
>switch partition p1
Done
p1> stat system memory
done

Citrix ADC Memory Information:
Maximum Memory Available (MB): 50
Memory Currently Available (MB): 50
Memory Allocated (MB) 7
Memory Allocated (%) 14.95
InUse Memory  (MB) 7
InUse Memory (%) 14.95
Free Memory (MB) 42

>stat partition p1

Partition(s) Summary
   MinBW MaxBW MaxConn MaxMem

p1 10240 10240  1024  10

```



```
Partition Stats:

                        Rates (/s)   Total
Current Bandwidth          --          0
Current Connections        --          0
Memory Usage (%)           --          14
Total Packet Drops         0           7
Total Drops (KB)           0           0
Total Connection Drops     0           0
<!--NeedCopy-->
```

- Mémoire de configuration : puisque chaque configuration est répliquée dans chaque moteur de paquets, la mémoire est allouée à l'intérieur de chaque moteur de paquets. Par exemple, si la commande « add lb vserver » prend environ 10 Ko dans peach Packet Engine et que nous avons créé une partition de 10 Mo dans un système 5 — Packet Engine, alors au total, elle consomme 50 Ko de mémoire de partition.
- La valeur précise de la mémoire requise pour une configuration spécifique peut être mesurée en appliquant la configuration et en exécutant la commande suivante sur Citrix ADC shell :

```
root@ns# nsconmsg -s nsppeid=0 -s nspartid=1 -g mem_cur_usedsize -d
   current
Displaying performance information
Citrix ADC V20 Performance Data
Citrix ADC NS11.0: Build 65.572.nc, Date: Apr 7 2016, 10:32:51

reltime:mili second between two records Thu Feb 23 13:45:18 2017
 Index rtime totalcount-val delta rate/sec symbol-name&device-no
    0  22681     1597631     8965  5333     mem_cur_usedsize
       partition_ctx(p1) (PART-1)
<!--NeedCopy-->
```

Dans cette expérience, environ 9 Ko de mémoire sont utilisés dans PPE-0 pour l'ID de partition 1. Chaque partition configurée sur Citrix ADC possède un ID unique.

La commande suivante permet de mesurer l'estimation de la mémoire pour le système complet (y compris tous les moteurs de paquets) pour une partition donnée.

```
root@ns# nsconmsg -s nspartid=1 -g mem_cur_used -d current
Displaying performance information
Citrix ADC V20 Performance Data
Citrix ADC NS11.0: Build 65.572.nc, Date: Apr 7 2016, 10:32:51

reltime:mili second between two records Thu Feb 23 13:44:27 2017
Index rtime totalcount-val delta rate/sec symbol-name&device-no
```



```
8   0    7000    7881865       6403    5333    mem_cur_usedsize
       partition_ctx(p1) (PART-1)
9   <!--NeedCopy-->
```

Liste des traps SNMP introduits dans Citrix ADC 12.0

Nom du trap	Description
partitionCONNLimitExceeded	La limite de connexion de la partition est épuisée et les nouvelles connexions sont supprimées
partitionCONNLimitNormal	La partition peut désormais accepter de nouvelles connexions
partitionBWLimitExceeded	La limite BW de la partition est épuisée et les paquets sont abandonnés
paritionBWThresholdReached	Utilisation actuelle de la BW > = 80 %
partitionCONNThresholdReached	Nombre de connexions actives actuelles > = 80 %
paritionCONNThresholdNormal	Nombre de connexions actives actuelles < = 60 %
partitionMEMThresholdReached	Utilisation actuelle de la mémoire PE > = 80%
partitionMEMThresholdNormal	Utilisation actuelle de la mémoire PE < = 60%
partitionMEMLimitExceeded	Utilisation actuelle de la mémoire PE > = 95%

Références supplémentaires

Calculateur de bande passante réseau client Exchange bêta

Combien de bande passante ai-je besoin pour exécuter Microsoft Online Services

Conception de référence Citrix Gateway SaaS et O365 Cloud Validated

January 8, 2020

Généralités

Software as a Service (SaaS) est un modèle de distribution de logiciels permettant de fournir des logiciels à distance en tant que service Web. Applications SaaS couramment utilisées, y compris les abonnements Microsoft Office 365.

Les applications SaaS sont désormais accessibles à l'aide de Citrix Workspace à l'aide du service Citrix Gateway. Le service Citrix Gateway associé à Citrix Workspace offre une expérience utilisateur unifiée pour les applications SaaS configurées, les applications virtuelles configurées ou toute autre ressource d'espace de travail.

La livraison d'applications SaaS à l'aide du service Citrix Gateway vous offre une solution simple, sécurisée, robuste et évolutive pour gérer les applications. Les applications SaaS fournies sur le cloud présentent les avantages suivants :

Configuration simple — Facile à utiliser, à actualiser et à consommer.
Single Sign-on — Connectez-vous sans tracas avec Single Sign-on.
Modèle standard pour différentes applications : configuration basée sur des modèles d'applications populaires.

Application SaaS Citrix Gateway

Dans la section **Détails de l'application** , remplissez comme suit :

- Emplacement = En dehors de mon réseau d'entreprise
- Nom = Office 365 * URL = `https://login.microsoftonline.com/login.srf`
- Domaines connexes : *.login.microsoftonline.com
- Description = (par défaut)

Dans la section **Connexion unique** , remplissez comme suit :

- URL d'assertion = `https://login.microsoftonline.com/login.srf`
- Audience = urn:federation:MicrosoftOnline
- Format nom ID = Persistant
- ID nom = GUID Active Directory
- Attributs avancés :

  Nom de l'attribut :`IDPEmail`

  Format d'attribut : Non spécifié

  Valeur d'attribut : Email

Fédération d'applications SaaS O365 vers Citrix Gateway

Commandes PowerShell pour configurer le mode FEDERATED sur Microsoft Cloud :

- PS> `connect-msolservice`

> *Remarque :* un compte Microsoft Cloud doit être utilisé pour se connecter à `msolservice`.
>
> Par exemple, *admin.user@onmicrosoft.com*

- PS> `Install-Module AzureAD -Force`
- PS> `Import-Module AzureAD -Force`
- PS> `Install-Module MSOnline -Force`
- PS> `Import-module MSOnline -Force`

Configurez les paramètres de **fédération** uniques à l'abonnement client Citrix Gateway :

- PS> `$dom = "ad-domain.com"`

> *Remarque :*
> *l'espace de noms ad-domain.com est le domaine d'authentification utilisateur*

- `PS> $fedBrandName = "CitrixNS(TME)"`
- `PS> $url = "https://customerID.cloud.com/cgi/tmlogout"`
- `PS> $uri = "https://citrix.com/customerID"`
- `PS> $ecpUrl = "https://customerID.cloud.com/saml/login"`

> *Remarque :*
> *`customerID`est l'URL Citrix Workspace*

Fournir le certificat IdP SAML à partir de Citrix Gateway :

- `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`
- `PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

Exécutez la chaîne PS pour terminer la fédération `msol` vers Citrix Gateway :

- `PS> Set-MsolDomainAuthentication -DomainName $dom -federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $ecpUrl -LogOffUri $url -PreferredAuthenticationProtocol SAMLP`

Valider la fédération de domaine et les paramètres sont terminés :

- `PS> Get-MsolDomainFederationSettings`

```
DomainName: customerID.com

ActiveLogOnUri https://customerID.cloud.com/saml/login
```



```
FederationBrandName customerID(TME)

IssuerUri https://citrix.com/customerID

LogOffUri https://customerID.cloud.com/cgi/tmlogout

PassiveLogOnUri https://citrix.comcustomerID

SigningCertificate MIIG3zCCBMegAwIBAgIJAMUTG1zqJgUZMA0GCSqGSIb3DQEBCwUAMIGcMQswCQYD
```

Applications de la suite Office 365

- Outlook https://outlook.office365.com/
- OneDrive Entreprise https://customerid.sharepoint.com/
- Word https://office.live.com/start/Word
- Excel https://office.live.com/start/Excel
- PowerPoint https://office.live.com/start/PowerPoint
- OneNote https://www.onenote.com/
- SharePoint https://customerid.sharepoint.com/
- Teams https://teams.microsoft.com/
- Yammer https://www.yammer.com/office365
- Dynamics 365 https://customerid.dynamics.com/
- Flow https://flow.microsoft.com/

Liens de référence

Référence du module Azure PowerShell

Référence des commandes Azure PowerShell

Déployer la synchronisation d'annuaire Office 365 dans Microsoft Azure

Citrix Gateway Service SSO avec contrôle d'accès Conception de référence validée Citrix

January 8, 2020

Citrix Gateway Service

Citrix Gateway Service est une offre Citrix qui fournit l'authentification, l'authentification unique et permet la livraison rapide et sécurisée des applications Citrix VDI et SaaS.

Citrix Gateway Service fournit également l'accès SSO aux SaaS et aux applications Web. La fonctionnalité SSO Software as a Service (SaaS) est un service cloud entièrement géré dans Citrix Cloud qui fournit un accès à distance et une authentification unique aux applications SaaS hébergées publiquement et aux applications Web hébergées par l'entreprise.

Les applications SaaS sont désormais accessibles à l'aide de Citrix Gateway Service dans l'abonnement utilisateur Workspace. Citrix Gateway Service fournit un accès authentifié aux applications SaaS tierces s'exécutant dans des fournisseurs d'applications SaaS externes hébergés publiquement.

Le service Citrix Gateway associé à Citrix Workspace offre une expérience utilisateur unifiée pour les applications SaaS configurées, les applications virtuelles configurées ou toute autre ressource d'espace de travail.

La livraison d'applications SaaS à l'aide de NetScaler Gateway Service vous offre une solution simple, sécurisée, robuste et évolutive pour gérer les applications. Les applications SaaS fournies sur le cloud présentent les avantages suivants :

- Configuration simple — Facile à utiliser, à actualiser et à consommer.
- Single Sign-on — Ouverture de session sans tracas avec Single Sign-on.
- Modèle standard pour différentes applications : configuration basée sur des modèles d'applications populaires.

Fonctionnalités du service Citrix Gateway

- Simplicité : réduire la complexité du déploiement et de la gestion de NetScaler à l'aide d'une offre basée sur le cloud
- Toujours à jour : Simplifiez la gestion de Citrix Gateway avec un produit toujours à jour
- Sécurité et haute disponibilité : améliorer la sécurité et la disponibilité des services XenApp et XenDesktop
- Vitesse : permet de déployer et de gérer Citrix Gateway plus rapidement et plus facilement
- Commodité : les services de passerelle sont regroupés et vendus ensemble pour simplifier la gestion des cas d'utilisation auxquels les services informatiques sont le plus souvent confrontés.

Citrix Gateway Service
Réduisez les coûts, simplifiez la gestion et améliorez l'expérience utilisateur grâce à un accès distant sécurisé.

Vue d'ensemble du service de contrôle d'accès

Grâce au service de contrôle d'accès, les administrateurs peuvent offrir une expérience cohérente qui intègre l'authentification unique, l'accès à distance et l'inspection du contenu dans une solution unique pour le contrôle d'accès de bout en bout. Les administrateurs informatiques peuvent régir l'accès aux applications SaaS approuvées avec une expérience d'authentification unique simplifiée. Grâce au service Contrôle d'accès, les administrateurs peuvent également protéger le réseau et les périphériques des utilisateurs finaux de l'entreprise contre les programmes malveillants et les fuites de données en filtrant l'accès à des sites Web et à des catégories de sites Web spécifiques. Les administrateurs peuvent appliquer des stratégies de sécurité d'accès améliorées pour un accès sécurisé aux applications SaaS. Une fois authentifiés, les employés ont accès à toutes les applications métier critiques à partir de n'importe quel appareil, qu'ils se trouvent au bureau, à la maison ou en voyage.

Les administrateurs peuvent surveiller les activités des utilisateurs, telles que

- sites Web malveillants, dangereux ou inconnus visités
- la bande passante consommée
- comportements risqués de téléchargement et de téléchargement.

En utilisant Analytics autour des sites Web et des catégories de sites Web accessibles, les administrateurs peuvent prendre des mesures correctives pour protéger le réseau d'entreprise. En même temps, le service offre aux utilisateurs finaux un accès transparent et sécurisé à toutes leurs applications hébergées.

Les administrateurs peuvent également restreindre les actions, telles que l'impression restreinte, les téléchargements et l'accès au Presse-papiers (copier-coller).

Le diagramme suivant est une représentation visuelle du service de contrôle d'accès.

Service de passerelle avec fonctions de contrôle d'accès

Voici quelques-unes des tâches clés que vous pouvez effectuer avec le service Contrôle d'accès :

- Publiez des applications SaaS avec accès à authentification unique.
- Définissez des stratégies de sécurité améliorées pour les applications SaaS. (Par exemple, filigrane, restriction copier-coller et empêcher les téléchargements.)
- Définissez une stratégie d'accès pour les catégories de sites Web et les sites Web à bloquer.
- Définissez une stratégie d'accès pour les catégories de sites Web et les sites Web à rediriger vers le service Secure Browser.
- Comprendre l'activité des utilisateurs et des sites Web dans le contexte des applications SaaS et les corréler aux stratégies définies.

- Apporter des modifications de stratégie pour autoriser ou bloquer l'accès au site Web, et activer l'accès dans une session de service de navigateur sécurisé.

Etapes de publication SaaS de Citrix Gateway Service

Prise en charge des applications logicielles en tant que service

Démarrer en quatre étapes simples

1. Inscrivez-vous à Citrix Cloud
2. Demande d'évaluation de NetScaler Gateway Service
3. NetScaler Gateway Service est provisionné
4. Accéder à l'interface utilisateur de NetScaler Gateway Service

Démarrer avec Citrix Cloud ici

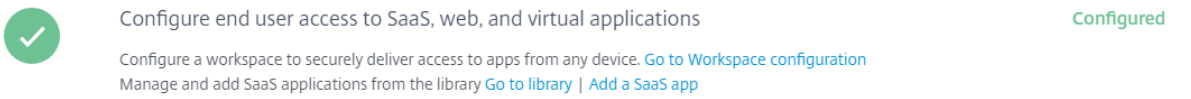
Démarrer avec Citrix Workspace ici

Configuration de l'application SaaS de Citrix Gateway Service

Dans cet exemple, nous parcourons les étapes de configuration nécessaires pour configurer Citrix Gateway Service avec l'application SaaS Salesforce.com.

Configurer l'accès des utilisateurs finaux aux applications SaaS, Web et virtuelles configurées

Configurez un espace de travail pour fournir un accès sécurisé aux applications à partir de n'importe quel appareil. Accéder à la configuration de l'espace de travail
Gérer et ajouter des applications SaaS à partir de la bibliothèque Aller à la bibliothèque | Ajouter une application SaaS



Pour ajouter une application SaaS à partir du catalogue d'applications Citrix Gateway Service, procédez comme suit

Accédez à l'instance d'abonnement Citrix à l'URL suivante

Connexion au compte Citrix Cloudet fournissez vos informations d'identification de connexion à vos organisations.

1. Lancez la vignette **Citrix Gateway Service** à partir du portail d'administration Citrix Cloud.
2. Lancez le lien « Get Started » pour configurer une application SaaS SSO.
3. Sélectionnez un modèle d'application SaaS dans la liste Catalogue d'applications.

   Dans cet exemple, nous allons configurer Salesforce pour SSO en tant qu'application Workspace SaaS.
4. Complétez les paramètres spécifiques à l'application SaaS requis :

   > **Remarque :**
   >
   > Dans cet exemple, nous sélectionnons « En dehors de mon réseau d'entreprise » car il s'agit d'une application SaaS hébergée par un abonnement d'application tiers.
5. Gérez les abonnés aux applications SaaS de l'espace de travail.
6. Attribuez des utilisateurs à l'application SaaS à partir du domaine des utilisateurs.

   > **Remarque :**
   >
   > vous vous authentifiez dans votre espace de travail via les informations d'identification suivantes :
   >
   > - Windows Active Directory
   > - Azure Active Directory

Configuration du contrôle d'accès pour les applications SaaS

Citrix Access Control (CAC), qui s'appuie sur les fonctionnalités d'authentification unique et d'authentification multifacteur (MFA) incluses dans le service de passerelle pour offrir un contrôle de stratégie plus détaillé pour l'accès et l'utilisation des SaaS et des applications Web. Associée à des analyses avancées basées sur l'analyse du comportement des utilisateurs et leurs scores de risque, la CAC renforce la position globale de sécurité de la fourniture de l'espace de travail numérique sécurisé aux utilisateurs finaux de l'entreprise.

Contrôle d'accès Paramètres de sécurité améliorés

- Activer une sécurité renforcée : lance et surveille le Web ou l'application SaaS dans le navigateur intégré Citrix, et achemine le trafic inconnu vers le contrôle d'accès.
- Restreindre l'accès au Presse-papiers : désactive les opérations de coupe/copier/coller entre l'application et le Presse-papiers système
- Restreindre l'impression : désactive la possibilité d'imprimer à partir du navigateur de l'application.
- Restreindre la navigation : désactive les boutons du navigateur de l'application suivante/arrière.
- Restreindre les téléchargements : désactive la possibilité de téléchargement de l'utilisateur à partir de l'application.
- Afficher le filigrane : affiche un filigrane sur l'écran de l'utilisateur affichant le nom d'utilisateur et l'adresse IP de la machine de l'utilisateur.

Contrôle d'accès pour les paramètres d'accès au contenu

Configurez le filtrage Web pour autoriser/bloquer l'accès des utilisateurs finaux et redirigez-les vers Citrix Secure Browser Service.

- Sélectionnez **Configurer l'accès au contenu**
- Sélectionner **Modifier**
- Activer la liste des sites Web Filtrer
  - Ajout/Suppression de sites Web bloqués ou autorisés
  - Ajout/Suppression de catégories de sites Web bloqués ou autorisés

---

Lancement de l'application Citrix Workspace avec contrôle d'accès

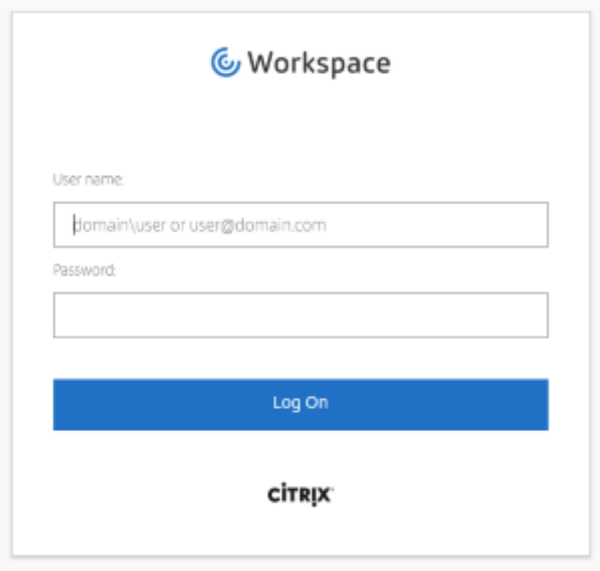
L'application Workspace SaaS se trouve au nom de domaine complet suivant pour les abonnements hébergés US-Americas :

Connexion au compte Citrix Cloud

Vous pouvez accéder à votre expérience d'espace de travail via l'application Workspace, disponible en 3 versions :

- Bureau (Windows/Mac)
- Mobile (iOS/Android)
- Web (HTML5)

1. À l'aide d'un navigateur Web, connectez-vous à l'URL de l'espace de travail.



2. Sélectionnez la vignette d'application SaaS dans l'espace de travail.
3. L'application est lancée de manière transparente dans un onglet de navigateur, avec SSO natif.

Liens de référence

Conception de référence validée pour haute disponibilité Citrix ADC avec IP frontale Azure Load Balancer

January 8, 2020

Généralités

Implémentez un déploiement Citrix ADC haute disponibilité dans Microsoft Azure en utilisant l'équilibrage de charge Azure (ALB) comme équilibreur de charge frontal (FE).

Vous pouvez déployer une paire d'appliances virtuelles Citrix ADC avec plusieurs cartes réseau dans une configuration active-passive haute disponibilité (haute disponibilité) sur Azure. Chaque carte réseau peut contenir plusieurs adresses IP.

Configuration de Citrix ADC VPX en mode haute disponibilité dans Azure Service Management

Le mode actif-passif offre une fonction de basculement. Dans ce mode, les instances VPX synchronisent leurs états de configuration. Lorsque l'instance principale tombe en panne, l'instance sec-

ondaire prend le relais.

Pour plus d'informations sur la haute disponibilité des appliances Citrix ADC, voir Haute disponibilité

Dans un déploiement Microsoft Azure, une configuration haute disponibilité de deux machines virtuelles Citrix ADC est obtenue à l'aide de l'équilibreur de charge Azure, qui distribue le trafic client sur les serveurs virtuels configurés sur les deux instances Citrix ADC. Deux types d'équilibreurs de charge Azure sont disponibles pour la haute disponibilité :
l'équilibrage de charge externe Azure : si le trafic client provient d'Internet, vous devez déployer l'équilibreur de charge externe entre Internet et les instances Citrix ADC VPX pour distribuer le trafic client.
Équilibreur de charge interne Azure : si le trafic client provient du service cloud ou est transféré par une passerelle ou un pare-feu au sein du service cloud, vous devez déployer l'équilibreur de charge interne pour distribuer le trafic client.
Pour obtenir une haute disponibilité sur Azure, vous devez ajouter les deux machines virtuelles Citrix ADC en tant que jeu d'équilibrage de charge et configurer les points de terminaison.

Hypothèses de déploiement actif-passif de Citrix ADC

- Configuration de réseau indépendant (INC) haute disponibilité
- L'équilibrage de charge Azure (ALB) en mode retour direct du serveur (DSR)
- Tout le trafic passe par le nœud principal.
- Le nœud secondaire reste en mode veille jusqu'à ce que le nœud principal tombe en panne.

> **Remarque :**
>
> pour qu'un déploiement haute disponibilité Citrix ADC sur le cloud Azure fonctionne, vous avez besoin d'une IP publique flottante (PIP) qui peut être déplacée entre les deux nœuds haute disponibilité Citrix ADC. L'équilibrage de charge Azure (ALB) fournit ce PIP flottant, qui est déplacé automatiquement vers le deuxième nœud en cas de basculement.
>
> *Le paramètre IP flottant est configuré dans les règles d'équilibrage de charge ALB telles que définies à l'étape 4 de la section* ***Configuration ALB****.*

Présentation de la fonctionnalité IPSET de Citrix ADC

Un ensemble d'adresses IP est un ensemble d'adresses IP configurées sur l'appliance Citrix ADC en tant qu'adresses IP de sous-réseau (SNIP) ou adresses IP virtuelles (VIP). Un ensemble d'adresses IP est identifié avec un nom significatif qui aide à identifier l'utilisation des adresses IP qu'il contient. Pour créer un ensemble d'adresses IP, ajoutez un ensemble d'adresses IP appartenant à Citrix ADC. Les adresses SNIP et VIP peuvent être présentes dans le même ensemble d'adresses IP.

Vue d'ensemble de l'équilibrage de charge Azure

Déployez les instances de haute disponibilité de Citrix ADC à l'aide du modèle ARM (Azure Resource Manager) Citrix ADC 12.1 High Availability (haute disponibilité).

Ce modèle guide le déploiement du mode Active-Passif haute disponibilité de Citrix ADC. Préconfiguré pour inclure des composants et des paramètres pour offrir une expérience de haute disponibilité transparente. Vous trouverez des détails sur la topologie à l'adresse Haute disponibilité.

Une fois le déploiement réussi, une paire d'appliances Citrix ADC est préconfigurée en mode HA-INC. Le modèle Citrix ADC VPX haute disponibilité prend en charge différents SKU de Citrix ADC tels que BYOL et licence horaire telles que VPX 10, VPX 200, VPX 1000 et VPX 3000.

> **Remarque :**
>
> le modèle ARM pour Citrix ADC contient des variables d'équilibrage de charge Azure spécifiques en tant que ressources.

Conditions préalables à la configuration du déploiement

- Configuration de l'équilibreur de charge Azure
- Configuration de Citrix ADC

Configuration de l'équilibreur de charge Azure

1. Ajoutez une adresse IP frontale pour chaque service Citrix ADC qui sera disponible via l'équilibreur de charge Azure.
2. Ajoutez le pool principal alb pour chaque application.
3. Ajoutez la sonde d'intégrité alb pour chaque application.
4. Ajoutez la règle d'équilibrage de charge alb.
5. Ajouter une ou plusieurs règles de sécurité entrantes au groupe de sécurité réseau (NSG)

Configuration de Citrix NetScaler

NetScaler nécessite l'ajout d'IPSETS pour mapper les ressources Citrix ADC à la configuration IP frontale Azure.

> **Remarque :**
>
> Répétez les étapes suivantes pour chaque VIP nécessitant une IP publique frontale de l'ALB.

1. Ajouter les adresses IP publiques frontales Azure à Citrix ADC

```
add ns ip 23.99.xx.xx 255.255.255.255 -type vip (Azure Frontend Ip
    )
```

2. Créer et lier l'IPSET sur le Citrix ADC pour l'IP frontale Azure

```
add ipset net_1
bind ipset net_1 23.99.xx.xx
```

3. Mettez à jour Citrix ADC VIP avec IPSET

```
set lb vserver net_1 -ipset net_1
```

Vérifier la connectivité du port à l'ALB

Utilisez un outil comme `https://ping.eu/port-chk/` ou similaire pour vérifier que les services ALB et Citrix ADC sont disponibles.

```
    Adresse IP ou nom d'hôte :
    23.99.xx.xx
    Numéro de port : « 80, 443, etc. »
    23.99.xx.xx : le port 80 est ouvert ---
```

Résolution des problèmes

- `nstcpdump` - vérifiez la configuration IP frontale de Citrix ADC
- `nstrace` - vérifier la sonde d'intégrité ALB

Outil de dimensionnement de base de données pour XenDesktop 7

January 8, 2020

Actuellement, le dimensionnement des bases de données pour XenDesktop 7 repose sur la capacité d'interpréter et de comprendre l'article de la base de données de dimensionnement de la base de donnéesCTX139508. Cela n'aide pas si vous savez que vous avez une variation sur les environnements

répertoriés. Pour vous aider, l'un de nos principaux ingénieurs logiciels, Chris Gilbert, a créé un outil simple qui peut aider à générer des informations de dimensionnement personnalisées.

Pourquoi un outil ?

Beaucoup ont demandé un fichier Excel ou une formule simple pour définir le dimensionnement des bases de données, mais ces méthodes ne sont pas optimales en fonction du niveau de complexité et des facteurs impliqués.

L'outil masque la complexité des calculs et permet des différences entre XenDesktop 7.5 et 7.6. Les données qu'il consomme et affiche sont plutôt brutes, mais les commentaires pour les améliorations sont les bienvenus.

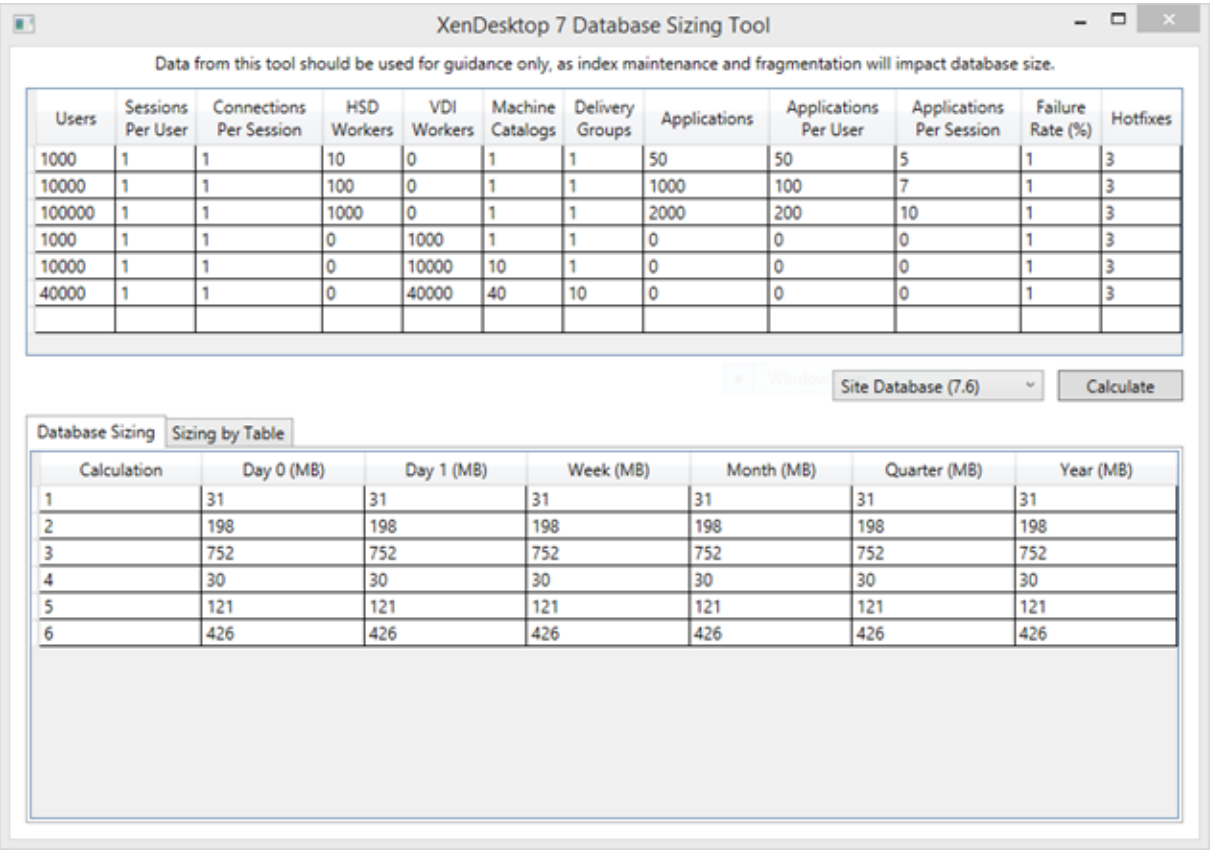
Télécharger les informations

L'outil est un fichier MSI compressé, il est donc facile à installer et à désinstaller. La seule dépendance de l'outil est sur .Net 4.0 ; il n'a besoin d'aucune partie de XenDesktop.

Téléchargez l'outil à partir deCTX209080.

Comment utiliser l'outil

Lorsque vous démarrez l'outil, vous verrez apparaître une fenêtre avec une section en haut, ce qui permet d'entrer des paramètres sur l'environnement attendu. Les jeux par défaut sont VDI et HSD de différentes tailles et devraient ressembler à la capture d'écran suivante :

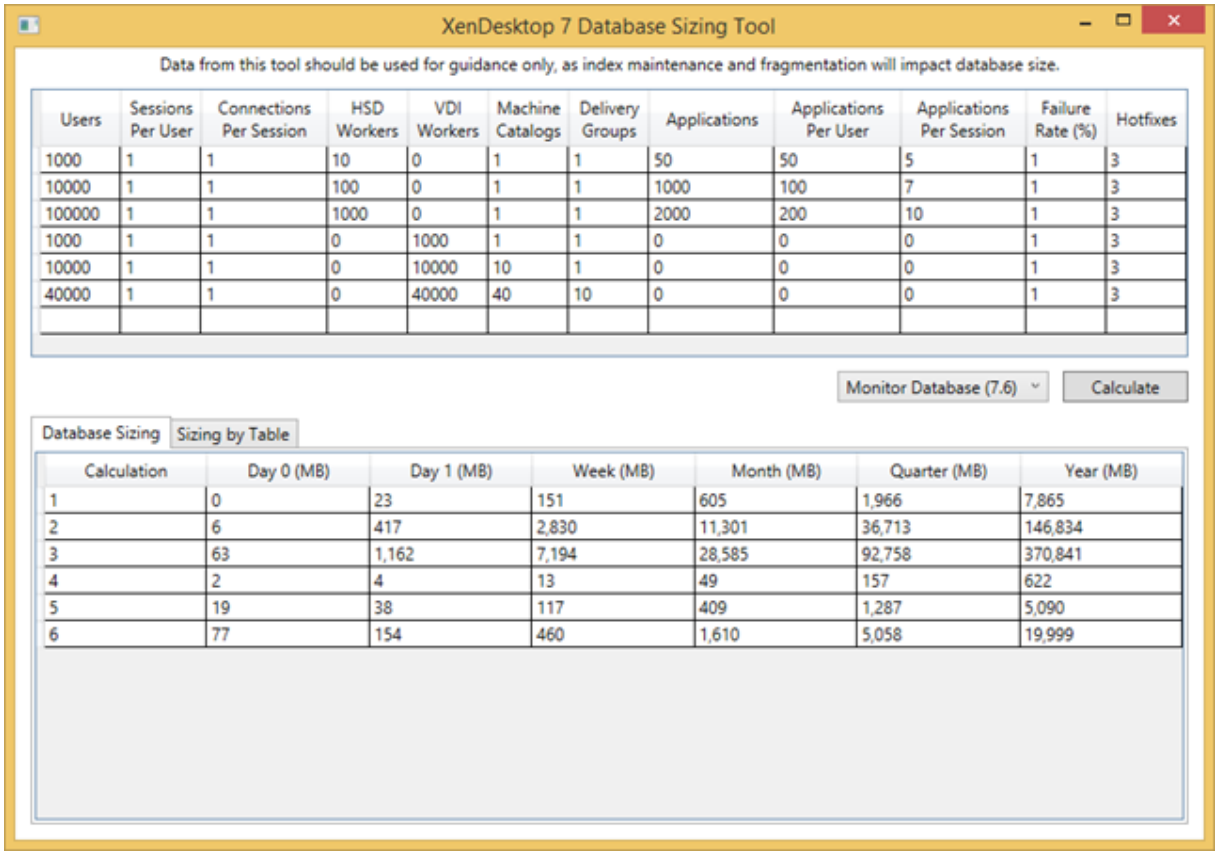


Vous pouvez soit actualiser l'une des lignes, ou simplement commencer à taper des numéros dans la ligne du bas vide, et cela ajoutera d'autres lignes.

Si vous choisissez ensuite le type de base de données et la version de XenDesktop et cliquez sur **Calculer**, le programme exécutera les mathématiques et produira des conseils de dimensionnement vus dans la section inférieure de la capture d'écran ci-dessus.

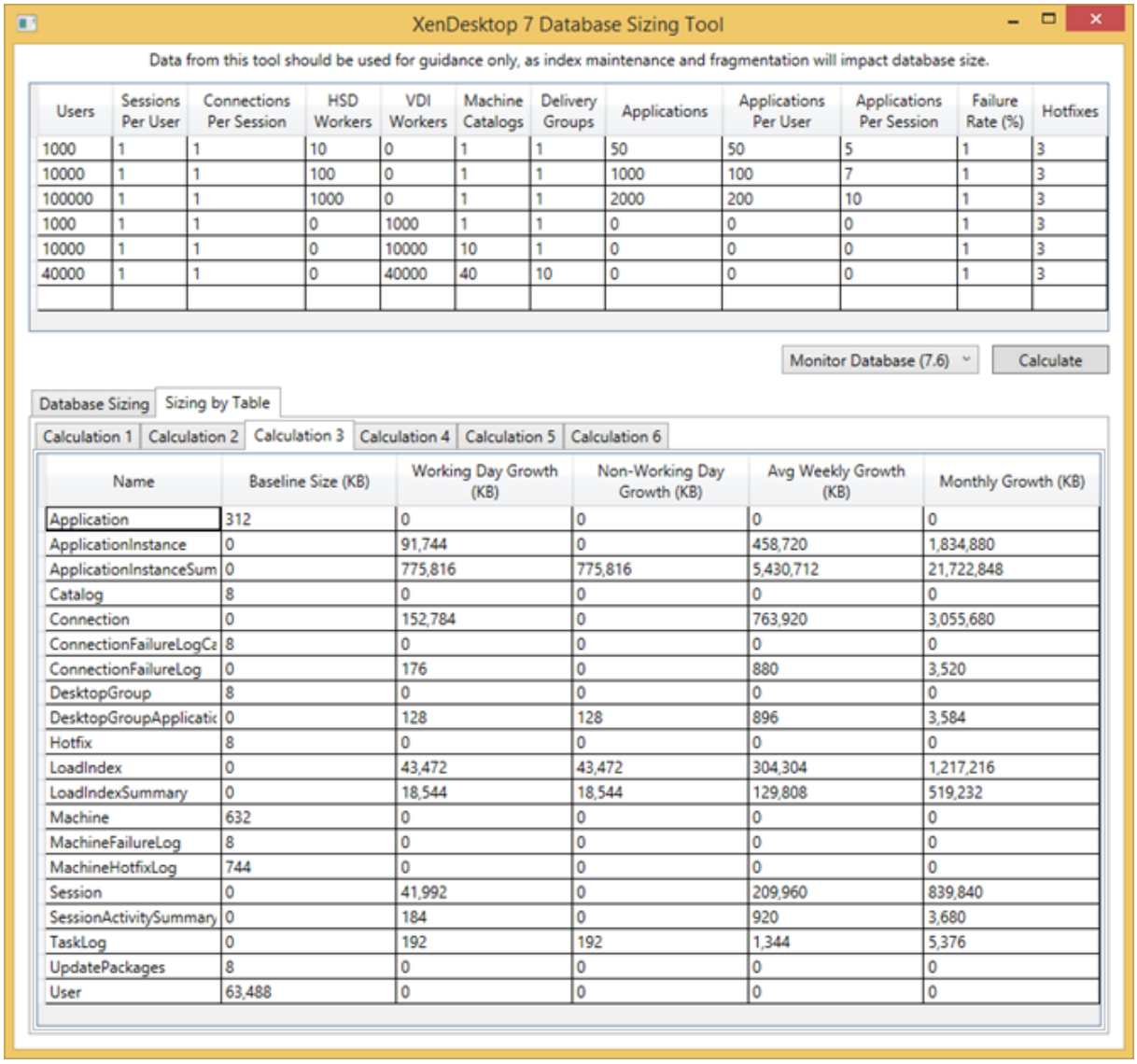
Les données produites comprennent une ligne pour chacune des lignes entrées dans la section supérieure. Les colonnes indiqueront une taille approximative à différents moments dans le temps. Pour les bases de données de site, la taille tend à atteindre une taille maximale et à rester là, car elle n'accumule pas de données. Pour la surveillance, la base de données s'agrandit au fil du temps, en fonction des paramètres de toilettage configurés pour la surveillance. Notez que cela dépend également de la licence (par exemple, seuls les clients Platinum peuvent configurer l'intervalle de toilettage à plus de sept jours).

Ainsi, pour la surveillance, les données se présentent comme suit :



Détails du tableau

Pour plus de détails sur les tables qui consomment réellement de l'espace, cliquez sur l'onglet « Dimensionnement par tableau », à l'intérieur duquel il y a un onglet pour chaque calcul :



Users	Sessions Per User	Connections Per Session	HSD Workers	VDI Workers	Machine Catalogs	Delivery Groups	Applications	Applications Per User	Applications Per Session	Failure Rate (%)	Hotfixes
1000	1	1	10	0	1	1	50	50	5	1	3
10000	1	1	100	0	1	1	1000	100	7	1	3
100000	1	1	1000	0	1	1	2000	200	10	1	3
1000	1	1	0	1000	1	1	0	0	0	1	3
10000	1	1	0	10000	10	1	0	0	0	1	3
40000	1	1	0	40000	40	10	0	0	0	1	3

Name	Baseline Size (KB)	Working Day Growth (KB)	Non-Working Day Growth (KB)	Avg Weekly Growth (KB)	Monthly Growth (KB)
Application	312	0	0	0	0
ApplicationInstance	0	91,744	0	458,720	1,834,880
ApplicationInstanceSum	0	775,816	775,816	5,430,712	21,722,848
Catalog	8	0	0	0	0
Connection	0	152,784	0	763,920	3,055,680
ConnectionFailureLogCa	8	0	0	0	0
ConnectionFailureLog	0	176	0	880	3,520
DesktopGroup	8	0	0	0	0
DesktopGroupApplicatic	0	128	128	896	3,584
Hotfix	8	0	0	0	0
LoadIndex	0	43,472	43,472	304,304	1,217,216
LoadIndexSummary	0	18,544	18,544	129,808	519,232
Machine	632	0	0	0	0
MachineFailureLog	8	0	0	0	0
MachineHotfixLog	744	0	0	0	0
Session	0	41,992	0	209,960	839,840
SessionActivitySummary	0	184	0	920	3,680
TaskLog	0	192	192	1,344	5,376
UpdatePackages	8	0	0	0	0
User	63,488	0	0	0	0

Cette vue plus détaillée vous montre quelles tables peuvent devenir volumineuses afin que vous puissiez éventuellement régler le toilettage de surveillance pour garder certaines zones plus petites. La ventilation couvre la taille de base (telle que la taille fixe). Généralement, les tables basées sur les utilisateurs ou les machines ont une croissance quotidienne (informations d'équilibrage de charge historique) et n'ont une croissance que les jours ouvrables (connexions et sessions). Elles sont ensuite regroupées dans une colonne de croissance hebdomadaire (en supposant cinq jours ouvrables par semaine de sept jours), puis dans la colonne mensuelle.

Exportation des données dans Excel

Pour exporter l'une des tables dans Excel, il vous suffit de cliquer dans le tableau, de sélectionner et de copier tout le contenu, puis de le coller dans Excel.

Cet article a été modifié à partir d'un billet de blog écrit par Chris Gilbert. Vous pouvez trouver le billet

original, lire les commentaires et poster des commentaires ici : https://www.citrix.com/blogs/2014/11/20/database-sizing-tool-for-xendesktop-7/.

Implémentation et configuration

January 23, 2020

Gestion des réseaux

Authentification multi-facteurs Citrix Gateway et Microsoft Azure

Guide de déploiement de zone privée DNS de Citrix ADC pour Azure

Espace de travail

Utilisation du cache d'hôte local pour les mises à niveau de base de données sans interruption de service

Connexion à l'infrastructure Citrix via RDP via un hôte Linux Bastion dans AWS

bases de données SQL Server et Citrix

Évolutivité du service d'authentification fédérée Citrix (téléchargement PDF)

Mises à jour des modèles de gestion des stratégies de groupe pour XenApp et XenDesktop

XenApp et XenDesktop 7.11 à la version actuelle : Améliorations de latence et de blocage des requêtes SQL

Conseils de dimensionnement de base de données pour XenDesktop 7.6

Mise à jour des chaînes de connexion à la base de données lors de l'utilisation de solutions de haute disponibilité SQL Server

Dimensionnement et mise à l'échelle du cache hôte local

Équilibrage de charge du serveur d'impression universel Citrix dans XenApp et XenDesktop 7.9

Citrix Endpoint Management

Déploiement

Pour obtenir la documentation XenMobile Server la plus récente et complète, reportez-vous à la section XenMobile Server.

Authentification multi-facteurs Microsoft Azure et Citrix Gateway

March 2, 2021

Citrix Gateway présente toutes les applications hébergées, SaaS, Web, d'entreprise et mobiles aux utilisateurs sur n'importe quel appareil et n'importe quel navigateur. Il utilise nFactor Authentication pour authentifier les utilisateurs par rapport à Microsoft AD local et utilise Microsoft AD FS pour Azure Multi-Factor Authentication (MFA).

Généralités

Citrix Gateway

Citrix Gateway fournit aux utilisateurs un point d'accès unique et une authentification unique (SSO) aux applications professionnelles et aux données déployées dans un datacenter et le cloud. Il est livré sous forme de SaaS sur un large éventail d'appareils : ordinateurs portables, ordinateurs de bureau, clients légers, tablettes et téléphones intelligents. Citrix Gateway assure la consolidation, contribue à réduire l'encombrement de l'infrastructure d'accès à distance, réduit les coûts, facilite la gestion et offre une meilleure expérience utilisateur. Citrix Gateway facilite la transition informatique vers des environnements de cloud hybride et SaaS.

- **Fédération et authentification unique**

Citrix Gateway fournit une identité fédérée et prend en charge SAML 2.0, OAuth et OpenID pour obtenir une authentification unique sur toutes les applications, qu'il s'agisse d'applications Web, VDI, d'entreprise ou SaaS.

- **Répertoire des utilisateurs sur site**

Citrix Gateway fournit l'authentification SSO aux applications SaaS telles qu'Office 365 et Salesforce, et conserve l'annuaire des utilisateurs sur site. Il peut être implémenté en tant que IdP ou proxy pour Microsoft Active Directory Federation Services (AD FS).

- **Authentification multifacteur (nFactor)**

Citrix Gateway fournit des mécanismes d'authentification nFactor et permet un contrôle granulaire sur qui accède au réseau, ce qui est accessible et comment et quand il est accessible. Il prend en charge tous les mécanismes d'authentification tels que RADIUS, TACACS, NTLM, Diameter, SAML 2.0, OAuth 2.0 et OpenID
2.0.

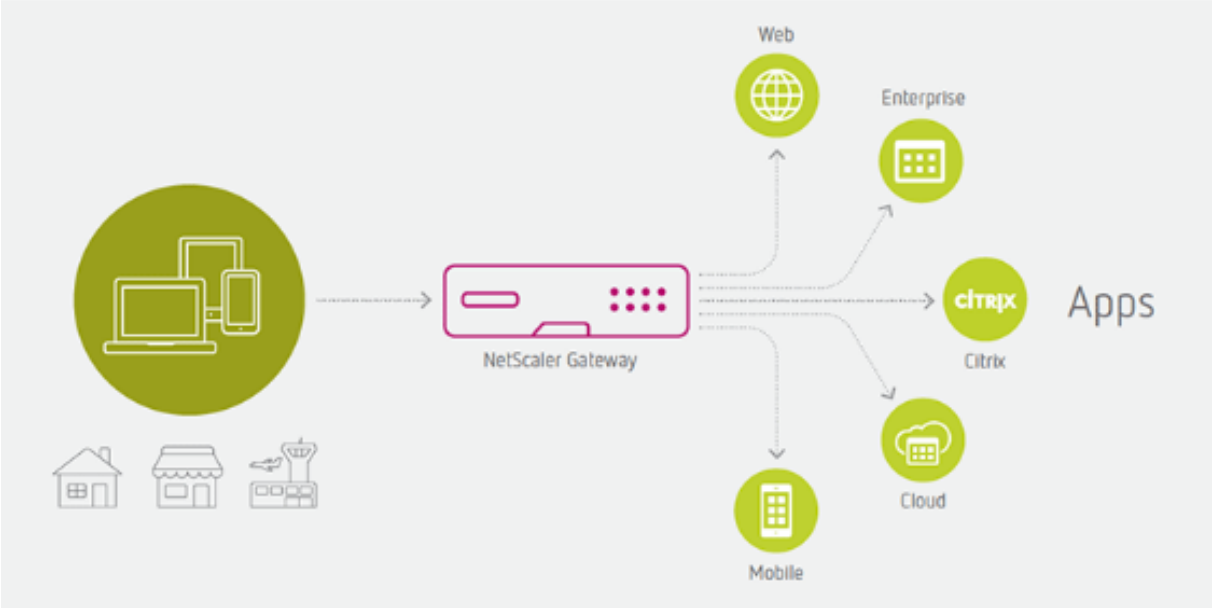
- **Stratégies de contrôle d'accès contextuelles**

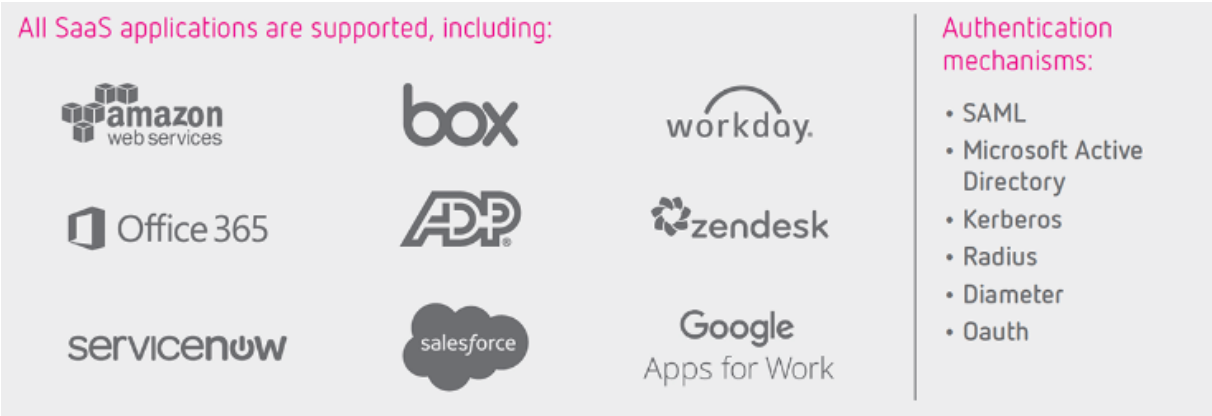
Citrix Gateway permet un contrôle d'accès granulaire aux applications professionnelles en fonction de l'état de la machine de l'utilisateur final, de l'utilisateur, de l'emplacement de l'utilisateur et d'autres

données. Un administrateur informatique peut créer, gérer et appliquer les stratégies pour accéder aux données en toute sécurité dans un environnement d'application. Ces stratégies peuvent être implémentées pour les applications VDI, Web, mobiles, d'entreprise et SaaS.

- **Visibilité et surveillance**

Citrix Application Delivery Management inclut Gateway Insight, qui fournit une visibilité de l'expérience utilisateur de bout en bout pour toutes les applications accessibles via Citrix Gateway. Il fournit des informations aux équipes de support des applications pour résoudre les problèmes liés aux échecs d'authentification, y compris les échecs de vérification EPA et les échecs d'authentification unique.





Microsoft Azure MFA

Les gens se connectent aux ressources organisationnelles dans des scénarios de plus en plus complexes. Les utilisateurs se connectent à partir d'appareils appartenant à l'entreprise, personnels et

publics, sur et hors du réseau de l'entreprise à l'aide de téléphones intelligents, de tablettes, de PC et d'ordinateurs portables, souvent sur plusieurs plates-formes. Dans ce monde toujours connecté, multi-appareils et multi-plateformes, la sécurité des comptes utilisateur est plus importante que jamais. Les mots de passe, quelle que soit leur complexité, utilisés sur les appareils, les réseaux et les plates-formes ne sont plus suffisants pour assurer la sécurité du compte utilisateur, en particulier lorsque les utilisateurs ont tendance à réutiliser les mots de passe entre les comptes. Les attaques d'hameçonnage sophistiquées et d'autres attaques d'ingénierie sociale peuvent entraîner l'affichage et la vente de noms d'utilisateur et de mots de passe sur le Web sombre.

La sécurité du processus de vérification en deux étapes réside dans son approche à plusieurs niveaux. La compromission de plusieurs facteurs d'authentification représente un défi important pour les attaquants. Même si un attaquant parvient à apprendre le mot de passe de l'utilisateur, il est inutile sans avoir également la possession de la méthode d'authentification supplémentaire. Il fonctionne en exigeant deux ou plusieurs des méthodes d'authentification suivantes :

- Quelque chose que vous savez (généralement un mot de passe)
- Quelque chose que vous avez (un appareil de confiance qui n'est pas facilement dupliqué, comme un téléphone)
- Quelque chose que vous êtes (biométrie)

Azure Multi-Factor Authentication aide à protéger l'accès aux données et aux applications. Il fournit une couche supplémentaire de sécurité en utilisant une seconde forme d'authentification. Les organisations peuvent utiliser l'accès conditionnel pour adapter la solution à leurs besoins spécifiques.

Méthodes de déploiement Microsoft Azure MFA

Il existe différentes méthodes pour exploiter Azure MFA en tant que deuxième facteur d'authentification. Ces méthodes sont brièvement expliquées ci-dessous avec leurs avantages et leurs inconvénients.

Serveur Azure MFA

Le serveur Microsoft Azure Multi-Factor Authentication était la méthode d'origine et il va être obsolète. Il ne devrait pas être envisagé pour une nouvelle mise en œuvre comme

- Il n'y a pas d'autre investissement de la part de Microsoft sur cette méthode.
- Il n'y a pas d'intégration avec SSPR et Azure MFA basé sur le cloud.
- Il n'existe pas d'outil de migration transparente du serveur MFA vers la solution basée sur le cloud MFA.

Extension de serveur de stratégie réseau MFA Azure

Network Policy Server (NPS) extension pour Azure MFA est une solution prise en charge qui utilise l'adaptateur NPS pour se connecter avec Azure MFA Cloud. Il peut être utilisé comme serveur RADIUS

local.

- La carte NPS (RADIUS) fournit un emplacement réseau à l'intérieur/à l'extérieur de la règle MFA ou marche/arrêt.
- Il n'est pas compatible avec les stratégies d'accès conditionnel Azure AD similaires à la méthode d'intégration SAML. Les stratégies d'accès conditionnel offrent des expériences utilisateur beaucoup plus riches et meilleures.
- Les utilisateurs doivent être enregistrés dans MFA avant d'utiliser l'adaptateur NPS. Contrairement à Azure MFA Cloud et Accès conditionnel, si l'utilisateur n'est pas enregistré, l'extension NPS ne parvient pas à authentifier l'utilisateur, ce qui génère plus d'appels vers le centre d'assistance.
- Lorsque l'adaptateur NPS invoque MFA, il frappe les utilisateurs enregistrés option par défaut. Il n'y a pas de notification visuelle à l'utilisateur que MFA est nécessaire et à venir. Il n'y a pas d'interface utilisateur pour modifier les méthodes MFA pendant un processus fermé. Si l'utilisateur n'a pas son périphérique par défaut avec lui, il échouera. L'utilisateur doit revenir au portail selfservice et réinitialiser l'option par défaut, puis essayer de se connecter à nouveau.

Microsoft AD FS et Azure MFA

Si votre organisation est fédérée avec Azure AD, mais que le hachage des mots de passe ne sont pas synchronisés avec Azure AD, vous pouvez utiliser AD local pour LDAP (Lightweight Directory Access Protocol) et activer Azure MFA dans le cadre des stratégies d'accès sur les parties relais AD FS. À partir de Windows Server 2016, vous pouvez désormais configurer Azure MFA pour l'authentification principale.

- L'adaptateur MFA Azure est intégré à Windows Server 2016, et il n'est pas nécessaire d'effectuer une installation supplémentaire.
- L'adaptateur Azure MFA s'intègre directement à Azure AD et ne nécessite pas de serveur Azure MFA local.
- Si les utilisateurs ne sont pas inscrits à MFA, ils sont guidés tout au long du processus lors de la prochaine connexion. Cela garantit moins d'appels au service d'assistance et un meilleur processus pour les utilisateurs.
- Les utilisateurs reçoivent une notification visuelle indiquant que MFA est nécessaire et à venir. Les utilisateurs peuvent modifier l'option de Gateway lors d'un processus fermé dans l'interface utilisateur.

Azure AD et Azure MFA

Si votre organisation synchronise le hachage des mots de passe dans Azure AD, Azure MFA peut être exploité via des stratégies d'accès conditionnel pour demander aux utilisateurs une authentification de second facteur.

- Cette méthode ne nécessite aucune installation supplémentaire sur site.
- Si les utilisateurs ne sont pas inscrits à MFA, ils sont guidés tout au long du processus lors de la prochaine connexion. Cela garantit moins d'appels au service d'assistance et un meilleur processus pour les utilisateurs.
- Les utilisateurs reçoivent une notification visuelle indiquant que MFA est nécessaire et à venir. Les utilisateurs peuvent modifier l'option de Gateway lors d'un processus fermé dans l'interface utilisateur.

Authentification pass-through Azure AD et Azure MFA

Azure AD Pass-through Authentication (PTA) permet aux utilisateurs de se connecter à des applications locales et basées sur le cloud à l'aide des mêmes mots de passe. Lorsque les utilisateurs se connectent à l'aide d'Azure AD, cette fonctionnalité valide les mots de passe des utilisateurs directement par rapport à Active Directory local. Azure AD PTA est une alternative à la synchronisation de hachage de mot de passe Azure AD, qui offre le même avantage de l'authentification dans le cloud aux organisations.

- Azure AD PTA nécessite l'installation d'un agent léger sur site.
- Azure AD PTA protège les comptes d'utilisateurs en travaillant de manière transparente avec les stratégies d'accès conditionnel Azure AD, y compris Azure MFA.
- Les utilisateurs peuvent effectuer des tâches de gestion des mots de passe en libre-service dans le cloud.
- Les mots de passe locaux ne sont jamais stockés dans le cloud sous quelque forme que ce soit.
- L'agent établit uniquement des connexions sortantes à partir de votre réseau. Par conséquent, il n'est pas nécessaire d'installer l'agent dans un réseau de périmètre, également connu sous le nom de DMZ.

Situation actuelle

Un environnement présentant les caractéristiques suivantes nécessite l'utilisation d'Azure MFA comme deuxième facteur d'authentification :

- AD local avec synchronisation Azure AD est configuré.
- La synchronisation de hachage de mot de passe Azure AD est désactivée.
- L'accès aux applications O365 est requis.
- L'accès aux applications virtuelles Citrix et aux postes de travail locaux est requis.
- L'accès aux applications avec une méthode d'authentification moderne (SAML, OAuth) est requis.
- L'accès aux applications avec une méthode d'authentification héritée est requis.

Points de conception

Voici les points de conception de la solution proposée :

- Accédez aux applications hébergées, SaaS, d'entreprise et Web dans un seul portail et en toute sécurité est nécessaire.
- Les utilisateurs ne doivent entrer leurs informations d'identification qu'une seule fois au cours du processus d'authentification.
- L'authentification unique doit être fournie pour toutes les applications hébergées, SaaS, d'entreprise et Web.

Solution proposée

Généralités

La solution proposée repose sur les éléments suivants :

- Citrix Gateway local
- Microsoft AD local
- Microsoft AD FS local
- Citrix ADC local en tant que proxy AD FS
- Microsoft Azure MFA

Citrix Gateway exploite la fonctionnalité d'authentification, d'autorisation et d'audit (Citrix ADC AAA) et les mécanismes d'authentification nFactor pour authentifier l'utilisateur avec la stratégie LDAP et exploiter la stratégie d'accès sur le relais AD FS pour déclencher le processus de validation Azure MFA. Une fois Azure MFA validé l'utilisateur, AD FS génère l'assertion SAML (réponse SAML) et redirige l'utilisateur vers Citrix Gateway. À ce stade, l'utilisateur est authentifié et Citrix Gateway présente toutes les applications que l'utilisateur est autorisé à utiliser.

La solution nécessite deux enregistrements DNS publics et deux adresses IP publiques :

Description	Valeur
Nom de domaine complet Citrix Gateway	access.ctxdemos.com
Authentification, autorisation et audit de Citrix FQDN	aaa.ctxdemos.com

La solution utilise un certificat SSL public :

Description	Valeur
Nom commun	access.ctxdemos.com
Autre nom du sujet	sts.ctxdemos.com
Autre nom du sujet	aaa.ctxdemos.com

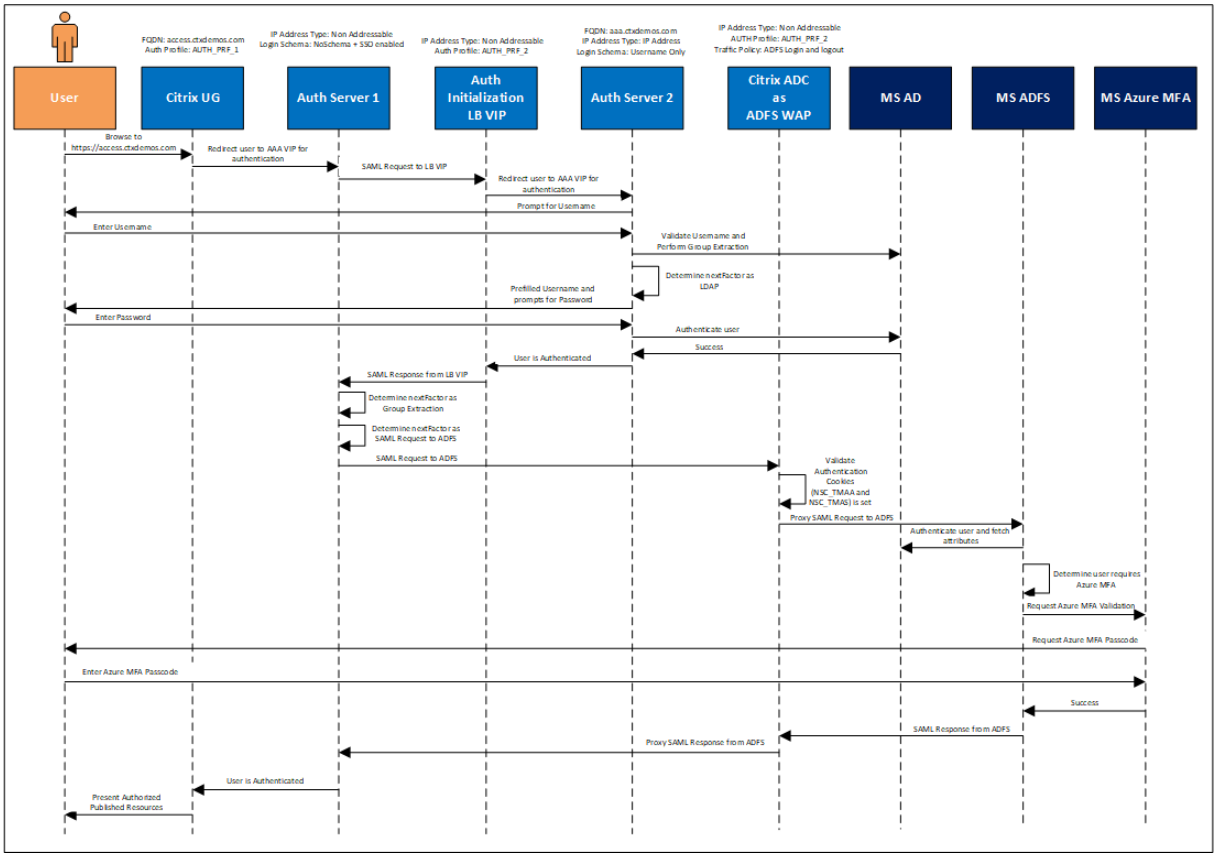
La solution utilise également un certificat SSL générique émis par Microsoft Certificate Authority Services internes :

Description	Valeur
Nom commun	*.ctxdemos.com

Flux d’authentification

Diagramme de séquence

Le diagramme de séquence suivant illustre le flux d’authentification de la solution :



Étapes d'authentification

Les étapes d'authentification sont les suivantes :

1. L'utilisateur accède à https://access.ctxdemos.com.
2. Citrix Gateway redirige l'utilisateur vers le premier VIP Citrix ADC AAA (non adressable).
3. First Citrix ADC AAA VIP utilise une ouverture de session sans schéma, qui est configurée avec une authentification unique. Ensuite, il commence à traiter les stratégies d'authentification avancées.
4. La première stratégie d'authentification est le SP SAML vers un VIP LB non adressable pour générer des cookies d'authentification.
5. L'assistant LB VIP est configuré pour utiliser le second Citrix ADC AAA VIP (Addressable) pour l'authentification. Ainsi, il redirige l'utilisateur vers la deuxième authentification, autorisation et audit VIP.
6. Le second Citrix ADC AAA VIP utilise le schéma de connexion `Username Only`, qui invite l'utilisateur à saisir le nom d'utilisateur. Ensuite, il commence à traiter les stratégies d'authentification avancées.
7. La première stratégie d'authentification est une Extraction de groupe, qui interroge le nom d'utilisateur dans un AD local et valide si l'utilisateur appartient au groupe de sécurité AzureMFACAUsers. Une fois que le résultat de la validation est réussi, il commence à traiter le facteur d'authentification suivant qui est la stratégie LDAP.
8. La stratégie LDAP utilise le schéma de connexion `UsernameAndPassword` et un champ de nom d'utilisateur prérempli et invite l'utilisateur à saisir le mot de passe AD.
9. Lorsque l'authentification sur le deuxième VIP Citrix ADC AAA est terminée avec succès, elle revient à l'assistant LB VIP qui génère une réponse SAML pour la première authentification, autorisation et audit VIP.
10. Le premier VIP Citrix ADC AAA commence à traiter le facteur suivant, qui est une extraction de groupe pour s'assurer que les groupes de l'utilisateur sont extraits d'AD et stockés dans la variable d'authentification, d'autorisation et d'audit à utiliser ultérieurement dans le processus.
11. Premier Citrix ADC AAA VIP commence à traiter le facteur suivant, qui est un SP SAML vers AD FS Proxy VIP sur Citrix ADC.

    > **Remarque :**
    >
    > Citrix ADC est fédéré avec la batterie de serveurs AD FS. Les étapes détaillées sont expliquées dans les sections suivantes.

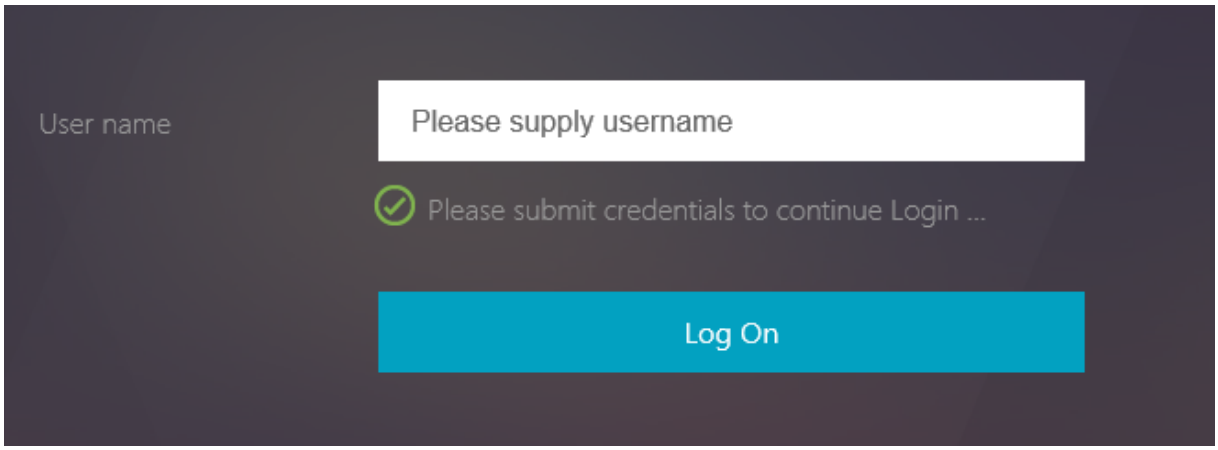
12. AD FS Proxy VIP valide que les cookies d'authentification (NSC_TMAA et NSC_TMAS) sont définis. Ensuite, il envoie la requête SAML à un serveur AD FS back-end (les serveurs AD FS back-end

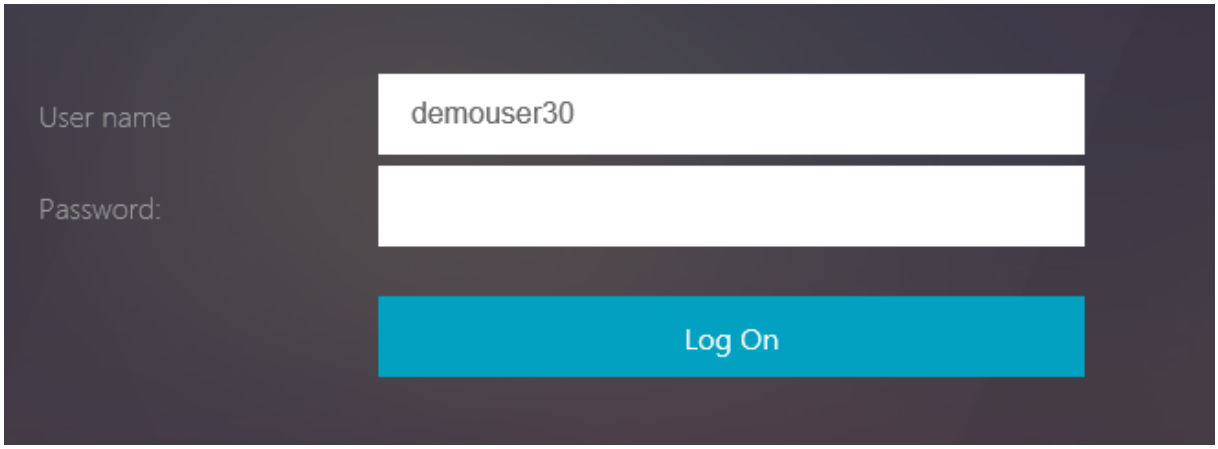
doivent être équilibrés en charge sur un Citrix ADC interne pour une haute disponibilité et une résilience du service).

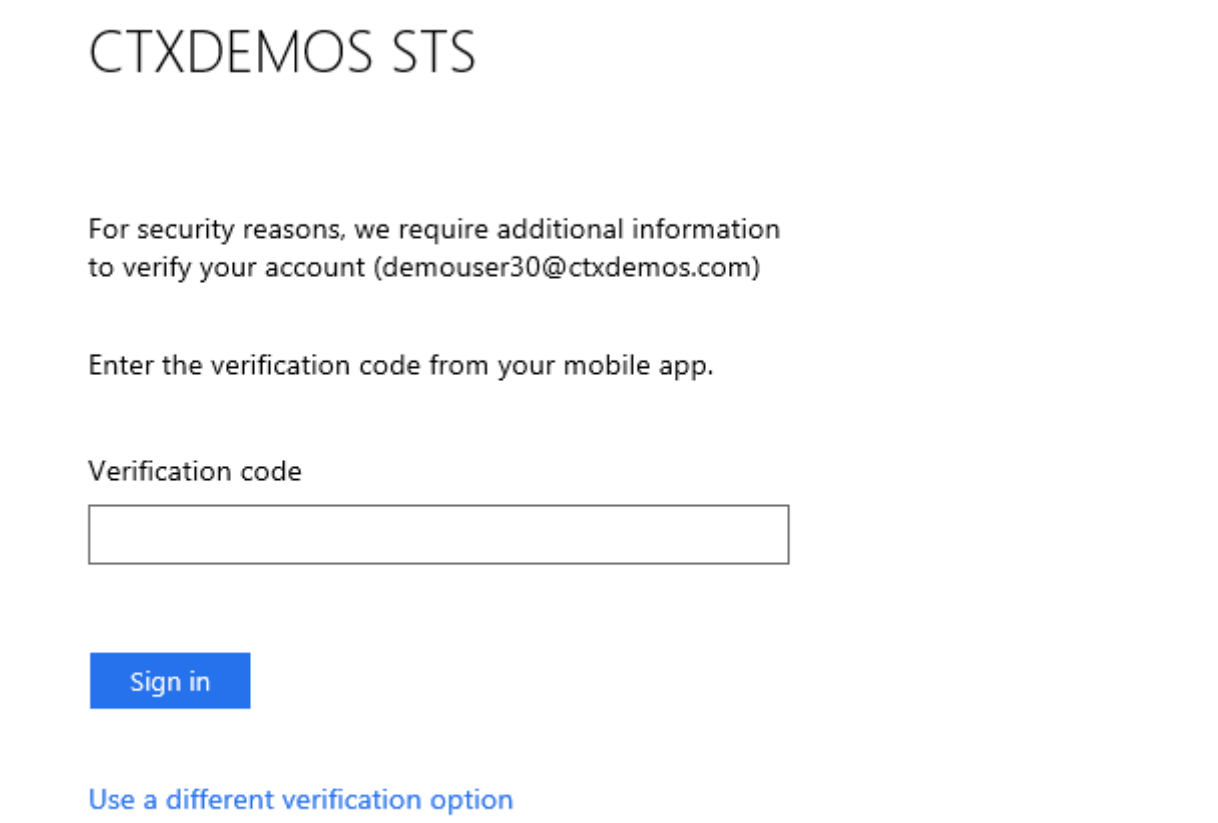
13. Le serveur AD FS traite la demande SAML. Étant donné que la stratégie d'accès sur la partie relais est définie sur « Autoriser tous les utilisateurs et exiger MFA pour l'authentification », elle déclenche le processus d'authentification Azure MFA.
14. Azure MFA traite le nom d'utilisateur. S'il est déjà enregistré, il défie l'utilisateur avec la méthode configurée. Si ce n'est pas le cas, il invite l'utilisateur à s'inscrire et à définir les méthodes d'authentification primaire et secondaire.
15. Une fois le processus d'authentification Azure MFA terminé avec succès, AD FS génère une réponse SAML pour Citrix Gateway (First Citrix ADC AAA VIP).
16. First Citrix ADC AAA VIP reçoit une réponse SAML et confirme que le processus d'authentification de l'utilisateur est terminé.
17. Citrix Gateway envoie des informations d'authentification à Citrix StoreFront, qui énumère toutes les applications et tous les postes de travail que l'utilisateur est autorisé à utiliser. En outre, il traite l'appartenance au groupe de l'utilisateur pour présenter des signets publiés sur Citrix Gateway.

Écrans d'authentification

La plupart des étapes mentionnées ci-dessus sont transparentes pour les utilisateurs car elles se produisent en interne entre différents VIP sur Citrix ADC. L'expérience utilisateur est illustrée ci-dessous :







Implémentation

Microsoft AD FS

Exigences relatives au certificat

Les serveurs de fédération requièrent les certificats du tableau suivant :

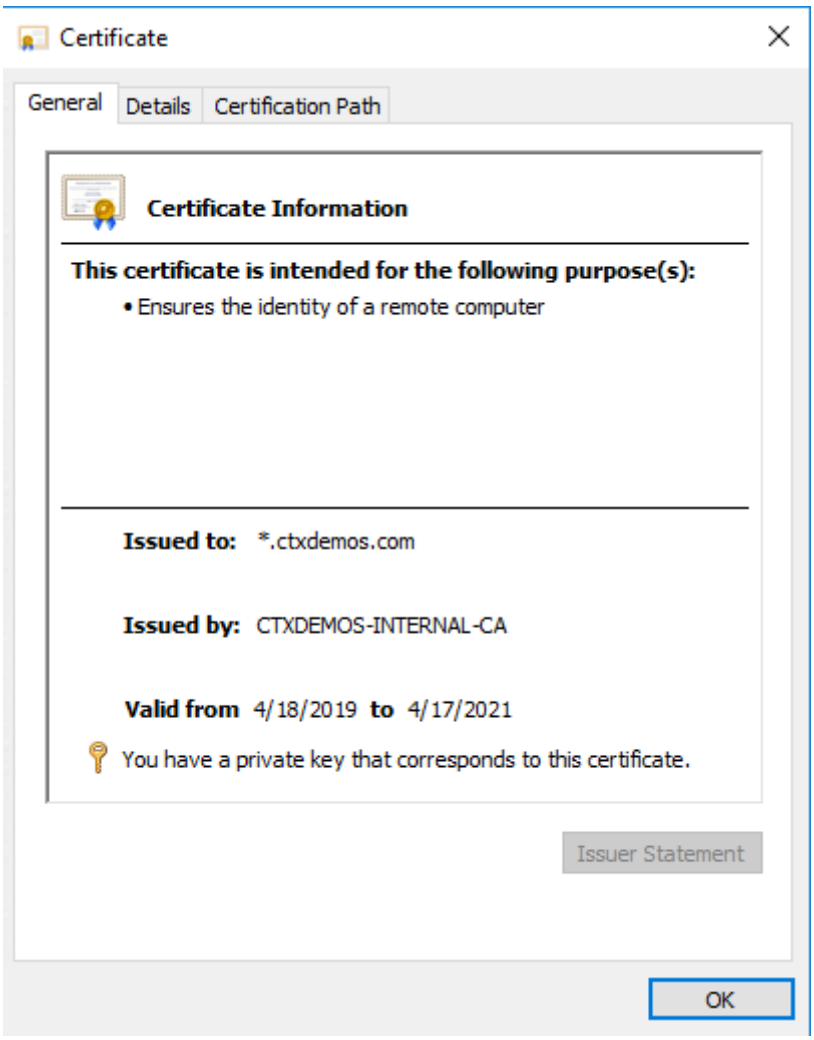
Type de certificat	Description	Ce qui doit être connu avant de déployer
Certificat SSL (Secure Sockets Layer)	Il s'agit d'un certificat SSL (Secure Sockets Layer) standard utilisé pour sécuriser les communications entre les serveurs de fédération et les clients.	Ce certificat doit être lié au site Web par défaut dans Internet Information Services (IIS) pour un serveur de fédération ou un proxy de serveur de fédération. Pour un serveur proxy de fédération, la liaison doit être configurée dans IIS avant d'exécuter l'Assistant Configuration du serveur proxy de fédération avec succès. Recommandation : Étant donné que ce certificat doit être approuvé par les clients d'AD FS, utilisez un certificat d'authentification de serveur émis par une autorité de certification publique (tierce). Par exemple, Verisign. Conseil : le nom de l'objet de ce certificat est utilisé pour représenter le nom du service de fédération pour chaque instance d'AD FS que vous déployez. Pour cette raison, vous pouvez envisager de choisir un nom de sujet sur tout nouveau certificat émis par une autorité de certification qui représente le mieux le nom de votre entreprise ou de votre organisation auprès des partenaires.

Type de certificat	Description	Ce qui doit être connu avant de déployer
Certificat de communication de service	Ce certificat permet la sécurité des messages WCF pour sécuriser les communications entre les serveurs de fédération.	Par défaut, le certificat SSL est utilisé comme certificat de communication de service. Cela peut être modifié à l'aide de la console de gestion AD FS.
Certificat de signature de jeton	Il s'agit d'un certificat X509 standard utilisé pour signer en toute sécurité tous les jetons émis par le serveur de fédération.	Le certificat de signature de jeton doit contenir une clé privée et s'enchaîner à une racine approuvée dans le service de fédération. Par défaut, AD FS crée un certificat auto-signé. Toutefois, vous pouvez modifier ce certificat ultérieurement en un certificat émis par une autorité de certification à l'aide du composant logiciel enfichable Gestion AD FS, en fonction des besoins de votre organisation.
Certificat de déchiffrement de jetons	Il s'agit d'un certificat SSL standard qui est utilisé pour déchiffrer tous les jetons entrants chiffrés par un serveur de fédération partenaire. Il est également publié dans les métadonnées de la fédération.	Par défaut, AD FS crée un certificat auto-signé. Toutefois, vous pouvez modifier ce certificat ultérieurement en un certificat émis par une autorité de certification à l'aide du composant logiciel enfichable Gestion AD FS, en fonction des besoins de votre organisation.

Configuration de l'environnement de démonstration

Type de certificat	Configuration de l'environnement de démonstration
Certificat SSL (Secure Sockets Layer)	Certificat interne émis par l'autorité de certification émettrice interne sur le serveur AD FS. Certificat public approuvé sur Citrix ADC.
Certificat de communication de service	Certificat interne délivré par l'autorité de certification interne d'AHS.
Certificat de signature de jeton	Généré automatiquement par le service AD FS.
Certificat de déchiffrement de jetons	Généré automatiquement par le service AD FS.

Dans l'environnement de démonstration, un certificat générique est inscrit et installé sur le serveur.

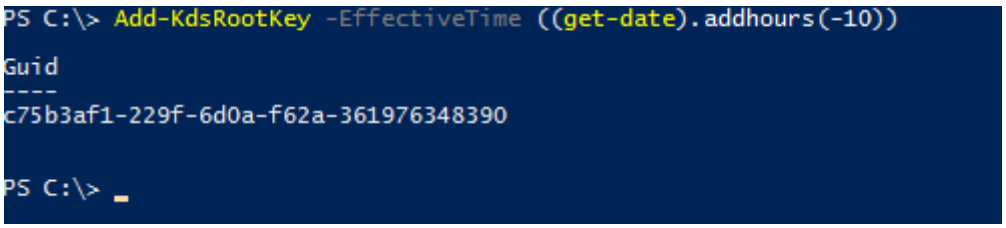


Exigences relatives au compte de service

Vous pouvez créer un compte de service ou tirer parti des comptes de service gérés par groupe (GMSA). Pour utiliser GMSA, vous devez créer une clé racine du service de distribution de clés. Alors, lancez PowerShell et exécutez la commande suivante :

```
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10))
<!--NeedCopy-->
```

Cette commande crée une clé racine du service de distribution de clés, stockée dans Active Directory, et vous permet de créer un compte de service géré (GMSA) de groupe en tant que compte de service AD FS que vous créez ultérieurement. Exécutez cette commande avec les droits d'administrateur de domaine.



Exigences en matière d'enregistrement DNS

Vous avez besoin d'un enregistrement DNS A pour votre nom de service de fédération AD FS en interne et en externe. Dans l'environnement de démonstration, l'enregistrement DNS interne pointe vers l'adresse IP du serveur AD FS et l'enregistrement DNS externe pointe vers l'adresse IP publique Citrix Gateway.

Nom de l'enregistrement	Portée	Type	Adresse IP
sts.ctxdemox.com	Interne	A	22.22.22.6
sts.ctxdemox.com	Externe	A	40.85.225.175

Ajouter le rôle AD FS et configurer la batterie de serveurs AD FS

Ajouter le rôle AD FS

Pour ajouter le rôle AD FS à Windows Server 2016, lancez PowerShell et exécutez la commande suivante :

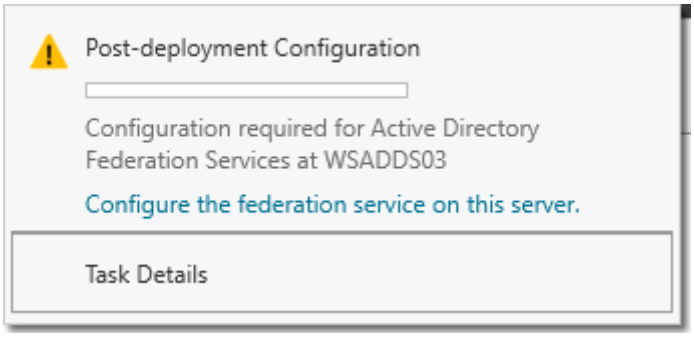
```
Install-WindowsFeature AD FS-Federation -IncludeManagementTools
<!--NeedCopy-->
```



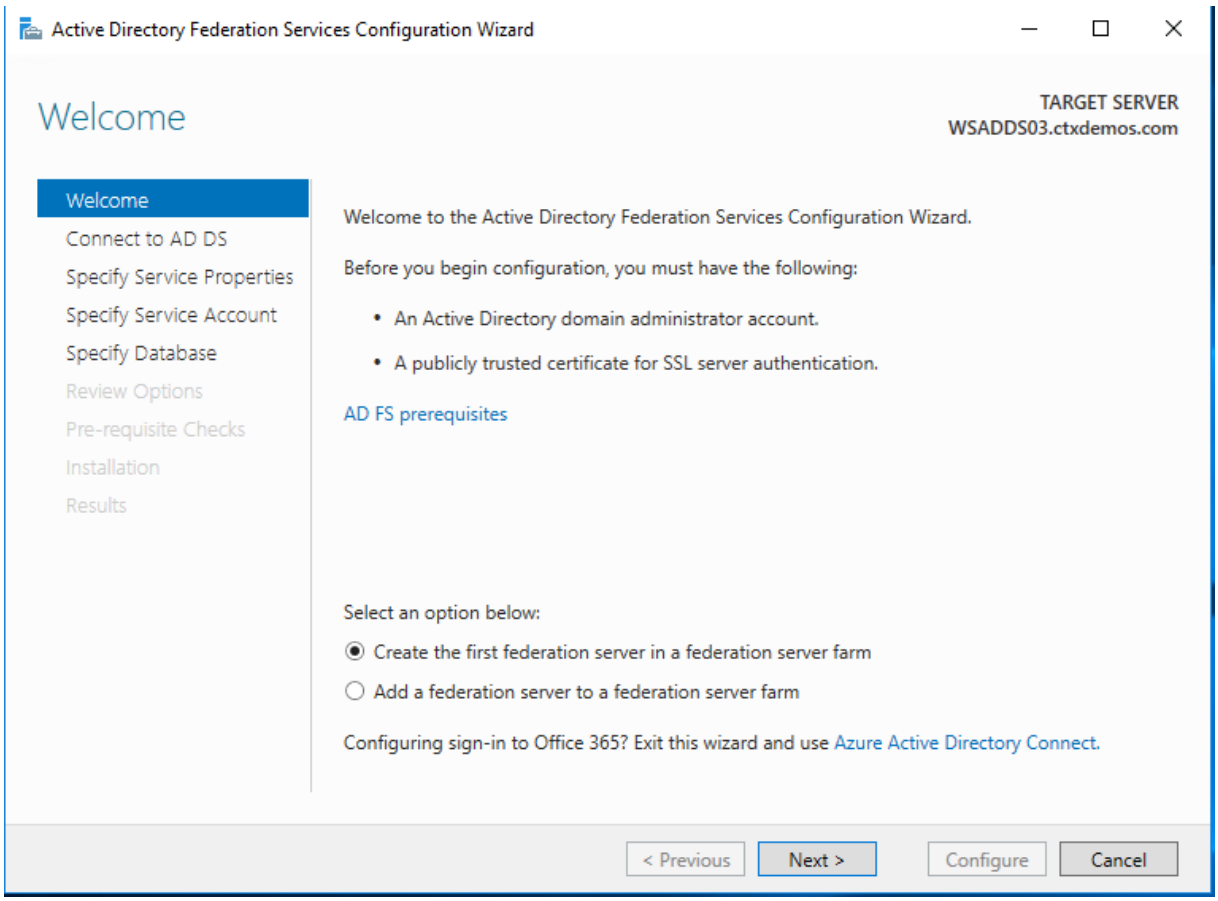
```
PS C:\> Install-WindowsFeature ADFS-Federation -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Federation Services}
WARNING: To finish configuring this server for the federation server role using Windows PowerShell, see
http://go.microsoft.com/fwlink/?LinkId=224868.

PS C:\> _
```

Configurer la batterie de serveurs AD FS

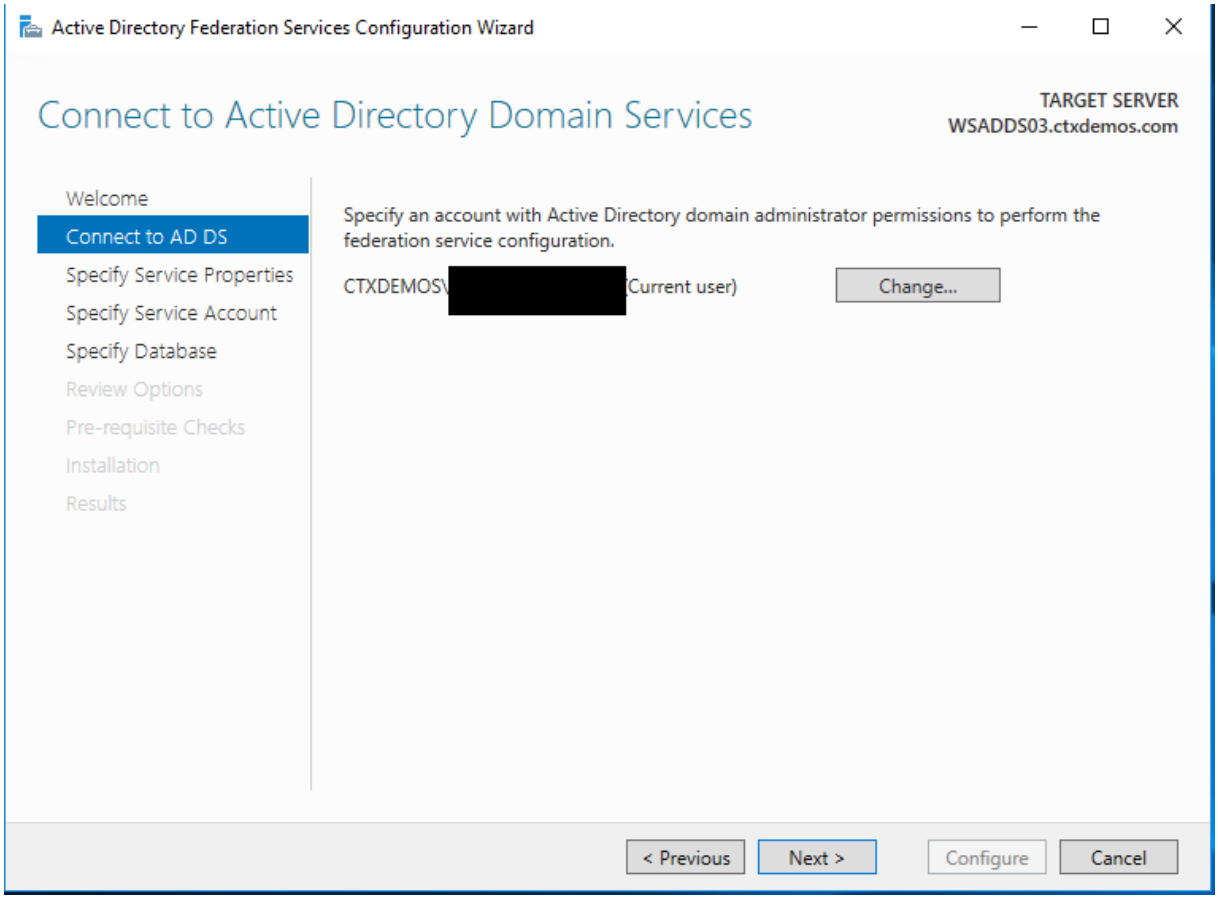
Vous pouvez maintenant commencer votre configuration après déploiement AD FS à partir du Gestionnaire de serveur . Cliquez sur **Configurer le service de fédération sur ce serveur**.



Sur la page **Bienvenue** , sélectionnez **Créer le premier serveur de fédération dans une batterie de serveurs de fédération** , puis cliquez sur **Suivant**.

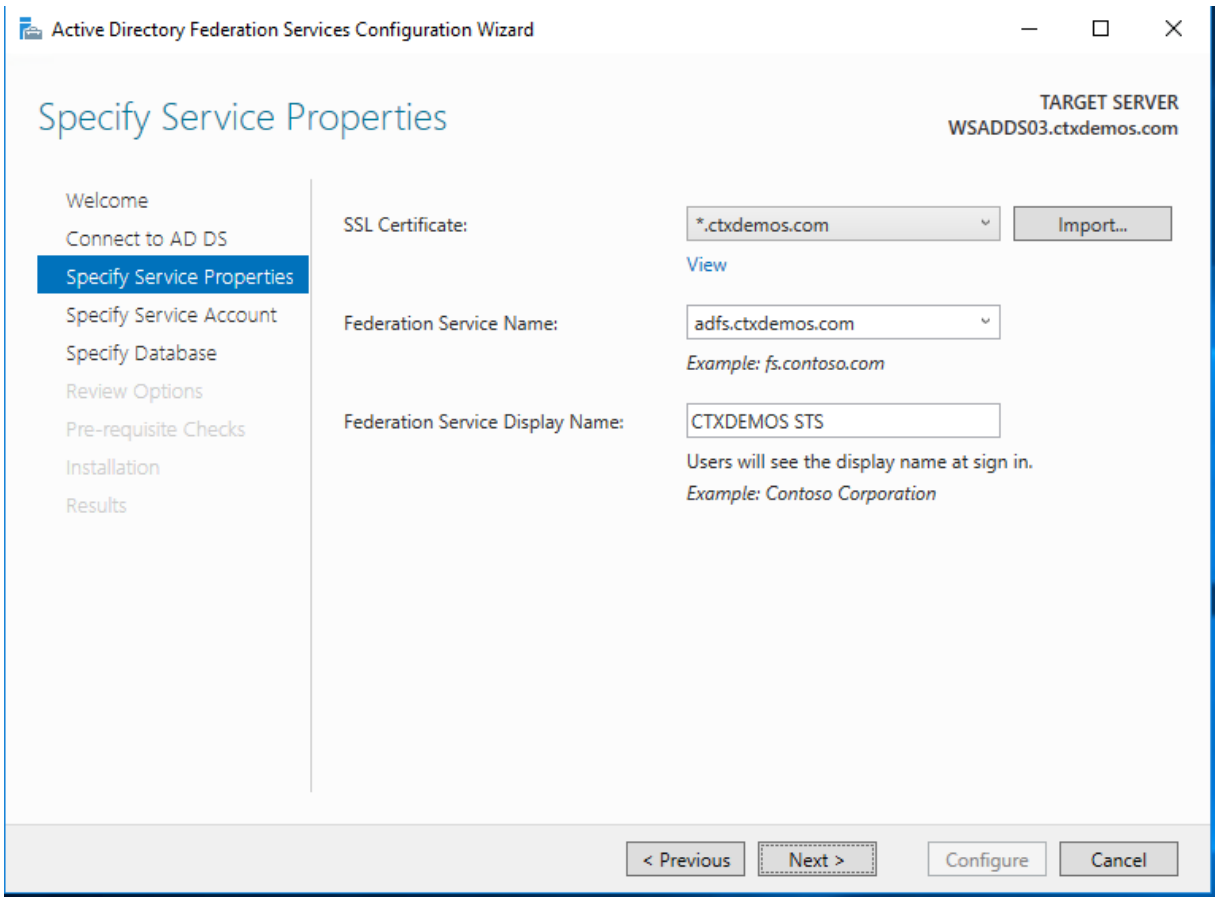


Dans la page **Se connecter aux services de domaine Active Directory**, assurez-vous que le compte Administrateur de domaine est spécifié, puis cliquez sur **Suivant**.

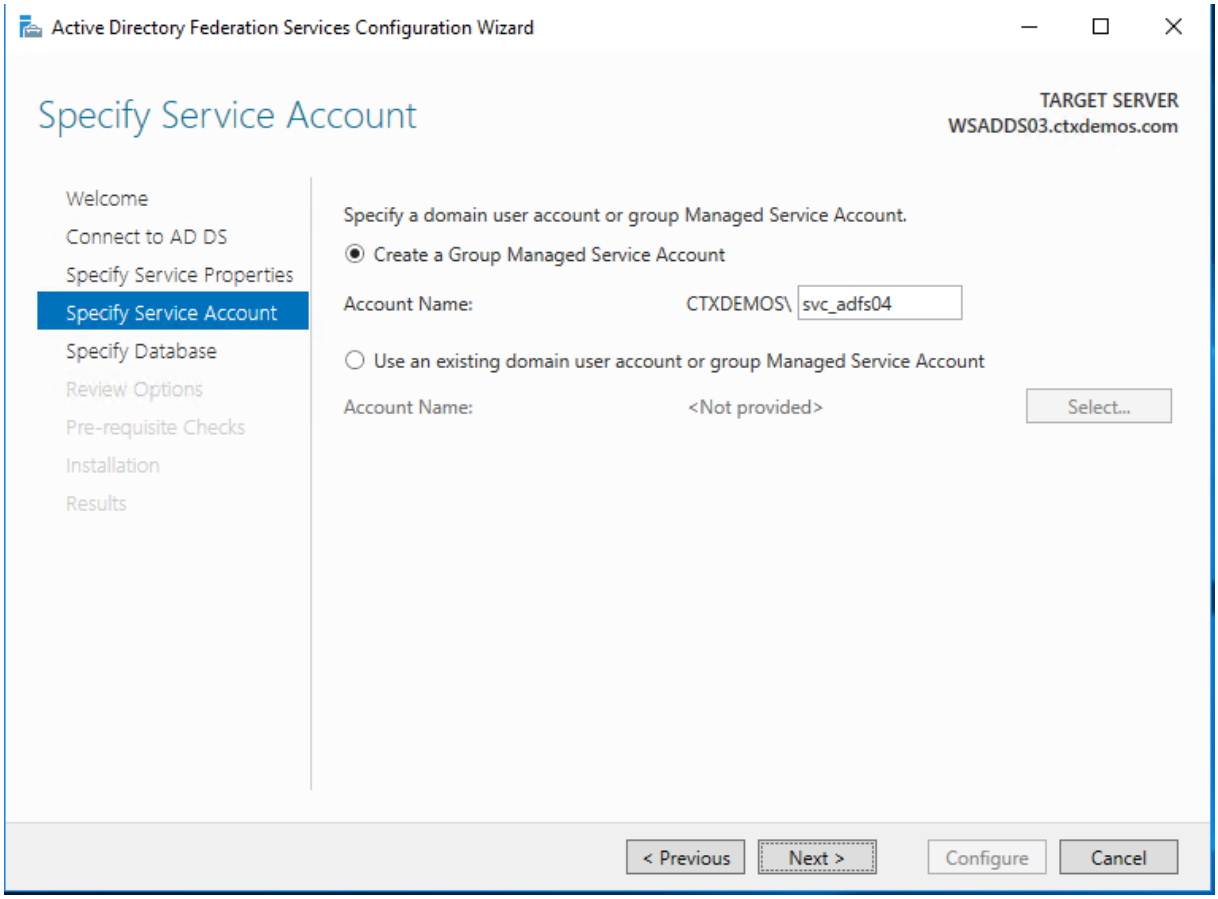


Dans la page **Spécifier les propriétés du service**, procédez comme suit, puis cliquez sur **Suivant** :

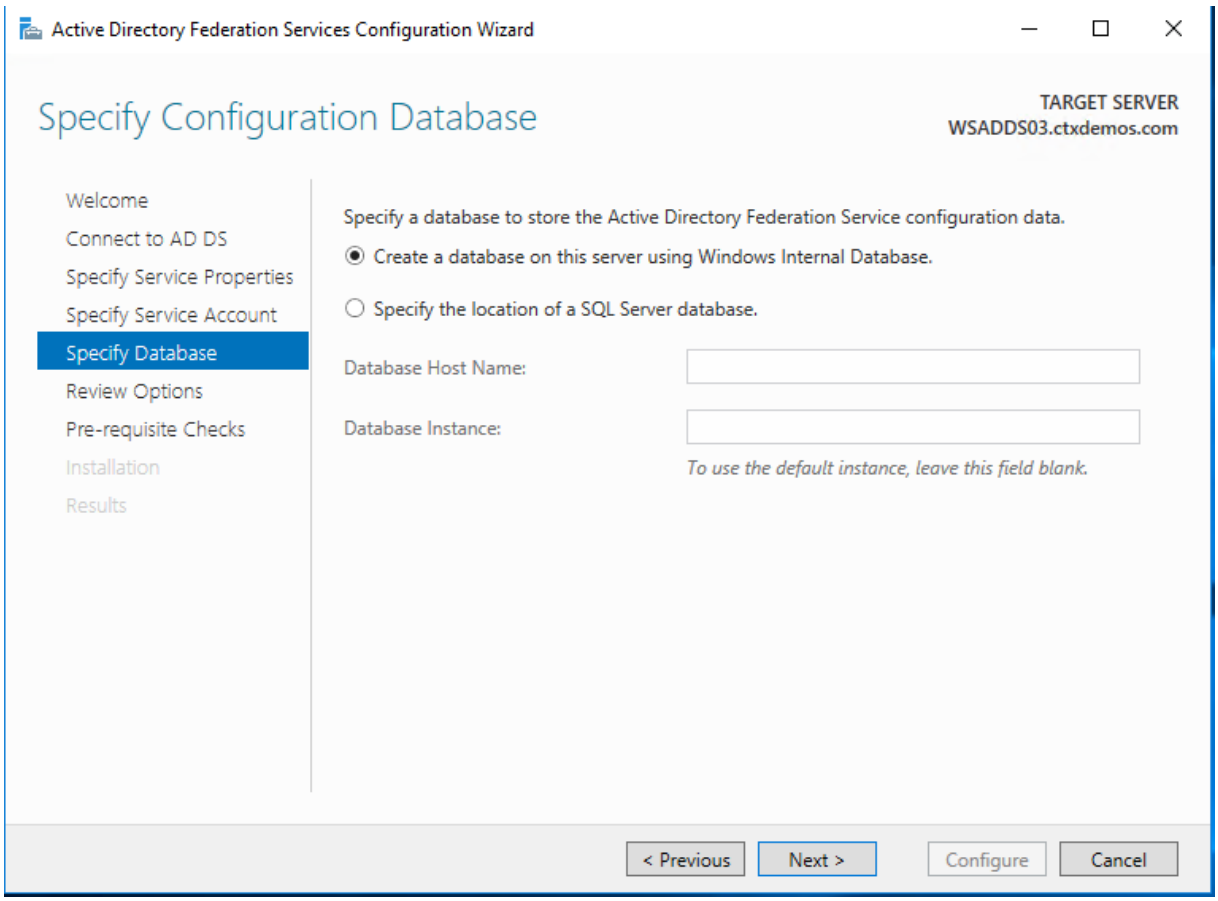
- Choisissez le certificat qui a été installé sur le serveur lors des étapes précédentes.
- Le nom du service de fédération est automatiquement renseigné en fonction du nom du sujet du certificat.
- Placez le nom complet du service de fédération. Par exemple, **CTXDEMOS STS**.



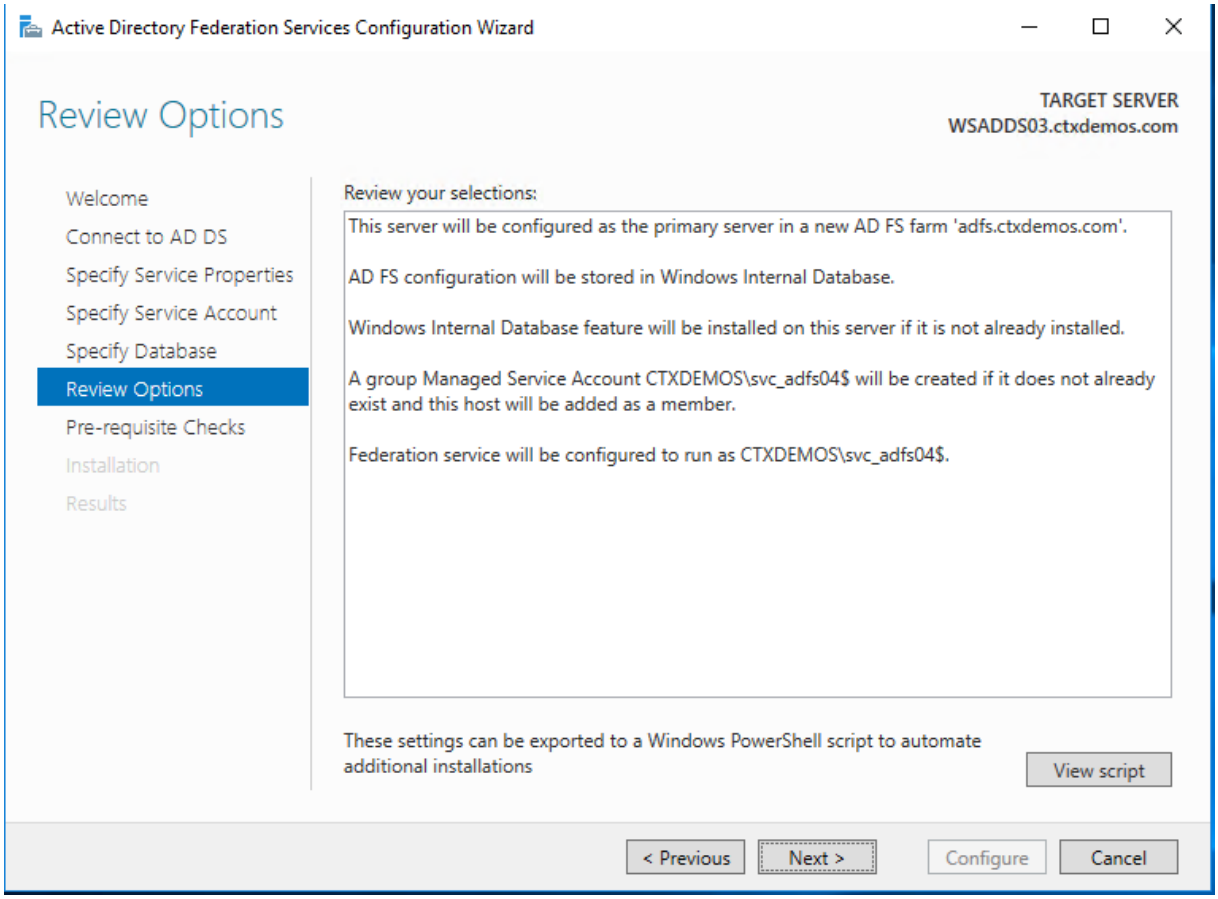
Dans la page **Spécifier un compte de service**, sélectionnez **Créer un compte de service géré par groupe** et entrez un nom unique pour ce compte. Les comptes de services gérés de groupe sont pris en charge dans Windows Server 2012 et sont livrés avec des mots de passe stricts et complexes qui sont modifiés automatiquement tous les 30 jours. Cliquez sur **Next**.



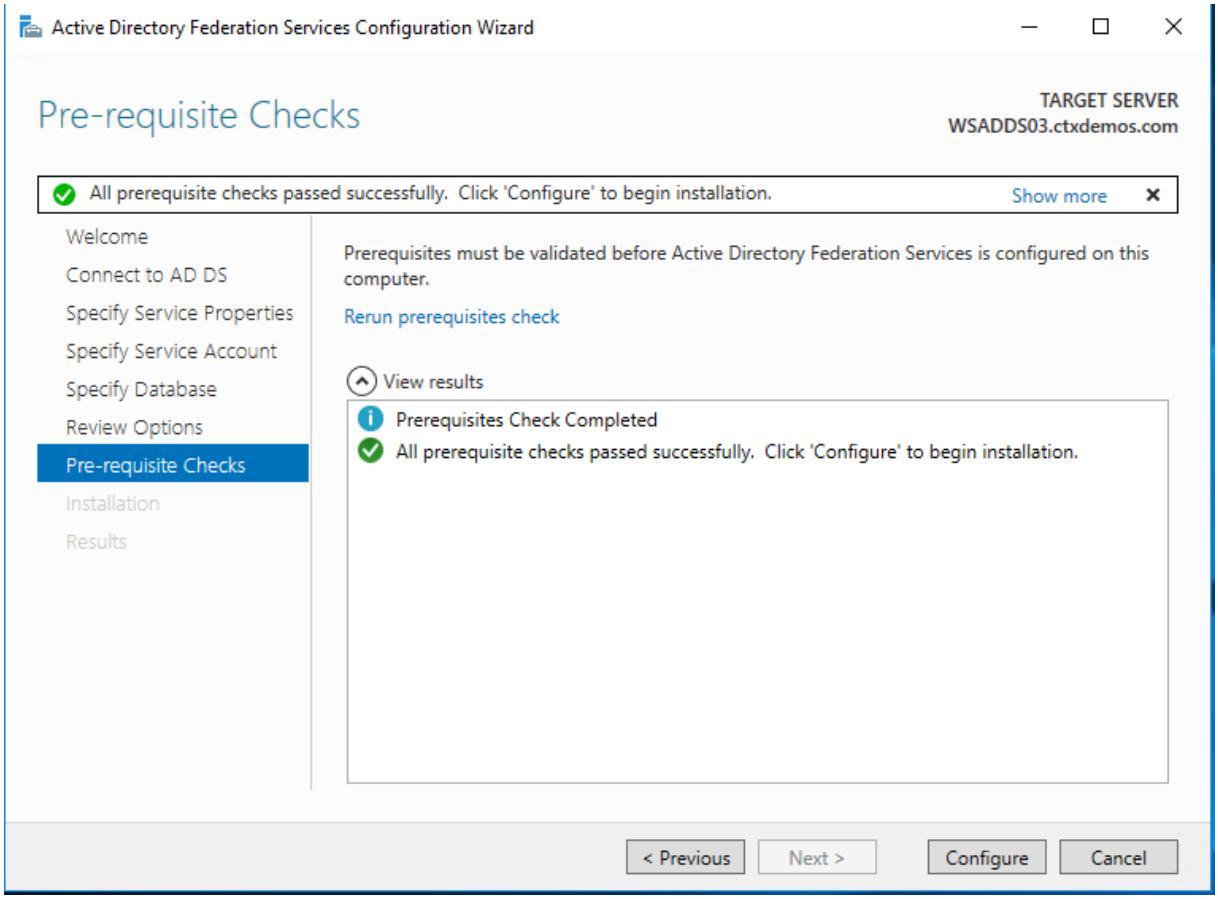
Dans la page **Spécifier la base de données de configuration**, sélectionnez spécifier l'emplacement d'une base de données SQL Server. Cliquez sur **Next**.



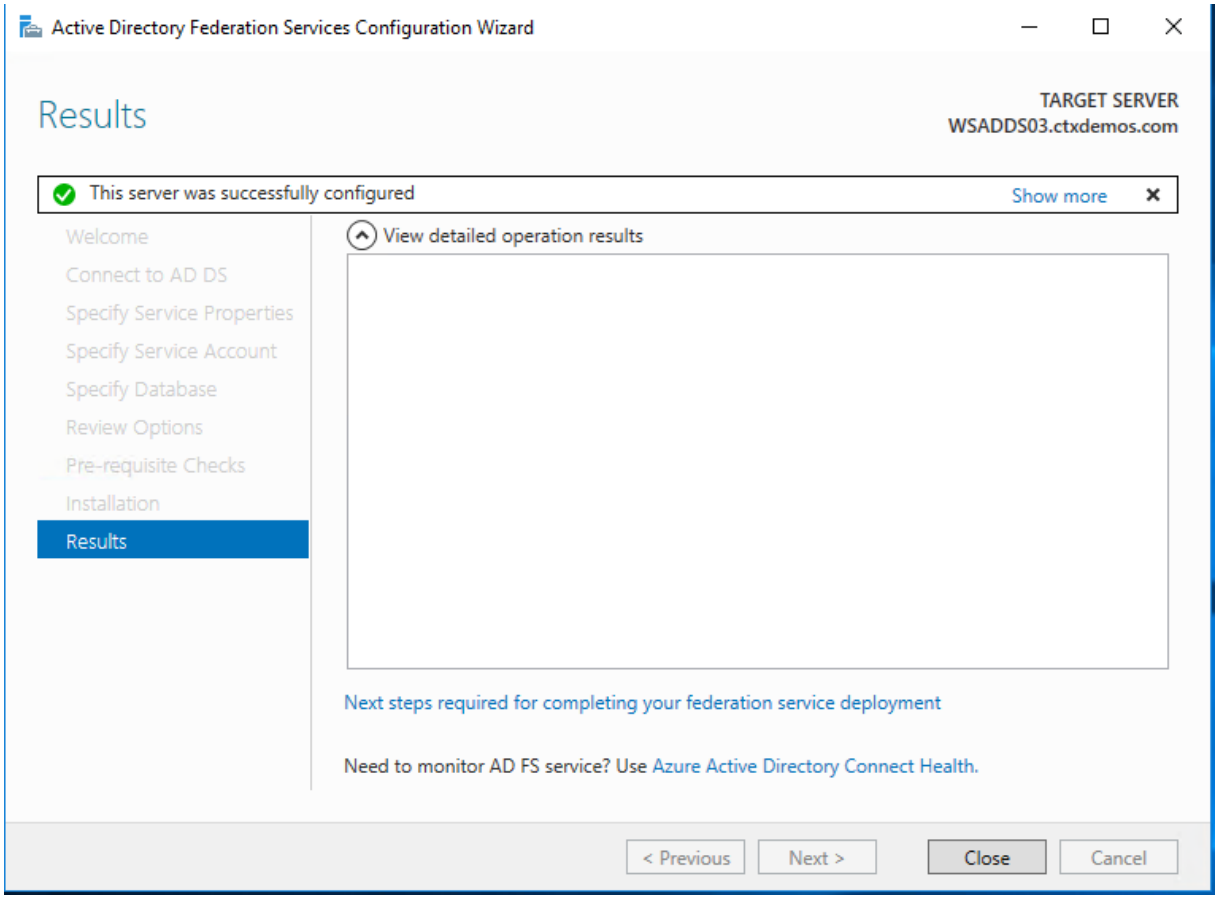
Dans la page **Options de révision**, vérifiez vos sélections de configuration, puis cliquez sur **Suivant**.



Dans la page **Vérifications préalables**, vérifiez que toutes les vérifications préalables sont terminées avec succès, puis cliquez sur **Configurer**.



Sur la page **Résultats**, vérifiez que l'installation est réussie. Cliquez sur **Fermer** pour quitter l'Assistant.



> **Remarque :**
>
> pour effectuer les étapes suivantes, vous aurez besoin de votre ID de locataire Azure.
>
> Vous pouvez obtenir l'ID de locataire Azure en suivant les étapes décrites dans l'article Get AzureID Tenant Detail de la documentation Microsoft.
>
> La documentation Microsoft fournit également des informations sur le GUID client Azure MFA dans Configurer les serveurs AD FS 2016 et Azure MFA.

Configurer la batterie de serveurs AD FS - automatisée

Vous pouvez exécuter le script PowerShell suivant :

```
#
# Windows PowerShell script for AD FS Deployment
#
Import-Module ADFS
Install-AdfsFarm `
-CertificateThumbprint:"BD02F30D90A96EEE4A5934F2EA979E7A052584AE" `
-FederationServiceDisplayName:"CTXDEMOS STS" `
-FederationServiceName:"adfs.ctxdemos.com" `
```



```
-GroupServiceAccountIdentifier:"C
<!--NeedCopy-->
```

Configurer AD FS avec Azure MFA

Configurer les serveurs AD FS

Sur chacun de vos serveurs AD FS, lancez PowerShell et exécutez les commandes suivantes :

```
# Install Windows PowerShell MSOnline Module
Install-Module MSOnline

# Import Windows PowerShell MSOnline Module
Import-Module MSOnline

# Get the Azure Global Administrator credential
$credential = Get-Credential

# Sign in to your Azure Active Directory environment
Connect-MsolService -Credential $credential

# Set a variable for the Azure Tenant name
$azureTenantID = "ctxdemos.onmicrosoft.com"

# Set a variable for the Azure MFA Client GUID
$azureMFAClientGUID = "981f26a1-7f43-403b-a875-f8b09b8cd720"

# Generate a certificate for the Azure MFA on AD FS server
$azureMFACertificate = New-AdfsAzureMfaTenantCertificate -TenantId
   $azureTenantID

# Add the new credentials to the Azure MFA Client Service Principal
New-MsolServicePrincipalCredential -AppPrincipalId $azureMFAClientGUID
   -Type asymmetric -Usage verify -
Value $azureMFACertificate
<!--NeedCopy-->
```

Configurer la batterie de serveurs AD FS

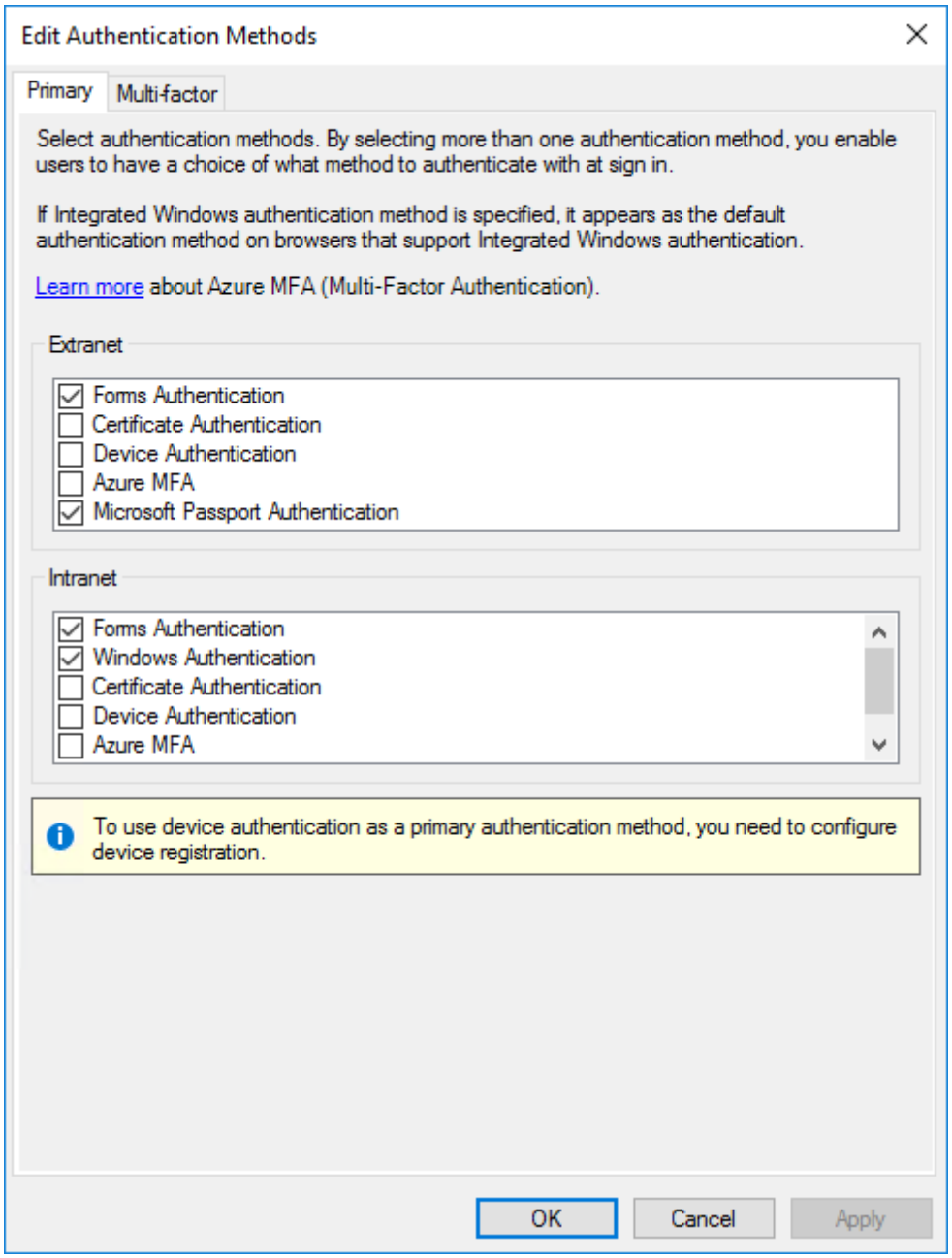
Uniquement sur l'un des serveurs AD FS, exécutez la commande suivante :

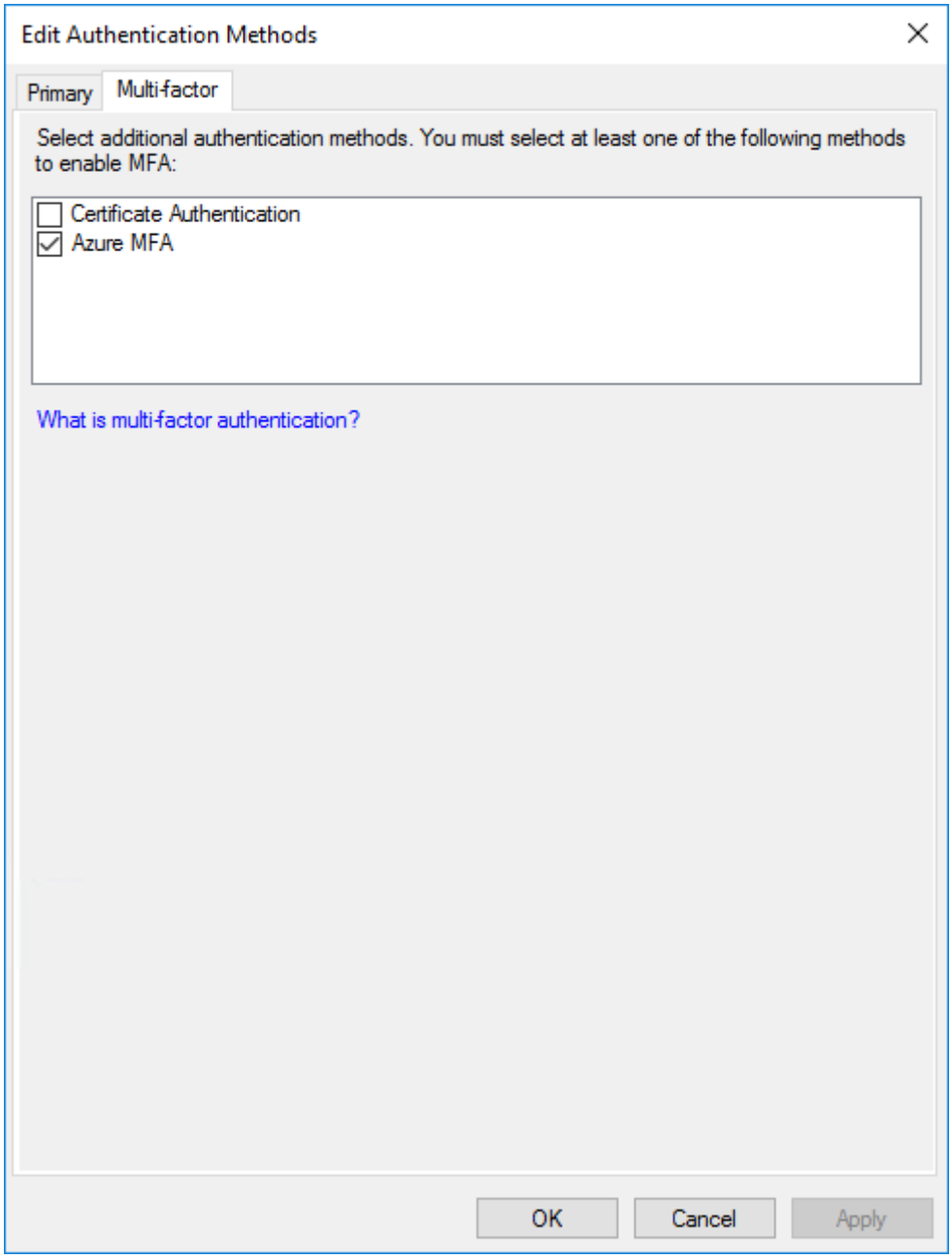
```
Set-AdfsAzureMfaTenant -TenantId $azureTenantID -ClientId
   $azureMFAClientGUID
```



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

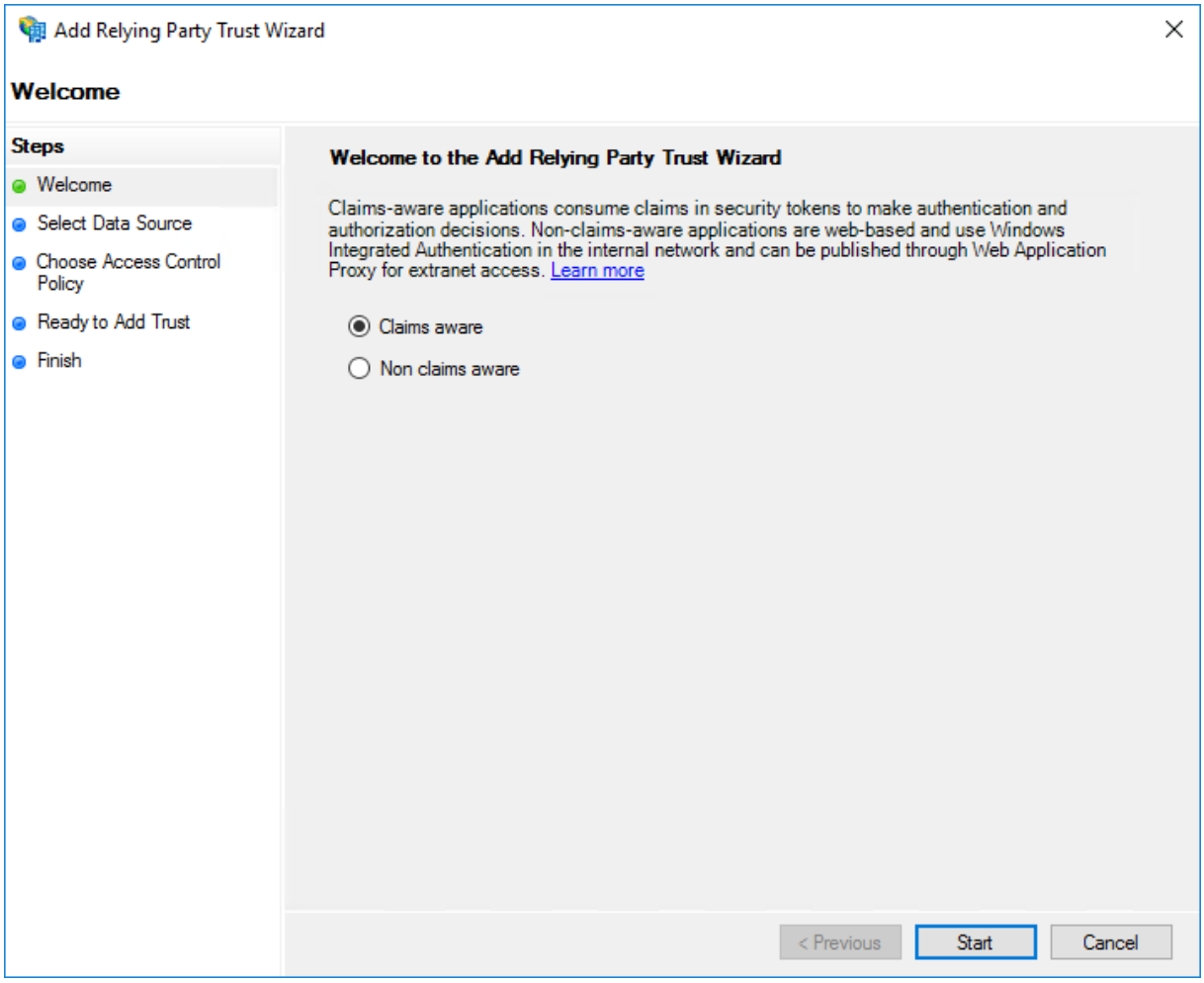
Redémarrez le service AD FS sur chacun de vos serveurs. Ensuite, vous verrez que Azure MFA est disponible en tant que méthode d'authentification principale et multifacteur pour l'utilisation de l'intranet et de l'extranet.



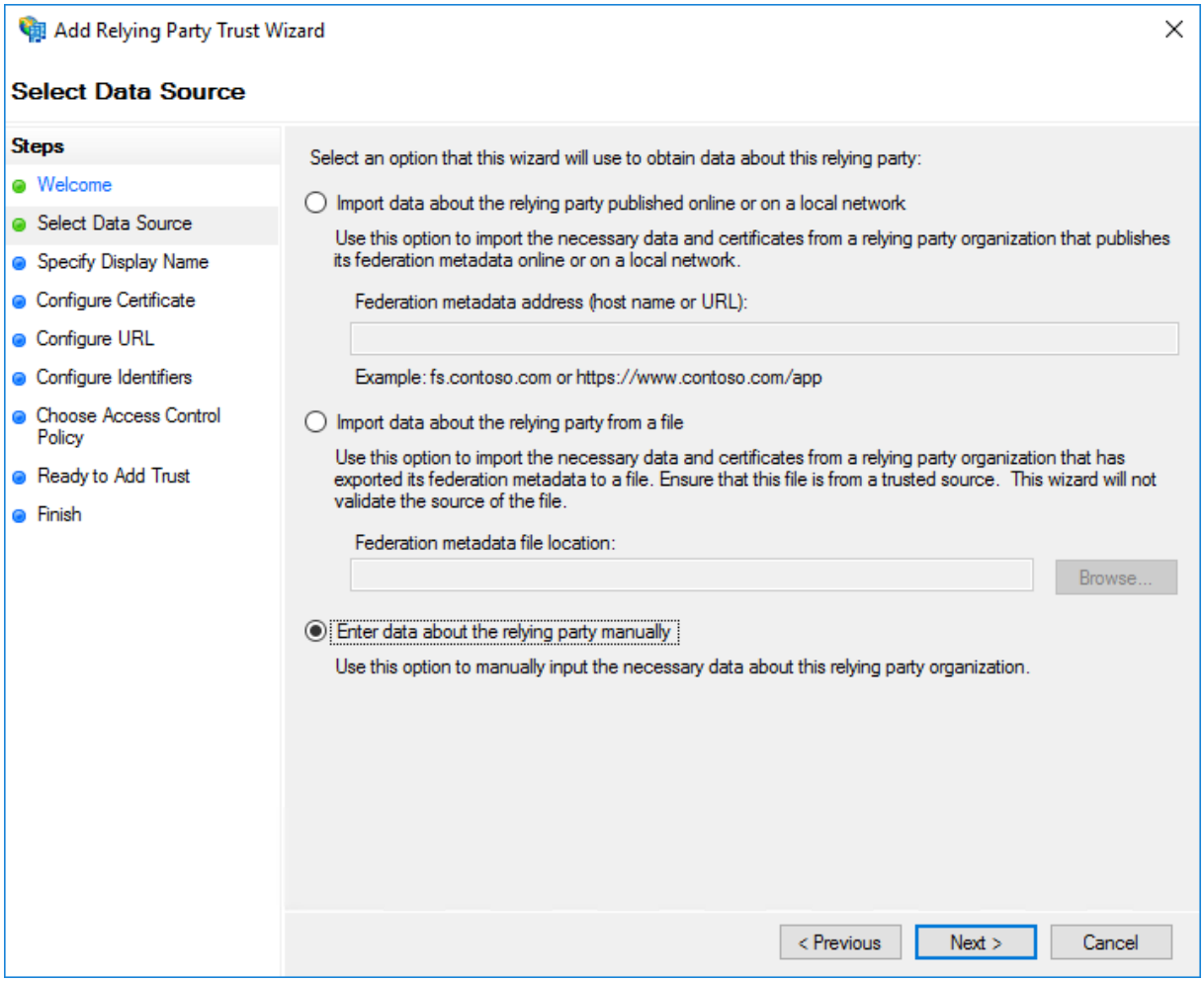


Configurer AD FS avec Citrix ADC

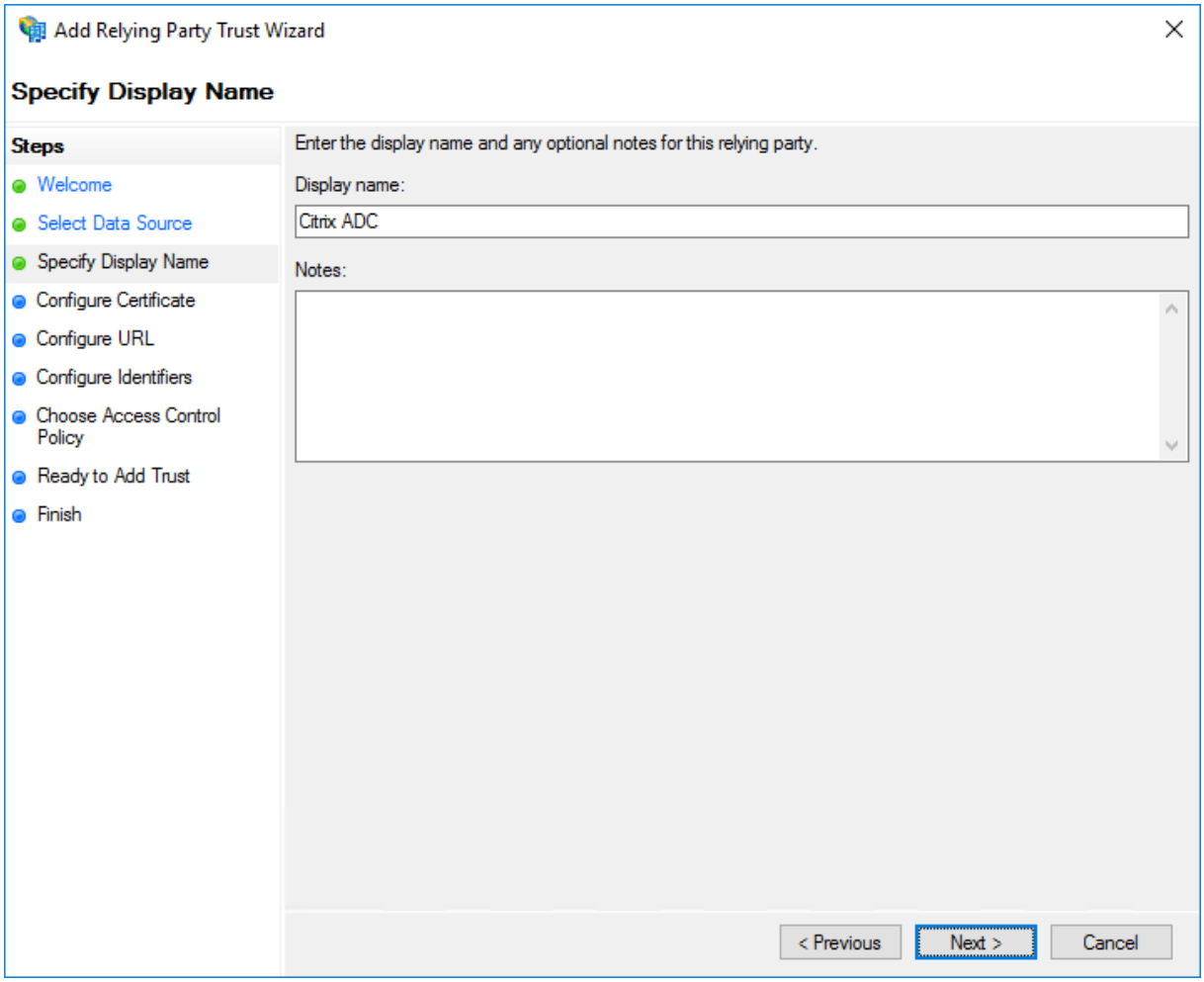
Vous devez créer une approbation de fédération entre AD FS et Citrix ADC. Dans la console de gestion AD FS, accédez à **Approuver de partie de confiance** et sélectionnez **Ajouter une approbation de partie de confiance**.



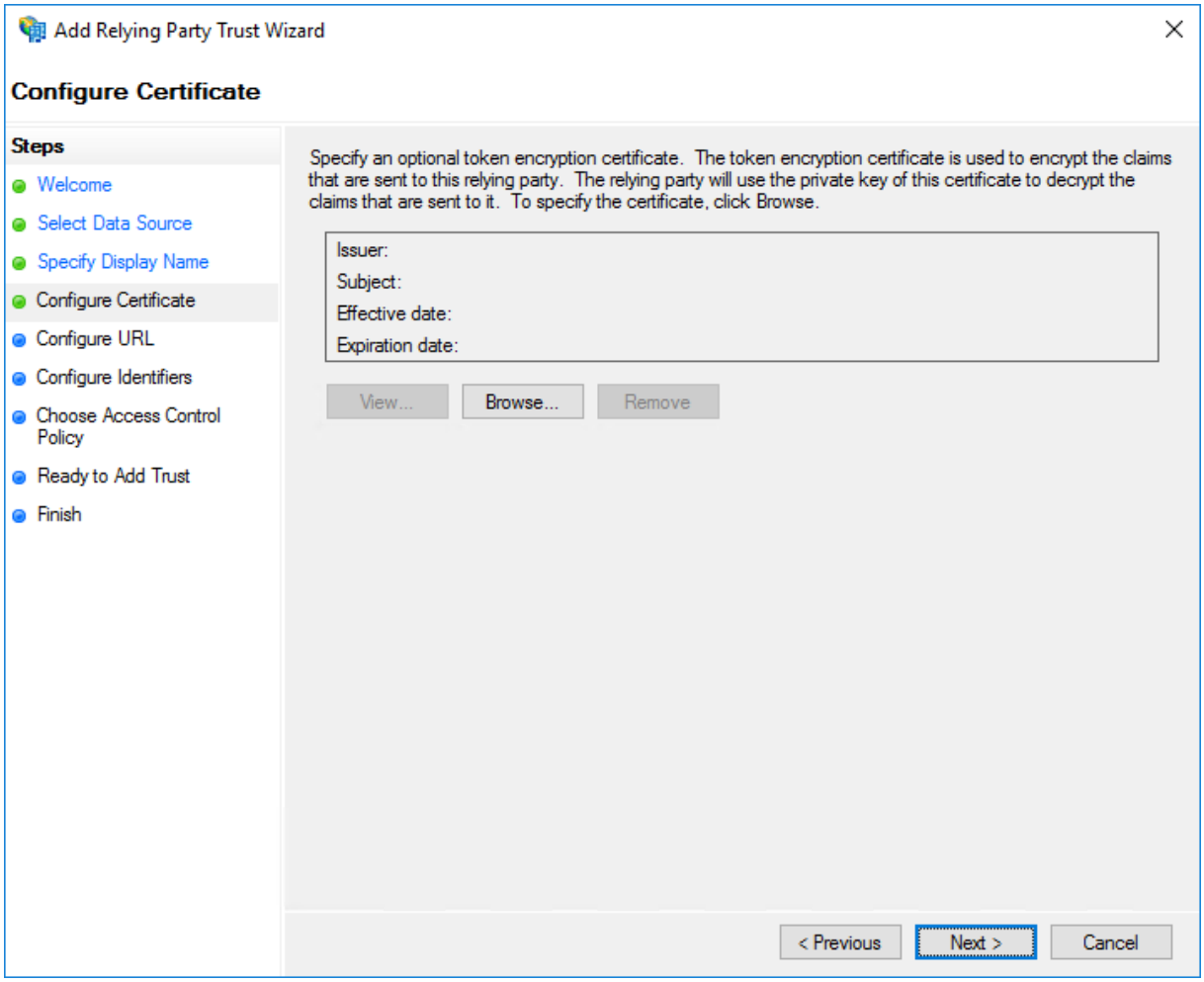
Sélectionnez **Entrer manuellement les données relatives à la partie de confiance**, puis cliquez sur **Suivant**.



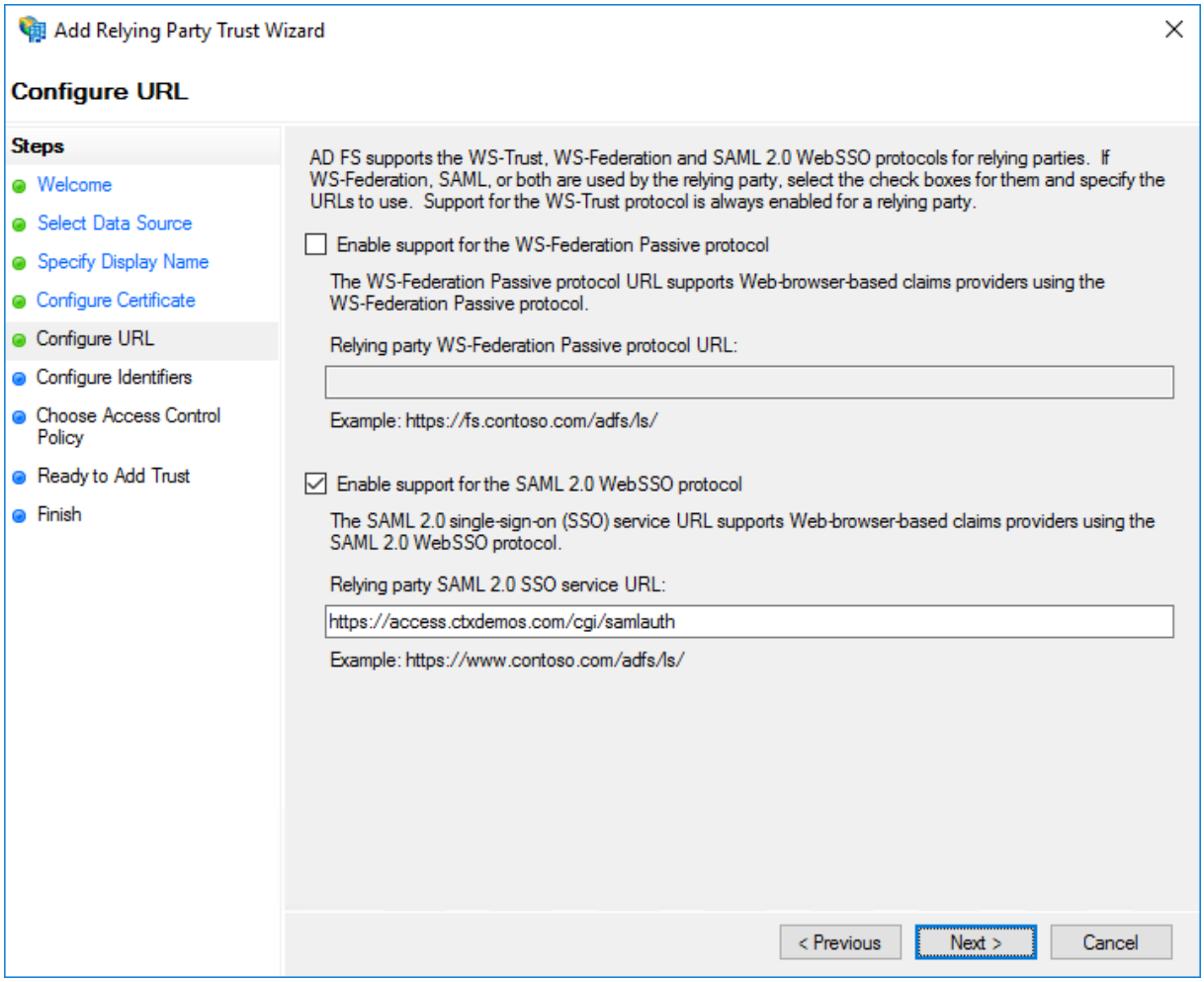
Entrez un nom d'affichage descriptif et des notes facultatives. Cliquez sur **Next**.



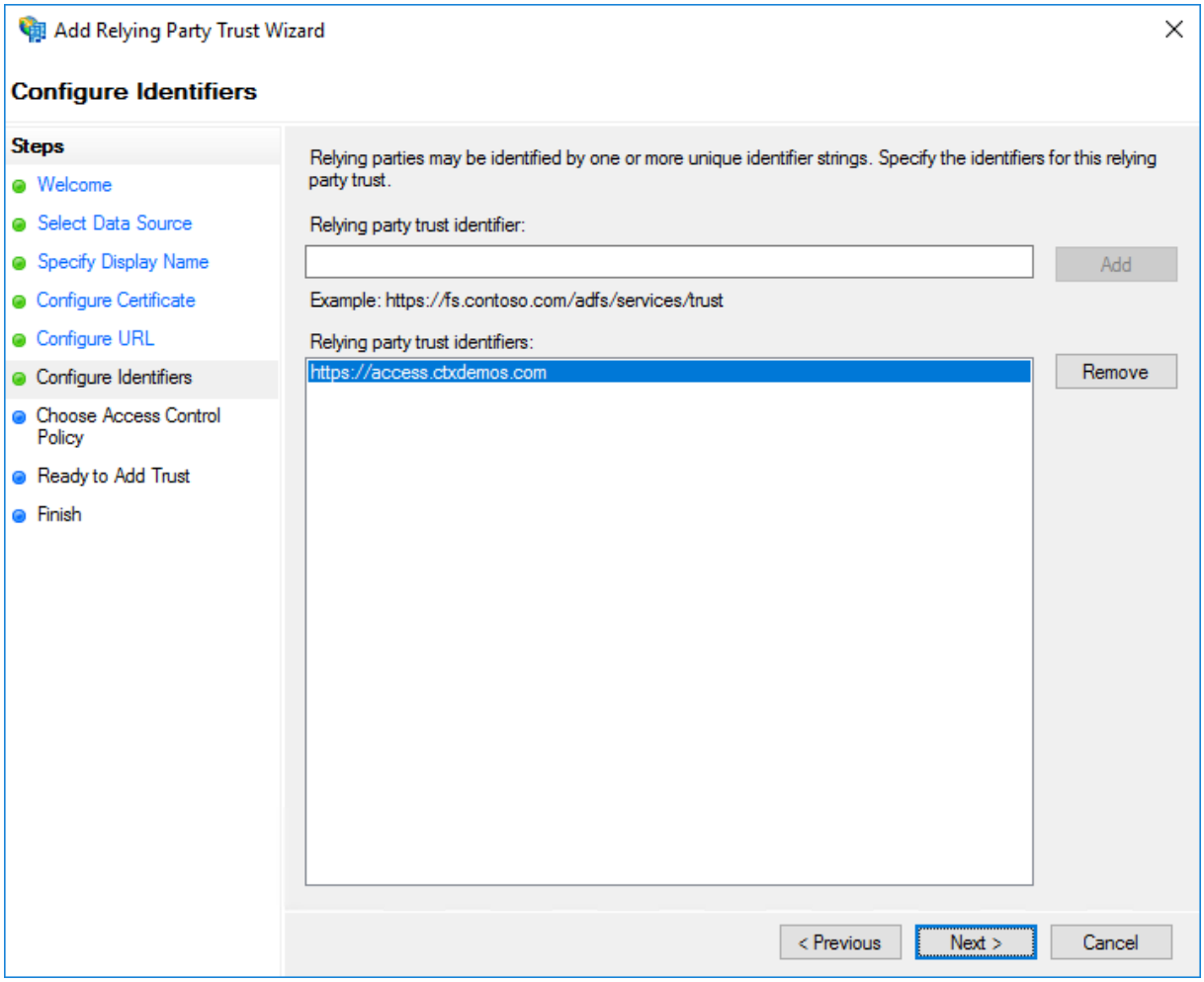
Cliquez sur **Next**.



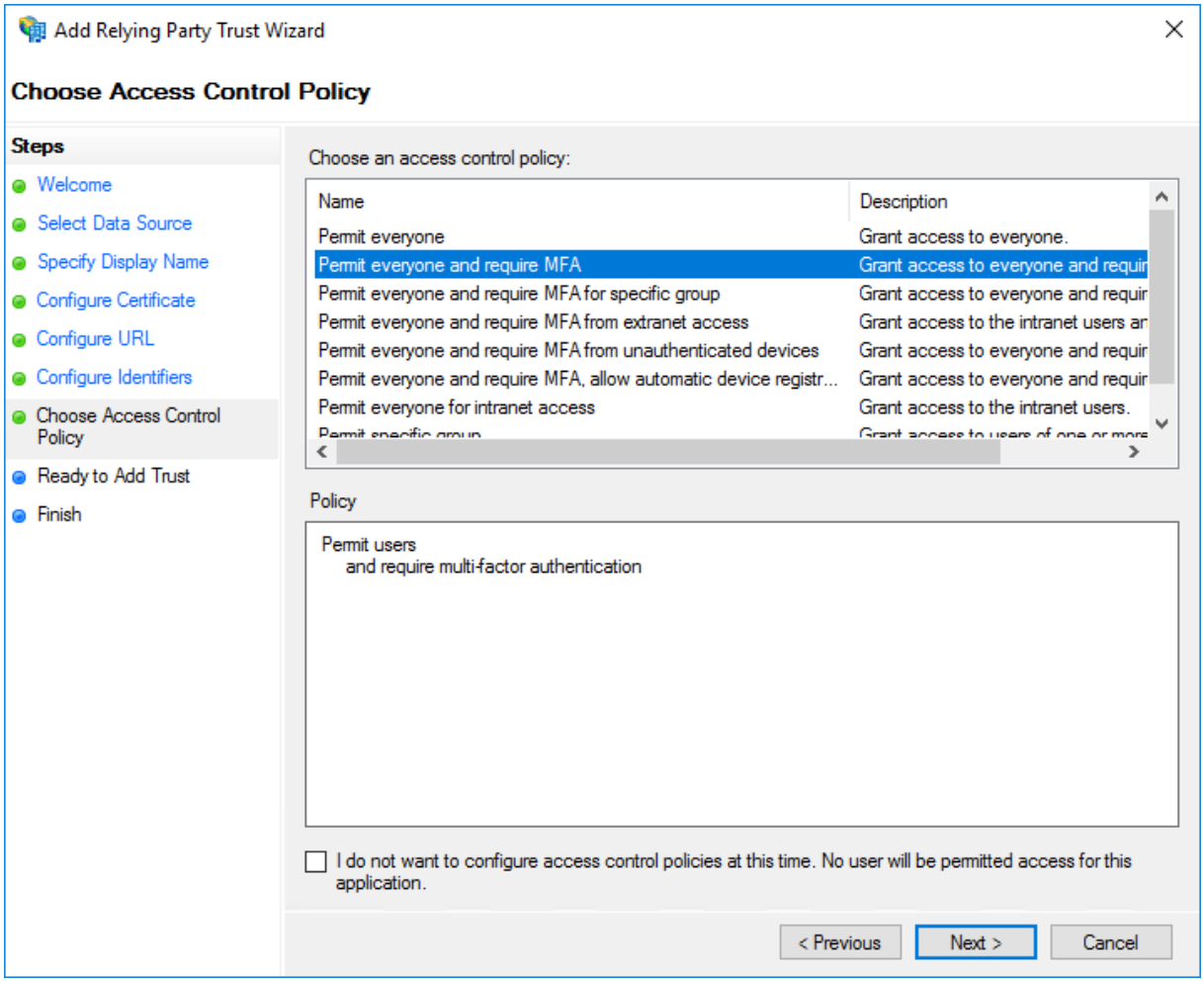
Sélectionnez **Activer la prise en charge du protocole SAML 2.0 WebSSO** et entrez `https://CitrixGatewayFQDN/cgi/samlauth`. Dans l'environnement de démonstration, l'adresse est `https://access.ctxdemos.com/cgi/samlauth`. Cliquez sur **Next**.



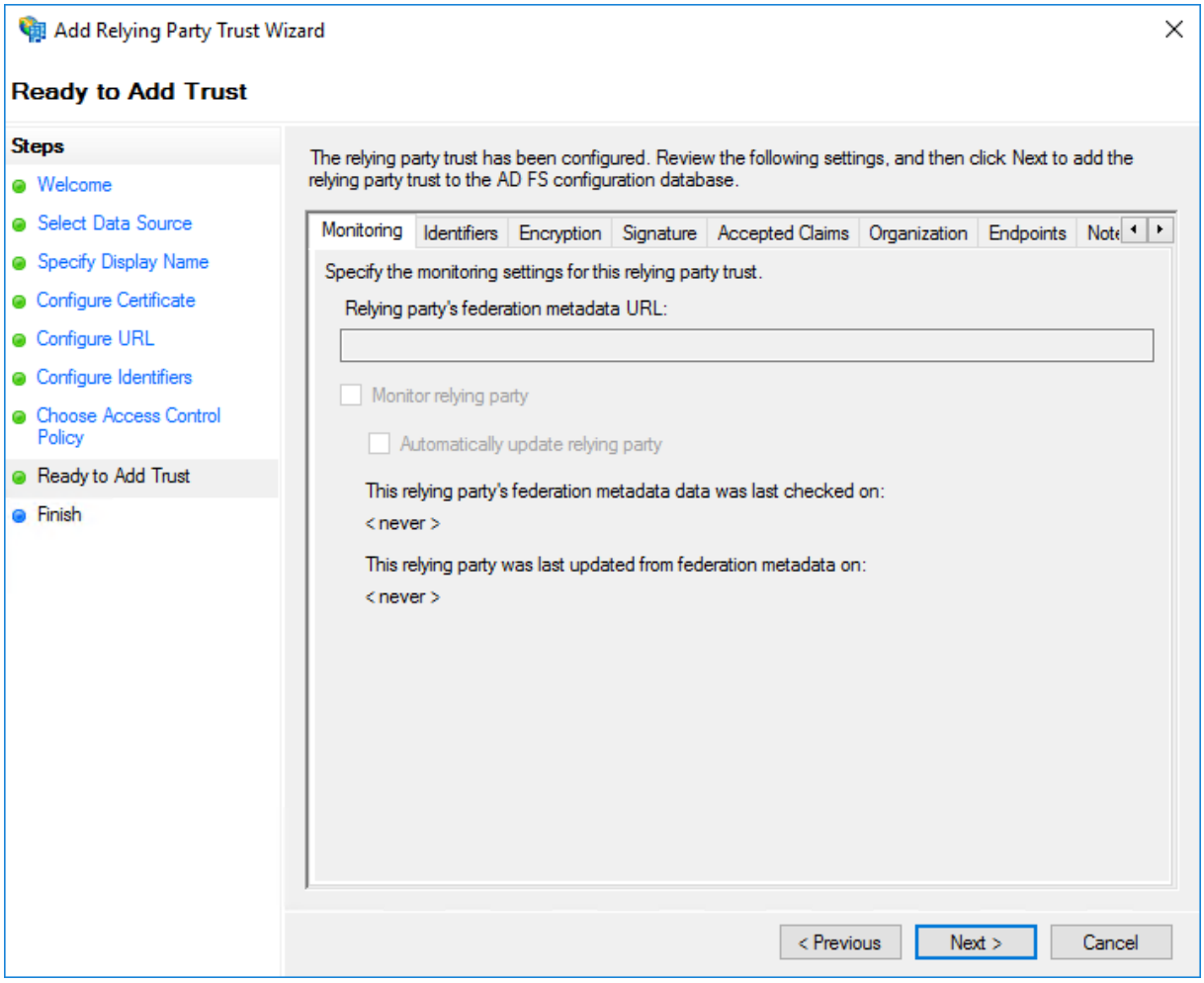
Entrez une chaîne d'identificateur unique pour l'approbation de partie de confiance. Dans l'environnement de démonstration, l'adresse est `https://access.ctxdemos.com`. Cet identificateur sera utilisé comme URL d'émetteur dans le profil SAML Citrix ADC. Cliquez sur **Next**.



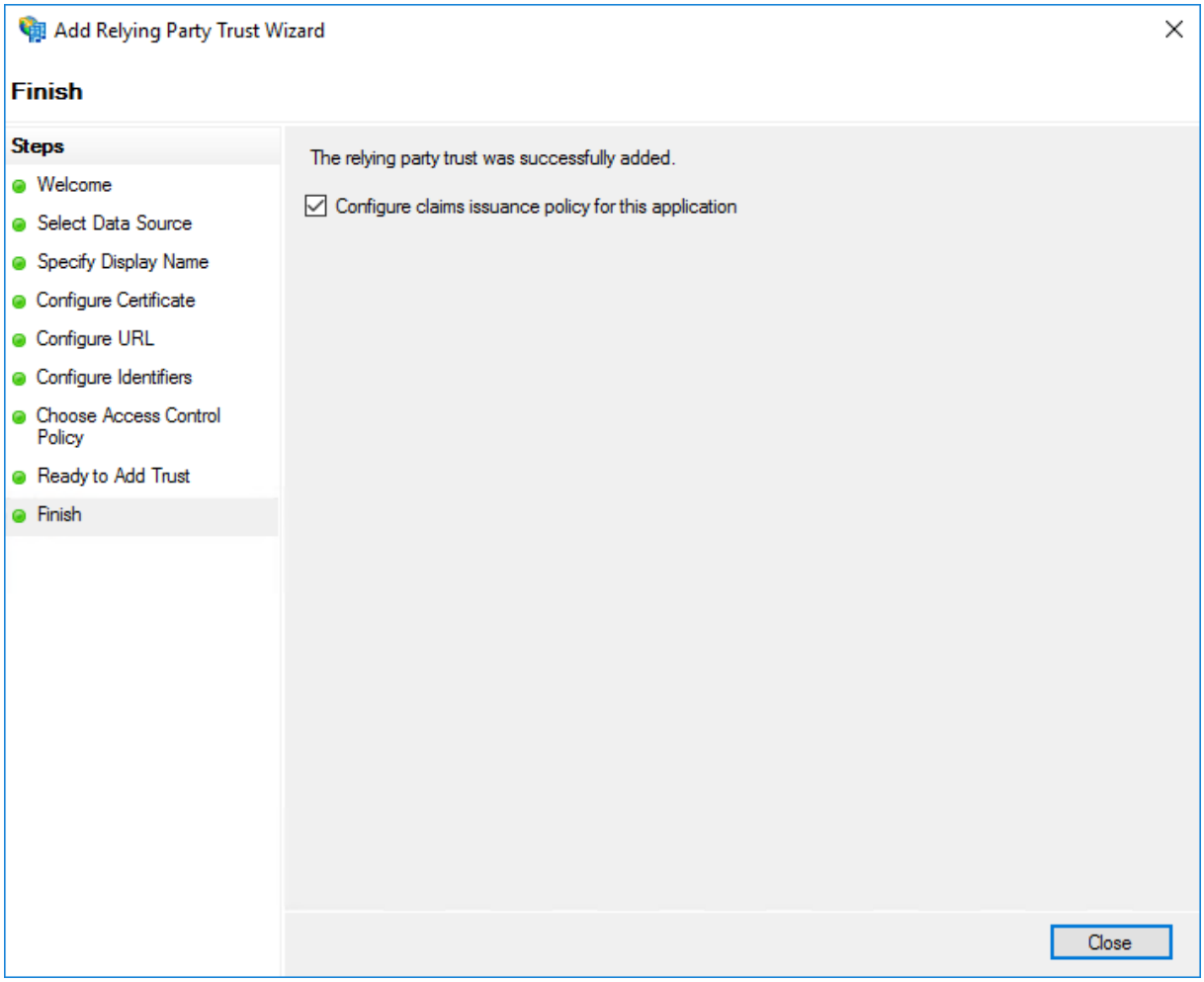
Sur la page **Choisir une stratégie de contrôle d'accès** , sélectionnez **Autoriser tout le monde et exiger MFA**. Cliquez sur **Next**.



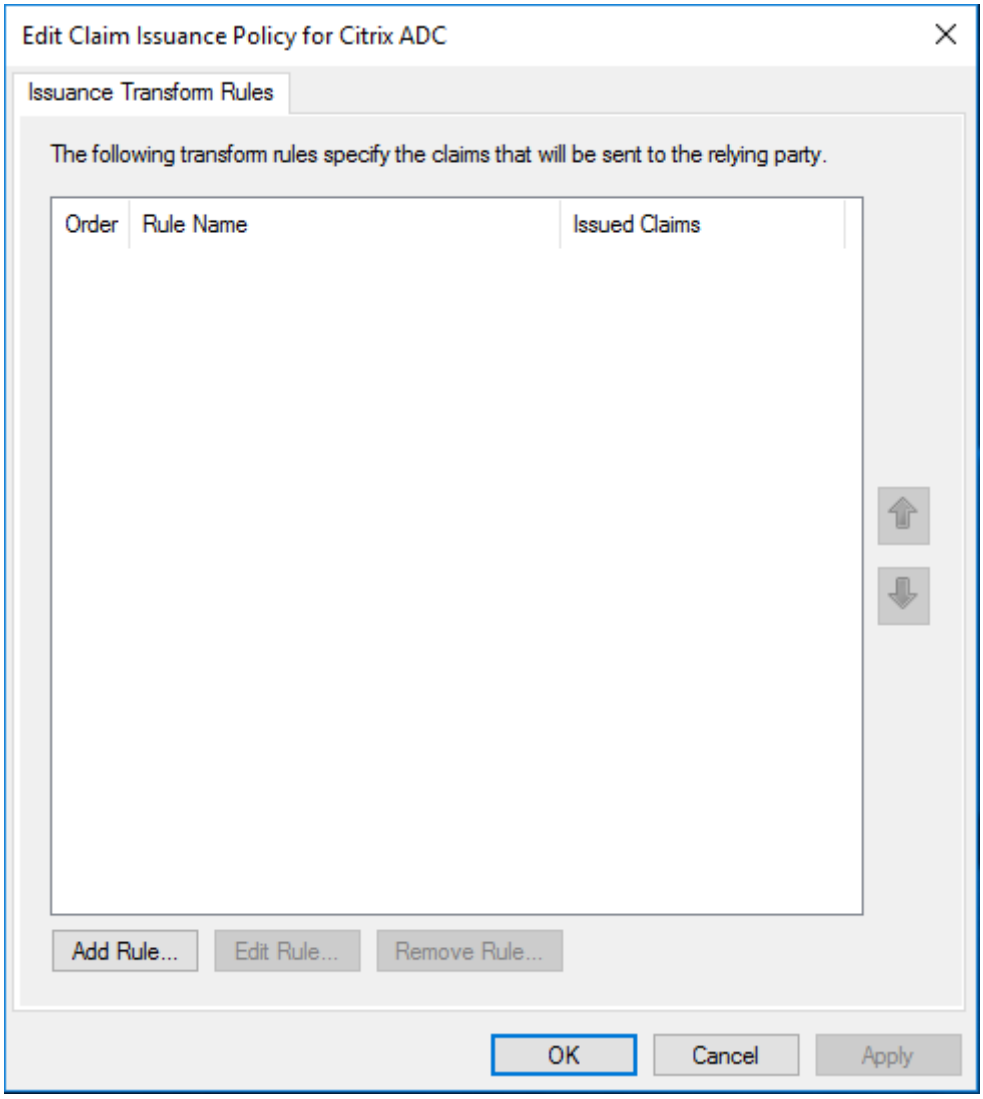
Cliquez sur **Next**.



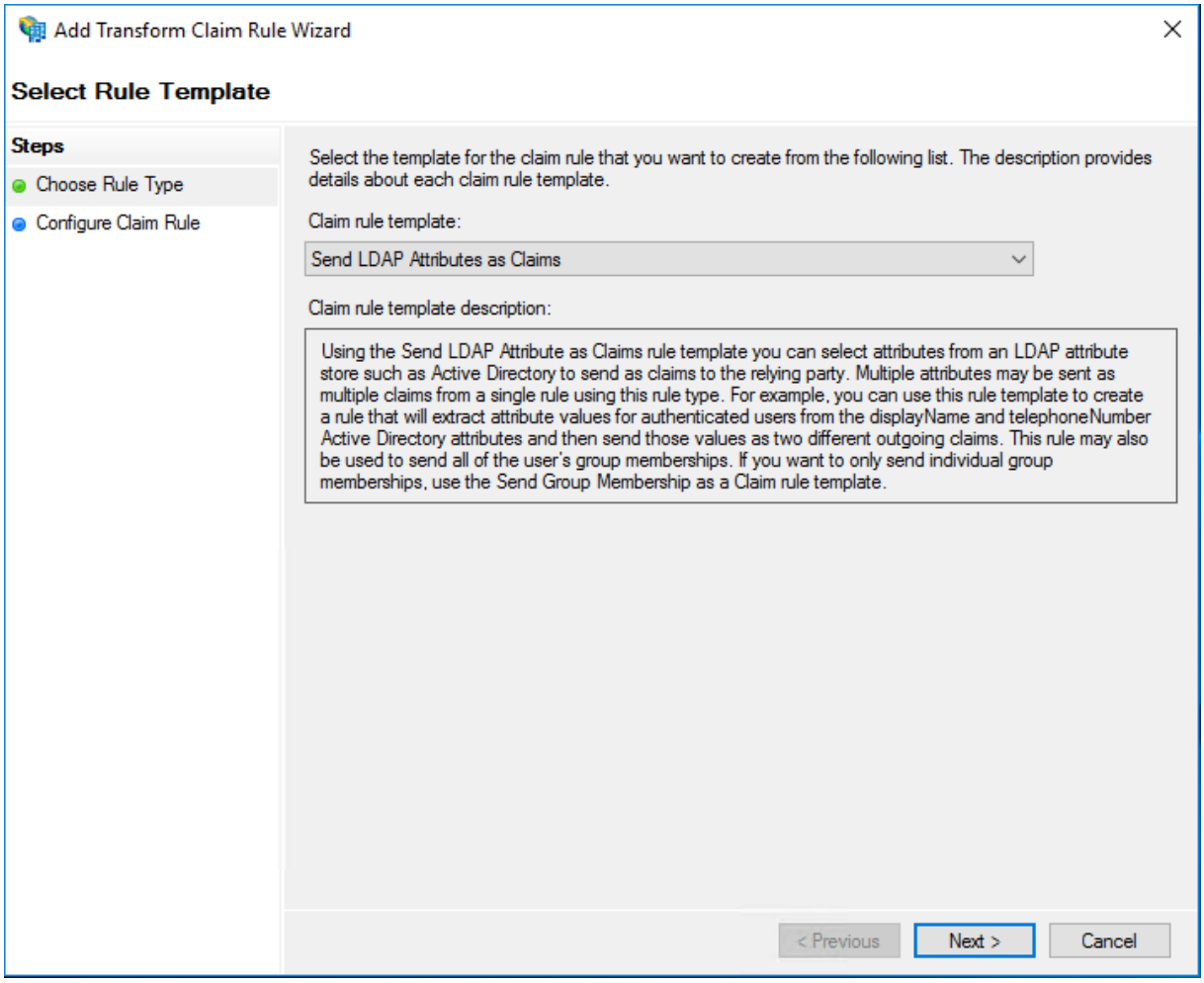
Sur la page **Fin**, sélectionnez **Configurer la stratégie d'émission de revendications pour cette application** . Cliquez sur **Fermer**.



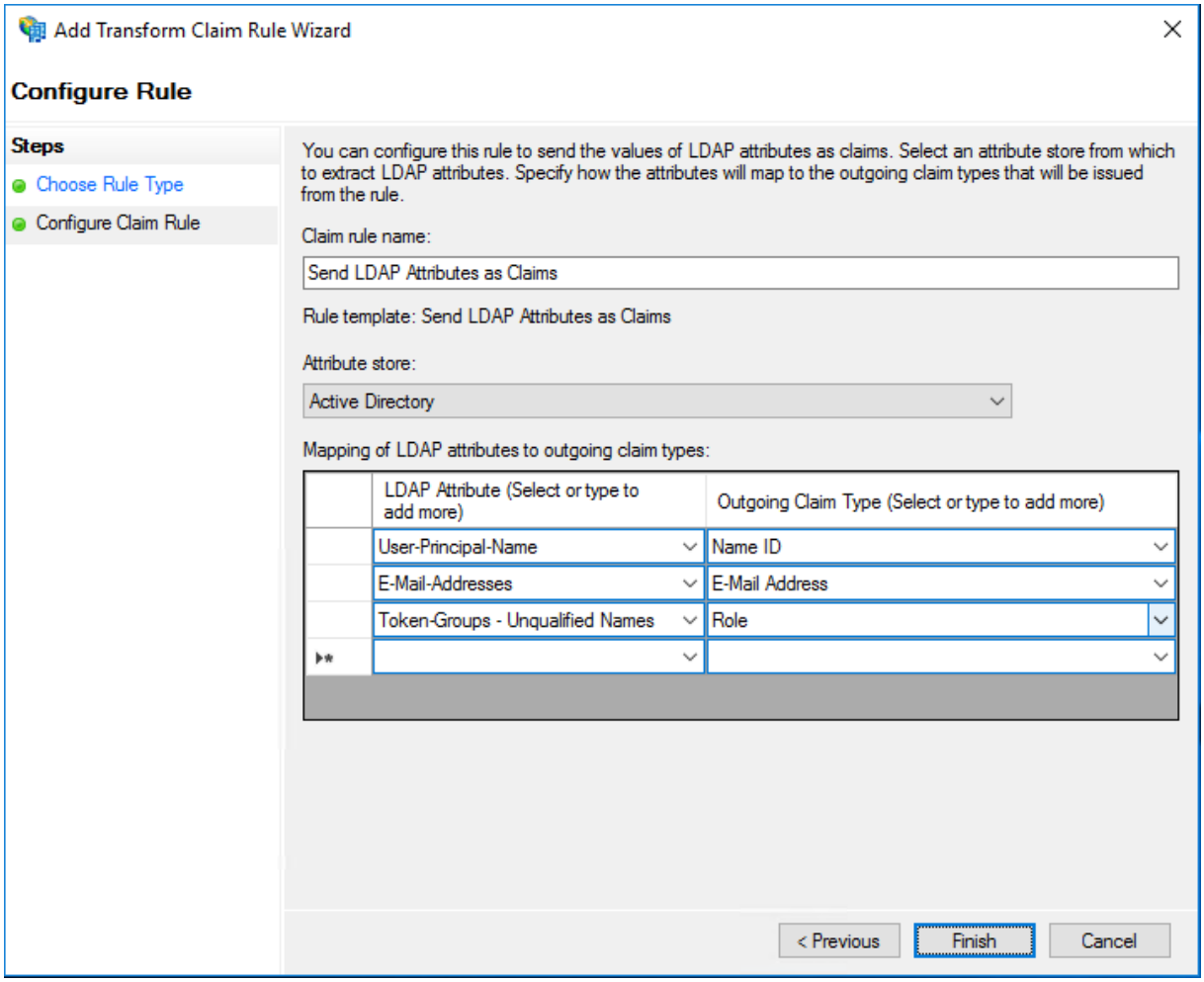
Dans la page **Règles de transformation d'émission**, cliquez sur **Ajouter une règle**.



Cliquez sur **Next**.

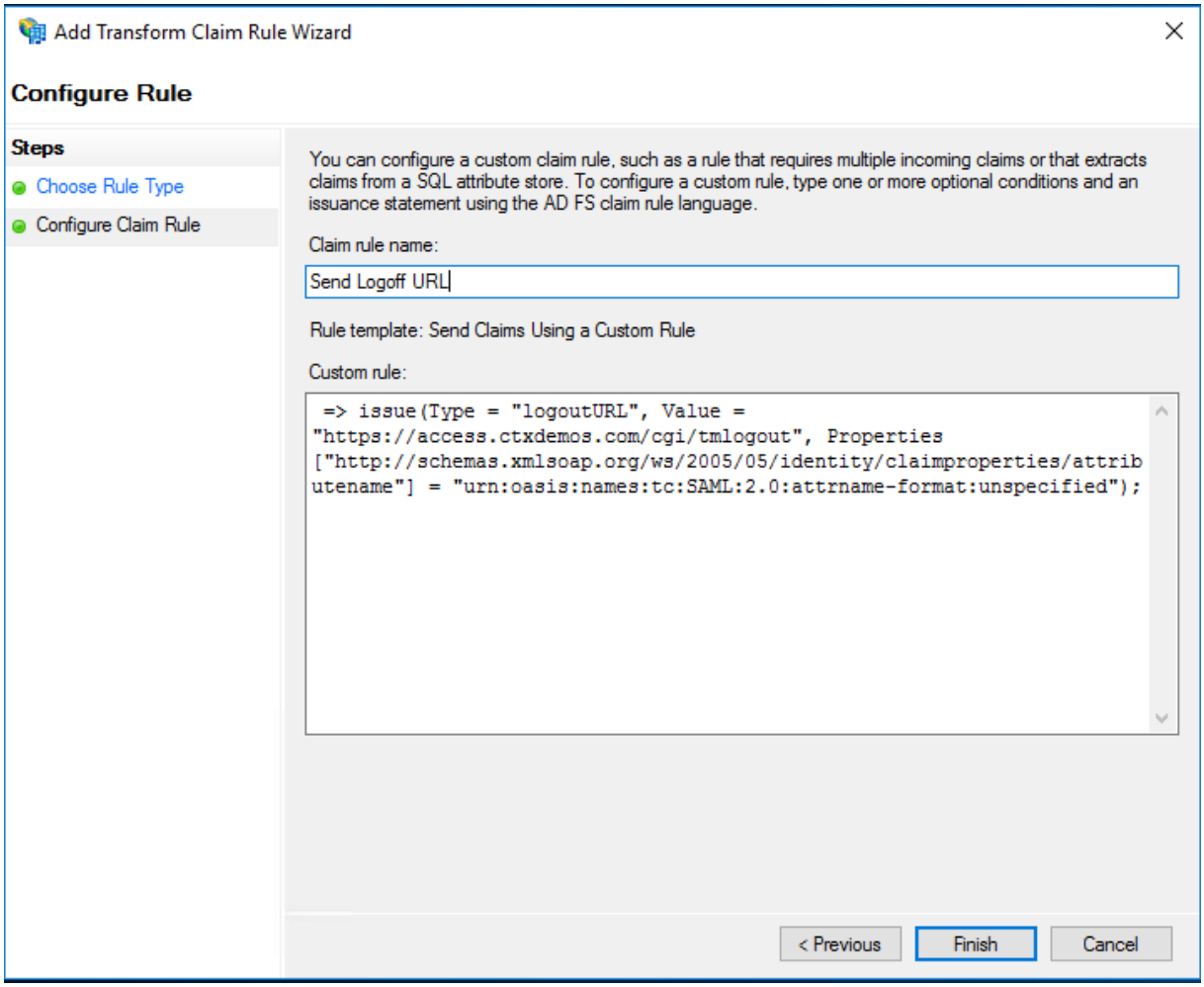


Entrez un nom descriptif dans le champ **Nom de la règle de réclamation**. Sous **Magasin d'attributs**, sélectionnez **Active Directory**. Sélectionnez ensuite les éléments suivants : **Attributs LDAP** et **Types de revendications sortantes**.



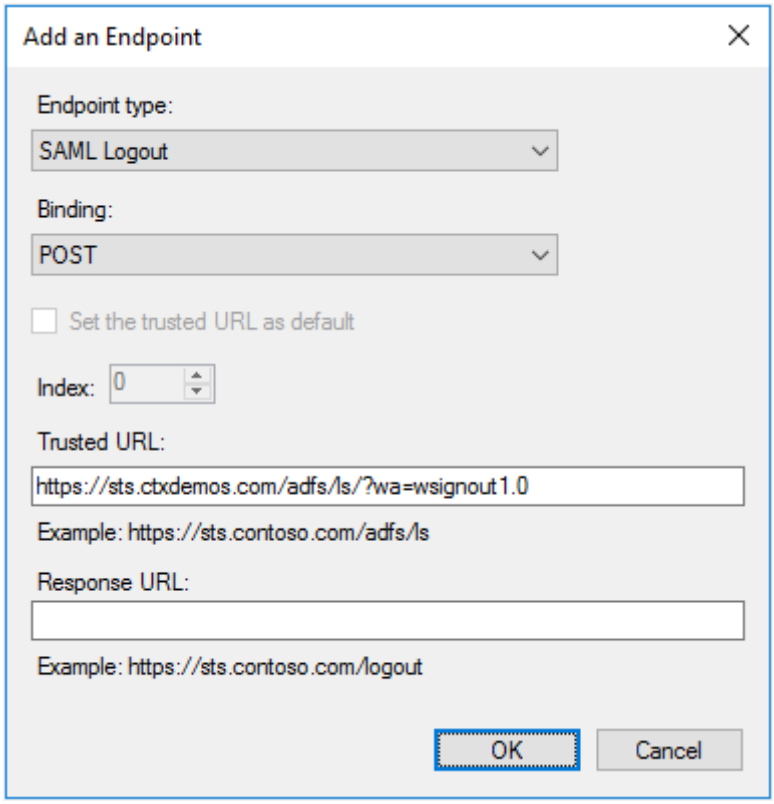
Créez une nouvelle règle et utilisez **Envoyer des réclamations à l'aide d'une règle personnalisée** comme **modèle de règle de réclamation**. Entrez un nom descriptif pour le nom de la **règle de revendication** et entrez la chaîne suivante pour la **règle personnalisée** :

```
1 => issue(Type = "logoutURL", Value = "https://access.ctxdemos.com/cgi/
    tmlogout", Properties["http://schemas.xmlsoap.org/ws/2005/05/
    identity/claimproperties/attributename"] = "urn:oasis:names:tc:SAML
    :2.0:attrname-format:unspecified");
2 <!--NeedCopy-->
```

Lorsque les stratégies d'émission de réclamations sont créées, cliquez sur **OK**.

Cliquez avec le bouton droit sur **Appropriation de partie de confiance > Citrix ADC**, puis sélectionnez **Propriétés**. Sélectionnez **Endpoints** et ajoutez un point de terminaison en cliquant sur **Ajouter SAML pour la déconnexion**. Dans la liste **Type de point de terminaison**, sélectionnez **Déconnexion SAML**. Pour **Liaison**, sélectionnez **POST** et pour **URL de confiance**, entrez `https://sts.ctxdemos.com/adfs/ls/?wa=wsignout1.0`. Cela agira comme une URL de déconnexion lors de la déconnexion de Citrix ADC. Cliquez sur **OK**.



Cliquez avec le bouton droit sur **Appropriation de partie de confiance > Citrix ADC**, puis sélectionnez **Propriétés**. Sélectionnez **Encryption** et ajoutez un certificat SSL public installé sur Citrix Gateway. Ce certificat sera utilisé pour déchiffrer une demande SML entrante à partir de Citrix ADC. Répétez la même chose sur l'onglet **Signature**. Ce certificat sera utilisé pour vérifier la signature d'une demande SAML entrante. Cliquez sur **OK**.

Activer la page de connexion initiée par l'IdP

Vous pouvez activer la page d'authentification initiée par l'IdP AD FS. Vous utiliserez l'authentification initiée par IdP pour présenter une page d'erreur personnalisée aux utilisateurs MFA non enregistrés. Pour l'activer, exécutez la commande suivante :

```
1 Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
2 <!--NeedCopy-->
```

Tester la batterie AD FS

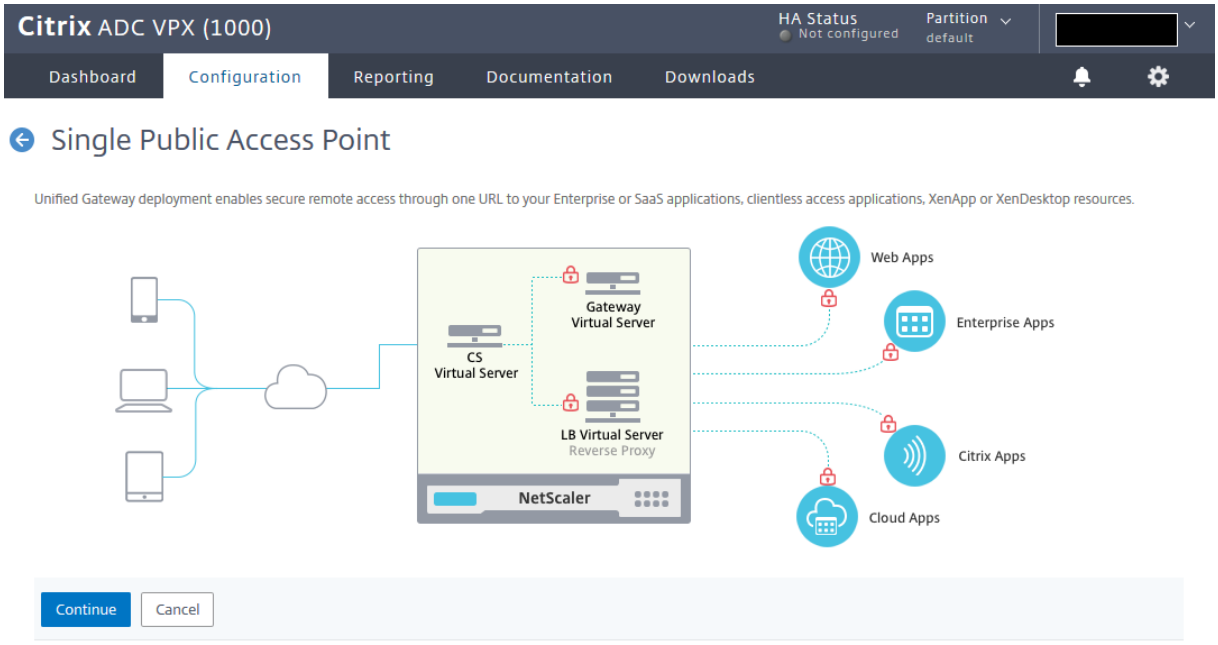
Ouvrez un navigateur Web et accédez à :

- https://sts.ctxdemos.com/FederationMetadata/2007-06/FederationMetadata.xml
- https://sts.ctxdemos.com/adfs/fs/federationserverservice.asmx
- https://sts.ctxdemos.com/adfs/ls/idpinitatedsignon.aspx

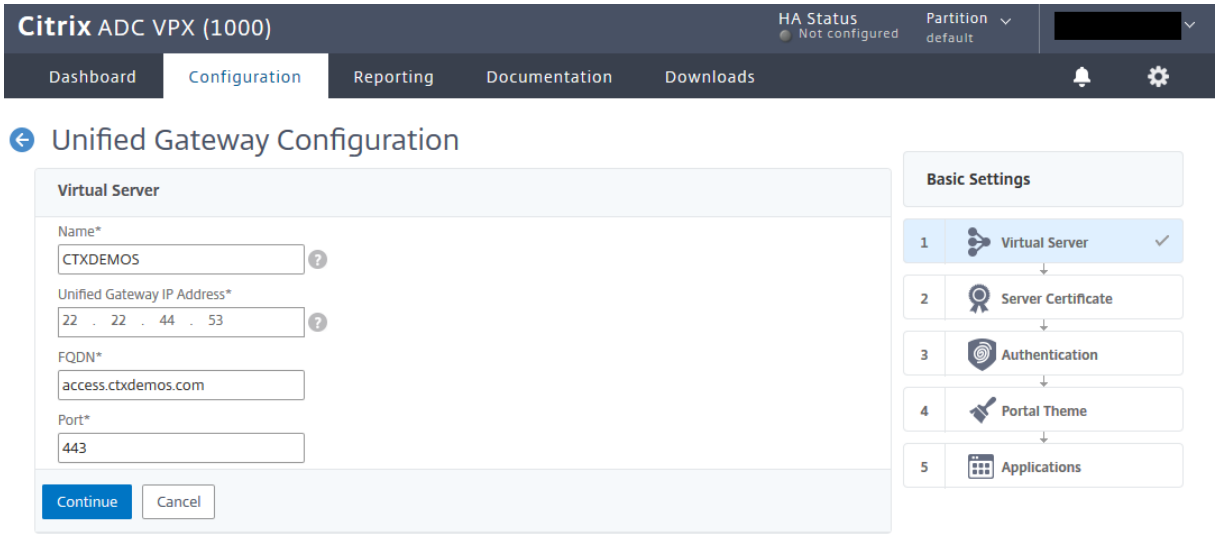
Citrix ADC et Citrix Gateway

Configurer Citrix Gateway

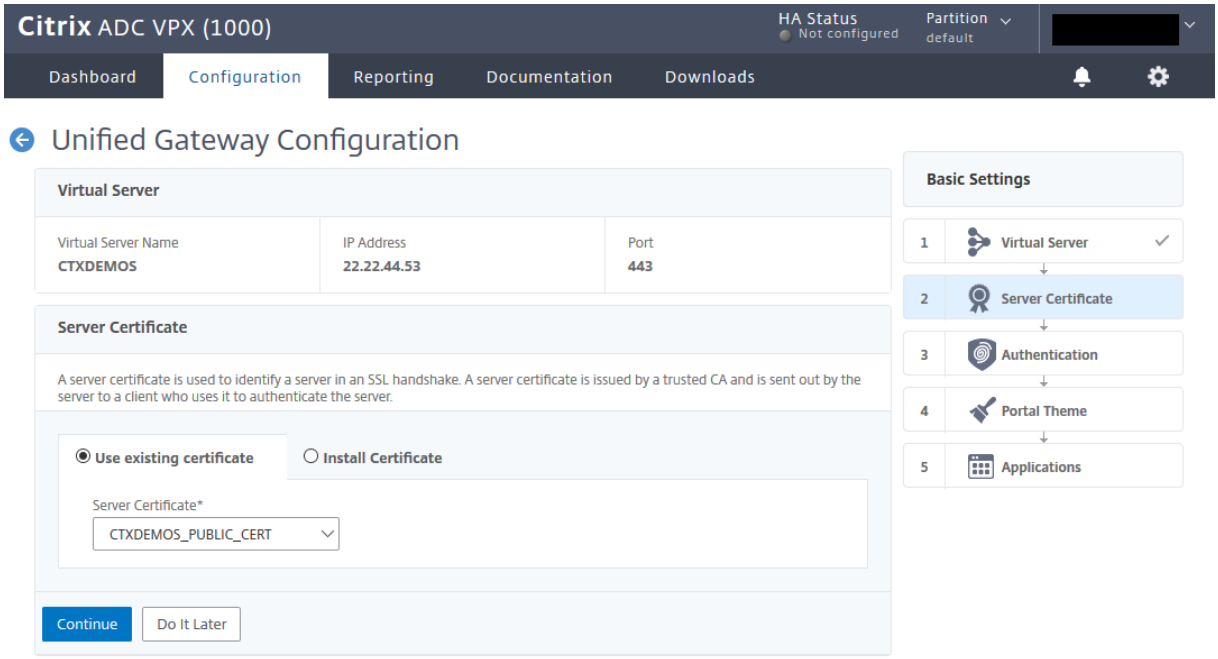
Vous pouvez configurer Citrix Gateway via l'assistant. Connectez-vous à Citrix ADC Management GUI, accédez à **Unified Gateway**, puis cliquez sur **Créer une nouvelle passerelle**. Cliquez ensuite sur **Continuer**.



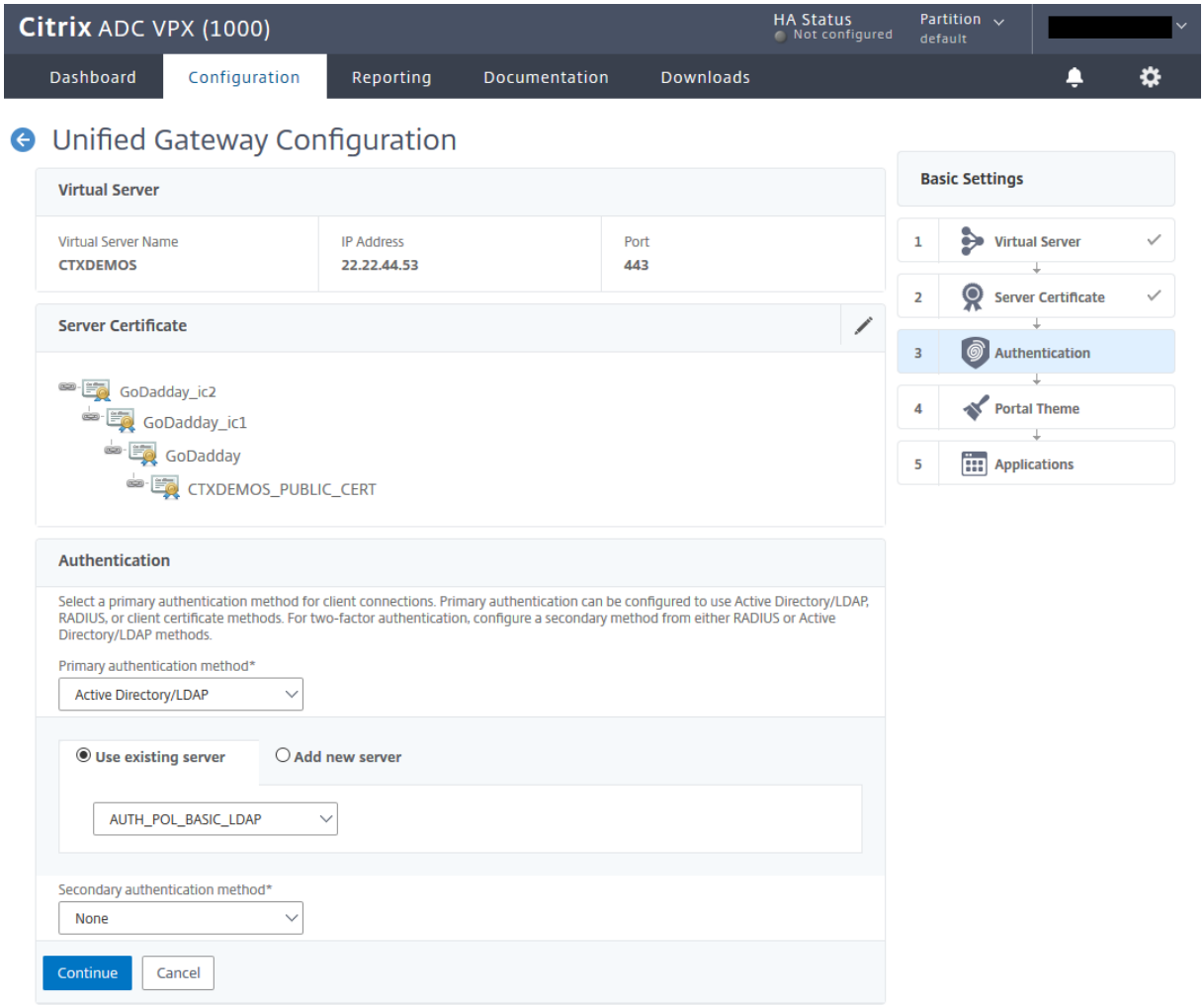
Entrez le nom, l'adresse IP et le nom de domaine complet pour **Unified Gateway**, puis cliquez sur **Continuer**.



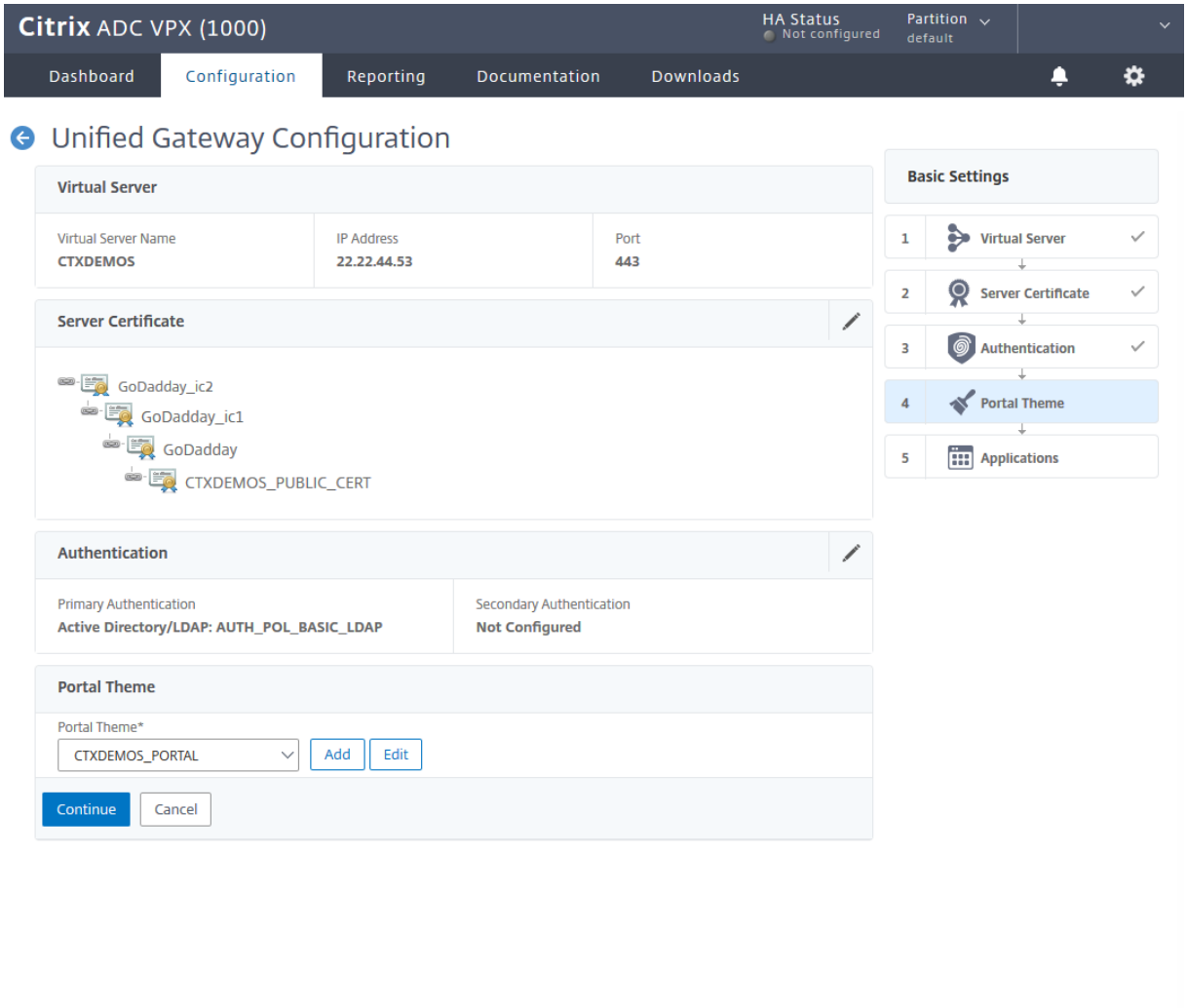
Sélectionnez le certificat SSL public et cliquez sur **Continuer**.



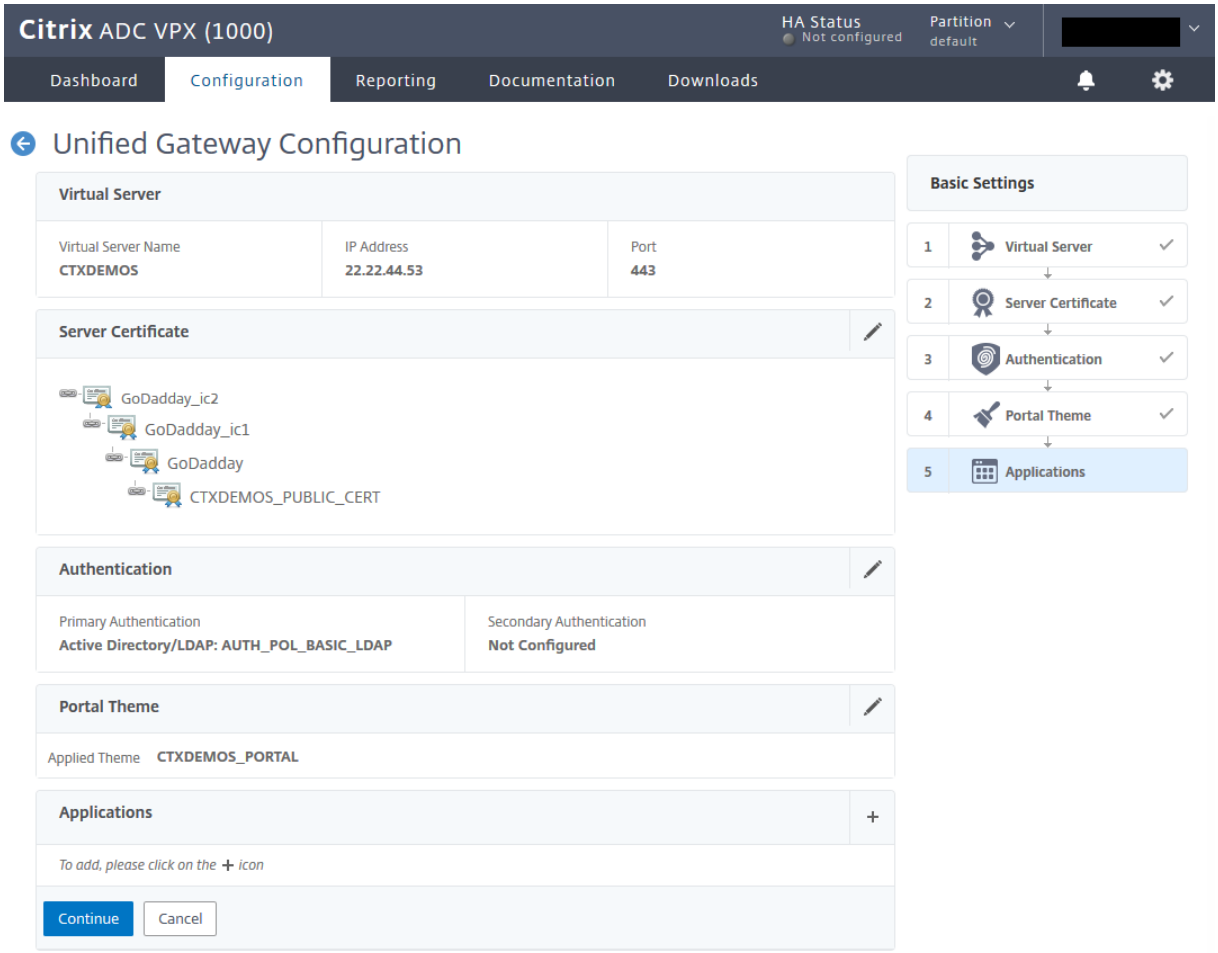
Créez une stratégie LDAP de base et liez-la à **Unified Gateway**. Cliquez sur **Continuer**.



Créez un thème de portail basé sur RFWeBui et liez-le à **Unified Gateway**. Cliquez sur **Continuer**.

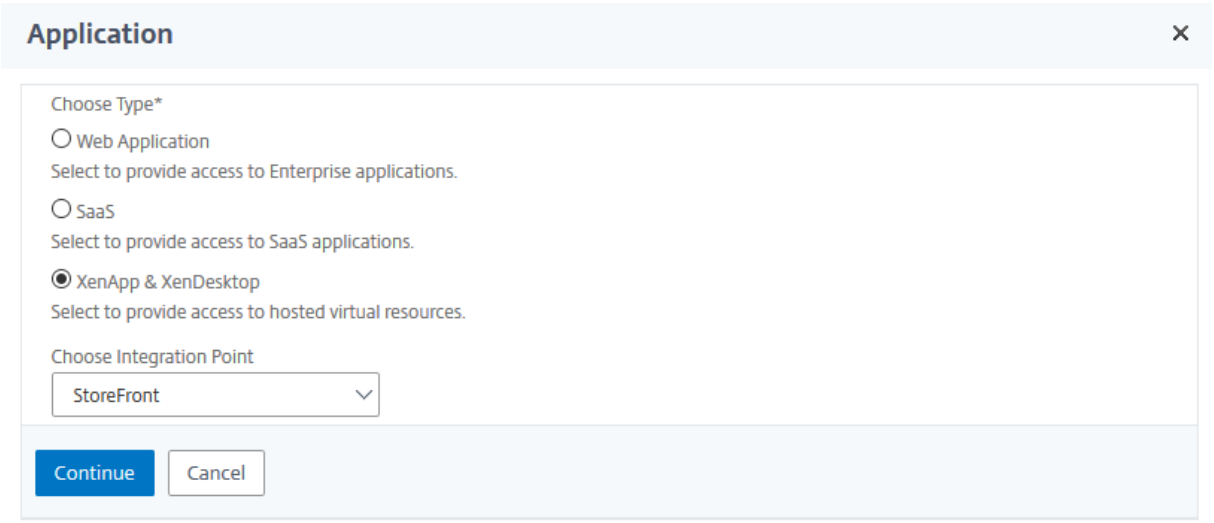


Sélectionnez le signe plus (+) devant les applications pour intégrer Citrix Gateway à StoreFront.

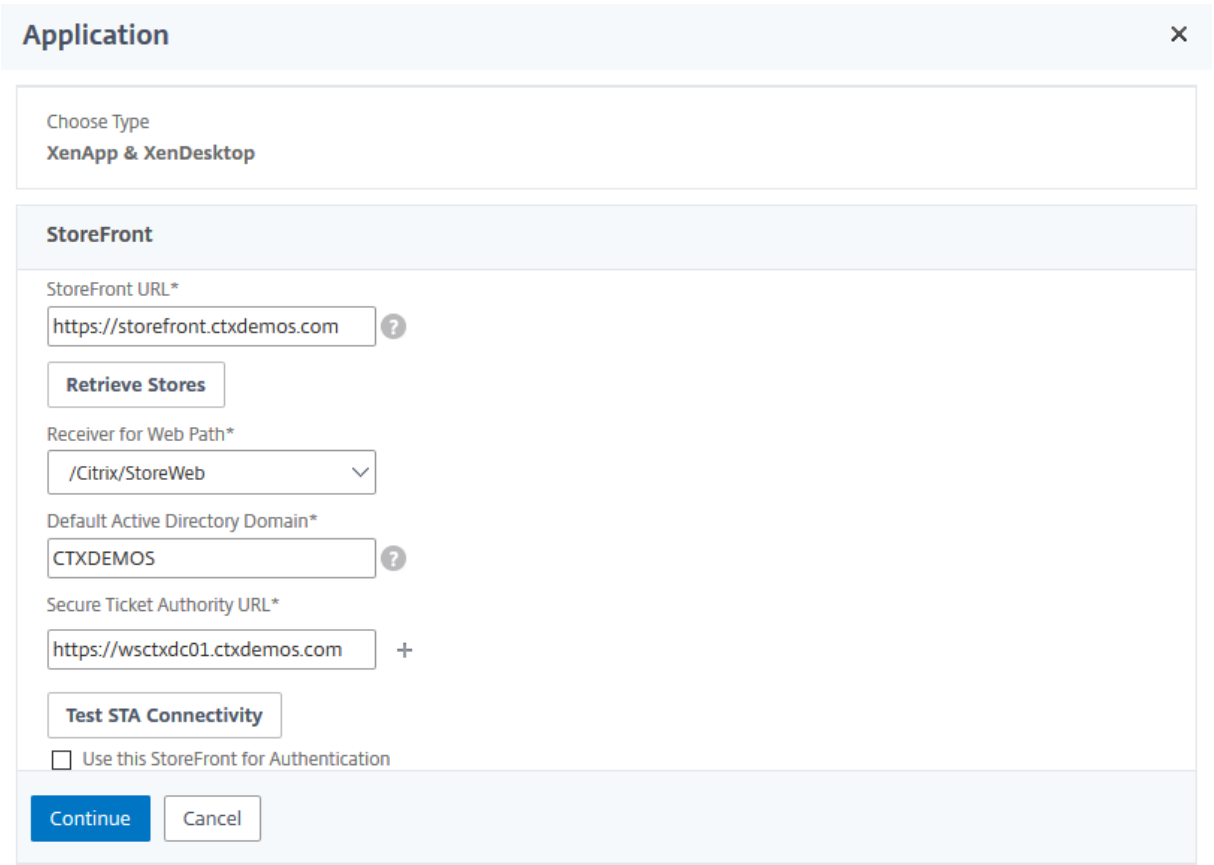


Intégrer Citrix StoreFront dans Citrix Gateway

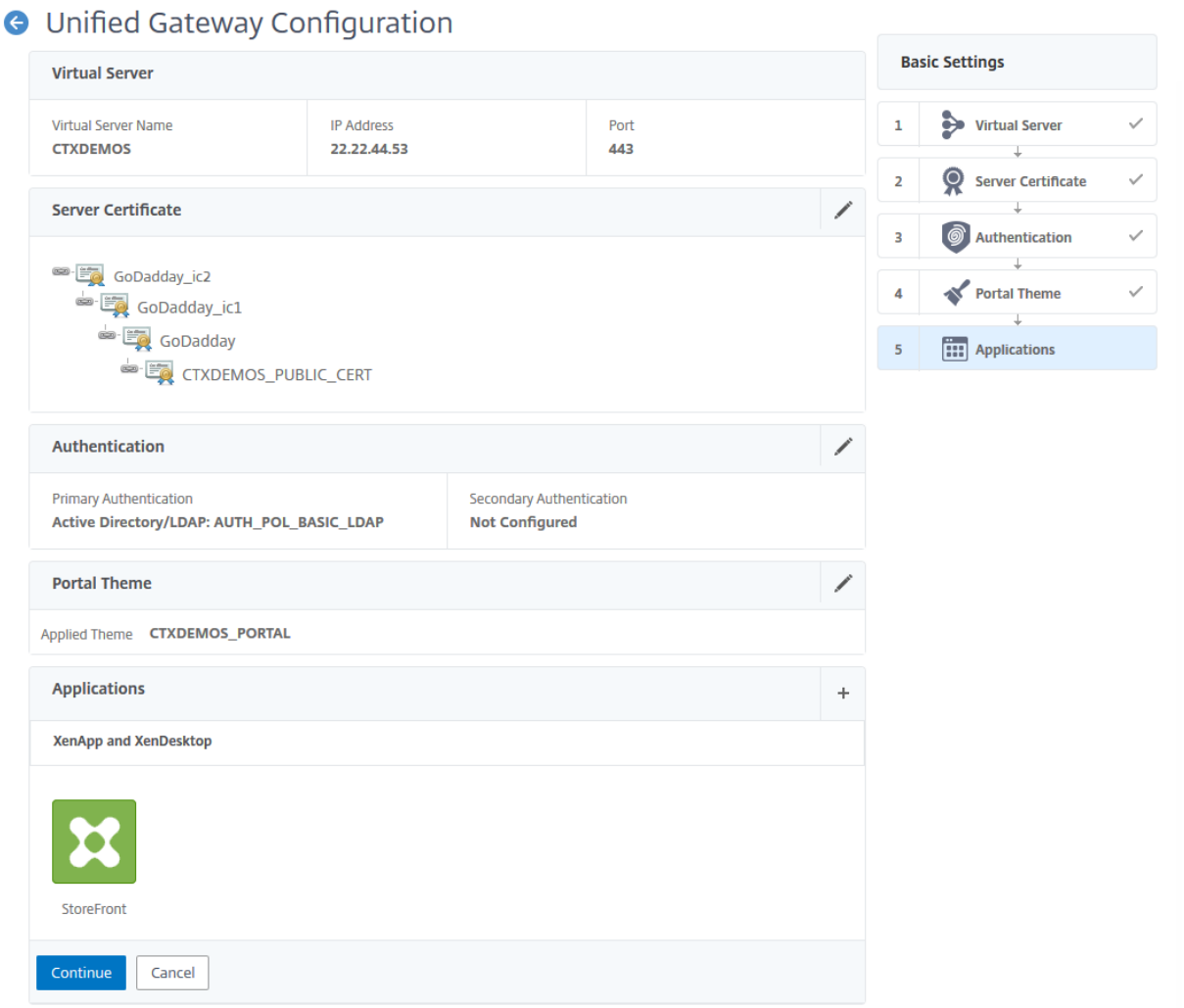
Dans la page Application, sélectionnez **XenApp & XenDesktop**, puis dans la liste **Choisir un point d'intégration**, sélectionnez **StoreFront**. Cliquez sur **Continuer**.



Entrez une URL StoreFront et cliquez sur **Récupérer les magasins**. Entrez ensuite les paramètres du **domaine Active Directory par défaut** et de **l'URL de Secure Ticket Authority**. Cliquez sur **Tester la connectivité STA**, puis sur **Continuer**.



Cliquez sur **Terminé**, puis sur **Continuer**.



Configurer Citrix Gateway et intégrer StoreFront — CLI

```
# Create Session Policy and Action for Citrix Receiver
add vpn sessionAction AC_OS_22.22.44.50 -transparentInterception OFF -
    defaultAuthorizationAction ALLOW -SSO ON -icaProxy ON -wihome "https
    ://access.ctxdemos.com/Citrix/ExternalWeb" -ClientChoices OFF -
    ntDomain CTXDEMOS -clientlessVpnMode OFF -storefronturl "https://
    access.ctxdemos.com"
add vpn sessionPolicy PL_OS_22.22.44.50 "HTTP.REQ.HEADER("User-Agent").
    CONTAINS("CitrixReceiver") && HTTP.REQ.HEADER("User-Agent").CONTAINS
    ("CitrixVPN").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("
    NSGiOSplugin").NOT" AC_OS_22.22.44.50

# Create Session Policy and Action for Citrix Web Client
add vpn sessionAction AC_WB_22.22.44.50 -transparentInterception ON -
    defaultAuthorizationAction ALLOW -forceCleanup cookie -SSO ON -
```



```
    ssoCredential PRIMARY -icaProxy OFF -wihome "https://storefront.
    ctxdemos.com/Citrix/ExternalWeb" -wiPortalMode COMPACT -
    ClientChoices OFF -ntDomain CTXDEMOS -clientlessVpnMode ON -
    clientlessPersistentCookie ALLOW
add vpn sessionPolicy PL_WB_22.22.44.50 "HTTP.REQ.HEADER("User-Agent").
    CONTAINS("CitrixReceiver").NOT" AC_WB_22.22.44.50

# Create Session Policy and Action for Citrix Gateway Client
add vpn sessionAction UG_VPN_SAct_22.22.44.50 -transparentInterception
    ON -defaultAuthorizationAction ALLOW -SSO ON -ClientChoices ON -
    clientlessVpnMode ON
add vpn sessionPolicy UG_VPN_SPol_22.22.44.50 true UG_VPN_SAct_22
    .22.44.50

# Create Responder Policy and Action for Gateway Logout
add responder action RESACT_GATEWAY_LOGOFF_REDIRECT redirect ""https://
    " + HTTP.REQ.HOSTNAME.HTTP_URL_SAFE" -responseStatusCode 302
add responder policy RESPOL_GATEWAY_LOGOFF_REDIRECT "HTTP.REQ.URL.
    CONTAINS("/cgi/logout")" RESACT_GATEWAY_LOGOFF_REDIRECT

# Create Citrix Gateway vServer
add vpn vserver UGVS_VPN_UGCTXDEMOS SSL 0.0.0.0 -loginOnce ON -
    Listenpolicy NONE -vserverFqdn access.ctxdemos.com
set ssl vserver UGVS_VPN_UGCTXDEMOS -ssl3 DISABLED -tls1 DISABLED -
    tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -
    maxage 157680000 -IncludeSubdomains YES
bind ssl vserver UGVS_VPN_UGCTXDEMOS -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver UGVS_VPN_UGCTXDEMOS -cipherName
    CTXDEMOS_FRONTEND_APLUS
bind vpn vserver UGVS_VPN_UGCTXDEMOS -portaltheme CTXDEMOS_PORTAL
bind vpn vserver UGVS_VPN_UGCTXDEMOS -staServer "https://wsctxdc01.
    ctxdemos.com"
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy
    RESPOL_GATEWAY_LOGOFF_REDIRECT -priority 100 -gotoPriorityExpression
     END -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy PL_OS_22.22.44.50 -
    priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy PL_WB_22.22.44.50 -
    priority 110 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver UGVS_VPN_UGCTXDEMOS -policy UG_VPN_SPol_22.22.44.50 -
    priority 58000 -gotoPriorityExpression NEXT -type REQUEST

# Create Content Switching Policy and Action for Citrix Gateway
add cs action CSACT_UGCTXDEMOS -targetVserver UGVS_VPN_UGCTXDEMOS
add cs policy CSPOL_UGCTXDEMOS -rule "is_vpn_url  ||  HTTP.REQ.URL.PATH
```



```
    .SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Citrix/External")" -action
    CSACT_UGCTXDEMOS
32
33 # Create Content Switching vServer for Citrix Gateway
34 add cs vserver CSVS_UGCTXDEMOS SSL 22.22.44.50 443 -cltTimeout 180
35 set ssl vserver CSVS_UGCTXDEMOS -ssl3 DISABLED -tls1 DISABLED -tls11
    DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage
    157680000 -IncludeSubdomains YES
36 bind ssl vserver CSVS_UGCTXDEMOS -certkeyName CTXDEMOS_PUBLIC_CERT
37 bind ssl vserver CSVS_UGCTXDEMOS -cipherName CTXDEMOS_FRONTEND_APLUS
38 bind cs vserver CSVS_UGCTXDEMOS -policyName CSPOL_UGCTXDEMOS -priority
    63000
39
40 # Create Responder Policy and Action for HTTP to HTTPS Redirection
41 add responder action RESACT_HTTP_TO_HTTPS redirect ""https://" + HTTP.
    REQ.HOSTNAME.HTTP_URL_SAFE + HTTP.REQ.URL.PATH_AND_QUERY.
    HTTP_URL_SAFE" -responseStatusCode 301
42 add responder policy RESPOL_HTTP_TO_HTTPS HTTP.REQ.IS_VALID
    RESACT_HTTP_TO_HTTPS
43
44 # Create Always On Server and Service
45 add server LBSRV_ALWAYS_UP 127.0.0.1
46 add service LBSVC_ALWAYS_UP LBSRV_ALWAYS_UP HTTP 80 -gslb NONE -
    maxClient 0 -maxReq 0 -cip ENABLED cip-header -usip YES -
    useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -
    TCPB NO -CMP NO
47
48 # Create Always On vServer for Citrix Gateway
49 add lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS HTTP 22.22.44.50
    80 -persistenceType NONE -cltTimeout 180
50 bind lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS LBSVC_ALWAYS_UP
51 bind lb vserver CSVS_UGCTXDEMOS_REDIRECT_HTTP_TO_HTTPS -policyName
    RESPOL_HTTP_TO_HTTPS -priority 100 -gotoPriorityExpression END -type
     REQUEST
52 <!--NeedCopy-->
```

Configurer le premier serveur d'authentification

```
1 # Create Initialization SAML SP Policy and Action and Bind it to Citrix
     ADC AAA Authentication vServer
2 add authentication samlAction AUTH_ACT_SAML_SP_VPN_TO_LB -
    samlIdPCertName CTXDEMOS_PUBLIC_CERT -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -samlRedirectUrl "https://access.ctxdemos.com/
    samltolb" -signatureAlg RSA-SHA256 -digestMethod SHA256 -samlBinding
```



```
      REDIRECT -groupNameField Groups
3 add authentication Policy AUTH_POL_SAMP_SP_VPN_TO_LB -rule TRUE -action
      AUTH_ACT_SAML_SP_VPN_TO_LB
4
5 # Create Authentication Policy and Action for SAML SP to ADFS
6 add authentication samlAction AUTH_ACT_SAML_SP_ADFS -samlIdPCertName
    CTXDEMOS_ADFS_TOKEN_SIGNING -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -samlRedirectUrl "https://sts.ctxdemos.com/adfs
    /ls/" -samlUserField "Name ID" -samlRejectUnsignedAssertion OFF -
    samlIssuerName "https://access.ctxdemos.com" -Attribute1 "E-Mail
    Address" -signatureAlg RSA-SHA256 -digestMethod SHA256 -logoutURL "
    https://sts.ctxdemos.com/adfs/ls/wa=wsignout1.0" -forceAuthn ON
7 add authentication Policy AUTH_POL_SAML_SP_ADFS -rule TRUE -action
    AUTH_ACT_SAML_SP_ADFS
8
9 # Create Authentication Policy Label for for SAML SP to ADFS
10 add authentication policylabel AUTH_POLLBL_ADFS_AZUREMFA -loginSchema
    LSCHEMA_INT
11 bind authentication policylabel AUTH_POLLBL_ADFS_AZUREMFA -policyName
    AUTH_POL_SAML_SP_ADFS -priority 100 -gotoPriorityExpression NEXT
12
13 # Create Authentication Policy and Action for Group Extraction
14 add authentication ldapAction AUTH_ACT_LDAP_GROUP_EXTRACTION_AZUREMFACA
     -serverIP 22.22.22.61 -serverPort 636 -ldapBase "DC=ctxdemos,DC=com
    " -ldapBindDn "CN=svc_ctxadc01,OU=Services,OU=Accounts,DC=ctxdemos,
    DC=com" -ldapBindDnPassword 0
    c4fe86d56a865ef514a15affd1429f3e079ce1089731d4a407772d21036f3c8 -
    encrypted -encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -
    searchFilter "memberOf:1.2.840.113556.1.4.1941:=CN=AzureMFACAUsers,
    OU=Groups,OU=Authorizations,DC=ctxdemos,DC=com" -groupAttrName
    memberOf -subAttributeName cn -secType SSL -authentication DISABLED
    -nestedGroupExtraction ON -maxNestingLevel 5 -groupNameIdentifier
    sAMAccountName -groupSearchAttribute memberOf -
    groupSearchSubAttribute CN -Attribute1 mail -Attribute2 objectGUID
15 add authentication Policy AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -
    rule TRUE -action AUTH_ACT_LDAP_GROUP_EXTRACTION_AZUREMFACA
16
17 # Create Authentication Policy Label for Group Extraction
18 add authentication policylabel
    AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -loginSchema
    LSCHEMA_INT
19 bind authentication policylabel
    AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -policyName
    AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -priority 100 -
    gotoPriorityExpression NEXT -nextFactor AUTH_POLLBL_ADFS_AZUREMFA
```



```
20
21
22 # Create Login Schema Policy and Profile for First Citrix ADC AAA
       Authentication vServer
23 add authentication loginSchema LSCHEMA_PRF_NOSCHEMA -
       authenticationSchema noschema -SSOCredentials YES
24 add authentication loginSchemaPolicy LSCHEMA_POL_NOSCHEMA -rule TRUE -
       action LSCHEMA_PRF_NOSCHEMA
25
26 # Create First Citrix ADC AAA Authentication vServer
27 add authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN SSL 0.0.0.0
28 set ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -ssl3 DISABLED -tls1
       DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS
       ENABLED -maxage 157680000 -IncludeSubdomains YES
29 bind ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -certkeyName
       CTXDEMOS_PUBLIC_CERT
30 bind ssl vserver AAAVS_CTXDEMOS_COM_FOR_VPN -cipherName
       CTXDEMOS_FRONTEND_APLUS
31 bind authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN -policy
       LSCHEMA_POL_NOSCHEMA -priority 100 -gotoPriorityExpression END
32 bind authentication vserver AAAVS_CTXDEMOS_COM_FOR_VPN -policy
       AUTH_POL_SAMP_SP_VPN_TO_LB -priority 100 -nextFactor
       AUTH_POLLBL_LDAP_GROUP_EXTRACTION_AZURAMFACA -gotoPriorityExpression
        NEXT
33
34 # Create First Citrix ADC AAA Authentication Profile
35 add authentication authnProfile AAA_AUTH_PRF_VPN -authnVsName
       AAAVS_CTXDEMOS_COM_FOR_VPN -AuthenticationHost aaa.ctxdemos.com
36
37 # Set Authentication Profile on Gateway vServer
38 set vpn vserver UGVS_VPN_UGCTXDEMOS -authnProfile AAA_AUTH_PRF_VPN
39 <!--NeedCopy-->
```

Configurer un deuxième serveur d'authentification

```
1 # Create Authentication Policy and Action for LDAP
2 add authentication ldapAction AUTH_ACT_LDAP -serverIP 22.22.22.61 -
      serverPort 636 -authTimeout 60 -ldapBase "DC=ctxdemos,DC=com" -
      ldapBindDn "CN=svc_ctxadc01,OU=Services,OU=Accounts,DC=ctxdemos,DC=
      com" -ldapBindDnPassword 273881819
      af883e70c33d83c0546eac84e81d6eeba904f2d65bbebf2819c025a -encrypted -
      encryptmethod ENCMTHD_3 -ldapLoginName sAMAccountName -groupAttrName
       memberOf -subAttributeName cn -secType SSL -passwdChange ENABLED -
      nestedGroupExtraction ON -maxNestingLevel 5 -groupNameIdentifier
```



```
    sAMAccountName -groupSearchAttribute memberOf -
    groupSearchSubAttribute CN -Attribute1 userprincipalname -Attribute2
     mail -Attribute3 userParameters
add authentication Policy AUTH_POL_LDAP_USER_NAME_PASSWORD -rule TRUE -
    action AUTH_ACT_LDAP

# Create Login Schema Policy and Profile for Second Citrix ADC AAA
    Authentication vServer - Username (Pre-filled ) and Password
add authentication loginSchema LSCHEMA_USER_NAME_PASSWORD -
    authenticationSchema "/nsconfig/loginschema/CTXDEMOS_USER_NAME_PASS.
    xml" -SSOCredentials YES
add authentication loginSchemaPolicy LSCHEMA_POL_USER_NAME_PASSWORD -
    rule TRUE -action LSCHEMA_USER_NAME_PASSWORD

# Create Authentication Policy Label for LDAP Username and Password
add authentication policylabel AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -
    loginSchema LSCHEMA_USER_NAME_PASSWORD
bind authentication policylabel AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -
    policyName AUTH_POL_LDAP_USER_NAME_PASSWORD -priority 110 -
    gotoPriorityExpression NEXT

# Create Login Schema Policy and Profile for Second Citrix ADC AAA
    Authentication vServer - Username Only
add authentication loginSchema LSCHEMA_USER_NAME_ONLY -
    authenticationSchema "/nsconfig/loginschema/CTXDEMOS_USER_NAME_ONLY.
    xml"
add authentication loginSchemaPolicy LSCHEMA_POL_NOPASSWORD -rule TRUE
    -action LSCHEMA_USER_NAME_ONLY

# Create Citrix ADC AAA Session Policy and Profile
add tm sessionAction AAA_SESSION_PRF_CTXDEMOS -SSO ON -ssoDomain
    CTXDEMOS -persistentCookie ON -persistentCookieValidity 30
add tm sessionPolicy AAA_SESSION_POL_CTXDEMOS TRUE
    AAA_SESSION_PRF_CTXDEMOS

# Create Second Citrix ADC AAA Authentication vServer
add authentication vserver AAAVS_CTXDEMOS_COM SSL 22.22.44.51 443
set ssl vserver AAAVS_CTXDEMOS_COM -ssl3 DISABLED -tls1 DISABLED -tls11
     DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage
     157680000 -IncludeSubdomains YES
bind ssl vserver AAAVS_CTXDEMOS_COM -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver AAAVS_CTXDEMOS_COM -cipherName CTXDEMOS_FRONTEND_APLUS
bind authentication vserver AAAVS_CTXDEMOS_COM -portaltheme
    CTXDEMOS_PORTAL
bind authentication vserver AAAVS_CTXDEMOS_COM -policy
```



```
    AAA_SESSION_POL_CTXDEMOS -priority 100 -gotoPriorityExpression NEXT
28 bind authentication vserver AAAVS_CTXDEMOS_COM -policy
    LSCHEMA_POL_NOPASSWORD -priority 110 -gotoPriorityExpression END
29 bind authentication vserver AAAVS_CTXDEMOS_COM -policy
    AUTH_POL_LDAP_GROUP_EXTRACTION_AZURAMFACA -priority 140 -nextFactor
    AUTH_POLLBL_LDAP_USER_NAME_PASSWORD -gotoPriorityExpression NEXT
30
31 # Create Second Citrix ADC AAA Authentication Profile
32 add authentication authnProfile AAA_AUTH_PRF -authnVsName
    AAAVS_CTXDEMOS_COM -AuthenticationHost aaa.ctxdemos.com
33 <!--NeedCopy-->
```

Configurer Citrix ADC en tant que WAP AD FS

Exécutez les commandes suivantes dans Citrix ADC CLI pour configurer Citrix ADC en tant que proxy WAP (AD FS Web Application Proxy) :

```
1  # Pattern Set - ADFS Proxy Hostname
2  add policy patset PATSET_ADFS_HOSTNAME
3  bind policy patset PATSET_ADFS_HOSTNAME sts.ctxdemos.com -index 1 -
       charset ASCII
4  # Policy Expression - ADFS Proxy Hostname
5  add policy expression is_ADFS_HOSTNAME "HTTP.REQ.HEADER("Host").
       TO_LOWER.CONTAINS_ANY("PATSET_ADFS_HOSTNAME")"
6
7  # Pattern Set - ADFS Proxy Path for NoAuth
8  add policy patset PATSET_ADFS_PATH_NOAUTH
9  bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust" -
       index 1 -charset ASCII
10 bind policy patset PATSET_ADFS_PATH_NOAUTH "/federationmetadata
       /2007-06/federationmetadata.xml" -index 2 -charset ASCII
11 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/fs/
       federationserverservice.asmx" -index 3 -charset ASCII
12 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/ls/FormsSignIn.aspx"
       -index 4 -charset ASCII
13 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust/2005/
       usernamemixed" -index 5 -charset ASCII
14 bind policy patset PATSET_ADFS_PATH_NOAUTH "/adfs/services/trust/mex" -
       index 6 -charset ASCII
15
16 # Policy Expression - ADFS Proxy Path for NoAuth
17 add policy expression is_ADFS_PROXY_NOAUTH "HTTP.REQ.URL.PATH.TO_LOWER.
       CONTAINS_ANY("PATSET_ADFS_PATH_NOAUTH")"
18
```



```
# Pattern Set - ADFS Proxy Path for Passive Client
add policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE
bind policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE "/adfs" -index 1 -
    charset ASCII
bind policy patset PATSET_ADFS_PATH_ACTIVE_PASSIVE "/cgi/selfauth" -
    index 2 -charset ASCII

# Policy Expression - ADFS Proxy Path for Passive Client
add policy expression is_ADFS_PROXY_ACTIVE_PASSIVE "(HTTP.REQ.HEADER("
    Host").TO_LOWER.CONTAINS_ANY("PATSET_ADFS_HOSTNAME") && HTTP.REQ.URL
    .PATH.TO_LOWER.STARTSWITH_ANY("PATSET_ADFS_PATH_ACTIVE_PASSIVE"))"

# Rewrite Policies for ADFS PIP
add rewrite action RWACT_X_MS_Proxy insert_http_header X-MS-Proxy ""
    NETSCALER""
add rewrite policy RWPOL_X_MS_Proxy true RWACT_X_MS_Proxy

add rewrite action RWACT_X_MS_Forwarded_Client_IP insert_http_header X-
    MS-Forwarded-Client-IP CLIENT.IP.SRC
add rewrite policy RWPOL_X_MS_Forwarded_Client_IP true
    RWACT_X_MS_Forwarded_Client_IP

add rewrite action RWACT_X_MS_Endpoint_Absolute_Path insert_http_header
     X-MS-Endpoint-Absolute-Path HTTP.REQ.URL
add rewrite policy RWPOL_X_MS_Endpoint_Absolute_Path true
    RWACT_X_MS_Endpoint_Absolute_Path

add rewrite action RWACT_X_MS_Target_Role insert_http_header X-MS-
    Target-Role ""PrimaryComputer""
add rewrite policy RWPOL_X_MS_Target_Role true RWACT_X_MS_Target_Role

add rewrite action RWACT_X_MS_ADFS_Proxy_Client_IP insert_http_header X
    -MS-ADFS-Proxy-Client-IP CLIENT.IP.SRC
add rewrite policy RWPOL_X_MS_ADFS_Proxy_Client_IP true
    RWACT_X_MS_ADFS_Proxy_Client_IP

add rewrite action RWACT_X_MS_Client_User_Agent insert_http_header X-MS
    -Client-User-Agent "HTTP.REQ.HEADER("User-Agent")"
add rewrite policy RWPOL_X_MS_Client_User_Agent true
    RWACT_X_MS_Client_User_Agent

add rewrite action RWACT_ADFS_PROXYMEX replace HTTP.REQ.URL.
    PATH_AND_QUERY ""/adfs/services/trust/proxymex" + HTTP.REQ.URL.
    SET_TEXT_MODE(IGNORECASE).PATH_AND_QUERY.STRIP_START_CHARS("/adfs/
    services/trust/mex").HTTP_URL_SAFE"
```



```
47 add rewrite policy RWPOL_ADFS_PROXYMEX "is_ADFS_HOSTNAME && HTTP.REQ.
       URL.TO_LOWER.STARTSWITH("/adfs/services/trust/mex")"
       RWACT_ADFS_PROXYMEX
48
49 add rewrite policy RWPOL_ADFS_PROXY_HEADERS-NOACT TRUE NOREWRITE
50
51 add rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS http_req
52 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS RWPOL_X_MS_Proxy
       100 NEXT
53 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_X_MS_Forwarded_Client_IP 110 NEXT
54 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_X_MS_Endpoint_Absolute_Path 120 NEXT
55 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_X_MS_Target_Role 130 NEXT
56 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_X_MS_ADFS_Proxy_Client_IP 140 NEXT
57 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_X_MS_Client_User_Agent 150 NEXT
58 bind rewrite policylabel RWPOLLBL_ADFS_PROXY_HEADERS
       RWPOL_ADFS_PROXYMEX 160 NEXT
59
60 # Create ADFS Server and Service Group
61 add server LBSRV_ADFS wsadfs01.ctxdemos.com
62 add serviceGroup LBSVCGRP_ADFS_443 SSL -maxClient 0 -maxReq 0 -cip
       ENABLED X-MS-Forwarded-Client-IP -usip NO -useproxyport YES -sp ON -
       cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP YES
63 bind ssl serviceGroup LBSVCGRP_ADFS_443 -cipherName CTXDEMO_BACKEND
64 set ssl serviceGroup LBSVCGRP_ADFS_443 -ssl3 DISABLED -tls1 DISABLED -
       tls11 DISABLED
65 bind serviceGroup LBSVCGRP_ADFS_443 LBSRV_ADFS 443
66
67 # Create ADFS Proxy NoAuth Load Balancing vServer
68 add lb vserver LBVS_ADFS_PROXY_NOAUTH SSL 0.0.0.0 0 -persistenceType
       NONE -cltTimeout 180
69 set ssl vserver LBVS_ADFS_PROXY_NOAUTH -ssl3 DISABLED -tls1 DISABLED -
       tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -
       maxage 157680000 -IncludeSubdomains YES
70 bind ssl vserver LBVS_ADFS_PROXY_NOAUTH -certkeyName CTXDEMOS-PUBLIC
71 bind ssl vserver LBVS_ADFS_PROXY_NOAUTH -cipherName CTXDEMO_BACKEND
72 bind lb vserver LBVS_ADFS_PROXY_NOAUTH LBSVCGRP_ADFS_443
73 bind lb vserver LBVS_ADFS_PROXY_NOAUTH -policyName
       RWPOL_ADFS_PROXY_HEADERS-NOACT -priority 100 -gotoPriorityExpression
        NEXT -type REQUEST -invoke policylabel RWPOLLBL_ADFS_PROXY_HEADERS
74
```



```
# Create ADFS Proxy NoAuth Content Switching Policy and Action
add cs action CSACT_ADFS_PROXY_NOAUTH -targetLBVserver
    LBVS_ADFS_PROXY_NOAUTH
add cs policy CSPOL_ADFS_PROXY_NOAUTH -rule is_ADFS_PROXY_NOAUTH -
    action CSACT_ADFS_PROXY_NOAUTH

# Create ADFS Proxy Active-Passive Load Balancing vServer
add lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE SSL 0.0.0.0 0 -
    persistenceType NONE -cltTimeout 180 -Authentication ON -
    authnProfile AAA_AUTH_PRF
set ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -ssl3 DISABLED -tls1
    DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS
    ENABLED -maxage 157680000 -IncludeSubdomains YES
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE LBSVCGRP_ADFS_443
bind ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -certkeyName CTXDEMOS-
    PUBLIC
bind ssl vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -cipherName
    CTXDEMO_FRONTEND_APLUS
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName
    RWPOL_ADFS_PROXY_HEADERS-NOACT -priority 100 -gotoPriorityExpression
     NEXT -type REQUEST -invoke policylabel RWPOLLBL_ADFS_PROXY_HEADERS

# Create ADFS Proxy Active-Passive Content Switching Policy and Action
add cs action CSACT_ADFS_PROXY_ACTIVE_PASSIVE -targetLBVserver
    LBVS_ADFS_PROXY_ACTIVE_PASSIVE
add cs policy CSPOL_ADFS_PROXY_ACTIVE_PASSIVE -rule
    is_ADFS_PROXY_ACTIVE_PASSIVE -action CSACT_ADFS_PROXY_ACTIVE_PASSIVE

# Bind Content Switching Policies to Citrix Gateway Content Switching
    vServer
bind cs vserver CSVS_UGCTXDEMOS -policyName CSPOL_ADFS_PROXY_NOAUTH -
    priority 100
bind cs vserver CSVS_UGCTXDEMOS -policyName
    CSPOL_ADFS_PROXY_ACTIVE_PASSIVE -priority 300

# Create Citrix ADC AAA Traffic Policies and Bind them to ADFS Proxy
    Active-Passive Load Balancing vServer
add tm formSSOAction AAATM_SSOPRF_ADFS_LOGIN -actionURL "/adfs/ls" -
    userField UserName -passwdField Password -ssoSuccessRule true -
    nameValuePair AuthMethod=FormsAuthentication -responsesize 15000 -
    submitMethod POST
add tm trafficAction AAATM_PRF_ADFS_LOGIN -appTimeout 1 -SSO ON -
    formSSOAction AAATM_SSOPRF_ADFS_LOGIN -persistentCookie OFF -
    InitiateLogout OFF -kcdAccount NONE -userExpression "HTTP.REQ.USER.
    ATTRIBUTE(3)" -passwdExpression "HTTP.REQ.USER.ATTRIBUTE(2)"
```



```
add tm trafficPolicy AAATM_POL_ADFS_LOGIN "HTTP.REQ.URL.TO_LOWER.STARTSWITH("/adfs/ls")" AAATM_PRF_ADFS_LOGIN
add tm trafficAction AAATM_PRF_ADFS_LOGOUT -appTimeout 1 -persistentCookie OFF -InitiateLogout ON -kcdAccount NONE
add tm trafficPolicy AAATM_POL_ADFS_LOGOUT "HTTP.REQ.URL.TO_LOWER.STARTSWITH("/adfs/ls") && HTTP.REQ.URL.QUERY.VALUE("wa").EQ("wsignout1.0")" AAATM_PRF_ADFS_LOGOUT
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName AAATM_POL_ADFS_LOGIN -priority 100 -gotoPriorityExpression END -type REQUEST
bind lb vserver LBVS_ADFS_PROXY_ACTIVE_PASSIVE -policyName AAATM_POL_ADFS_LOGOUT -priority 110 -gotoPriorityExpression END -type REQUEST
<!--NeedCopy-->
```

Configurer un flux d'authentification initial

```
# Pattern Set - Gateway and AAA Hostname
add policy patset PATSET_GATEWAY_HOSTHEADER
bind policy patset PATSET_GATEWAY_HOSTHEADER access.ctxdemos.com -index 1 -charset ASCII
bind policy patset PATSET_GATEWAY_HOSTHEADER aaa.ctxdemos.com -index 2 -charset ASCII
# Policy Expression - Gateway and AAA Hostname
add policy expression is_GATEWAY_HOSTNAME "HTTP.REQ.HEADER("Host").TO_LOWER.CONTAINS_ANY("PATSET_GATEWAY_HOSTHEADER")"

# Create Initialization Load Balancing vServer
add lb vserver LBVS_SAML_SP_INITIALIZATION SSL 0.0.0.0 0 -persistenceType NONE -cltTimeout 180 -Authentication ON -authnProfile AAA_AUTH_PRF
set ssl vserver LBVS_SAML_SP_INITIALIZATION -ssl3 DISABLED -tls1 DISABLED -tls11 DISABLED -tls13 ENABLED -ocspStapling ENABLED -HSTS ENABLED -maxage 157680000 -IncludeSubdomains YES
bind lb vserver LBVS_SAML_SP_INITIALIZATION LBSVC_ALWAYS_UP
bind ssl vserver LBVS_SAML_SP_INITIALIZATION -certkeyName CTXDEMOS_PUBLIC_CERT
bind ssl vserver LBVS_SAML_SP_INITIALIZATION -cipherName CTXDEMOS_FRONTEND_APLUS

# Create Initialization Content Switching Policy and Action
add cs action CSACT_SAML_SP_INITIALIZATION -targetLBVserver LBVS_SAML_SP_INITIALIZATION
add cs policy CSPOL_SAML_SP_INITIALIZATION -rule "is_GATEWAY_HOSTNAME
```



```
    && HTTP.REQ.URL.PATH.TO_LOWER.STARTSWITH("/samltolb")" -action
    CSACT_SAML_SP_INITIALIZATION
18
19 # Bind Content Switching Policies to Citrix Gateway Content Switching
    vServer
20 bind cs vserver CSVS_UGCTXDEMOS -policyName
    CSPOL_SAML_SP_INITIALIZATION -priority 500
21
22 # Create Initialization Citrix ADC AAA Traffic Policy and Action and
    Bind it to Load Balancing vServer
23 add tm samlSSOProfile AAATM_SAMLSSOPRF_VPN_TO_LB -samlSigningCertName
    CTXDEMOS_PUBLIC_CERT -assertionConsumerServiceURL "https://access.
    ctxdemos.com/cgi/samlauth" -relaystateRule "HTTP.REQ.URL.QUERY.VALUE
    ("RelayState")" -signatureAlg RSA-SHA256 -digestMethod SHA256 -
    Attribute1 Password -Attribute1Expr AAA.USER.PASSWD -Attribute2
    Groups -Attribute2Expr AAA.USER.GROUPS -encryptAssertion ON -
    samlSPCertName CTXDEMOS_PUBLIC_CERT
24 add tm trafficAction AAATM_PRF_VPN_TO_LB -SSO ON -persistentCookie OFF
    -InitiateLogout OFF -kcdAccount NONE -samlSSOProfile
    AAATM_SAMLSSOPRF_VPN_TO_LB
25 add tm trafficPolicy AAATM_POL_VPN_TO_LB "HTTP.REQ.URL.STARTSWITH("/
    samltolb")" AAATM_PRF_VPN_TO_LB
26 bind lb vserver LBVS_SAML_SP_INITIALIZATION -policyName
    AAATM_POL_VPN_TO_LB -priority 100 -gotoPriorityExpression END -type
    REQUEST
27 <!--NeedCopy-->
```

Groupes de chiffrement

```
1 # Create Cipher Group for Backend vServers
2 add ssl cipher CTXDEMOS_BACKEND
3 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-AES256-GCM-SHA384 -
    cipherPriority 1
4 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-CHACHA20-POLY1305-
    SHA256 -cipherPriority 2
5 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.3-AES128-GCM-SHA256 -
    cipherPriority 3
6 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-RSA-AES256-
    GCM-SHA384 -cipherPriority 4
7 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-RSA-AES128-
    GCM-SHA256 -cipherPriority 5
8 bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-
    GCM-SHA384 -cipherPriority 6
```



```
bind ssl cipher CTXDEMOS_BACKEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 7

# Create Cipher Group for Frondend vServers
add ssl cipher CTXDEMOS_FRONTEND
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-AES256-GCM-SHA384 -cipherPriority 1
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-CHACHA20-POLY1305-SHA256 -cipherPriority 2
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.3-AES128-GCM-SHA256 -cipherPriority 3
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 4
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384 -cipherPriority 5
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES128-SHA256 -cipherPriority 6
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-ECDSA-AES256-SHA384 -cipherPriority 7
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-ECDSA-AES128-SHA -cipherPriority 8
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-ECDSA-AES256-SHA -cipherPriority 9
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 10
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 11
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256 -cipherPriority 12
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384 -cipherPriority 13
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-RSA-AES128-SHA -cipherPriority 15
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-ECDHE-RSA-AES256-SHA -cipherPriority 16
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-DHE-RSA-AES128-GCM-SHA256 -cipherPriority 17
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1.2-DHE-RSA-AES256-GCM-SHA384 -cipherPriority 18
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-DHE-RSA-AES-128-CBC-SHA -cipherPriority 19
bind ssl cipher CTXDEMOS_FRONTEND -cipherName TLS1-DHE-RSA-AES-256-CBC-SHA -cipherPriority 20

# Create Cipher Group for Frondend vServers - A+
```



```
add ssl cipher CTXDEMOS_FRONTEND_APLUS
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-AES256-GCM-SHA384 -cipherPriority 1
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-CHACHA20-POLY1305-SHA256 -cipherPriority 2
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.3-AES128-GCM-SHA256 -cipherPriority 3
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384 -cipherPriority 4
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256 -cipherPriority 5
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-CHACHA20-POLY1305 -cipherPriority 6
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES256-SHA384 -cipherPriority 7
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-ECDSA-AES128-SHA256 -cipherPriority 8
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES256-GCM-SHA384 -cipherPriority 9
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES128-GCM-SHA256 -cipherPriority 13
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-CHACHA20-POLY1305 -cipherPriority 14
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES-256-SHA384 -cipherPriority 15
bind ssl cipher CTXDEMOS_FRONTEND_APLUS -cipherName TLS1.2-ECDHE-RSA-AES-128-SHA256 -cipherPriority 16
<!--NeedCopy-->
```

Fichier XML de schéma de connexion

CTXDEMOS_USER_NAME_PASS.XML

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response/1">
    <Status>success</Status>
    <Result>more-info</Result>
    <StateContext/>
    <AuthenticationRequirements>
        <PostBack>/nf/auth/doAuthentication.do</PostBack>
        <CancelPostBack>/Citrix/Authentication/ExplicitForms/CancelAuthenticate</CancelPostBack>
        <CancelButtonText>Cancel</CancelButtonText>
```



```
10          <Requirements>
11              <Requirement>
12                  <Credential>
13                      <ID>login</ID>
14                      <SaveID>ExplicitForms-Username</SaveID>
15                      <Type>username</Type>
16                  </Credential>
17                  <Label>
18                      <Text>User name</Text>
19                      <Type>plain</Type>
20                  </Label>
21                  <Input>
22                      <AssistiveText>Please supply username</
                           AssistiveText>
23                      <Text>
24                          <Secret>false</Secret>
25                          <ReadOnly>false</ReadOnly>
26                          <InitialValue>${
27  AAA.USER.NAME }
28  </InitialValue>
29                          <Constraint>.+</Constraint>
30                      </Text>
31                  </Input>
32              </Requirement>
33              <Requirement>
34                  <Credential>
35                      <ID>passwd</ID>
36                      <SaveID>ExplicitForms-Password</SaveID>
37                      <Type>password</Type>
38                  </Credential>
39                  <Label>
40                      <Text>Password:</Text>
41                      <Type>plain</Type>
42                  </Label>
43                  <Input>
44                      <Text>
45                          <Secret>true</Secret>
46                          <ReadOnly>false</ReadOnly>
47                          <InitialValue/>
48                          <Constraint>.+</Constraint>
49                      </Text>
50                  </Input>
51              </Requirement>
52              <Requirement>
53                  <Credential>
```



```
                    <ID>saveCredentials</ID>
                    <Type>savecredentials</Type>
                </Credential>
                <Label>
                    <Text>Remember my password</Text>
                    <Type>plain</Type>
                </Label>
                <Input>
                    <CheckBox>
                        <InitialValue>false</InitialValue>
                    </CheckBox>
                </Input>
            </Requirement>
            <Requirement>
                <Credential>
                    <ID>loginBtn</ID>
                    <Type>none</Type>
                </Credential>
                <Label>
                    <Type>none</Type>
                </Label>
                <Input>
                    <Button>Log On</Button>
                </Input>
            </Requirement>
        </Requirements>
    </AuthenticationRequirements>
</AuthenticateResponse>
<!--NeedCopy-->
```

CTXDEMOS_USER_NAME_ONLY.XML

```
<?xml version="1.0" encoding="utf-8"?>
<AuthenticateResponse xmlns="http://citrix.com/authentication/response
    /1">
    <Status>success</Status>
    <Result>more-info</Result>
    <StateContext/>
    <AuthenticationRequirements>
        <PostBack>/nf/auth/doAuthentication.do</PostBack>
        <CancelPostBack>/Citrix/Authentication/ExplicitForms/
            CancelAuthenticate</CancelPostBack>
        <CancelButtonText>Cancel</CancelButtonText>
        <Requirements>
            <Requirement>
```



```
12                  <Credential>
13                      <ID>login</ID>
14                      <SaveID>ExplicitForms-Username</SaveID>
15                      <Type>username</Type>
16                  </Credential>
17                  <Label>
18                      <Text>User name</Text>
19                      <Type>plain</Type>
20                  </Label>
21                  <Input>
22                      <AssistiveText>Please supply username</
                           AssistiveText>
23                      <Text>
24                          <Secret>false</Secret>
25                          <ReadOnly>false</ReadOnly>
26                          <InitialValue/>
27                          <Constraint>.+</Constraint>
28                      </Text>
29                  </Input>
30              </Requirement>
31              <Requirement>
32                  <Credential>
33                      <Type>none</Type>
34                  </Credential>
35                  <Label>
36                      <Text> Please submit credentials to continue Login
                           ...</Text>
37                      <Type>confirmation</Type>
38                  </Label>
39                  <Input/>
40              </Requirement>
41              <Requirement>
42                  <Credential>
43                      <ID>saveCredentials</ID>
44                      <Type>savecredentials</Type>
45                  </Credential>
46                  <Label>
47                      <Text>Remember my password</Text>
48                      <Type>plain</Type>
49                  </Label>
50                  <Input>
51                      <CheckBox>
52                          <InitialValue>false</InitialValue>
53                      </CheckBox>
54                  </Input>
```



```
55              </Requirement>
56              <Requirement>
57                  <Credential>
58                      <ID>loginBtn</ID>
59                      <Type>none</Type>
60                  </Credential>
61                  <Label>
62                      <Type>none</Type>
63                  </Label>
64                  <Input>
65                      <Button>Log On</Button>
66                  </Input>
67              </Requirement>
68          </Requirements>
69      </AuthenticationRequirements>
70  </AuthenticateResponse>
71  <!--NeedCopy-->
```

Références

Authentification vers NetScaler à l'aide d'AD FS 4.0 sur Server 2016, Citrix FAS et Azure MFA dans Azure Cloud. (2018). Extrait de https://www.jgspiers.com/authentication-to-netscaler-using-ad-fs-4-0-server-2016-citrix-fas-azure-mfa-azure-cloud/

Configurez Azure MFA en tant que fournisseur d'authentification avec AD FS. (2019). Extrait de https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/operations/configure-ad-fs-and-azure-mfa

Déploiement d'une batterie de serveurs de fédération. (2017). Extrait de https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/deploying-a-federation-server-farm

Déploiement ADFS du service d'authentification fédérée. (2018). Extrait de https://docs.citrix.com/fr-fr/citrix-virtual-apps-desktops/secure/federated-authentication-service/fas-architectures/fas-adfs.html

Guide de déploiement de NetScaler en tant que proxy Active Directory Federation Services. (s.d.). Extrait de https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/guide-to-deploying-netscaler-as-an-active-directory-federation-services-proxy.pdf

Comment cela fonctionne : Azure Multi-Factor Authentication. (2018). Extrait de https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-mfa-howitworks

Planification d'un déploiement Azure Multi-Factor Authentication basé sur le cloud. (2019). Extrait de https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted

Tijl Van den Broeck. (7 déc. 2017). ADFS v3 sur Windows Server 2012 R2 avec NetScaler. Extrait de https://www.citrix.com/blogs/2015/05/29/adfs-v3-on-windows-server-2012-r2-with-netscaler/

Transition vers le cloud hybride et le SaaS avec Citrix Gateway. (s.d.). Extrait de https://www.citrix.com/products/citrix-gateway/resources/netscaler-unified-gateway.html

Connexion utilisateur à l'aide de l'authentification directe Azure Active Directory. (2018). Extrait de https://docs.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta

Écrit par Saman Salehian, ingénieur en chef des ventes en réseau.

Utilisation du cache d'hôte local pour les mises à niveau de base de données sans interruption de service

January 8, 2020

La fonctionnalité Local Host Cache (LHC) permet aux opérations de courtage de connexion dans un site XenApp ou XenDesktop de continuer en cas de panne. La procédure suivante montre comment LHC peut être utilisé pour effectuer une mise à niveau sans interruption de service du site lorsqu'il n'y a pas de zones secondaires. Consultez les futures mises à jour car Citrix cherche à développer ce guide afin d'inclure une procédure pour les environnements comportant plusieurs zones.

Avant de poursuivre, il est recommandé de revoir la fonctionnalité Cache hôte local, ses exigences et ses limites :https://docs.citrix.com/fr-fr/xenapp-and-xendesktop/7-15-ltsr/manage-deployment/local-host-cache.html

Il existe également un guide de concept avancé sur le dimensionnement et la mise à l'échelle du cache d'hôte local qui peut être trouvé ici :https://docs.citrix.com/fr-fr/advanced-concepts/implementation-guides/local-host-cache-sizing-scaling.html

Avertissement : Effectuez ces étapes dans un environnement de test avant de les implémenter dans un environnement de production en direct pour vous assurer que vous êtes familier avec le processus et que vous êtes préparé à tout problème ou question spécifique à l'environnement qui peut survenir. Il est également recommandé d'utiliser la dernière mise à jour cumulative (CU) LTSR disponible car plusieurs correctifs liés au LHC peuvent bénéficier à votre environnement.

Généralités

1. Configurez l'environnement pour cette procédure.
2. Déterminer le courtier principal élu.
3. Forcer une panne pour déclencher la fonctionnalité de cache d'hôte local.
4. Autoriser les VDA à se réinscrire auprès des courtiers secondaires élus.

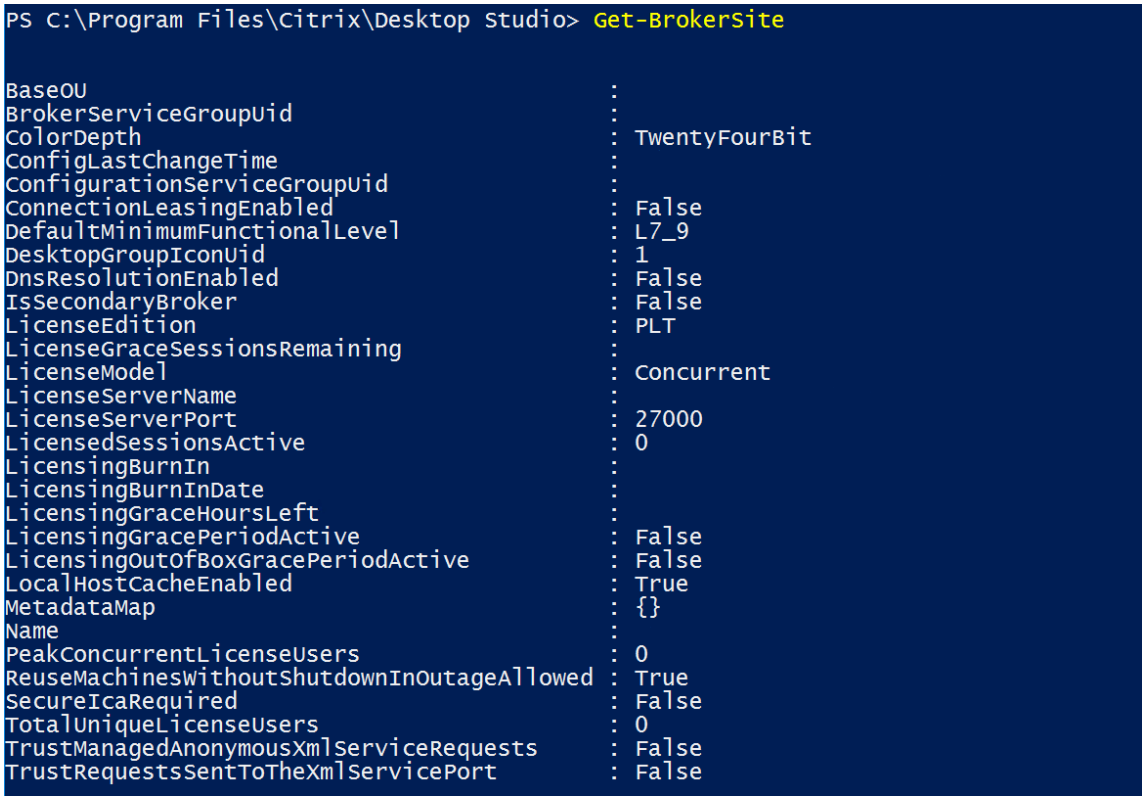
5. Effectuez la mise à niveau du produit sur un courtier secondaire non sélectionné.
6. Effectuez la mise à niveau obligatoire du site, y compris la mise à niveau de
7. Effectuez des mises à niveau de produits sur tous les courtiers secondaires non sélectionnés restants.
8. Quittez la panne et le mode Cache hôte local.
9. Autoriser les VDA à s'enregistrer à nouveau avec les Delivery Controller récemment mis à niveau.
10. Effectuez la mise à niveau du produit sur le dernier Delivery Controller restant (courtier secondaire précédemment élu).
11. Renvoyer l'environnement à la configuration par défaut.

Procédure

1. Vérifiez si le cache d'hôte local est activé à l'aide de l'applet de commande PowerShell suivante.

   ```
   Get-BrokerSite
   ```

   Cherchez`LocalHostCacheEnabled : True`

   Si la valeur est false, activez le cache d'hôte local.

   ```
   Set-BrokerSite -LocalHostCacheEnabled $true -ConnectionLeasingEnabled
   $false
   ```

   Cette applet de commande désactive également la fonctionnalité de location de connexion.

N'activez pas à la fois le cache d'hôte local et le crédit-bail de connexion.

2. Par défaut, les VDA de bureau gérés par l'alimentation dans les groupes de mise à disposition groupés dont la propriété « ShutdownDesktopSafterUse » est activée sont placés en mode de maintenance en cas de panne. Pour remplacer le comportement par défaut, vous devez l'activer à l'échelle du site et pour chaque groupe de mise à disposition affecté. Exécutez les applets de commande PowerShell suivantes.

```
Set-BrokerSite -ReuseMachinesWithoutShutdownInOutageAllowed $true
```

```
Set-BrokerDesktopGroup -Name "<Delivery Group Name>"- ReuseMachinesWithoutShutdow
 $true
```

3. Si le service Broker a été configuré pour utiliser des ports VDA, StoreFront ou StoreFront TLS personnalisés, effectuez les opérations suivantes pour vous assurer que le service haute disponibilité (HA) est également configuré avec les ports personnalisés corrects.

   - Vérifiez les paramètres de port du Service Broker en cours sur chaque Broker en exécutant la commande suivante :`%programfiles%\Citrix\Broker\Service\BrokerService.exe -show`

     ```
     C:\Program Files\Citrix\Broker\Service>BrokerService.exe -show
     SDK Port: 80
     VDA Port: 80
     StoreFront Port: 80
     StoreFront TLS Port: 443
     Log File:
     ```

   - Vérifiez les paramètres de port de service HA actuels sur chaque Broker en exécutant la commande suivante :`%programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -show`

     ```
     C:\Program Files\Citrix\Broker\Service>HighAvailabilityService.exe -show
     SDK Port: 89
     VDA Port: 80
     StoreFront Port: 80
     StoreFront TLS Port: 443
     Log File:
     ```

   - Si les ports VDA, StoreFront ou StoreFront TLS répertoriés pour le service HA ne correspondent pas au service Broker, utilisez les commutateurs de ligne de commande appropriés répertoriés ci-dessous pour définir les paramètres de port du service HA afin qu'ils correspondent en conséquence.

```
1 %programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
     VdaPort <port>
2 %programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
     StoreFrontPort <port>
```



```
%programfiles%\Citrix\Broker\Service\HighAvailabilityService.exe -
    StoreFrontTlsPort <port>
<!--NeedCopy-->
```

```
C:\Program Files\Citrix\Broker\Service>HighAvailabilityService.exe -VdaPort 80
Stopping service: CitrixHighAvailabilityService
Starting service: CitrixHighAvailabilityService
Command completed successfully
```

> **Remarque :**
> Il est prévu que le port SDK soit différent entre le service Broker et le service HA.
>
> Lors de la modification du port StoreFront du service Broker, le port StoreFront du service HA sera mis à jour pour correspondre automatiquement. Toutefois, le service recevant la mise à jour automatique devra toujours être redémarré manuellement pour commencer à utiliser le nouveau port.

4. Lors d'une panne, le courtier secondaire élu gérera toutes les connexions. Lorsque la panne commence, le courtier secondaire ne dispose pas de données d'enregistrement VDA actuelles, mais dès qu'un VDA communique avec lui, un processus de réenregistrement est déclenché. Au cours de ce processus, le courtier secondaire obtient également des informations de session actuelles sur ce VDA. Pour accélérer le réenregistrement des VDA de l'intervalle de 5 minutes par défaut à un intervalle de 1 minute, ce paramètre doit être appliqué à tous les contrôleurs du site.

   ```
   New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
   HeartbeatPeriodMs -PropertyType DWORD -Value 60000
   ```

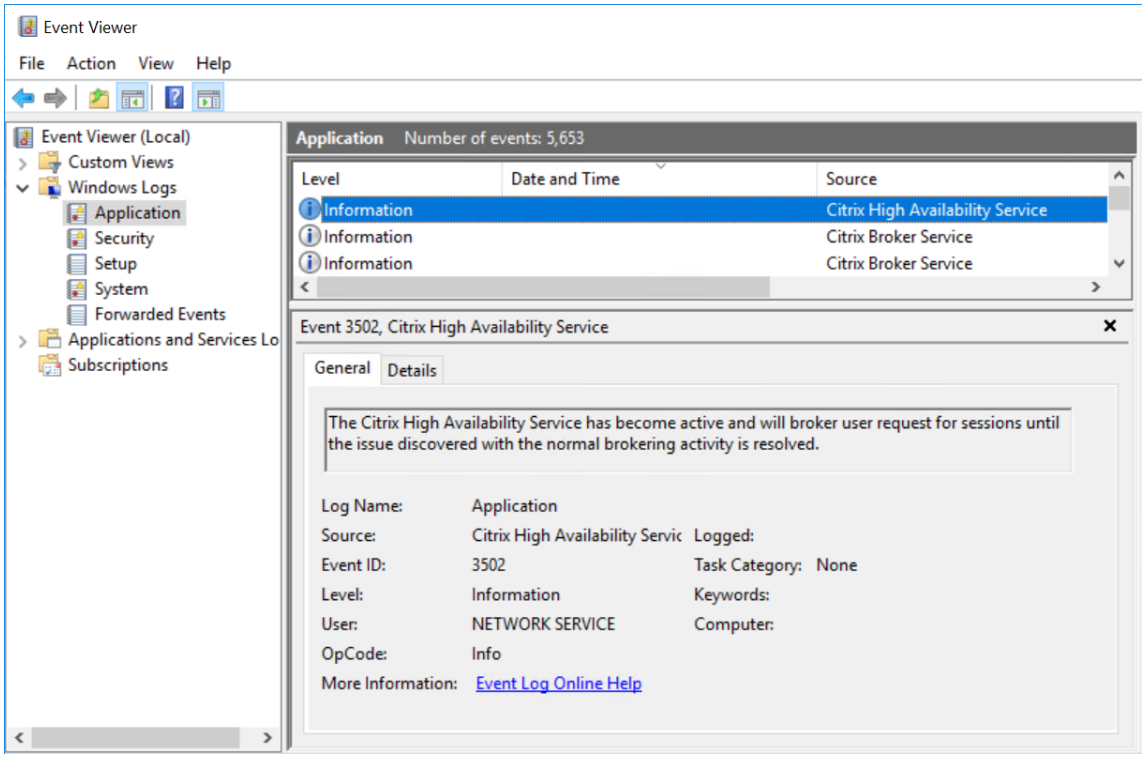
5. Pour surveiller les réenregistrements de VDA, lancez Citrix Studio et cliquez sur le nœud **Configuration > Controllers** et affichez le nombre de VDA enregistrés auprès des courtiers principaux. Laissez Citrix Studio ouvert pour voir le nombre de VDA tomber à zéro au fur et à mesure que les VDA s'enregistrent à nouveau auprès du courtier secondaire élu pendant la panne. Veuillez noter que vous ne pouvez pas utiliser Citrix Studio pour afficher le nombre de VDA enregistrés auprès du courtier secondaire.

6. Pour forcer la panne et passer en mode LHC, modifiez le registre de chaque Delivery Controller.

   ```
   New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
   OutageModeForced -PropertyType DWORD -Value 1
   ```

7. Pour déterminer si la panne a été déclenchée et que chaque courtier principal est entré en mode LHC, accédez au nœud Application des journaux d'événements sur chaque contrôleur et recherchez l'événement suivant à partir du service de haute disponibilité Citrix.

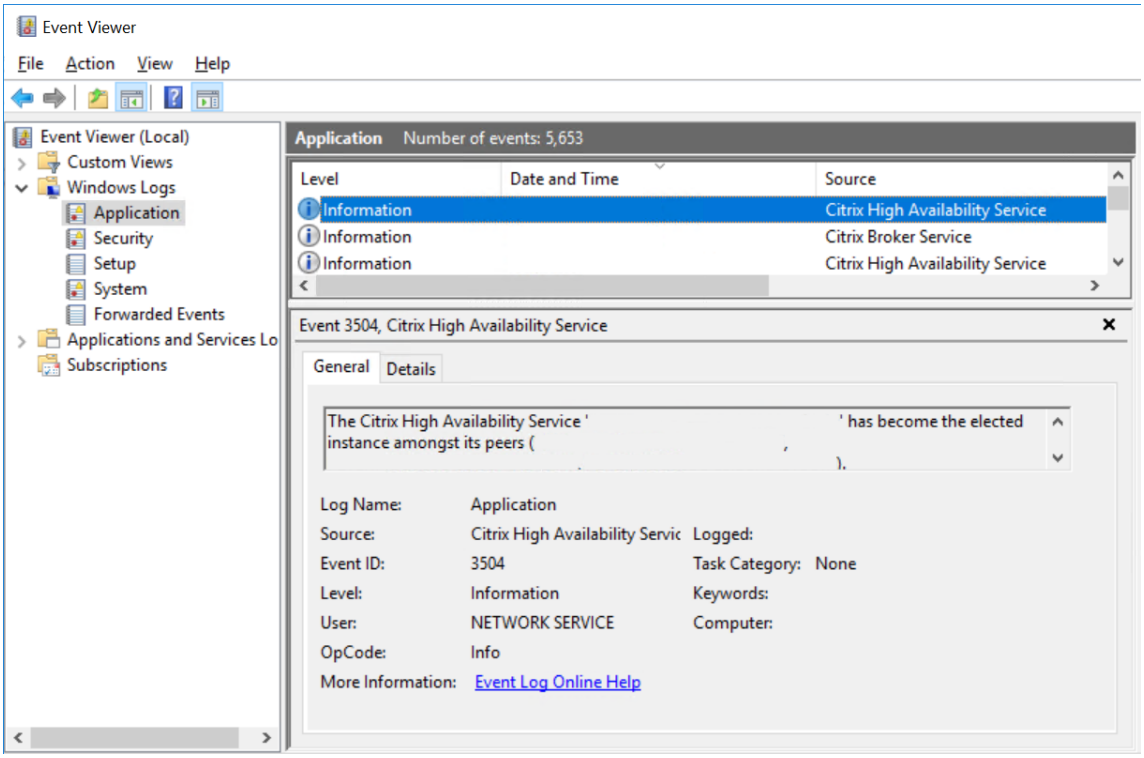
   3502 : Le service de haute disponibilité Citrix est devenu actif et courtier les demandes des utilisateurs pour les sessions jusqu'à ce que le problème détecté avec l'activité de courtage normale soit résolu.



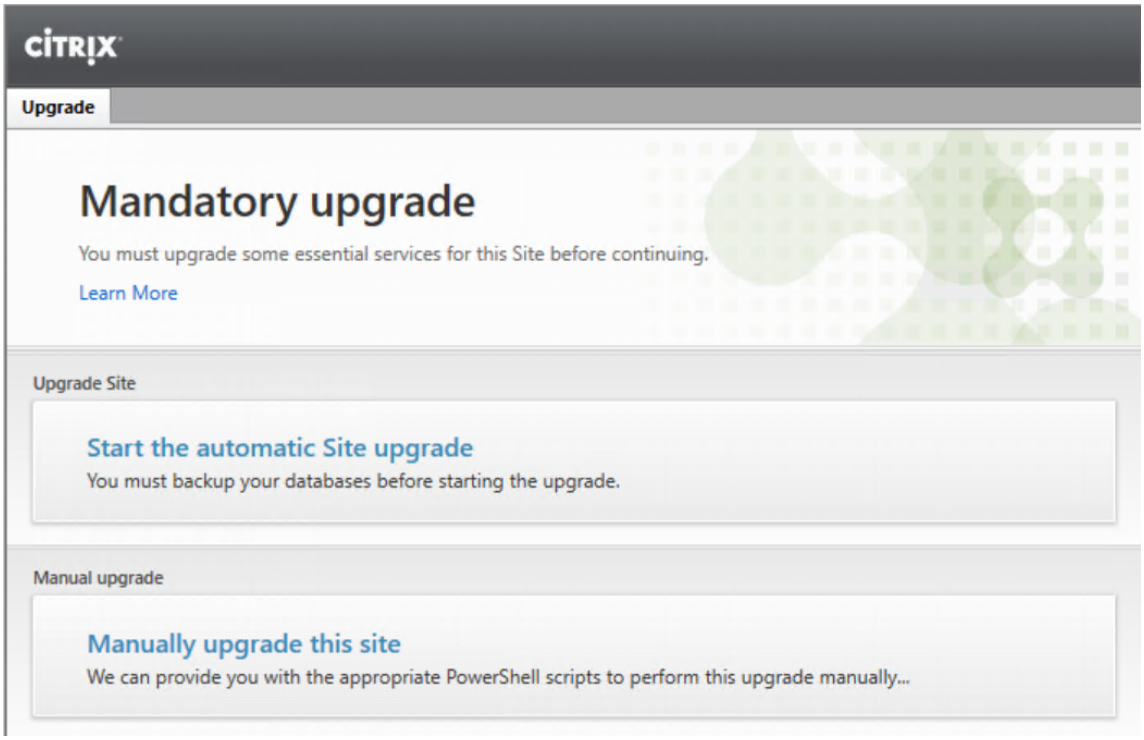
8. Vérifiez que tous les VDA se sont réenregistrés auprès du courtier secondaire élu en actualisant le nœud Controllers dans Citrix Studio. Tous les VDA se sont probablement réenregistrés lorsque les courtiers principaux n'affichent aucun VDA enregistré.

9. Les courtiers secondaires utilisent la liste alphabétique des noms de domaine complets des machines sur lesquelles ils s'exécutent pour déterminer (choisir) quel courtier secondaire sera chargé des opérations de courtage dans la zone en cas de panne. Pour confirmer quel courtier secondaire a été choisi, recherchez l'événement suivant à partir du service de haute disponibilité Citrix dans les journaux d'application d'événements Windows.

   3504 : Le « FQDN du contrôleur élu » Citrix High Availability Service est devenu l'instance élue parmi ses homologues (*liste des FQDN du contrôleur homologue*).



10. Choisissez l'un des contrôleurs homologues non sélectionnés et effectuez la mise à niveau du produit sur le contrôleur non sélectionné.
11. À partir du contrôleur récemment mis à niveau, lancez Citrix Studio et effectuez la mise à niveau obligatoire du site, y compris la mise à niveau de la base de données.



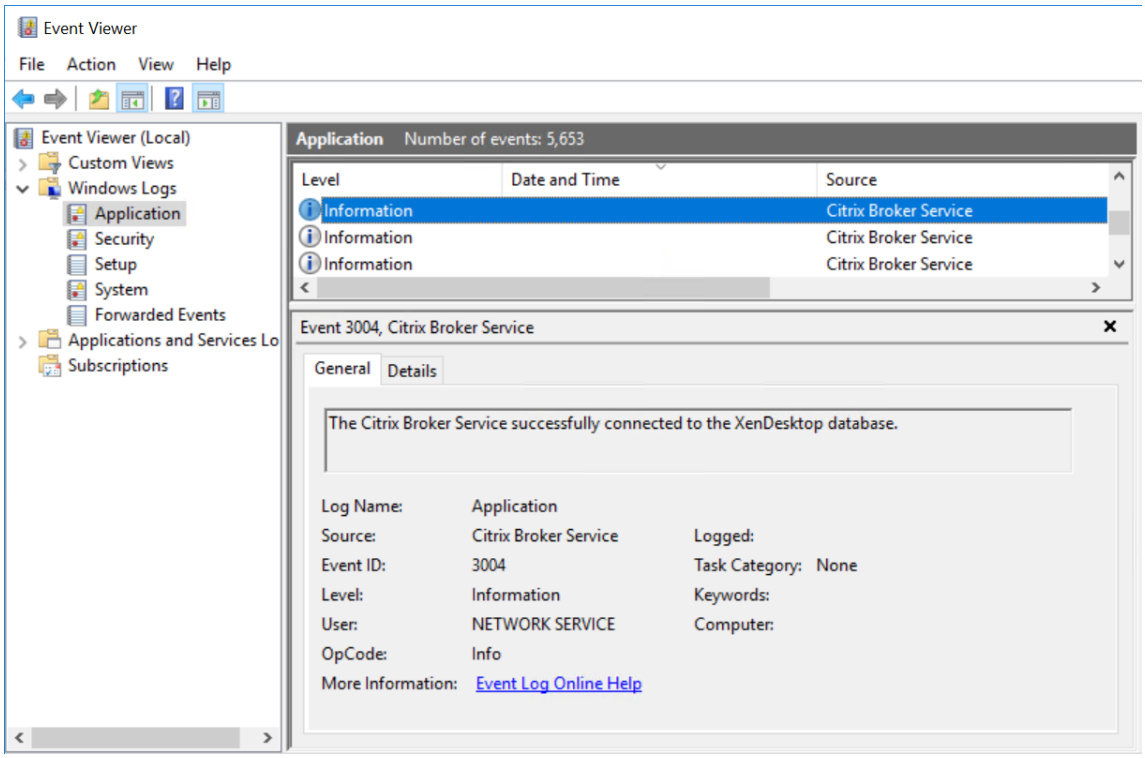
12. Effectuez des mises à niveau de produits sur les contrôleurs homologues non sélectionnés restants. Assurez-vous de ne pas perturber le contrôleur élu qui gère toujours toutes les connexions nouvelles et actives dans l'environnement.

13. Une fois que tous les contrôleurs non sélectionnés ont été mis à niveau, il est temps de sortir le site de la panne et de quitter le mode LHC. Pour supprimer le déclencheur de panne forcée, modifiez le Registre de chaque Controller. La clé peut également être supprimée si vous préférez.

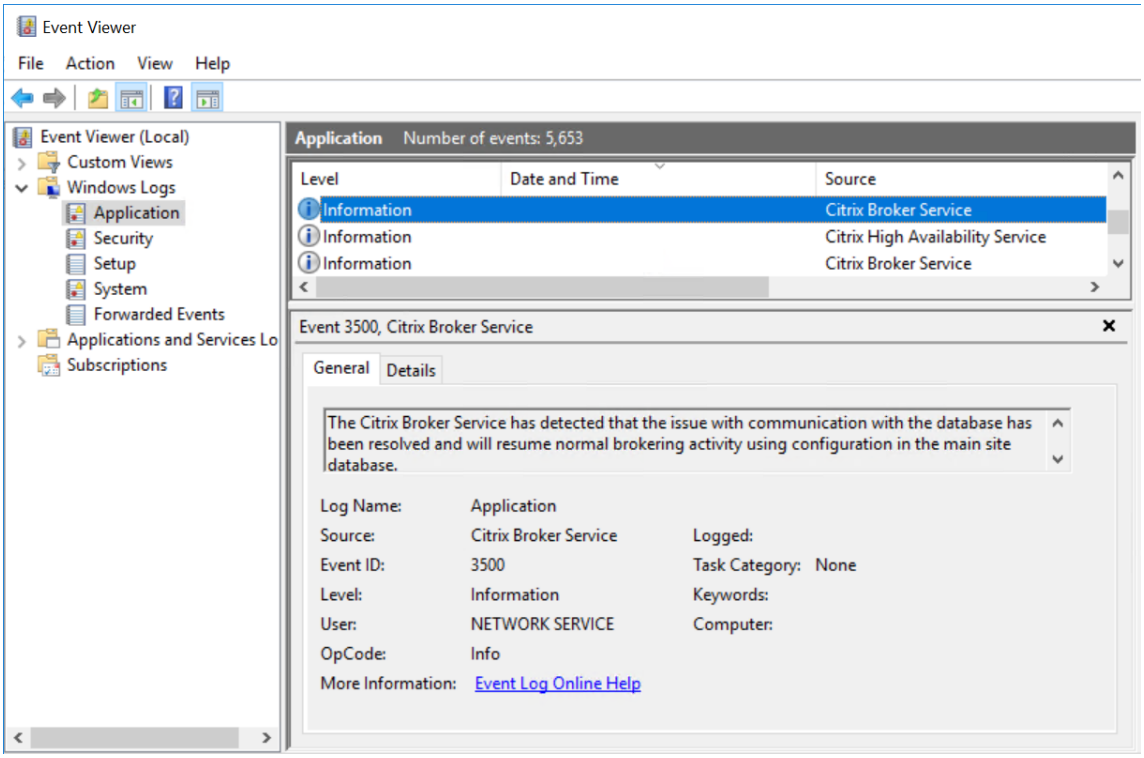
    ```
    Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer\LHC -Name
    OutageModeForced -Value 0
    ```

14. Pour confirmer si le site est hors du mode de panne, recherchez sur chaque contrôleur les événements suivants à partir du service Citrix Broker dans le journal des événements Application.

    3004 : Le service Citrix Broker s'est correctement connecté à la base de données XenDesktop.



    3500 : Le service Citrix Broker a détecté que le problème de communication avec la base de données a été résolu et reprendra l'activité de courtage normale en utilisant la configuration dans la base de données du site principale.



15. Actualisez le nœud Controllers à partir de Citrix Studio pour regarder les VDA s'enregistrer à nouveau auprès des Controller mis à niveau. Vérifiez que tous les VDA se sont réenregistrés correctement.
16. Effectuez la mise à niveau du produit sur le dernier contrôleur restant qui a servi de courtier secondaire élu pendant la panne.
17. Réglez l'intervalle d'enregistrement du VDA à la valeur par défaut de 5 minutes en modifiant le Registre sur chaque Controller (la clé peut également être supprimée si vous préférez).

    ```
    Set-ItemProperty -Path HKLM:\SOFTWARE\Citrix\DesktopServer -Name
    HeartbeatPeriodMs -PropertyType DWORD -Value 300000
    ```

18. Utilisez les applets de commande suivantes si vous souhaitez revenir au comportement par défaut des groupes de mise à disposition gérés par l'alimentation.

    ```
    1 Set-BrokerSite  -ReuseMachinesWithoutShutdownInOutageAllowed
        $false
    2 Set-BrokerDesktopGroup -Name "<Delievery Group Name>" -
        ReuseMachinesWithoutShutdownInOutage $false
    3 <!--NeedCopy-->
    ```

La mise à niveau sans interruption de service utilisant le cache hôte local doit maintenant être terminée.

envoyé par Roman Siryk, Sr. Product Dev Manager et Joseph Wu, Sr. Ingénieur Qualité

Connexion à l'infrastructure Citrix via RDP via un hôte Linux Bastion dans AWS

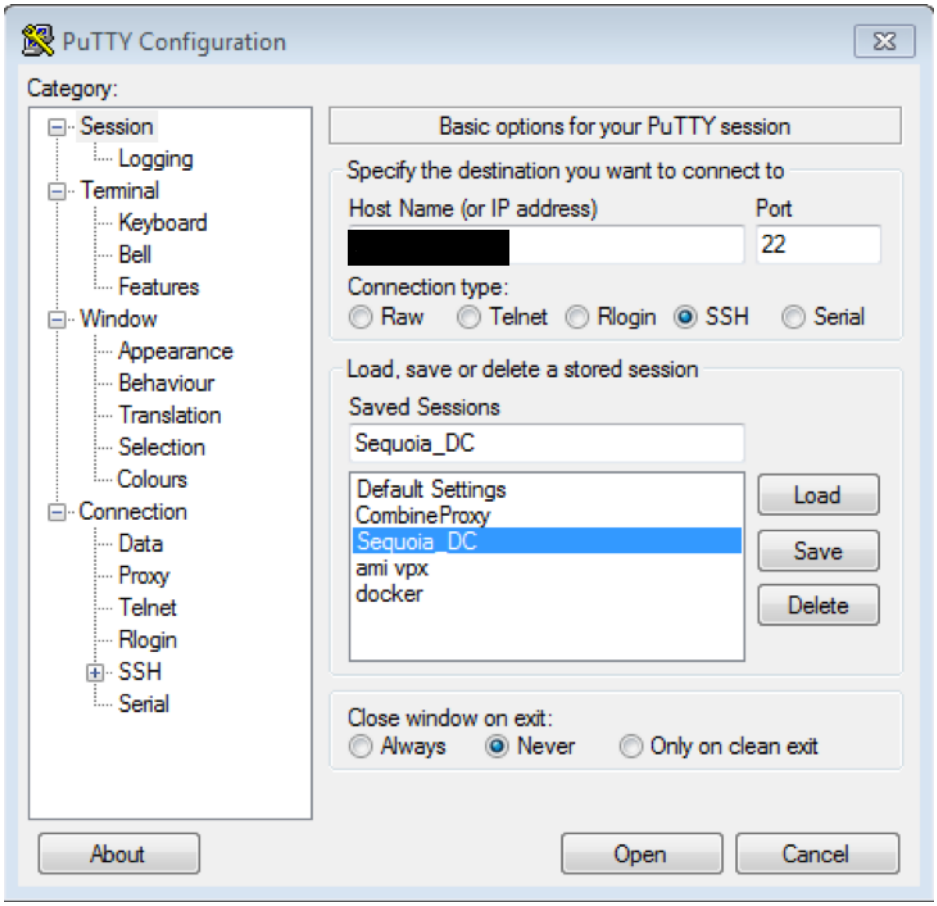
May 22, 2019

Lors de la configuration d'un environnement Citrix Virtual Apps and Desktops dans AWS, il est important de garder à l'esprit les considérations de sécurité. Un hôte bastion est couramment utilisé pour renforcer la sécurité et la séparation entre les réseaux externes et internes, et est généralement une instance Linux dépouillée qui héberge un serveur proxy. Pour les implémentations Citrix dans AWS, un administrateur peut avoir accès à l'hôte bastion, mais aucun accès réseau direct à l'infrastructure Citrix. Comme l'infrastructure Citrix est composée d'instances Windows et comprend un méta-installateur basé sur l'interface graphique, la connectivité via un hôte bastion basé sur Linux devient un problème.

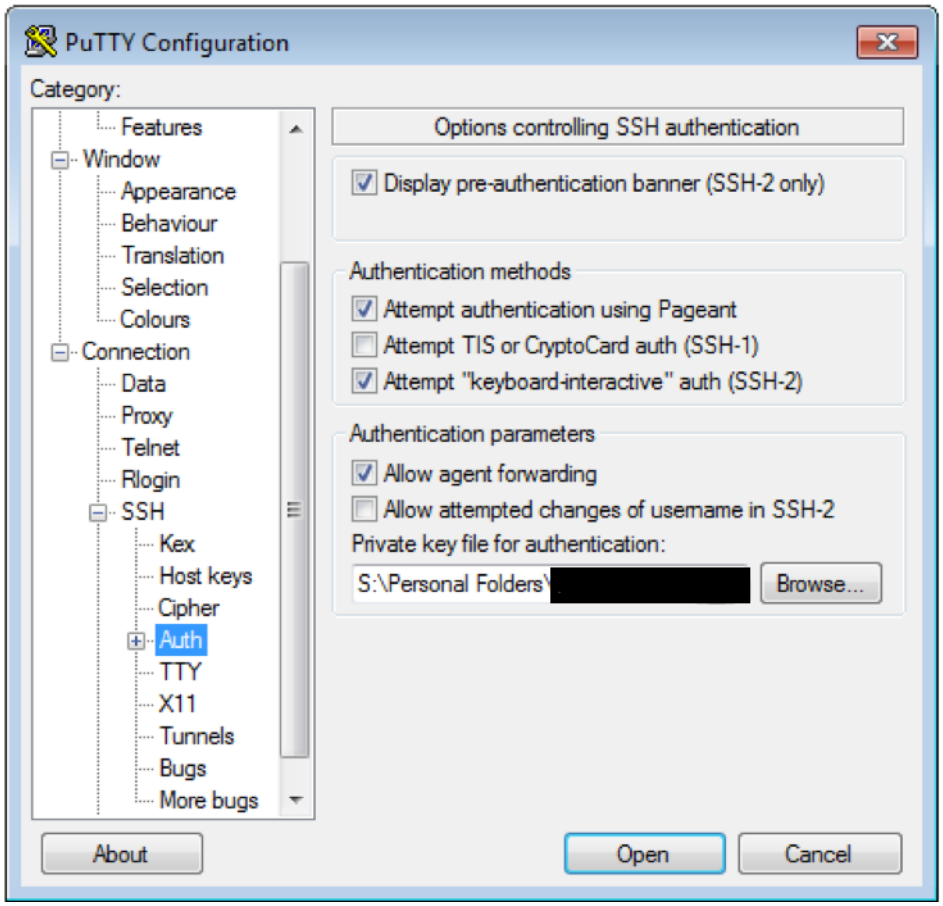
La connexion à une instance Linux dans AWS via un hôte bastion est aussi simple que PuTTY au bastion et SSH dans l'instance souhaitée. Pour créer une session RDP vers une instance Windows via un hôte bastion est possible en utilisant le transfert de port. Le transfert de port est le reprogrammation de l'adresse IP de destination et d'un numéro de port. Il rend les services sur un réseau protégé disponibles du côté opposé d'une passerelle, tel qu'un routeur. Dans ce cas, utilisez le transfert de port pour mapper votre port local au port RDP sur l'instance souhaitée en créant un tunnel dans votre utilitaire SSH/Tunneling préféré.

Par exemple, dans la console PuTTY, créez une session SSH. Entrez l'adresse IP publique de l'hôte bastion, fournissez la clé privée dans la section **Auth** , puis créez un tunnel. Le port source du tunnel doit être un port local inutilisé, tel que localhost 5000 et plus. L'adresse IP est l'adresse IP de l'hôte de destination (l'instance Windows que vous essayez d'atteindre) avec le port RDP ajouté (3389). Assurez-vous d'enregistrer vos configurations. Connectez-vous à l'hôte du bastion et connectez-vous. Ensuite, démarrez une session RDP pour votre port local.

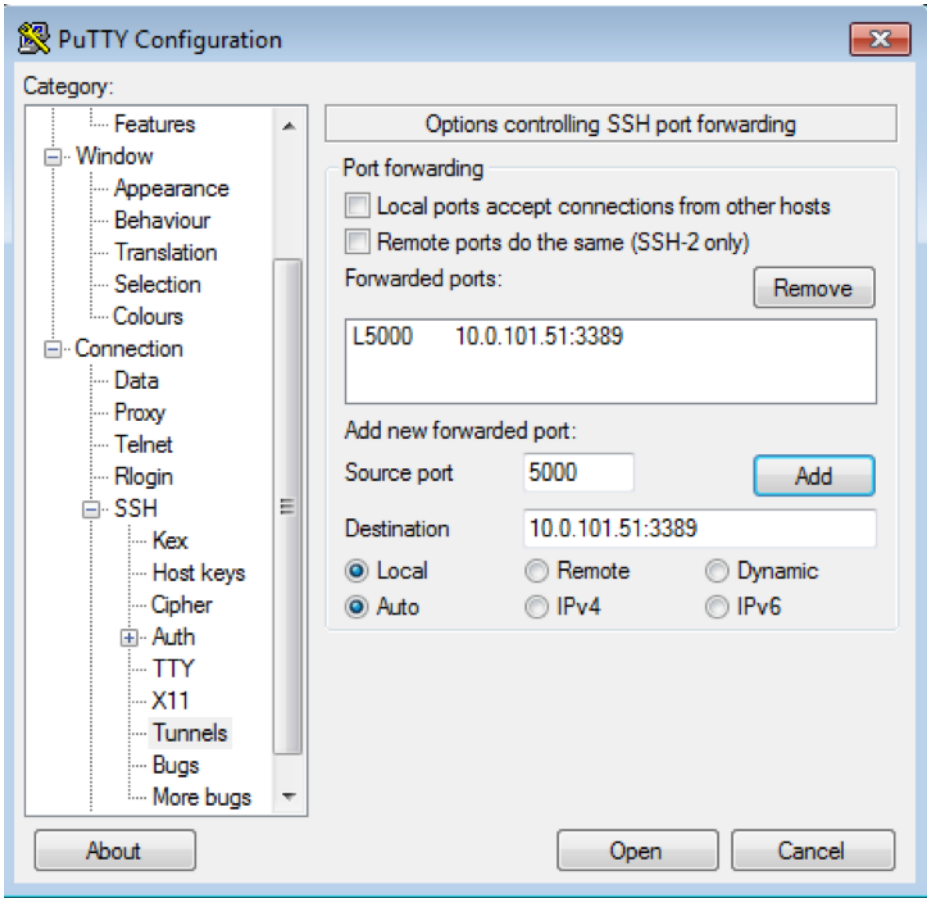
Définissez le nom d'hôte ou l'adresse IP publique de l'hôte bastion.



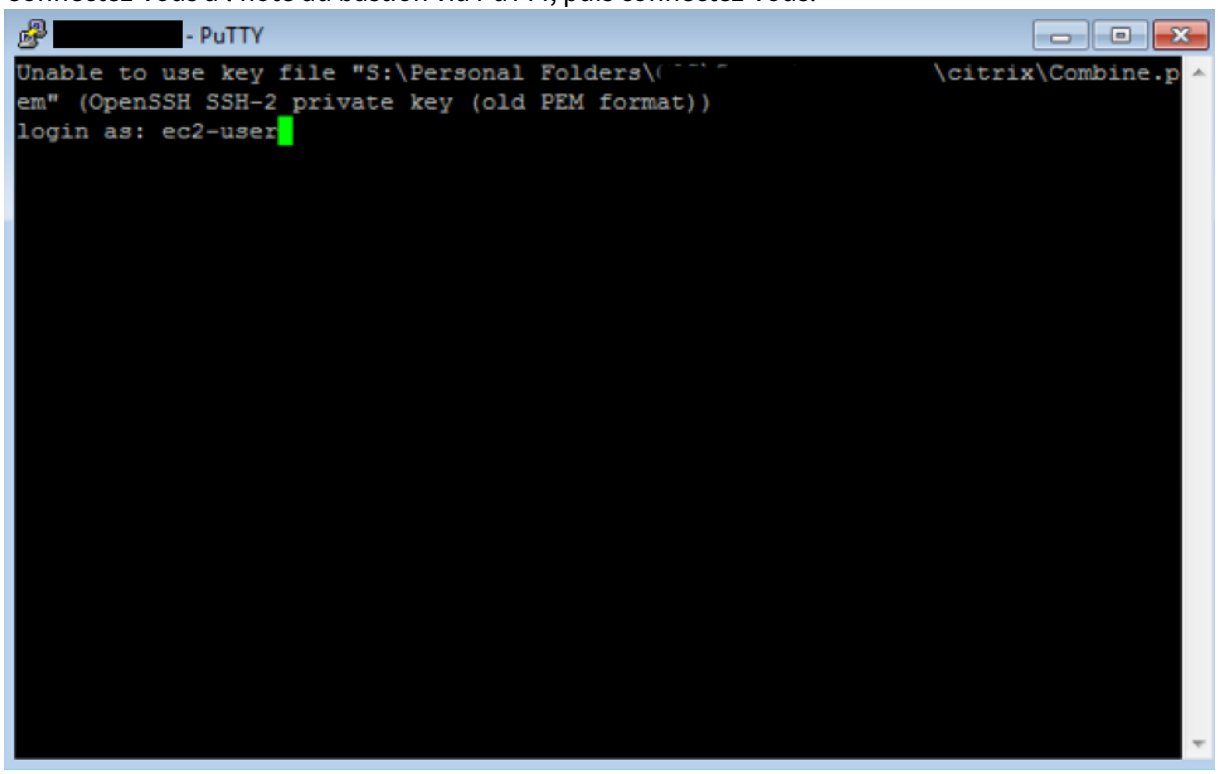
Dans **SSH > Auth**, définissez le fichier de clé privée au format .ppk.



Dans **SSH > Tunnels**, ajoutez le nouveau port transféré. Le **port source** doit être le port inutilisé arbitraire et la **destination** doit être l'adresse IP du serveur de destination derrière l'hôte bastion, avec le port RDP ajouté. Dans le champ **Port source** , cliquez sur **Ajouter** pour connecter un nouveau port transféré.



Connectez-vous à l'hôte du bastion via PuTTY, puis connectez-vous.



Démarrez une session RDP à l'aide de l'hôte local pour atteindre le serveur de destination.

envoyé par Jill Fetscher, Citrix Principal Consultant

Guide de déploiement de zone privée DNS de Citrix ADC pour Azure

January 8, 2020

Introduction

Citrix ADC, anciennement connu sous le nom de NetScaler, est un produit de classe mondiale dans l'espace de contrôleur de mise à disposition d'applications (ADC) avec la capacité éprouvée d'équilibrer la charge, de gérer le trafic global, de compression et de sécuriser les applications.

Azure DNS est un service sur l'infrastructure Microsoft Azure pour héberger des domaines DNS et fournir la résolution de noms.

Azure DNS Private Zones est un service axé sur la résolution des noms de domaine dans un réseau privé. Avec Private Zones, les clients peuvent utiliser leurs propres noms de domaine personnalisés plutôt que les noms fournis par Azure disponibles aujourd'hui.

Généralités sur Azure DNS

Le système de noms de domaine, ou DNS, est responsable de la traduction (ou de la résolution) d'un nom de service à son adresse IP. Service d'hébergement pour les domaines DNS, Azure DNS fournit la résolution de noms à l'aide de l'infrastructure Microsoft Azure. Outre la prise en charge des domaines DNS orientés vers Internet, Azure DNS prend désormais en charge les domaines DNS privés.

Azure DNS fournit un service DNS fiable et sécurisé pour gérer et résoudre les noms de domaine dans un réseau virtuel sans avoir besoin d'une solution DNS personnalisée. En utilisant des zones DNS privées, vous pouvez utiliser vos propres noms de domaine personnalisés plutôt que les noms fournis par Azure disponibles aujourd'hui. L'utilisation de noms de domaine personnalisés vous aide à adapter votre architecture de réseau virtuel au mieux aux besoins de votre organisation. Il fournit la résolution de noms pour les machines virtuelles (VM) au sein d'un réseau virtuel et entre les réseaux virtuels. En outre, les clients peuvent configurer des noms de zones avec une vue à horizon divisé, ce qui permet à une zone DNS privée et publique de partager un nom.

Pourquoi Citrix GSLB pour Azure DNS zone privée ?

Dans le monde d'aujourd'hui, les entreprises souhaitent faire passer leurs charges de travail du cloud local au cloud Azure. La transition vers le cloud leur permet de tirer parti du temps de mise sur le marché, des dépenses en capital et des prix, de la facilité de déploiement et de la sécurité. Le service de zone privée Azure DNS fournit une proposition unique pour les entreprises qui transitent une partie de leurs charges de travail vers le cloud Azure. Ces entreprises peuvent créer leur nom DNS privé, qu'elles possédaient pendant des années dans des déploiements sur site, lorsqu'elles utilisent le service de zone privée. Avec ce modèle hybride de serveurs d'applications intranet dans le cloud Azure connectés via des tunnels VPN sécurisés, le seul défi est de savoir comment un utilisateur peut avoir un accès transparent à ces applications intranet. Citrix ADC résout ce cas d'utilisation unique avec sa fonctionnalité d'équilibrage de charge globale, qui achemine le trafic d'application vers les charges de travail/serveurs distribués les plus optimales, sur site ou sur le cloud Azure, et fournit l'état d'intégrité du serveur d'applications.

Cas d'utilisation

Les utilisateurs du réseau sur site et de différents réseaux virtuels Azure doivent pouvoir se connecter aux serveurs les plus optimaux d'un réseau interne pour accéder au contenu requis. Cela garantit que l'application est toujours disponible, le coût optimisé et l'expérience utilisateur est bonne. La gestion privée du trafic (PTM) Azure est la principale exigence ici. Azure PTM garantit que les requêtes DNS des utilisateurs se résolvent à une adresse IP privée appropriée du serveur d'applications.

Solution de cas d'utilisation

Citrix ADC inclut la fonctionnalité d'équilibrage de charge serveur global (GSLB), qui peut aider à répondre à la demande Azure PTM. GSLB agit comme un serveur DNS, qui obtient les requêtes DNS et résout la requête DNS en une adresse IP appropriée pour fournir :

- Basculement DNS transparent
- Migration progressive de locaux vers le cloud

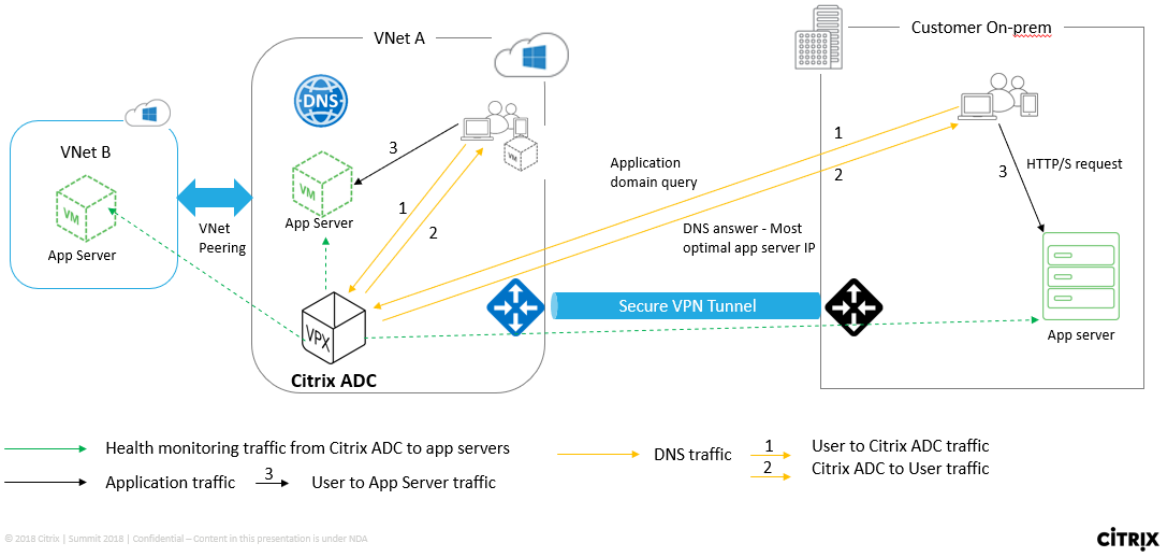
- A/B Test d'une nouvelle fonctionnalité

Parmi les nombreuses méthodes d'équilibrage de charge prises en charge, les méthodes suivantes peuvent être utiles dans cette solution :

1. Round Robin
2. Proximité statique (sélection de serveur basée sur l'emplacement) : Il peut être déployé de deux façons
   a) GSLB basé sur le sous-réseau client EDNS (ECS) sur Citrix ADC
   b) Déployer un redirecteur DNS pour chaque réseau virtuel

Topologie

- Le déploiement Citrix ADC GSLB pour la zone DNS privée Azure semble logiquement illustré à la Figure 1.



- Un utilisateur peut accéder à n'importe quel serveur d'applications sur Azure ou sur site basé sur Citrix ADC GSLB méthode d'équilibrage de charge dans une zone DNS privée Azure
- Tout le trafic entre le réseau virtuel sur site et Azure est via un tunnel VPN sécurisé uniquement
- Le trafic d'application, le trafic DNS et le trafic de surveillance sont affichés dans la topologie précédente.
- Selon la redondance requise, Citrix ADC et le redirecteur DNS peuvent être déployés dans les réseaux virtuels et les datacenters. Pour des raisons de simplicité, un seul Citrix ADC est affiché ici, mais nous recommandons au moins un ensemble de redirecteurs ADC et DNS Citrix pour la région Azure.
- Toutes les requêtes DNS utilisateur vont d'abord au redirecteur DNS qui a des règles définies pour transférer les requêtes vers le serveur DNS approprié.

Configuration de Citrix ADC pour Azure DNS Private Zone

Produits et Versions testés

Produit	Version
Azure	Abonnement Cloud
Citrix ADC VPX	BYOL (Apportez votre propre licence)

> **Remarque :** le déploiement est testé et reste le même avec Citrix ADC version 12.0 et supérieure.

Prérequis et notes de configuration

Voici les conditions préalables générales et la configuration testée pour ce guide. Veuillez effectuer une vérification croisée avant de configurer Citrix ADC :

- Compte portail Microsoft Azure avec un abonnement valide
- Assurez la connectivité (Secure VPN Tunnel) entre le cloud sur site et Azure. Pour configurer un tunnel VPN sécurisé dans Azure, consultez Étape par étape : Configuration d'une passerelle VPN site à site entre Azure et local

Description de la solution

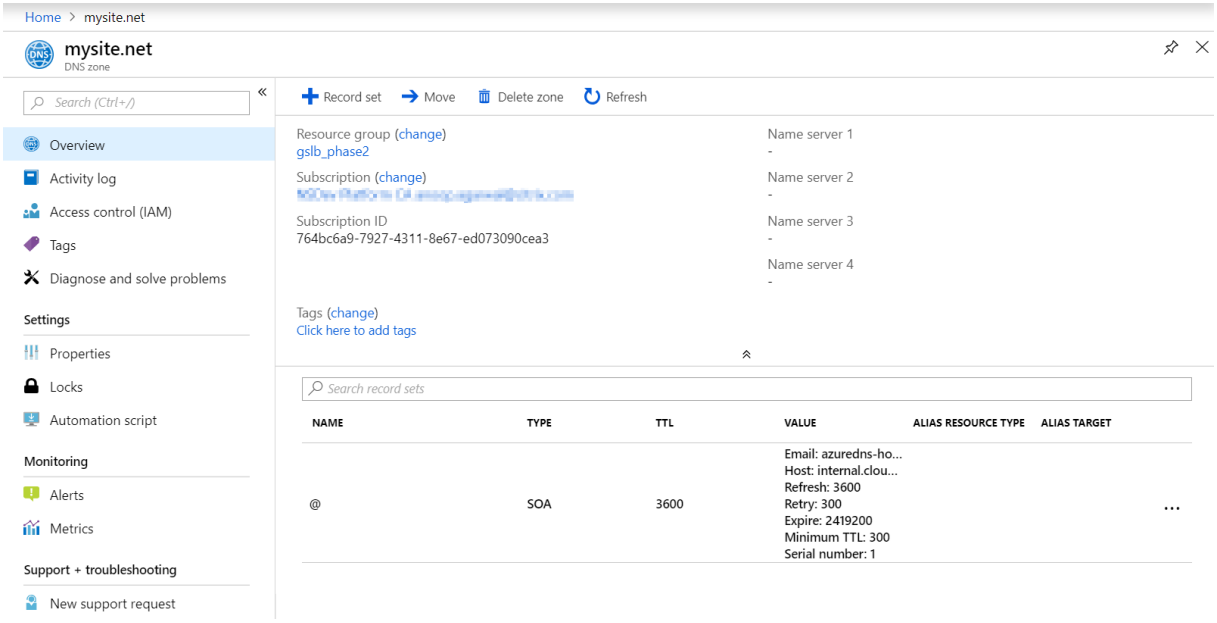
Supposons que le client souhaite héberger une application Azure DNS zone privée (rr.ptm.mysite.net) qui s'exécute sur HTTPS et est déployée sur Azure et sur site avec un accès intranet basé sur la méthode d'équilibrage de charge GSLB round robin. Pour réaliser ce déploiement en activant la zone DNS privée de GSLB pour Azure avec Citrix ADC se compose de deux parties : la configuration de l'appliance Azure, sur site et Citrix ADC.

Partie 1 : Configuration d'Azure, installation locale

Comme indiqué dans Topologie, configurez Azure Virtual Network (vNet A, vNet B dans ce cas) et la configuration locale.
Étape 1 : Créer une zone DNS privée Azure avec nom de domaine (mysite.net)
Étape 2 : Créer deux réseaux virtuels (vNet A, vNet B) dans le modèle Hub et Spoke dans une région Azure
Étape 3 : Déployer App Server, DNS Forwarder, client Windows 10 Pro, Citrix ADC dans vNet A
Étape 4 : Déployer App Server et déployer un redirecteur DNS si des clients se trouvent dans vNet B
Étape 5 : Déployer le serveur d'applications, le redirecteur DNS et le client professionnel Windows 10 sur site

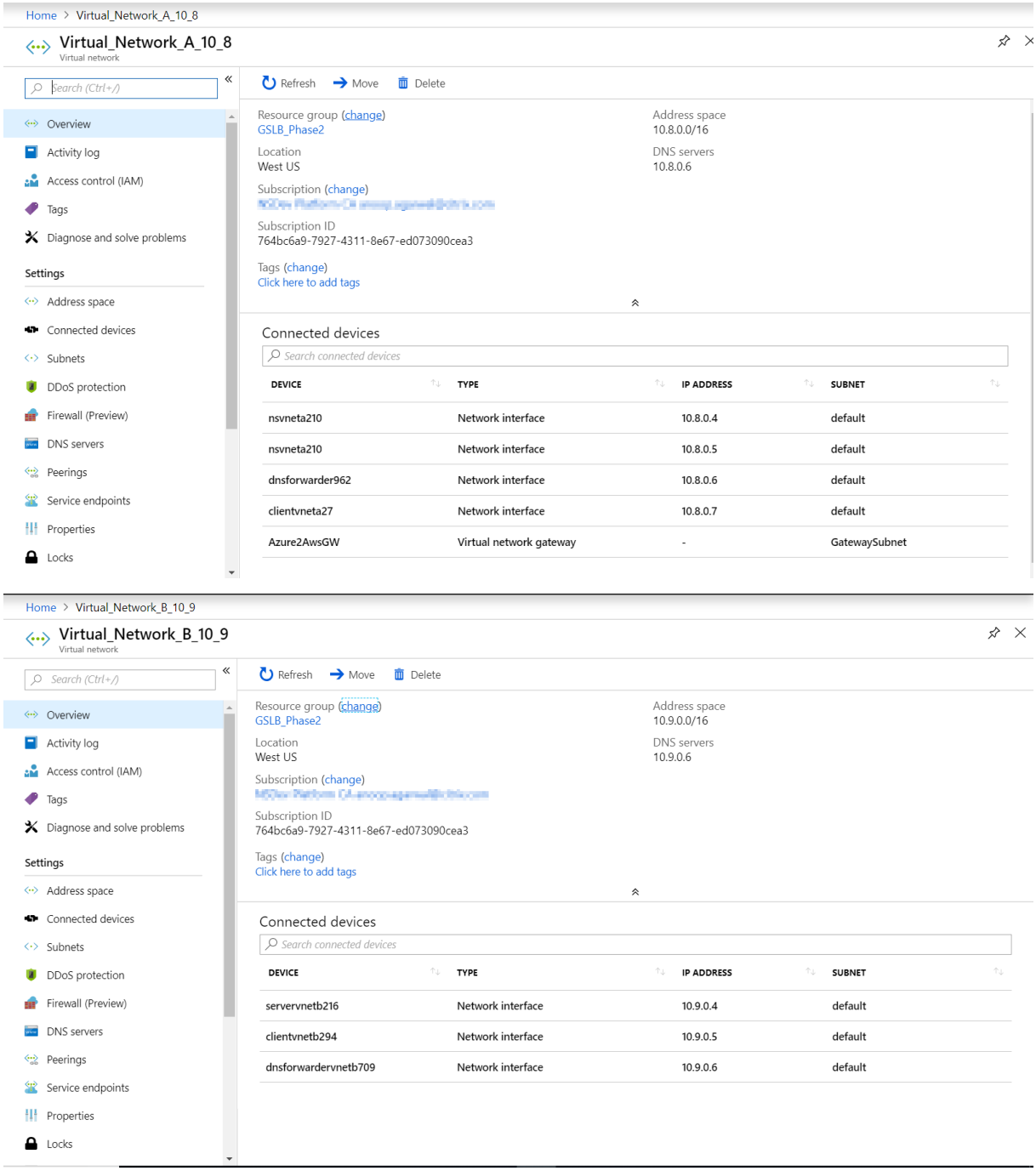
Zone DNS privée Azure

Connectez-vous au portail Azure et sélectionnez ou créez un tableau de bord. Maintenant, cliquez sur **créer une ressource et recherchez la zone DNS** pour en créer une (mysite.net dans ce cas) comme indiqué dans l'image suivante.



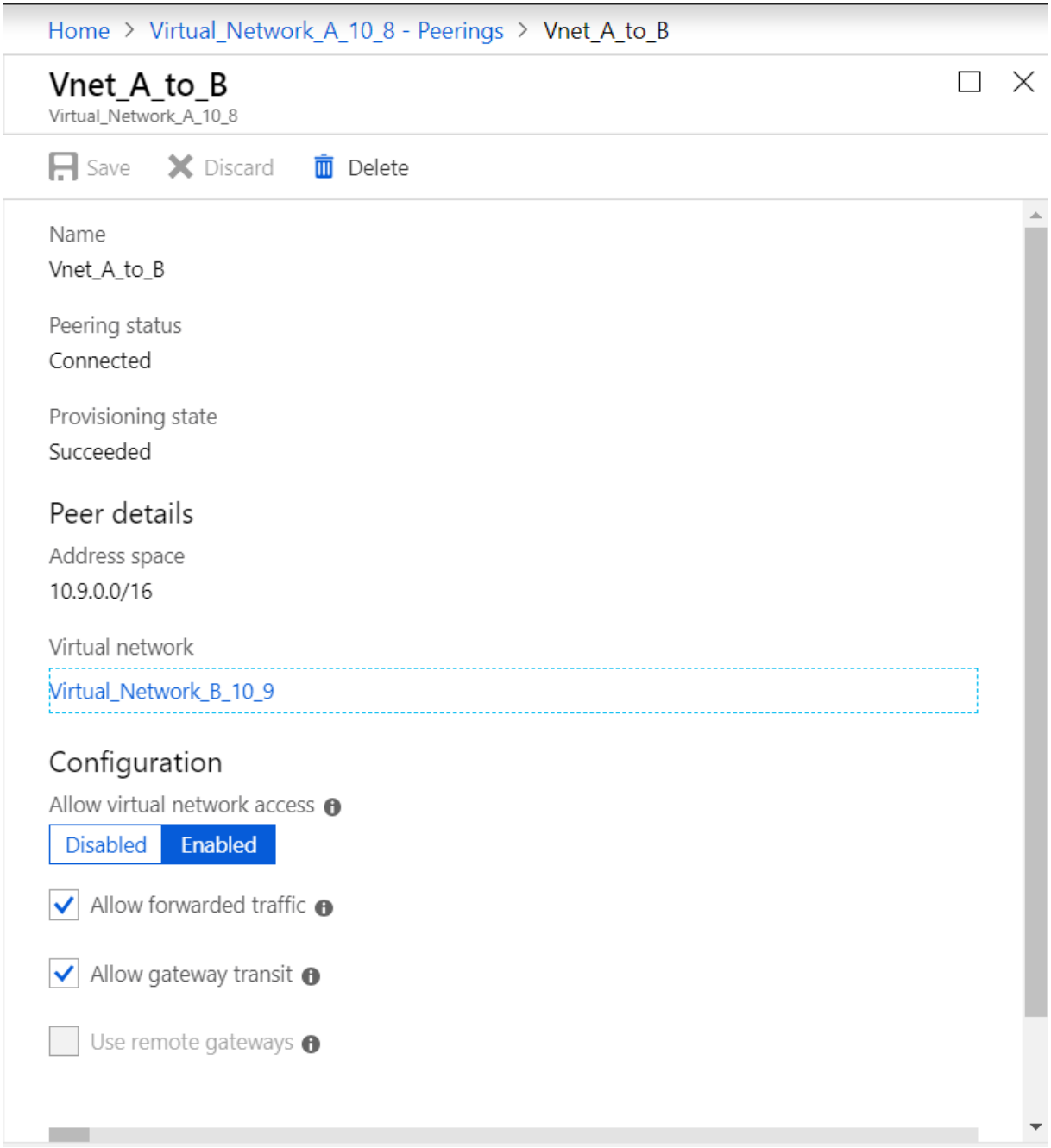
Réseaux virtuels Azure (vNet A, vNet B) dans le modèle Hub et en étoile

Sélectionnez le même tableau de bord et cliquez sur **créer une ressource et recherchez des réseaux virtuels pour** créer deux réseaux virtuels à savoir VNet A, VNet B dans la même région et les homologues pour former un modèle Hub and Spoke comme indiqué dans l'image suivante. Reportez-vous à la section Implémentation d'une topologie réseau hub spoke dans Azure pour plus d'informations sur la configuration d'une topologie concentrée et en étoile.

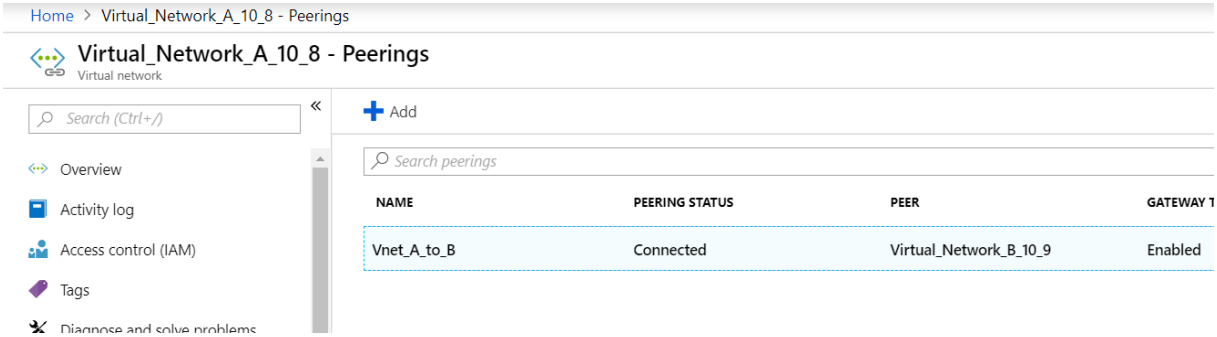


Appairage VNet A vers VNet B

Pour homologue vNet A et vNet B cliquez sur Appairages dans le menu des paramètres de vNet A et vNet B homologue, activez Autoriser le trafic transféré et Autoriser le transit de passerelle comme indiqué dans l'image suivante.

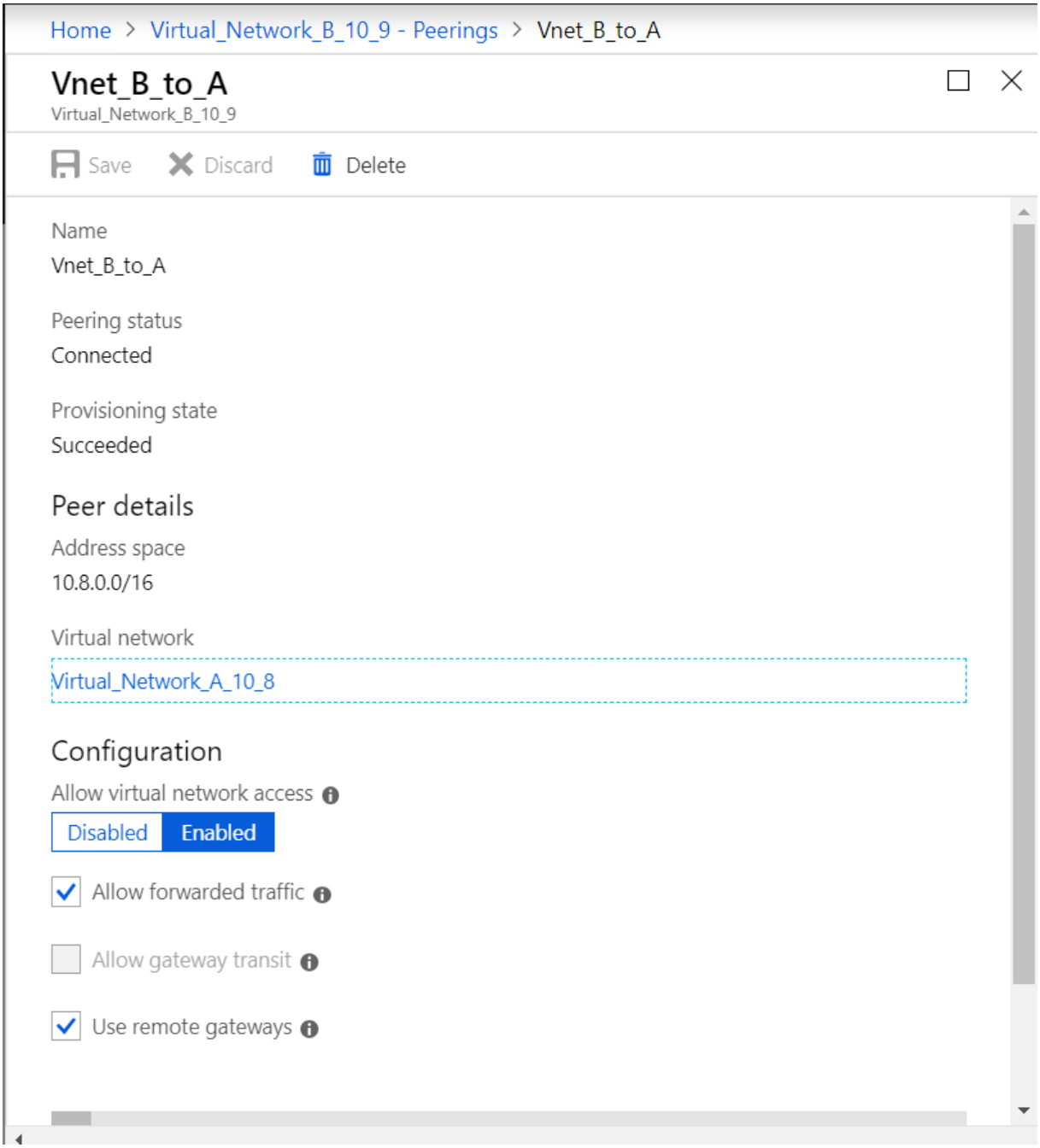


Après avoir réussi l'appairage, vous voyez comme indiqué dans l'image suivante :

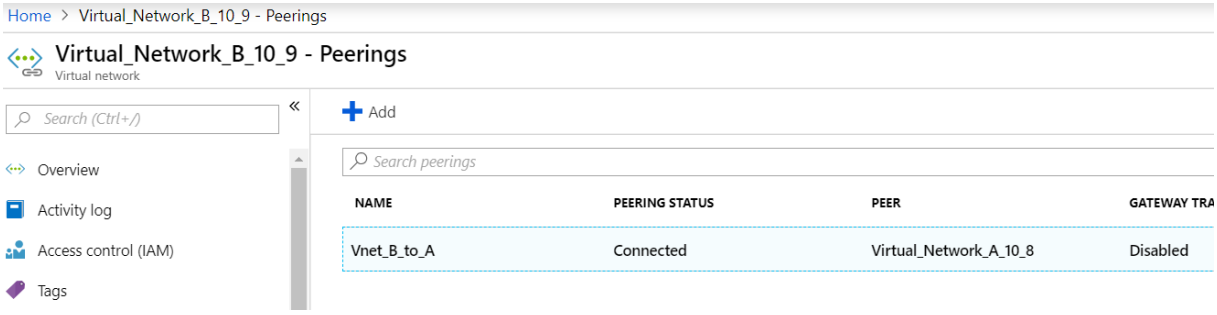


Appairage VNet B vers VNet A

Pour homologue vNet B et vNet A cliquez sur **Appairages** dans le menu des paramètres de vNet B et vNet A homologue, activez Autoriser le trafic transféré et Utiliser les passerelles distantes comme indiqué dans l'image suivante.



Après avoir réussi l'appairage, vous voyez comme indiqué dans l'image suivante :



Déployer App Server, DNS Forwarder, client Windows 10 Pro, Citrix ADC dans le vNet A

Nous discutons brièvement du serveur d'applications, du redirecteur DNS, du client Windows 10 pro et de Citrix ADC sur vNet A. Sélectionnez le même tableau de bord, cliquez sur créer une ressource, recherchez les instances respectives et attribuez une adresse IP à partir du sous-réseau vNet A

Serveur d'applications

Le serveur d'applications n'est rien d'autre que le serveur Web (serveur HTTP) où un serveur Ubuntu 16.04 est déployé en tant qu'instance sur Azure ou sur site VM et exécute une commande CLI : sudo apt install apache2 pour le faire en tant que serveur web

Client Windows 10 Pro

Lancez l'instance pro Windows 10 en tant que machine client sur vNet A et sur site aussi.

Citrix ADC

Citrix ADC complète la zone privée Azure DNA par un contrôle d'intégrité et des analyses de Citrix MAS. Lancez un Citrix ADC à partir d'Azure Marketplace en fonction de vos besoins. Ici, nous avons utilisé Citrix ADC (BYOL) pour ce déploiement. Veuillez vous référer à l'URL ci-dessous pour des étapes détaillées sur Comment déployer Citrix ADC sur Microsoft Azure. Après le déploiement, utilisez Citrix ADC IP pour configurer Citrix ADC GSLB. Voir Déployer une instance NetScaler VPX sur Microsoft Azure

Redirecteur DNS

Il est utilisé pour transférer les demandes client des domaines hébergés liés à Citrix ADC GSLB (ADNS IP) .Lancez un serveur Ubuntu 16.04 en tant qu'instance Linux (serveur Ubuntu 16.04) et reportez-vous ci-dessous URL sur la façon de le configurer en tant que redirecteur DNS.

> **Remarque :** Pour la méthode d'équilibrage de charge Round Robin GSLB, un redirecteur DNS pour la région Azure est suffisant, mais pour la proximité statique, nous avons besoin d'un redi-

> recteur DNS par réseau virtuel. Téléchargez les modèles de démarrage rapide à partir dehttps://github.com/Azure/azure-quickstart-templates/tree/master/301-dns-forwarder

Après avoir déployé redirecteur, modifiez les paramètres du serveur DNS du réseau virtuel A de la valeur par défaut à personnalisée avec l'adresse IP du redirecteur DNS vNet A comme indiqué dans l'image suivante, puis modifiez le fichier `named.conf.options` dans le redirecteur DNS vNet A pour ajouter des règles de transfert pour le domaine (mysite.net) et (ptm.mysite.net) à l'adresse IP ADNS de Citrix ADC GSLB. Maintenant, redémarrez le redirecteur DNS pour refléter les modifications apportées dans le fichier `named.conf.options`.

Paramètres du redirecteur DNS VNet A

```
zone "mysite.net" {

           type forward;
forwarders {
  168.63.129.16;  }
 ;
 }
 ;
zone "ptm.mysite.net" {

    type forward;
    forwarders {
  10.8.0.5;  }
 ;
 }
 ; > **Remarque :** Pour l'adresse IP de zone de domaine (« mysite.net »), utilisez l'adresse IP DNS de votre région Azure. Pour l'adresse IP de zone de sous-domaine (« ptm.mysite.net »), utilisez toutes les adresses IP ADNS de vos instances GSLB.
```

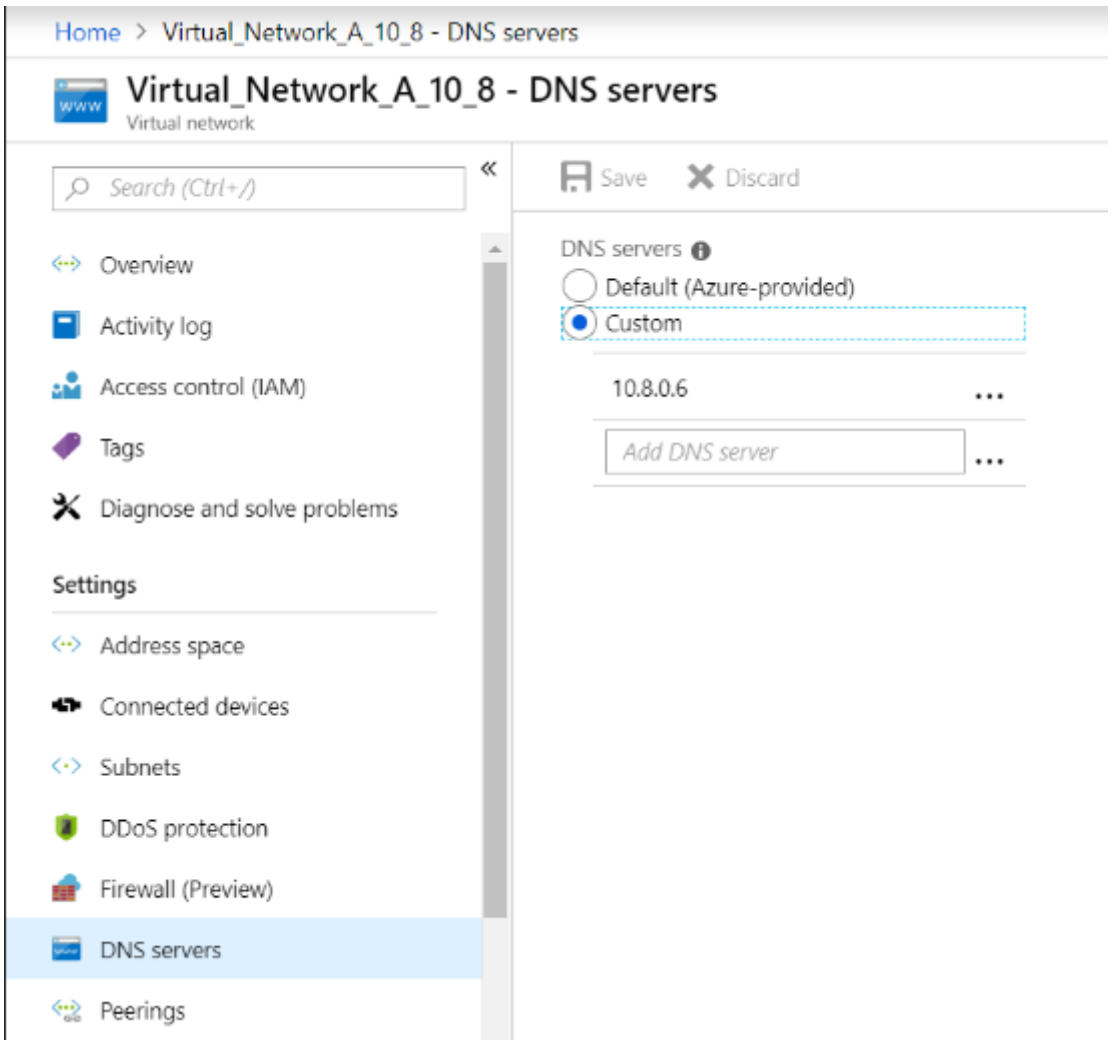
Déployer App Server et déployer un redirecteur DNS si des clients se trouvent dans le vNet B

Maintenant, pour Virtual Network B, sélectionnez le même tableau de bord, cliquez sur **créer une ressource**, puis recherchez les instances respectives et affectez une adresse IP à partir du sous-réseau VNet B. Lancez le serveur d'applications et le redirecteur DNS s'il existe un équilibrage de charge GSLB de proximité statique similaire au vNet A.
Modifiez les paramètres du redirecteur DNS VNet B`named.conf.options` comme illustré :

```
Paramétres du redirecteur DNS VNet B :
zone "ptm.mysite.net" {

```



```
    type forward;
    forwarders {
  10.8.0.5;  }
;
}
;
```



Déployer le serveur d'applications, le redirecteur DNS et le client professionnel Windows 10 sur site

Maintenant, sur site, lancez les machines virtuelles sur le nu et apportez le serveur d'applications, le redirecteur DNS et le client professionnel Windows 10 similaire à VNet A.
Modifiez les paramètres du redirecteur DNS local dans le,`named.conf.options` comme illustré dans l'exemple suivant.

Paramètres du redirecteur DNS local

```
zone "mysite.net" {

           type forward;
           forwarders {
  10.8.0.6;  }
 ;
 }
 ;
zone "ptm.mysite.net" {

    type forward;
    forwarders {
  10.8.0.5;  }
 ;
 }
 ;
```

Ici,`mysite.net` nous avons donné l'adresse IP du redirecteur DNS de vNet A au lieu de l'adresse IP du serveur de zone DNS privée Azure car il s'agit d'une adresse IP spéciale non accessible à partir de locaux. Par conséquent, cette modification est nécessaire dans le paramètre de redirecteur DNS de local.

Partie 2 : Configuration de Citrix ADC

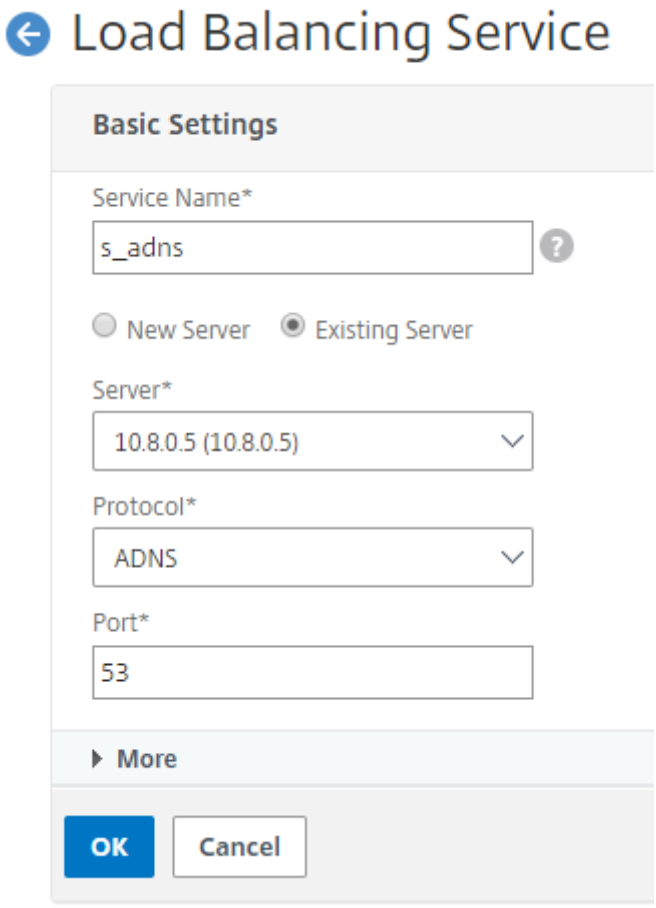
Comme indiqué dans Topologie, déployer Citrix ADC sur le réseau virtuel Azure (vNet A dans ce cas) et y accéder via l'interface graphique de Citrix ADC.

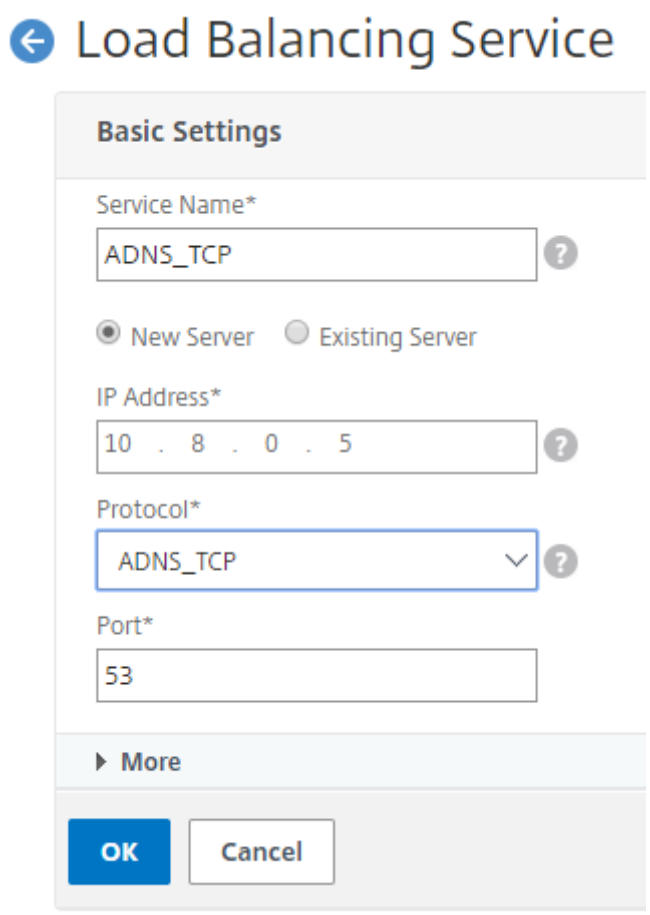
Configuration de Citrix ADC GSLB

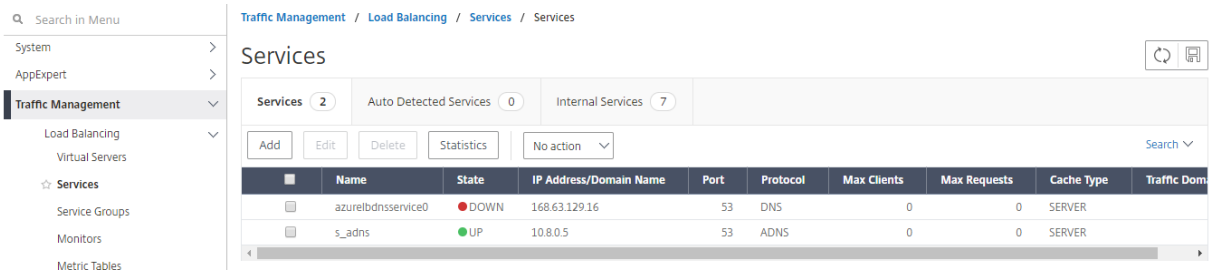
Étape 1 : Créer un service ADNS
Étape 2 : Créer des sites — local et distant
Étape 3 : Créer des services pour les serveurs virtuels locaux
Étape 4 : Créer des serveurs virtuels pour les services GSLB

Ajouter un service ADNS

Connectez-vous à l'interface graphique de Citrix ADC. Sous l'onglet **Configuration** , accédez à **Gestion du trafic > Équilibrage de charge > Services** . Ajouter un service. Il est recommandé de configurer le service ADNS à la fois dans TCP et UDP comme indiqué ici :

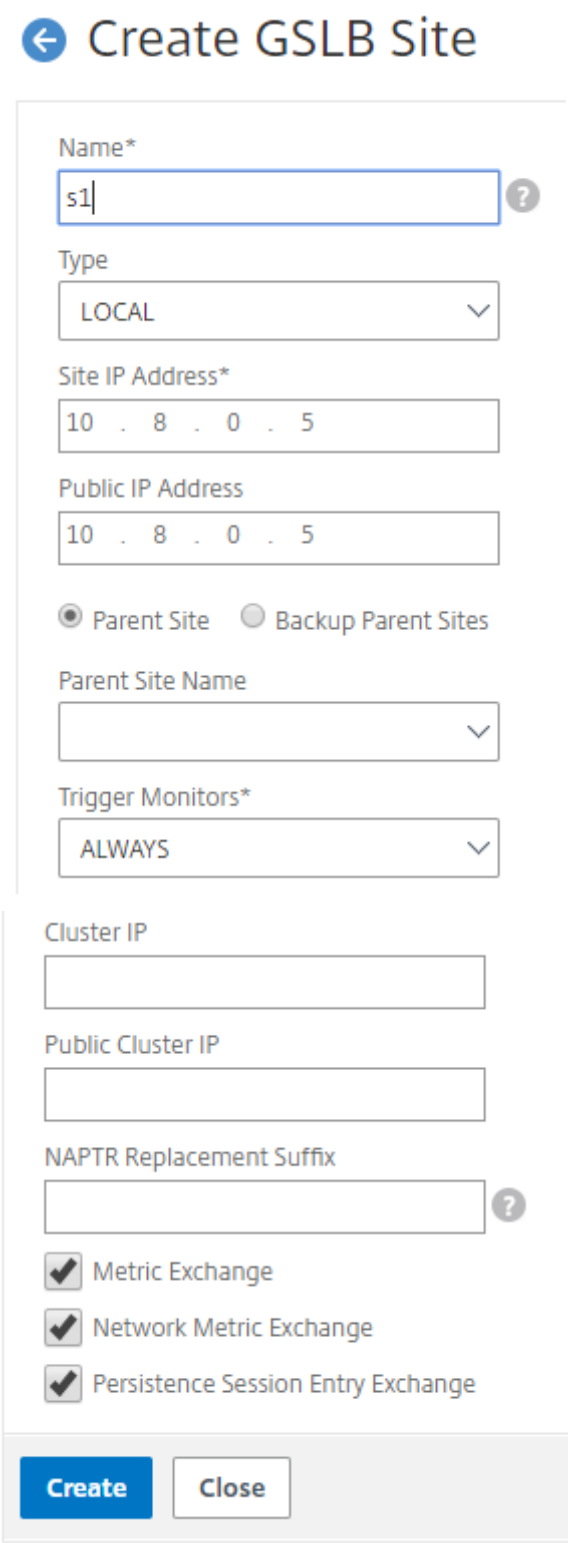


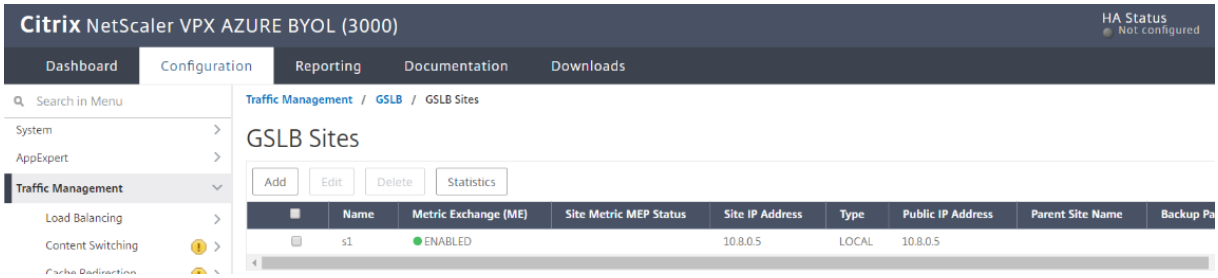




Ajouter des sites GSLB

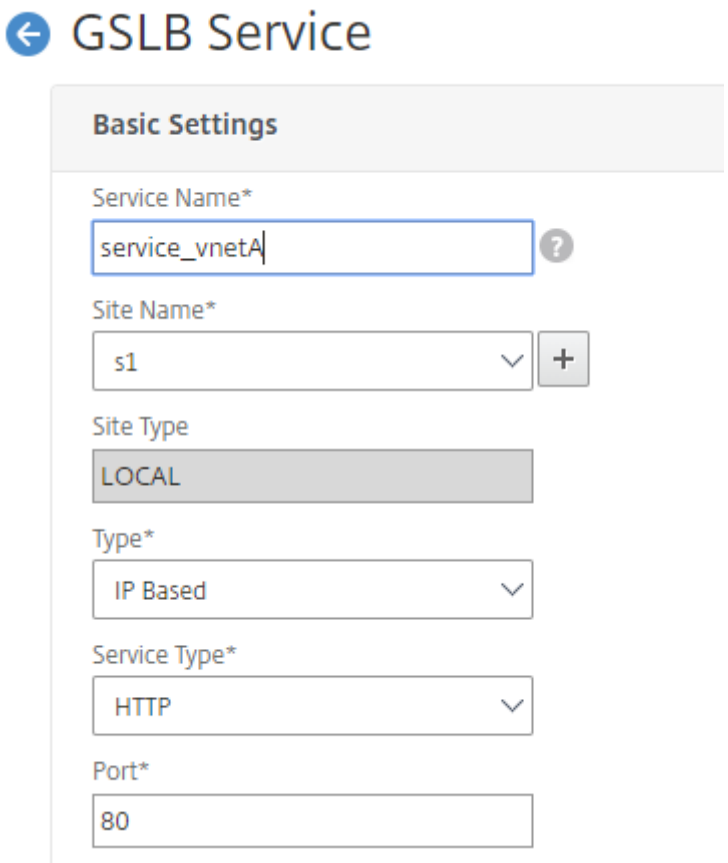
Ajoutez des sites locaux et distants entre lesquels GSLB sera configuré. Sous l'onglet **Configuration** , accédez à **Gestion du trafic > GSLB > Sites GSLB** . Ajoutez un site comme indiqué ici et répétez la même procédure pour d'autres sites.

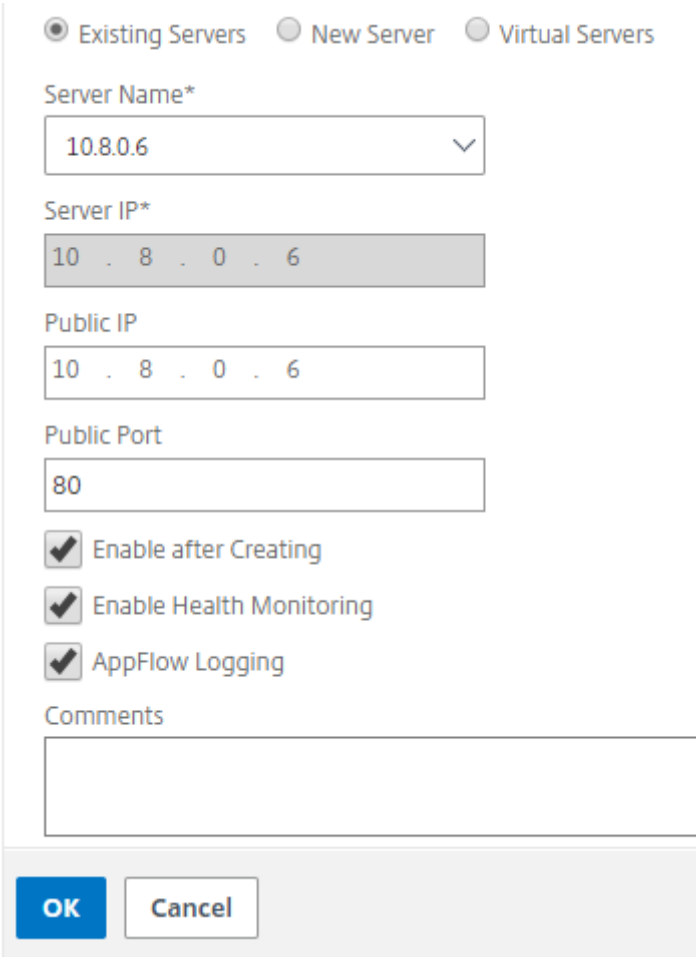




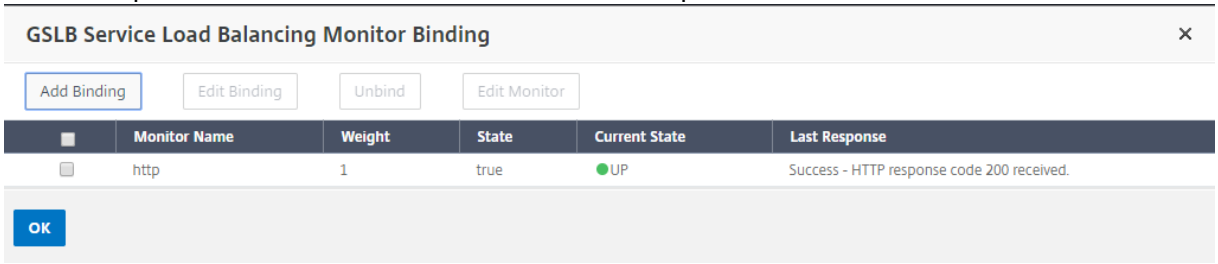
Ajouter des services GSLB

Ajoutez des services GSLB pour les serveurs virtuels locaux et distants qui équilibrent la charge des serveurs App. Sous l'onglet **Configuration** , accédez à **Gestion du trafic > GSLB > Services GSLB** . Ajoutez les services comme illustré dans les exemples suivants. Lier le moniteur HTTP pour vérifier l'état du serveur.

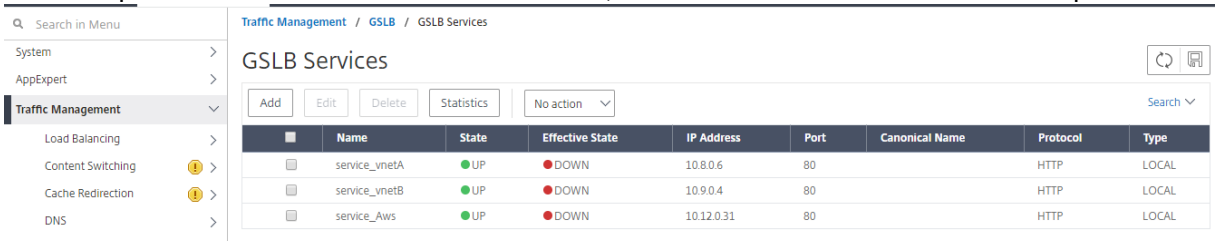




Après avoir créé le service, accédez à l'onglet Paramètres avancés du service GSLB et ajoutez l'onglet Moniteurs pour lier le service GSLB à un moniteur HTTP pour afficher l'état du service

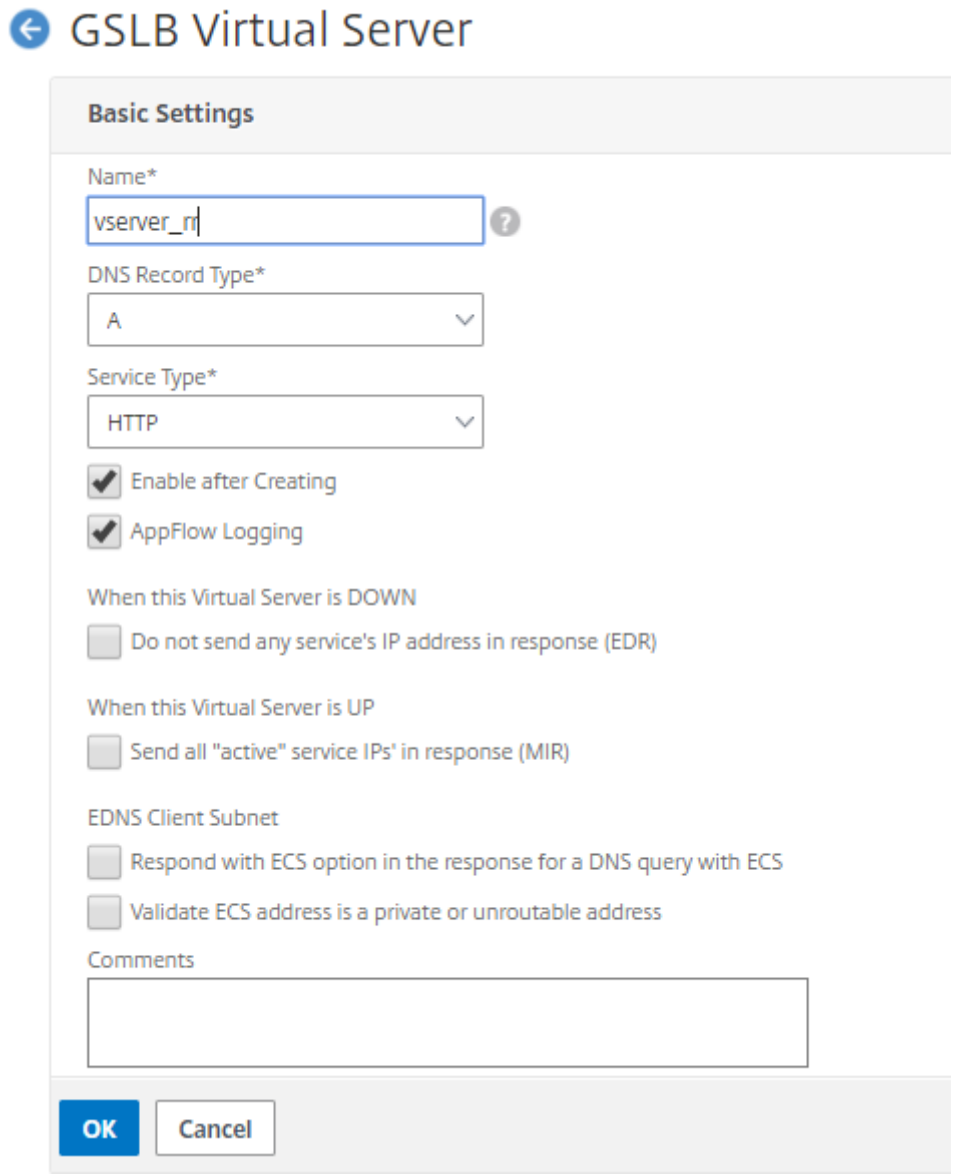


Une fois que vous vous liez avec le moniteur HTTP, l'état des services est UP comme indiqué ici :

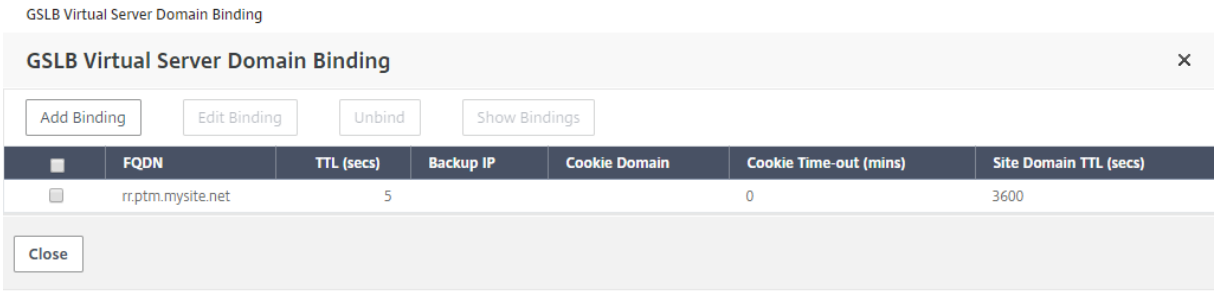


Ajouter un serveur virtuel GSLB

Ajoutez un serveur virtuel GSLB via lequel les services GSLB alias des serveurs d'applications sont accessibles. Sous l'onglet **Configuration** , accédez à **Gestion du trafic > GSLB > Serveurs virtuels GSLB** . Ajoutez les serveurs virtuels comme indiqué dans l'exemple suivant. Liez les services GSLB et le nom de domaine.

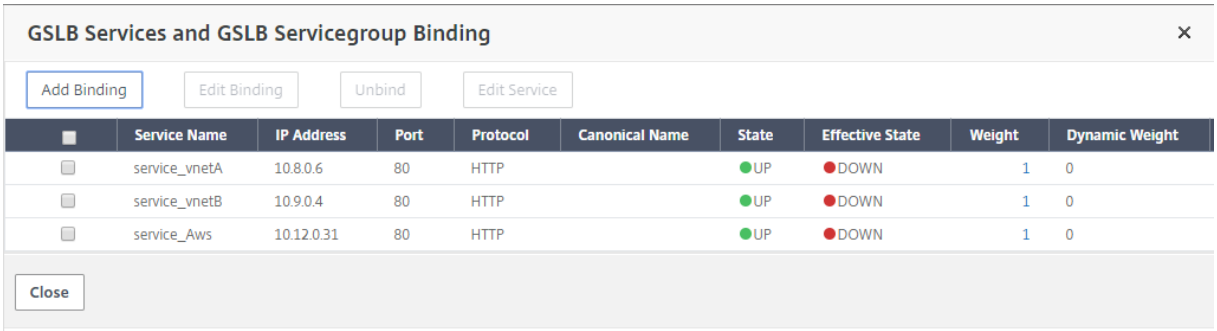


Après avoir créé le serveur virtuel GSLB et sélectionné la méthode d'équilibrage de charge appropriée (Round Robin dans ce cas), lier les services et les domaines GSLB pour terminer l'étape

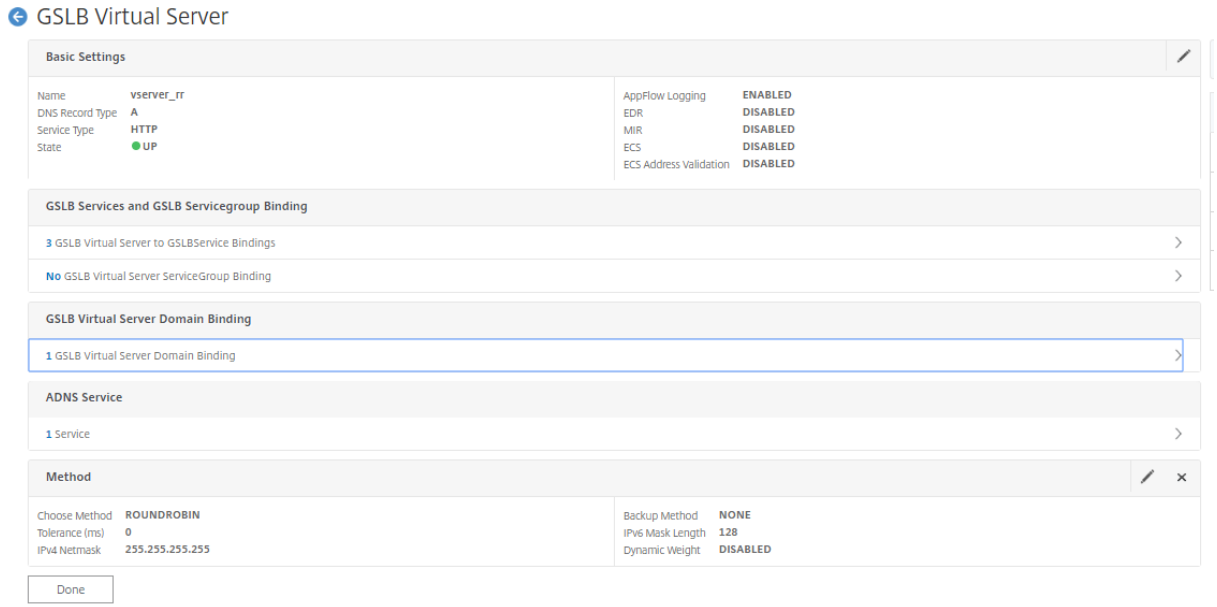


Accédez à l'onglet **Paramètres avancés** à l'intérieur du serveur virtuel et **ajoutez l'onglet Domaines** pour lier un domaine

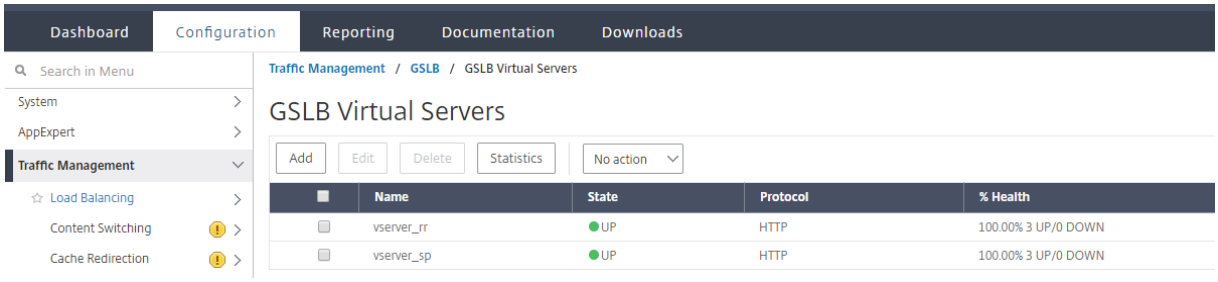
Allez dans **Avancé > Services** et cliquez sur la flèche pour lier un service GSLB et lier les trois services (vNet A, vNet B, local) au serveur virtuel



Après avoir lié les services GSLB et le domaine au serveur virtuel, il apparaît comme illustré ici :



Vérifiez si le serveur virtuel GSLB est en place et 100% sain. Lorsque le moniteur montre que le serveur est en état de fonctionnement, cela signifie que les sites sont synchronisés et que les services principaux sont disponibles.



Pour tester le déploiement, accédez maintenant à l'URL`rr.ptm.mysite.net` du domaine à partir d'une machine cliente Cloud ou d'une machine cliente locale. Supposons qu'il y ait accès à partir de la machine cliente Windows cloud, voir que même sur site serveur d'applications est accessible dans une zone DNS privée sans aucun besoin de solutions DNS tierces ou personnalisées.

Conclusion

Citrix ADC, la solution de distribution d'applications leader, est le mieux adapté pour fournir des fonctionnalités d'équilibrage de charge et de GSLB pour la zone privée Azure DNS. En s'abonnant à Azure DNS Private Zone, l'entreprise peut compter sur la puissance et l'intelligence de Citrix ADC Global Server Load Balancing (GSLB) pour distribuer le trafic intranet entre les charges de travail situées dans plusieurs géographies et entre les centres de données, connectés via des tunnels VPN sécurisés. Cette collaboration garantit aux entreprises un accès transparent à une partie de leur charge de travail qu'elles souhaitent transférer vers le cloud public Azure.

Vue d'ensemble des preuves d'ouverture de session du service d'authentification fédérée Citrix

January 8, 2020

Introduction

Le service FAS (Federated Authentication Service) est un composant Citrix qui s'intègre à votre autorité de certification Active Directory, permettant ainsi aux utilisateurs d'être authentifiés de manière transparente dans un environnement Citrix. Pour plus d'informations sur l'architecture et le déploiement FAS, reportez-vous à la section Documentation du service d'authentification fédérée.

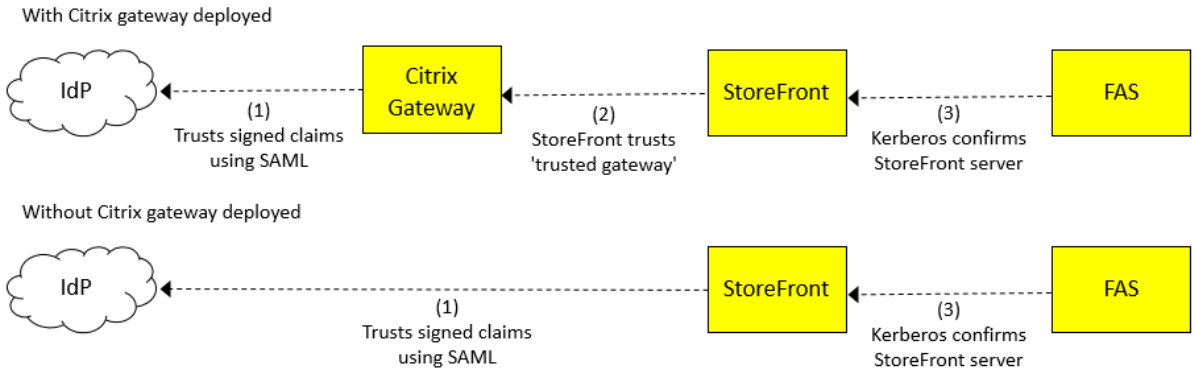
Vous pouvez déployer FAS pour permettre aux utilisateurs d'ouvrir une session unique à un VDA (ou à une application publiée) sans avoir besoin d'un mot de passe ou d'une carte à puce. La fonctionnalité de preuve d'ouverture de session FAS fournit des preuves d'ouverture de session transmises à FAS par Citrix Gateway et StoreFront. FAS peut valider les preuves pour s'assurer qu'elles ont été émises par un fournisseur d'identité (IdP) de confiance.

Cet article décrit comment configurer la fonctionnalité de preuve d'ouverture de session FAS.

Généralités

Confiance FAS

L'infrastructure FAS implique une « chaîne de confiance » entre Citrix Gateway (NSG), StoreFront (SF) et FAS ; chaque flèche pointe du composant *d'approbation* vers le composant *approuvé* :



L'élément clé de confiance entre chacun de ces composants est le nom d'utilisateur principal (UPN) de l'utilisateur qui accède au système. L'UPN circule à travers les liens (dans la direction opposée aux flèches). L'UPN peut également être transformé en un UPN différent à mesure qu'il circule dans le système, mais cela n'est pas directement pertinent pour ce sujet.

Le fournisseur d'identité (IdP) est l'endroit où les utilisateurs s'authentifient. L'IdP est souvent un site Web tiers tel qu'Okta ou Azure. Les utilisateurs s'authentifient auprès de l'IdP en fournissant un ensemble d'informations d'identification (par exemple un mot de passe ou quelque chose de plus complexe). Les composants plus loin dans la chaîne acceptent que l'UPN soit authentique en raison de la chaîne de confiance entre les composants.

La confiance est établie de la manière suivante, marquée 1, 2, 3 dans le diagramme ci-dessus :

(1) Citrix Gateway ou StoreFront fait confiance à l'IdP à l'aide d'un protocole impliquant des revendications signées (par exemple, une revendication indiquant l'UPN de l'utilisateur). La partie d'approbation peut vérifier les revendications faites par l'IdP car elle est configurée avec le certificat qu'elle utilise pour vérifier la validité de la signature. Il existe deux protocoles principaux utilisés pour la vérification : SAML (Security Assertion Markup Language) et OpenID Connect. La fonctionnalité de preuve d'ouverture de session ne prend actuellement en charge que SAML.

(2) Cette approbation est établie en configurant StoreFront avec les détails de Citrix Gateway approuvé. Le protocole entre ces composants, « CitrixAgBasic », permet à StoreFront de confirmer qu'il est appelé par une passerelle Citrix Gateway.

(3) Cette fiducie est établie en utilisant Kerberos. FAS est configuré avec une liste de serveurs StoreFront approuvés. Kerberos est utilisé pour vérifier que l'identité du serveur StoreFront appelant est

sur cette liste.

Sécurité

L'authentification sécurisée repose sur une chaîne de confiance correctement établie. La chaîne de confiance est renforcée par la validation des preuves fournies par l'IdP, qui est la base de confiance pour l'authentification sécurisée. Ceci est important, car les informations d'identification utilisateur fournies à FAS via la chaîne de confiance incluent le nom d'utilisateur (l'UPN), mais n'incluent pas un secret (comme un mot de passe) que FAS peut lui-même valider. L'exposition du mot de passe est donc limitée à l'IdP. La plupart des systèmes d'authentification fédérés fonctionnent de cette façon, y compris FAS.

Preuve d'ouverture de session

La fonctionnalité de preuve d'ouverture de session FAS fournit une assurance de sécurité supplémentaire dans un déploiement FAS. Il vous permet de définir des règles qui autorisent ou refusent l'accès au FAS.

La preuve d'ouverture de session (ou simplement « preuve ») est un élément de données créé par l'IdP lorsque l'utilisateur s'authentifie. Ces données circulent, avec l'UPN, dans tout le système. Au moment du lancement du VDA, le FAS peut vérifier que les preuves sont valides avant de permettre le lancement de continuer.

Actuellement, seuls les IdP qui prennent en charge SAML sont pris en charge. La preuve est la réponse SAML, qui est un document XML contenant un ensemble de réclamations signées par l'IdP. (L'IdP est la racine de la confiance pour l'authentification).

Plug-in FAS

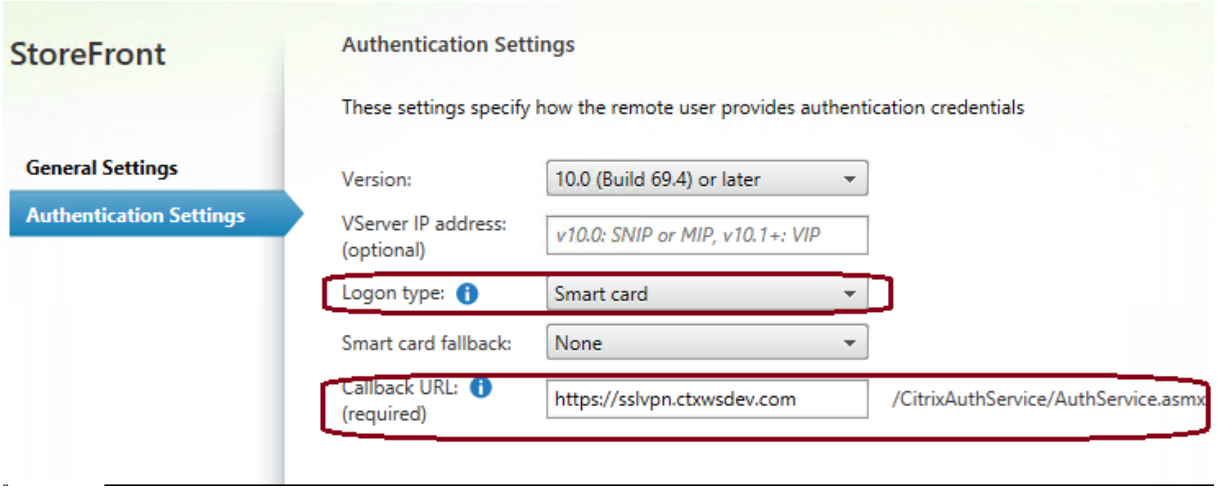
FAS n'a aucune capacité intégrée pour vérifier que les preuves d'ouverture de session sont valides. Au lieu de cela, vous devez écrire votre propre plug-in FAS à l'aide du SDK FAS Assertion. Votre plug-in est responsable de vérifier l'UPN fourni et les preuves (réponse SAML).

Configurer la collection de preuves d'ouverture de session

Étape 1 - Créez votre déploiement

Créez un déploiement à l'aide de Citrix Gateway, StoreFront et FAS comme d'habitude. Configurez Citrix Gateway ou StoreFront pour utiliser l'authentification SAML à votre IdP.

> **Important :**
>
> Si vous utilisez Citrix Gateway, lorsque vous configurez StoreFront avec les détails de votre Citrix Gateway, vous *devez* configurer une **URL de rappel** , car les preuves d'ouverture de session sont transmises via le rappel :



Citrix vous recommande de configurer le **type d'ouverture de session en** tant que « carte à puce », ce qui aide les clients natifs à effectuer l'authentification SAML.

Vérifiez que votre déploiement fonctionne correctement. En d'autres termes, vérifiez que vous pouvez vous connecter et lancer des sessions VDA sans être invité à fournir des informations d'identification sur le VDA.

Étape 2 - Installer l'exemple de plug-in d'assertion FAS

Le SDK FAS Assertion inclut un exemple de plug-in que vous pouvez utiliser comme base pour votre propre plug-in.

> **Remarque :**
>
> Citrix vous recommande vivement de commencer par installer l'exemple de plug-in sans apporter de modifications.

Pour obtenir des instructions sur l'installation du plug-in, consultez le fichier *Readme.txt* fourni avec le kit SDK d'assertion FAS.

Étape 3 - Vérifiez que le plug-in d'assertion FAS fonctionne

Une fois le plug-in installé, des événements supplémentaires sont écrits dans la section **Logs/Application Windows** du journal des événements de votre serveur FAS. Pour obtenir une description de la journalisation et du suivi, consultez le Kit de développement logiciel (SDK) d'assertion FAS.

Étape 4 - Activer la collecte de preuves sur Citrix Gateway

Si vous utilisez Citrix Gateway pour l'authentification, vous devez activer la fonctionnalité de collecte de preuves afin que les preuves soient transmises de Citrix Gateway à StoreFront. Pour ce faire, utilisez la console d'administration Citrix ADC pour activer l'option « Stocker la réponse SAML » pour votre serveur de Gateway, reportez-vous à la section Authentification SAML.

Étape 5 - Activer la collecte de preuves sur StoreFront

> **Remarque :**
>
> Si vous activez la preuve d'ouverture de session, vous *devez* déployer un module de plug-in FAS Assertion sur le serveur FAS.

Par défaut, StoreFront n'envoie pas de preuves au FAS (même si l'authentification SAML est configurée). Pour activer l'utilisation de preuves d'ouverture de session dans StoreFront, utilisez PowerShell suivant pour l'activer pour le service d'authentification associé à un magasin nommé : Store.

```
Get-Module "Citrix.StoreFront.* -ListAvailable | Import-Module

$StoreName = "Store" $StoreVirtualPath = "/Citrix/" + $StoreName $store
    = Get-STFStoreService -VirtualPath $StoreVirtualPath $auth = Get-
   STFAuthenticationService -StoreService $store

$auth.AuthenticationOptions.CollectFasEvidence = $true

$auth.Save()
<!--NeedCopy-->
```

Étape 6 - Modifier l'exemple de plug-in d'assertion FAS

Le code squelette dans l'exemple de plug-in accepte toute preuve. Mettez à jour le code dans l'exemple pour vérifier que la preuve d'ouverture de session fournie (réponse SAML) est valide.

Il est de votre responsabilité de vous assurer que les preuves fournies sont vérifiées. Considérez :

- vérifier que les revendications SAML ont une signature cryptographiquement valide
- vérifier que les revendications SAML sont signées avec le certificat de l'IdP
- vérifier que l'UPN dans les revendications SAML correspond à l'UPN présenté
- vérifier que les demandes ont été délivrées dans un délai acceptable (ce qui est « acceptable », c'est à vous de déterminer)

SDK d'authentification StoreFront

Vous pouvez utiliser le SDK d'authentification StoreFront pour effectuer une personnalisation avancée des données de preuves. Pour plus d'informations, consultez le document « Custom Federated Logon Service Sample 1811.pdf » fourni dans le SDK ou disponible surhttps://developer-docs.citrix.com/.

Informations connexes

- Documentation du service d'authentification fédérée Citrix
- Documentation du Kit de développement logiciel (SDK) StoreFront PowerShell
- Citrix Federated Authentication Service SDK d'assertion dehttps://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/

Modèles de stratégie HDX pour XenApp et XenDesktop 7.6 vers la version actuelle

January 8, 2020

XenApp et XenDesktop inclut des modèles de stratégie HDX qui simplifient le déploiement pour les utilisateurs. Ce document fournit des considérations de conception lorsque vous utilisez ces modèles pour créer des stratégies. Nous avons également fourni des conseils de planification pour vous aider à déterminer les paramètres appropriés pour un cas d'utilisation donné.

Le public visé par ce document est un administrateur Citrix avancé qui connaît bien les concepts HDX, les modèles de stratégie et les versions précédentes du produit.

Ce document ne remplace pas la documentation complète sur le produitStratégies XenApp et XenDesktop.

XenApp et XenDesktop prend en charge les modèles intégrés fournis avec le produit et les modèles personnalisés mis à disposition sur leSite de support Citrix. Ce document se concentre sur les modèles intégrés.

Modèle de sécurité et de contrôle

Utilisez ce modèle dans les environnements où la tolérance au risque est faible, pour minimiser les fonctionnalités activées par défaut dans XenApp et XenDesktop. Ce modèle inclut des paramètres qui désactivent l'accès de la machine utilisateur à

- impression
- presse-papiers
- périphériques

- mappage de lecteurs
- redirection de port
- Accélération éclair

L'application du modèle de sécurité et de contrôle peut utiliser plus de bande passante et réduire la densité utilisateur par serveur.

Modèle d'évolutivité élevée des serveurs

Appliquez ce modèle pour économiser sur les ressources du serveur. Ce modèle équilibre entre l'expérience utilisateur et l'évolutivité du serveur. Il offre une bonne expérience utilisateur tout en augmentant le nombre d'utilisateurs que vous pouvez héberger sur un seul serveur. Entre autres paramètres, ce modèle active le mode de compatibilité Thinwire (n'utilise pas de codec vidéo) et empêche le rendu vidéo côté serveur.

Vous pouvez utiliser ce modèle pour fournir une densité utilisateur maximale par serveur. Cette conception est destinée aux VDA exécutant des systèmes d'exploitation modernes comme Windows 8, Windows 10 et Windows Server 2012 R2. Citrix fournit également un modèle séparé avec le suffixe « - système d'exploitation hérité » pour Windows 7 et Windows Server 2008 R2.

Ce que ce modèle fait

Désactive l'utilisation du codec vidéo pour la compression des graphiques. Cette modification améliore à elle seule la densité des utilisateurs par serveur tout en échangeant sur les graphiques de rendu du serveur. La plupart des applications utilisateur ne sont pas affectées par cette modification tout en réduisant l'expérience de lecture multimédia rendue par le serveur. Pour augmenter encore la densité, les paramètres de ce modèle empêchent la lecture multimédia rendue par le serveur sur les applications Windows par défaut tout en autorisant les technologies de redirection Citrix dans la mesure du possible.

Comment utiliser ce modèle

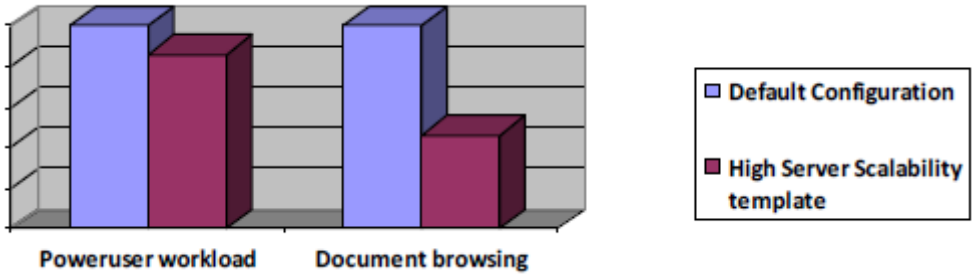
La meilleure pratique consiste à appliquer une stratégie créée à partir de ce modèle à tous les utilisateurs d'un serveur. Vous pouvez définir des exceptions (comme différents paramètres d'impression ou même des modes graphiques avancés comme Framehawk ou DCR) en appliquant une stratégie de priorité supérieure filtrée aux utilisateurs souhaités.

Considérations lors de l'utilisation de ce modèle

- Il n'y a pas de conditions préalables côté client pour le travail des tâches graphiques simples (suite bureautique, etc.) avec une stratégie créée à partir de ce modèle est utilisée.

- Pour s'adapter à la redirection de lecture multimédia avec un impact minimal sur l'utilisateur, utilisez les périphériques clients Windows ou Linux avec le dernier récepteur qui fournit le meilleur support de redirection multimédia. iOS et Mac obtiennent des options de lecture multimédia limitées. Assurez-vous également que les utilisateurs disposent d'Internet Explorer et du Lecteur Windows Media comme applications par défaut.
- Pour s'adapter à la redirection de lecture multimédia avec un impact minimal sur l'utilisateur, utilisez les périphériques clients Windows ou Linux avec le dernier récepteur qui fournissent le meilleur support de redirection multimédia. iOS et Mac obtiennent des options de lecture multimédia limitées. Assurez-vous également que les utilisateurs disposent d'Internet Explorer et du Lecteur Windows Media comme applications par défaut.
- Comme déjà mentionné, la lecture multimédia rendue par le serveur peut être sous-optimale ou évitée du tout en fonction des applications et du type de média utilisé.
- Le modèle désactive certains effets de personnalisation et graphiques comme le papier peint du Bureau et les animations de menu. Bien qu'il y ait plus d'optimisations possibles dans le système d'exploitation, celles-ci peuvent entraîner des effets d'évolutivité indésirables et ne doivent être appliquées qu'après avoir testé et comparé les paramètres de ce modèle. Parmi ceux-ci, « Afficher le contenu tout en faisant glisser », traditionnellement désactivé dans les scénarios d'accès à distance, mais activé sur le modèle. La désactivation de cette option ne profite pas aux performances globales du modèle en raison du comportement du mode de compatibilité Thinwire, utilisé dans ce modèle.
- Les ajouts de produits tels que Lync Optimization Pack et Citrix Universal Printer Server améliorent l'expérience utilisateur et améliorent potentiellement la densité de l'utilisateur.
- En plus de l'augmentation de la densité d'utilisateurs par serveur, l'utilisation de ce modèle peut également réduire la bande passante requise par session pour les interfaces graphiques simples (comme Microsoft Office).
- L'impression est configurée pour mapper uniquement l'imprimante cliente par défaut (empêchant le mappage automatique de plusieurs imprimantes clientes par session) et utiliser le pilote Citrix Universal Printer. L'implémentation des deux paramètres peut réduire le traitement pendant l'établissement et la déconnexion de la session.
- Dans certains scénarios, l'utilisation de la redirection de composition de bureau (DCR) peut aider à améliorer la densité des utilisateurs par serveur. Ce mode graphique n'est pas recommandé dans ce modèle car il est uniquement compatible avec les VDA Windows 7, 8 et 8.1 et les récepteurs Windows ou Mac.

Économies de processeur lors de l'utilisation du modèle High Server Scalability



VDA : session unique 1920x1080, Windows 10 32 bits, 2 Go de RAM 2VCPU @3 .2 GHz

Avertissement : Il s'agit d'un exemple de comparaison. Les économies réelles dépendent du flux de travail spécifique de l'utilisateur.

Après la description et les considérations relatives à chacun des modèles, une comparaison indicative est fournie pour visualiser les économies réalisées dans la consommation des ressources à l'aide des modèles. Ils ne sont pas destinés à servir de référence de performance, car ils sont basés sur des tests simples effectués à l'aide d'une seule session de la charge de travail LogInVSI 4.1 « Power user ». Veuillez tester l'utilisation des charges de travail typiques de votre organisation pour déterminer l'évolutivité du système pertinente à cet environnement.

Évolutivité élevée des serveurs — système d'exploitation hérité

Ce modèle High Server Scalability s'applique uniquement aux VDA exécutant Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle repose sur le mode graphique hérité qui est plus efficace pour ces systèmes d'exploitation.

Ce modèle est fourni pour une densité maximale d'utilisateur par serveur sur des VDA avec des systèmes d'exploitation Windows 7 et Windows Server 2008 R2. Il utilise le mode graphique Thinwire hérité, optimisé pour ces systèmes d'exploitation, et fournira des résultats similaires à ceux de XenApp 6.5 et XenDesktop 5.6.

Comment utiliser ce modèle

Le mode graphique hérité est une stratégie de machine et doit être appliqué à toutes les sessions d'un serveur. Des exceptions aux paramètres autres que les graphiques (comme des paramètres d'impression différents) peuvent être obtenues en appliquant une stratégie de priorité plus élevée filtrée aux utilisateurs désirés.

Ce que ce modèle fait

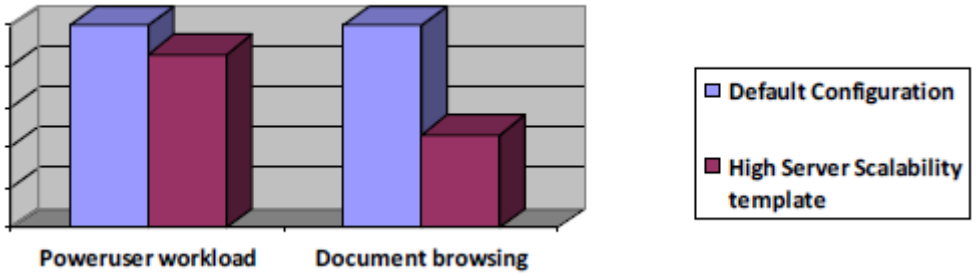
Tous les autres paramètres, sauf « Mode graphique hérité » et « Afficher le contenu lors du déplacement », sont les mêmes que le modèle High Server Scalability. Toutes les mêmes considérations s'appliquent à moins que les considérations suivantes ne soient précisées.

Consultez le site Documentation produit Citrix pour une description détaillée du mode Thinwire Legacy.

Considérations lors de l'utilisation de ce modèle

- Les administrateurs peuvent s'attendre à une expérience utilisateur et une évolutivité similaires à celles de XenApp 6.5 et XenDesktop 5.6 lorsque le rastériseur logiciel VDA (une fonctionnalité 7.x) est désactivé. Voir Élargissement de la compatibilité d'affichage des applications 3D dans XenDesktop — liste noire, une solution de contournement provisoire pour plus de détails.
- Le cas échéant, l'utilisation de DCR peut également améliorer la densité d'utilisateur par serveur.

Économies de processeur lors de l'utilisation de High Server Scalability — modèle de système d'exploitation hérité



VDA : session unique 1920x1080, Windows 7 32 bits, 2 Go de RAM 2VCPU @3 .2 GHz

Avertissement : Le graphique est un exemple de comparaison. Les économies réelles dépendent du flux de travail spécifique de l'utilisateur.

Optimisé pour le modèle WAN

Ce modèle est conçu pour les utilisateurs qui travaillent dans des succursales (connexions WAN partagées) ou depuis des sites distants utilisant des connexions à faible bande passante qui accèdent à des applications dotées d'interfaces graphiques simples et contenant très peu de contenu vidéo (adapté au Thinwire Compatibility Mode). Ce modèle échange l'expérience de lecture vidéo et une certaine évolutivité du serveur pour optimiser l'efficacité de la bande passante.

Ce modèle fonctionne pour améliorer l'expérience utilisateur lors de la connexion avec des connexions à faible bande passante accédant aux applications avec des interfaces utilisateur graphiques simples. La conception de modèle est pour les VDA exécutant des systèmes d'exploitation modernes comme Windows 10 et Windows Server 2012 R2, un modèle séparé avec le suffixe '- système d'exploitation hérité' est fourni pour Windows 7 et Windows Server 2008 R2.

Ce que ce modèle fait

Ce modèle désactive l'utilisation du codec vidéo pour la compression des graphiques. Cette modification est très efficace pour réduire les exigences en bande passante pour les applications Office et autres, mais elle peut réduire la qualité vidéo rendue par le serveur et pourrait réduire l'interactivité si les interfaces sont hautement graphiques, telles que les applications CAO.

Le modèle permet toutes les redirections multimédia Citrix (activées par défaut) pour Windows Media Layer et Flash et l'optimisation à la volée des médias Windows si nécessaire pour le lien WAN utilisé.

N'utilisez PAS ce modèle si les utilisateurs visualisent continuellement le multimédia. Dans ce cas, utilisez les paramètres par défaut ou personnalisez ce modèle en activant la compression à l'aide du codec vidéo.

Comment utiliser ce modèle

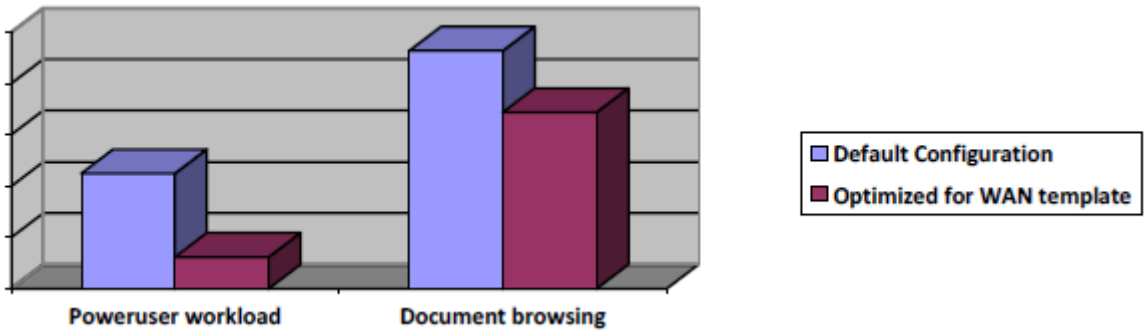
Vous pouvez appliquer les stratégies créées à partir de ce modèle aux groupes de mise à disposition desservant des utilisateurs sur les liens WAN décrits ou sur une base par utilisateur (avec une priorité de stratégie élevée). La connexion utilisateur détermine les stratégies et utilise les filtres de stratégie de paramètre utilisateur disponibles, tels que l'adresse IP du client, la condition d'accès NetScaler Gateway, etc.

Considérations lors de l'utilisation de ce modèle

- Il n'y a pas de conditions préalables côté client pour l'utilisation de tâches graphiques simples (suite bureautique, etc.) avec une stratégie créée à partir de ce modèle est utilisée.
- Les résultats négatifs obtenus lors de l'utilisation de ce modèle peuvent indiquer que les utilisateurs visualisent en permanence le contenu multimédia. Consultez les recommandations ci-dessus si ce comportement utilisateur est accepté.
- La lecture multimédia rendue par le serveur peut être sous-optimale car la fréquence d'images est limitée à un maximum de 16 cibles.
- Les images graphiques complexes avec des couleurs dégradées (comme une ligne d'horizon) ne changeront pas progressivement, mais par étapes, car le réglage du modèle « profondeur de couleur pour les graphiques simples » sous-échantillonne les couleurs de l'écran à 16 bits par pixel afin de réduire les besoins en bande passante.

- Le modèle désactive certains effets de personnalisation et graphiques tels que le papier peint du Bureau et les animations de menu. Bien qu'il y ait plus d'optimisations possibles dans le système d'exploitation, celles-ci peuvent entraîner des effets d'évolutivité indésirables et ne doivent être appliquées qu'après avoir testé et comparé les paramètres de ce modèle. Parmi ceux-ci, 'Afficher le contenu lors du glissement', traditionnellement désactivé dans les scénarios d'accès distant mais activé sur le modèle. La désactivation de cette option ne profite pas aux performances globales du modèle en raison du comportement du mode de compatibilité Thinwire, utilisé dans ce modèle.
- Les ajouts de produits tels que Lync Optimization Pack et Citrix Universal Printer Server améliorent l'expérience utilisateur et améliorent potentiellement la densité de l'utilisateur.
- En plus de l'optimisation pour le réseau étendu, l'utilisation de ce modèle peut également augmenter la densité des utilisateurs par serveur si les sessions ont principalement des interfaces graphiques simples (comme Microsoft Office).
- L'impression est configurée pour mapper uniquement l'imprimante cliente par défaut (empêchant le mappage automatique de plusieurs imprimantes clientes par session) et utiliser le pilote Citrix Universal Printer. Le modèle implémente les deux paramètres pour réduire la bande passante requise pour l'impression.
- Le pilote d'imprimante universel est activé pour toutes les imprimantes. Il peut garantir une faible bande passante, quelle que soit l'imprimante. Bien que certains pilotes spécifiques à l'imprimante et l'utilisation d'un serveur d'impression puissent donner de meilleurs résultats que le pilote d'imprimante générique, nous ne pouvons pas l'activer pour une utilisation générale car ils nécessitent des configurations ou des tests supplémentaires.
- La connexion directe aux serveurs d'impression est désactivée et les imprimantes réseau connectées au périphérique client utilisent le pilote Citrix Generic Printer pour traverser le WAN et spool le travail d'impression à partir du client. L'exécution de ces actions est effectuée pour gérer la bande passante d'impression (optimisée à l'intérieur de la session ICA) et parce que nous ne pouvons pas prédire comment les pilotes spécifiques à l'imprimante se comportent sur la liaison WAN.
- La redirection de composition du bureau (DCR) n'est pas recommandée dans les liens de bande passante restreinte et est désactivée dans ce modèle.

Économies de bande passante lors de l'utilisation du modèle Optimized for WAN



VDA : session unique 1920x1080, Windows 10 32 bits, 2 Go de RAM 2vCPU @3.2GHz

Avertissement : Il s'agit d'un exemple de comparaison. Les économies réelles dépendent du flux de travail spécifique de l'utilisateur.

Optimisé pour WAN — modèle de système d'exploitation hérité

Ce modèle Optimisé pour WAN s'applique uniquement aux VDA exécutant Windows Server 2008 R2 ou Windows 7 et versions antérieures. Ce modèle repose sur le mode graphique hérité qui est plus efficace pour ces systèmes d'exploitation.

Ce modèle améliore l'expérience utilisateur lors de la connexion à des systèmes d'exploitation hérités, tels que Windows 7 ou Windows Server 2008 R2, VDA avec des connexions à faible bande passante accédant aux applications avec des interfaces utilisateur simples graphiquement. Il utilise le mode graphique Thinwire hérité qui fournit des résultats similaires à ceux de XenApp 6.5 et XenDesktop 5.6.

Comment utiliser ce modèle

Le mode graphique hérité est une stratégie de machine et s'applique à toutes les sessions d'un serveur. Vous pouvez définir des exceptions à des paramètres autres que les graphiques (comme des paramètres d'impression différents) en configurant une stratégie de priorité supérieure filtrée pour les utilisateurs souhaités.

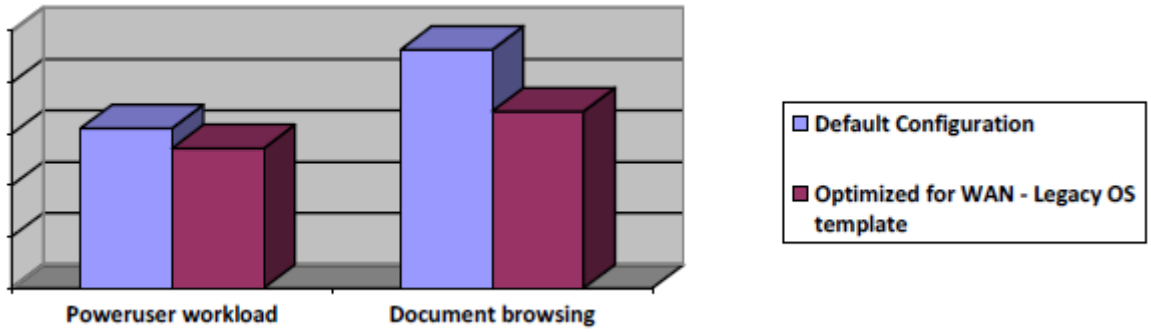
Ce que ce modèle fait

Tous les autres paramètres sauf 'Mode graphique hérité ', 'Afficher le contenu lors du glisser' et 'Extra Color Compression' sont les mêmes que le modèle Optimisé pour WAN. Toutes les considérations de ce modèle, sauf indication contraire ci-dessous, s'appliquent.

Pour obtenirParamètres de stratégie graphiqueune description détaillée du mode Thinwire Legacy, reportez-vous au site Documentation produit Citrix.

Considérations lors de l'utilisation de ce modèle

- Les administrateurs peuvent s'attendre à une expérience utilisateur et une efficacité de bande passante similaires à celles de XenApp 6.5 et XenDesktop 5.6.



VDA : session unique 1920x1080, Windows 7 32 bits, 2 Go de RAM 2vCPU @3.2GHz

Avertissement : Il s'agit d'un exemple de comparaison. Les économies réelles dépendent du flux de travail spécifique de l'utilisateur.

Modèle Expérience utilisateur très haute définition

Ce modèle applique les paramètres par défaut qui maximisent l'expérience utilisateur. Utilisez ce modèle dans les scénarios où plusieurs stratégies sont traitées par ordre de priorité.

Le produit est livré configuré pour offrir une expérience utilisateur haute définition. Un examen attentif de ce modèle montre qu'il applique les valeurs par défaut, à l'exception de la qualité visuelle élevée et de l'impression de meilleure qualité, qui définissent ces valeurs plus élevées que la valeur par défaut.

Quand utiliser ce modèle

Utilisez ce modèle pour garantir une expérience utilisateur maximale en utilisant la stratégie créée, qui a priorité sur les autres stratégies avec des filtres spécifiques (comme les utilisateurs VIP).

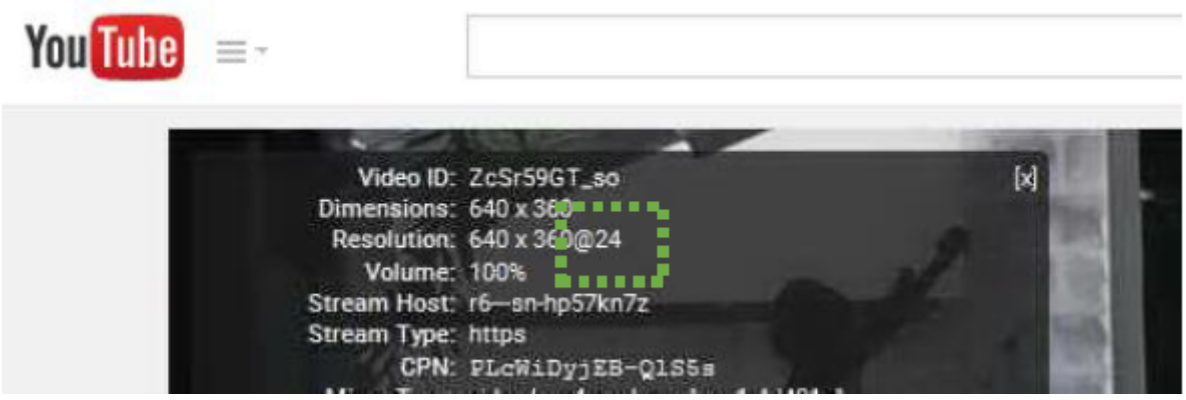
Comment utiliser ce modèle : créez et appliquez une stratégie avec un filtre pour sélectionner les utilisateurs ou scénarios souhaités et avec une priorité plus élevée que les autres stratégies créées à partir des modèles. Vous pouvez utiliser cette stratégie avec la base d'utilisateurs générale, telle que les stratégies d'évolutivité du serveur ou WAN.

Considérations lors de l'utilisation de ce modèle

- Nécessite une mise à jour du matériel client et de Citrix Receivers. Par exemple, les processeurs plus rapides que 2,0 GHz avec prise en charge h.264 et Receiver pour Windows 4.x/Mac

11.8/Linux 13.0. Si la machine utilisateur ne répond pas aux exigences, une stratégie créée avec ce modèle peut avoir des effets négatifs.

- Comme mentionné dans la description de la stratégie intégrée, l'application de ce modèle peut consommer plus de bande passante et réduire la densité utilisateur par serveur.
- Considérez une solution GPU VDA. Les applications utilisateur haut de gamme, graphiques ou ayant des besoins de traitement extrêmes, peuvent tirer parti de la puissance de traitement d'un GPU, ce qui permet de meilleures performances et, dans certains cas, une meilleure évolutivité du serveur. Pour plus d'informationsHDX 3D Pro, consultez la documentation de production Citrix.
- Comme pour la configuration par défaut, ce modèle permettra l'utilisation d'un codec vidéo (h.264) pour la compression des graphiques d'écran si le Receiver le prend en charge et l'a activé. La qualité visuelle est automatiquement ajustée par le codec vidéo selon les besoins et le paramètre « Qualité visuelle » n'est pas nécessaire.
- Le paramètre de haute qualité visuelle s'applique lorsque vous utilisez ce modèle sans le codec vidéo (h.264) de compression (pour augmenter la densité utilisateur par serveur) uniquement, ce qui entraîne le mode graphique appelé mode de compatibilité Thinwire. Les administrateurs peuvent y parvenir en plaçant une stratégie de priorité plus élevée avec le codec vidéo de compression'Non utilisé ou si le client n'a pas ou a désactivé la prise en charge du codec vidéo (voir matrice de compatibilité client). Dans ces circonstances, une expérience utilisateur très haute définition ne sera possible que si le VDA et le périphérique client se connectent via un réseau LAN à large bande passante sans restriction.
- Ce modèle utilise également le paramètre de fréquence d'images cible de 30 ips, ce qui convient à la plupart des cas d'utilisation nécessitant une expérience HD ; les 30 ips par défaut doivent être considérés comme une ligne de base initiale qui peut être ajustée pour répondre à l'expérience HD des utilisateurs finaux (diffusions YouTube de 24 à 30 ips par défaut). Les utilisateurs avec des applications graphiques et GPU haut de gamme peuvent demander des valeurs supérieures jusqu'à 60 ips).



- Ce modèle permet la redirection multimédia du Lecteur Windows Media et Flash vers Citrix Receiver pour Windows et Linux et Windows Media Player uniquement vers les périphériques IOS.

Utilisez le dernier Citrix Receiver dans le client pour tirer parti des améliorations récentes.

- Le modèle configure l'impression pour la meilleure expérience utilisateur, y compris la meilleure qualité de sortie d'impression et toutes les options de configuration disponibles. Si les utilisateurs installent un grand nombre d'imprimantes sur leurs périphériques et que les pilotes d'imprimante du fabricant ne sont pas optimisés pour l'impression à distance, cela pourrait entraîner une utilisation très élevée de la bande passante, une réduction de la densité utilisateur par serveur et d'éventuels problèmes d'interopérabilité au niveau du VDA.

Annexe

Voici les paramètres de stratégie détaillés dans les modèles.

Modèle	Expérience utilisateur très haute définition	Évolutivité élevée des serveurs	Évolutivité élevée des serveurs — système d'exploitation hérité	Optimisé pour WAN	Optimisé pour le réseau étendu — système d'exploitation hérité
Bande passante					
Limite globale de bande passante de session				0 Remarque : simplement pour exposer le paramètre	
Graphiques					
Mode graphique hérité	Désactivé		Activé		Activé
Redirection de composition de bureau				Désactivé	Désactivé
Utiliser le codec vidéo pour la compression	Utiliser le cas où disponible	Ne pas utiliser	s.o.	Ne pas utiliser	s.o.

Modèle	Expérience utilisateur très haute définition	Évolutivité élevée des serveurs	Évolutivité élevée des serveurs — système d'exploitation hérité	Optimisé pour WAN	Optimisé pour le réseau étendu — système d'exploitation hérité
Fréquence d'images cible	30	16	12	16	16
Fréquence d'images minimale cible	10	8	8	8	8
Qualité visuelle	Élevé	Moyen	s.o.	Faible	s.o.
Profondeur de couleur préférée pour des graphismes simples	24bpp		s.o.	16bpp	s.o.
Niveau de compression avec perte	s.o.	s.o.		s.o.	Élevé
Profondeur de couleur maximale autorisée	s.o.	s.o.		s.o.	16bpp
Compression de couleur supplémentaire	Désactivé	Désactivé	Désactivé	Désactivé	Activé
UI du bureau					
Fond d'écran	Autorisé	Interdit	Interdit	Interdit	Interdit

Modèle	Expérience utilisateur très haute définition	Évolutivité élevée des serveurs	Évolutivité élevée des serveurs — système d'exploitation hérité	Optimisé pour WAN	Optimisé pour le réseau étendu — système d'exploitation hérité
Afficher le contenu de la fenêtre tout en faisant glisser	Autorisé	Autorisé	Interdit	Autorisé	Interdit
Aperçu des fenêtres dynamiques	Activé			Désactivé	
Animations de menu	Autorisé	Interdit	Interdit		
Multimédia					
Optimisation pour la redirection multimédia Windows Media via WAN		Interdit	Autorisé		
Limiter la qualité vidéo			Maximum 480p		
Prévention de secours des médias Windows	Non configuré	Lire tout le contenu uniquement sur le client			
Prévention de repli vidéo Flash	Non configuré	Seul un petit contenu			

Modèle	Expérience utilisateur très haute définition	Évolutivité élevée des serveurs	Évolutivité élevée des serveurs — système d'exploitation hérité	Optimisé pour WAN	Optimisé pour le réseau étendu — système d'exploitation hérité
Erreur de prévention de secours vidéo Flash * .swf		Appliquer l'exemple par défaut (voir stratégie)			
Conférence multimédia	Autorisé	Interdit			
Audio					
Qualité audio	Audio haute définition	Moyenne optimisée pour la parole	Faible — pour les connexions à basse vitesse		
Impression					
Création automatique d'imprimantes clientes	Création automatique de toutes les imprimantes clientes	Créer automatique-ment l'imprimante par défaut du client uniquement	Créer automatique-ment l'imprimante par défaut du client uniquement		
Connexions directes serveurs d'impression	Activé		Désactivé		

Modèle	Expérience utilisateur très haute définition	Évolutivité élevée des serveurs	Évolutivité élevée des serveurs — système d'exploitation hérité	Optimisé pour WAN	Optimisé pour le réseau étendu — système d'exploitation hérité
Utilisation universelle du pilote d'imprimante (UDP)	Utiliser l'impression universelle uniquement si le pilote demandé n'est pas disponible	Utiliser l'impression universelle uniquement	Utiliser l'impression universelle uniquement		
Limite de qualité d'impression universelle	Pas de limite		Résolution moyenne (600 DPI)		
Paramètres par défaut de l'optimisation de l'impression universelle	ImageCompres = BestQuality ; Autres paramètres = par défaut	ImageCompres = Standard-Quality ; Autres paramètres = par défaut	ImageCompres = ReducedQual-ity ; Autres paramètres = par défaut		
Redirection de fichier					
Utiliser des écritures asynchrones	Désactivé		Activé		

Remarque :

- Les paramètres en gras sont égaux aux valeurs par défaut.
- Les paramètres assignés aux valeurs par défaut permettent de garantir les résultats souhaités lors de l'utilisation de stratégies empilées.
- Les cases barrées marquent les paramètres (dans cette ligne) qui ne sont pas applicables

> au mode graphique de chaque modèle.
> - Les cases vides représentent les paramètres qui n'ont pas de recommandation spécifique pour le modèle dans cette colonne.
> - Le tableau ne répertorie pas tous les paramètres de stratégie, uniquement ceux utilisés dans les modèles intégrés. Pour obtenir la liste complète des stratégies, consultez leDocumentation produit Citrixsite Web.

Considérations relatives à la mise à disposition de graphiques

Utilisation par Thinwire du codec vidéo pour la compression

Dans XenApp/XenDesktop version 7.6 FP3, HDX apporte une prise en charge améliorée pour fournir des graphiques simples comme les applications Office de base. Nous faisons cela pour permettre à nos clients de continuer à prolonger la durée de vie des liaisons réseau déjà déployées, des périphériques clients et des récepteurs verrouillés. À

, nous permettons maintenant à l'administrateur de contrôler quand utiliser un codec vidéo pour encoder les graphiques Thinwire.

Par défaut, le produit est toujours livré avec l'utilisation du codec vidéo activée (lorsque disponible), adapté à la plupart des scénarios d'utilisation générale.

Lorsque l'évolutivité élevée du serveur est primordiale et que les liaisons *Optimized for WAN* (bande passante limitée) sont en cours d'utilisation, Citrix recommande de désactiver l'utilisation du codec vidéo. Lorsque vous n'utilisez pas le codec vidéo, la session peut se concentrer sur l'optimisation de la livraison de texte et de graphiques simples (qui sont la base de la plupart des applications métier) avec les exigences minimales de CPU et de bande passante.

Les performances vidéo rendues par le serveur ne seront pas optimales si la bande passante est limitée. Pour plus d'informations, reportez-vousMode de compatibilité Thinwireà la documentation produit Citrix.

Systèmes d'exploitation hérités qui permettent l'utilisation de GDI (Windows 7 et Windows Server 2008 R2)

Citrix recommande d'activer le mode graphique hérité. La conception du mode Thinwire hérité est pour l'architecture des systèmes d'exploitation Windows hérités et il reste dans de nombreux cas d'utilisation les modes graphiques les plus optimisés pour ces systèmes d'exploitation.

Afficher le contenu de la fenêtre tout en faisant glisser

Contrairement aux recommandations données pour les versions précédentes, le mode de compatibilité Thinwire fonctionne mieux lorsque l'option Afficher le contenu de la fenêtre pendant le déplace-

ment est autorisée.

Désactivez la stratégie pour le mode graphique hérité et une meilleure évolutivité dans les scénarios où le codec vidéo (h.264) pour la compression est requis, mais la densité maximale de l'utilisateur est souhaitée.

Fréquence d'images cible et cadence minimale cible

Pour les modèles High Server Scalability et Optimized for WAN (liens de bande passante contraints), ciblés pour une utilisation graphique simple, Citrix recommande de réduire le paramètre de fréquence d'images cible à 16 ou 12 et de réduire le minimum cible à 8. Ces paramètres aident à atteindre l'objectif souhaité pour ces modèles.

Nous avons sélectionné la cadence cible de 16, car c'est le minimum absolu pour que l'œil humain détecte le mouvement.

Le VDA et le client négocient en permanence la fréquence de trame appropriée à livrer au cours de la session. En général, la fréquence d'images est maintenue au minimum requis pour afficher les changements à l'écran. Lorsque des mouvements élevés sont détectés, de la lecture vidéo au glissement de la fenêtre en passant par le défilement, la session tentera de fournir chaque changement d'écran jusqu'à la fréquence d'images cible. Dans les connexions à bande passante restreinte, il peut ne pas être possible de maintenir la fréquence d'images cible et le VDA équilibre automatiquement l'augmentation de la compression graphique de l'écran et la baisse de la fréquence d'images jusqu'à ce qu'elle atteigne la fréquence d'images minimale Target, puis l'augmentation de la compression jusqu'à ce qu'elle soit prédéfinie (non configurable) et enfin réduire encore la fréquence d'images au besoin. Pensez à cela comme un affichage adaptatif automatique (une technique utilisée dans les produits Citrix précédents).

> **Remarque : Le** fait de définir la qualité visuelle à faible n'affecte pas le texte à contraste élevé (par exemple noir sur blanc), et il est toujours livré avec une haute qualité.

Profondeur de couleur

Différent du mode hérité, le super-codec XenDesktop et XenApp 7.x n'a pas de contrôle sur la profondeur des couleurs et reçoit 24 bits par pixel. En FP3, dans le cadre de l'amélioration de Thinwire sans utiliser de codec vidéo pour la compression, nous avons ajouté l'option d'envoyer les graphiques de session en 16 bits par pixel (contrôlé par la **profondeur de couleur préférée pour un réglage graphique simple**). Cette option réduit la bande passante requise pour les graphiques simples, et elle n'est perceptible que lorsque vous utilisez des dégradés de couleurs. Dans ce cas, les périphériques peuvent utiliser une consommation de CPU du serveur légèrement plus élevée.

Pour le mode graphique hérité, dans les modèles du système d'exploitation hérité pour l'évolutivité et le WAN, le paramètre **Profondeur de couleur maximale autorisée** est également limité à 16 ou 12.

Notez que lorsque vous utilisez le mode graphique hérité, une profondeur de couleur inférieure peut être demandée ou livrée en fonction d'autres conditions.

Un mot sur DCR**

Desktop Composition Redirection (DCR) est un canal virtuel d'affichage introduit par Citrix dans XenDesktop 5.5. Bien que cette technologie présente de nombreux avantages, elle est actuellement disponible pour les VDA Windows 7, 8 et 8.1, la prise en charge réduite de Citrix Receiver et, principalement, l'adoption par les clients a été faible. En outre, la DCR n'est pas recommandée pour les liaisons WAN à faible bande passante. Pour cette raison, à partir du FP3, ce canal virtuel est désactivé par défaut et les modèles Optimisé pour WAN le désactivent activement.

Lire plus en mode graphique HDX

Pour plus d'informations sur la vérification du mode graphique utilisé, consultez le CentreComment faire pour déterminer le mode d'affichage HDXde connaissances du support Citrix.

Considérations multimédias

Dans tous les modèles et par défaut sur le produit, la redirection de la lecture multimédia est autorisée. Voici les paramètres supplémentaires utilisés dans les modèles :

Optimisation pour la redirection multimédia Windows Media via WAN

Autorisé par défaut, le transcodage juste à temps du contenu multimédia pour une diffusion efficace sur un WAN est intensif et donc interdit dans le modèle High Server Scalability. Veuillez noter que si un GPU NVIDIA est mis à la disposition du serveur et que le paramètre : **Utiliser le GPU pour optimiser la redirection multimédia Windows Media sur WAN** est activé, vous pouvez décharger le traitement vers le GPU.

Limiter la qualité vidéo

Ces paramètres s'appliquent uniquement à l'optimisation pour la redirection multimédia Windows Media. Une valeur équivalente à un petit lecteur vidéo intégré a été sélectionnée comme recommandation initiale dans le modèle 'Optimized for WAN' où il est utilisé. Sinon, ce paramètre n'est pas configuré.

Conférence multimédia

La redirection d'une webcam à partir du client utilisée dans une application de communications unifiées ou de conférence exécutée dans le VDA augmentera les ressources serveur requises. Cette fonctionnalité est désactivée dans le modèle d'évolutivité High Server.

Pour plus d'informations sur le paramètre de stratégie de redirection multimédia et Flash, consultez les rubriques suivantes sur le site Citrix Production Documentation :

- Paramètres de stratégie multimédia
- Paramètres de stratégie de redirection Flash

Considérations audio

Le produit est livré avec un son de haute qualité par défaut (environ 128 Kbit/s). Cette valeur s'applique également au modèle de définition très haute dans le cas où une stratégie créée à partir de ce modèle a une priorité plus élevée que d'autres stratégies.

Les valeurs répertoriées dans le tableau suivant sont pour la direction audio (sortie et entrée) individuellement.

Modèle	Expérience en très haute définition et paramètre par défaut	Évolutivité élevée des serveurs	Optimisé pour WAN
Paramètre de qualité audio	Élevé	Moyen	Faible
Bande passante prévue utilisée	128 Kbit/s	60 Kbits/s	44 Kbits/s

Considérations relatives à l'impression

XenApp et XenDesktop incluent un pilote d'imprimante universel qui peut fonctionner avec la plupart des imprimantes connectées au client. Par défaut, le VDA utilise ce pilote uniquement si le VDA ne trouve pas le pilote spécifique à l'imprimante. Par défaut, toutes les imprimantes attachées au client sont mappées dans la session.

Les nouveaux modèles intégrés utilisent les paramètres d'impression suivants qui diffèrent des valeurs par défaut :

Créer automatiquement l'imprimante par défaut du client uniquement

Évolutivité élevée du serveur et optimisée pour le réseau étendu — La création d'une imprimante au lieu d'un grand nombre permet de réaliser des économies sur les deux scénarios.

Les utilisateurs peuvent modifier l'imprimante client par défaut pendant la session, et l'imprimante mappée sera mise à jour même dans des scénarios à double saut.

Utiliser l'imprimante universelle [pilote] uniquement

Évolutivité élevée du serveur : empêche le VDA d'avoir à rechercher des pilotes d'imprimante à chaque connexion, ce qui permet d'économiser les opérations d'E/S de disque et la charge du serveur en raison des pilotes de modèle de pré-imprimante.

Optimisé pour le réseau étendu : le pilote d'imprimante universel peut garantir une faible bande passante, quelle que soit l'imprimante. Bien que certains pilotes spécifiques à l'imprimante et l'utilisation d'un serveur d'impression (qui nécessite une configuration supplémentaire) puissent donner de meilleurs résultats que le pilote d'imprimante générique, nous ne pouvons pas le recommander pour une utilisation générale car ils nécessitent des configurations ou des tests supplémentaires.

Connexions directes aux serveurs d'impression

Activé par défaut, ce paramètre permet d'accéder directement à une imprimante réseau configurée dans le client à partir de la session. L'activation de ce paramètre peut potentiellement améliorer les options disponibles pour l'utilisateur (selon l'imprimante) et économiser du trafic sur le périphérique client.

Pour Optimisé pour les modèles WAN, ce paramètre est désactivé car il est probable que l'imprimante réseau soit au même endroit que l'utilisateur (il doit récupérer l'impression, n'est-ce pas ?) et nous pouvons donc nous assurer que la taille de la tâche d'impression sera petite lors de l'impression à l'aide du pilote Citrix Universal Printer. En outre, la bande passante utilisée par la tâche d'impression respecte les limites de bande passante de session.

bases de données SQL Server et Citrix

January 8, 2020

Microsoft SQL Server est un composant important de tout déploiement Citrix Virtual Apps and Desktops. Planifier et comprendre les interactions Citrix SQL est très utile pour vous et votre organisation dans le maintien d'un environnement Citrix sain et performant. L'absence de haute disponibilité SQL

Server et de ressources de calcul abondantes a un effet négatif sur l'expérience utilisateur et le temps de disponibilité de l'infrastructure Citrix.

Résumé de la base de données

Trois bases de données sont nécessaires/créées lors du déploiement Citrix Virtual Apps and Desktops :

Site : (également connu sous le nom de Configuration du site) stocke la configuration du site en cours d'exécution, ainsi que les données dynamiques liées au courtage, telles que l'état actuel de la session, la connexion, la charge et les informations d'état du VDA.

Journalisation de la configuration : (également appelée Journalisation) stocke des informations sur les modifications de configuration du site et les activités administratives. Cette base de données est utilisée lorsque la fonctionnalité Configuration de la journalisation est activée (par défaut = activé).

Surveillance : stocke les données utilisées par Director, telles que les informations de session et de connexion.

Dans les versions précédentes de Citrix Virtual Apps and Desktops, telles que XenApp et XenDesktop 7.6, la base de données requise pour Citrix Virtual Apps and Desktops a été créée en tant que base de données unique lors de la configuration initiale du site (via Studio ou en exécutant des scripts sur SQL Server). Après l'installation, l'administrateur pourrait le scinder en différentes bases de données pour améliorer les performances ou se conformer aux consignes de sauvegarde/sécurité.

Avec les versions plus récentes de Citrix Virtual Apps and Desktops, vous pouvez créer les bases de données lors de la configuration initiale du site, ainsi que via Studio, ou en exécutant des scripts sur SQL Server. Votre base de données est automatiquement divisée en trois bases de données distinctes.

Pour les environnements avec de grandes bases de données de surveillance, une configuration idéale serait d'héberger la base de données de surveillance sur un serveur différent des bases de données de configuration du site et de journalisation de la configuration. Il enregistre plus de données, les changements se produisent plus fréquemment et les données ne sont pas considérées comme aussi critiques que les autres bases de données. Pour en savoir plus, consultezGuide de dimensionnement de la base de données la page 97 du Manuel VDI.

Chaque mise à jour cumulative (CU) pour la version de service à long terme (LTSR) contient des correctifs au schéma de base de données SQL. Par exemple, reportez-vous à la section CTX230536. Pour protéger au mieux votre environnement contre les problèmes inattendus, assurez-vous que vous disposez d'un processus de mise à niveau régulière de votre environnement vers la dernière CU. Assurez-vous également que la surveillance appropriée du serveur SQL et de la base de données sont en place pour détecter les événements de défaillance et les problèmes liés à l'utilisation élevée des ressources et à l'espace libre.

Interaction Citrix avec SQL

Les courtiers Citrix Virtual Apps and Desktops utilisent la base de données comme bus de messages pour les communications des courtiers, le stockage des données de configuration, de surveillance et d'audit. Les bases de données sont constamment utilisées et peuvent consommer des ressources de calcul importantes sur le serveur SQL.

Par exemple, l'énumération des ressources (ressources identifiées et présentées à l'utilisateur), le lancement des ressources et les étapes de démarrage de session nécessitent que Citrix Delivery Controller interagisse avec le serveur SQL.

Énumération : après l'authentification réussie via Citrix ADC et StoreFront, le Delivery Controller contacte la base de données du site Citrix pour vérifier quelles applications sont disponibles pour l'utilisateur, en fonction des informations d'identification AD. Lorsque les ressources sont identifiées, des informations supplémentaires, telles que les noms des applications, des postes de travail, des icônes, sont extraites de la base de données.

Lancement : Lorsque l'utilisateur sélectionne l'application ou le bureau à lancer, StoreFront lance une demande de lancement au Delivery Controller. Ensuite, le Delivery Controller contacte la base de données du site sur le serveur SQL pour sélectionner le VDA approprié à envoyer l'utilisateur.

Initialisation de session : après le démarrage de la session, le VDA est en contact avec Delivery Controller pour écrire des informations de session dans la base de données du site.

Recommandations de base de données

Pour s'assurer qu'une panne de serveur SQL a un impact minimal sur l'infrastructure Citrix Virtual Apps and Desktops, les clients peuvent choisir parmi les options de haute disponibilité suivantes prises en charge par Citrix :

- Groupes de disponibilité AlwaysOn
- Clustering de basculement AlwaysOn
- Groupes de disponibilité de base
- Hyperviseur HA *

> Remarque :
>
> Bien que Citrix prenne en charge Hypervisor HA, il n'est pas recommandé de l'utiliser dans des environnements hébergeant des applications EHR, où la disponibilité est de la plus haute importance.

Citrix et Epic recommandent d'utiliser la même approche de haute disponibilité pour les trois bases de données, même si la journalisation de la configuration et la surveillance de la disponibilité de la base de données ne sont pas nécessaires pour l'établissement de sessions utilisateur final. Par exemple, si vous envisagez d'utiliser le groupe de disponibilité SQL Always-On comme stratégie HA, utilisez-le pour les trois objets de base de données.

Nous vous recommandons également d'effectuer une sauvegarde quotidienne complète des bases de données Citrix elles-mêmes, en particulier la base de données du site. Les périodes de conservation varient en fonction des besoins de l'organisation, mais il est courant de conserver sept jours de sauvegardes complètes et d'au moins un mois de sauvegardes hebdomadaires. Les calendriers de sauvegarde des journaux de transactions doivent être basés sur une combinaison des normes de votre organisation et du taux de croissance du journal des transactions par rapport à la quantité de stockage disponible que vous devez allouer. Assurez-vous de surveiller le stockage disponible sur votre serveur SQL.

Alignez votre modèle de récupération pour les bases de données Citrix avec les exigences de l'approche de haute disponibilité que vous adoptez.

Conformément à la recommandation de Microsoft, les clients doivent configurer des plans de maintenance qui s'exécutent tous les soirs et toutes les semaines pour gérer les index de base de données. Les plans de maintenance peuvent simplement consister à réorganiser les index pendant la nuit pendant la semaine, et à reconstruire les index les fins de semaine.

Cette recommandation évite tout impact sur les performances de la reconstruction d'index volumineux pendant les opérations quotidiennes, en particulier pour une base de données de surveillance de grande taille.

Microsoft recommande que les index soient reconstruits s'ils sont fragmentés de plus de 30 % et réorganisés s'ils sont inférieurs à 30 %. Voir laMaintenance de la base de donnéessection.

Cache hôte local

Pour tenir compte des scénarios dans lesquels la base de données devient indisponible, Citrix a ajouté la fonctionnalité Local Host Cache (LHC) à la plate-forme Citrix Virtual Apps and Desktops 7.x (7.12 et versions ultérieures, y compris XenApp et XenDesktop 7.15 LTSR). L'activation de cette option permet aux utilisateurs d'applications publiées de se connecter si la communication entre Delivery Controller et la base de données de configuration du site Citrix est interrompue. Si SQL est configuré dans une architecture hautement disponible, telle que Always On, Mirroring ou Clustering, cette fonctionnalité offre une tolérance de pannes supplémentaire lorsqu'une panne SQL complète survient ou que la connectivité réseau est interrompue.

Cela ne doit pas être considéré comme une alternative à la haute disponibilité SQL, car la fonctionnalité de gestion de site n'est pas disponible pendant une panne SQL et le processus de basculement n'est pas instantané. En cas de panne SQL, la fonctionnalité de courtage est perdue jusqu'à ce qu'elle ait été transférée au LHC et que les VDA aient été réenregistrés. Ce scénario est également rencontré lors de la transition vers le mode normal de fonctionnement lorsque la connectivité/disponibilité SQL est restaurée.

Local Host Cache conserve une copie des données de site statiques dans une base de données locale SQL Express LocalDB sur chaque Delivery Controller, et s'appuie sur ces données lors d'une panne

de base de données pour prendre en charge en continu les enregistrements VDA et les demandes de courtage de session.

Considérations relatives à la conception du cache hôte local

En raison de la variation de la taille des déploiements de membres de la communauté Epic, il est recommandé de travailler en étroite collaboration avec Citrix pour déterminer les ressources supplémentaires nécessaires à l'utilisation du LHC.

- Considérations relatives à l'évolutivité
  - Les limites maximales documentées pour le LHC dans XenApp et Xendesktop 7.15 sont de 10 000 VDA dans une zone unique et de 40 000 VDA dans un déploiement multi-zone. Dans un environnement Citrix Virtual Apps, l'évolutivité du LHC et de la zone dépend du taux d'ouverture de session et du nombre d'utilisateurs. Par conséquent, l'évolutivité réelle observée dans votre environnement peut être inférieure aux maximums publiés. Pour cette architecture, nous vous recommandons d'envisager des zones supplémentaires si votre nombre de sessions attendu dépasse 10 000 et/ou si votre taux d'ouverture de session est supérieur à 10 utilisateurs par seconde.
- Dimensionnement du Delivery Controller : lorsque LHC est actif, le Delivery Controller (DC) principal élu par zone gère tous les enregistrements VDA, énumérations, lancements et mises à jour.
  - RAM : les services de cache de l'hôte local peuvent consommer 2 Go plus de RAM en fonction de la durée de l'interruption et du nombre de lancements d'utilisateur pendant la panne.
  - CPU : En raison de la charge CPU supplémentaire sur le contrôleur de domaine choisi, des cœurs supplémentaires doivent être considérés pour compenser.

  Une configuration d'UC de Controller, notamment le nombre de cœurs disponibles pour SQL Server Express LocalDB, affecte directement les performances de cache d'hôte local, encore plus que l'allocation de mémoire. Cette surcharge CPU est observée uniquement pendant la période d'interruption lorsque la base de données est inaccessible et que le service haute disponibilité est actif.

  Bien que LocalDB puisse utiliser plusieurs cœurs (jusqu'à 4), il est limité à une seule socket. Ajouter plus de sockets, par exemple, avoir 4 sockets avec 1 cœur chacune, n'améliore pas les performances. Citrix recommande plutôt d'utiliser plusieurs sockets avec plusieurs cœurs. Dans les tests Citrix, une configuration 2x3 (2 sockets, 3 cœurs) a fourni de meilleures performances que les configurations 4x1 et 6x1.
- Stockage : en mode cache de l'hôte local, l'utilisation du stockage augmente d'environ 1 Mo toutes les 2 à 3 minutes, en supposant une moyenne de 10 ouvertures de session par seconde.

La consommation de stockage augmente par rapport au taux d'ouverture de session. Pour plus d'informations, consultez l'Cache hôte localarticle.

Effets d'une panne de base de données

En cas de panne totale de la base de données, presque toutes les fonctions critiques du Delivery Controller sont affectées, ce qui souligne l'importance de concevoir et d'implémenter l'une des stratégies SQL HA recommandées. Le tableau suivant fait état de ces effets :

Composant	Impact de la panne de base de données
Base de données de configuration du site	Les utilisateurs ne peuvent pas se connecter ou se reconnecter à un poste de travail virtuel. **Remarque : Le** cache hôte local (LHC) permet aux utilisateurs disposant de bureaux partagés hébergés, d'applications Windows et navigateur hébergés et de bureaux personnels de se reconnecter à leurs applications et postes de travail même lorsque la base de données du site n'est pas disponible. En mode LHC, les données de surveillance ne sont pas collectées et les modifications de configuration ne peuvent pas être apportées au Site.
Base de données de surveillance	Director n'affiche aucune donnée historique et Studio ne peut pas être démarré. Le courtage des demandes d'utilisateurs entrantes et des sessions utilisateur existantes n'est pas affecté.
Base de données de journalisation de la configuration	Si **Autoriser les modifications lorsque la base de données est déconnectée** a été activée dans les préférences de journalisation Citrix Virtual Apps and Desktops, une panne de la base de données de journalisation de configuration n'a aucun impact (sauf les modifications de configuration ne sont pas enregistrées). Sinon, les administrateurs ne peuvent pas apporter de modifications à Citrix Virtual Apps and Desktops.

Recommandation de dimensionnement SQL

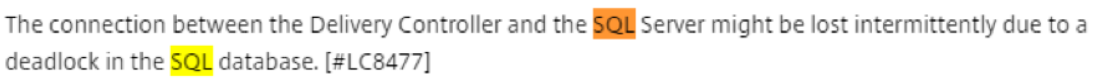
Le serveur SQL doit être dimensionné correctement pour garantir les performances et la stabilité d'un environnement. Étant donné que chaque produit Citrix utilise SQL Server d'une manière différente et que chaque client a des modèles d'utilisation différents, aucune recommandation générique de dimensionnement globale ne peut être fournie. Au lieu de cela, les recommandations de dimensionnement du serveur SQL par produit sont fournies ci-dessous, et les performances doivent être soigneusement surveillées pendant le déploiement afin de valider les hypothèses de dimensionnement.

Pour un environnement SQL hébergeant uniquement des bases de données liées à Citrix, les serveurs SQL doivent être provisionnés avec un minimum de 4 vCPU et 8 Go de RAM pour un maximum de 10 000 utilisateurs. Pour les déploiements plus importants ou les déploiements avec des taux d'ouverture de session élevés, nous recommandons un minimum de 8 vCPU et 16 Go de RAM. Pour plus d'informations sur les concepts de dimensionnement de base de données SQL pour les déploiements Citrix Virtual Apps and Desktops 7.x, reportez-vous à la section Taille de la base de données Citrix XenDesktop 7.x. Cet article contient également des informations sur les caractéristiques de la charge de travail, telles que le taux de croissance estimé du journal des transactions.

Gardez à l'esprit que la base de données de surveillance varie en taille en fonction des paramètres de rétention des données. XenApp et XenDesktop 7.15 LTSR dispose de plus d'options que 7.6 LTSR, une fois que la capacité de capturer des données granulaires de performances VDA a été ajoutée au produit. Pour plus d'informations sur la configuration de ces paramètres, reportez-vous à la section Surveillance des paramètres de stratégie et tenez-en compte dans les calculs de dimensionnement de la base de données.

Mises à jour et correctifs CU

Plusieurs fois par an, Citrix publie des CU pour Citrix Virtual Apps and Desktops LTSR. Ces UC ne contiennent que des mises à jour de sécurité et des corrections de bogues, sans nouvelles fonctionnalités introduites. Citrix recommande d'exécuter les CU les plus récentes, car elles corrigent les problèmes identifiés dans le produit. Certains de ces correctifs sont liés à SQL. Ils abordent les problèmes, tels que le verrouillage, les blocages, les procédures de magasin, qui ont été identifiés par Citrix ou nos clients. Par exemple, il existe un certain nombre de correctifs liés à SQL dans les UC XenApp 7.6 jusqu'à CU5. La recommandation serait de passer en revue la section **Problèmes résolus** pour chaque CU et de rechercher **SQL** dans la page.



> Remarque :
>
> LC8477 a été publié en 7.6 CU5 et 7.17

Références supplémentaires

- XenApp et XenDesktop 7.15 LTSR
- Manuel VDI
- Dimensionnement de la base de données Citrix
- Cache d'hôte local Citrix

Contribué par Henry Vernov, ingénieur système principal.

Mises à jour des modèles de gestion des stratégies de groupe pour XenApp et XenDesktop

January 8, 2020

Les modèles sont une source de création de stratégies à partir d'un point de départ prédéfini. Vous pouvez les importer ou les exporter. Les modèles Citrix intégrés, optimisés pour des environnements ou des conditions réseau spécifiques, peuvent être utilisés comme suit :

- Source pour créer vos propres stratégies et modèles à partager entre les Sites.
- Une référence pour faciliter la comparaison des résultats entre les déploiements car vous pouvez citer les résultats, par exemple, "… lors de l'utilisation du modèle Citrix x ou y…"
- Méthode de communication de stratégies avec Citrix Support ou des tiers approuvés en important ou en exportant des modèles.

À propos de cet article

Cet article contient des liens pour télécharger des modèles supplémentaires et des mises à jour vers les modèles Citrix intégrés au package de gestion des stratégies de groupe XenApp et XenDesktop.

Bien que vous puissiez toujours trouver des modèles fournis par Citrix Studio et dans un éditeur d'objet de stratégie de groupe (après avoir installé le package de gestion de stratégie de groupe), nous voulons être en mesure de vous fournir rapidement des mises à jour et des modèles pour des scénarios au-delà de ce qui est inclus dans le package d'installation.

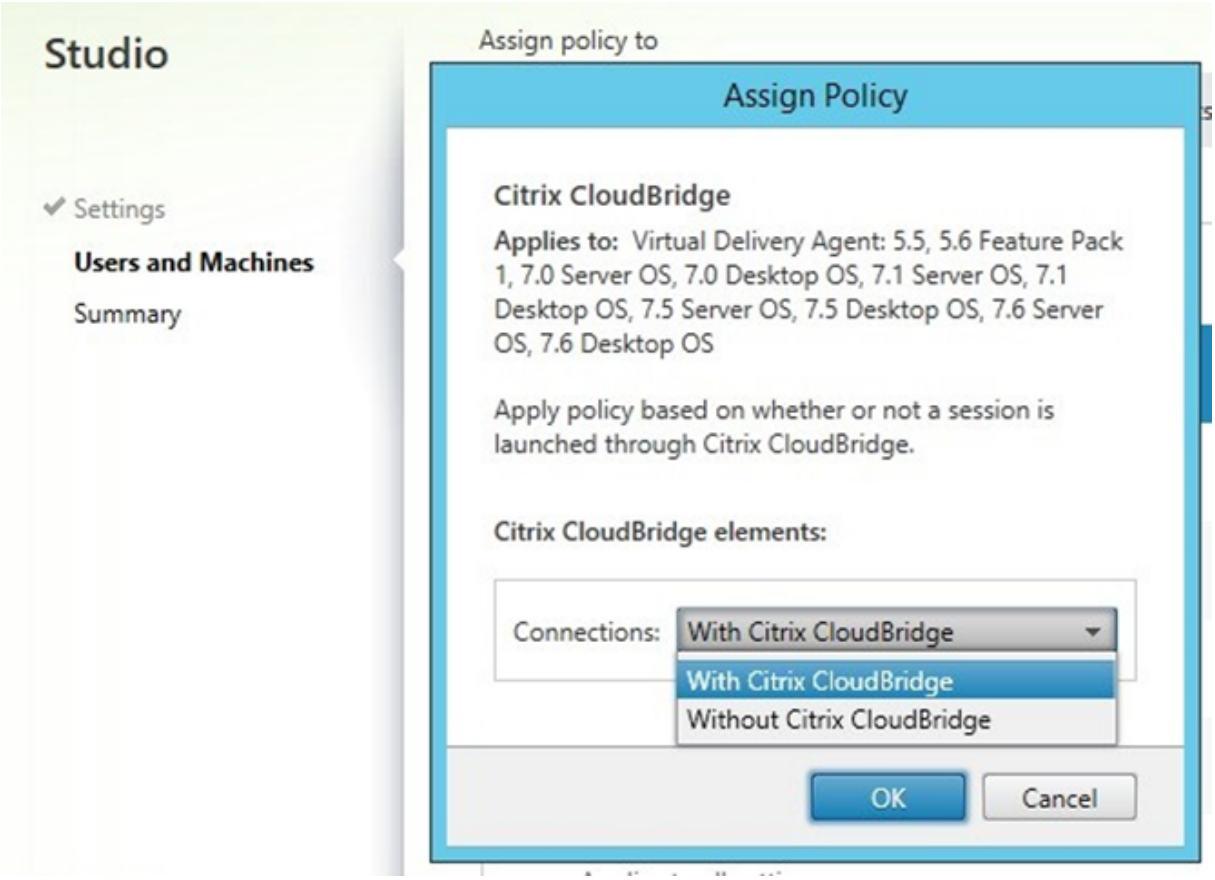
Les modèles de cet article doivent être utilisés avec la dernière version de XenApp et XenDesktop, sauf indication contraire. Alors que leur nom et leur description sont en anglais, vous pouvez les importer et les utiliser dans d'autres langues.

Modèles

Réseau étendu CloudBridge

Ce modèle est une mise à jour d'un modèle Citrix intégré, conçu pour maximiser les avantages de l'accélération WAN CloudBridge. Il configure les paramètres qui permettent à XenApp et XenDesktop de maximiser les avantages des périphériques d'accélération WAN CloudBridge dans le chemin entre un client et un VDA.

Vous pouvez affecter ce modèle spécifiquement aux sessions où CloudBridge est présent à l'aide du filtre de stratégie « Avec Citrix CloudBridge », ce qui permet d'utiliser différents paramètres de stratégie pour CloudBridge et pour d'autres connexions.



- Télécharger le modèle
  Remarque : Il apparaîtra sous la forme d'un modèle personnalisé après l'avoir importé.

Citrix Receiver pour Chrome

Ce modèle expose certains paramètres de stratégie disponibles qui ont un effet exclusif ou spécial sur les sessions à partir des points de terminaison Chromebook.

- Télécharger le modèle

Citrix Receiver pour HTML5

Ce modèle inclut les paramètres applicables aux sessions utilisant Citrix Receiver pour HTML5. Dans cette version de Citrix Receiver, vous devez activer WebSockets car dans l'installation par défaut de XenApp et XenDesktop, il est désactivé.

- Télécharger le modèle

Améliorer l'expérience utilisateur dans les réseaux peu fiables

Ce modèle active le protocole graphique basé sur Framehawk UDP et expose certains des paramètres de stratégie disponibles qui ont un effet exclusif ou spécial sur ces sessions.

- Télécharger le modèle

Sessions d'application de passage (double saut)

Dans les déploiements avec des bureaux virtuels administrés, regroupés ou hébergés par RDS, il est courant de fournir aux utilisateurs des applications qui ne se trouvent pas dans l'image de bureau à l'aide d'une session pass-through vers XenApp. Ce modèle est destiné aux déploiements XenApp fournissant des applications aux postes de travail.

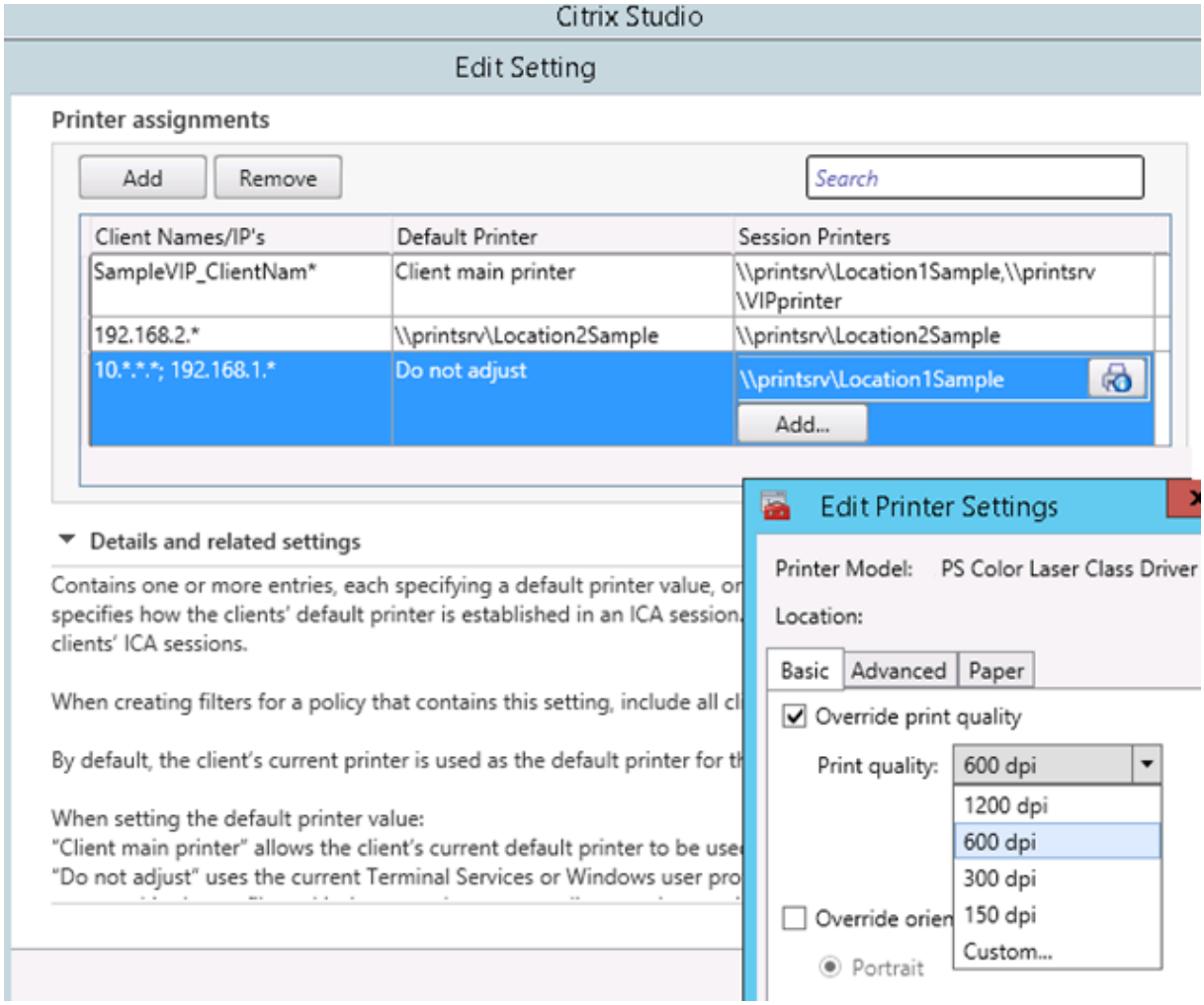
Il devrait diminuer l'utilisation du processeur dans le serveur de session d'application et, en même temps, permettre à la session de bureau d'optimiser la remise au périphérique client de point de terminaison. Pour ce faire, désactivez le codec vidéo pour la compression dans les graphiques et distribuez des graphiques compressés de l'application au bureau.

IMPORTANT : L'utilisation de ce modèle augmente le trafic entre les applications et les postes de travail.

- Télécharger le modèle

Serveur d'impression universel Citrix

Il s'agit d'un exemple de modèle conçu pour être utilisé comme point de départ pour configurer votre déploiement de Citrix Universal Print Server. Une stratégie résultante permet d'utiliser des pilotes spécifiques à l'imprimante s'ils sont déjà installés par l'administrateur du VDA ; sinon, le pilote d'imprimante universelle Citrix est utilisé. Il répertorie également des exemples d'affectations d'imprimante (nouvelle alternative aux imprimantes de session et paramètres d'imprimante par défaut), qui doivent être remplacées par les affectations appropriées pour votre déploiement. Ce modèle nécessite un accès domaine aux imprimantes pour une configuration correcte.



- Télécharger le modèle

Modèles pour les versions précédentes

Le lien suivant inclut les modèles pour les versions antérieures à 7.6FP3. Ces modèles apparaissent en tant que modèles personnalisés lors de leur importation.

- Télécharger les modèles

Avertissement

Les exemples mentionnés ci-dessus et les modèles de politique téléchargés (l'exemple de code) vous sont fournis en l'état sans aucune représentation, garantie ou condition de quelque nature que ce soit. Vous pouvez les utiliser, les modifier et les distribuer à vos propres risques. CITRIX DÉCLINE TOUTE GARANTIE, EXPRESSE, IMPLICITE, ÉCRITE, ORALE OU LÉGALE, Y COMPRIS, SANS S'Y LIMITER, LES GARANTIES DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, DE TITRE ET DE

NON-CONTREFAÇON. Sans limiter la généralité de ce qui précède, vous reconnaissez et acceptez que (a) l'exemple de code peut présenter des erreurs, des défauts de conception ou d'autres problèmes, pouvant entraîner la perte de données ou des dommages à la propriété ; (b) il peut ne pas être possible de rendre l'exemple de code pleinement fonctionnel ; et (c) Citrix peut, sans préavis ou responsabilité envers vous, cessez de rendre disponible la version actuelle et/ou toute version future de l'exemple de code. En aucun cas, le code ne doit être utilisé pour appuyer des activités ultra-dangereuses, y compris, mais sans s'y limiter, les activités de soutien à la vie ou de dynamitage. NI CITRIX NI SES SOCIÉTÉS AFFILIÉES OU MANDATAIRES NE SERONT RESPONSABLES, EN CAS DE VIOLATION DE CONTRAT OU DE TOUTE AUTRE THÉORIE DE RESPONSABILITÉ, DE TOUT DOMMAGE QUE CE SOIT DÉCOULANT DE L'UTILISATION DU CODE TYPE, Y COMPRIS, SANS S'Y LIMITER, LES DOMMAGES DIRECTS, SPÉCIAUX, ACCESSOIRES, PUNITIFS, CONSÉCUTIFS OU AUTRES, MÊME S'ILS SONT AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES. Bien que le copyright dans le code appartient à Citrix, toute distribution du code doit inclure uniquement votre propre attribution de copyright standard, et non celle de Citrix. Vous acceptez d'indemniser et de défendre Citrix contre toute réclamation découlant de votre utilisation, modification ou distribution du code.

*Cet article est apparu à l'origine dans le Centre de connaissances Citrix Support.

XenApp et XenDesktop 7.11 à la version actuelle : Améliorations de latence et de blocage des requêtes SQL

January 8, 2020

Les informations sur les performances pour le courtage avec latence ont été fournies dans l'articleXenApp et XenDesktop 7.7 : zones, latence et performances de courtage. Cet article décrit les améliorations pour le courtage avec latence de XenApp et XenDesktop 7.11. Il décrit également les améliorations visant à éviter le blocage lors de l'enregistrement VDA.

Courtage avec des améliorations de latence

Dans XenApp et XenDesktop 7.11, nous avons revisité le code SQL de courtage principal qui détermine quel VDA est le moins chargé, puis envoie une demande de lancement à ce VDA. Nous avons décidé de passer d'un algorithme d'équilibrage de charge « parfait » à un algorithme d'équilibrage de charge « assez bon ».

Avant XenApp et XenDesktop 7.11, le code recherchait le VDA le moins chargé et verrouillait ou bloquerait d'autres demandes de lancement jusqu'à ce que ce VDA devienne disponible. Cela a bloqué toutes les autres demandes de courtage.

À partir de XenApp et XenDesktop 7.11, le code recherche le programme de travail le moins chargé qui n'est pas actuellement verrouillé. Cela signifie que, bien que nous ne puissions pas obtenir le tra-

vailleur le moins chargé - peut-être que nous n'obtenons que le deuxième ou le troisième moins chargé - nous pouvons le faire sans verrouiller toutes les autres demandes de lancement. Si nous ne trouvons pas de programme de travail déverrouillé, nous nous asseyons et attendons les verrouillages. Avec suffisamment de VDA, il est rare de les trouver tous verrouillés en même temps, mais quand cela arrive, le comportement est le même qu'avec l'algorithme précédent.

Dans certains scénarios, les administrateurs peuvent remarquer une légère différence dans l'équilibrage de charge, mais il doit être très attentif pour remarquer que nous n'utilisons pas le VDA le moins chargé.

Il existe d'autres emplacements dans le code de courtage principal où les problèmes de blocage SQL ont été améliorés. Citrix recommande que les grands sites utilisent un courtier 7.13 ou 7.6 CU3 pour avoir toutes les améliorations actuellement connues.

Résultats du rendement

Le tableau suivant ajoute deux points de données aux données duarticle précédentpour afficher le courtage résultant avec des améliorations de latence :

Version du produit	**7.7**	**7.11+**	**7.7**	**7.7**	**7.11+**
Latence (ms)	90	90	250	250	250
Demandes simultanées	48	48	36	48	48
Temps de réponse moyen (s)	12.9	3.7	26.7	S.O.	7.6
Demandes de courtage par seconde	3.7	12.6	1.3	S.O.	6.3
Erreurs (%)	0	0	4.6	42.8	0
Délai de lancement de 10 000 utilisateurs	44 min 55 s	13 min 10 s	2 h 03 min	s.o.	26 min 27 s

Comme vous pouvez le voir avec une latence de 250 ms, XenApp et XenDesktop 7.11 surpasse maintenant le code 7.7 à 90 ms. Donc, plutôt que de passer du temps à tester beaucoup de points de données, nous avons testé un qui a échoué précédemment. Vous pouvez voir qu'avec 7.11 ou ver-

sion ultérieure, les utilisateurs bénéficient d'un courtage plus rapide des ressources, même avec une latence entre un courtier et le serveur SQL.

Les clients des Controller LTSR 7.6 CU3 bénéficient également des mêmes améliorations. Bien que nous ne nous attendions pas à ce que LTSR 7.6 CU3 soit déployé avec latence, ces modifications améliorent encore les performances même sans latence - et nous savons que certains clients ont LTSR 7.6 CU3 avec une certaine latence.

Sérialisations de tempête d'enregistrement

Malheureusement, un domaine que nous savons qu'il y a un verrou est l'enregistrement VDA. La raison de la serrure est d'éviter les blocages lors de l'enregistrement des travailleurs. Nous avons maintenant une meilleure compréhension de la cause des blocages, ce qui était dû au fait que les sessions d'un travailleur ne sont pas verrouillées dans un ordre cohérent sur plusieurs threads d'enregistrement. Nous faisons maintenant le verrouillage de session par identifiant de session, ce qui arrête le blocage des enregistrements VDA.

Nous avons testé ce changement de comportement en interne et constaté qu'il a aidé à résoudre certains problèmes lors de nos tests d'échelle de réenregistrement. Cependant, parce que certains clients ont des environnements très complexes, nous n'avons pas complètement supprimé ce verrou, pour laisser du temps pour plus de tests. Au lieu de cela, nous avons fourni un accordable sur l'utilisation de ce verrou pour les clients avec XenApp et XenDesktop 7.12 ou version ultérieure. Ce réglage se trouve dans la table chb_Config.Site de la base de données XenApp et XenDesktop 7.12 :

```
1 sélectionnez SerializeMultiSessionAudits,
     SerializeMultiSessionDeregistrations à partir de chb_Config.site
2
3 SerializeMultiSessionAudits SerializeMultiSessionDeregistrations
4
5 -------------------------- ----------------------------------
6
7 1 1
```

Vous pouvez définir ces indicateurs sur 0 pour supprimer l'utilisation du verrou :

```
1 update chb_config.Site set SerializeMultiSessionAudits=0,
     SerializeMultiSessionDeregistrations=0
2
3 sélectionnez SerializeMultiSessionAudits,
     SerializeMultiSessionDeregistrations à partir de chb_Config.site
4
5 (1 ligne (s) affectée (s))
6
7 SerializeMultiSessionAudits SerializeMultiSessionDeregistrations
```



```
 8
 9  -------------------------- ----------------------------------
10
11  0 0
```

On s'attend à ce que les versions futures ne fassent pas ce verrouillage, et qu'elles fournissent l'accordable aux clients qui ont besoin de réactiver le verrouillage.

Cet article a été modifié à partir d'un billet de blog écrit par Chris Gilbert. Pour lire le blog original et pour voir les commentaires, allez à https://www.citrix.com/blogs/2017/03/06/latency-and-sql-blocking-query-improvements.

Guide de dimensionnement de base de données pour XenApp et XenDesktop versions 7.6 à la version actuelle

January 8, 2020

Avertissement

Ce document contient des liens vers des sites Web contrôlés par des parties autres que Citrix. Citrix n'est pas responsable du contenu ou de l'utilisation de ces sites Web tiers et n'approuve pas ou n'accepte aucune responsabilité. Citrix vous fournit ces liens uniquement à titre de commodité, et l'inclusion de tout lien n'implique pas l'approbation par Citrix du site Web lié. Il est de votre responsabilité de prendre des précautions pour vous assurer que ce que vous choisissez pour votre utilisation est exempt de virus ou d'autres éléments de nature destructrice.

Généralités

Un déploiement XenDesktop 7 typique se compose de trois bases de données, comme suit :

- Base de données de configuration de site
  Stocke la configuration actuelle et l'état du déploiement XenDesktop
- Monitoring Database
  Stocke les données historiques à afficher dans Director
- Base de données de journalisation de la configuration
  Suit les modifications de configuration apportées au déploiement de XenDesktop

Par défaut, les bases de données de journalisation et de surveillance de la configuration (bases de données secondaires) se trouvent sur le même serveur que la base de données de configuration du

site. Initialement, les trois bases de données ont le même nom. Citrix vous recommande de modifier l'emplacement des bases de données secondaires après la création d'un site.

Un déploiement typique utilise également la base de données temporaire, TempDB, fournie par SQL Server.

Chaque base de données a un but différent et se développe à un rythme différent.

Ce document fournit des informations sur chaque base de données et met en évidence les principales considérations à prendre en compte lors du dimensionnement des bases de données pour prendre en charge XenDesktop 7.

Note : Tous les chiffres fournis sont des estimations. Il faut s'attendre à des variations entre les déploiements.

Les différences de taille entre les postes de travail partagés hébergés (HSD) et l'infrastructure de bureau virtuel (VDI) sont également notées dans ce document. Les environnements mixtes devront combiner les estimations des deux types de postes de travail pour générer une estimation de la taille globale de la base de données.

Modifications du document pour XenDesktop 7.6

Ce document a été étendu à la section 7.6 XenDesktop. Cela devait permettre des mises à jour sur les modifications de taille des fonctions ajoutées dans 7.6. Les trois nouvelles fonctionnalités qui ont un impact sur le dimensionnement de la base de données sont les suivantes :

- Connection Leasing : les fichiers de bail compressés sont stockés dans la base de données du site
- Surveillance de l'utilisation des applications : les détails de toutes les applications utilisées dans l'environnement sont stockés dans la base de données du moniteur
- Surveillance de l'inventaire des correctifs — détails des correctifs Citrix appliqués aux Controller, VDA et images VDA dans l'environnement

Les informations sur le dimensionnement du tableau ont été mises à jour ci-dessous. La croissance des transactions par seconde et du journal des transactions était semblable dans 7,6 à 7,5, de sorte qu'aucune mise à jour n'a été apportée à ces sections.

Considérations de haut niveau

Base de données du site

La base de données du site contient des informations de configuration pour l'exécution du système.

Son utilisation est caractérisée par :

- La taille maximale est atteinte pendant les heures de pointe lorsque les ouvertures de session des utilisateurs génèrent des informations de session et de connexion à suivre.
- La taille minimale est atteinte lorsqu'il n'y a pas de session active et que les VDA sont tous arrêtés et non enregistrés.
- La taille maximale est atteinte après 48 heures, car la base de données stocke très peu d'informations persistantes.
  Cela est dû à un petit journal des connexions maintenu dans la base de données du site pendant 48 heures.
- La taille de ligne de base de données augmente à mesure que les informations de configuration d'un site augmentent.
  Autrement dit, plus de travailleurs et d'utilisateurs consomment plus d'espace de base de données.
- Des niveaux élevés de transactions par seconde se produisent pendant l'ouverture de session, car chaque ouverture de session utilisateur nécessite plusieurs transactions individuelles et évolue en fonction du taux de lancement simultané.
- Bruit de fond de faible niveau des transactions de pulsation VDA. Chaque VDA fournit un rythme cardiaque une fois toutes les 5 minutes et cette mise à jour déclenche une transaction sur la base de données.

Impact de la défaillance

Une panne de la base de données du site rend le système impossible à gérer et à surveiller. Les connexions existantes sont maintenues. Dans XenDesktop 7.6 Connection Leasing permet de créer de nouvelles connexions et reconnexions. Dans les versions précédentes, de nouvelles connexions et reconnexions ne sont pas possibles.

Base de données de surveillance

La base de données de surveillance contient des informations historiques sur le site. Ces informations sont utilisées par Director pour afficher des informations historiques.

Son utilisation est caractérisée par :

- La taille maximale est contrôlée par la période de rétention configurée, comme suit :
  - Pour les clients non-Platinum, la valeur par défaut est de 7 jours, avec une période maximale de 7 jours.
  - Pour les clients Platinum, la valeur par défaut est de 90 jours, sans période maximale.
- La taille maximale peut prendre un certain temps à atteindre, car le système doit atteindre la période de rétention configurée.
- Des niveaux faibles de transactions par seconde se produisent en raison de la nature par lots des mises à jour par le service de surveillance. Il est rare de voir les transactions par seconde

passer les 20 transactions par seconde.
- Certaines transactions en arrière-plan causées par des appels de consolidation réguliers du service de surveillance.
- Le traitement du jour au lendemain est effectué pour supprimer les données en dehors de la période de rétention configurée.

Impact de la défaillance

Une panne de la base de données de surveillance empêche la collecte de données pour le site, ce qui signifie que les données ne sont pas visibles au sein de Director.

Base de données de journalisation de la configuration

La base de données de journalisation de la configuration contient un journal historique de toutes les modifications de configuration apportées au site. Ces informations sont utilisées pour générer des rapports ou pour être affichées dans Studio.

Son utilisation est caractérisée par :

- La taille maximale est difficile à prévoir car elle dépend de l'activité de configuration.
- Toutes les actions, par exemple, la réinitialisation de session, à partir de Director sont consignées dans cette base de données, de sorte qu'il peut y avoir une croissance lente lorsque les administrateurs utilisent Director.
- Transactions minimales se produisant sur la base de données lorsqu'aucune modification de configuration n'est apportée.
- Un faible taux de transaction pendant les mises à jour, car les mises à jour sont groupées dans la mesure du possible.
- Suppression manuelle des données. Les données de la base de données de journalisation de la configuration ne sont soumises à aucune stratégie de rétention et ne sont pas supprimées, sauf si elles sont effectuées manuellement par un administrateur.

Impact de la défaillance

L'impact d'une panne de la base de données de journalisation de la configuration dépend de la configuration du site, comme suit :

- Si le site n'autorise pas les modifications lorsque la base de données de journalisation de la configuration n'est pas disponible, il n'est pas possible de reconfigurer le déploiement XenDesktop.
- Si le site autorise les modifications lorsque la base de données de journalisation de la configuration n'est pas disponible, des modifications de configuration non suivies peuvent être apportées au déploiement XenDesktop.

Base de données temporaire

La base de données temporaire est une base de données à l'échelle du système fournie par SQL Server. Il est utilisé comme magasin de versions pour l'isolation de snapshots en lecture. XenDesktop 7 utilise cette fonctionnalité SQL Server pour réduire la contention de verrouillage dans les bases de données XenDesktop.

La taille du magasin de versions dépend du nombre de transactions actives. En général, cependant, il ne dépasse pas quelques MBs.

Les performances de TempDB ont un impact sur les performances du courtage XenDesktop, car toutes les transactions qui génèrent de nouvelles données nécessitent de l'espace TempDB. XenDesktop, cependant, a tendance à avoir des transactions de courte durée, ce qui permet de garder la taille du magasin de version petite.

La base de données temporaire est également utilisée lorsque les requêtes génèrent de grands ensembles de résultats intermédiaires.

Des conseils sur le dimensionnement et la configuration du TempDB peuvent être trouvés dans MSDN :

http://technet.microsoft.com/en-us/library/ms175527(v=sql.105).aspx

La zone principale de conflit est centrée sur le nombre de fichiers à utiliser. Les anciennes versions de SQL Server, telles que SQL Server 2000, nécessitent plus de fichiers que les versions plus récentes. Pour plus d'informations sur le nombre de fichiers à utiliser, voir :

http://www.sqlskills.com/blogs/paul/a-sql-server-dba-myth-a-day-1230-tempdb-should-alwayshave-one-data-file-per-processor-core/

Isolation de cliché validée en lecture

Citrix recommande que toutes les bases de données XenDesktop 7 utilisent l'isolation de snapshots validés en lecture. Pour plus d'informations, reportez-vous à la section Comment faire pour activer l'instantané validé en lecture dans XenDesktop.

Dimensionnement des bases de données

La taille des bases de données dépend d'un certain nombre de facteurs clés, notamment le nombre de sessions et de connexions créées au cours d'une journée de travail.

Une session est un poste de travail ou une application exécutée pendant une période de temps qui peut être déconnecté et reconnecté à.

Une connexion est une fois qu'un utilisateur se connecte à une session. La déconnexion ferme la connexion, mais pas la session. Lorsqu'un utilisateur se reconnecte, cela crée une nouvelle connexion à une session existante.

Base de données du site

La taille maximale de la base de données de site est basée sur le nombre de VDA et de sessions actives, comme suit :

Utilisateurs	Applications	Type	Taille de crête prévue 7,5 (Mo)	Taille de crête prévue 7,6 (Mo)
1 000	50	HSD	30	31
10 000	100	HSD	60	198
100 000	200	HSD	330	752
1 000	S.O.	VDI	30	30
10 000	S.O.	VDI	115	121
40 000	S.O.	VDI	390	426

Chaque application publiée ajoute 110 Ko à la base de données pour stocker chaque icône unique.

> Remarque :
>
> L'augmentation de la taille de 7.6 est due au fait que les baux de connexion sont stockés dans la base de données dans le cadre de la réplication entre les Controller.

Base de données de surveillance

Parmi les trois bases de données, on s'attend à ce que la base de données de surveillance devienne la plus importante au fil du temps.

Sa taille dépend de nombreux facteurs, y compris les suivants :

- Nombre d'utilisateurs
- Nombre de sessions
- Nombre de connexions
- Tâches VDI ou HSD
- Période de rétention configurée

Voici des estimations de la taille de la base de données à un certain nombre de points de données. Ces données sont une estimation basée sur les données vues lors du test de mise à l'échelle XenDesktop. On estime que les estimations sont réalistes.

Toutefois, les clients qui tiennent à jour leur base de données peuvent constater que leur base de données est plus petite que les estimations.

Les utilisateurs HSD sont basés sur 100 utilisateurs par serveur HSD.

Périodes de rétention maximales

La quantité maximale de données conservées est contrôlée par licence, comme suit :

- Les clients non-Platinum peuvent conserver jusqu'à 1 semaine (7 jours) de données.
- Les clients Platinum peuvent conserver des données illimitées ; la valeur par défaut est de 3 mois (90 jours).

Les périodes de rétention peuvent être ajustées à l'aide de l'*applet de commande Set-MonitorConfiguration* .

Une fois que les données sont plus anciennes que la période de rétention configurée, elles sont supprimées de la base de données.

Taille de la base de données de surveillance XenDesktop 7.5

Estimations avec 1 connexion et 1 session par utilisateur avec une semaine de travail de 5 jours

Utilisateurs	Type	1 semaine (Mo)	1 mois (Mo)	3 mois (MB)	1 an (MB)
1 000	HSD	151	70	230	900
10 000	HSD	2 830	600	1,950	7,700
100 000	HSD	1,500	5,900	19,000	76,000
1 000	VDI	15	55	170	670
10 000	VDI	120	440	1,400	5,500
40 000	VDI	464	1,700	5,400	21,500

Estimations avec 2 connexions et 1 session par utilisateur avec une semaine de travail de 5 jours

Utilisateurs	Type	1 semaine (Mo)	1 mois (Mo)	3 mois (MB)	1 an (MB)
1 000	HSD	30	100	330	1,300
10 000	HSD	240	925	3 000	12,000
100 000	HSD	2,400	9,200	30,000	119,000
1 000	VDI	25	85	280	1,100
10 000	VDI	200	750	2,500	9,800
40 000	VDI	800	3 000	9,700	38,600

Notez que les HSD génèrent plus de données au fil du temps en raison de la journalisation des informations d'équilibrage de charge, mais sont initialement d'une taille similaire à celle des postes de travail VDI.

XenDesktop 7.6 Surveillance du dimensionnement de la base de données

Les principaux changements par rapport à 7.5 sont :

- Informations sur les correctifs
  Les données ci-dessous sont basées sur 3 correctifs par tâche (VDI ou HSD)
- Historique de l'utilisation des applications
  Ceci est principalement pertinent pour les systèmes HSD.

Estimations avec 1 connexion et 1 session par utilisateur avec une semaine de travail de 5 jours

Utilisateurs	Type	1 semaine (Mo)	1 mois (Mo)	3 mois (MB)	1 an (MB)
1 000	HSD	151	605	1,966	7,865
10 000	HSD	2 830	11,301	36,712	146,834
100 000	HSD	7,194	28,585	92,758	370,841
1 000	VDI	13	49	157	622
10 000	VDI	117	409	1,287	5,090
40 000	VDI	460	1,610	5,058	19,999

Estimations avec 2 connexions et 1 session par utilisateur avec une semaine de travail de 5 jours

Utilisateurs	Type	1 semaine (Mo)	1 mois (Mo)	3 mois (MB)	1 an (MB)
1 000	HSD	159	635	2,063	8,251
10 000	HSD	2,904	11,599	37,684	150,718
100 000	HSD	7,940	31,572	102,465	409,672
1 000	VDI	21	79	253	1,008
10 000	VDI	191	708	2,258	8,974
40 000	VDI	759	2,805	8,941	35,532

Base de données de journalisation de la configuration

Il est beaucoup plus difficile de fournir des conseils pour dimensionner la base de données de journalisation de la configuration car elle varie considérablement en fonction de l'activité quotidienne de Director et de la taille du site configuré.

Les activités qui ont un impact sur les sessions ou les utilisateurs sont enregistrées et comprennent, par exemple, la fermeture de session et la réinitialisation. Les activités passives, telles que la liste des sessions d'un utilisateur, ne le sont pas.

Le mécanisme utilisé pour déployer des postes de travail a également un impact sur la taille des données enregistrées.

Dans les environnements HSD qui n'utilisent pas MCS, la taille de la base de données tend à se situer entre 30 Mo et 40 Mo.

Pour les environnements MCS, la taille de la base de données peut facilement dépasser 200 Mo en raison de la journalisation de toutes les données de construction de machines virtuelles.

Aucune modification significative n'a été apportée à la base de données de journalisation de la configuration 7.6.

Activité de base de données lors de l'ouverture de session de 100 000 sessions HSD

Pendant les tests d'évolutivité, simulant 100 000 ouvertures de session HSD, la croissance du journal des transactions a été mesurée selon deux taux d'ouverture de session, comme suit :

- 100 000 utilisateurs se connectent plus d'une heure
- 100 000 utilisateurs se connectent plus de 2 heures

Ces taux ont été choisis pour fournir des exemples de points de données.

L'environnement comprend :

- 2 Delivery Controller
- 43 tâches HSD VDA
- 3 serveurs SQL, configurés avec les bases de données, conservés dans un groupe de disponibilité Always On

Des détails sur les configurations de serveur sont fournis à la fin de ce document.

Croissance du journal des transactions

La croissance du journal des transactions pour toutes les bases de données a été surveillée à l'aide du compteur du moniteur de performances SQLServer : Bases de données — Fichier (s) journal (s) utilisé (s) Taille (Ko).

Base de données du site

Lorsque le système est inactif, le journal des transactions augmente de 3,5 Mo par heure. Il s'agit d'une combinaison de battements cardiaques VDA et Broker Service.

Test	Croissance totale de l'ouverture de session (Mo)	Croissance totale de la fermeture de session (Mo)
100k sur 1 heure	1 900	1 150
100k sur 2 heures	1 900	1 150

La croissance du log est linéaire sur la période mesurée. Ces données suggèrent que, par ouverture de session utilisateur, le journal des transactions augmente de 20 Ko. Par fermeture de session utilisateur, le journal des transactions augmente de 12 Ko.

Par conséquent, la croissance par jour est de 32 Ko par cycle d'ouverture de session utilisateur et de fermeture de session.

Base de données de surveillance

Lorsque le système est inactif, le journal des transactions augmente de 30,5 Mo par heure. Il s'agit d'une combinaison de procédures stockées de consolidation et de mises à jour de l'index de charge HSD VDA.

Test	Croissance totale de l'ouverture de session (Mo)	Croissance totale de la fermeture de session (Mo)
100 000 sur 1 heure	670	190
100 000 sur 2 heures	650	220

La croissance logarithmique est linéaire sur la période mesurée. Ces données suggèrent que par ouverture de session utilisateur, le journal des transactions augmente de 7 Ko. Par fermeture de session utilisateur, le journal des transactions augmente de 2 Ko.

Par conséquent, la croissance par jour est de 9 Ko par cycle d'ouverture de session utilisateur et de fermeture de session.

Transactions par seconde

La croissance du journal des transactions pour toutes les bases de données a été surveillée à l'aide des compteurs de surveillance de performances suivants :

- SQLServer : Bases de données — Transactions/seconde
- SQLServer : Bases de données — Écriture de transactions/seconde

Base de données du site

Lorsque le système est inactif, il y a 5 transactions/seconde dont 1 Write Transaction/seconde maintient les battements cardiaques VDA et Broker.

> **Note :** Ces chiffres sont des estimations tirées des périodes indiquées. La charge exacte varie en fonction du nombre de lancements simultanés par seconde.

Test	Transactions d'ouverture de session par seconde	Transactions d'écriture d'ouverture de session par seconde	Transactions de fermeture de session par seconde	Transactions d'écriture de fermeture de session par seconde
100 000 sur 1 heure	870	310	250	100
100 000 sur 2 heures	475	170	140	60

Base de données de surveillance

Lorsque le système est inactif, les procédures stockées de consolidation s'exécutent une fois par minute et génèrent des transactions. Toutefois, le niveau des transactions est faible. En général, il existe 2 à 3 transactions et 1 transaction d'écriture pour chaque procédure stockée de consolidation, et 3 procédures stockées de consolidation sont exécutées. Pendant les périodes actives, les frais généraux augmentent au fur et à mesure que de plus en plus de travaux sont effectués.

> **Note :** Ces chiffres sont des estimations tirées des périodes indiquées.

Test	Transactions d'ouverture de session par seconde	Transactions d'écriture d'ouverture de session par seconde	Transactions de fermeture de session par seconde	Transactions d'écriture de fermeture de session par seconde
100 000 sur 1 heure	4	2.	4	2.

Test	Transactions d'ouverture de session par seconde	Transactions d'écriture d'ouverture de session par seconde	Transactions de fermeture de session par seconde	Transactions d'écriture de fermeture de session par seconde
100 000 sur 2 heures	4	2.	3.5	2.

Utilisation UC

Tous les serveurs SQL utilisés pour ce test étaient des serveurs hex-core double avec hyper-threading activé. Les spécifications matérielles exactes sont fournies à la fin de ce document.

Les serveurs étaient connus pour être surdimensionnés pour la charge en cours d'exécution. Cela nous a permis d'identifier les limites et maximums placés sur le matériel. Il est prévu que la charge CPU SQL aurait pu être gérée par un serveur SQL avec un seul quad-core, plutôt qu'un système double hex-core.

Pendant les tests, la CPU système a été surveillée à l'aide du compteur de moniteur de performances Processeur — % Processor Time —_Total.

Réplica principal

Alors que le processeur inactif fonctionnait à 0- 2% de la CPU disponible. Les procédures stockées de consolidation ont provoqué des pics toutes les minutes pendant ~ 1s à 8- 10% de la CPU du système. On s'attend à ce que ce chiffre évolue en fonction de la quantité de données traitées.

Au cours de l'ouverture de session de 100 000 utilisateurs en 1 heure, le processeur a bondi à 7 % et a augmenté linéairement à 11 % à mesure que davantage de sessions et d'utilisateurs étaient présents dans l'environnement. Notez que les pics de procédures stockées de consolidation ont ajouté 7 % à la CPU totale, entraînant les pics atteignant 18 % du CPU.

Pendant la fermeture de session CPU a fonctionné à 3,5%, avec 7% CPU supplémentaire pour les procédures stockées de consolidation. Dans l'ensemble, cela suggère que < 20 % d'un double cœur était nécessaire pour maintenir le taux d'ouverture de session et de fermeture de session.

Remarque : Le Planificateur Windows Server 2012 utilise uniquement les hyper-threads si nécessaire, c'est-à-dire jusqu'à ce que le système atteigne 50 % de charge, il n'exécute qu'un thread par cœur si possible, de sorte qu'une charge de 20 % sur 24 hyper-threads s'exécute sur 4.8 cœurs.

Compte tenu de la charge de travail, on pense qu'il s'agit d'un test de stress lourd et qu'un serveur SQL quad-core unique serait approprié pour les déploiements XenDesktop.

Réplicas secondaires

Les réplicas secondaires ont été trouvés pour configurer 2% CPU pendant l'ouverture de session et 1,5% pendant la fermeture de session. Ceci est à prévoir car, pour la plupart, les réplicas stockent des données à partir du primaire sur leurs disques, et seul le réplica synchrone est impliqué dans les transactions, car le réplica principal ne valide pas une transaction tant que le secondaire l'a reconnu.

Sur la base des recommandations pour que le matériel HA corresponde au réplica principal, cette charge serait très facilement gérée par un serveur spécifié de la même manière.

Utilisation temporaire de la base de données

Le TempDB est utilisé à de nombreuses fins, y compris la banque de versions, l'espace pour les jeux de requêtes volumineux et d'autres utilisations de tables temporaires.

Dimensionnement TempDB

Dans cette configuration SQL TempDB a été configuré pour avoir 8 fichiers de base de données, chacun d'une taille fixe de 5 Go. Cela permet une meilleure utilisation simultanée de TempDB, mais fournit également beaucoup d'espace et ne déclenche aucun événement de croissance automatique. Sur la base des données capturées, il a été surdimensionné pour ce déploiement. Il y avait cependant beaucoup d'espace disque disponible.

Il suit également les indications générales selon lesquelles le nombre de fichiers de base de données TempDB est compris entre un quart et la moitié du nombre de CPU disponibles, mais ne dépasse pas 8 sans savoir qu'il existe une contestation réelle.

Notez qu'un seul fichier journal TempDB est utilisé, car SQL Server ne bénéficie pas de plusieurs fichiers journaux.

Boutique de versions

TempDB contient un magasin de versions pour les versions de lignes liées à l'isolement d'instantané validé en lecture utilisée par les bases de données XenDesktop.

L'utilisation peut être mesurée à l'aide des compteurs de performance suivants :

- SQLServer : Transactions — Taille du magasin de versions (Ko)
- SQLServer : Transactions — Taux de nettoyage de version (Ko/s)
- SQLServer : Transactions — Taux de génération de versions (Ko/s)

Pour 100 000 ouvertures de session sur une heure, la taille du magasin de versions est restée comprise entre 10 Mo et 30 Mo, avec un effet de dent de scie au fur et à mesure que les versions ont été créées

puis nettoyées. Pendant la fermeture de session, la plage était de 10 Mo à 21 Mo. En cas d'inactivité, la taille du magasin de versions variait de 1 Mo à 4 Mo.

Le débit de génération de version se situait dans la plage de 250 à 500 Ko pendant l'ouverture de session, de 150 à 400 Ko/s pendant la fermeture de session et de 0 à 250 Ko/s lorsqu'il est inactif.

Le nettoyage de version s'exécute une fois par minute et atteint 2 500 Ko/s pendant l'ouverture de session, 1 750 Ko/s pendant la fermeture de session et 400 Ko/s pendant les périodes d'inactivité.

E/S disque

Au cours des tests d'ouverture de session, les E/S de disque ont été mesurées avec les compteurs de performance suivants :

- PhysicalDisk — Octets de lecture de disque/seconde
- PhysicalDisk — Octets d'écriture de disque/seconde
- PhysicalDisk — Lectures de disque/seconde
- PhysicalDisk — Écritures de disque/seconde

Les E/S de lecture ont été jugées minimales, car le serveur SQL a pu contenir toutes les données en mémoire, provoquant très peu d'activité de lecture sur le système.

En raison de la disposition des bases de données et du système de stockage, les volumes ont été divisés, un volume contenant tous les fichiers de données et un second volume contenant tous les fichiers journaux des transactions.

Les données montrent un motif difficile à placer dans une table. En général, le journal des transactions avait un octet d'écriture de 800 Ko/s pour le test d'une heure et de 400 Ko/s pour le test de 2 heures. Une fois par minute, lorsque les procédures stockées de consolidation s'exécutent, le journal des transactions affichait des pics atteignant 30 Mo/s.

L'analyse des procédures stockées de consolidation montre que parfois les statistiques rendent le plan de requête sous-optimal et qu'une table temporaire se déverse dans TempDB. Cela déclenche les écritures dans le journal des transactions pour TempDB.

Ce transfert de données se traduit par un état stable de 300 opérations d'entrée/sortie par seconde (IOPS) en écriture pour le test d'une heure et de 200 E/S par seconde pour le test de 2 heures. Les pics des procédures stockées de consolidation ajoutent 2 à 300 E/S par seconde lors de l'exécution. Notez que dans un environnement volumineux, les procédures stockées de consolidation s'exécutent pendant moins d'une seconde.

Lorsque chaque base de données est cochée, les données sont synchronisées à partir des tables en mémoire vers les fichiers de données du volume de données.

Pour plus d'informations sur le point de contrôle SQL, reportez-vous à la section http://technet.microsoft.com/enus

Ces points de contrôle sont des périodes d'activité très courtes, généralement inférieures à 1.

Pendant l'ouverture de session, les points de contrôle ont consommé 6 à 7 Mo/s et 500 E/S par seconde en écriture. Pendant la fermeture de session, les points de contrôle ont consommé 7 Mo/s, variant entre 200 et 700 E/S par seconde. Les chiffres varient parce que les bases de données Site et Monitoring ont des quantités différentes de données au point de contrôle.

Maintenance de la base de données

La maintenance de la base de données dans un déploiement important est importante. Si la base de données n'est pas correctement gérée, des pannes de base de données peuvent se produire en raison d'un manque d'espace dans la base de données, par exemple si le journal des transactions est configuré pour autogrow et remplit le disque, ou si le journal des transactions est d'une taille fixe et devient plein.

Maintenance du journal des transactions

Lors de l'utilisation des fonctionnalités de haute disponibilité de SQL Server, par exemple, Groupes de disponibilité Always On ou Mise en miroir de bases de données, les bases de données XenDesktop s'exécutent en mode de journalisation complète des transactions.

En s'exécutant en mode de journalisation complète des transactions, le journal des transactions continue de croître jusqu'à ce qu'une sauvegarde de base de données ou de journal des transactions soit effectuée.

Cela peut provoquer des problèmes si les fichiers journaux de transactions ne sont pas surveillés car, par défaut, SQL Server configure les fichiers journaux pour une croissance automatique. Cela provoque 2 problèmes :

1. Les fichiers journaux de transactions peuvent consommer beaucoup d'espace disque.
2. Chaque fois que le journal des transactions augmente, il bloque toutes les transactions jusqu'à ce que l'espace du journal ait été réduit à zéro.

Citrix recommande que les fichiers journaux soient sauvegardés régulièrement. Cela peut être fait avec des travaux planifiés ou des plans de maintenance.

Vous pouvez également utiliser l'agent SQL Server pour surveiller lorsque la taille utilisée du journal dépasse un seuil et exécuter une tâche de sauvegarde.

Dans les tests d'échelle, un journal de taille fixe de 4 Go a été utilisé, et une alerte a été définie pour sauvegarder le journal dans un autre fichier lorsque le fichier journal a atteint 80 % de volume. Cela a empêché le journal de croître et de consommer tout l'espace disque, et a également arrêté la réduction à zéro de l'espace disque et le blocage de la base de données.

Un exemple de travail exécuterait un script tel que :


```
BACKUP LOG [CitrixXenDesktop-SiteDB] TO DISK = N'D:\LogBackup\
    CitrixXenDesktopSiteDB.bak' WITH NOFORMAT, NOINIT, COMPRESSION, NAME
     = N'Site-Transaction Log Backup', SKIP, NOREWIND, NOUNLOAD
```

Le compteur de performances SQL à utiliser pour l'alerte est :

SQLServer : Bases de données - Percent journal utilisé - CitrixXenDesktopSiteDB

Répétez cette opération pour chacune des 3 bases de données.

La sauvegarde du fichier journal a été jugée avoir un impact minimal sur un environnement XenDesktop en cours d'exécution, il y a une augmentation marginale des temps de courtage, mais pas quelque chose que nous pensons être significatif.

Pour plus d'informations sur la configuration des tâches, voir :http://msdn.microsoft.com/en-us/library/ms187880.aspx

Pour plus d'informations sur la configuration des alertes, voir :http://msdn.microsoft.com/en-us/library/ms191508.aspx

Maintenance de l'index

Lorsque plus de données sont entrées dans la base de données, certains des index commencent à devenir moins complets, c'est-à-dire moins d'enregistrements sont stockés dans chaque page SQL. Une page SQL est de 8 Ko. La base de données augmente ainsi ses besoins de stockage, tant en mémoire que sur disque. En conservant les index, la plénitude de la page peut être augmentée, ce qui réduit les besoins en mémoire de la base de données.

Citrix recommande que les plans de maintenance de la configuration des clients soient exécutés tous les soirs et toutes les semaines pour gérer les index. Les plans de maintenance peuvent simplement consister à réorganiser les index pendant la nuit pendant la semaine, et à reconstruire les index les fins de semaine.

Cette recommandation évite tout impact sur les performances de la reconstruction d'index volumineux pendant les opérations quotidiennes, en particulier pour une base de données de surveillance de grande taille.

Microsoft recommande que les index soient reconstruits s'ils sont fragmentés de plus de 30 % et réorganisés s'ils sont inférieurs à 30 %. Pour plus d'informations, reportez-vousRéorganiser et reconstruire les indexà la bibliothèque Microsoft TechNet.

Après réorganisation des index, les statistiques devraient également être mises à jour. Ceci est particulièrement important à mesure que la base de données se développe ; sinon certaines statistiques peuvent être médiocres et SQL peut générer des plans de requête SQL sous-optimaux.

En termes d'espace enregistré, le script Microsoft ci-dessous a été exécuté sur une base de données de surveillance de 1,2 Go. Il a amélioré le remplissage de la page et libéré 300 Mo d'espace.

Scripts tiers

Microsoft

Microsoft recommande la mise à jour des index pour leurs bases de données SQL WSUS à l'aide du script disponible à partir de :

http://gallery.technet.microsoft.com/scriptcenter/6f8cde49-5c52-4abd-9820-f1d270ddea61

En modifiant le « USE SUSDB », ce script peut également être exécuté sur des bases de données XenDesktop. Ce script suit les meilleures pratiques de Microsoft consistant à reconstruire des index fragmentés de plus de 30 % et à réorganiser ceux de moins de 30 %. Il met ensuite à jour les statistiques de la base de données.

Ola Hallengren

Des scripts plus avancés sont également disponibles à partir de :

http://ola.hallengren.com/

Ces scripts sont bien considérés dans la communauté SQL Server. Plus précisément, les scripts Index disponibles à partir de :

http://ola.hallengren.com/sql-server-index-and-statistics-maintenance.html

Ces scripts peuvent être utilisés pour un contrôle plus précis sur les niveaux pour réorganiser ou reconstruire les index.

Configuration du serveur de test

Configuration de SQL Server

Le groupe de disponibilité SQL comprend 3 serveurs Dell R720XD spécifiés de manière identique.

Spécification du système :

- 2 CPU Intel Xeon Hex-core E5-2630 fonctionnant à 2,30 GHz avec hyper-threading activé
- 64 GO DE RAM ECC
- PERC H710P Mini avec 1 Go de mémoire cache avec batterie
- 26 disques durs SAS à 10 000 tr/min 300 Go

Les disques ont été divisés en volumes suivants :

- Volume système
  - Contenant le système d'exploitation et le fichier de page
  - 2 disques comme miroir RAID 1

    - Capacité totale 278 Go
- Volume de base de données
    - Contenant l'instance SQL Server et les fichiers de données de base de données
    - 16 disques sous forme de bande miroir RAID 10
    - Capacité totale 2 231 Go
- Volume du journal
    - Contenant les fichiers journaux de base de données
    - 8 disques sous forme de bande miroir RAID 10
    - Capacité totale 1 115 Go
- Logiciel :
    - Windows Server 2012 R2 Édition Standard, avec mises à jour Windows actuelles au moment du test (août 2014)
    - SQL Server Enterprise 2012 SP2 avec mise à jour cumulative 1
- Modifications de configuration
    - SQL Server a été configuré pour utiliser un maximum de 61 440 Mo
    - Le confinement de la base de données a été activé sur toutes les instances SQL
    - Le service Agent SQL Server a été configuré pour démarrer automatiquement
- Configuration du groupe de disponibilité :
    - Tous les serveurs ont été placés dans un cluster de basculement Windows
    - Un groupe de disponibilité Always On a été configuré dans le cluster
    - Les réplicas secondaires ont été configurés pour être commit synchrone, exigeant que les transactions soient validées sur les deux réplicas avant la fin de la transaction
    - Le routage du réplica en lecture seule a été configuré et activé pour le groupe de disponibilité

Delivery Controller et serveurs de test HSD

Le Delivery Controller et les serveurs de test HSD fonctionnaient sur la même configuration matérielle, à l'aide des lames HP BL460c G1. Deux serveurs ont été utilisés pour les Delivery Controller et 43 serveurs ont fourni la charge de travail HSD simulée.

Remarque : Bien que ces serveurs soient relativement anciens, la charge de travail sur les serveurs HSD est faible, car la simulation de session se concentre principalement sur la charge sur les Delivery Controller plutôt que sur les serveurs HSD.

Spécification du système :

- 2 processeurs Intel Xeon L5320 quatre cœurs fonctionnant à 1,86 GHz, non compatibles hyperthread
- 16 GO DE RAM ECC
- Carte Raid HP Smart Array E200I (pas de cache avec batterie)
- Disque dur SAS de 36 Go ou 72 Go

Logiciel :

- Windows Server 2012 R2 Édition Standard, avec mises à jour Windows actuelles au moment du test (août 2014)
- Citrix XenDesktop 7.6

Analyse du cache de RAM PVS avec débordement

January 8, 2020

Cet article fournit des informations sur la détermination précise de la taille du cache RAM lors de l'utilisation du *cache RAM de fonctionnalité avec débordement sur disque*.

Le cache RAM avec débordement sur disque est une fonctionnalité PVS dans laquelle les écritures vDisk sont écrites en premier lieu sur la RAM du pool Windows non paginée. Une fois que la taille du cache RAM spécifiée par l'utilisateur a atteint sa taille spécifiée, PVS vide le contenu du cache RAM sur le disque afin de créer de la place pour de nouvelles données. La taille du cache RAM fluctue en fonction du modèle de charge de travail et d'autres variations. PoolMon est un outil pour prendre un instantané de la taille d'utilisation actuelle du cache RAM en recherchant le *VhdR*de pool tag.

Pour plus d'informations sur cette fonctionnalité PVS, reportez-vous au blog surutilisation du cache RAM avec débordement.

> **Important**
>
> Les outils décrits dans cet article sont destinés aux administrateurs ayant une connaissance avancée de Provisioning Services. Ces informations peuvent être utilisées pour aider à déboguer des problèmes liés aux performances qui vont au-delà de l'utilisation d'outils et de processus couramment utilisés, y compris ProcMon (ProcMonitor). Avec ces informations, vous aurez une meilleure compréhension du fonctionnement du pilote PVS.

Moniteur de pool de mémoire

PoolMon (poolmon.exe) fait référence au Moniteur de pool de mémoire. Il est utilisé pour afficher les données (allocations de mémoire à partir des pools de noyau paginés et non paginés système, et les pools de mémoire utilisés pour les sessions des services Terminal Server) collectées par un système d'exploitation. Ces données sont regroupées par balise d'allocation de pool.

Avecmémoire de pool non paginée, vous pouvez utiliser l'PoolMonoutil pour vérifier l'existence du **tag de pool**désigné par *VhdR*. VhdR est utilisé pour l'allocation du cache RAM ; cette balise, avec le pool tag *VhdL*, est utile lors de la création de scripts pour aider à analyser les données associées au cache RAM dans la mémoire de pool non paginée.

> **Conseil**
>
> Les développeurs et les testeurs utilisent généralement PoolMon pour détecter les fuites de mémoire lorsqu'un pilote est créé, le code du pilote est modifié ou pour tester le pilote sous tension. PoolMon peut également être utilisé à chaque étape du processus de test pour vérifier le modèle d'allocation de mémoire et les opérations libres d'un pilote, y compris pour déterminer la quantité de mémoire de pool que le pilote utilise à un moment donné. Pour plus d'informations sur l'utilisation du Moniteur de pool de mémoire, reportez-vous à la sectionSite du Réseau des développeurs Microsoft.

Utilisation de l'Analyseur de performances Windows

Windows Performance Analyzer (WPA) est un outil qui vous permet de créer des graphiques et des tables de données liés aux événements (en particulier, le suivi des événements pour Windows) qui sont enregistrés par l'enregistreur de performances Windows (WPR). Utilisez le WPA pour identifier les goulots d'étranglement des performances lors du débogage des problèmes liés au pilote PVS, à la pile de stockage et aux problèmes liés aux performances qui se produisent lors de l'écriture sur le disque VHDX. Avec ces outils, vous pouvez exécuter des évaluations et ouvrir n'importe quel fichier journal de suivi des événements pour analyse. Reportez-vous au site Microsoft Developer Network pour plus d'informations sur leAnalyseur de performances Windows.

> **Remarque**
>
> Le WPA et le WPR sont inclus dans le Kit d'évaluation et de déploiement Windows (Windows ADK) ; pour plus d'informations sur ce kit de déploiement, reportez-vous à la section Site Web Microsoft. Visitez le site Web de Microsoft pour obtenir la dernière version duAnalyseur de performances Windows.

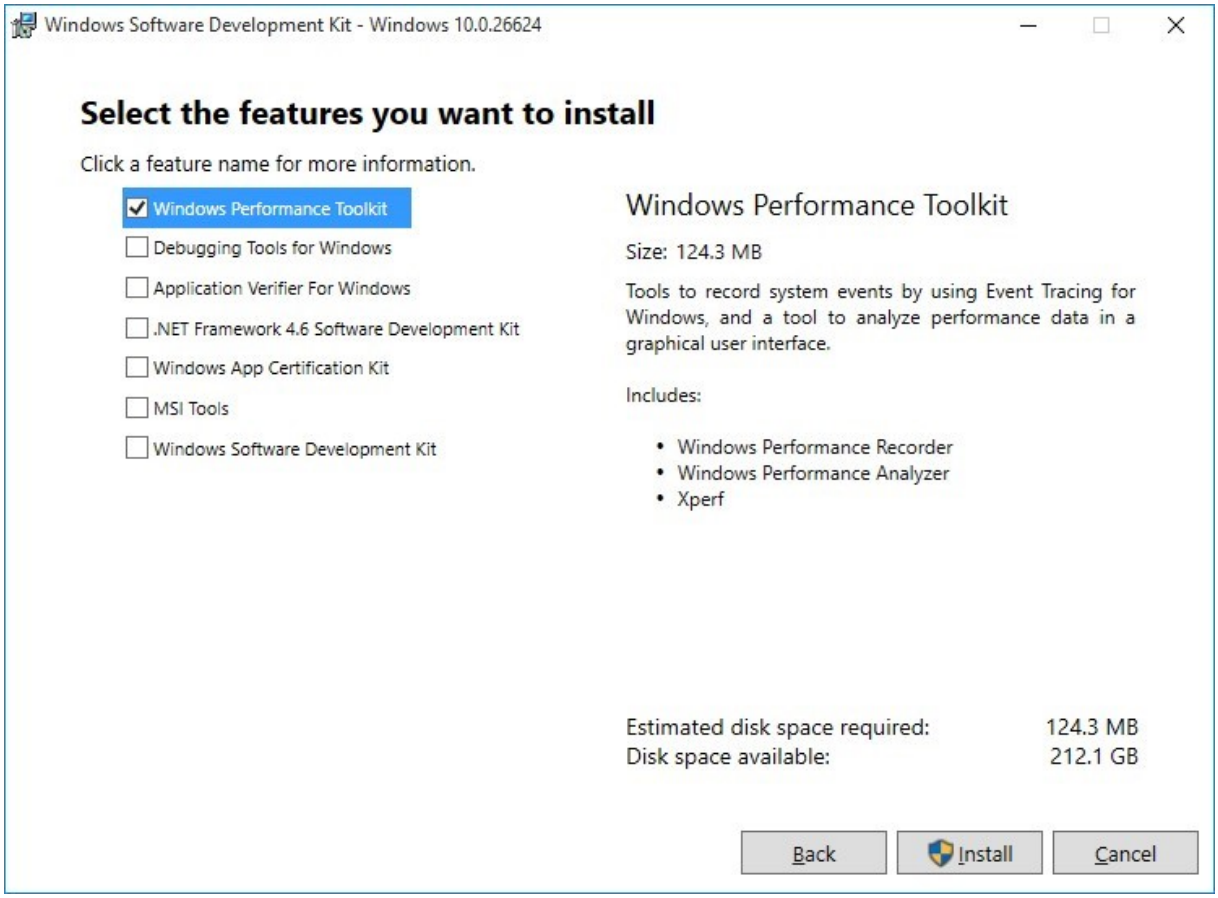
Fonctionnement de l'Analyseur de performances Windows avec Provisioning Services

PVS génère des événements capturés par le mécanisme ETW (Event Tracing for Windows). Cette fonctionnalité permet de suivre et de consigner les événements qui sont soulevés par les applications en mode utilisateur et les pilotes en mode noyau. ETW est implémenté dans le système d'exploitation Windows et fournit un moyen facile pour les développeurs d'utiliser un ensemble de fonctionnalités de suivi d'événements. Pour plus d'informations, reportez-vous à la Réseau des développeurs Microsoft.

Installation de l'Analyseur de performances Windows

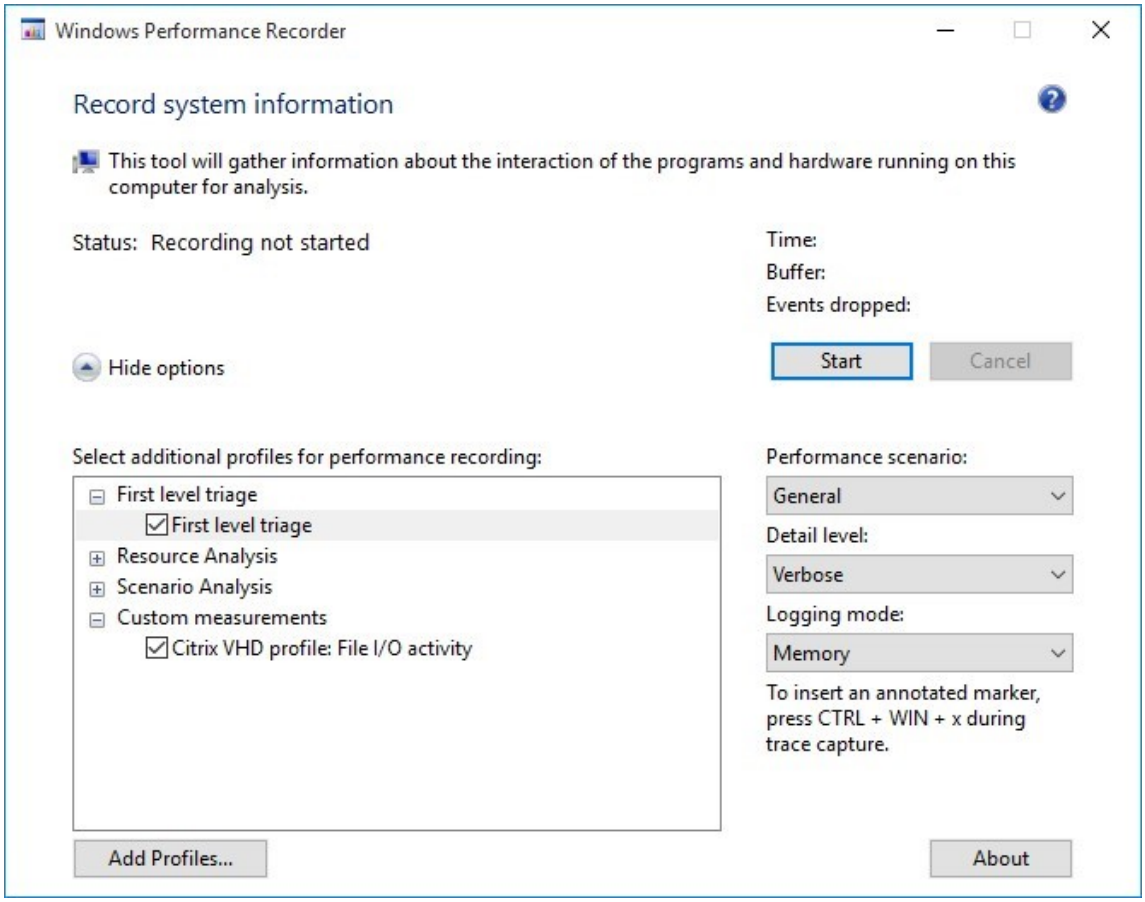
WPA doit être installé sur l'image principale.

Le WPA fait partie de ladernier SDKpour le système d'exploitation Windows 10. Vous pouvez installer sélectivement le kit Performance Toolkit qui inclut à la fois le WPA et le WPR :



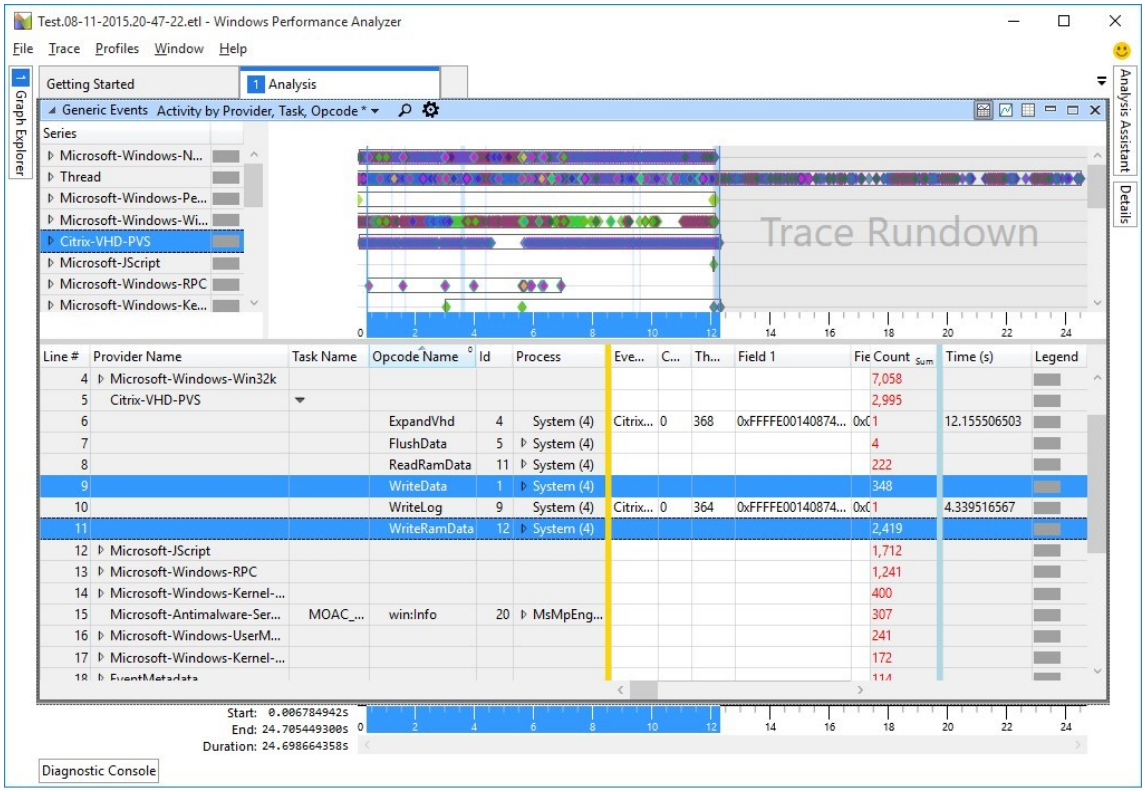
Après avoir installé le WPA et le WPR, utilisez le WPR pour simuler l'activité des E/S du disque PVS et des fichiers. Une fois ce trafic créé, analysez les données à l'aide du WPA. Pour effectuer ces actions :

1. Lancez le WPR sur le périphérique cible et cliquez sur **Ajouter des profils**.
2. Dans l'écran Ajouter des profils, accédez au modèle ou au profil spécifique au PVS. Cela vous permet de recevoir les événements générés par le fournisseur d'événements PVS. Après avoir importé le profil, revenez à l'écran WPR et sélectionnez les options supplémentaires que vous souhaitez analyser et cliquez sur le bouton **Démarrer** :



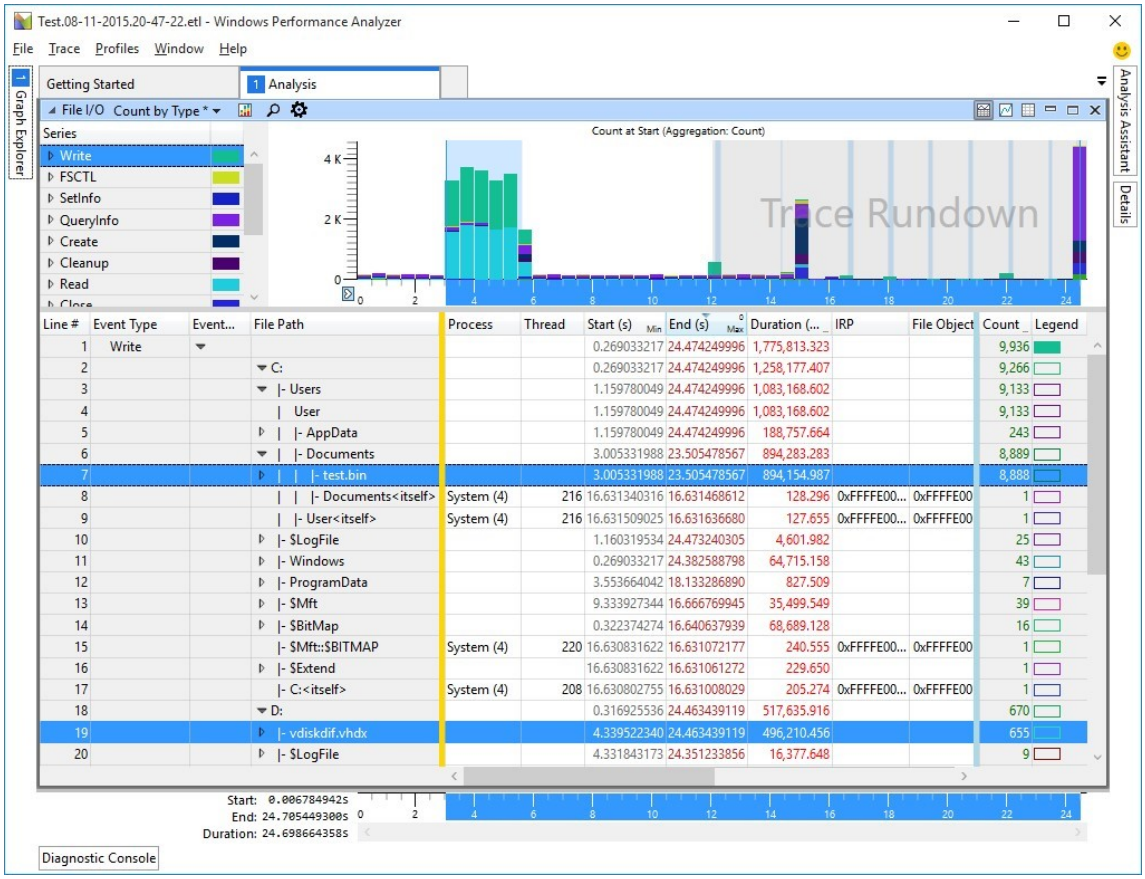
Après avoir ajouté les options et cliqué sur Démarrer, vous pouvez simuler l'activité PVS. Dans cet exemple, un nouveau cache d'écriture avec un petit tampon de mémoire (128 Mo) est créé. Un fichier plus volumineux (279 Mo) est copié dans C:\Users\User\Documents\test.bin pour forcer le pilote PVS à écrire des données dans le pool non paginé pour vérifier ce qui se passe en cas de basculement, ce qui commence à écrire sur le disque local (par exemple, D:\vdiskdif.vhdx). Après avoir copié le fichier et forcé le tampon à dépasser la capacité, vous pouvez arrêter le processus de capture dans WPR et ouvrir les résultats à l'aide de WPA.

3. À l'aide du WPA, ouvrez l' **Explorateur de graphiques**, développez **Activité système**et sélectionnez **Evénements génériques**. À l'aide de l'écran ci-dessous, affichez le contenu des sections WriteData et WriteRamData. Cette information affiche le nombre exact de fichiers écrits sur C : vDisk (2419 fichiers), y compris le fichier VHDX sur le lecteur D : (348 fichiers) :



> **Conseil**
>
> La valeur WriteData est inférieure à la valeur affichée car elle est mise en cache dans la RAM et n'a pas été vidée sur le disque.

4. Revenez à l'écran **Explorateur de graphiques** , puis développez **Fichier E/S** et **Nombre par type** . L'image ci-dessous illustre la réduction des E/S (nombre de fichiers) et la durée entre l'écriture dans C:\Users\User\Documents\test.bin et le fichier cache d'écriture spillover situé à D:\vdiskdif.vhdx. À l'aide de ces données, vous pouvez afficher les goulots d'étranglement potentiels en termes de performances et exclure efficacement le pilote de filtre PVS comme un problème :



5. Après avoir affiché le nombre de fichiers et la durée entre les écritures (entre le fichier journal et le cache d'écriture débordant), vous pouvez aller plus loin dans le processus de débogage pour comprendre où les données sont écrites initialement (et où elles finissent) à l'aide de décalages de disque. Dans l'Analyseur de performances Windows, ouvrez l' **Explorateur de graphiques** , développez **Activité système** et sélectionnez **Événements génériques** . Modifiez la vue des colonnes pour permettre à l'outil WPA d'afficher la transition des données dans les différentes couches de stockage. Pour un débogage supplémentaire, revenez à l'environnement PVS et définissez le tampon de cache RAM sur 0 Mo, puis réexécutez les outils de l'enregistreur (WPR) et de l'analyseur (WPA). L'image ci-dessous illustre comment se produit le débordement vers le disque :

Extension de la durée de vie de vos applications Web héritées à l'aide de Citrix Secure Browser

January 8, 2020

Dans le monde des applications et des cadres Web, la diversité doit être adoptée. Différents types d'utilisateurs, de groupes et d'entreprises ont besoin d'accéder aux outils, applications et autorisations appropriés pour se connecter aux applications d'entreprise Web. Dans la plupart des cas, il existe des facteurs de conformité qui dictent la façon d'accéder à ces applications. Les entreprises qui ont besoin de prendre en charge des sous-systèmes plus anciens, avec des cadres de navigateur plus anciens, ont du mal à fournir un accès adéquat et à satisfaire aux exigences de conformité pour les applications critiques de l'entreprise. Le document suivant décrit comment utiliser Citrix Secure Browser pour étendre l'accès et la durée de vie de vos applications Web et navigateurs hérités tout en créant une stratégie de mise à jour et de migration.

La solution nécessite la publication d'un navigateur conforme qui permet l'accès aux utilisateurs externes ou internes, indépendamment de la façon dont l'utilisateur se connecte ou du navigateur qu'ils utilisent pour se connecter au site interne. Cette solution utilise XenDesktop Server OS VDA, StoreFront, NetScaler Gateway et XenApp Secure Browser. Les utilisateurs redirigent les navigateurs ou les points de terminaison compatibles pour utiliser un navigateur natif lorsqu'il répond à toutes les exigences définies par l'administrateur informatique ; et si la stratégie détecte un navigateur ou un point de terminaison non conforme, redirige l'utilisateur vers une session de navigateur publié contenant à distance. Les utilisateurs n'ont besoin de connaître qu'une URL par ressource (ce qui réduit les coûts

de formation et de support), quelle que soit la façon dont ils se connectent à l'environnement.

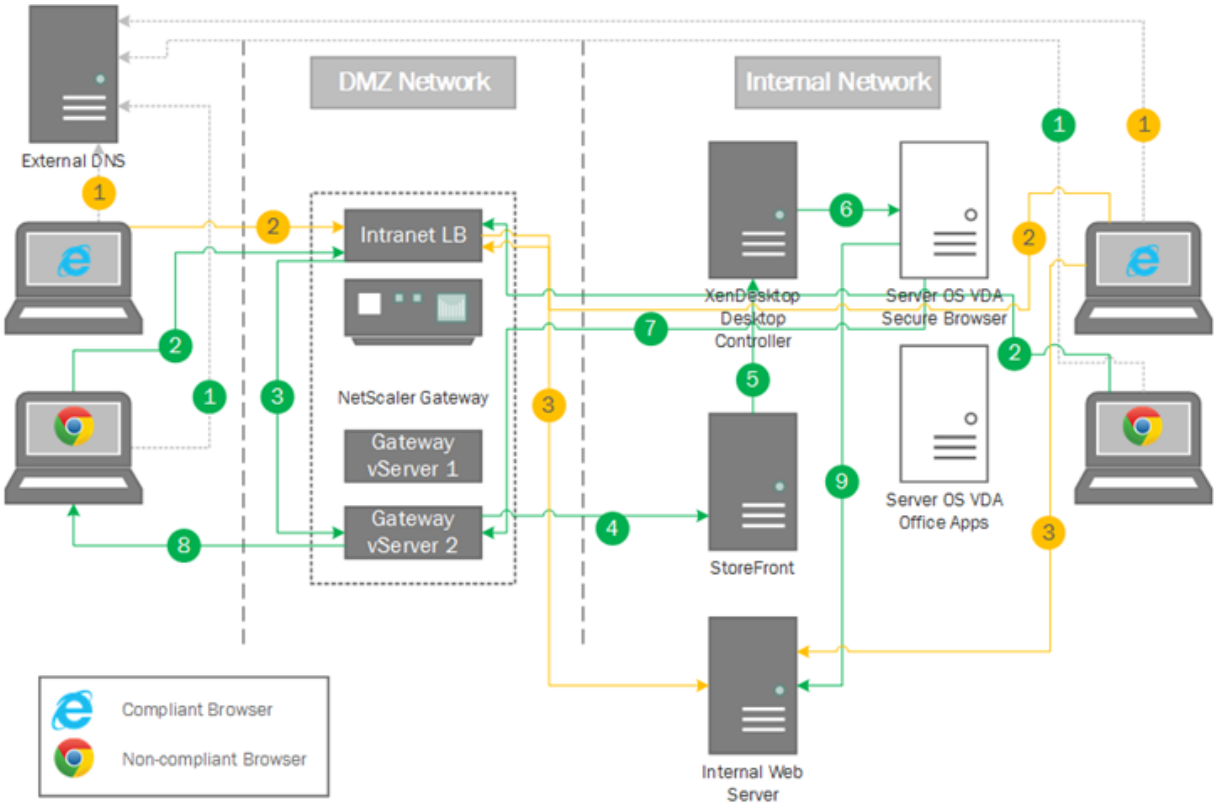
Architecture

La section suivante explique comment les utilisateurs accèdent au site interne, que l'utilisateur se connecte à partir d'un réseau interne ou externe. Dans le scénario, un type de navigateur (Internet Explorer) est le navigateur conforme et un autre (Google Chrome) comme non conforme. Il appartient à chaque entreprise de déterminer comment et quels navigateurs sont mis en correspondance avec la politique de conformité.

Pour cette solution, nous supposons que NetScaler Gateway est configuré pour un accès externe aux applications publiées, ceci est représenté dans la Figure 1 comme Gateway vServer 1. Le deuxième serveur virtuel (Gateway vServer 2) redirige les utilisateurs pour lancer la session HTML5 Receiver pour Secure Browser.

Cas d'utilisation

Il est nécessaire de maintenir les applications Web héritées qui ne sont plus prises en charge par les navigateurs actuels. Dans ce cas, le service informatique doit toujours gérer un site Web conçu pour Internet Explorer 8 et le fournisseur ne publie plus d'améliorations pour prendre en charge les nouveaux navigateurs ou autres. Pour résoudre ce problème, l'administrateur informatique publie un navigateur sécurisé pour permettre aux utilisateurs qui répondent aux exigences du navigateur d'accéder au site. Le diagramme ci-dessous explique chaque connexion dans le workflow pour les utilisateurs internes et externes.



Flux de travail de connectivité

1. Chaque utilisateur entre dans l'URL du site qui résout à partir d'un serveur DNS externe, dans notre exemple,`https://train.qckr.net`
2. Le navigateur se connecte à l'équilibreur de charge NetScaler Gateway et détermine les exigences de conformité.
3. Lorsque le navigateur n'est pas conforme, les utilisateurs internes et externes redirigent vers le serveur virtuel NetScaler Gateway. Lorsque le navigateur est conforme, NetScaler Gateway met en proxy la connexion au site interne via l'équilibreur de charge pour les utilisateurs externes et redirige le navigateur local vers le site pour les utilisateurs internes.
4. Le serveur virtuel démarre automatiquement une session énumérée par StoreFront.
5. StoreFront contacte le contrôleur XenDesktop pour obtenir des informations sur la session et le routage.
6. La session démarre via le groupe de bureau Secure Browser ; dans ce cas, il s'agit d'un VDA avec OS de serveur avec un navigateur conforme publié.
7. La session se connecte via le proxy ICA sur l'appliance NetScaler Gateway.
8. Citrix Receiver pour HTML5 établit la session de l'utilisateur dans le navigateur natif.
9. Le site interne s'affiche via la session Secure Browser avec Citrix Receiver pour HTML5.

Configuration et configuration

Cette section explique comment implémenter la solution pour les environnements XenDesktop actuels avec la connectivité à distance NetScaler Gateway.

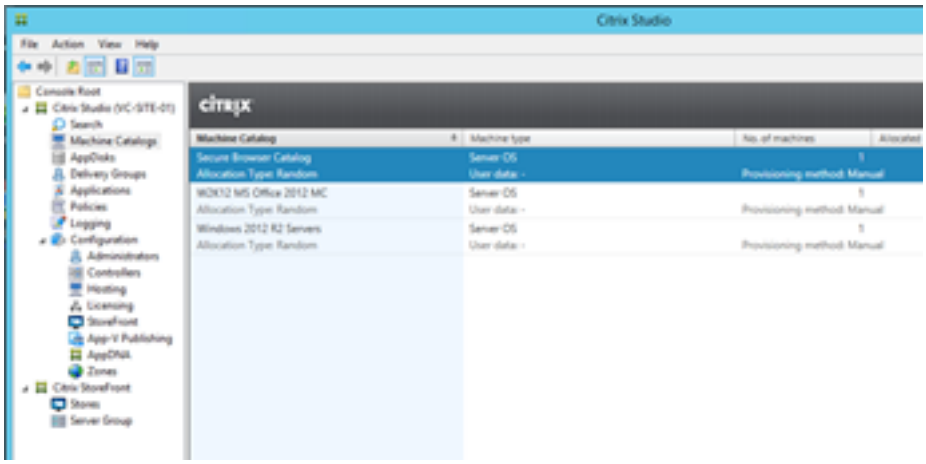
Exigences de la solution

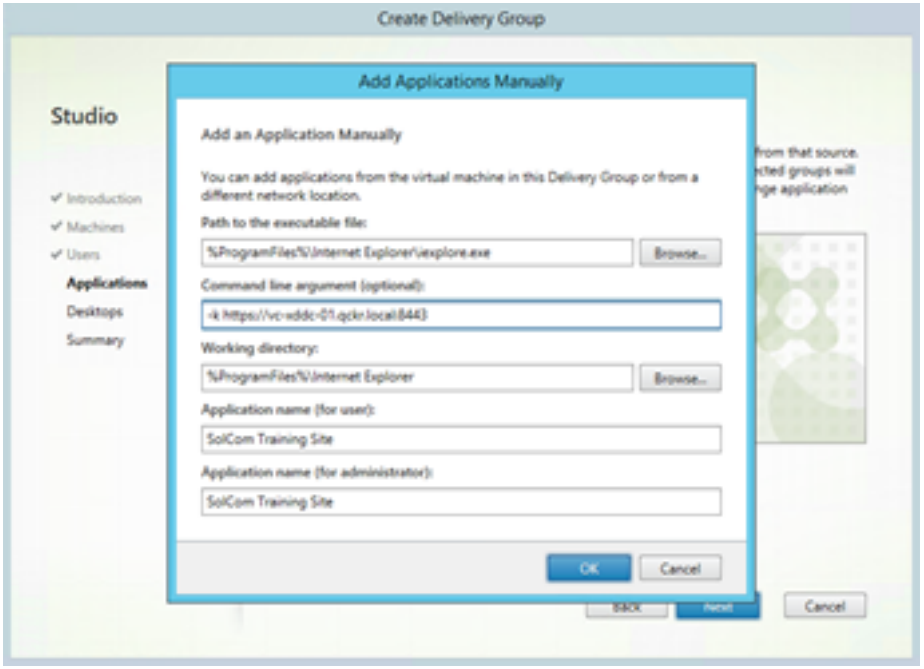
La configuration nécessite l'installation et la configuration des composants suivants :

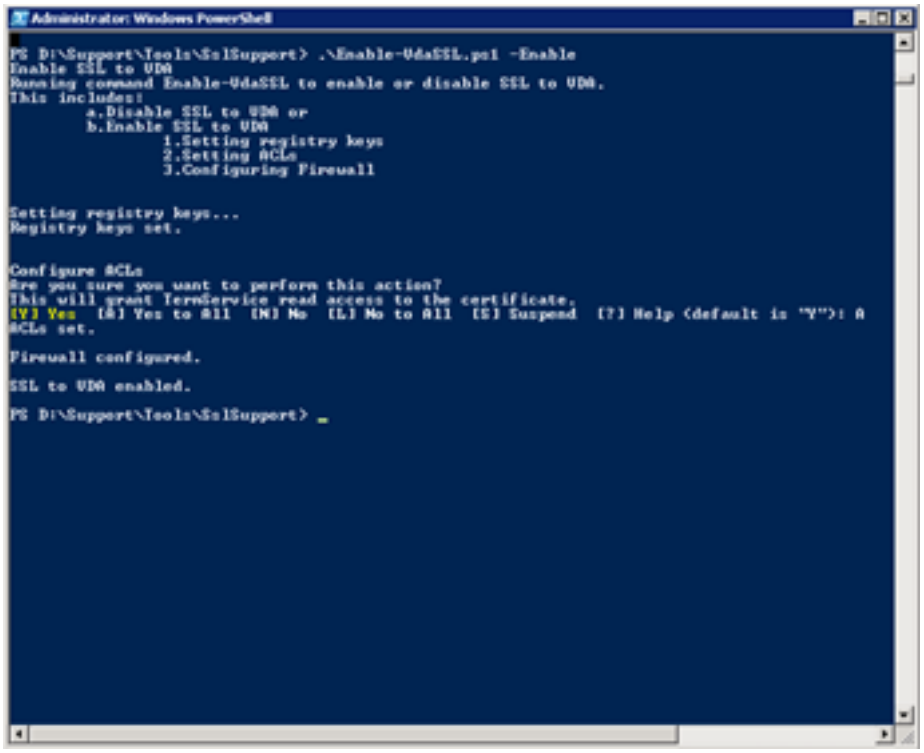
- Serveur XenDesktop Desktop Controller
- Serveur Citrix StoreFront avec un magasin configuré pour un accès externe
- NetScaler Gateway avec un serveur virtuel XenDesktop
- VDA avec OS de serveur avec l'utilisation du navigateur installé comme navigateur sécurisé
- Adresse DNS externe qui pointe vers un nouvel équilibreur de charge NetScaler
- Adresse DNS externe qui pointe vers un nouveau serveur virtuel NetScaler Gateway

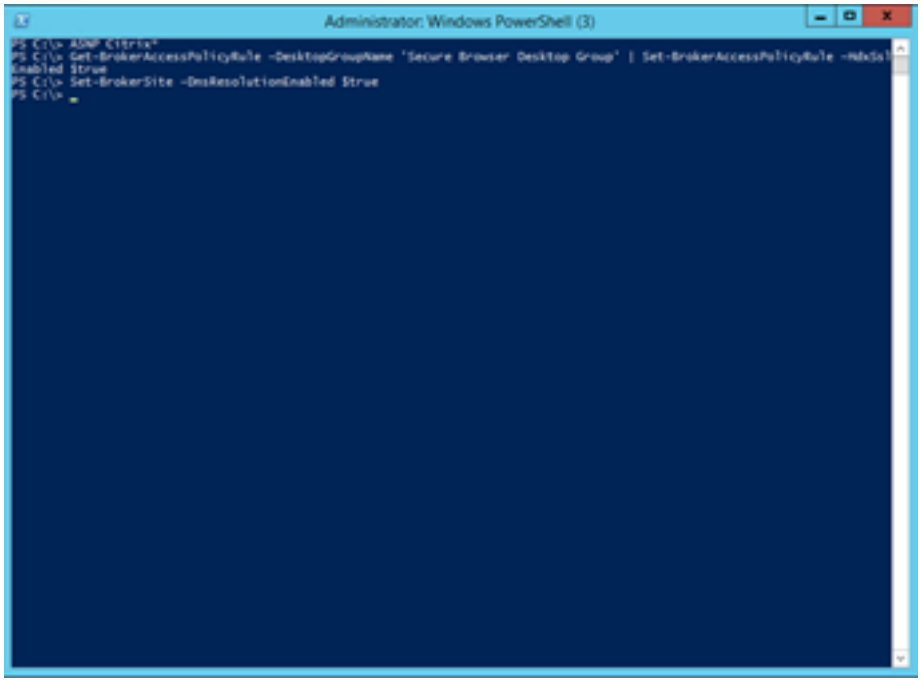
Configuration

Contrôleur XenDesktop









Ajoutez le VDA du SE de serveur à un nouveau catalogue de machines nommé **Secure Browser Catalog**.

Créez un groupe de mise à disposition pour **Secure Browser Catalog** et publiez Internet Explorer. Dans les paramètres de ligne de commande, tapez -k <URL of Internal Site>.** Le paramètre -k consiste à ouvrir Internet Explorer en mode Kiosque. Dans cet exemple, nous publions Internet Explorer 8 et utilisons un site interne pour l'URL.

Vous pouvez affecter le groupe de mise à disposition à des utilisateurs et groupes spécifiques. Vous n'avez pas besoin d'ajouter un accès au bureau s'il n'est pas nécessaire pour le cas d'utilisation.

Sur le VDA du système d'exploitation de serveur, installez un certificat d'authentification serveur ou client, qui active SSL sur la communication Controller et VDA.

Montez le support d'installation XenDesktop 7.6 ou version ultérieure. Ouvrez une fenêtre de commande PowerShell, puis exécutez *%MediaDrive%:\Support\Tools\SslSupport\Enable-VdaSSL.ps1 –Enable*

Redémarrez l'instance VDA du système d'exploitation de serveur.

Sur XenDesktop Controller, ouvrez une fenêtre de commande PowerShell et exécutez la commande *ASNP Citrix**.

Exécutez les trois commandes suivantes pour activer le courtier vers la communication sécurisée VDA :

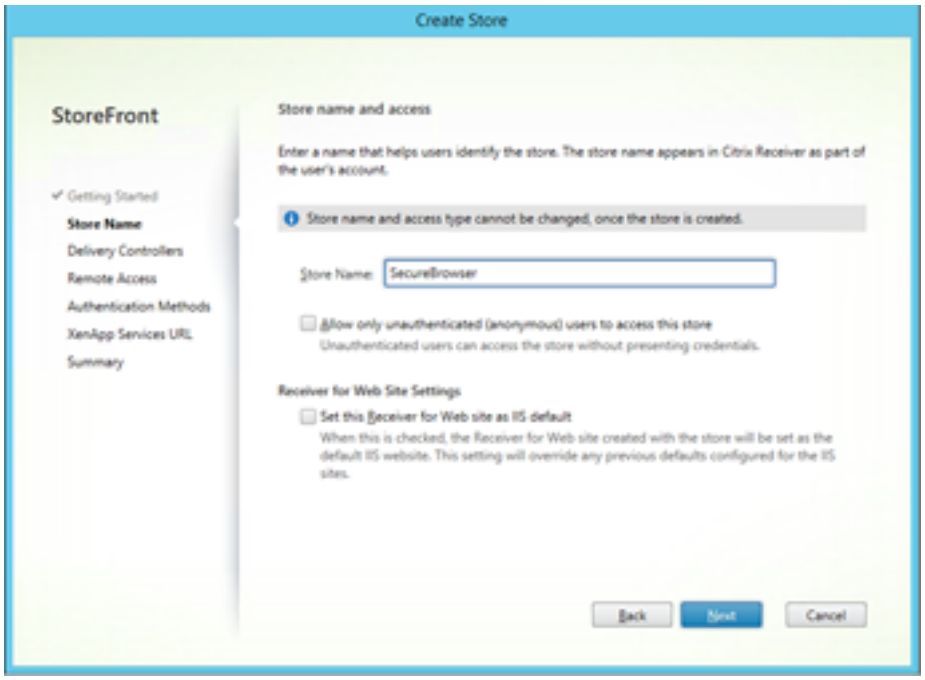
```
1 Get-BrokerAccessPolicyRule -DesktopGroupName 'Secure Browser Desktop
     Group' | Set-BrokerAccessPolicyRule -HdxSslEnabled $true*
2 <!--NeedCopy-->
```

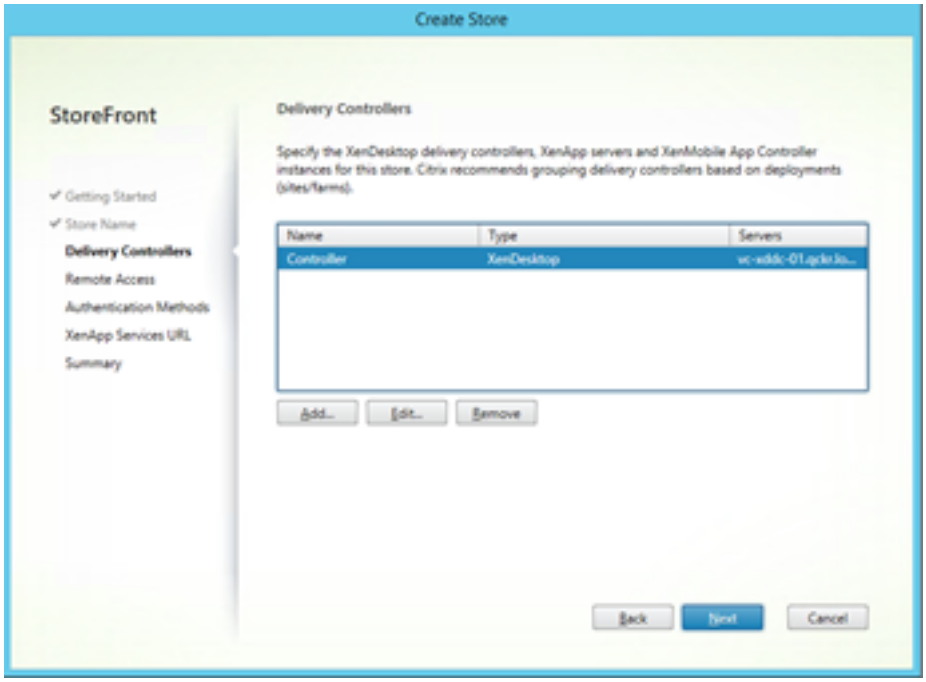


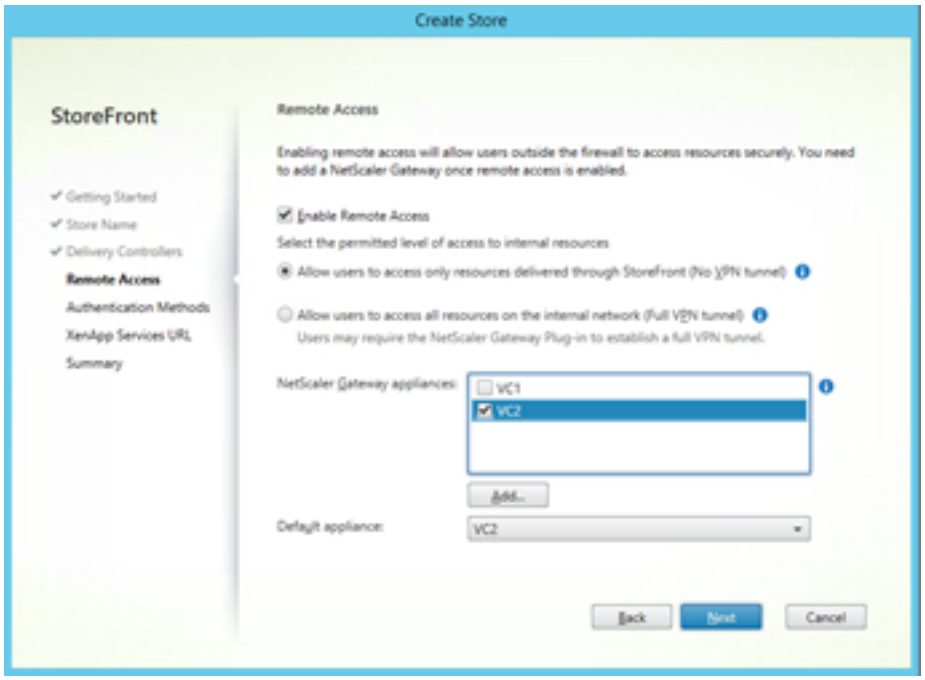
```
Set-BrokerSite  - DnsResolutionEnabled $true
<!--NeedCopy-->
```

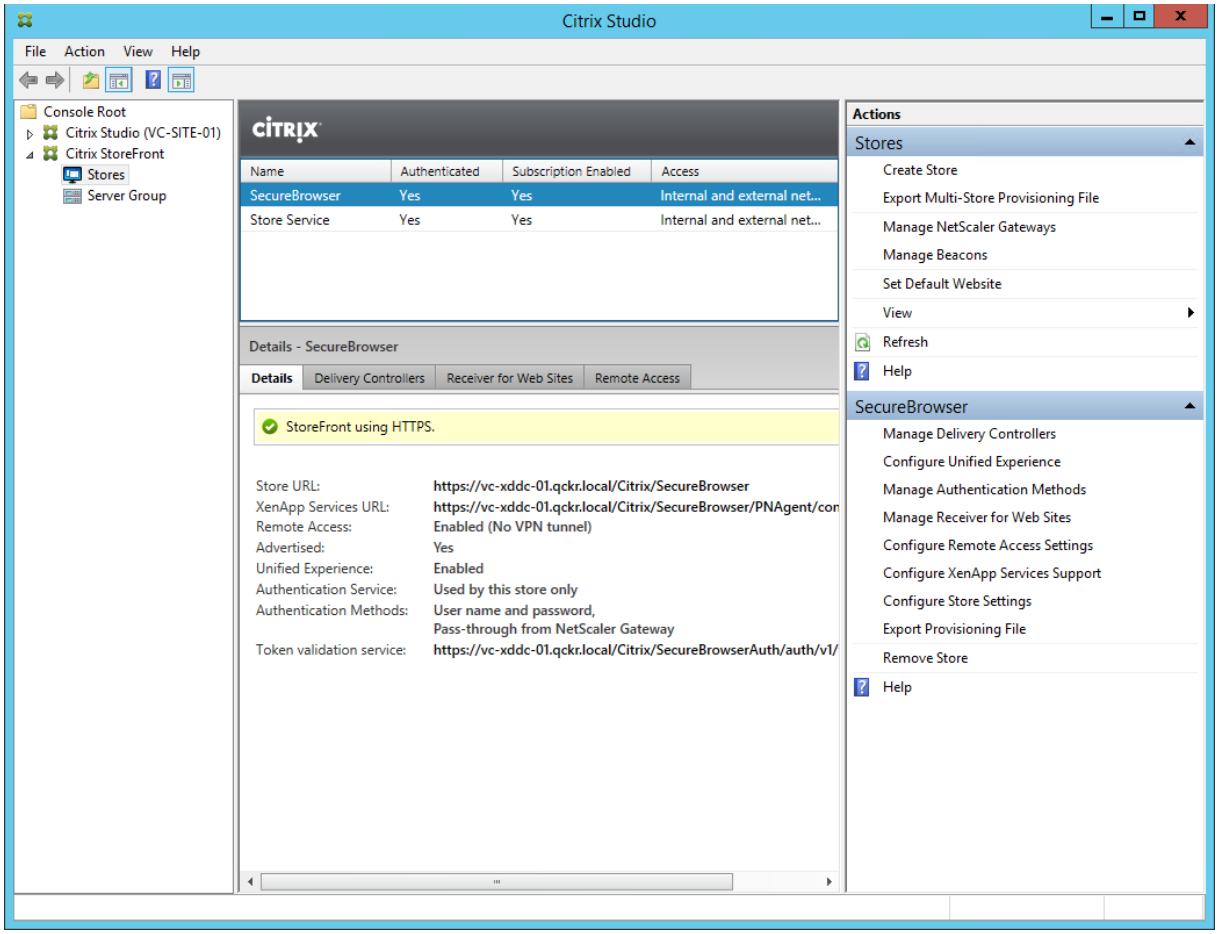
```
Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $true*
<!--NeedCopy-->
```

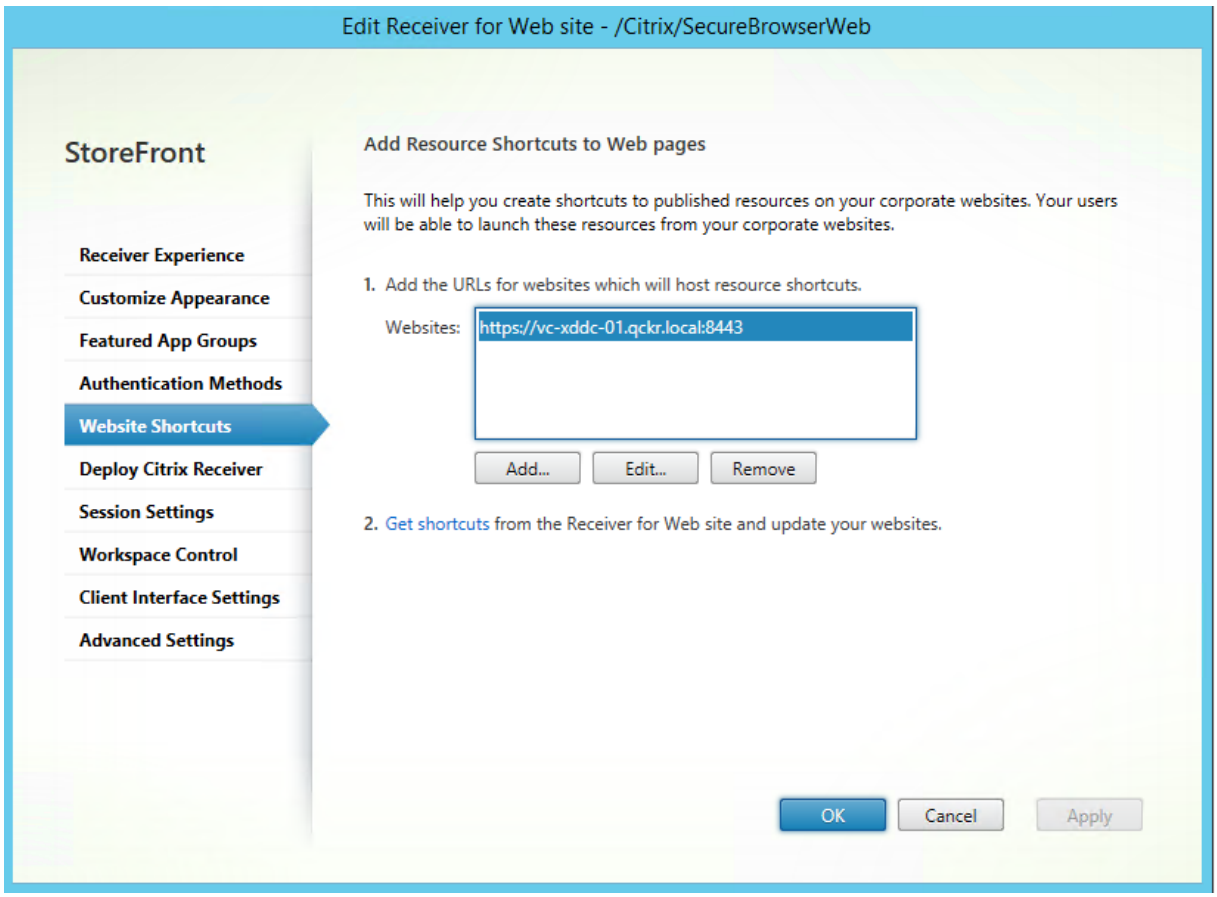
StoreFront

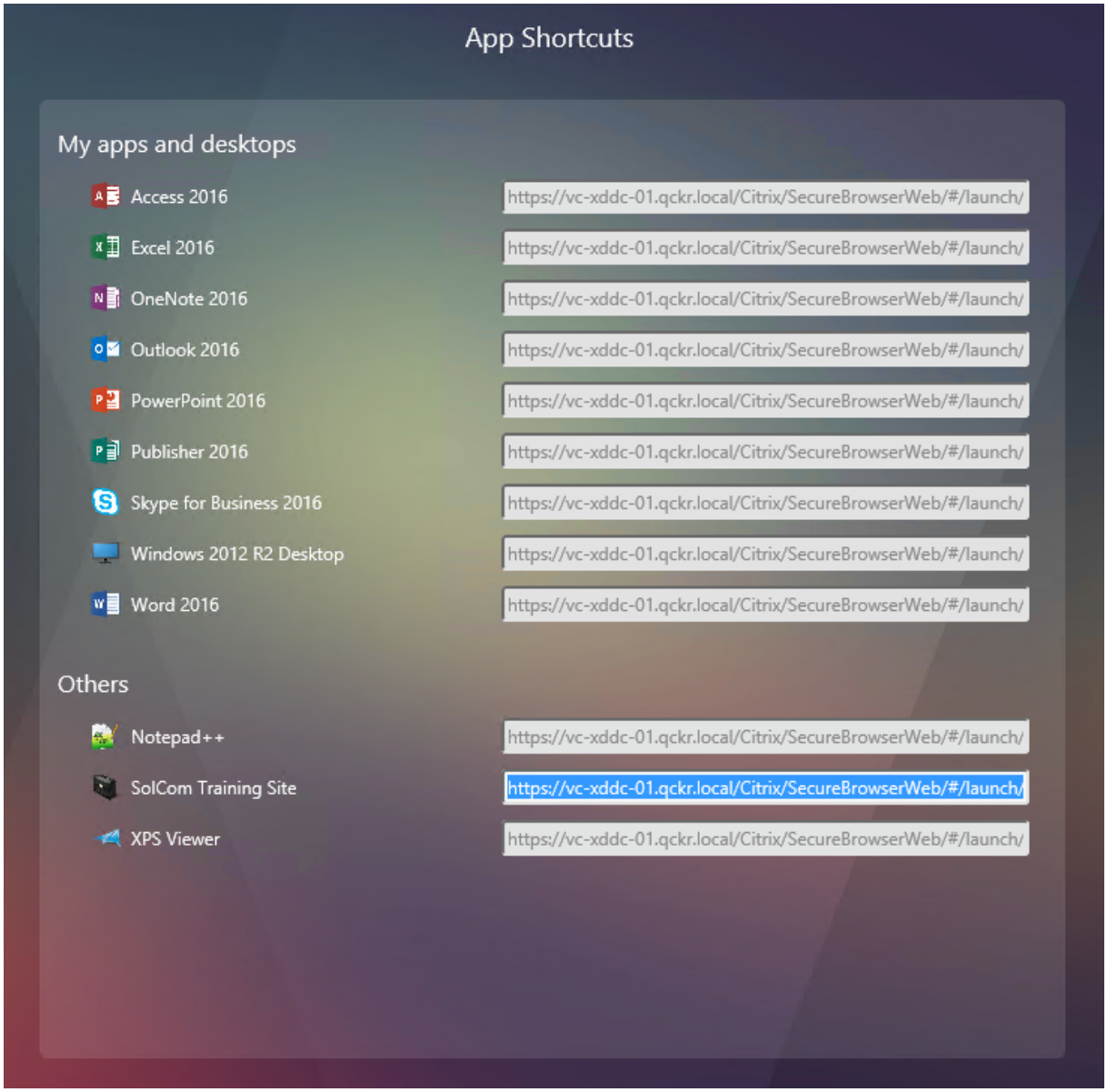


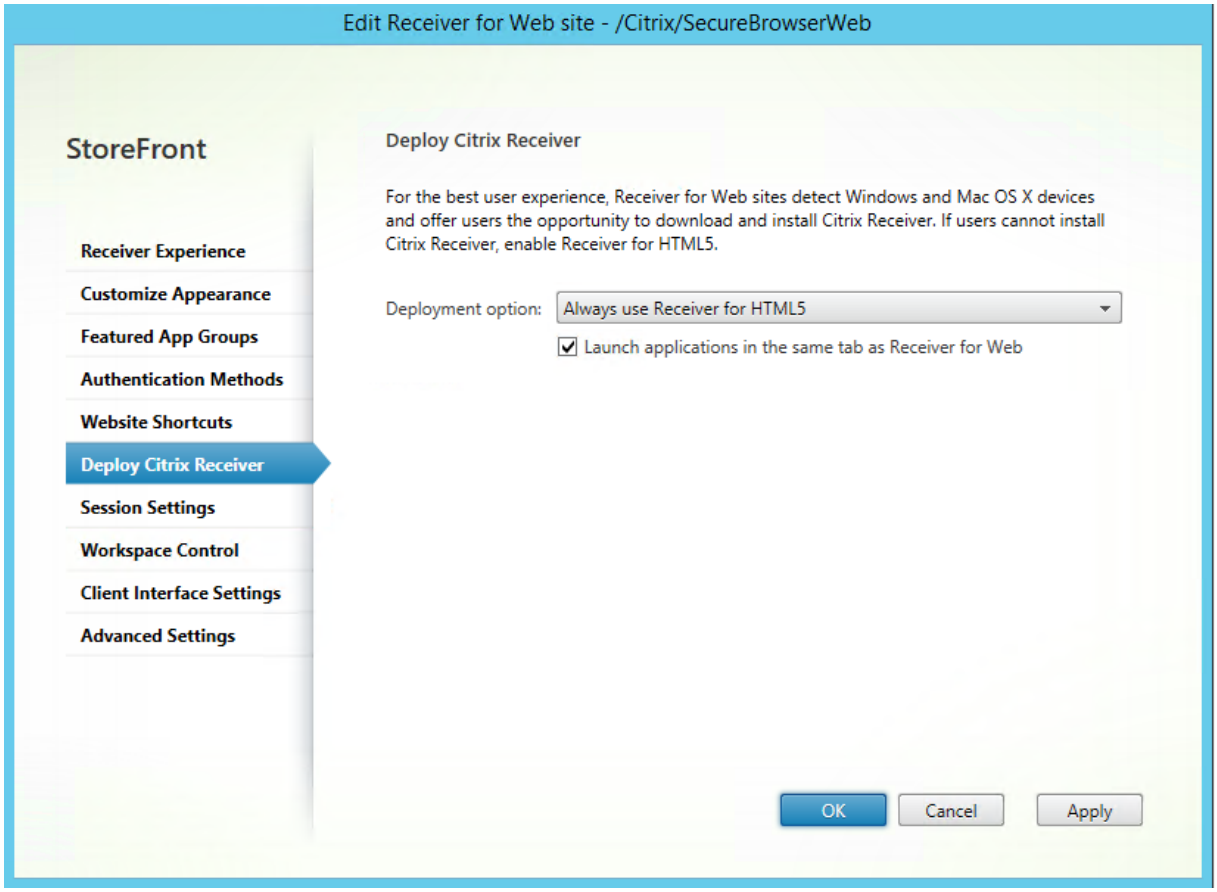


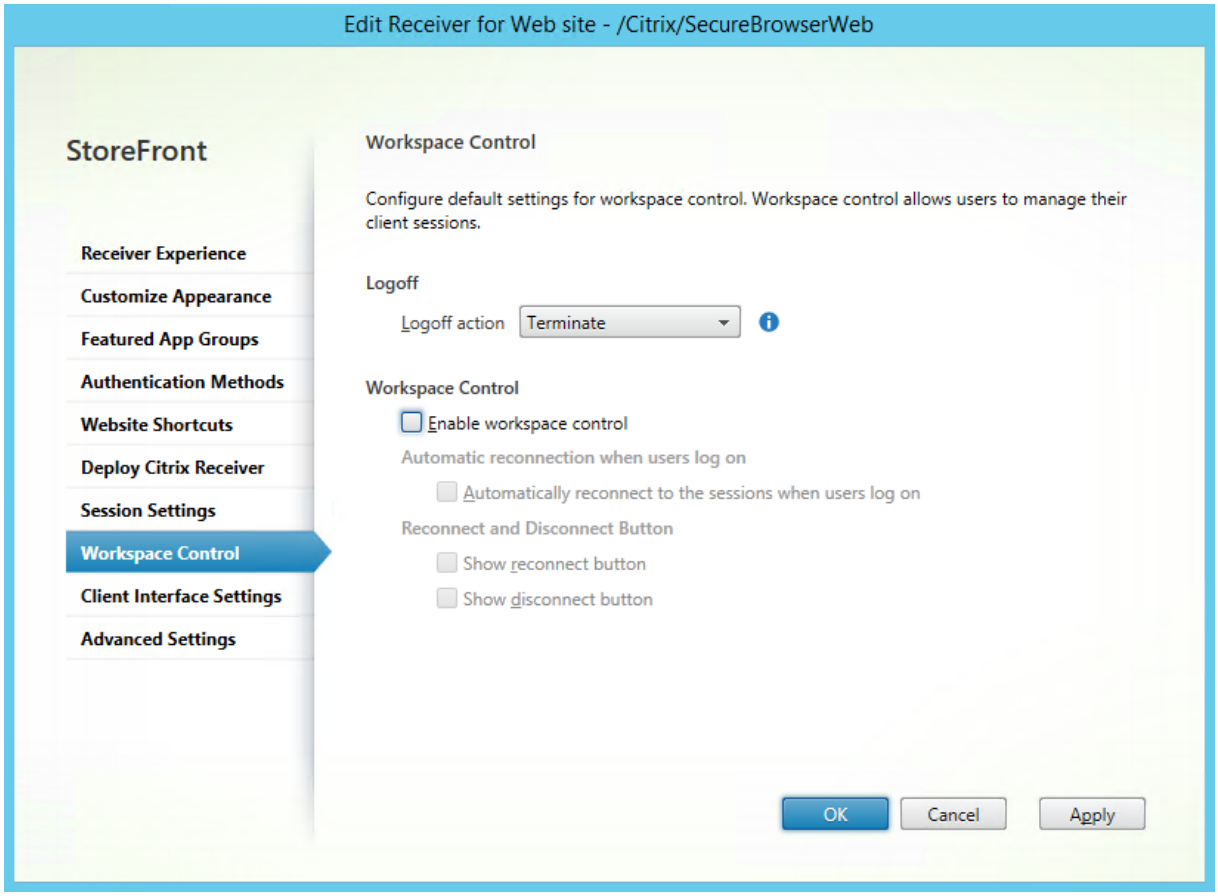


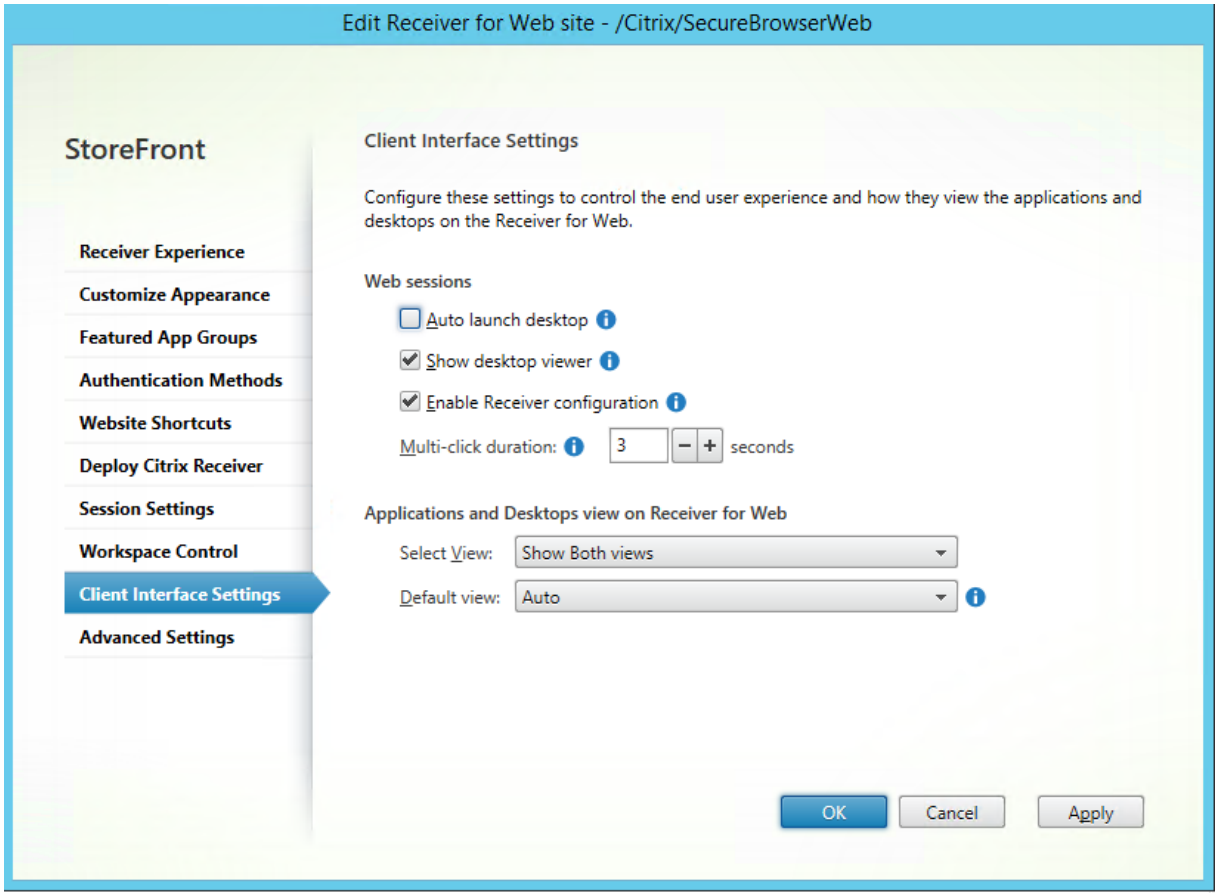


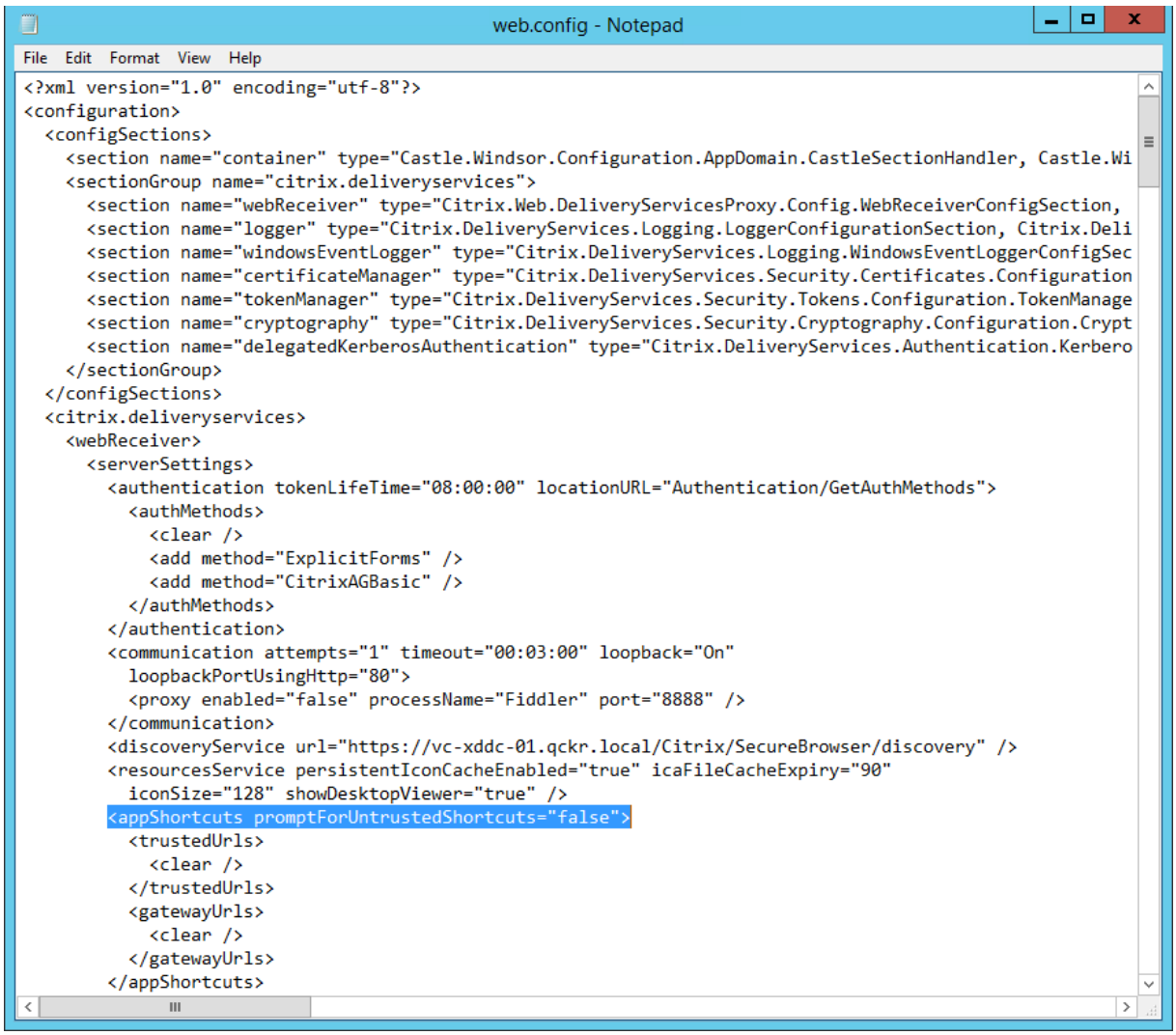












Créez un nouveau magasin appelé **SecureBrowser** et sélectionnez **Autoriser uniquement les utilisateurs non authentifiés à accéder à ce magasin** . Le trafic est authentifié car tous les utilisateurs transitent un jeton de NetScaler Gateway au contrôleur.

Ajoutez le contrôleur XenDesktop.

Activez **l'accès distant** et ajoutez une deuxième passerelle NetScaler Gateway que vous allez configurer dans les étapes suivantes. Pour cette configuration, vous n'avez pas besoin d'utiliser l' **adresse **Callback** ou VIP** dans la configuration StoreFront / NetScaler Gateway.

Terminez la création du magasin à l'aide des valeurs par défaut de l'assistant.

Après avoir créé le magasin, cliquez sur **Gérer Receiver pour les sites Web**.

Dans la page **Gérer Receiver pour les sites Web** , cliquez sur **Configurer** , accédez à **Raccourcis de site** Web, ajoutez l'URL interne du site Web et cliquez sur le lien **Obtenir les raccourcis** .

Ouvrez une session en tant qu'utilisateur régulier avec accès à l'application **Secure Browser** publiée.

Copiez l'URL de l'application Secure Browser et enregistrez-le dans un fichier texte pour l'utiliser ultérieurement dans la configuration de NetScaler Gateway.

Revenez à **Modifier les propriétés du site Receiver pour Web** , cliquez sur Déployer Citrix Receiver et sélectionnez **Toujours utiliser Receiver pour HTML5**. Sélectionnez l'option **Lancer les applications dans le même onglet que Receiver pour Web**.

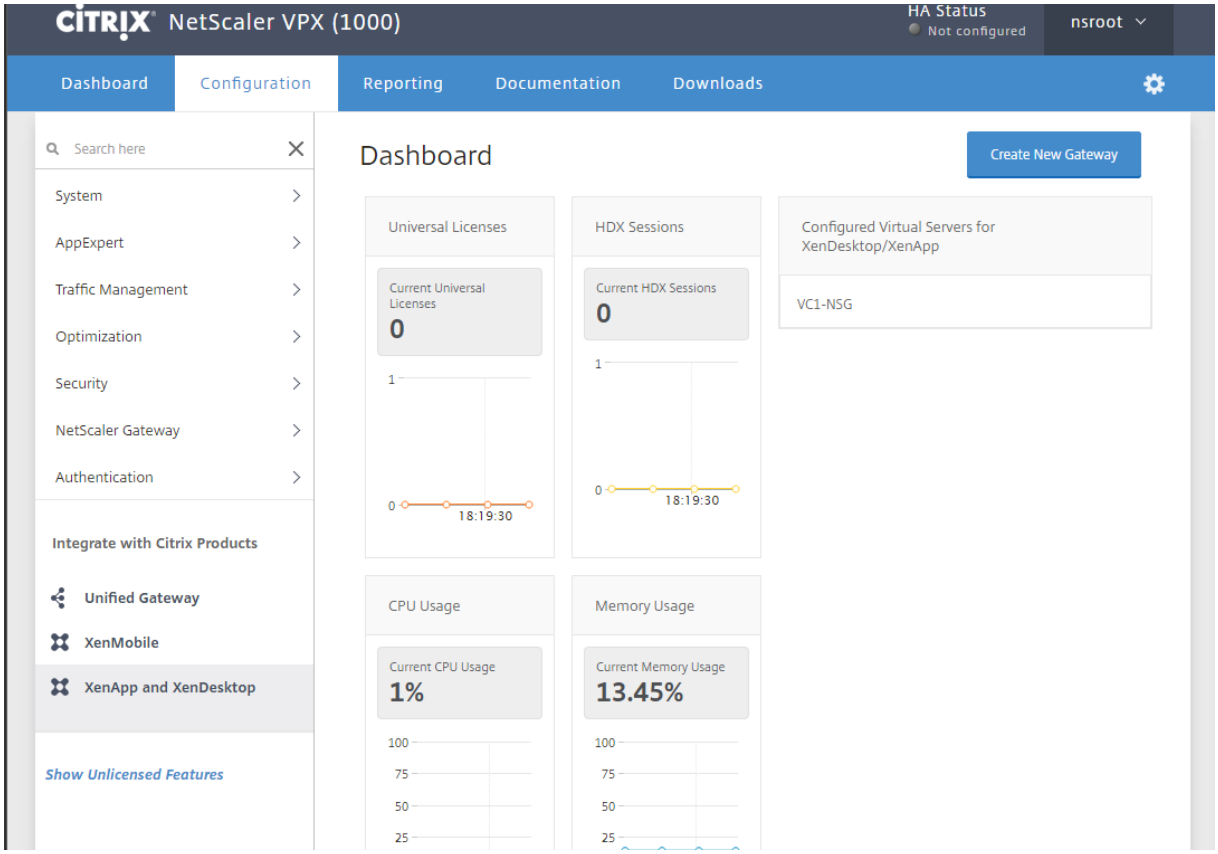
Cliquez sur **Contrôle de l'espace de travail**, dans l' **action de fermeture**de session, sélectionnez **Terminer**. Désactivez l'option **Activer le contrôle de l'espace de travail**.

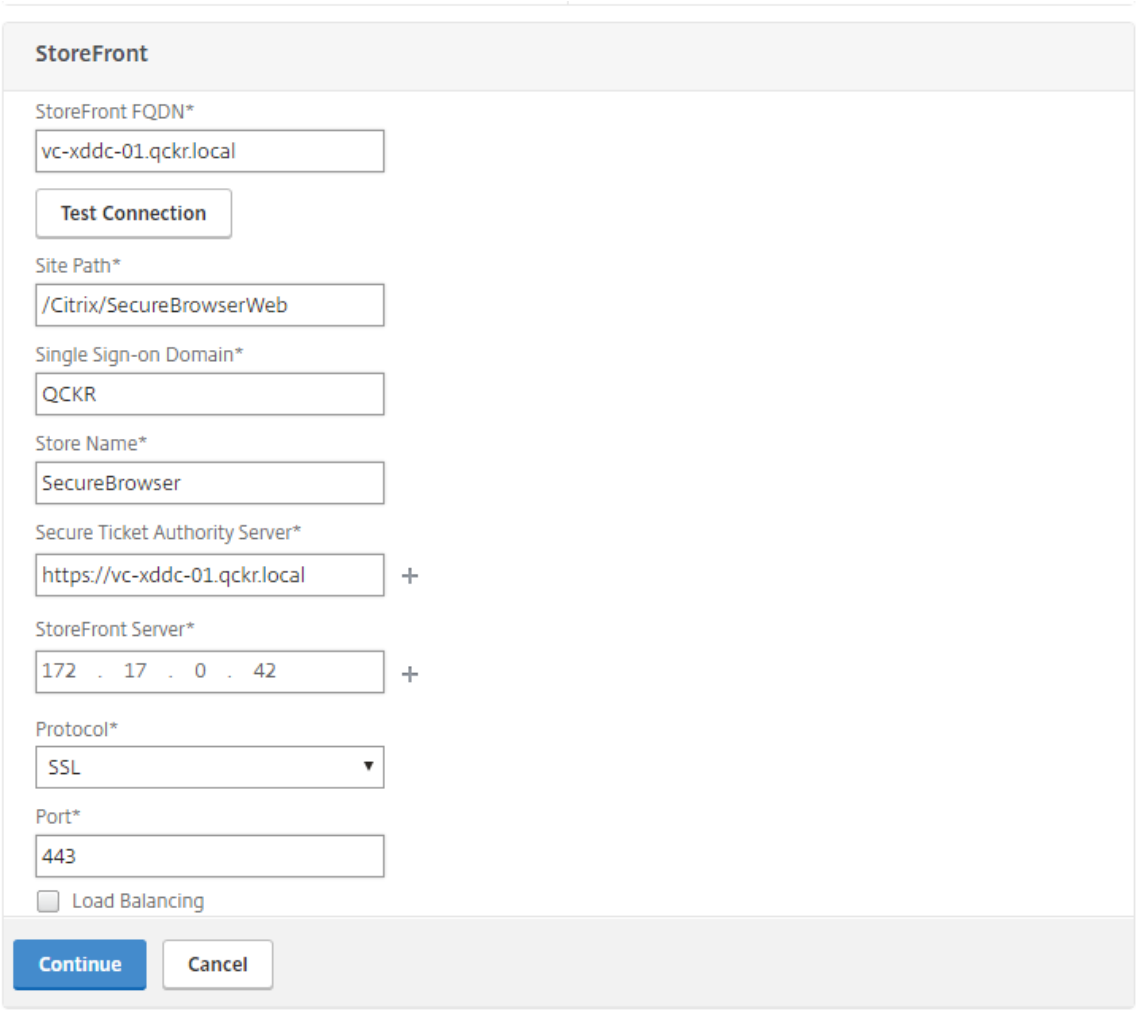
Cliquez sur **Paramètres de l'interface client**, désactivez l'option **Démarrage automatique du bureau**et cliquez sur **OK**pour enregistrer les paramètres.

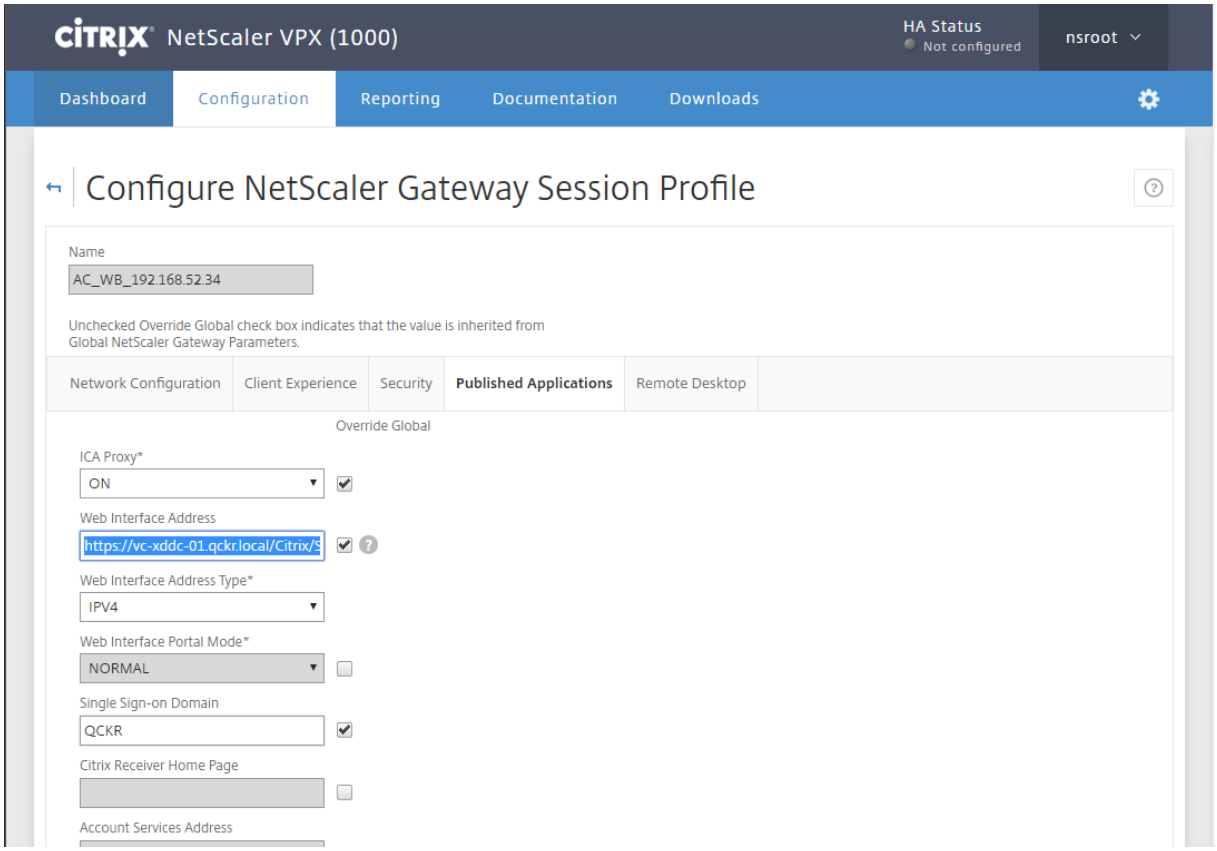
Dans un éditeur de texte, ouvrez le fichier C:\inetpub\wwwroot\Citrix\SecureBrowserWeb\web.config.

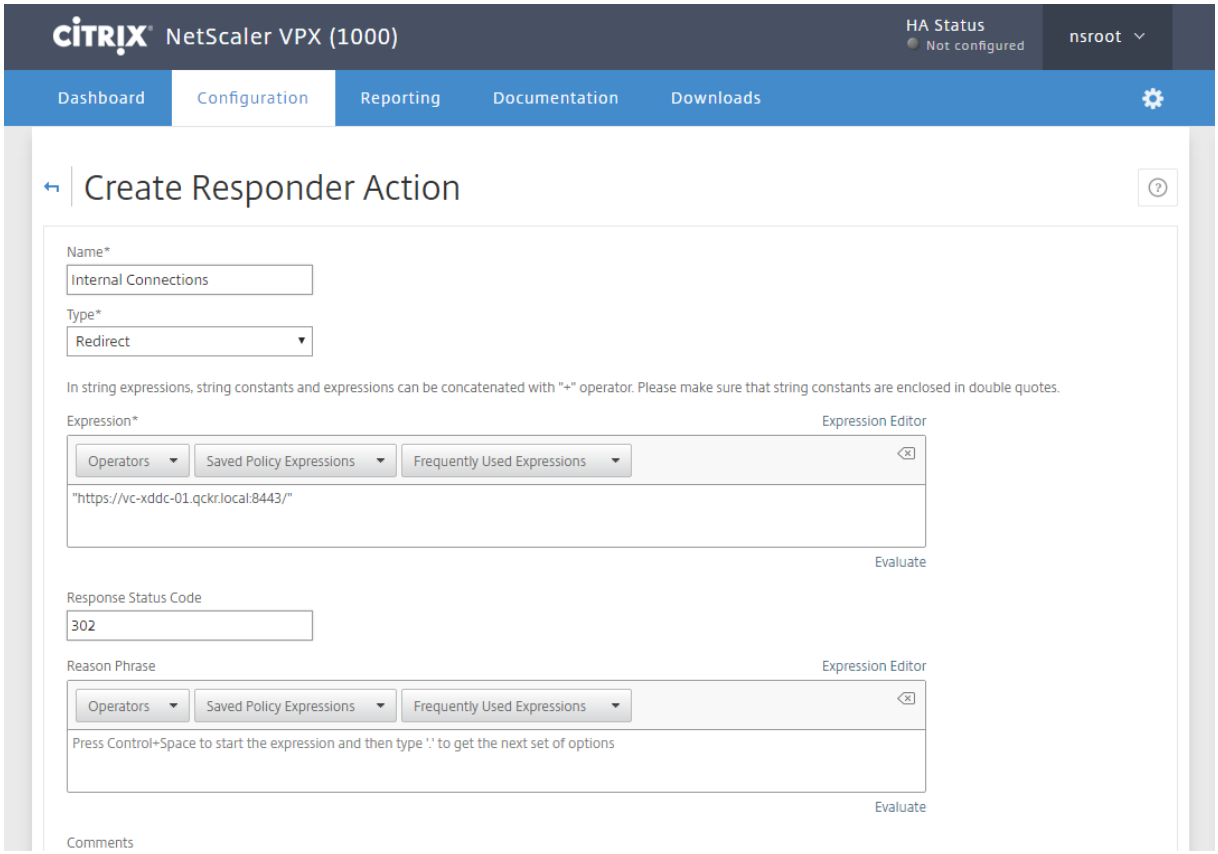
Recherchez le paramètre *<appShortcuts promptForUntrustedShortcuts="true">*, définissez-le sur **false** et enregistrez les modifications. La désactivation de ce paramètre empêche StoreFront de demander aux utilisateurs s'ils souhaitent lancer l'application.

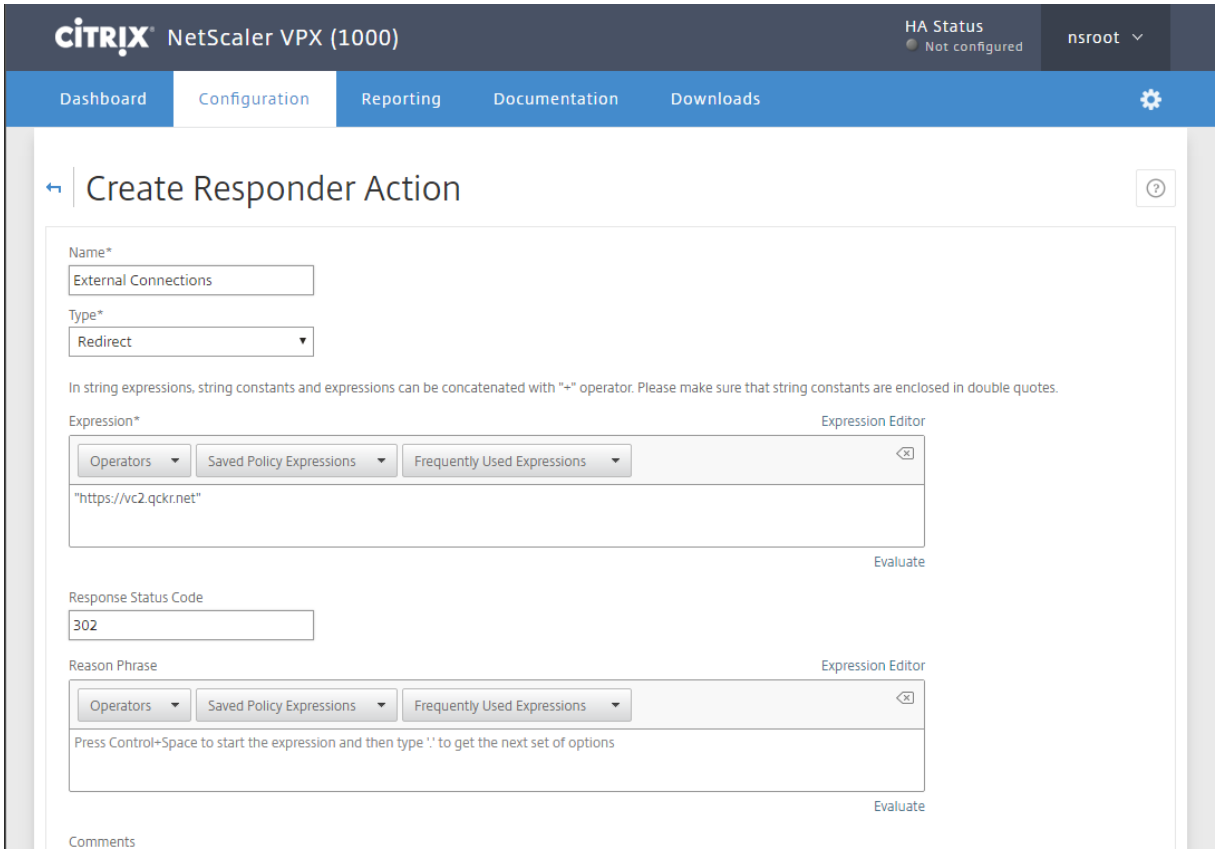
NetScaler Gateway

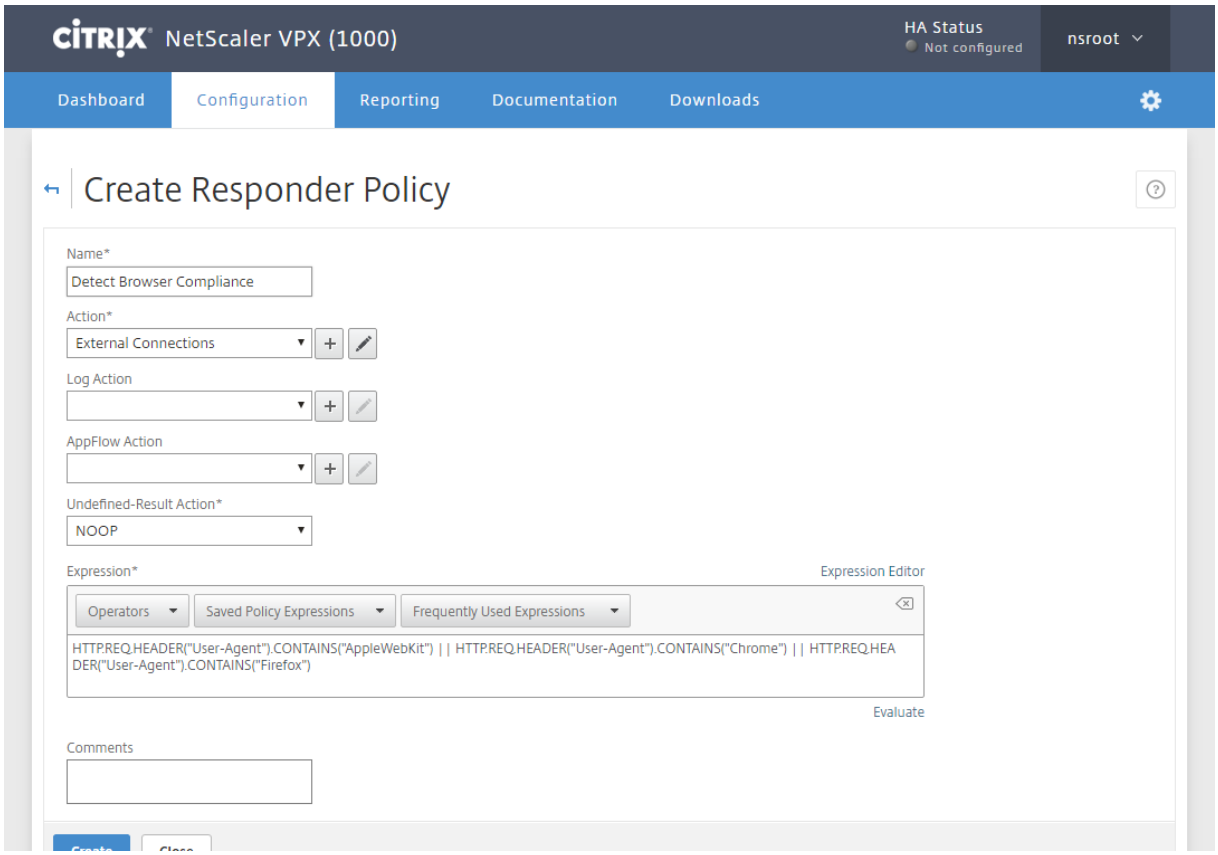


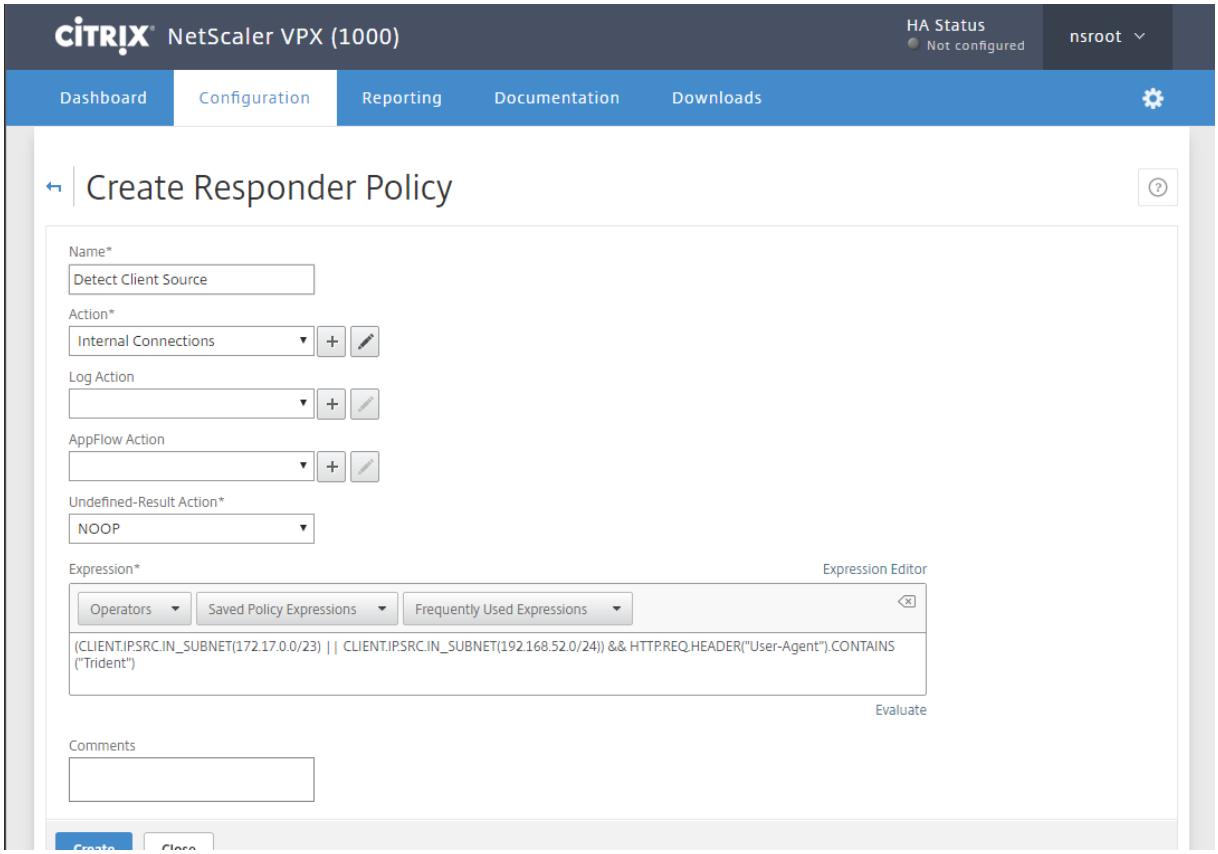


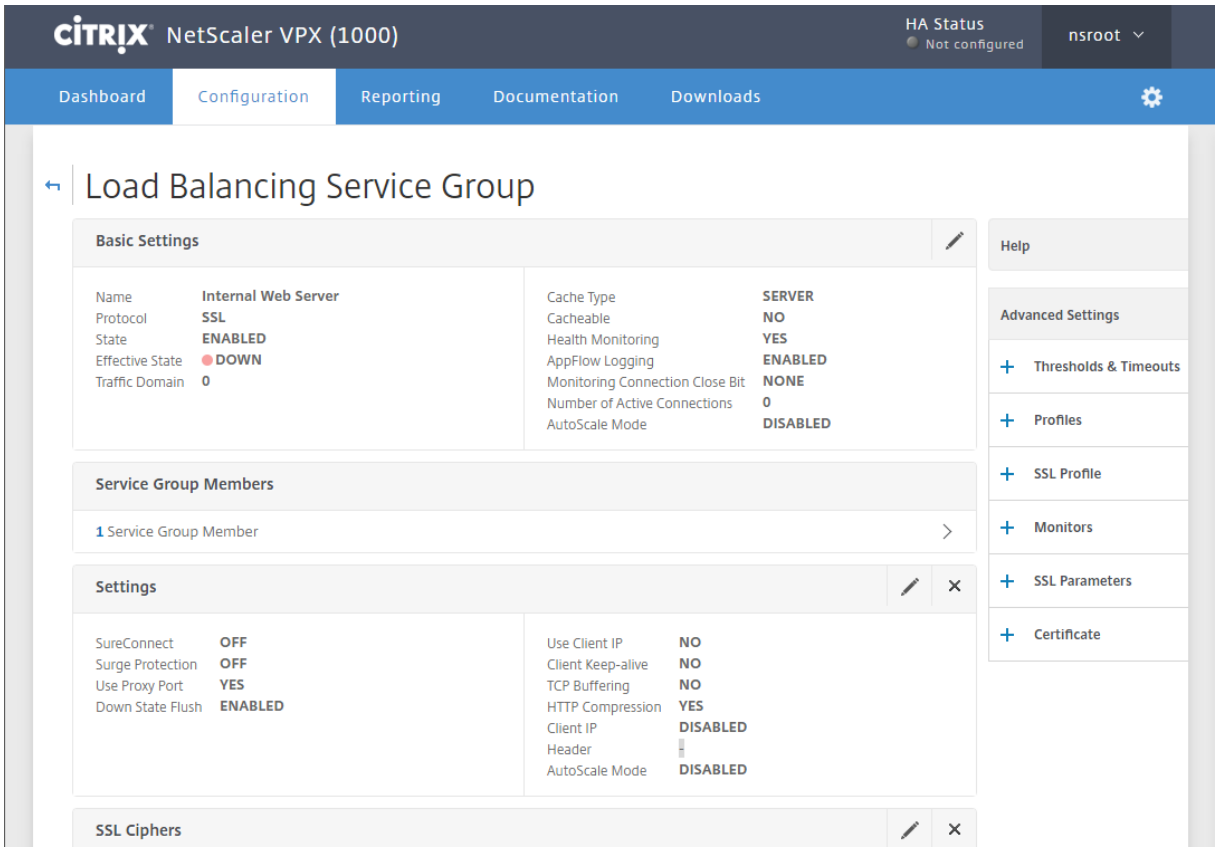


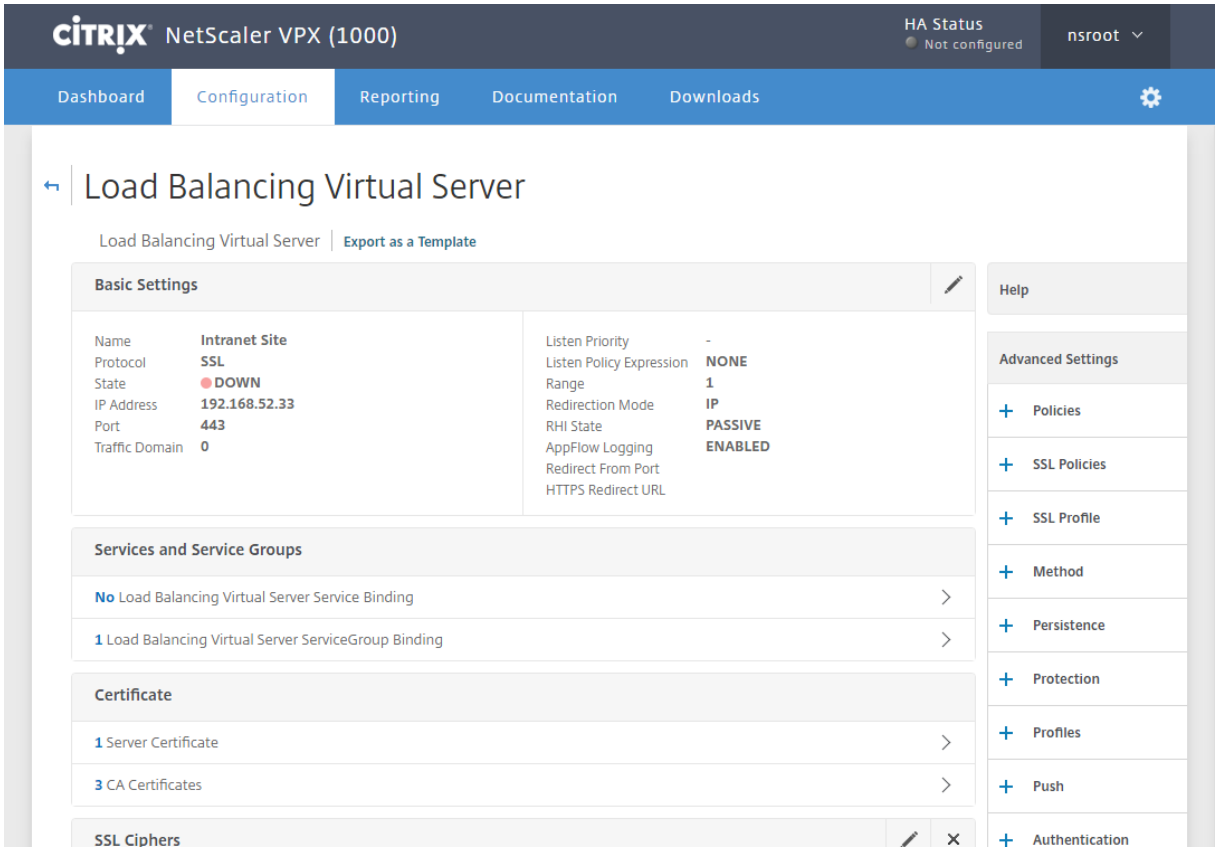


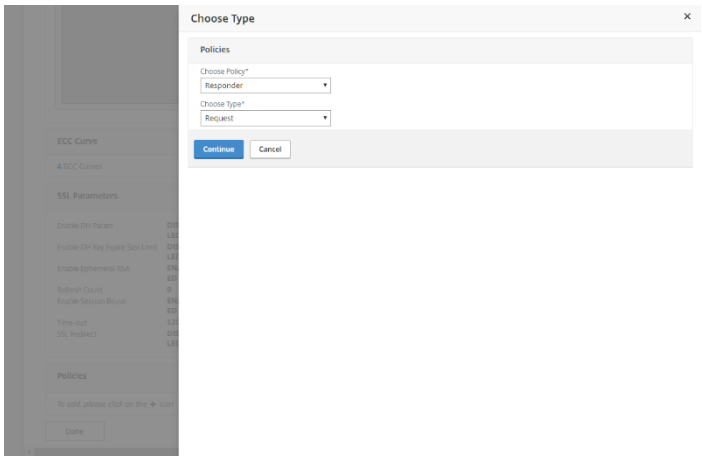


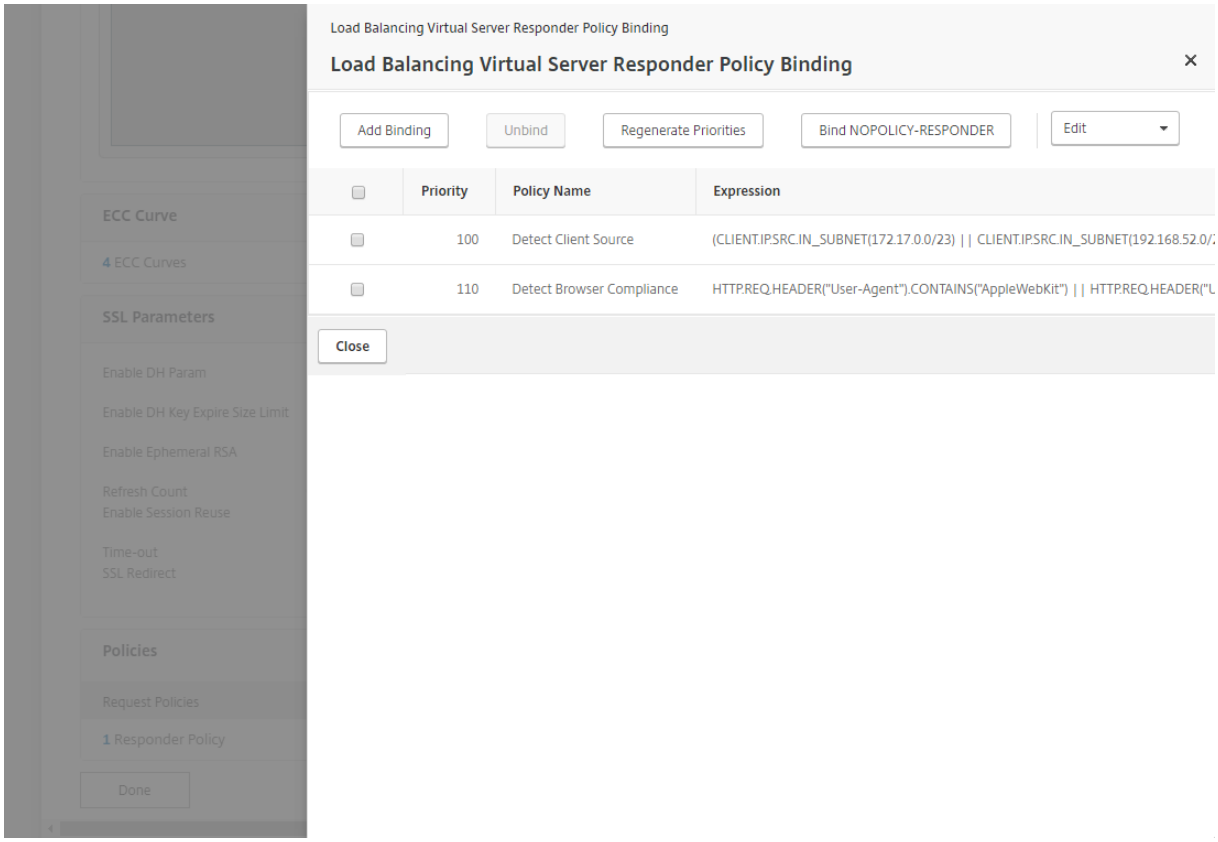












Dans l'interface graphique de NetScaler Gateway, dans le volet de navigation, cliquez sur **XenApp et XenDesktop**, puis sur le **tableau de bord**, cliquez sur **Créer une passerelle**.

Dans les propriétés StoreFront, définissez le **chemin du site sur** /Citrix/SecureBrowserWeb et définissez le nom du **magasin** sur *SecureBrowser* comme nouveau magasin dans le serveur StoreFront.

Continuez l'Assistant et enregistrez le nouveau serveur virtuel.

Sur le nœud **NetScaler Gateway** , développez **Stratégies** et accédez à **Session** .

Sélectionnez l'onglet **Actions** , modifiez l'action nouvellement créée pour le deuxième serveur virtuel, puis modifiez l'action **AC_WB_** policy.

Sous l'onglet **Applications publiées, collez l'URL Raccourcis** d'application que vous avez précédemment enregistrée dans le champ **Adresse de l'interface Web** , puis cliquez sur **OK** .

Dans le volet de navigation, cliquez sur le nœud **AppExpert**, développez la section **Répondeur**, puis cliquez sur **Actions**.

Ajoutez une nouvelle **action**, nommez-la *Connexions interne*set définissez le type sur **Redirection**.

Dans le champ **Expression** , ajoutez l'URL du site interne pour vous connecter entre guillemets, tels que`https://mysite.acme.com`

Cliquez sur **Créer** pour enregistrer l'action.

Ajoutez une nouvelle action, nommez-la *Connexions externe*set définissez le type sur **Redirection**.

Dans le champ **Expression** , ajoutez l'URL du deuxième serveur virtuel NetScaler Gateway entouré de guillemets, tels que`https://gateway.acme.com`

Cliquez sur **Créer** pour enregistrer l'action.

Accédez au nœud **Stratégies du répondeur** .

Ajoutez une nouvelle stratégie, nommez-la *Détecter la conformité du navigateur*, dans la liste déroulante **Action**, sélectionnez l'action **Connexions externes**que vous avez créée précédemment.

Définissez **l'action de résultat indéfini** sur **NOOP**.

Dans le champ **Expression** , ajoutez le texte suivant :

HTTP.REQ.HEADER (« User-Agent ») .CONTAINS (« AppleWebKit »)	HTTP.REQ.HEADER (« User-Agent ») .CONTAINS (« Chrome »)	HTTP.REQ.HEADER (« User-Agent ») .CONTAINS (« Firefox »)

Les expressions ci-dessus détectent les navigateurs non conformes ou, dans ce cas, pas Internet Explorer.

Cliquez sur **Créer** pour enregistrer les modifications.

Ajoutez une nouvelle stratégie, nommez-la *Détecter la source du client*, définissez l' **action Action**sur **Connexions internes**précédemment créée.

Définissez **l'action de résultat indéfini** sur **NOOP**.

Dans le champ Expression, ajoutez le texte suivant :

(CLIENT.IP.SRC.IN_SUBNET(172	CLIENT.IP.SRC.IN_SUBNET (192.168.52.0/24)) & & HTTP.REQ.HEADER (« User-Agent ») .CONTAINS (« Trident »)

Remplacez ou ajoutez chaque sous-réseau ci-dessus pour correspondre à votre environnement réseau interne. L'agent utilisateur, dans ce cas, correspond à la version configurée d'Internet Explorer et que le client se connecte à partir du réseau interne.

Cliquez sur **Créer** pour enregistrer les modifications.

Dans le volet de navigation, développez **Gestion du trafic > Équilibrage de charge**, puis sélectionnez

Serveurs. Ajoutez le serveur utilisé pour héberger le site interne.

Dans le volet de navigation, cliquez sur **Groupes de services** sous **Équilibrage de charge** g, ajoutez un nouveau groupe de services, définissez le **protocole** sur **SSL** et liez le **serveur** créé à l'étape précédente à la liste **Membres du groupe de services** .

Cliquez sur **Terminé**.

Dans le volet de navigation, cliquez sur **Serveurs virtuels** dans le nœud **Équilibrage de charge** , cliquez sur **Ajouter** et nommez le *site intranet du* serveur.

Définissez le **protocole** sur **SSL** et tapez l'adresse IP de l'équilibreur de charge.

Liez le **serveur Web interne du groupe de services** créé à l'étape précédente et configurez les certificats pour l'accès externe. Liez le certificat d'autorité de certification racine interne aux certificats de l'autorité de certification afin que l'équilibreur de charge puisse décharger SSL vers le serveur Web interne.

Dans le volet d'informations, dans **Paramètres avancés**, cliquez sur **+ Stratégies**. Cliquez sur le signe plus (+) pour lier une nouvelle stratégie.

Sélectionnez **Répondeur pour Choisir une stratégie** , puis cliquez sur **Continuer** . Sélectionnez **Détecter la source du client** et définissez la priorité sur 100.

Cliquez sur **Liaison**.

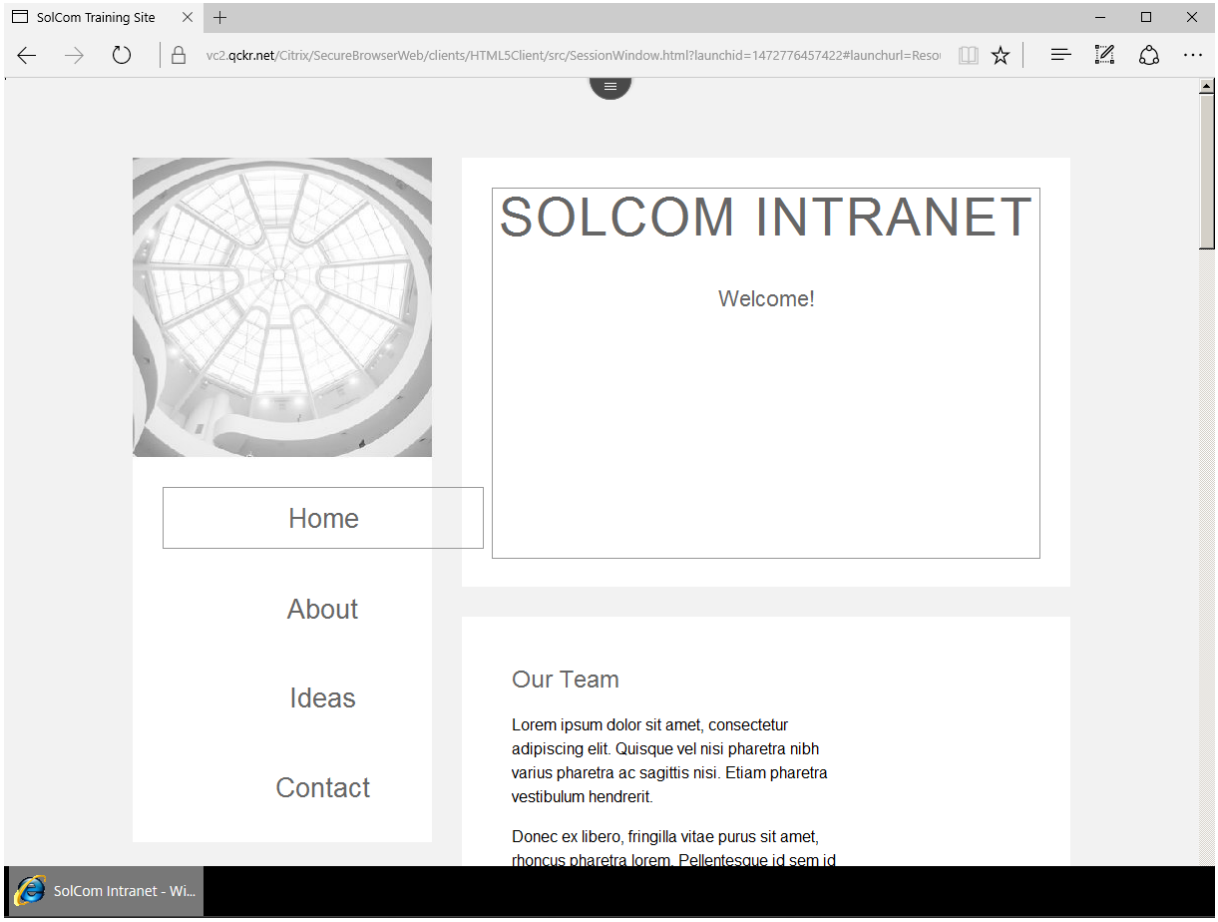
Cliquez sur la section Stratégie du **répondeur**, cliquez sur **Ajouter une liaison**, sélectionnez **Détecter la conformité du navigateur** et définissez la priorité sur **110**. Cliquez sur **Liaison**.

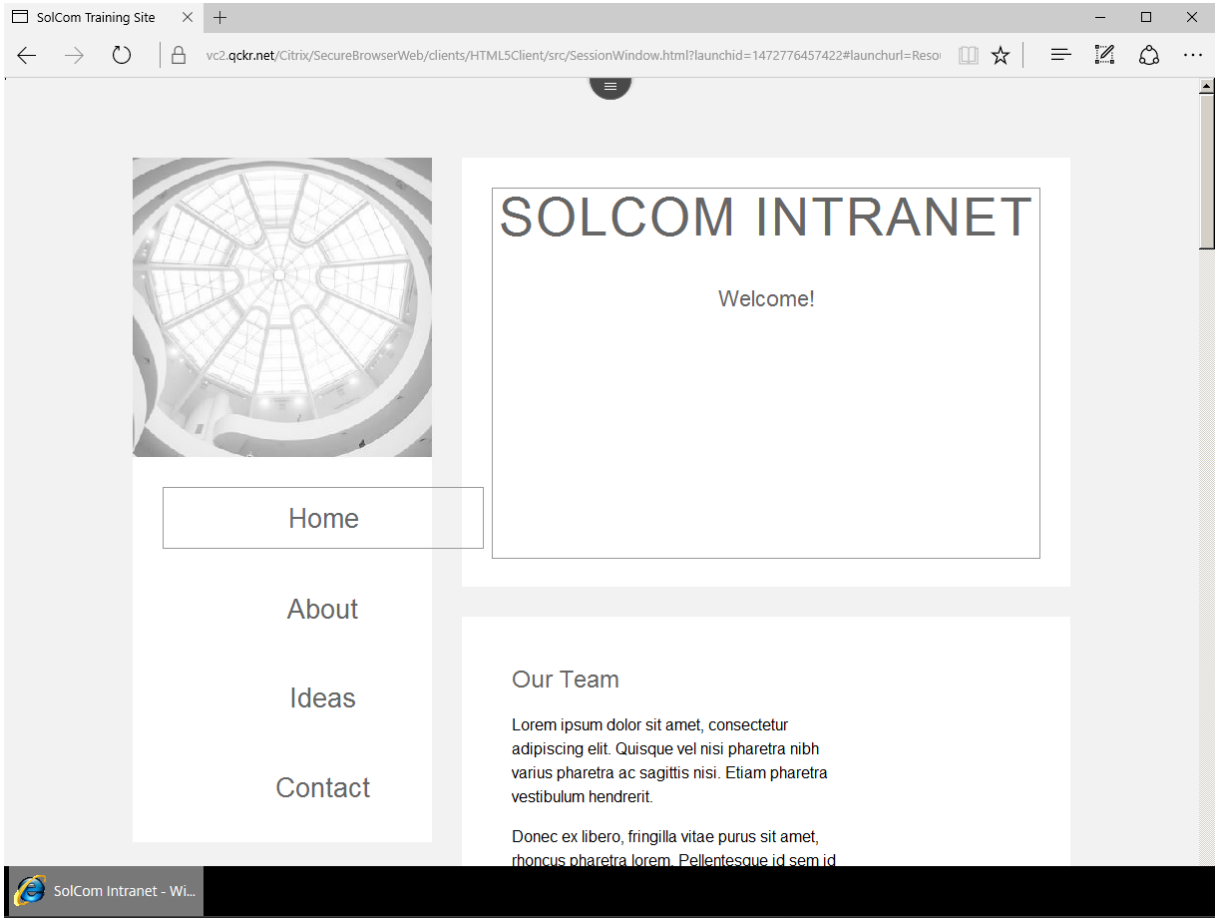
Cliquez sur **Fermer** , puis sur **Terminé** .

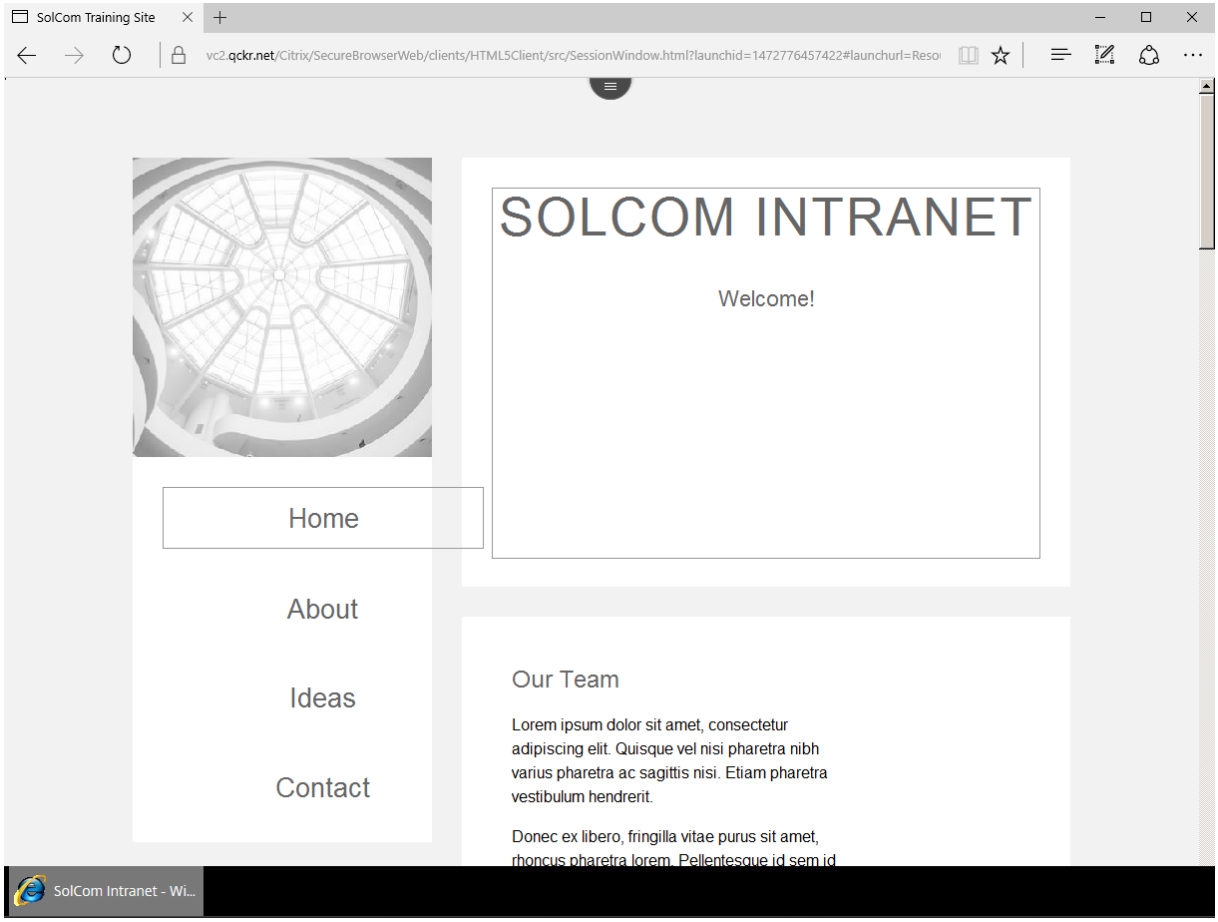
Enregistrez la configuration NetScaler Gateway.

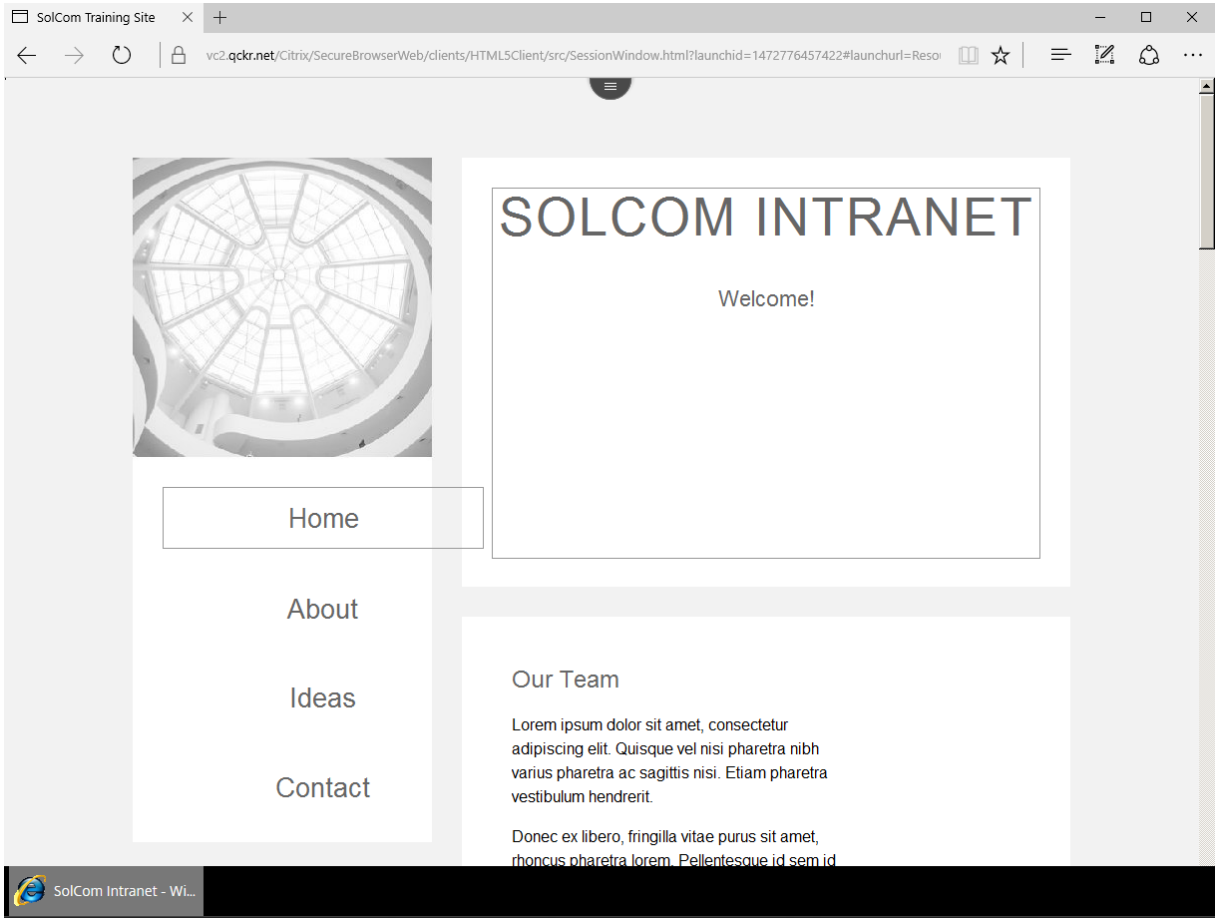
Résultats et attentes des cas d'utilisation

Cette section passe en revue les cas d'utilisation et les résultats attendus de la façon dont chaque utilisateur se connecte à la configuration précédente. Dans tous les cas d'utilisation suivants, l'utilisateur ouvre un navigateur installé localement et tape l'URL externe du site de formation.









Utilisateur externe avec navigateur non conforme

Résultat attendu : l'utilisateur lance la session Citrix Receiver dans un onglet de navigateur qui rend le site avec le navigateur sécurisé publié.

Utilisateur externe avec navigateur conforme

Résultat attendu : NetScaler Gateway proxie le trafic entre le navigateur local et le site Web interne.

Utilisateur interne avec navigateur non conforme

Résultat attendu : l'utilisateur lance la session Citrix Receiver dans un onglet de navigateur rendant le site avec le navigateur sécurisé publié.

Utilisateur interne avec navigateur conforme

Résultat attendu : la session utilisateur redirige vers le site interne ; NetScaler Gateway ne fournit pas de proxy la connexion puisque le client se connecte à partir du réseau interne.

Limitations connues

- L'URL dynamique passant au serveur virtuel NetScaler Gateway ne prend pas en charge l'utilisation de Citrix Receiver pour HTML5 pour Secure Browser.
  - Pour transmettre une URL de lancement au serveur virtuel, désactivez le proxy ICA dans le profil de session. Le proxy ICA est requis pour Citrix Receiver pour HTML5.
- Citrix Receiver pour HTML5 ne prend pas en charge la redirection de contenu.
  - Les administrateurs peuvent configurer Citrix Receiver dans StoreFront pour les sites Web.
- Environnements qui ont plusieurs sites distincts, créent des stratégies de session NetScaler Gateway différentes pour chaque site et les lient au serveur virtuel ou créent un portail de lancement interne qui peut héberger des URL pour les sites internes.

Références

- Comment sécuriser les connexions ICA dans XenApp et XenDesktop 7.6 à l'aide de SSL

Dimensionnement et mise à l'échelle du cache hôte local

January 8, 2020

Le cache hôte local a été introduit dans XenApp et XenDesktop 7.12 pour remplacer la fonctionnalité de location de connexion fournie dans XenDesktop 7.6. Local Host Cache couvre plus de scénarios que la location de connexion, mais nécessite des considérations de conception différentes.

Vous trouverez des détails sur les considérations relatives à la conception des fonctions de location de connexion à l'adressehttps://www.citrix.com/blogs/2014/11/11/xendesktop-7-6-connection-leasing-design-considerations/.

- Le cache hôte local prend en charge plus de cas d'utilisation que la location de connexion.
- Lorsqu'il est opérationnel, le cache hôte local nécessite plus de ressources (CPU et mémoire) que la location de connexion.
- En mode panne, un seul courtier par zone gère les enregistrements VDA et les sessions de courtier.
- Un processus électoral détermine quel courtier sera actif en cas de panne, mais ne tient pas compte des ressources du courtier.
- Si un courtier unique dans une zone ne serait pas capable de gérer toutes les ouvertures de session pendant le fonctionnement normal, cela ne fonctionnera pas bien en mode panne.
- Aucune gestion de site n'est disponible en mode panne.
- Un SQL Server hautement disponible reste la conception recommandée.

- Pour les scénarios de connectivité de base de données intermittente, il est toujours préférable d'isoler SQL Server et de laisser le site en mode panne jusqu'à ce que tous les problèmes sous-jacents soient résolus.
- Il y a une limite de 5 000 VDA par zone (non appliquée).
- Il n'y a pas de limite de 14 jours.
- Les postes de travail groupés ne sont pas pris en charge en mode panne, dans la configuration par défaut.

Architecture

La location de connexion a été introduite dans XenDesktop 7.6 pour permettre un accès continu aux ressources pendant les périodes d'interruption de la base de données du site. Il ne prend pas en charge les postes de travail groupés VDI et, par défaut, les utilisateurs doivent se connecter à une ressource au cours des 14 jours précédents. Une autre restriction était qu'il tenterait de connecter les utilisateurs au dernier hôte de poste de travail ou d'application auquel ils se sont connectés pendant le fonctionnement normal. Si cela n'était pas disponible, la connexion ne serait pas négociée.

L'architecture des deux technologies (location de connexion et cache hôte local) est très différente, et elles nécessitent des ressources différentes pour fonctionner. La location de connexion crée des fichiers de location XML individuels, qui peuvent nécessiter plusieurs Go d'espace disque, en fonction du nombre de ressources dans un site. Local Host Cache utilise une base de données SQL Server locale et est plus efficace dans l'utilisation de l'espace disque, mais nécessite beaucoup plus de mémoire et de CPU que la location de connexion. Les deux ont des phases de synchronisation où les détails de la base de données du site principal sont synchronisés avec les courtiers (Controllers). La synchronisation initiale de la location de connexion peut entraîner des E/S par seconde considérables en raison du nombre total de fichiers individuels créés sur le système de fichiers. Bien que Local Host Cache utilise une base de données SQL qui nécessite encore des E/S par seconde, il a l'avantage d'optimiser SQL ces écritures.

Dans une configuration de location de connexion avec plusieurs courtiers, chaque courtier a une copie des baux XML et est capable de courtier des connexions lors d'une panne, ce qui aide à équilibrer la charge. Toutefois, avec Local Host Cache, un courtier unique est choisi pour courtier toutes les connexions et gérer les enregistrements VDA. Tous les VDA du site se réinscriront auprès de ce courtier unique et, à ce titre, ce courtier connaîtra une plus grande demande de ressources par rapport à un site multi-courtier en fonctionnement normal, en particulier dans les sites comptant un grand nombre de VDA.

Local Host Cache utilise Microsoft LocalDB, qui apparaît dans le Gestionnaire des tâches en tant que processus sqlserver.exe. Il a été configuré pour utiliser jusqu'à 1 Go de mémoire pour la mise en cache du pool de mémoire tampon de base de données. Cependant, le processus va se développer au-delà de cela car le moteur SQL a besoin de mémoire pour lui-même et d'autres caches plus petits. En général, plus la panne est longue et plus les ressources sont accessibles en mode panne,

plus l'utilisation de la mémoire LocalDB augmentera. Toutefois, lorsque la connectivité de la base de données de site est restaurée, sqlserver.exe conservera cette mémoire et ne la renvoie pas immédiatement au pool principal.

Effet des sockets CPU et des cœurs en mode panne

Dans les versions précédentes de XenApp et XenDesktop, les administrateurs ne se préoccupaient pas nécessairement de la configuration du processeur de la machine Broker (Controller) : la disposition du nombre de sockets et de cœurs, soit dans une machine physique ou virtuelle.

Local Host Cache utilise une version d'exécution de SQL Server appelée LocalDB qui dispose d'une licence spécifique qui le limite au moindre des quatre cœurs ou d'un socket unique. Cela peut avoir un effet significatif sur les performances lorsque la machine physique ou virtuelle a été configurée avec plusieurs sockets avec un seul ou double cœur. Une machine de courtage avec 4 sockets et un cœur par socket limitera LocalDB à utiliser un seul cœur, alors que la même machine virtuelle configurée comme une machine à 1 socket 4 core signifie que LocalDB peut accéder aux 4 cœurs (bien que les partager avec d'autres processus). En mode panne, LocalDB exécutera le même courtier et le même code SQL que pendant le fonctionnement normal. La plupart des requêtes SQL peuvent être gourmandes en CPU et avoir un impact direct sur les performances du courtage en mode panne.

D'autres facteurs incluent la configuration du site elle-même :

- Nombre de demandes publiées
- Nombre d'utilisateurs faisant l'objet d'un courtage
- Taux auquel les utilisateurs tentent de lancer des sessions
- Performances Active Directory

À mesure que l'utilisation totale du processeur du courtier approche 100 %, le temps de réponse du courtage augmentera, les ouvertures de session prendront plus de temps à traiter et certaines tentatives d'ouverture de session peuvent échouer.

Sites avec plusieurs courtiers

En mode panne de site, seul un courtier traite les demandes d'enregistrement et d'ouverture de session. Dans un site multi-courtiers, un processus électoral a lieu pour désigner le courtier qui sera actif pendant la panne. Toutefois, ce processus électoral ne tient pas compte des ressources matérielles dont disposent les courtiers. Cela signifie que dans un site où les courtiers ont des quantités différentes de ressources, le courtier élu ne sera pas nécessairement le plus puissant en termes de CPU ou de RAM, ce qui pourrait potentiellement conduire à de mauvaises performances en mode panne. Il est important que chaque courtier réponde aux exigences supplémentaires de Local Host Cache, au cas où il serait choisi.

Synchronisation avec la base de données du site

Le service CitrixConfigSync gère l'importation de données de la base de données du site dans une copie locale sur les courtiers. Il surveille la base de données du site pour les modifications apportées à la configuration du site et déclenche une nouvelle importation lorsque des modifications se produisent. Une copie de la base de données locale en cours est effectuée avant le début de l'importation. Plus le nombre de ressources (telles que les VDA) dans un site est important, plus l'importation prendra de temps, mais elle devrait être inférieure à dix minutes pour un site avec 5000 VDA.

Emplacement de la base de données

La base de données locale est stockée dans :

C:\Windows\ServiceProfiles\NetworkService\HaDatabaseName.mdf

Pour garantir la fiabilité, le service CitrixConfigSync effectue une sauvegarde de l'importation de base de données synchronisée précédemment réussie, avant de démarrer une nouvelle synchronisation de base de données de site. Si, pour une raison quelconque, la synchronisation ne réussit pas, la sauvegarde est utilisée jusqu'à ce qu'une synchronisation réussie soit terminée. Vous ne devez pas copier la base de données manuellement.

Comparaison de Local Host Cache avec la location de connexion

	Location de connexion	Cache hôte local
Espace disque	2 Go recommandés	Dépend de la configuration du site. Pour 50 hôtes RDS avec 125 000 utilisateurs, 300 Mo sont utilisés.
RAM	100 MO	3 Go, ~ 1 Go pour SQL Server, 2 Go pour High Availability Service et CitrixConfigSync Service.
Temps de synchronisation de la configuration	Dépendante IOPS ; 40 000 VDA : ~ 26 minutes	5 000 VDA : ~ 7 minutes

	Location de connexion	Cache hôte local
Temps d'activation en cas de panne	150 secondes, délai d'attente SQL de 30 secondes + délai d'attente de 120 secondes (configurable)	Dépend du nombre de VDA et de la dernière synchronisation d'enregistrement avec le courtier. Seul un courtier unique sera disponible pour l'enregistrement VDA en mode panne, donc pour un grand nombre de VDA, cela peut prendre plusieurs minutes avant que tous les VDA ne soient enregistrés.
Temps de restauration des opérations normales	120 secondes pour la désactivation du crédit-bail, alors les VDA doivent se réenregistrer auprès des courtiers	Comme ci-dessus, les VDA devront annuler leur inscription auprès du courtier secondaire et se réinscrire auprès du courtier principal.
Nombre de VDA pris en charge	50,000	5,000. Un site peut avoir plus que cela, mais le temps nécessaire pour synchroniser la base de données du site augmentera avec le nombre de VDA. Les performances d'un courtier unique avec un grand nombre de VDA peuvent entraîner le fait que certaines connexions ne soient pas négociées pendant la panne.
Gestion du site en cas de panne	Non	Non

Configuration des limites de mémoire LocalDB

Le processus LocalDB a été limité à 1 Go de RAM pour la mise en cache, ce qui ne devrait pas normalement être modifié. Cette valeur peut être modifiée si nécessaire ; pour que les modifications prennent effet, le site doit fonctionner normalement (pas en mode d'interruption) et une synchronisation de la

base de données du site doit être forcée.

Pour réduire la mémoire à 768 Mo :

Étape 1. Modifiez le fichier C:\Program Files\Citrix\Broker\Service\HighAvailabilityService.exe.config.

Recherchez la section <appSettings> et ajoutez une entrée :

```
<add key="MaxServerMemoryInMB"value="768"/>
```

Étape 2. Pour forcer la synchronisation de la base de données, arrêtez le service de haute disponibilité. Si sqlserver.exe est en cours d'exécution, arrêtez-le à l'aide du Gestionnaire des tâches ou de PowerShell.

Étape 3. Maintenant, apportez une modification triviale au site, par exemple modifiez la description d'un groupe de mise à disposition en ajoutant un ".", puis retirez-le à nouveau. Ensuite, démarrez le service de haute disponibilité ; cela devrait démarrer sqlserver.exe et une synchronisation doit se produire.

Une réduction excessive de la mémoire affectera les performances et n'est pas recommandée. Cependant, l'augmenter à 2 Go n'améliore pas les performances de manière significative, et la ressource CPU est plus un goulot d'étranglement que la RAM.

Activation ou désactivation du cache hôte local

La location de connexion et le cache hôte local peuvent être désactivés, mais un seul d'entre eux peut être actif à la fois.

Set-BrokerSite –ConnectionLeasingEnabled $False

Set-BrokerSite –LocalHostCacheEnabled $True

Limitations

Les postes de travail doivent avoir été affectés avant de pouvoir être utilisés en mode panne. Les postes de travail non affectés ne seront pas disponibles pour le courtage. Cela peut entraîner l'indisponibilité des postes de travail et la création de rapports « en mode maintenance » si une panne survient avant que toutes les affectations aient été synchronisées, même si un utilisateur s'est vu attribuer un poste de travail.

Les postes de travail groupés ne sont pas pris en charge en mode panne, dans la configuration par défaut. Il existe une solution de contournement, mais elle a des implications potentielles en matière de sécurité et de performances. Si vous configurez un groupe de mise à disposition contenant des postes de travail groupés pour ne pas redémarrer à la fermeture de session, tous les postes de travail groupés sous tension de ce groupe seront disponibles en mode panne. Toutefois, après la déconnexion d'un utilisateur, le Bureau ne sera pas dans un état propre car le Bureau n'est pas redémarré. Cela pourrait

être un problème de sécurité dans n'importe quel scénario. Si l'utilisateur suivant de ce bureau est un administrateur local de ce bureau, les données d'un utilisateur précédent peuvent être accessibles. Et bien que ce risque soit moins préoccupant pour les utilisateurs standard (non administrateurs), gardez à l'esprit que les applications pourraient se comporter de manière incorrecte et causer des problèmes de performances au fil du temps.

Important : les administrateurs doivent examiner attentivement les implications potentielles de l'utilisation de cette solution de contournement pour l'utilisation de postes de travail groupés non redémarrés en mode panne.

Comme dans le cas de la location de connexion, aucune modification de site ne peut être apportée en cas de panne ; la base de données est effectivement un instantané de la base de données du site principal et est supprimée chaque fois qu'une nouvelle synchronisation se produit.

Comparaison des performances du courtier vCPU 6 et 8 dans des conditions de stress

Un site a été configuré avec 50 travailleurs RDS et 5075 VDA VDI. Chaque travailleur RDS est capable de prendre en charge 2500 utilisateurs simulés. Un taux de lancement de 20 utilisateurs par seconde a été fixé. Différents nombres de demandes publiées ont été ajoutés au site.

Pour les travailleurs RDS, 100 000 utilisateurs ont été lancés, pour VDI 5075.

Les tests ont été effectués en mode normal et local Host Cache opérationnel (panne).

Dans le système 6 vCPU, il y a très peu d'espace CPU, et un petit nombre d'exceptions (< 10) se sont produites lorsque le nombre d'applications publiées était > 0.

Les mises à jour Windows ont été désactivées par la stratégie de groupe car au cours d'un certain nombre d'exécutions, le processus tiworker.exe (Windows Installer Module) a été trouvé utiliser presque un noyau entier pendant des périodes prolongées. Cela a entraîné un grand nombre d'échecs de lancement, de sorte que les tests ont été réexécutés. Le processeur de courtier est assez ancien, mais le processus tiworker consommera un seul cœur d'un nouveau, affectant le test.

Configuration de l'hyperviseur

- XenServer 7.0
- AMD Opteron 8431 2,4 GHz — 4x6 cœurs
- 128 GO DE RAM
- Mise en cache en lecture activée
- Windows Storage Server 2012R2 avec stockage basé sur SSD

Configuration du courtier

- 2 prises avec 3 cœurs et 2 prises avec 4 cœurs

- 10 Go de RAM
- Windows Server 2016
- Groupe de mise à disposition unique pour chaque type de VDA
- Toutes les applications visibles par l'utilisateur
- XenDesktop 7.12

Configuration StoreFront

- 6 serveurs StoreFront
- Windows Server 2016
- 4 processeurs virtuels
- 10 Go de RAM

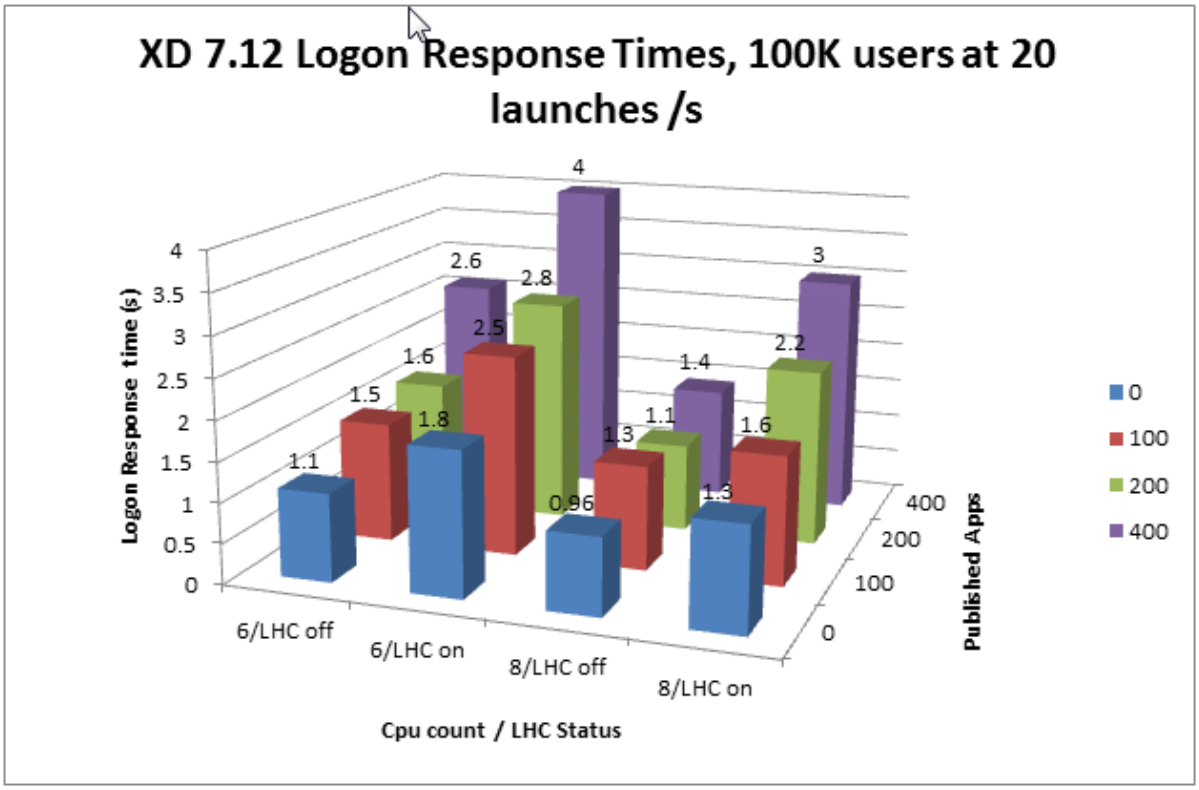
Configuration de NetScaler

- VPX 8000 version 11.063.16

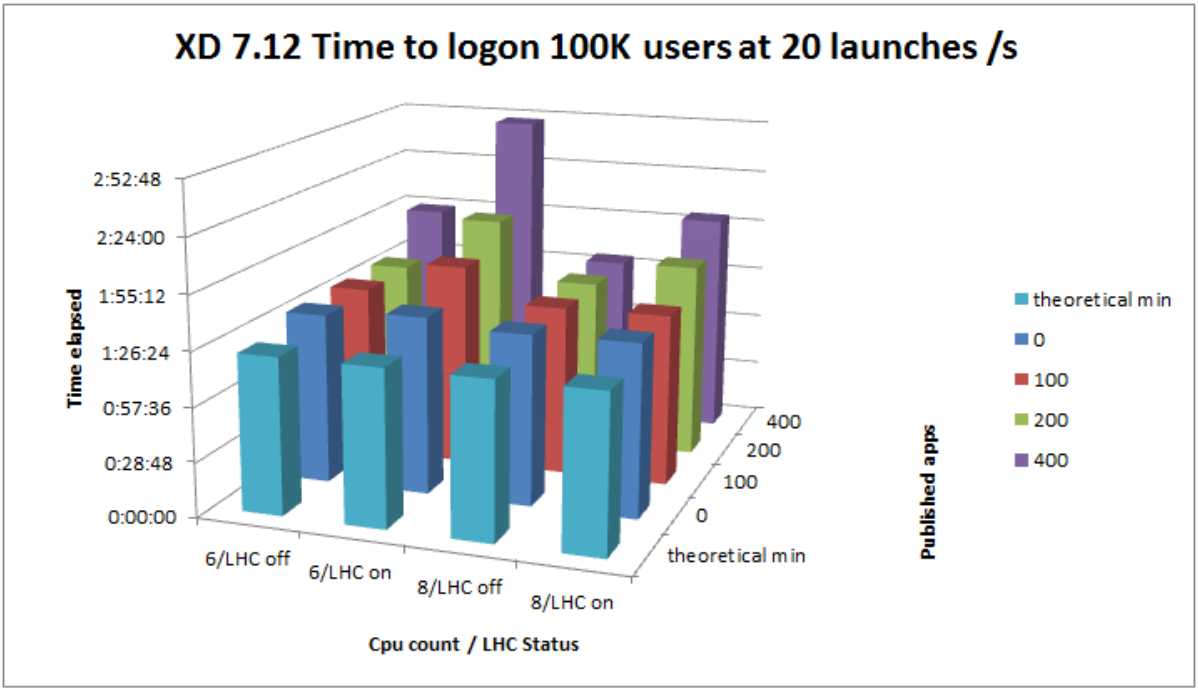
Configuration de SQL Server

- Intel E5-2630 2,3 GHz 2x12 cœurs
- SQL Server 2012
- 64 GO DE RAM

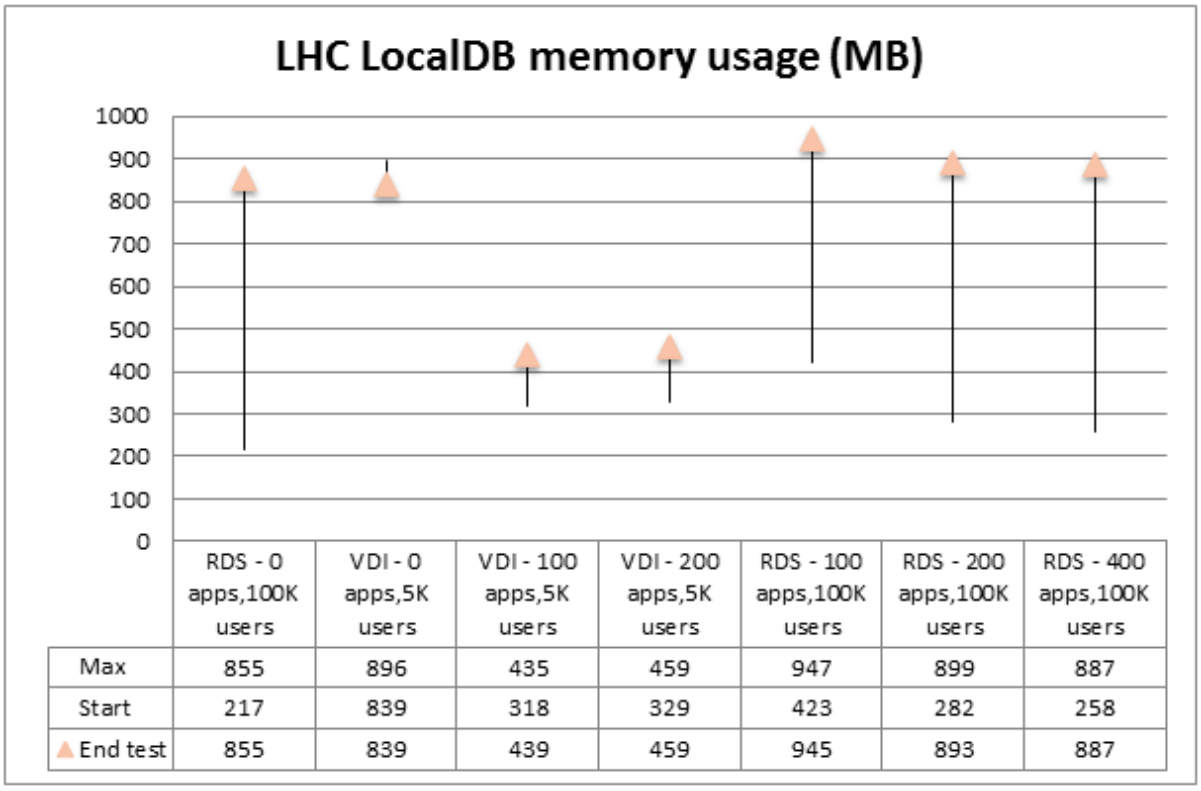
Remarque : Seule la base de données du site a été déconnectée ; les bases de données de surveillance et de configuration étaient toujours accessibles pendant le test. Cela signifie que le service Monitor consomme du CPU pendant les tests.



En général, à mesure que le nombre d'applications augmente, le temps de réponse d'ouverture de session augmente et les temps de réponse d'interruption sont pires que le fonctionnement normal. L'augmentation du nombre de vCPU améliore les temps de réponse. Gardez à l'esprit que le CPU utilisé dans les tests est assez vieux et les CPU plus modernes donneront généralement de meilleures performances.

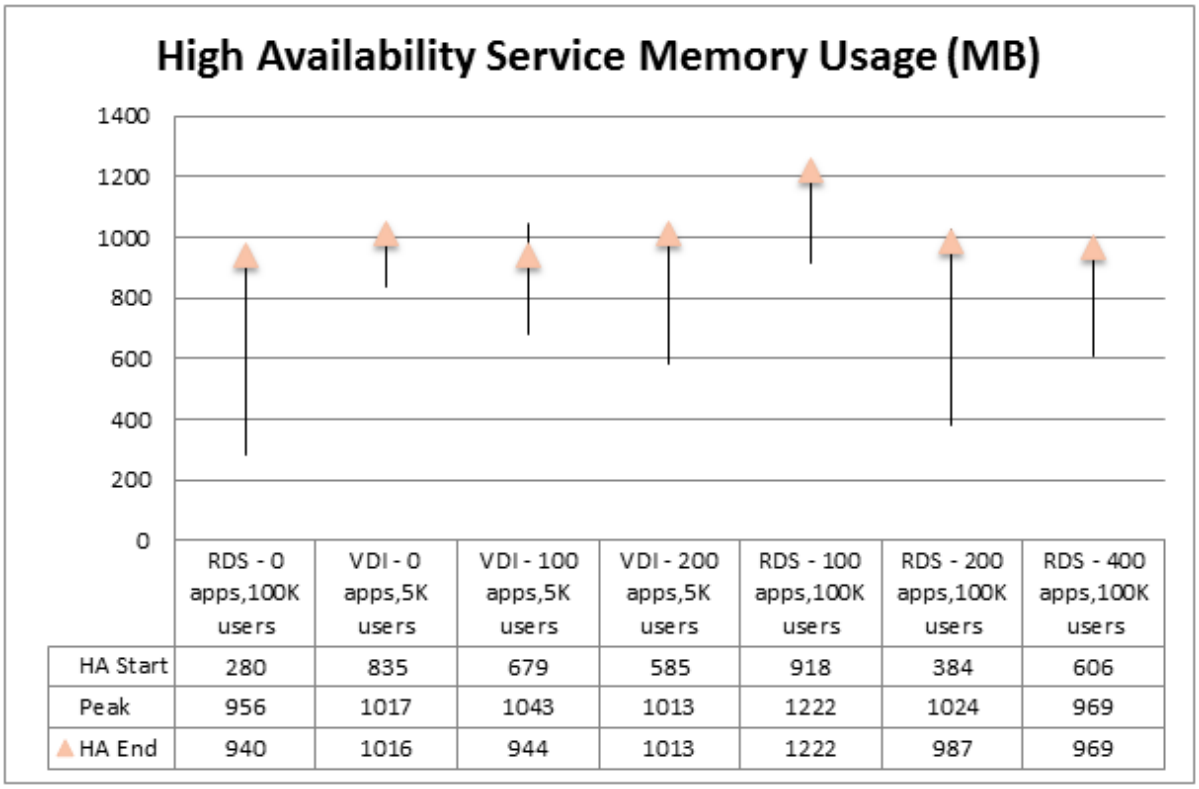


La ligne « min théorique » correspond au temps minimum absolu que prendrait 100 000 utilisateurs pour se connecter si l'environnement était capable de traiter 20 lancements par seconde, ce qui donne 1 heure 23 minutes 20 secondes. Dans ces tests, la ligne 0 applications a géré 1:30:57 dans le cas de 6 vCPU, et 1:30:48 dans le cas de 8 vCPU. Les performances du domaine Active Directory auront un impact sur la rapidité avec laquelle les utilisateurs sont authentifiés.

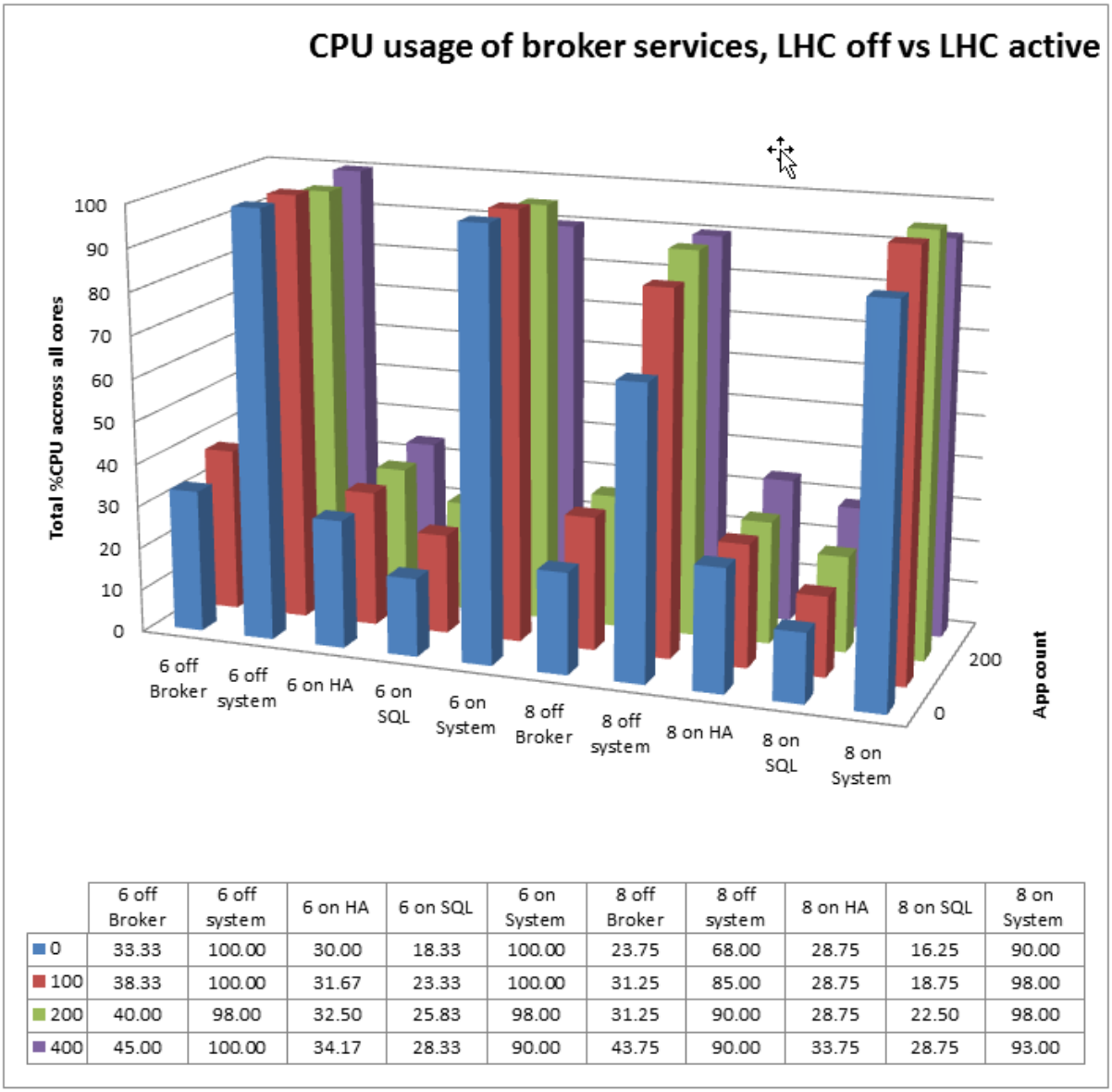


	RDS - 0 apps,100K users	VDI - 0 apps,5K users	VDI - 100 apps,5K users	VDI - 200 apps,5K users	RDS - 100 apps,100K users	RDS - 200 apps,100K users	RDS - 400 apps,100K users
Max	855	896	435	459	947	899	887
Start	217	839	318	329	423	282	258
End test	855	839	439	459	945	893	887

Dans des conditions normales, l'utilisation de la mémoire LocalDB augmente pendant le fonctionnement et s'accroche à cette mémoire à moins qu'il n'y ait une pression sur le système ; plus les utilisateurs sont traités, plus la mémoire utilisée est grande, jusqu'à la limite de 1 Go. Dans le premier test VDI, LocalDB n'avait pas libéré de mémoire de l'exécution RDS précédente. Pour les tests VDI suivants, le courtier a été redémarré avant le test et moins de mémoire a été utilisée.



	RDS - 0 apps,100K users	VDI - 0 apps,5K users	VDI - 100 apps,5K users	VDI - 200 apps,5K users	RDS - 100 apps,100K users	RDS - 200 apps,100K users	RDS - 400 apps,100K users
HA Start	280	835	679	585	918	384	606
Peak	956	1017	1043	1013	1222	1024	969
HA End	940	1016	944	1013	1222	987	969



	6 off Broker	6 off system	6 on HA	6 on SQL	6 on System	8 off Broker	8 off system	8 on HA	8 on SQL	8 on System
0	33.33	100.00	30.00	18.33	100.00	23.75	68.00	28.75	16.25	90.00
100	38.33	100.00	31.67	23.33	100.00	31.25	85.00	28.75	18.75	98.00
200	40.00	98.00	32.50	25.83	98.00	31.25	90.00	28.75	22.50	98.00
400	45.00	100.00	34.17	28.33	90.00	43.75	90.00	33.75	28.75	93.00

Remarque : les valeurs ont été normalisées à la CPU totale du système, donc 33,33% sont deux cœurs sur six, 30% sont 2-1/2 sur la configuration de 8 vCPU.

Le terme « désactivé » fait référence au fonctionnement normal du site ; « activé » signifie que le cache d'hôte local est actif.

Le taux de lancement de la demande de 20 utilisateurs par seconde est assez exigeant pour le courtier, même en fonctionnement normal. En fonctionnement normal, le système 6 vCPU n'a pas de marge de manœuvre ; le processeur du courtier augmente à mesure que le nombre d'applications publiées augmente, ce qui entraîne des temps de réponse plus lents. Lorsque le cache hôte local est actif, le service de courtier secondaire doit rivaliser avec LocalDB (SQL) pour la ressource CPU, ce qui donne des temps de réponse plus mauvais que le fonctionnement normal.

Dans le système 8 vCPU, il y a une certaine marge de manœuvre et le LocalDB va augmenter, mais

dans cet environnement, il a atteint un sommet de 2 à 1/2 cœurs, bien qu'il y ait une petite quantité de CPU encore disponible.

Pendant le fonctionnement normal, LocalDB ne consomme pas de CPU à moins qu'une synchronisation n'ait lieu.

En cas de panne, le courtier principal utilisera pratiquement aucun processeur.

Taille de la base de données

Pour la configuration VDI 5075, le LocalDB était d'environ 40 Mo, pour les 100 000 RDS, cela variait entre 100 et 300 Mo, selon le nombre d'applications et d'ouvertures de session. Comme une copie de la base de données est effectuée avant le début d'une nouvelle importation, autorisez 1 Go d'espace pour LocalDB.

Résumé

Lors d'une panne de base de données de site, le cache hôte local prend en charge un plus grand nombre de ressources et de conditions que la location de connexion, mais nécessite plus de CPU et de mémoire lors de l'exploitation.

Dans plusieurs sites de courtier, n'importe quel courtier peut être choisi comme courtier de panne, et donc tous doivent disposer de ressources suffisantes pour faire face en mode panne. Aucune évaluation des ressources de courtier n'est faite, donc dans un site avec des courtiers moins puissants et plus puissants, il est possible que le courtier le moins puissant soit élu en cas de panne.

La disposition des noyaux et des douilles doit être considérée dans le cadre de la conception des courtiers.

Le nombre d'applications publiées aura un effet sur les temps de réponse d'ouverture de session et le débit maximal d'ouverture de session.

Les courtiers avec une ressource CPU insuffisante peuvent entraîner des lancements échoués.

Deux cœurs supplémentaires et 2 Go de RAM constituent un bon point de départ pour tester les performances en mode d'interruption du cache hôte local par rapport à la location de connexion.

1 Go d'espace disque sera suffisant pour la base de données LocalDB.

Un courtier surchargé entraînera des connexions échouées.

Cet article a été écrit par Joe Deller.

Équilibrage de charge du serveur d'impression universel Citrix dans XenApp et XenDesktop 7.9

January 8, 2020

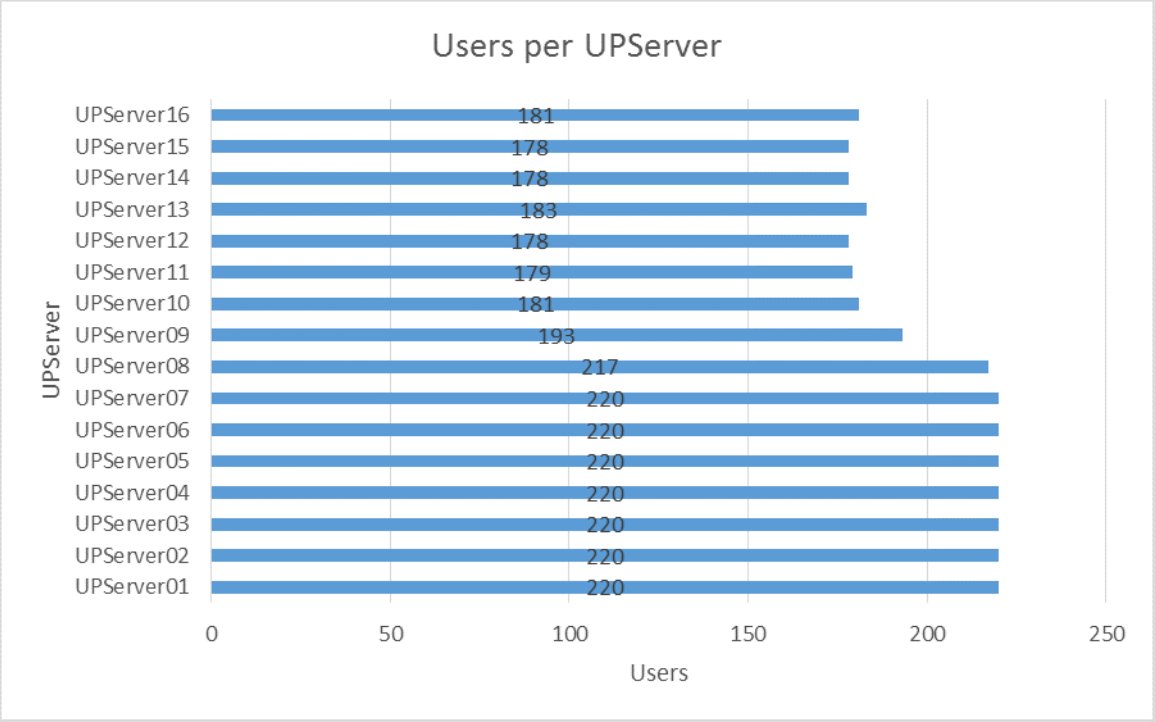
Comment nous avons testé

Tous les scénarios de test ont été réalisés dans le monde réel et l'impression finale a été la seule composante simulée. Les systèmes de test comprenaient des machines virtuelles XenServer, Windows 2012R2 pour l'infrastructure (DDC, StoreFront et Universal Print Server) et des systèmes VDA XenApp, Windows 10 pour les systèmes VDA XenDesktop et Windows 8.1 pour ICA lancé via Citrix Receiver. Chaque lanceur ICA était connecté à 10 imprimantes sans chevauchement d'imprimantes entre les lanceurs ICA, et des scripts personnalisés ont été utilisés afin que chaque session VDA XenApp soit dotée d'une imprimante aléatoire à utiliser. Les scripts personnalisés contrôlaient également l'impression à l'intérieur de chaque session en utilisant AutoIt pour effectuer des actions d'impression identiques. Enfin, nous avons utilisé un outil développé en interne pour coordonner les lancements de session ICA et collecter des données perfmon pour les tests.

Taille de l'équilibrage de charge du serveur d'impression universel

Comme tous les autres composants de votre environnement, le dimensionnement est essentiel pour que l'équilibrage de charge Universal Print Server fonctionne de manière optimale. Puisque l'impression d'un document volumineux est subjective selon vos besoins, cet article se concentre principalement sur le taux d'impression et utilise ce que nous considérons comme un travail moyen.

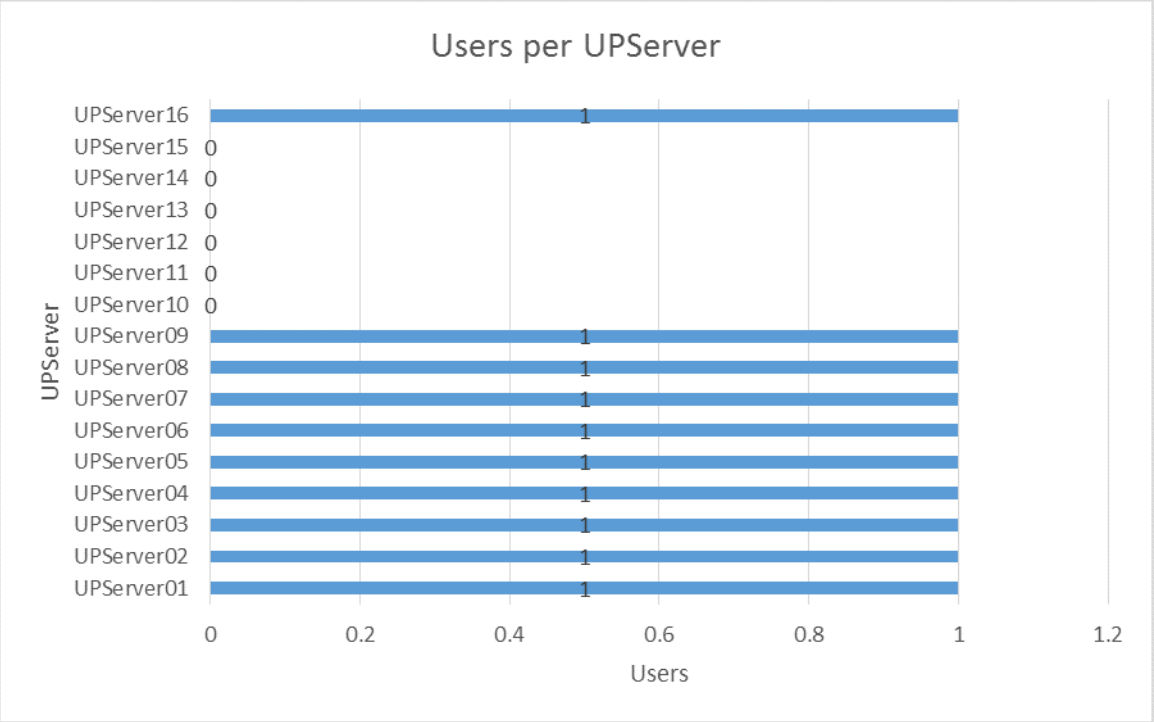
Grâce à des tests internes, il a été constaté que vous ne voulez pas trop ou trop peu d'instances Universal Print Server configurées dans l'équilibrage de charge. Et bien qu'il soit vrai, vous pouvez augmenter l'impression avec des instances de serveur d'impression universel supplémentaires, lorsque vous parlez de distribution d'imprimantes, ce n'est pas nécessairement le cas. En particulier, est le cas où vous avez trop d'instances de serveur d'impression universel configurées. Dans ce cas, il y a une inclinaison définitive des utilisateurs vers les premières instances du serveur d'impression universel disponibles.



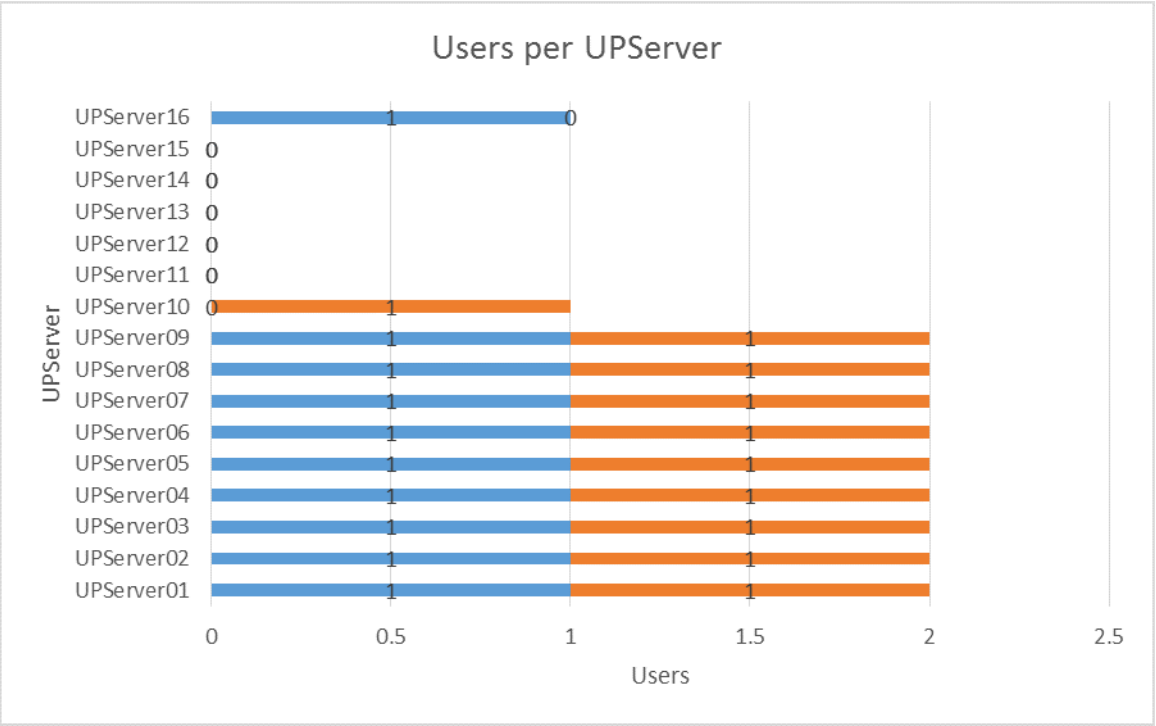
Le graphique fait référence à un scénario de test de 3 500 utilisateurs sur 48 serveurs XenApp utilisant 16 instances de serveur d'impression universel. Comme on peut le voir plus haut, les 8 premières instances Universal Print Server ont pris la majorité des connexions et il n'y avait pas de distribution uniforme des connexions. Ce scénario supposait également un faible taux d'impression dont nous discuterons plus tard.

Pour comprendre pourquoi cela se produit, nous devons examiner comment le mécanisme d'équilibrage de charge choisit une instance Universal Print Server. Disons que nous avons 16 instances Universal Print Server (numérotées 1-16) en équilibrage de charge et un seul serveur XenApp avec 10 utilisateurs maximum (un peu exagéré, mais vous verrez pourquoi). Supposons également que les instances du serveur d'impression universel équilibré de charge sont dans l'ordre numérique dans le serveur d'impression universel pour la stratégie d'équilibrage de charge.

Lorsqu'un utilisateur ouvre une session et crée une session (dans XenApp), l'instance Universal Print Server que l'utilisateur reçoit est aléatoire. Il peut s'agir de n'importe quelle instance Universal Print Server disponible et aucune préférence n'est donnée à aucun serveur. Dans cet exemple, disons qu'ils ont reçu le serveur 16 pour leurs connexions. Une fois que ce premier utilisateur est connecté et que sa création de session est terminée, un autre utilisateur se connecte. Cet utilisateur utilisera la première instance Universal Print Server dans la liste de la stratégie, dans ce cas le serveur 1. Un autre utilisateur se connecte et utilise maintenant le serveur 2. Poursuivre cette tendance fournira le chargement du serveur vu ci-dessous. Lorsque les 10 utilisateurs sont connectés, les instances 1 à 9 et 16 du serveur d'impression universel auront des connexions alors que les serveurs restants ne le font pas.



Nous ajoutons maintenant un serveur XenApp supplémentaire au mix, avec le même maximum de 10 utilisateurs. Ce serveur suit la même procédure que l'exemple précédent, à l'exception du fait que le premier utilisateur reçoit aléatoirement le serveur 4 au lieu du serveur 16. Dans ce cas, le même processus pour chaque connexion suivante se produit comme avant, sauf qu'il ignore sur le serveur 4 car il a une connexion établie actuellement. Dans ce cas, les serveurs 1-10 auront des connexions. Vous pouvez voir les utilisateurs supplémentaires en orange dans le graphique ci-dessous, et observer comment il équilibre.



Continuez à augmenter le nombre de serveurs et l'inclinaison qui se produit peut être clairement observée. En pratique, vous devez disposer d'une quantité d'hôtes XenApp équivalente ou multiple de vos instances Universal Print Server. Il est également conseillé de conserver le nombre de sessions utilisateur en tant que multiples des instances du serveur d'impression universel que vous prévoyez d'utiliser pour un chargement plus optimal. En regardant le scénario ci-dessus de ce point de vue, avec 2 serveurs XenApp et 16 instances Universal Print Server, nous voyons que notre charge utilisateur devrait être d'au moins 16 utilisateurs par serveur XenApp. Une autre façon d'examiner le même problème est que si nous ne prenons en charge que 10 utilisateurs par serveur XenApp, alors pas plus de 10 instances Universal Print Server sont nécessaires. Cela permettra d'assurer un chargement plus équilibré et d'utiliser plus efficacement les ressources disponibles.

Ce qui précède est un regard trop simpliste sur une configuration traitant de l'équilibrage strictement de la connexion utilisateur. Des configurations plus complexes avec beaucoup plus d'utilisateurs par serveur seraient la configuration probable observée. Avec l'augmentation du nombre d'utilisateurs, le taux d'impression mentionné précédemment joue un rôle plus important dans le dimensionnement du serveur d'impression universel. Nous vous recommandons d'utiliser la formule ci-dessous pour déterminer les instances de serveur d'impression universel requises pour votre environnement. Cela vous permettra de déterminer le nombre d'instances de serveur d'impression universel dont vous avez besoin pour l'équilibrage de charge en fonction de votre taux d'impression requis. Dans le but de simplifier le dimensionnement, cette formule peut être utilisée pour fournir des conseils pour une configuration plus idéale afin de fournir un taux d'impression requis. En général, vous serez le plus intéressé par la résolution pour N pour déterminer votre propre nombre de serveurs d'impression.


```
V\*P/N \< J
```

Où :

V = Nombre de VDA qui utilisent LB

P = Nombre moyen de travaux d'impression réseau actifs par minute par VDA

N = Nombre de serveurs d'impression équilibrés de charge

J = Nombre maximal de tâches par minute sur Universal Print Server

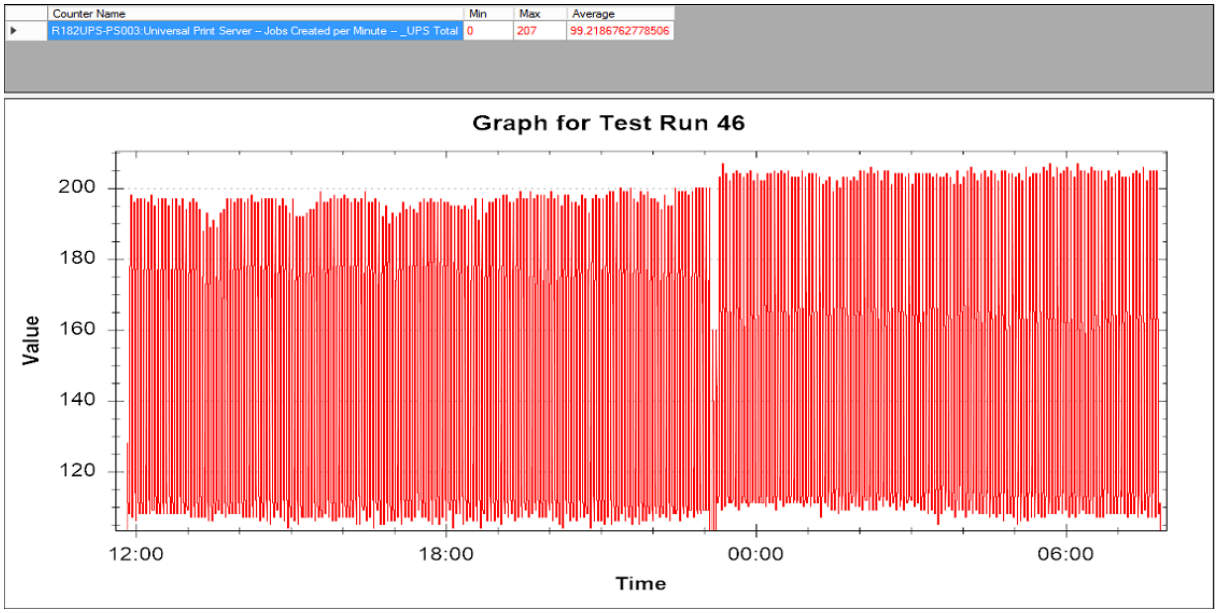
P peut être observé sur les VDA 7.8 et plus récents en regardant les compteurs perfmon Universal Print Client existants sur le VDA, plus précisément en surveillant la moyenne des tâches créées par minute compteur pour les imprimantes réseau pendant une journée de travail normale sur un VDA avec la stratégie Universal Print Server activée et le réseau mappées en sessions.

J doit être un nombre compris entre 50 et 100, en fonction des performances matérielles des serveurs d'impression et de la taille des documents à imprimer.

La formule ci-dessus est généralisée et dépend fortement des exigences de votre environnement. Il est important de bien comprendre les exigences d'impression de votre environnement avant d'implémenter l'équilibrage de charge Universal Print Server.

Tests 100 travaux par minute (JPM)

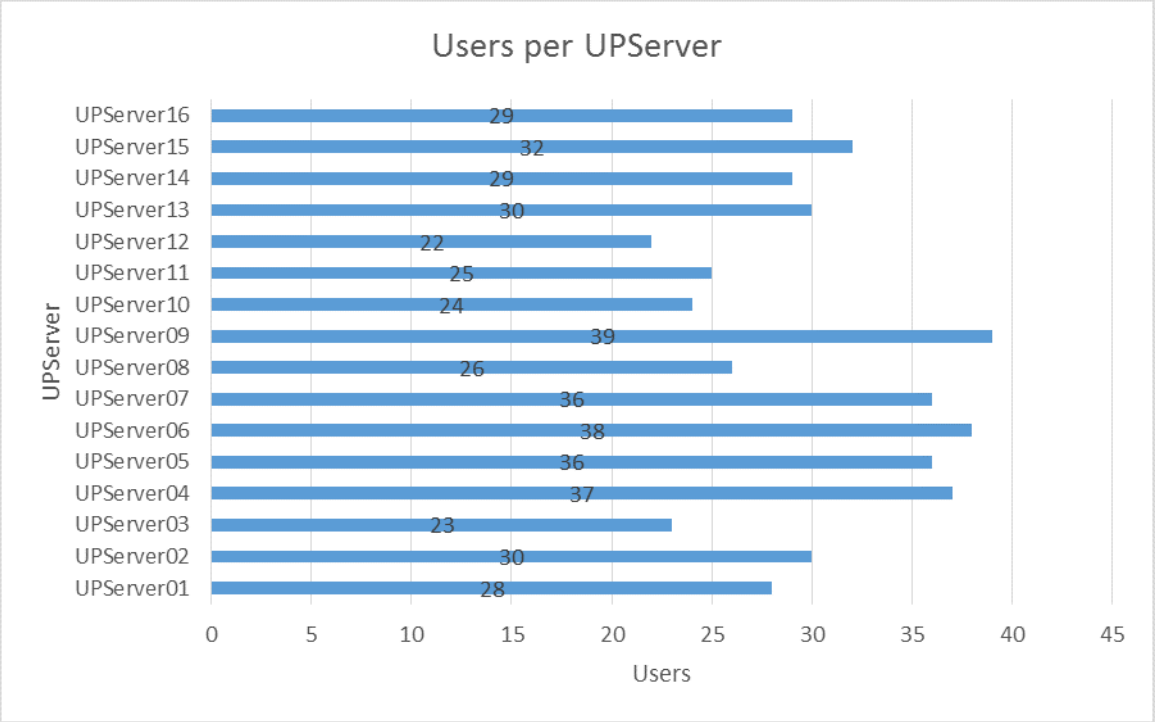
L'une des améliorations les plus importantes apportées au nouvel équilibrage de charge Universal Print Server est l'augmentation des tâches d'impression simultanées par minute. Le seuil de fréquence d'impression doublé de 100 tâches par minute permet désormais une densité encore plus grande sur une instance de serveur d'impression universel individuelle. La répartition entre plusieurs instances de serveur d'impression universel à charge équilibrée rend cette augmentation plus efficace. Voici la sortie perfmon du compteur Jobs Created per Minute (celui référencé dans la formule) qui se situe en moyenne à ~ 100 jobs par minute pour un cycle de test de 18 heures +.



Randomisation VDI

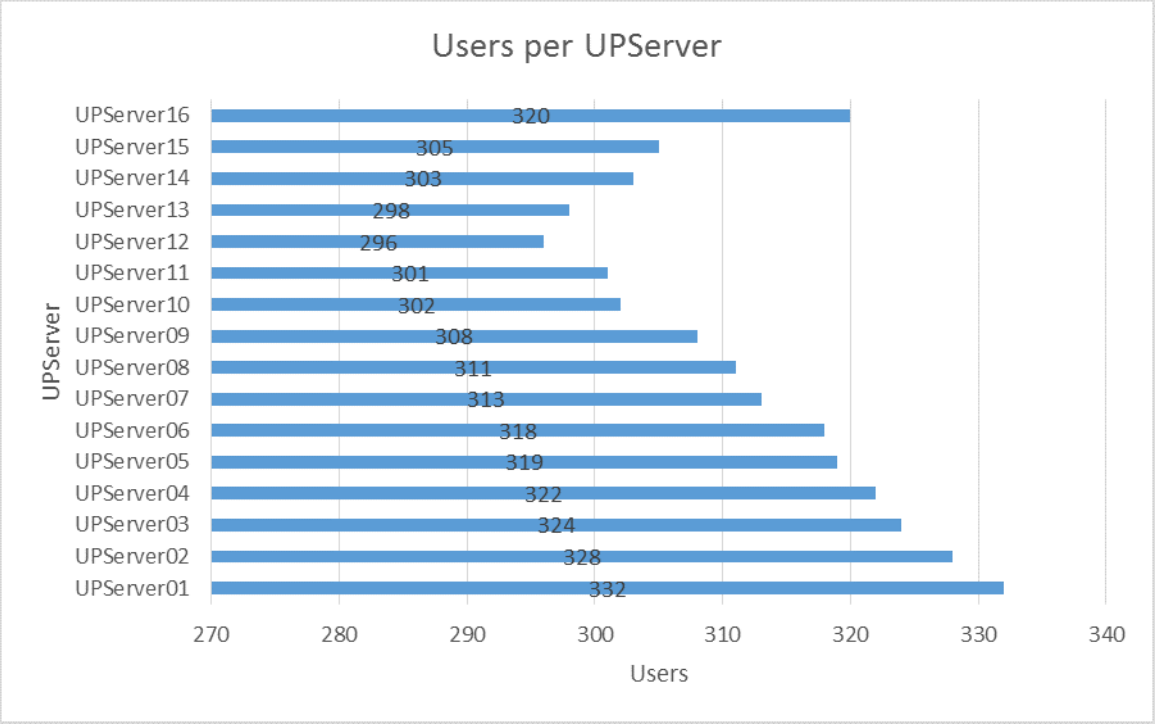
La méthode d'équilibrage de charge utilisée dans un environnement VDI est une implémentation de la fonction de randomisation uniquement. Comme indiqué précédemment, le processus d'équilibrage de charge se produit uniquement sur le VDA, randomisant la première connexion, puis les connexions suivantes sont équilibrées sur la liste des instances Universal Print Server. Comme une implémentation VDI a un seul utilisateur par VDA, la fonction de randomisation est la seule qui s'applique.

Pour s'assurer que la randomisation fonctionne, un test XenDesktop 500 utilisateurs a été exécuté à l'aide de 16 instances Universal Print Server. Cela correspond à environ 31 sessions par instance Universal Print Server (dans un monde parfaitement équilibré de charge), ce qui permet de déterminer clairement l'efficacité de la randomisation. Voici les connexions d'imprimante créées à la suite de ce test. Il est facile d'observer que les connexions sont attribuées de façon aléatoire à une instance de serveur d'impression universel.



5000 tests utilisateur

XenApp est l'endroit où le plus grand avantage de l'équilibrage de charge Universal Print Server sera réalisé en raison de la densité des serveurs XenApp eux-mêmes. Afin de déterminer dans quelle mesure l'équilibrage de charge Universal Print Server évolue dans un environnement plus grand nombre d'utilisateurs, il a été décidé qu'un essai de 5 000 utilisateurs était suffisamment important pour vérifier l'équilibrage de charge.

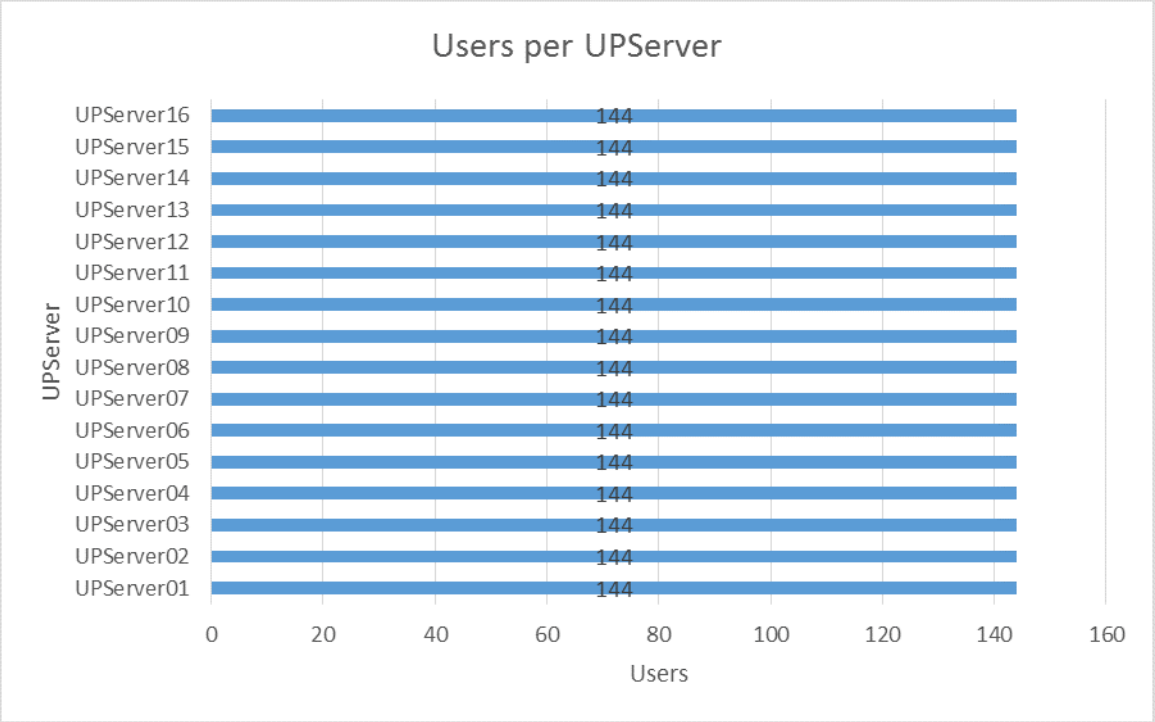


Ce qui précède est le résultat du test utilisateur de 5 000, utilisant 48 serveurs XenApp avec 16 instances de serveur d'impression universel. Ce nombre d'utilisateurs correspond à environ 100 utilisateurs par serveur XenApp, ou environ 6,5 utilisateurs par instance de serveur d'impression universel par serveur XenApp. Les résultats montrent l'inclinaison qui a été identifiée plus tôt, car il ne s'agit pas d'un test conçu de façon optimale. En fin de compte, il s'agit d'une démonstration de la fonction d'équilibrage de charge.

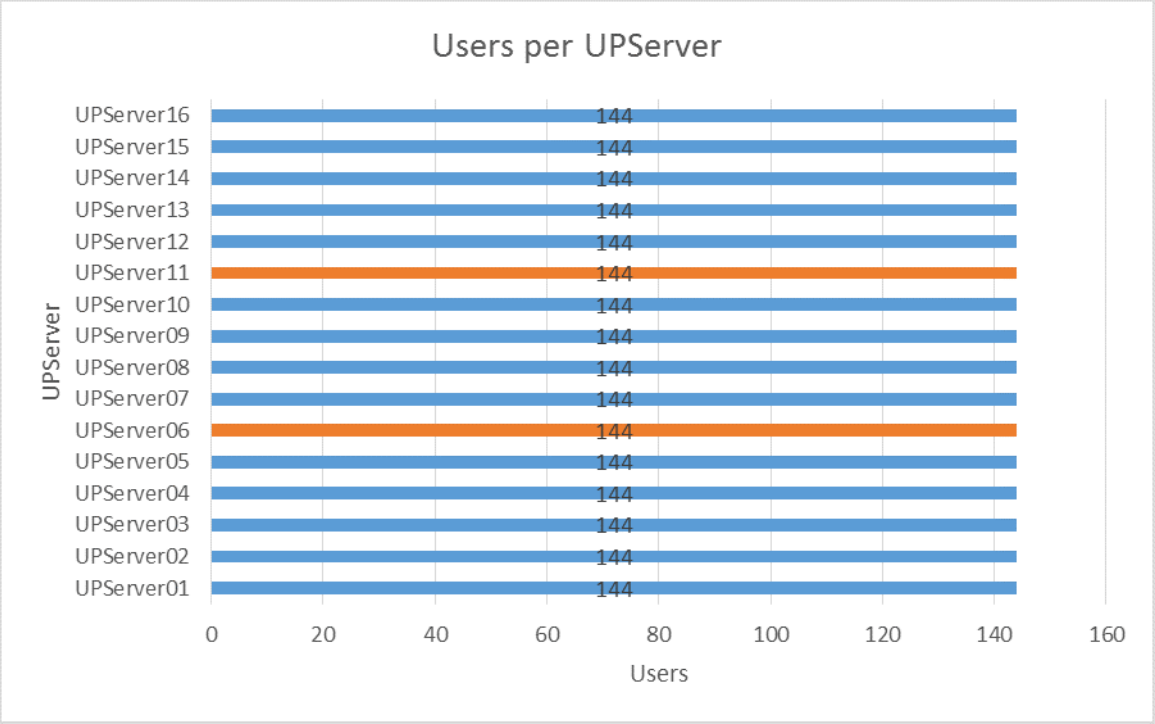
Basculement sur incident de l'équilibrage de charge du serveur d'impression universel

Par défaut, une instance de serveur d'impression universel ne sera pas signalée comme ayant échoué pour les années 180s MINIMUM et peut prendre aussi longtemps que 360s pour être considérée comme ayant échoué. Ce délai d'expiration est important à comprendre car cela provoque le basculement ne se produit pas à l'instant d'une défaillance d'instance du serveur d'impression universel. Il sera temps pour l'instance du serveur d'impression universel de tenter de récupérer avant que le basculement ne se produise. Si un basculement plus immédiat est nécessaire, des modifications devront être apportées en fonction de vos besoins environnementaux. Ces modifications peuvent être effectuées via la stratégie Citrix, ainsi que par l'intermédiaire de deux clés de Registre.

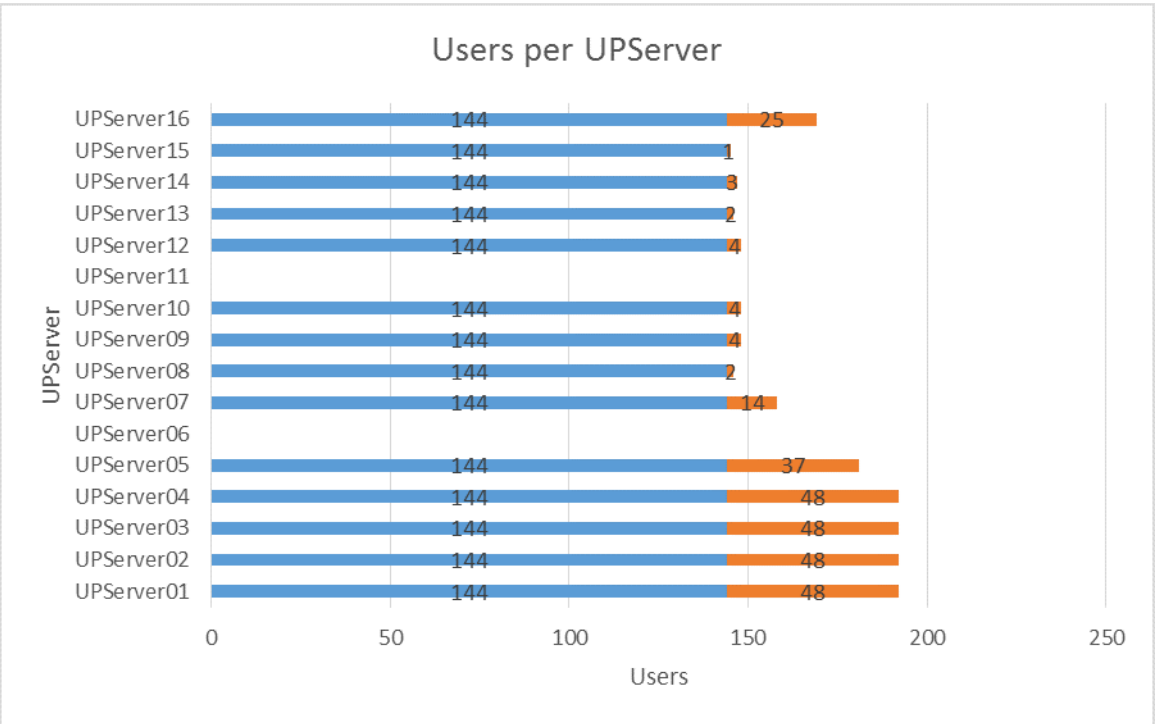
Vous trouverez ci-dessous une démonstration du basculement en action. 2 304 utilisateurs sur 48 serveurs XenApp sur 16 instances de serveur d'impression universel ont été utilisés pour illustrer l'équilibrage de charge initial et le ou les basculements ultérieurs. Les valeurs ci-dessus ont été sélectionnées afin qu'il fonctionne à 3 utilisateurs par instance Universal Print Server par serveur XenApp, idéalement.



Toutes les instances Universal Print Server sont chargées également et tous les utilisateurs sont connectés. Les instances de serveur d'impression universel UpServer06 et UPServer11 sont soumises à un arrêt forcé (en raison de l'utilisation de PING pour déterminer l'état de disponibilité d'une instance de serveur d'impression universel) au niveau de l'hyperviseur afin qu'elles soient considérées comme ayant complètement échoué. Ci-dessous, les connexions serveur concernées sont mises en surbrillance orange. Ensuite, les connexions au serveur échouées en orange sont redistribuées aux instances du serveur d'impression universel restantes encore en place.

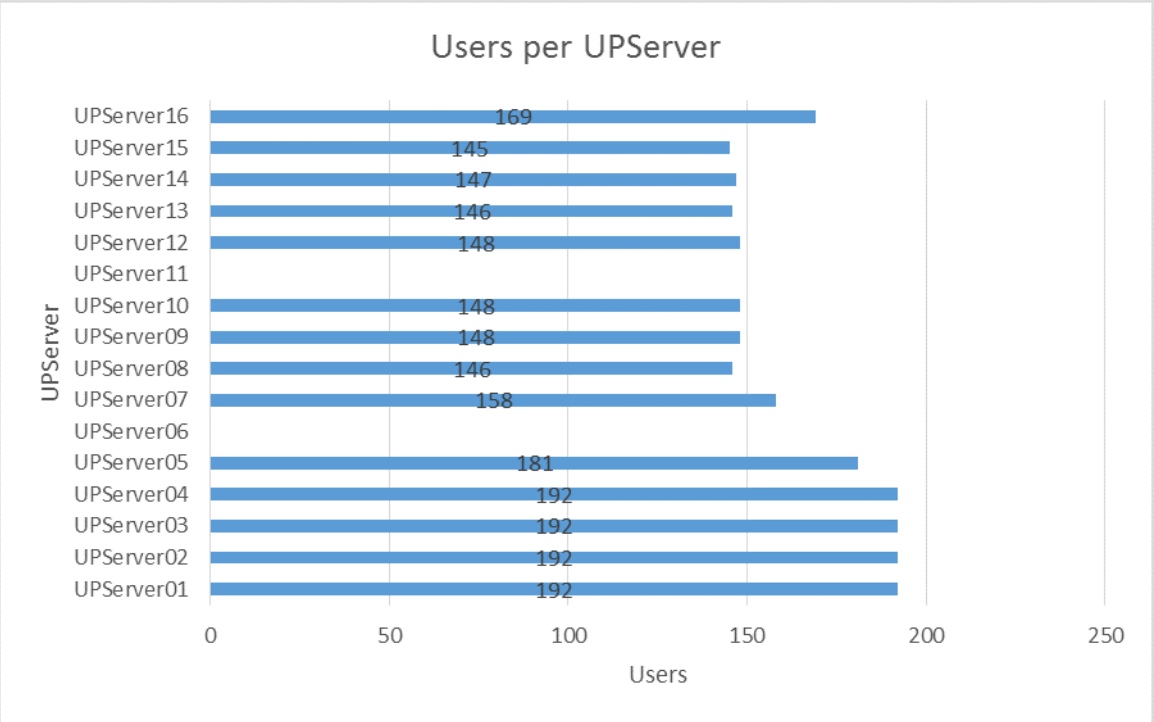


De nouvelles connexions sont ensuite établies avec les serveurs existants qui sont toujours disponibles. Ci-dessous, vous pouvez voir comment les connexions précédemment échouées sont redistribuées sur les serveurs existants.

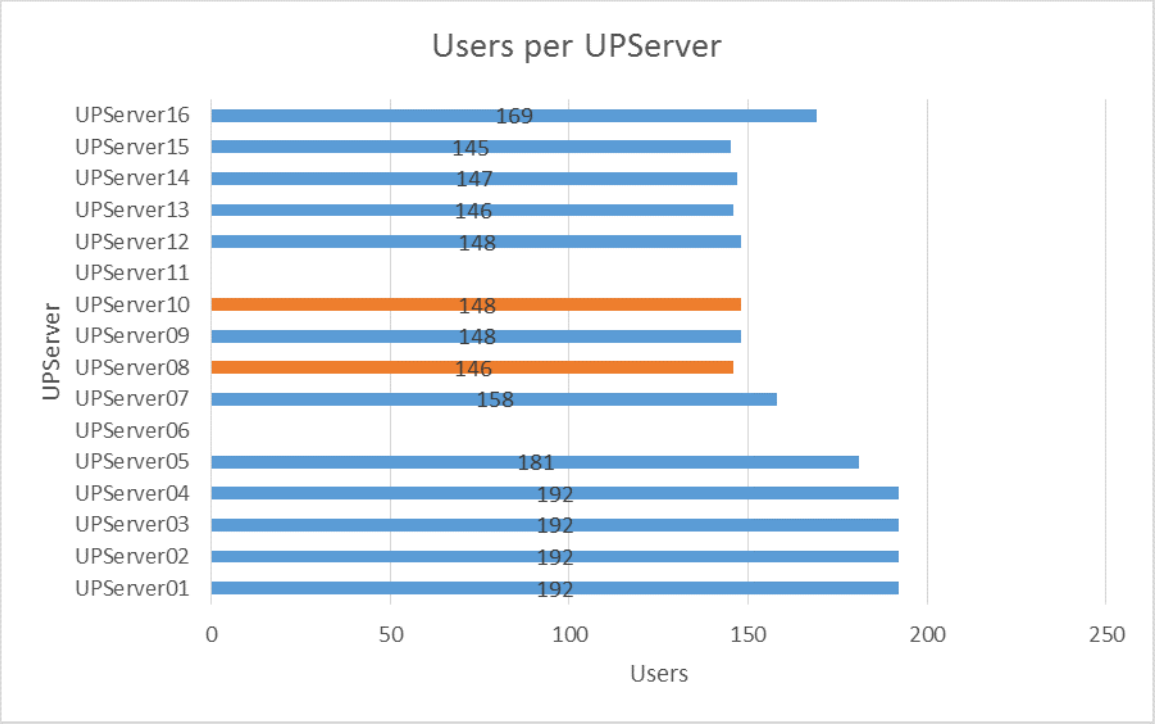


Comme cela a été mentionné précédemment, la connexion existante n'équilibrent pas dynamiquement la charge. L'équilibrage de charge se produit uniquement lors de l'ouverture de session utilisa-

teur. Par conséquent, lorsque les instances du serveur d'impression universel en échec redeviennent disponibles, aucun rééquilibrage ou retour arrière ne se produira. Cela peut être vu ci-dessous où les instances du serveur d'impression universel qui ont échoué sont remises en ligne, mais ne prennent aucune connexion existante.



Pour illustrer que ces instances de serveur d'impression universel sont à nouveau disponibles et acceptent les connexions, il est nécessaire d'ouvrir une session d'utilisateurs supplémentaires ou de forcer une défaillance d'autres instances du serveur d'impression universel. Ci-dessous, les instances Universal Print Server UpServer08 et UpServer10 ont été soumises à une défaillance forcée et leurs connexions respectives sont surlignées en orange.

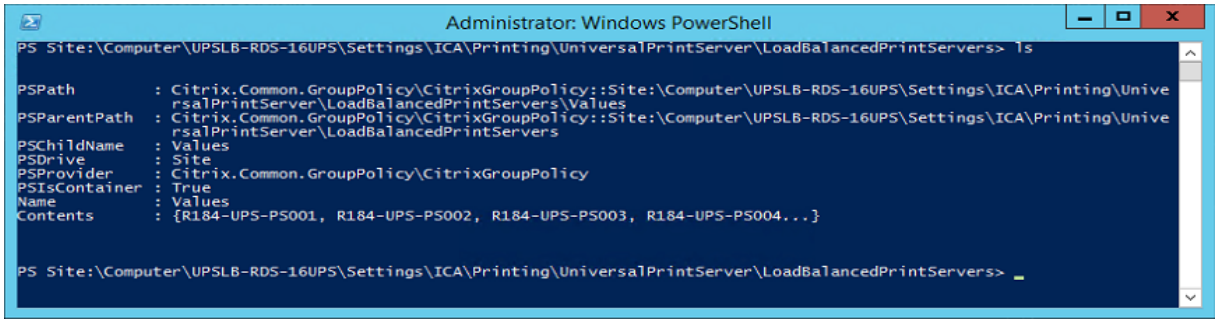


Avec l'échec, il peut être vu en conséquence que les connexions sont migrées vers d'autres serveurs. Dans ce cas, ils seront migrés vers les deux serveurs qui ont échoué précédemment, maintenant disponibles pour reprendre les connexions. Comme ces serveurs sont les moins chargés (pas de charge), ils prennent la majeure partie des connexions.

Ajout de plusieurs serveurs d'impression

Plusieurs instances de serveur d'impression universel peuvent être ajoutées à la stratégie d'équilibrage de charge de deux manières : via l'interface graphique de stratégie Citrix ou via les applets de commande PowerShell. L'interface graphique de stratégie Citrix est explicite dans son utilisation. Voici une méthode d'utilisation de PowerShell pour ajouter plus rapidement plusieurs instances de serveur d'impression universel à la stratégie d'équilibrage de charge.

1. Add-PSSnapin Citrix.Common.GroupPolicy
2. New-PSDrive –PSProvider CitrixGroupPolicy –Name Site –Root \ -Controller localhost
3. Site CD : Ordinateur
4. CD à la stratégie que vous souhaitez modifier (le nom de la stratégie qui contient votre stratégie UPSLB)
5. CD Settings\ICA\Printing\UniversalPrintServer\LoadBalancedPrintServers
6. Utiliser New-Item pour ajouter de nouvelles imprimantes à la liste



Il y a cependant quelques mises en garde avec l'utilisation de cette méthode. Tout d'abord, assurez-vous que vous entrez les informations correctement. Vous pouvez ajouter manuellement quelques imprimantes à la stratégie et afficher la façon dont elles sont présentées via l'écran PowerShell pour vous assurer que vous les ajoutez correctement. Deuxièmement, puisque vous évitez l'interface utilisateur de stratégie, il n'y a pas de validation des serveurs d'impression effectuée.

Compteurs Universal Print Server

Comme mentionné dans la section de dimensionnement, il existe de nouveaux compteurs perfmon qui peuvent être utilisés pour déterminer les informations sur les conditions actuelles d'impression. Des compteurs uniques existent à la fois sur l'instance Universal Print Server et sur les systèmes XenApp/XenDesktop.

Les compteurs pertinents pour l'instance globale du serveur d'impression universel seront situés sur l'instance du serveur d'impression universel correspondant, tels que le compteur de tâches créées par minute précédemment mentionné (ces compteurs sont uniquement pour cette instance de serveur d'impression universel et ne sont pas cumulatifs sur plusieurs). Des compteurs pertinents pour l'équilibrage de charge Universal Print Server existent sur chaque système XenApp/XenDesktop (l'équilibrage de charge se produit au niveau du VDA individuel), tels que le compteur Connexions actuelles.

Les compteurs spécifiques UPClient (composant VDA) peuvent être configurés pour capturer des données pour une instance Universal Print Server spécifique, toutes les instances Universal Print Server ou en tant que total pour toutes les instances Universal Print Server sur un VDA. Ces compteurs peuvent être vus directement via perfmon ou peuvent être scriptés via PowerShell. Les compteurs suivants seront disponibles sous la section Citrix Printing Load Balancing de perfmon. Ces compteurs peuvent également être sélectionnés en sélectionnant un total (_loadbalancers_total) pour le VDA ou en sélectionnant une instance de serveur d'impression universel (nom d'instance du serveur d'impression universel) disponible sur ce VDA spécifique.

Compteur de connexions d'imprimante actives :
Performance\Citrix Printing Load Balancer (SELECTION)\Active Printer Connections

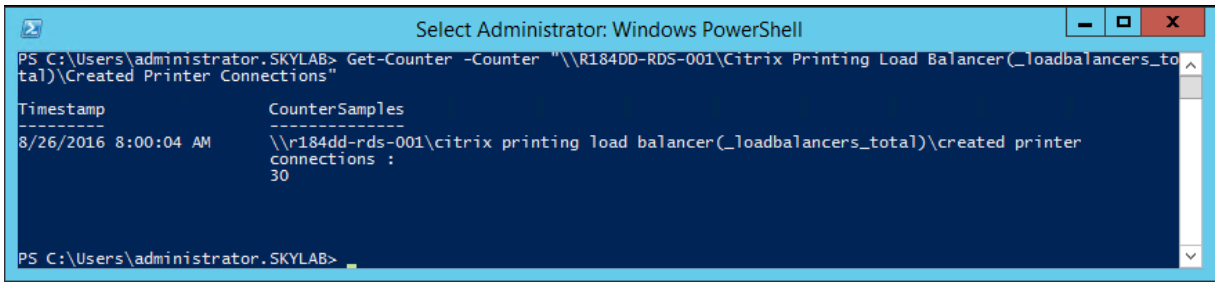
Compteur de connexions d'imprimante créées :
Performance\Citrix Printing Load Balancer (SELECTION)\Created Printer Connections

Compteur de connexions d'imprimante supprimées :
Performance\Citrix Printing Load Balancer (SELECTION)\Deleted Printer Connections

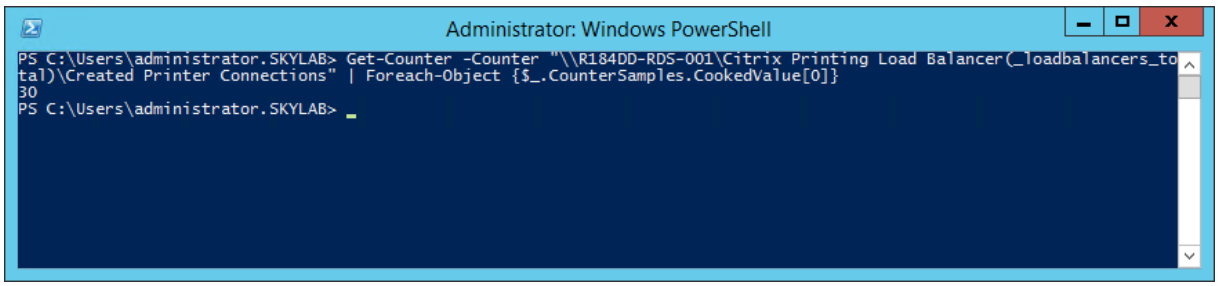
Comme il s'agit de compteurs perfmon standard, l'applet de commande Get-Counter intégrée à PowerShell peut être utilisée comme suit pour obtenir des informations à partir d'un VDA spécifique.

```
Get-Counter -Counter \\\\\VDAName\\Citrix Printing Load Balancer(SELECTION)
\\COUNTER
```

La commande ci-dessus récupère les informations COUNTER (Active/Created/Deleted Printer Connections) souhaitées à partir du VDAName souhaité (Nom, FQDN ou adresse IP du VDA) pour le SELECTION (nom de l'instance du serveur d'impression universel ou_loadbalancers_total). Cela fournira une liste complète de l'objet compteur.



Si vous n'êtes concerné que par la valeur réelle, vous devrez diriger cette commande dans une autre commande pour récupérer la valeur cuite (ou simplement la valeur des connexions). Pour ce faire, nous allons ajouter cette commande à la fin de la précédente :
| Foreach-Object {$_.CounterSamples.CookedValue [0]}



Environnement de test

L'environnement de test consistait en trois ensembles distincts de matériels regroupés exécutant XenServer 6.2 et 6.5. Il existait un seul pool XenServer 6.2 qui contenait les composants d'infrastructure Citrix (DDC, StoreFront, ICA Launchers, collection de métriques) et deux pools 6.5 contenant les instances Universal Print Server et les VDA de test RDS. Deux référentiels de stockage centralisés distincts ont été utilisés pour les tests (un pour chaque version de pool) et toutes les machines virtuelles de test y étaient situées. Tous les logiciels utilisés étaient les plus à jour au moment des essais effectués. Tous les essais ont été effectués avec les mêmes versions du conducteur et du

conducteur pour s'assurer que les résultats sont uniformes. D'autres conducteurs ont été testés ; les résultats individuels varient en fonction du conducteur utilisé.

Serveurs physiques XenServer 6.2 (x10)

- 2 x Intel Xeon E5620 à 2,40 GHz (4 cœurs HyperThreaded) — 16 processeurs
- 64 Go de mémoire
- Stockage NFS

Serveurs physiques XenServer 6.5 (x25)

- 2 x Intel Xeon E5-2640 à 2,50 GHz (6 cœurs HyperThreaded) — 24 processeurs
- 256 Go de mémoire
- Stockage NFS

VM du serveur d'impression universel

- 16 vCPU (16 socket x 1 core)
- 16 Go de vRAM
- 75 Go de stockage
- Windows Server 2012 R2

RDS VM

- 16 vCPU (16 socket x 1 core)
- 16 Go de vRAM
- 75 Go de stockage
- Windows Server 2012 R2

VM du lanceur ICA

- 2 vCPU (2 socket x 1 cœur)
- 4 Go de vRAM
- 60 Go de stockage
- Windows 8.1 x64 Entreprise

Stratégies Citrix Universal Print Server

ICA\Printing

- Préférence du pilote universel : XPS ; EMF ; PCL5c ; PCL4 ; PS

- Utilisation du pilote d'impression universel — Utiliser l'impression universelle uniquement
- Serveur d'impression universel activé — Activé sans repli sur l'impression à distance native de Windows
- Attendez la création des imprimantes — Activé
- Serveurs d'impression universels pour l'équilibrage de charge — Liste des serveurs d'impression

Universal Print Server et les machines virtuelles RDS/VDA ont été conservées dans les mêmes serveurs physiques groupés matériels afin de s'assurer que les tests étaient effectués sur des configurations matérielles cohérentes. Les serveurs DDC et StoreFront n'ont pas été inclus dans ce qui précède car ils n'ont pas d'impact sur l'équilibrage de charge du serveur d'impression universel, à l'exception de la propagation des stratégies à partir du DDC. Des stratégies minimales ont été utilisées dans le domaine, et le site XenDesktop/XenApp était une installation par défaut avec des stratégies par défaut, à l'exception des stratégies Universal Print Server et Load Balancing mentionnées ci-dessus.

Mise à jour des chaînes de connexion à la base de données lors de l'utilisation de solutions de haute disponibilité SQL Server

January 8, 2020

Citrix propose plusieurs scripts PowerShell qui mettent à jour les chaînes de connexion à la base de données XenApp et XenDesktop lorsque vous utilisez des solutions de base de données haute disponibilité SQL Server telles que AlwaysOn et la mise en miroir.

Les scripts, qui utilisent l'API XenApp et XenDesktop PowerShell, sont les suivants :

- **DBConnectionStringFuncs.ps1** : script de base qui effectue le travail réel. Ce script contient des fonctions courantes que les autres scripts utilisent.
- **Change_XD_Failover_Partner_v1.ps1** : met à jour (ajoute, modifie ou supprime) le partenaire de basculement. Ce script vous invite à indiquer l'emplacement du partenaire de basculement (FQDN) pour chaque base de données. (La fourniture d'un partenaire de basculement vide supprime le partenaire de basculement. Vous pouvez également utiliser l'option ClearPartner pour supprimer un partenaire.) Ne définissez pas le partenaire de basculement sur le même emplacement que le serveur de base de données principal.
- **Change_XD_To_ConnectionString.ps1** : utilise les chaînes de connexion fournies pour actualiser les chaînes de connexion vers les bases de données. Ce script garantit que certains services Citrix sont en cours d'exécution, puis met à jour ces services dans l'ordre correct sur tous les Controller du site. Enfermer les informations de chaîne de connexion pour chaque base de données entre guillemets.
- **Change_XD_To_MultiSubnetFailover.ps1** : active l'ajout et la suppression deMultisubnetFailover = true. Si vous utilisez AlwaysOn Availability Groups, Microsoft recommande que la chaîne de

connexion inclut MultiSubnetFailover = true. Cette option accélère la restauration lorsqu'un événement de haute disponibilité se produit et est recommandée pour les environnements à sous-réseau unique et multi-sous-réseau. Exécutez ce script une fois pour ajouter l'option. Si vous devez supprimer l'option, utilisez Change_XD_To_ConnectionString.ps1 pour exécuter à nouveau le script et fournir des chaînes sans le paramètre.

- **Change_XD_To_Null.ps1** : réinitialise toutes les chaînes de connexion sur l'hôte local car quelque chose a mal tourné. En réinitialisant les chaînes de connexion à null, ce script place le Controller dans un état « initial ». Si vous exécutez Studio après avoir exécuté ce script, il vous sera demandé si vous souhaitez créer un site ou rejoindre un site existant. Ceci est utile si quelque chose a mal tourné et qu'une réinitialisation est nécessaire. Après la réinitialisation, vous pouvez réessayer de définir les chaînes de connexion à l'aide de Change_XD_To_ConnectionString.ps1.

Vous pouvez également actualiser manuellement les chaînes de connexion à la base de données ; reportez-vous à la section Mise à jour manuelle des chaînes. Pour télécharger les scripts PowerShell, consultez laProcéduresection.

Exigences et considérations

- Vous devez être un administrateur de site complet pour exécuter les scripts.
- Exécutez les scripts dans la fenêtre **PowerShell** d'un Controller. PowerShell v3 est requis.
- Les composants principaux XenApp et XenDesktop doivent être installés et le site est opérationnel.
- Avant d'exécuter les scripts, désactivez la journalisation de la configuration obligatoire.
- L'option MultiSubnetFailover est prise en charge avec .NET 4.5 et versions ultérieures. Toutefois, le MMC que Studio utilise sur les machines Windows 7 ou 2008 R2 contient une version .NET antérieure, de sorte que vous pouvez voir l'erreur « Mot clé non pris en charge : multisubnetfailover » lorsque vous sélectionnez **Configuration** dans le volet de navigation **Studio** . Dans de tels cas, correctif ou mise à jour comme suit :
- Pour .NET 3.5 SP1, correctif avec http://support.microsoft.com/kb/2654347.
- Pour .NET 4.0, la mise à jour vers 4.0.2 minimum. 4.0.3 est recommandée : http://support.microsoft.com/kb/2600211.

Ensuite, utilisez le script Change_XD_To_MultiSubnetFailover.ps1 pour actualiser les chaînes de connexion à la base de données avec cette option.

Procédure

1. Téléchargez le fichier zip contenant les scripts de Citrix ShareFile.

2. Décompressez le fichier.
3. Assurez-vous que DBConnectionStringFuncs.ps1 se trouve dans le même dossier que le script que vous exécutez, car le script que vous exécutez utilise des fonctions dans DBConnectionStringFuncs.ps1.
4. Exécutez le script sur un Controller.

Si vous souhaitez définir le basculement de sous-réseaux multiples de votre site, vous devez uniquement exécuter le script Change_XD_To_MultiSubnetFailover.ps1. (Rappelez-vous : assurez-vous que le script DBConnectionStringFuncs.ps1 se trouve dans le même dossier.)

> Conseils :
>
> - Lorsque les chaînes de connexion sont mises à jour, il est normal de voir un message indiquant que “Server=SQLxxx\CITRIX\…” est en cours de modification en “Data Source=SQLxxx\CITRIX\…” Les termes Serveur et Source de données sont synonymes.
> - Si vous souhaitez manipuler les chaînes de connexion, regardez comment les scripts Change_XD_utilisent les fonctions de DBConnectionStringFuncs.ps1.

Mise à jour manuelle des chaînes

Pour actualiser les chaînes manuellement, exécutez les applets de commande XenApp et XenDesktop PowerShell.

Étape 1. Déplacer les bases de données SQL vers un autre serveur SQL et affecter les autorisations correctes

1. Sauvegardez les bases de données sur le serveur SQL d’origine et restaurez-les sur le nouveau serveur SQL.
2. Dans **SQL Management Studio > Sécurité > Logins**, ajoutez les comptes d’ordinateur Delivery Controller. Par exemple, CORP\DDC01$.
3. Lors de l’ajout de la connexion SQL, sur la page Mappage utilisateur, cliquez sur les trois bases de données Citrix : Base de données Site, Base de données de surveillance et Base de données de journalisation.
4. Pour chacune des trois bases de données Citrix, ajoutez le compte d’ordinateur Delivery Controller aux différents rôles de base de données. La base de données du site a beaucoup plus de rôles que les bases de données de journalisation et de surveillance.

```
Site database - ADIdentitySchema_ROLE

Site database - Analytics_ROLE                # for 7.8 and newer
Site database - AppLibrarySchema_ROLE         # for 7.8 and newer
Site database - chr_Broker
Site database - chr_Controller
Site database - ConfigLoggingSchema_ROLE
```



```
Site database - ConfigLoggingSiteSchema_ROLE
Site database - ConfigurationSchema_ROLE
Site database - DAS_ROLE
Site database - DesktopUpdateManagerSchema_ROLE
Site database - EnvTestServiceSchema_ROLE
Site database - HostingUnitServiceSchema_ROLE
Site database - Monitor_ROLE
Site database - MonitorData_ROLE
Site database - OrchestrationSchema_ROLE       # for 7.11 and newer
Site database - public
Site database - StorefrontSchema_ROLE          # for 7.8 and newer
Site database - TrustSchema_ROLE               # for 7.11 and newer
Monitoring database - Monitor_ROLE
Monitoring database - public
Logging database - ConfigLoggingSchema_ROLE
Logging database - public
<!--NeedCopy-->
```

Étape 2. Récupérer les connexions de base de données existantes (facultatif)

Exécutez les commandes suivantes pour afficher les chaînes de connexion à la base de données existantes :

```
## Load the Citrix snap-ins
asnp Citrix.*

## Get the current Delivery Controller database connections
Get-ConfigDBConnection
Get-AcctDBConnection
Get-AnalyticsDBConnection              #  for 7.6 and newer
Get-AppLibDBConnection                 #  for 7.8 and newer
Get-OrchDBConnection                   #  for 7.11 and newer
Get-TrustDBConnection                  #  for 7.11 and newer
Get-HypDBConnection
Get-ProvDBConnection
Get-BrokerDBConnection
Get-EnvTestDBConnection
Get-SfDBConnection
Get-MonitorDBConnection
Get-MonitorDBConnection -DataStore Monitor
Get-LogDBConnection
Get-LogDBConnection -DataStore Logging
Get-AdminDBConnection
<!--NeedCopy-->
```


Étape 3. Supprimer les connexions à la base de données existantes

Sur le Delivery Controller, ouvrez PowerShell en tant qu'administrateur et exécutez les commandes suivantes. Ce processus efface les connexions de base de données existantes.

```
## Load the Citrix snap-ins
asnp Citrix.*

## Disable configuration logging for the XD site:
Set-LogSite -State Disabled

## Clear the current Delivery Controller database connections

## Note: AdminDBConnection must be the last command

Set-ConfigDBConnection -DBConnection $null
Set-AcctDBConnection -DBConnection $null
Set-AnalyticsDBConnection -DBConnection $null             #  for 7.6
    and newer
Set-AppLibDBConnection -DBConnection $null                #  for 7.8
    and newer
Set-OrchDBConnection -DBConnection $null                  #  for 7.11
    and newer
Set-TrustDBConnection -DBConnection $null                 #  for 7.11
    and newer
Set-HypDBConnection -DBConnection $null
Set-ProvDBConnection -DBConnection $null
Set-BrokerDBConnection -DBConnection $null
Set-EnvTestDBConnection -DBConnection $null
Set-SfDBConnection -DBConnection $null
Set-MonitorDBConnection -DataStore Monitor -DBConnection $null
Set-MonitorDBConnection -DBConnection $null
Set-LogDBConnection -DataStore Logging -DBConnection $null
Set-LogDBConnection -DBConnection $null
Set-AdminDBConnection -DBConnection $null -force
<!--NeedCopy-->
```

Si un message d'erreur s'affiche, vous devez redémarrer tous les services Citrix.

```
Get-Service Citrix* | Stop-Service -Force
Get-Service Citrix* | Start-Service
<!--NeedCopy-->
```

Après le redémarrage des services Citrix, si vous voyez toujours les erreurs, vous devez redémarrer le serveur. Réexécutez l'ensemble de commandes d'origine pour confirmer que la connexion existante

est correctement supprimée.

Les applets de commande suivantes doivent renvoyer une sortie vide :

```
## Load the Citrix snap-ins
asnp Citrix.*

## Get the current Delivery Controller database connections
Get-ConfigDBConnection
Get-AcctDBConnection
Get-AnalyticsDBConnection               #  for 7.6 and newer
Get-AppLibDBConnection                  #  for 7.8 and newer
Get-OrchDBConnection                    #  for 7.11 and newer
Get-TrustDBConnection                   #  for 7.11 and newer
Get-HypDBConnection
Get-ProvDBConnection
Get-BrokerDBConnection
Get-EnvTestDBConnection
Get-SfDBConnection
Get-MonitorDBConnection
Get-LogDBConnection
Get-AdminDBConnection
<!--NeedCopy-->
```

Étape 4. Spécifier les nouvelles chaînes de connexion à la base de données

Ajustez les variables pour qu'elles correspondent à la chaîne de connexion souhaitée.

- Pour la chaîne de connexion SQL Server autonome :`Server=SQLServerName; Initial Catalog=DBName; Integrated Security=True`
- Pour la chaîne de connexion de mise en miroir de base de données :`Server=PrimarySQLServerName ; Initial Catalog=DBName; Integrated Security=True; Failover Partner= SecondSQLServer`
- Pour Always on High Availability :`Server=ListenerName; Initial Catalog=XDdb; Integrated Security=True; MultiSubnetFailover=True`

Exécutez les commandes suivantes pour définir les nouvelles chaînes de connexion.

```
$ServerName = "<dbserver>"
$SiteDBName = "<SiteDbName>"
$LogDBName = "<LoggingDbName>"
$MonitorDBName = "<MonitorDbName>"
$csSite = "Server=$ServerName;Initial Catalog=$SiteDBName;Integrated
    Security=True"
$csLogging = "Server=$ServerName;Initial Catalog=$LogDBName;Integrated
    Security=True"
```



```
$csMonitoring = "Server=$ServerName;Initial Catalog=$MonitorDBName;
    Integrated Security=True"


Set-AdminDBConnection -DBConnection $csSite
Set-ConfigDBConnection -DBConnection $csSite
Set-AcctDBConnection -DBConnection $csSite
Set-AnalyticsDBConnection -DBConnection $csSite              # for 7.6
    and newer
Set-HypDBConnection -DBConnection $csSite
Set-ProvDBConnection -DBConnection $csSite
Set-AppLibDBConnection  - DBConnection $csSite                # for 7.8
     and newer
Set-OrchDBConnection  - DBConnection $csSite                  # for
    7.11 and newer
Set-TrustDBConnection  - DBConnection $csSite                 # for
    7.11 and newer
Set-BrokerDBConnection -DBConnection $csSite
Set-EnvTestDBConnection -DBConnection $csSite
Set-SfDBConnection -DBConnection $csSite
Set-LogDBConnection -DBConnection $csSite
Set-LogDBConnection -DataStore Logging -DBConnection $csLogging
Set-MonitorDBConnection -DBConnection $csSite
Set-MonitorDBConnection -DataStore Monitor -DBConnection $csMonitoring
<!--NeedCopy-->
```

> Remarque :
>
> Vérifiez que toutes les`Set-<service>DBConnection` commandes précédentes ont renvoyé le résultat **OK**. Si le résultat est différent de **OK** pour l'une de ces commandes, il peut être nécessaire d'activer la journalisation ou le suivi pour déterminer la cause de l'échec de connexion.
>
> `Set-LogDBConnection -DBConnection $null` et `Set-MonitorDBConnection -DBConnection $null` renvoient **DBUnconfigured** au lieu de **OK**.

Étape 5. Tester les nouvelles chaînes de connexion à la base de données

1. Exécutez les commandes suivantes pour vérifier la connectivité à la base de données.

```
## Load the Citrix snap-ins
asnp citrix.*

$ServerName = "<dbserver>"
$SiteDBName = "<SiteDbName>"
$LogDBName = "<LoggingDbName>"
$MonitorDBName = "<MonitorDbName>"
```



```
$csSite = "Server=$ServerName;Initial Catalog=$SiteDBName;
    Integrated Security=True"
$csLogging = "Server=$ServerName;Initial Catalog=$LogDBName;
    Integrated Security=True"
$csMonitoring = "Server=$ServerName;Initial Catalog=$MonitorDBName
    ;Integrated Security=True"

Test-AcctDBConnection -DBConnection $csSite
Test-AdminDBConnection -DBConnection $csSite
Test-AnalyticsDBConnection -DBConnection $csSite   # for 7.6 and
    newer
Test-AppLibDBConnection -DBConnection $csSite      # for 7.8 and
    newer
Test-BrokerDBConnection -DBConnection $csSite
Test-ConfigDBConnection -DBConnection $csSite
Test-EnvTestDBConnection -DBConnection $csSite
Test-HypDBConnection -DBConnection $csSite
Test-LogDBConnection -DBConnection $csSite
Test-LogDBConnection -DataStore Logging -DBConnection $csLogging
Test-MonitorDBConnection -DBConnection $csSite
Test-MonitorDBConnection -Datastore Monitor -DBConnection
    $csMonitoring
Test-OrchDBConnection -DBConnection $csSite       # for 7.11 and
    newer
Test-ProvDBConnection -DBConnection $csSite
Test-SfDBConnection -DBConnection $csSite
Test-TrustDBConnection -DBConnection $csSite      # for 7.11 and
    newer
<!--NeedCopy-->
```

2. Redémarrez Citrix Studio.

Plus d'informations

- Comment faire pour configurer SQL Server autonome, la mise en miroir de bases de données et toujours en haute disponibilité

Découverte de Controller basée sur unité d'organisation Active Directory

January 8, 2020

Cette méthode de découverte du Delivery Controller est principalement prise en charge pour la compatibilité ascendante et n'est valable que pour les Virtual Delivery Agent (VDA) pour Windows Desktop OS, et non pour les VDA pour Windows Server.

Pour plus d'informations sur les autres méthodes que vous pouvez configurer qui permettent aux VDA de s'inscrire auprès des Controller (y compris les méthodes recommandées), voir Enregistrement VDA auprès des Controller.

La découverte basée sur Active Directory exige que tous les ordinateurs d'un site soient membres d'un domaine ; par ailleurs, le domaine utilisé par le Controller doit entretenir des relations de confiance avec le ou les domaines utilisés par les bureaux. Si vous utilisez cette méthode, vous devez configurer le GUID de l'unité d'organisation dans chaque registre de bureau.

Pour effectuer une découverte de contrôleur basée sur l'unité d'exploitation, exécutez le script PowerShell **Set-ADControllerDiscovery.ps1** sur le contrôleur (chaque contrôleur contient ce script dans le dossier`$Env:ProgramFiles\Citrix\Broker\Service\Setup Scripts`). Pour exécuter le script, vous devez disposer des autorisations CreateChild sur une unité d'organisation parent, ainsi que des droits d'administration complets.

Lorsque vous créez un site, une unité d'organisation correspondante doit être créée dans Active Directory si vous souhaitez que les bureaux reconnaissent les Controller d'un site à l'aide d'Active Directory. L'unité d'organisation peut être créée dans n'importe quel domaine de la forêt contenant vos ordinateurs. À titre de pratique exemplaire, l'unité d'organisation doit également contenir les Contrôleurs dans le Site, mais cela n'est pas appliqué ou requis. Un administrateur de domaine disposant des privilèges appropriés peut créer l'unité d'organisation en tant que conteneur vide, puis déléguer l'autorité administrative sur l'unité d'organisation à un administrateur Citrix.

Le script crée plusieurs objets essentiels. Seuls les objets Active Directory standard sont créés et utilisés. Il n'est pas nécessaire d'étendre le schéma.

- Un groupe de sécurité pour les Controller. Le compte d'ordinateur de tous les Contrôleurs du Site doit être membre de ce groupe de sécurité. Les bureaux d'un site acceptent les données provenant de Controller uniquement s'ils appartiennent à ce groupe de sécurité.

  Vérifiez que tous les Controller disposent du privilège « Accéder à cet ordinateur à partir du réseau » sur l'ensemble des bureaux virtuels exécutant le VDA. Vous pouvez le faire en accordant ce privilège au groupe de sécurité Controllers. Si les Controller ne disposent pas de ce privilège, les VDA ne pourront pas s'enregistrer.

- Objet Service Connection Point (SCP) qui contient des informations sur le Site, telles que le nom du Site. Si vous utilisez l'outil d'administration Utilisateurs et ordinateurs Active Directory pour inspecter une unité d'organisation de site, vous devrez peut-être activer les fonctionnalités avancées dans le menu Affichage pour afficher les objets SCP.

- Conteneur appelé RegistrationServices, qui est créé dans l'unité d'organisation du site. Celui-ci contient un objet SCP pour chaque Controller du site. À chaque démarrage du Controller, il

valide le contenu de son objet SCP et le met à jour si nécessaire.

Si différents administrateurs sont susceptibles d'ajouter et de supprimer des Controller une fois l'installation initiale effectuée, ils doivent disposer des autorisations requises pour créer et supprimer les enfants dans le conteneur RegistrationServices et les propriétés d'écriture sur le groupe de sécurité des Controller. Ces autorisations sont accordées automatiquement à l'administrateur qui exécute le script Set-adControllerDiscovery.ps1. L'administrateur de domaine ou l'administrateur d'installation d'origine peut accorder ces autorisations, et Citrix recommande de configurer un groupe de sécurité pour ce faire.

Lorsque vous utilisez une unité d'organisation de site :

- Les informations sont écrites dans Active Directory uniquement lorsque vous installez ou désinstallez ce logiciel, ou lorsqu'un Controller démarre et doit mettre à jour les informations dans son objet SCP (par exemple, lorsque le nom du Controller ou le port de communication a été modifié). Par défaut, le script Set-ADControllerDiscovery.ps1 définit les autorisations appropriées relatives aux objets de l'unité d'organisation d'un site, en accordant à chaque Controller un accès en écriture sur leurs objets SCP. Le contenu des objets de l'unité d'organisation du site permet d'établir une relation de confiance entre les bureaux et les Controller. Veiller à ce que :
  - Seuls les administrateurs autorisés peuvent ajouter ou supprimer des ordinateurs du groupe de sécurité Controllers, à l'aide de la liste de contrôle d'accès (ACL) du groupe de sécurité.
  - seuls les administrateurs autorisés et leur Controller respectif peuvent modifier les informations de l'objet SCP du Controller.
- Si votre déploiement utilise la réplication, soyez conscient des retards potentiels. Pour plus de détails, reportez-vous à la documentation Microsoft. Ce point est particulièrement important si vous créez l'unité d'organisation du site dans un domaine contenant des contrôleurs de domaine situés dans différents sites Active Directory. En fonction de l'emplacement des bureaux, des Controller et des contrôleurs de domaine, les modifications apportées à Active Directory lors de la création initiale de l'unité d'organisation du site, de l'installation ou de la désinstallation de Controller, de la modification d'un nom de Controller ou de ports de communication, peuvent ne pas être visibles sur les bureaux tant que les informations n'ont pas été répliquées dans le contrôleur de domaine approprié. Le retard de la réplication peut entraîner, entre autres, les conséquences suivantes : les bureaux ne peuvent pas établir de contact avec les Controller, et de ce fait, ne sont pas disponibles pour les connexions utilisateur.
- Ce logiciel utilise plusieurs attributs d'objet ordinateur standard dans Active Directory pour gérer les postes de travail. Selon votre déploiement, le nom de domaine complet de l'objet machine, tel qu'il est stocké dans l'enregistrement Active Directory du Bureau, peut être inclus dans les paramètres de connexion renvoyés à l'utilisateur pour établir une connexion. Assurez-vous que ces informations sont cohérentes avec les informations de votre environnement DNS.

Pour déplacer un Controller vers un autre site à l'aide de la découverte de Controller basée sur

l'unité d'organisation, suivez les instructions ci-dessus pour le déplacement d'un Delivery Controller. Lorsque vous supprimez le Controller de l'ancien site (étape 2), exécutez le script PowerShell : **Set-ADControllerDiscover –sync**. Le script assure la synchronisation entre l'unité d'organisation et l'ensemble actuel des Controller. Après avoir rejoint le site existant (étape 3), exécutez le même script sur un Controller dans le nouveau site.

Autorisations requises pour la découverte basée sur l'UI

Pour créer un site, l'administrateur Citrix qui exécute le script doit disposer de droits sur l'unité d'organisation du site pour créer des objets (SCP, conteneur et groupe de sécurité).

Si l'unité d'organisation du site n'est pas présente, l'administrateur doit également disposer des droits nécessaires pour la créer. Citrix recommande à l'administrateur du domaine AD de pré-créer cette unité d'organisation et de lui déléguer des droits à l'identité de l'administrateur du site Citrix. En option, le script peut également créer l'unité d'organisation du site. Pour cela, l'administrateur a besoin de la « création d'unité d'organisation » directement sur l'unité d'organisation parent de la nouvelle unité d'organisation. Cependant, comme indiqué, Citrix ne recommande pas cela.

Plus tard, pour ajouter ou supprimer un Delivery Controller dans le site, l'administrateur Citrix doit disposer des droits d'ajouter/supprimer une machine dans le groupe de sécurité, et de créer/supprimer un objet SCP.

En mode de fonctionnement normal, les Controller et les VDA doivent disposer des droits d'accès en lecture à tous les objets de l'unité d'organisation et des niveaux inférieurs. Les VDA accèdent à l'unité d'organisation sous leur propre identité de machine ; cette identité de machine doit disposer au minimum de droits en lecture dans l'unité d'organisation pour être en mesure de détecter les Controller. Un Controller a également besoin des droits pour définir des propriétés sur son propre objet SCP dans le conteneur.

L'octroi de tous les droits de l'administrateur Citrix aux Us enfants autorisera toutes ces actions. Toutefois, si votre déploiement comporte des exigences de sécurité plus strictes (par exemple, en limitant les personnes qui peuvent utiliser le script pour quelle action), vous pouvez utiliser l'Assistant Délégation de contrôle pour définir des droits spécifiques. L'exemple de procédure suivant accorde des droits pour créer le Site.

1. Créez une unité d'organisation pour contenir les objets enfants (Service Connection Point (SCP), conteneur et groupe de sécurité).
2. Sélectionnez l'unité d'organisation, puis cliquez avec le bouton droit de la souris et sélectionnez **Déléguer le contrôle**.
3. Dans l'Assistant Délégation de contrôle, spécifiez l'utilisateur de domaine auquel déléguer le contrôle pour l'unité d'organisation.
4. Dans la page **Tâches à déléguer**, sélectionnez **Créer une tâche personnalisée à déléguer**.

5. Sur la page **Type d'objet Active Directory** , acceptez la valeur par défaut **Ce dossier, les objets existants dans ce dossier et la création de nouveaux objets dans ce dossier**.
6. Sur la page **Autorisations** , activez les cases à cocher **Écrire et créer tous les objets enfants**.
7. Terminez l'Assistant pour confirmer les privilèges.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States