EdgeADC

Guide d'administration EdgeADC

VERSION DU LOGICIEL

5.0.0

Contenu

Propriétés du document

Numéro de document :2 .0.3.19.25.12.03

Date de création du document :19 March 2025

Document édité pour la dernière fois : 19 March 2025

Auteur du document : Jay Savoor

Document édité en dernier lieu par :

Document : EdgeADC - Version 5.0.0

Avis de non-responsabilité

Les captures d'écran et les graphiques de ce manuel peuvent différer légèrement de votre produit en raison de différences dans la version du produit. Edgenexus s'engage à faire tous les efforts raisonnables pour s'assurer que les informations contenues dans ce document sont complètes et exactes. Edgenexus n'assume aucune responsabilité en cas d'erreur. Edgenexus apportera des modifications et des corrections aux informations contenues dans le présent document dans les versions futures lorsque le besoin s'en fera sentir.

Droits d'auteur

Marques déposées

Le logo Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS sont des marques commerciales ou des marques déposées d'Edgenexus Limited. Toutes les autres marques sont la propriété de leurs détenteurs respectifs et sont reconnues.

Soutien d'Edgenexus

Si vous avez des questions techniques concernant ce produit, veuillez envoyer un ticket d'assistance à l'adresse suivante : support@edgenexus.io

Introduction

Vous lisez ce guide parce que vous avez l'intention de déployer le EdgeADC d'Edgenexus et d'équilibrer la charge de vos applications basées sur des serveurs de manière efficace et rentable.

Le EdgeADC est construit autour d'un moteur hautement sécurisé qui offre une grande évolutivité, une sécurité et des performances élevées, ainsi qu'une interface de gestion très facile à utiliser. Ces facteurs garantissent que ce que vous déployez offrira le meilleur coût de propriété possible.

L'objectif de ce document

Ce document a été rédigé pour vous permettre d'administrer le EdgeADC à l'aide de son interface web facile à utiliser. Les fonctions et leurs configurations sont décrites en détail, et nous espérons que cela vous suffira pour configurer l'EdgeADC selon vos besoins.

À qui s'adresse ce document ?

Ce document s'adresse aux personnes ayant des connaissances en matière de réseaux, en particulier de protocoles, d'applications et de serveurs.

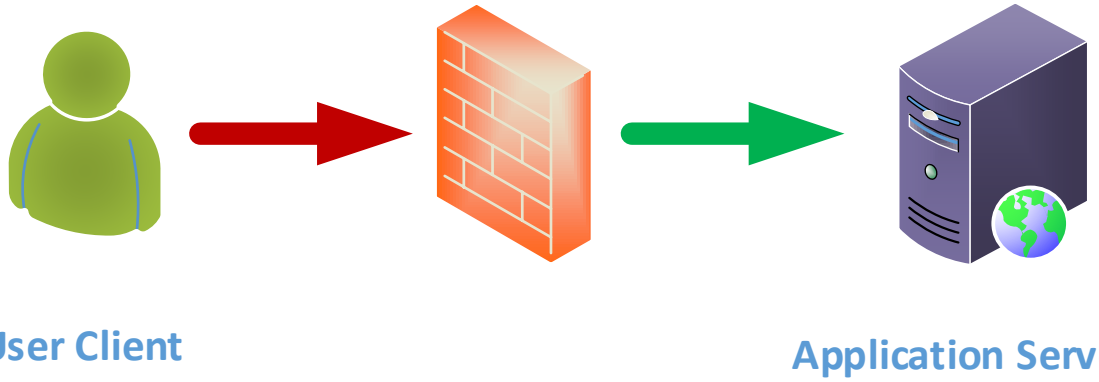
Équilibrage de charge 101

Qu'est-ce qu'un équilibreur de charge ou ADC ?

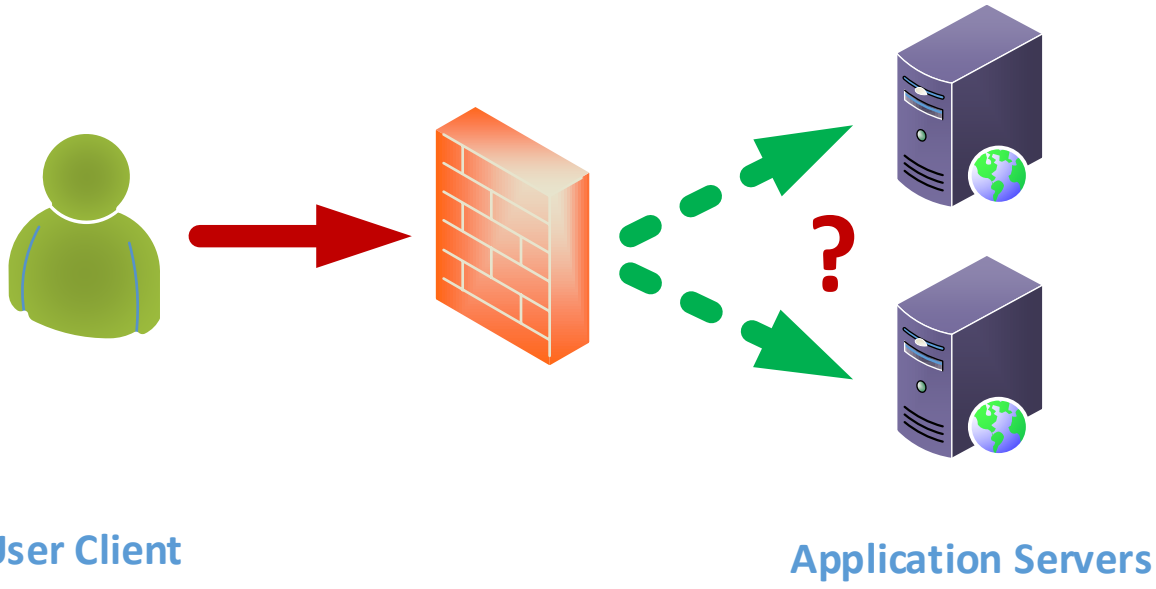
Les équilibreurs de charge ont considérablement évolué et leurs moteurs intègrent beaucoup plus d'intelligence qu'auparavant. Aujourd'hui, ils sont souvent appelés "contrôleurs de livraison d'applications" (ADC).

Avant de comprendre ce qu'est un équilibreur de charge ou un ADC, nous devons reconnaître les problèmes de l'informaticien et de l'utilisateur. Prenons un exemple.

- Une entreprise publie une application web sur Internet. L'application est hébergée sur un seul serveur web, les données résidant sur un serveur de base de données distinct.



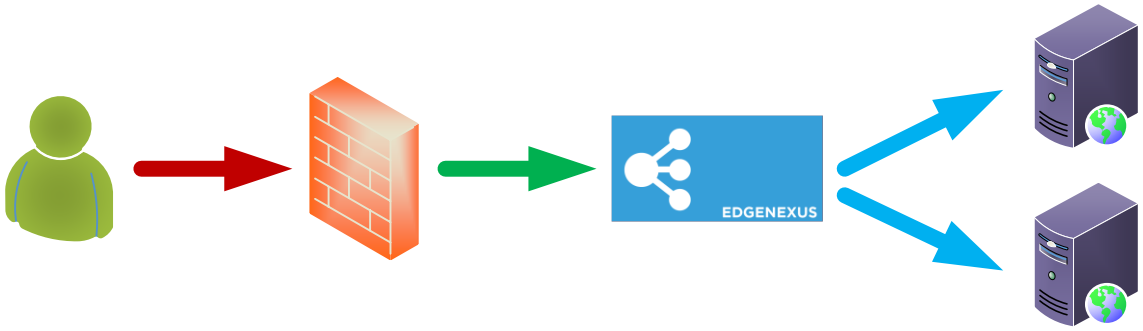
- Ce serveur utilise l'adresse IP 1.2.3.4 à titre d'exemple.
- Le nombre de clients accédant à l'application augmente régulièrement et certains ont signalé que les performances de l'application diminuaient.
- L'analyse du serveur montre que le trafic sur le serveur a augmenté massivement et continue de progresser.
- La décision est donc prise d'ajouter un autre serveur pour héberger l'application.
- Le nouveau deuxième serveur utilise l'adresse IP 1.2.3.5.
- Le problème est de savoir comment diriger le client vers le nouveau serveur et le serveur actuel afin de partager la charge et de garantir que la session de l'utilisateur est maintenue sur le premier serveur connecté.



- La réponse est un équilibreur de charge ou ADC.

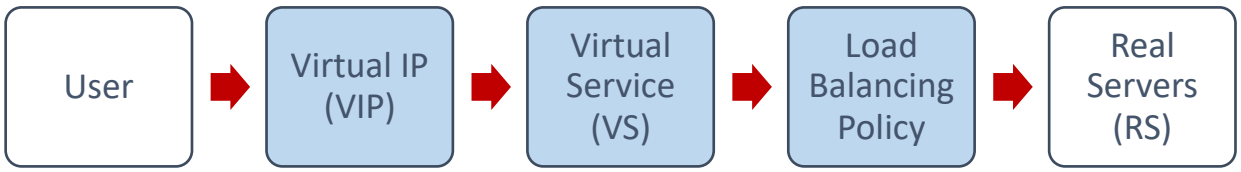
Maintenant, la solution.

- Nous plaçons un ADC devant les deux serveurs d'application.

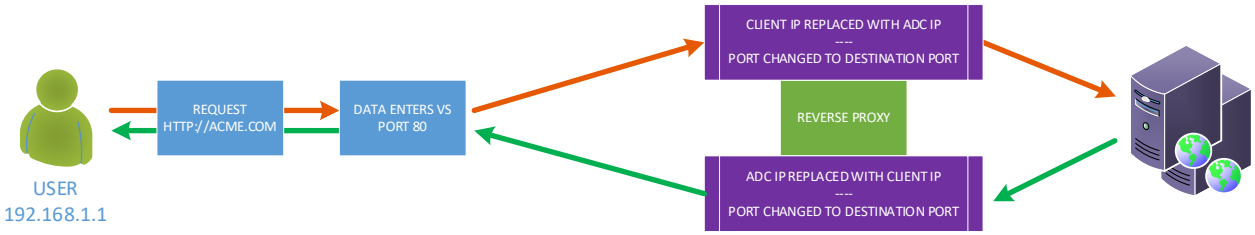


User Client **ADC** **Application Servers**

- L'ADC aura une adresse IP externe de 1.2.3.6, et le pare-feu redirigera les demandes vers cette adresse au lieu de 1.2.3.4.
- L'IP de l'ADC qui reçoit les demandes est appelée VIP, et la configuration est appelée service virtuel.
- L'ADC recevra les demandes des utilisateurs clients et les transmettra par proxy inverse aux serveurs réels à l'aide de stratégies d'équilibrage de la charge, tout en surveillant l'état des serveurs d'application pour garantir l'efficacité.



- L'ADC équilibre le trafic vers les serveurs en fonction de la politique d'équilibrage de charge utilisée, de la nature de la charge et de l'état des serveurs d'application.
- Le trafic provenant des serveurs sera renvoyé au client par l'intermédiaire de l'ADC dans la direction opposée.
- En raison de la nature du proxy inverse, le serveur et le client sont anonymes l'un par rapport à l'autre.



- La technologie du proxy inverse garantit un niveau de sécurité optimal.

Explication des VIP et des services virtuels (VS)

Un VIP est, par essence, une adresse IP définie pour être utilisée sur l'EdgeADC et qui permet aux utilisateurs d'accéder aux services qui y sont liés. C'est à peu près ce qu'est un VIP. En raison du mode de fonctionnement de l'EdgeADC, il n'est pas nécessaire que le VIP se trouve dans le même sous-réseau que les serveurs réels, et cette méthodologie de traduction d'adresse réseau rend la technologie très sûre pour les pirates qui tentent d'accéder aux serveurs internes.

Remarque : l'adresse IP du VIP ne peut pas être la même que l'adresse IP utilisée pour l'IP de gestion.

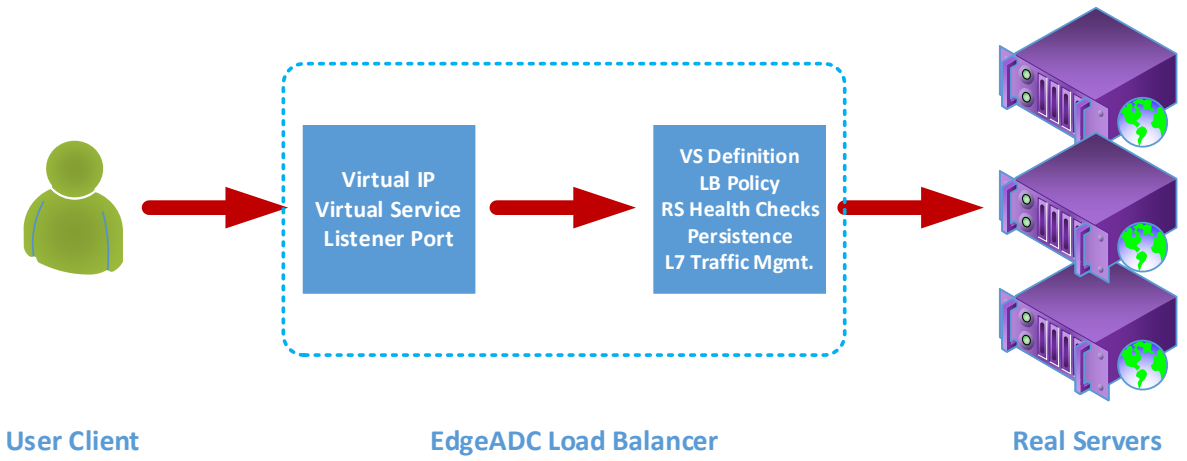
Les services virtuels sont au cœur des technologies de proxy et d'équilibrage de charge EdgeADC. L'IP virtuelle est l'adresse par laquelle le service virtuel est annoncé au réseau et au monde entier, à l'écoute du trafic et des demandes des clients qui souhaitent utiliser les applications qu'il sert.

Lorsque les clients atteignent le VS, celui-ci est configuré pour effectuer de nombreuses actions sur le trafic, y compris, mais sans s'y limiter, les actions suivantes :

- Proxy de la connexion du client
- Des fonctions spécifiques sont exécutées, telles que la compression, l'accélération, l'équilibrage de la charge, l'inspection du trafic, etc.
- Transférer les demandes du client vers les serveurs de destination définis dans les politiques d'équilibrage de charge du service virtuel.

On peut considérer que le VS est associé à une adresse IP (VIP) que l'EdgeADC écoute pour préparer les demandes de données. Lorsque des configurations TCP ou HTTP standard sont effectuées, le client se connecte à la VIP et l'EdgeADC traite la demande conformément à la définition qui constitue le VS. Une fois cette opération effectuée, l'EdgeADC envoie le trafic vers les serveurs réels spécifiés.

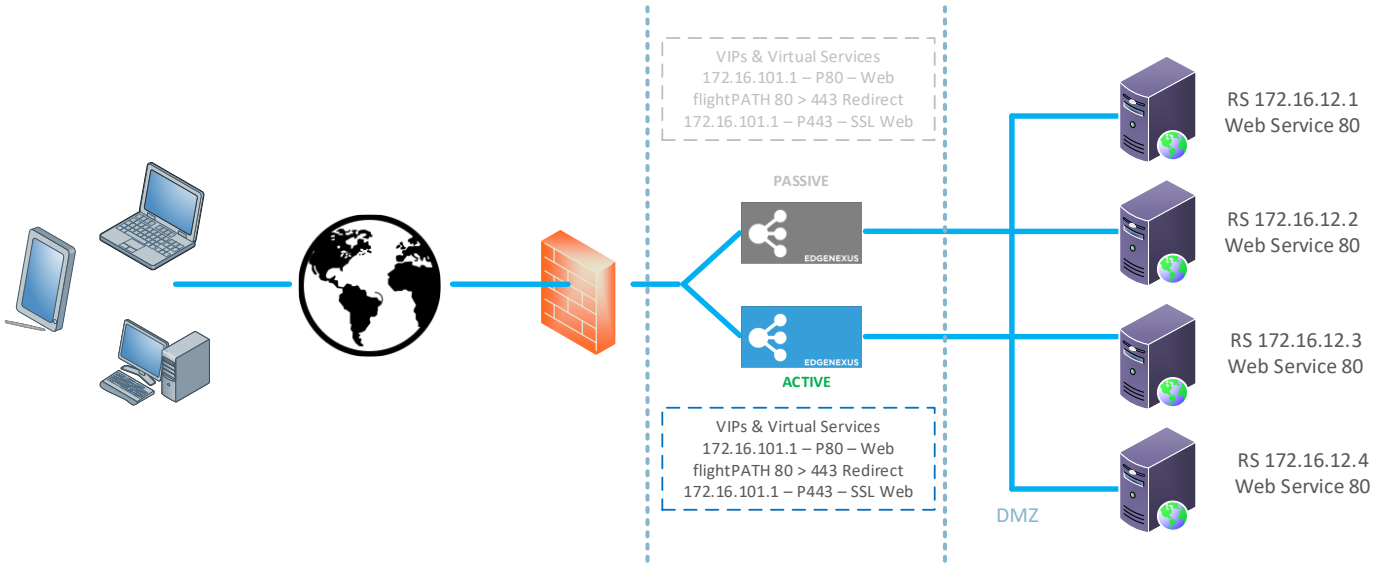
Le VS reçoit la connexion et les données dans une configuration typique, puis termine ou établit une procuration à l'aide du moteur de procuration inverse de l'EdgeADC. L'EdgeADC ouvre alors une nouvelle connexion avec les serveurs réels et transmet les données. Lorsque les serveurs réels répondent à la demande, l'EdgeADC envoie la réponse au client en utilisant un chemin inverse similaire, en fonction des paramètres définis dans l'option Connectivité de l'onglet Equilibrage de charge des serveurs réels.



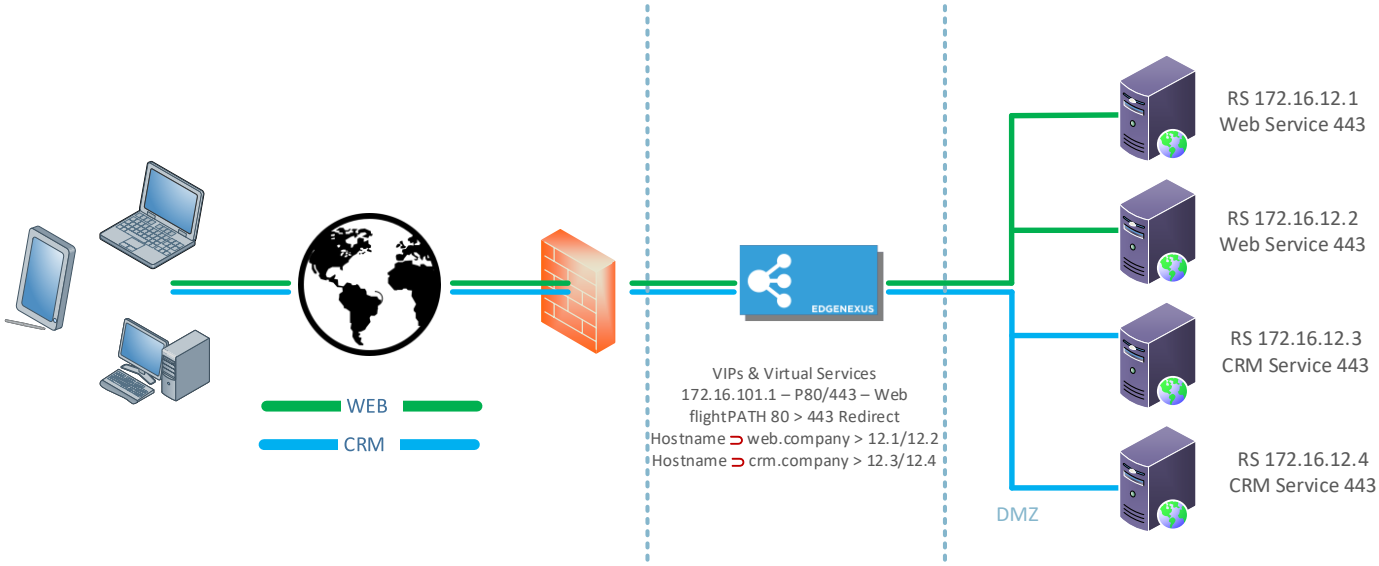
La définition d'un service virtuel comprend une adresse IP unique (VIP) et un ensemble de ports qui servent de points d'entrée vers différents services, à l'aide de divers protocoles.

Par exemple, vous devez équilibrer la charge d'une série de serveurs web pour assurer leur résilience. Supposons maintenant que l'on accède à ces systèmes par des communications sécurisées HTTPS à l'aide de https://myweb.company.com.

Si l'on examine la définition d'une telle configuration, elle comprendra un seul VIP avec deux entrées, l'une pour le port 80 et l'autre pour le port 443. Le VIP pour le port 80 sera associé à une règle flightPATH qui forcera la conversion du trafic en HTTPS. La deuxième entrée pour le port 443 enverra ensuite le trafic vers les serveurs réels définis sous cette entrée. De la même manière, vous pourriez avoir d'autres services sous le même VIP pour équilibrer le trafic vers les serveurs de messagerie ou d'autres serveurs d'application.



Avec des CDA moins fonctionnels, les services qui utilisent les mêmes ports auraient besoin de VIP différents, mais le CDA et son système flightPATH vous permettent d'utiliser un seul VIP avec plusieurs services qui utilisent les mêmes ports. Ainsi, vous pouvez avoir deux applications, toutes deux accessibles par 443 avec des noms d'hôtes différents, en utilisant un seul VIP. Un exemple est illustré ci-dessous.



Les systèmes EdgeADC sont extrêmement flexibles et permettent de définir des configurations fonctionnelles très complexes.

Qu'est-ce qu'un type de service d'équilibrage de charge ?

Les types de services d'équilibrage de charge consistent en des algorithmes et des méthodologies utilisés pour distribuer intelligemment ou équilibrer le trafic sur des pools de serveurs. La méthode et l'algorithme que l'ADC met à disposition dépendent du type de service ou d'application utilisé sur les serveurs dont la charge est équilibrée, ainsi que de l'état du réseau et des serveurs utilisés. Il convient de noter que le type de service d'équilibrage de charge que vous choisissez d'utiliser dépend également du niveau de trafic envoyé par l'ADC. Ainsi, lorsque le débit ou la charge du trafic est faible, les types de service d'équilibrage de charge peuvent être simples. Mais lorsque les charges sont plus importantes, vous devrez peut-être choisir des types plus complexes afin d'obtenir une répartition plus efficace de la charge sur les serveurs dorsaux.

Les types de services d'équilibrage de charge suivants sont disponibles au sein de l'EdgeADC.

DICOM	COUCHE 4 UDP	RPC
FTP	COUCHE 4 TCP/UDP	RPC/ADS
HTTP(S)	DNS	RPC/CA/PF
IMAP	POP3	SMTP
COUCHE 4 TCP	RDP	GSLB

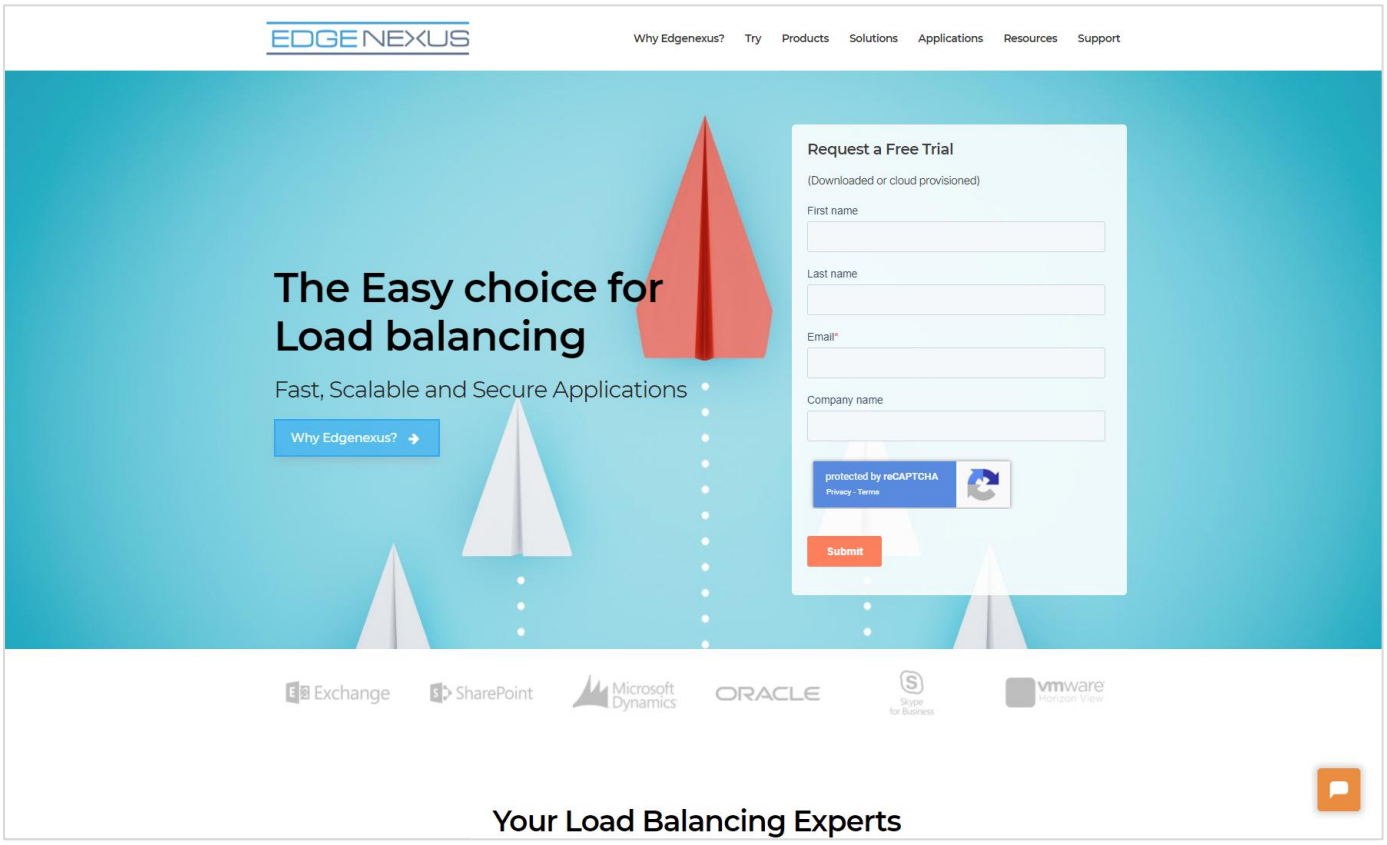
Le début du voyage

Téléchargement de l'EdgeADC

Avant l'installation, la première étape consiste à télécharger le EdgeADC adapté à votre environnement.

Nous fournissons des éditions pour la plupart des environnements virtualisés et une édition ISO pour l'installation directe sur du matériel nu.

La première étape consiste à remplir le formulaire d'évaluation qui se trouve sur le site web d'Edgenexus, à l'adresse https://www.edgenexus.io/products/load-balancer/free-trial/.



La procédure est simple. Après avoir rempli le formulaire et l'avoir envoyé, vous serez dirigé vers la page de téléchargement, où vous pourrez sélectionner l'image correspondant à votre environnement.

Les éditions EdgeADC sont disponibles pour les systèmes de virtualisation suivants :

- VMware ESX
- Microsoft Hyper-V
- Citrix XenServer
- Nutanix
- KVM

Vous pouvez également opter pour un essai dans le nuage en utilisant les éditions Microsoft Azure ou Amazon AWS marketplace.

Si vous choisissez de télécharger le logiciel pour une installation sur site, vous recevrez l'EdgeADC avec une licence d'essai intégrée de 14 jours. Nous vous recommandons de contactersales@edgenexus.io et de demander une clé de licence de 30 jours avec toutes les fonctionnalités activées.

Installation

Installi ng the EdgeADC

L'EdgeADC (ADC) peut être installé sur diverses plates-formes, chacune nécessitant son propre programme d'installation, qui est mis à votre disposition une fois que vous vous êtes inscrit pour le téléchargement.

Voici les différents modèles d'installation disponibles.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Proxmox (Utiliser OVA)
- ISO pour le matériel BareMetal

Le dimensionnement de la machine virtuelle que vous utiliserez pour héberger l'ADC dépend du scénario d'utilisation et du débit de données.

Installation sur VMware ESXi

L'ADC peut être installé sur VMware ESXi version 5.x et supérieure.

- Téléchargez le dernier paquet d'installation OVA d'ADC en utilisant le lien approprié fourni avec l'e-mail de téléchargement.
- Une fois téléchargée, décompressez-la dans un répertoire approprié sur votre hôte ESXi ou votre SAN.
- Dans votre client vSphere, sélectionnez File : Deploy OVA/OVF Template (Fichier : Déployer un modèle OVA/OVF).
- Parcourez et sélectionnez l'emplacement où vous avez enregistré vos fichiers ; choisissez le fichier OVF et cliquez sur **SUIVANT.**
- Le serveur ESX demande le nom de l'appliance. Saisissez un nom approprié et cliquez sur **NEXT**
- Sélectionnez le datastore à partir duquel votre appliance ADC sera exécutée.
- Sélectionnez un datastore disposant de suffisamment d'espace et cliquez sur **SUIVANT**
- Vous obtiendrez ensuite des informations sur le produit ; cliquez sur **SUIVANT.**
- Cliquez sur **NEXT.**
- Une fois que vous avez copié les fichiers sur le magasin de données, vous pouvez installer l'appliance virtuelle.

Lancez votre client vSphere pour voir la nouvelle appliance virtuelle ADC.

- Cliquez avec le bouton droit de la souris sur le VA et sélectionnez Power > Power-On.
- Votre VA démarre alors et l'écran de démarrage de l'ADC s'affiche sur la console.

Installation de l'interface VMXNET3

Le pilote VMXnet3 est pris en charge, mais vous devrez d'abord modifier les paramètres de la carte réseau.

***Note** - Ne mettez PAS à jour le logiciel VMware-tools*

Activation de l'interface VMXNET3 sur un VA fraîchement importé (jamais démarré)

1. Supprimer les deux cartes réseau de la VM
2. Cliquez avec le bouton droit de la souris sur la VM dans la liste et sélectionnez Mettre à niveau le matériel virtuel (ne lancez pas l'installation ou la mise à jour des outils VMware, effectuez **uniquement** la mise à niveau du matériel).
3. Ajouter deux cartes réseau et les sélectionner comme VMXNET3
4. Démarrez l'AV en utilisant la méthode standard. Il fonctionnera avec le VMXNET3

Activation de l'interface VMXNET3 sur un VA déjà en cours d'exécution

1. Arrêter la VM (commande CLI shutdown ou GUI power-off)
2. Obtenez les adresses MAC des deux NIC (n'oubliez pas l'ordre des NIC dans la liste !)
3. Supprimer les deux cartes réseau de la VM
4. Mettre à niveau le matériel de la VM (ne pas lancer l'installation ou la mise à jour des outils VMware, mais effectuer **uniquement** la mise à niveau du matériel).
5. Ajoutez deux cartes réseau et sélectionnez-les comme VMXNET3.
6. Définissez les adresses MAC pour les nouveaux NIC conformément à l'étape 2.
7. Redémarrer l'AV

Nous soutenons VMware ESXi comme plateforme de production. À des fins d'évaluation, vous pouvez utiliser VMware Workstation et Player.

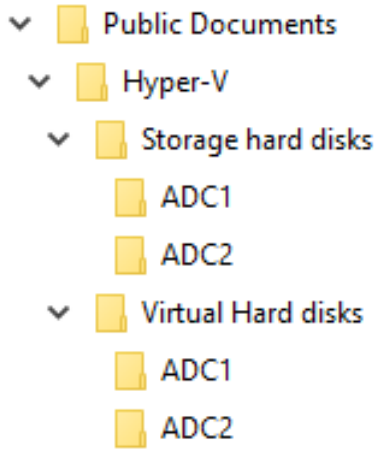
Veuillez vous référer à la section **CONFIGURATION DU PREMIER DEMARRAGE** pour continuer.

Installation sur Microsoft Hyper-V

L'appliance virtuelle ADC d'Edgenexus peut être facilement installée dans un cadre de virtualisation Microsoft Hyper-V. Ce guide suppose que vous avez correctement spécifié et configuré votre système Hyper-V et les ressources du système pour accueillir l'ADC et son architecture d'équilibrage de charge.

Chaque appareil a besoin d'une adresse MAC unique.

- Extrayez le fichier ADC-VA compatible Hyper-V téléchargé sur votre machine ou serveur local.
- Ouvrez Hyper-V Manager.
- Créez un nouveau dossier contenant le "disque dur virtuel" de l'ADC VA et un autre contenant le "disque dur de stockage", par exemple C:\Users\Public\Documents\Hyper-V\Disques durs virtuels\ADC1 et C:\Users\Public\Documents\Hyper-V\Disques durs de stockage\ADC1.
- **Note** : De nouveaux sous-dossiers spécifiques à l'ADC pour les disques durs virtuels et les disques durs de stockage doivent être créés pour chaque installation d'instance ADC virtuelle, comme indiqué ci-dessous :



- Copiez le fichier EdgeADC .vhd extrait dans le dossier "Storage hard disk" créé ci-dessus.
- Dans votre client Hyper-V Manager, faites un clic droit sur le serveur et sélectionnez "Importer une machine virtuelle"
- Recherchez le dossier contenant le fichier image ADC VA téléchargé et extrait précédemment.
- Sélectionnez la machine virtuelle - mettez en évidence la machine virtuelle à importer et cliquez sur Suivant.
- Sélectionnez la machine virtuelle - mettez en évidence la machine virtuelle à importer et cliquez sur Suivant.
- Choisissez le type d'importation - sélectionnez "**Copier la machine virtuelle (créer un nouvel identifiant unique)**" cliquez sur suivant
- Choisir les dossiers pour les fichiers de la machine virtuelle - la destination peut être laissée comme celle par défaut d'Hyper-V ou vous pouvez choisir de sélectionner un emplacement différent.
- Localiser les disques durs virtuels - recherchez et sélectionnez le dossier des disques durs virtuels créé ci-dessus et cliquez sur suivant.
- Choisissez les dossiers pour stocker les disques durs virtuels - recherchez et sélectionnez le dossier Storage hard disks créé précédemment et cliquez sur suivant.
- Vérifiez que les détails de la fenêtre Résumé de l'assistant d'importation sont corrects et cliquez sur Terminer.
- Cliquez avec le bouton droit de la souris sur la machine virtuelle **ADC** nouvellement importée et sélectionnez Démarrer

REMARQUE : CONFORMEMENT A HTTP://SUPPORT.MICROSOFT.COM/KB/2956569, VOUS DEVEZ IGNORER LE MESSAGE D'ETAT "DEGRADE (MISE A NIVEAU DES SERVICES D'INTEGRATION REQUISE)", QUI PEUT S'AFFICHER COMME SUIT APRES LE DEMARRAGE DE L'AV. AUCUNE ACTION N'EST REQUISE ET LE SERVICE N'EST PAS DÉGRADÉ.

- Pendant l'initialisation de la VM, vous pouvez cliquer avec le bouton droit de la souris sur l'entrée de la VM et sélectionner Connecter... La console EdgeADC s'affiche alors.

- Une fois que vous avez configuré les propriétés du réseau, le VA redémarre et présente la connexion à la console du VA.

Veuillez vous référer à la section **CONFIGURATION DU PREMIER DEMARRAGE** pour continuer.

Installation sur Citrix XenServer

L'appliance virtuelle ADC peut être installée sur Citrix XenServer.

- Extrayez le fichier ADC OVA ALB-VA sur votre machine ou serveur local.
- Ouvrez Citrix XenCenter Client.
- Dans votre client XenCenter, sélectionnez **"File : Import".**
- Recherchez et sélectionnez le fichier **OVA**, puis cliquez sur **"Ouvrir ensuite".**
- Sélectionnez l'emplacement de création de la VM lorsque cela vous est demandé.
- Choisissez le serveur XenServer que vous souhaitez installer et cliquez sur **"NEXT".**
- Sélectionnez le référentiel de stockage (SR) pour le placement des disques virtuels lorsque cela vous est demandé.
- Sélectionnez un SR avec suffisamment d'espace et cliquez sur **"SUIVANT".**
- Établissez la carte de vos interfaces de réseau virtuel. Les deux interfaces indiqueront Eth0 ; cependant, notez que l'interface du bas est Eth1.
- Sélectionnez le réseau cible pour chaque interface et cliquez sur **SUIVANT**
- **NE PAS** cocher la case "Utiliser le correctif du système d'exploitation".
- Cliquez sur **"SUIVANT"**
- Choisissez l'interface réseau à utiliser pour le transfert temporaire de la VM.
- Choisissez l'interface de gestion, généralement le réseau 0, et laissez les paramètres réseau sur DHCP. Sachez que vous devez attribuer des adresses IP statiques si vous ne disposez pas d'un serveur DHCP opérationnel pour le transfert. Si vous ne le faites pas, l'importation dira Connecting continuously puis échouera. Cliquez sur **"SUIVANT"**
- Passez en revue toutes les informations et vérifiez que les paramètres sont corrects. Cliquez sur **"FINIR".**
- Votre VM commencera à transférer le disque virtuel "ADC" et, une fois terminé, s'affichera sous votre XenServer.
- Dans votre client XenCenter, vous pouvez maintenant voir la nouvelle machine virtuelle.
  Cliquez avec le bouton droit de la souris sur la VA et cliquez sur "**START**".
- Votre VM démarre alors et l'écran de démarrage de l'ADC s'affiche.

- Une fois configurée, la connexion à l'AV se présente.

Veuillez vous référer à la section **CONFIGURATION DU PREMIER DEMARRAGE** pour continuer.

Installation sur KVM

La section suivante montre comment installer l'EdgeADC sur une plate-forme KVM. La plate-forme KVM utilisée pour cet exercice fonctionne sous un système d'exploitation CentOS v8 avec Cockpit et virtualisation installés.

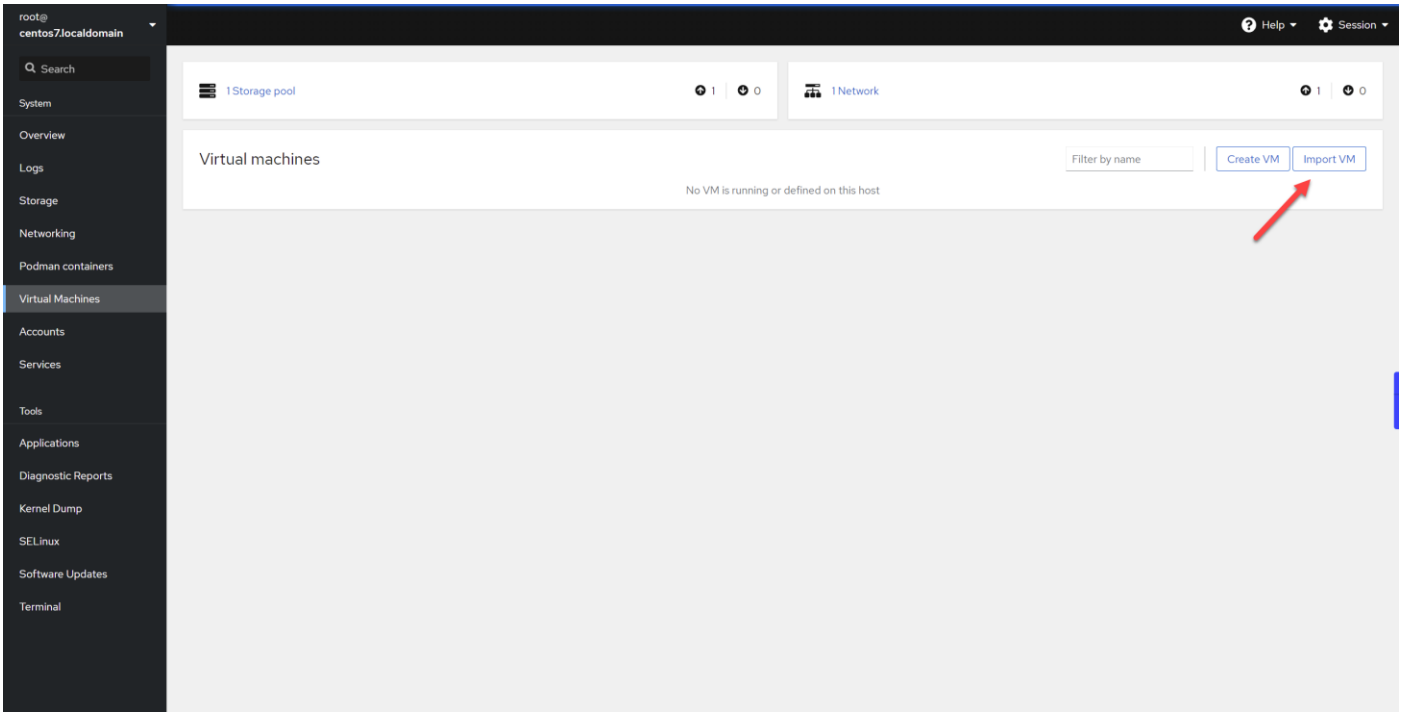
Exigences et versions

Ce guide s'applique à EdgeADC 4.2.6 et aux versions ultérieures.

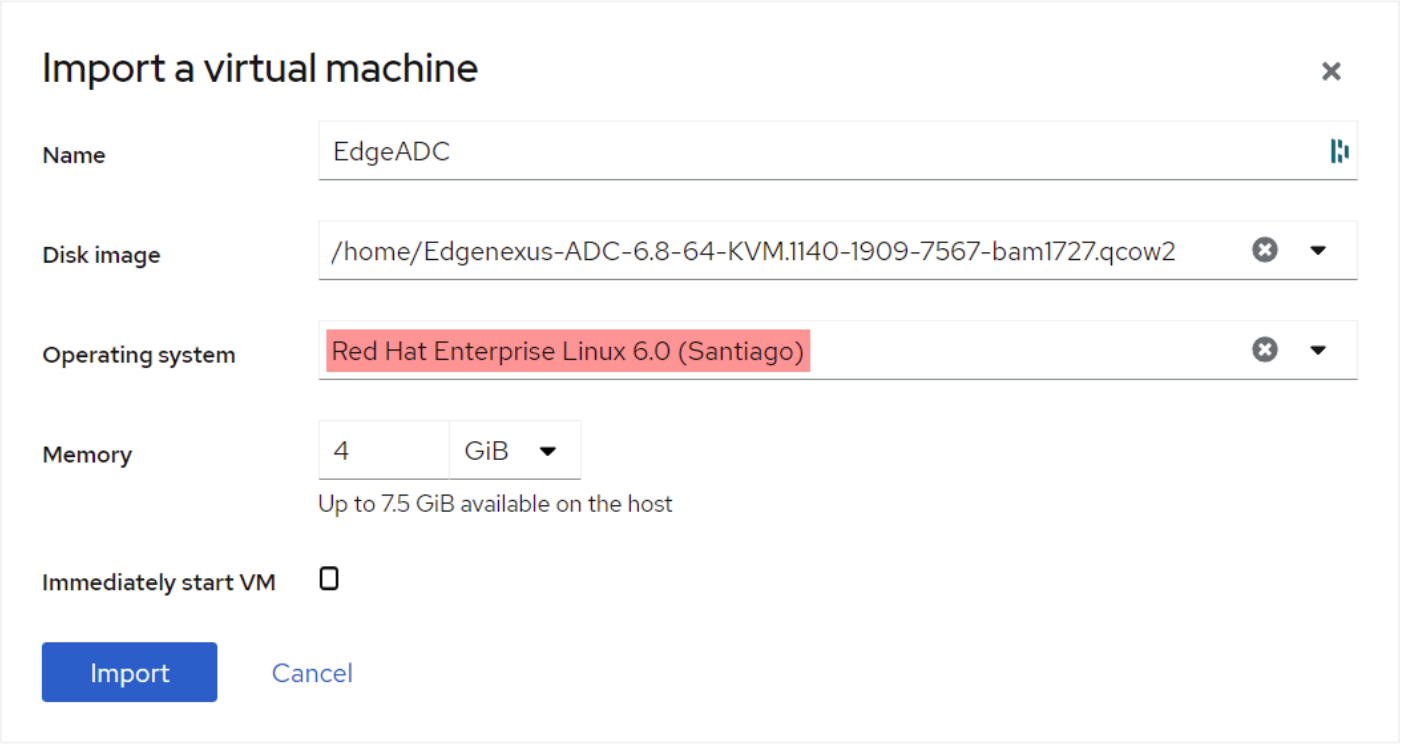
Les conseils ci-dessous ne couvrent pas l'installation du KVM ni sa mise en réseau.

Nous avons supposé que vous aviez téléchargé l'appliance virtuelle KVM et que vous l'aviez stockée sur l'hôte dans un endroit accessible.

- La première étape consiste à se connecter à la console Cockpit.

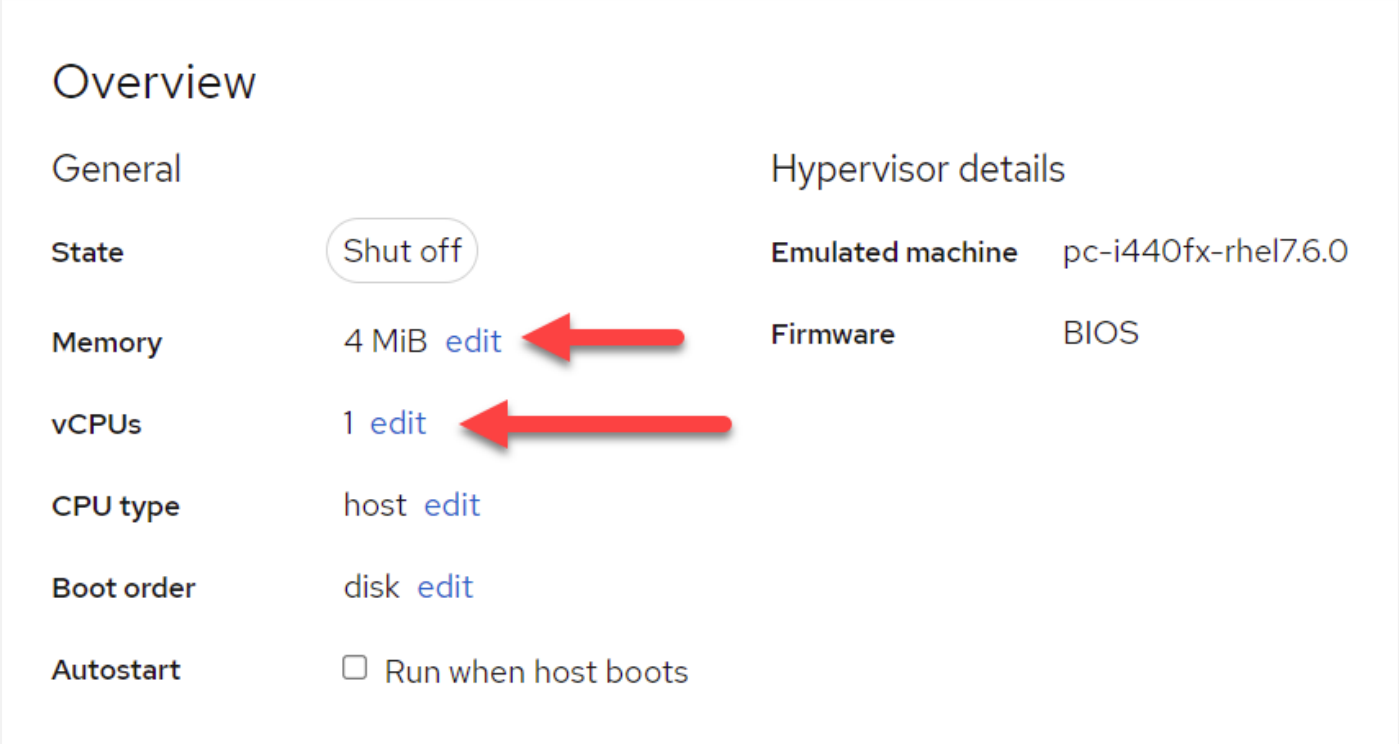


- Cliquez sur Importer VM
- La première boîte de dialogue vous permet de spécifier les détails de l'importation de l'appliance virtuelle. Voir l'image ci-dessous pour le contenu des champs. Vous devez spécifier Red Hat Enterprise 6.0 comme système d'exploitation.

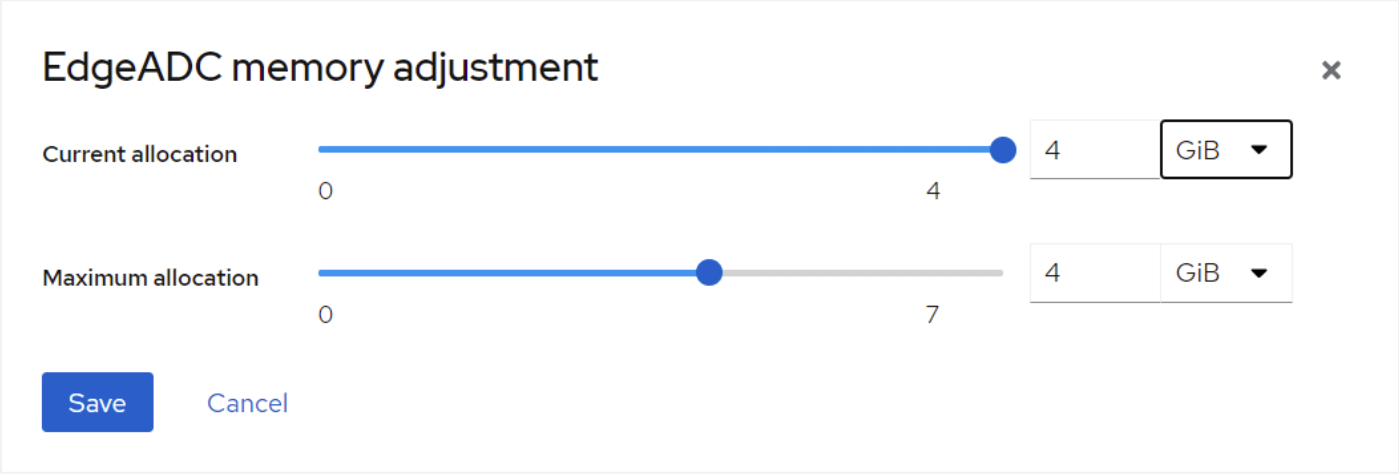


- Assurez-vous que la case "Démarrer immédiatement la VM" n'est pas cochée.

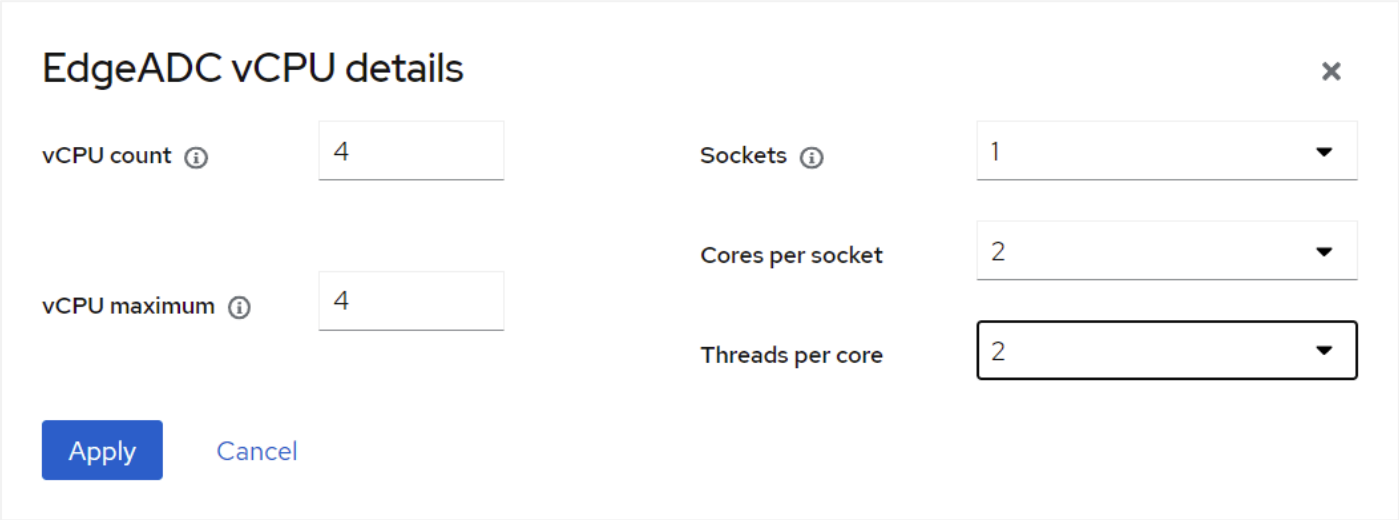
- Une fois que vous avez rempli les détails, cliquez sur le bouton "Importer".
- L'étape suivante consiste à spécifier l'allocation de vCPU et de mémoire que vous souhaitez utiliser.



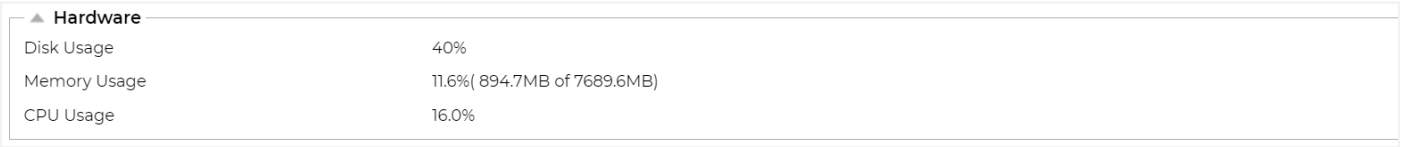
- Pour allouer la mémoire, vous verrez apparaître une boîte de dialogue similaire à celle ci-dessous.



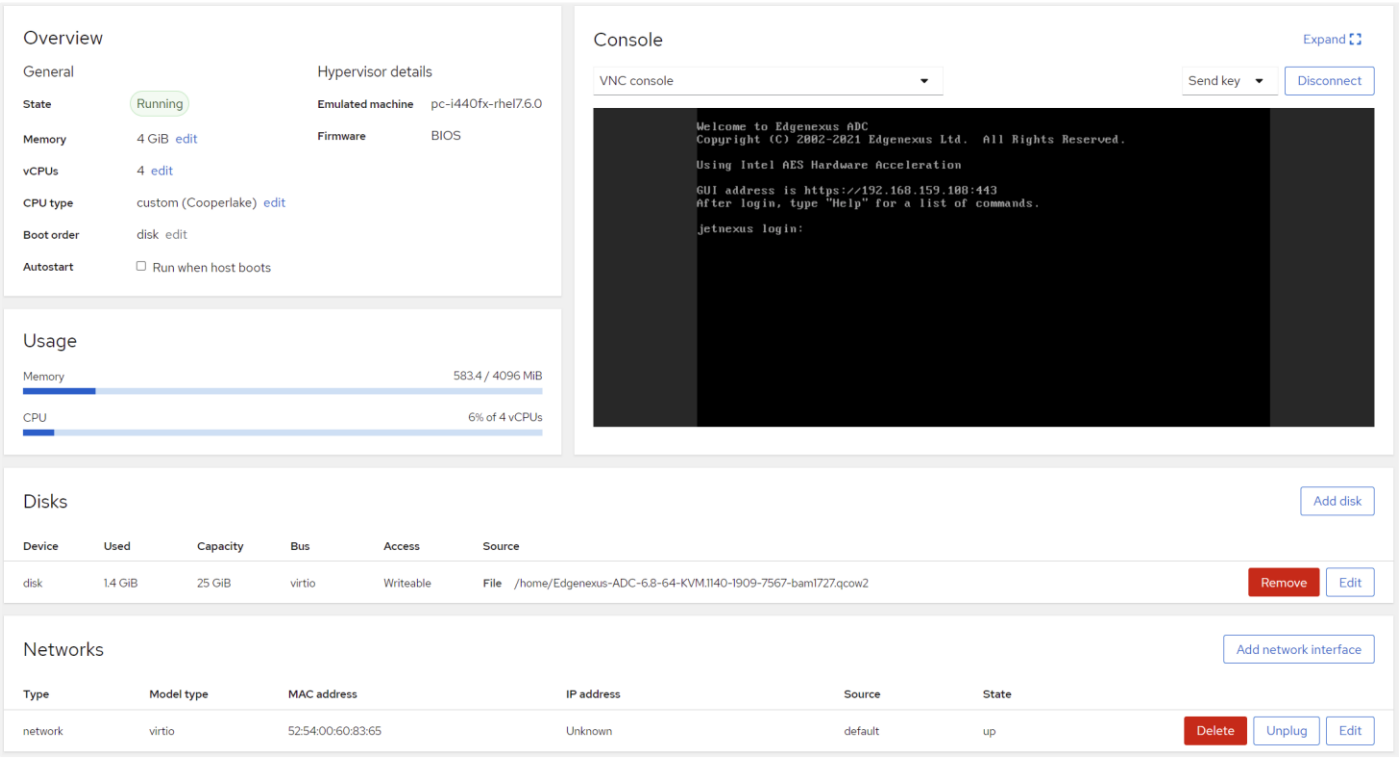
- Pour allouer la vCPU, vous verrez une boîte de dialogue similaire à celle ci-dessous.



- Les choix que nous avons faits ne sont que des exemples, mais ils sont réalisables, à moins que vous n'utilisiez un débit élevé avec le recryptage SSL, auquel cas vous devrez ajuster en conséquence en utilisant la section Matériel sous Affichage > Statistiques.



- Vous avez maintenant un ADC fonctionnel installé dans KVM. Voir l'image ci-dessous.



Installation sur Nutanix AHV

La section suivante montre comment installer l'EdgeADC sur une plateforme Nutanix AHV.

Exigences et versions

Ce guide s'applique à EdgeADC 4.2.6 et aux versions ultérieures.

Toutes les versions de l'hyperviseur Nutanix sont compatibles, mais la certification a été réalisée sur la version 5.10.9 de Nutanix.

- La première étape est de se connecter à Nutanix Prism Central.

Téléchargement de l'image EdgeADC

- Naviguer vers Infrastructure virtuelle > Images
- Cliquez sur le bouton Ajouter une image
- Sélectionnez le fichier image EdgeADC que vous avez téléchargé et cliquez sur le bouton Ouvrir pour télécharger l'image.
- Entrez un nom pour l'image dans le champ Description de l'image.
- Sélectionnez une catégorie appropriée
- Sélectionnez l'image et cliquez sur la flèche droite.
- Sélectionnez Toutes les images et cliquez sur Enregistrer.

Création de la VM

- Naviguer vers Infrastructure virtuelle > VMs
- Cliquez sur le bouton Créer une VM
- Saisissez un nom pour la VM, le nombre de CPU que vous souhaitez avoir et le nombre de cœurs que vous souhaitez allouer à la VM.
- Faites ensuite défiler la boîte de dialogue vers le bas et entrez la quantité de mémoire que vous souhaitez allouer à la VM. Vous pouvez commencer par 4 Go et augmenter cette quantité en fonction de l'utilisation.

Ajout du disque

- Ensuite, cliquez sur le lien Ajouter un nouveau disque
- Sélectionnez l'option Cloner à partir du service d'image dans le menu déroulant Opération.
- Sélectionnez l'image EdgeADC que vous avez ajoutée et cliquez sur le bouton Ajouter.
- Sélectionnez le disque qui servira de disque de démarrage.

Ajout du NIC, du réseau et de l'affinité

- Ensuite, cliquez sur le bouton Add New NIC. Vous aurez besoin de deux NIC.
- Sélectionnez le réseau et cliquez sur le bouton Ajouter
- Cliquez sur le bouton Définir l'affinité
- Sélectionnez les hôtes Nutanix sur lesquels la VM est autorisée à fonctionner, puis cliquez sur le bouton Enregistrer.
- Vérifiez les paramètres que vous avez définis et cliquez sur le bouton Enregistrer.

Mise sous tension de la VM

- Dans la liste des VM, cliquez sur le nom de la VM que vous venez de créer.
- Cliquez sur le bouton de mise sous tension de la VM
- Une fois la VM sous tension, cliquez sur le bouton Lancer la console.

Configuration de la mise en réseau EdgeADC

- Suivez les instructions de la section Premier environnement d'amorçage.
- Le EdgeADC est maintenant prêt à l'emploi et vous pourrez accéder à son interface graphique à l'aide de votre navigateur et de l'adresse IP de gestion.

Installation sur ProxMox

L'installation sur ProxMox est simple mais nécessite quelques étapes supplémentaires.

Nous utiliserons la version OVA de VMWare pour l'installation. Il s'agit d'un processus en plusieurs étapes qui nécessite une connaissance des commandes shell dans ProxMox. Cependant, nous avons fait en sorte que les instructions soient aussi faciles à suivre que possible. Nous partons du principe que vous connaissez ProxMox et n'allons donc pas approfondir les fonctionnalités de ProxMox.

Téléchargement de l'OVA sur ProxMox

Comme nous utilisons une version OVA, nous devons d'abord télécharger l'OVA sur ProxMox.

- Se connecter à la console ProxMox
- Créez un dossier appelé OVA_Import.
- Vous devez maintenant utiliser un client SFTP tel que WinSCP (Windows) ou CyberDuck (Mac) pour transférer le fichier OVA.
- Une fois le fichier transféré, vous le verrez dans le dossier que vous avez créé.
- Tapez la commande suivante pour extraire le contenu du fichier OVA.
- Tar xvf {nom de fichier}. Voir l'exemple ci-dessous.

```
tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
```

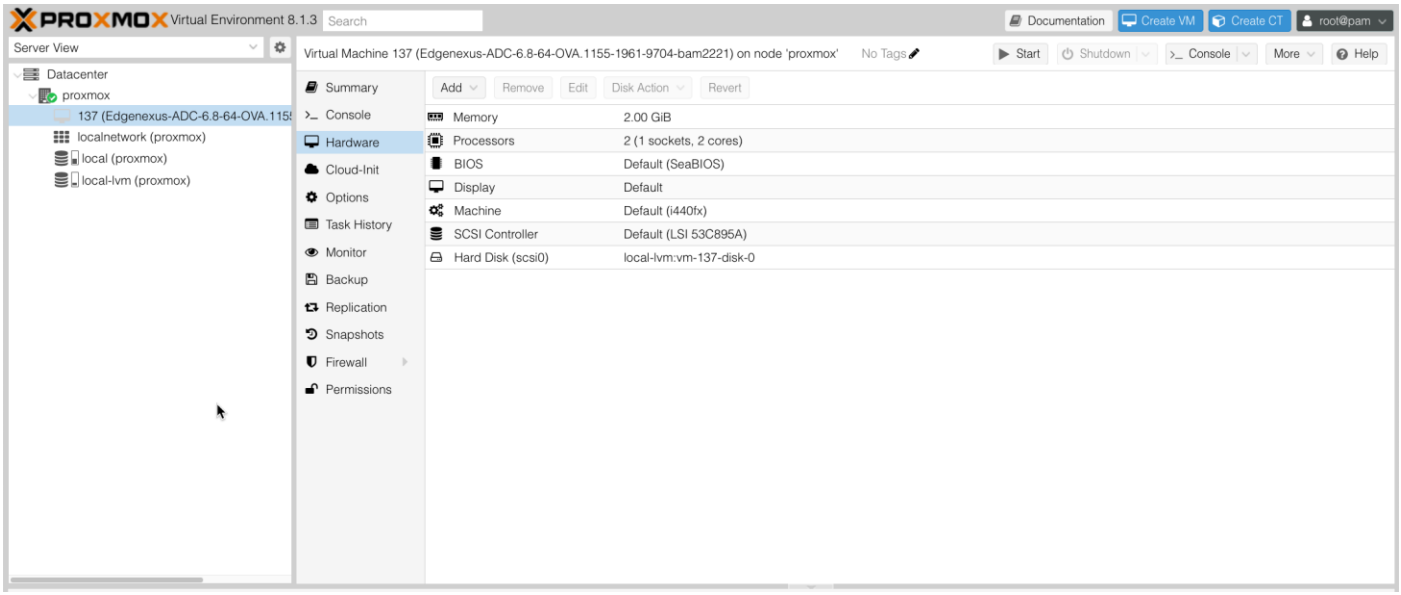
- Une fois extrait, vous devriez voir quelque chose comme l'exemple ci-dessous.

```
root@proxmox:~/OVA_Import# ls
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
root@proxmox:~/OVA_Import# tar xvf Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ova
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.ovf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221.mf
Edgenexus-ADC-6.8-64-OVA.1155-1961-9704-bam2221-disk1.vmdk
root@proxmox:~/OVA_Import#
```

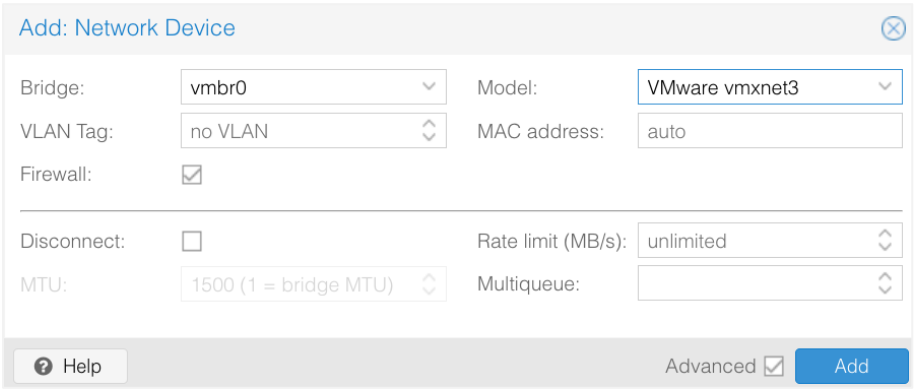
- Il y a trois fichiers. Les fichiers .ovf et .mf représentent la configuration. Le fichier .vmdk est le disque virtuel contenant l'ADC.
- L'étape suivante consiste à importer le VMDK dans ProxMox et à créer la machine virtuelle.
- Tapez la commande suivante pour créer la machine virtuelle à l'aide des fichiers de configuration.

```
qm importovf 137 ./{filename.ovf} local-lvm --format qcow2
```

- Dans cet exemple, nous avons donné un ID de 100, mais cela peut être différent pour votre installation si vous avez déjà des machines virtuelles créées dans ProxMox. Vous pouvez déterminer l'ID suivant en lançant le processus de création de machines virtuelles dans ProxMox, ou en choisissant un nombre supérieur à 100 qui soit hors de portée.
- La VM est maintenant créée.



- L'étape suivante consiste à ajouter une interface réseau à la VM.
- Cliquez sur Matériel dans le panneau de droite.
- Cliquez sur Ajouter et choisissez une interface réseau.



- Configurez-le comme le montre l'image ci-dessus. Il est important de choisir le modèle VMware vmxnet3.
- Cliquez sur Ajouter une fois la configuration effectuée.
- Vous pouvez ajouter des adaptateurs réseau en fonction de vos besoins.
- Vous pouvez maintenant démarrer la VM et suivre les instructions du chapitre Configuration du premier démarrage.

Configuration du premier démarrage

Lors du premier démarrage, l'ADC (également appelé VA ci-dessous) affiche l'écran suivant demandant la configuration pour les opérations de production.

Premier démarrage - Détails manuels du réseau

Lors du premier démarrage, vous disposez de 10 secondes pour interrompre l'attribution automatique des données IP via DHCP.

Pour interrompre ce processus, cliquez sur la fenêtre de la console et appuyez sur n'importe quelle touche. Vous pouvez alors saisir manuellement les données suivantes.

- Adresse IP
- Masque de sous-réseau
- Passerelle
- Serveur DNS

Ces modifications sont persistantes et survivent à un redémarrage ; il n'est pas nécessaire de les configurer à nouveau sur l'AV.

Premier démarrage - DHCP réussi

Si vous n'interrompez pas le processus d'attribution du réseau, votre CDA contactera un serveur DHCP après un délai d'attente pour obtenir les détails de son réseau. Si le contact est réussi, les informations suivantes seront attribuées à votre machine.

- Adresse IP
- Masque de sous-réseau
- Passerelle par défaut
- Serveur DNS

Nous vous conseillons de n'utiliser l'ADC avec une adresse DHCP que si cette adresse IP est liée en permanence à l'adresse MAC de l'ADC dans le serveur DHCP. Nous conseillons toujours d'utiliser une **ADRESSE IP FIXE** lors de l'utilisation des appliances virtuelles. Suivez les étapes de la section CHANGEMENT DE L'ADRESSE IP DE GESTION et des sections suivantes jusqu'à ce que vous ayez terminé la configuration du réseau.

Premier démarrage - Échec du DHCP

Si vous n'avez pas de serveur DHCP ou si la connexion échoue, l'adresse IP 192.168.100.100 sera attribuée.
L'adresse IP sera incrémentée de 1 jusqu'à ce que l'AV trouve une adresse IP libre. De même, l'AV

vérifiera si l'adresse IP est en cours d'utilisation et, si c'est le cas, elle sera à nouveau incrémentée et revérifiée.

Changement de l'adresse IP de gestion

Vous pouvez modifier l'adresse IP de l'AV à tout moment en utilisant la commande **set greenside=n.n.n.n.n,** comme indiqué ci-dessous.

```
set greenside={adresse IP}
```

Modification du masque de sous-réseau pour eth0

Les interfaces réseau utilisent le préfixe "eth" ; l'adresse réseau de base est appelée eth0. Le masque de sous-réseau ou masque de réseau peut être modifié à l'aide de la commande **set mask [NIC] [MASK]**. Vous pouvez voir un exemple ci-dessous.

```
set mask eth0 {mask}
```

Attribution d'une passerelle par défaut

L'AV a besoin d'une passerelle par défaut pour ses opérations. Pour définir la passerelle par défaut, utilisez la commande **route add default gw [GATEWAY IP]** comme indiqué dans l'exemple ci-dessous.

```
route add default gw {adresse IP}
```

Vérification de la valeur de la passerelle par défaut

Pour vérifier si la passerelle par défaut a été ajoutée et si elle est correcte, utilisez la commande **route**. Cette commande affiche les itinéraires du réseau et la valeur de la passerelle par défaut. Voir l'exemple ci-dessous.

```
Command:route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
255.255.255.255 *               255.255.255.255 UH    0      0        0 eth0
192.168.101.0   *               255.255.255.0   U     0      0        0 eth0
default         192.168.101.254 0.0.0.0         UG    0      0        0 eth0
```

Vous pouvez maintenant accéder à l'interface utilisateur graphique (GUI) pour configurer le CDA en vue d'une utilisation en production ou en évaluation.

Accès à l'interface web

Vous pouvez utiliser n'importe quel navigateur Internet avec JavaScript pour configurer, surveiller et déployer le CDA en vue d'une utilisation opérationnelle.

Dans le champ URL du navigateur, tapez **HTTPS://{adresse IP} ou HTTPS://{FQDN}.**

Par défaut, l'ADC utilise un certificat SSL auto-signé. Vous pouvez modifier l'ADC pour qu'il utilise le certificat SSL de votre choix.

Une fois que votre navigateur atteint l'ADC, il vous montrera l'écran de connexion. Les informations d'identification par défaut de l'ADC sont les suivantes :

Username: admin / Pwd: jetnexus

Tableau de référence des commandes

Commandement	Paramètre1	Paramètre2	Description	Exemple
date			Affiche la date et l'heure configurées actuellement	Tue Sept 3 13:00 UTC 2013
Défauts			Attribuer les paramètres d'usine par défaut à votre appareil	
sortie			Déconnexion de l'interface de ligne de commande	
aider			Affiche toutes les commandes valides	
ifconfig	[en blanc].		Visualiser la configuration de l'interface pour toutes les interfaces	ifconfig
	eth0		Visualiser la configuration de l'interface eth0 uniquement	ifconfig eth0
numéro d'identification de la machine (machineid)			Cette commande fournira l'identifiant de la machine utilisée pour accorder une licence à l'ADC ADC	EF4-3A35-F79
quitter			Déconnexion de l'interface de ligne de commande	
redémarrage			Mettre fin à toutes les connexions et redémarrer l'ADC ADC	redémarrage
redémarrer			Redémarrer les services virtuels ADC ADC	
itinéraire	[en blanc].		Afficher la table de routage	itinéraire
	ajouter	par défaut gw	Ajouter l'adresse IP de la passerelle par défaut	route add default gw 192.168.100.254
fixer	bord de verdure		Définir l'adresse IP de gestion de l'ADC	set greenside=192.168.101.1
	masque		Définit le masque de sous-réseau d'une interface. Les noms d'interface sont eth0, eth1....	set mask eth0 255.255.255.0
montrer			Affiche les paramètres de configuration globale	
arrêt			Mettre fin à toutes les connexions et mettre l'ADC hors tension ADC	
statut			Affiche les statistiques de données actuelles	
sommet			Afficher les informations sur le processus, telles que l'unité centrale et la mémoire	
viewlog	messages		Affiche les messages syslog bruts	Consulter les messages du journal

Remarque : les commandes ne sont pas sensibles à la casse. Il n'y a pas d'historique des commandes.

La console Web

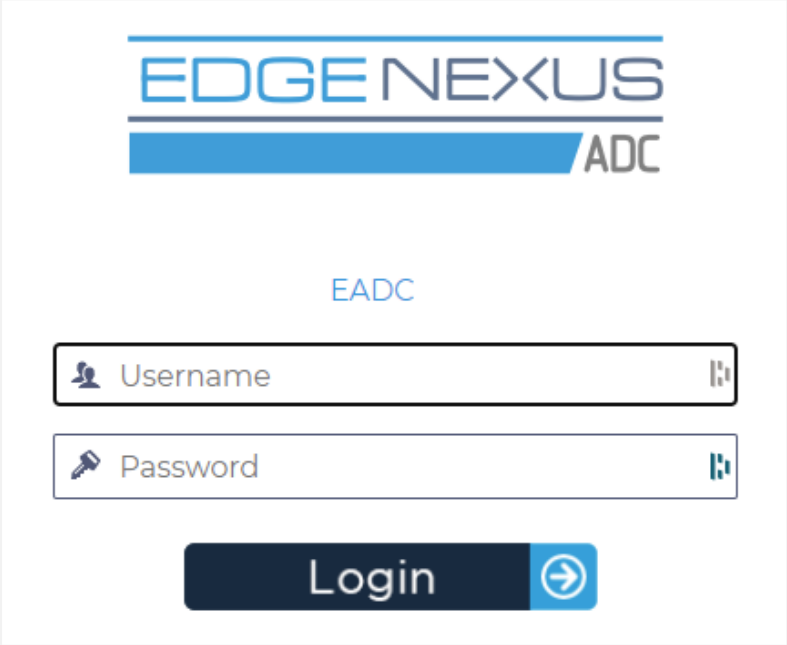
Lancement de la console Web ADC

Toutes les opérations sur l'ADC sont configurées et effectuées à l'aide de la console web. La console web est accessible à l'aide de n'importe quel navigateur avec JavaScript.

Pour lancer la console web de l'ADC, entrez l'URL ou l'adresse IP de l'ADC dans le champ URL. Nous prendrons l'exemple de adc.company.com :

https://adc.company.com

Une fois lancée, la console web de l'ADC se présente comme suit, vous permettant de vous connecter en tant qu'utilisateur administrateur.



Informations d'identification par défaut

Les identifiants de connexion par défaut sont les suivants

Username: admin / Pwd: jetnexus

Vous pouvez modifier cela à tout moment à l'aide de la configuration de l'utilisateur située dans *Système* > *Utilisateurs*.

Une fois que vous avez réussi à vous connecter, le tableau de bord principal de l'ADC s'affiche à l'écran.

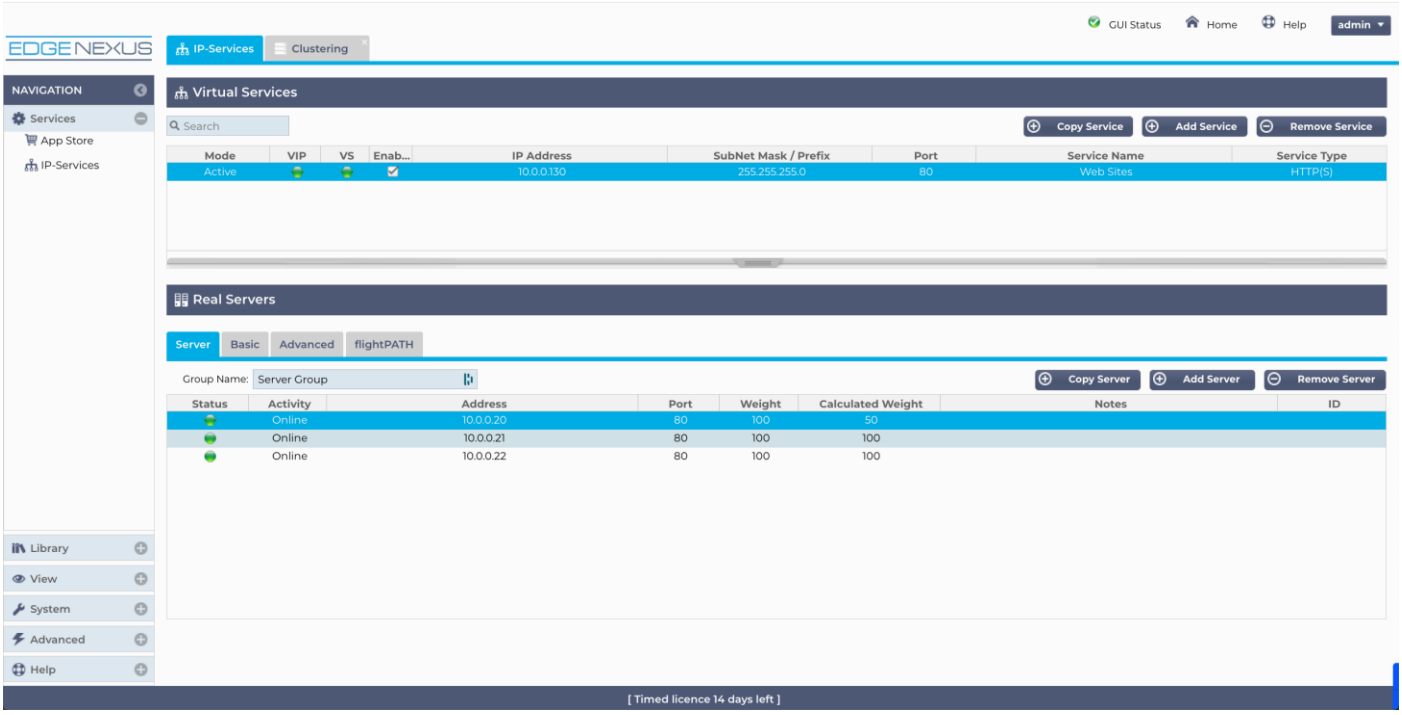
Utilisation d'un service d'authentification externe

Si vous souhaitez utiliser un service d'authentification externe, vous pouvez le faire en configurant un serveur d'authentification et un service d'authentification.

Des informations à ce sujet sont disponibles à l'Authentification et à l'Service d'authentification

Le tableau de bord principal

L'image ci-dessous illustre le tableau de bord principal ou "page d'accueil" de l'ADC. Il se peut que nous apportions occasionnellement quelques modifications pour l'améliorer, mais toutes les fonctions seront conservées.



La section Navigation sur le côté gauche vous permet de naviguer dans les différentes zones des fonctionnalités de l'ADC. Par défaut, la section Services est sélectionnée et la sous-section Services IP est ouverte, comme l'indique l'onglet situé au-dessus de la section Services virtuels. Cet onglet est fixe et toujours affiché.

Lorsque vous cliquez sur une section de la navigation, cette section est développée et son contenu est révélé. En cliquant sur une option dans une section, le contenu de la section s'ouvre sur le côté droit, et un onglet est placé en haut pour permettre de passer rapidement d'une option à l'autre.

Les différentes sections de navigation sont expliquées en détail dans les chapitres suivants.

Services

Services IP

La section Services IP de l'ADC vous permet d'ajouter, de supprimer et de configurer les différents services IP virtuels dont vous avez besoin pour votre cas d'utilisation particulier. Les paramètres et les options sont répartis dans les sections ci-dessous. Ces sections se trouvent à droite de l'écran de l'application.

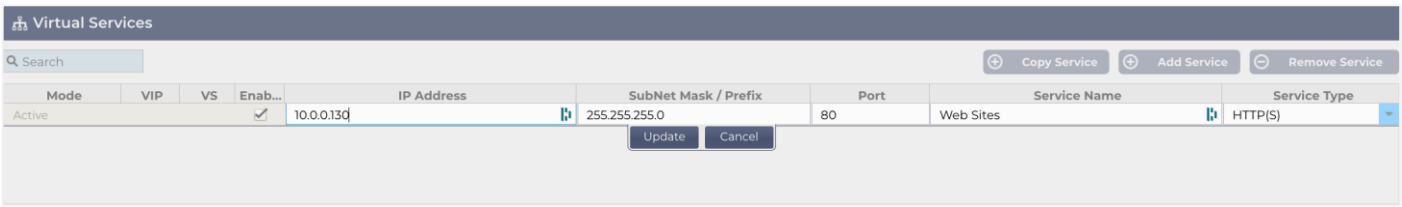
Services virtuels

Un service virtuel combine une IP virtuelle (VIP) et un port TCP/UDP sur lequel l'ADC est à l'écoute. Le trafic arrivant à l'IP virtuelle est redirigé vers l'un des serveurs réels associés à ce service. L'adresse IP virtuelle ne peut pas être la même que l'adresse de gestion de l'ADC, c'est-à-dire eth0, eth1 etc...

L'ADC détermine comment le trafic est redistribué aux serveurs en fonction d'une politique d'équilibrage de la charge définie dans l'onglet Basic de la section Real Servers.

Création d'un nouveau service virtuel à l'aide d'un nouveau VIP

- Cliquez sur le bouton Ajouter un service virtuel comme indiqué ci-dessus.



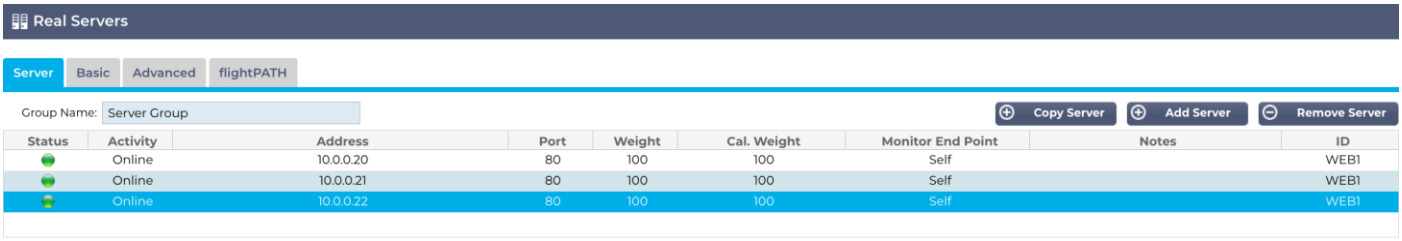
Vous entrez alors dans le mode d'**édition de la ligne.**

- Remplissez les quatre champs surlignés pour continuer, puis cliquez sur le bouton de mise à jour.

Veuillez utiliser la touche TAB pour naviguer dans les champs.

Champ d'application	Description
Adresse IP	Saisissez une nouvelle adresse IP virtuelle qui servira de point d'entrée cible pour l'accès au serveur réel. C'est vers cette adresse IP que les utilisateurs ou les applications se dirigeront pour accéder à l'application à charge équilibrée.
Masque de sous-réseau/Préfixe	Ce champ contient le masque de sous-réseau correspondant au réseau sur lequel se trouve le CDA.
Port	Le port d'entrée utilisé pour accéder au VIP. Cette valeur ne doit pas nécessairement être la même que celle du serveur réel si vous utilisez un proxy inverse.
Nom du service	Le nom du service est une représentation textuelle de l'objectif du VIP. Il est facultatif, mais nous vous recommandons de l'indiquer pour plus de clarté. Notez que ce champ est utilisé à d'autres fins spécifiques lors de l'utilisation de GSLB.
Type de service	Il existe de nombreux types de services différents que vous pouvez sélectionner. Les types de service de la couche 4 ne peuvent pas utiliser la technologie flightPATH.

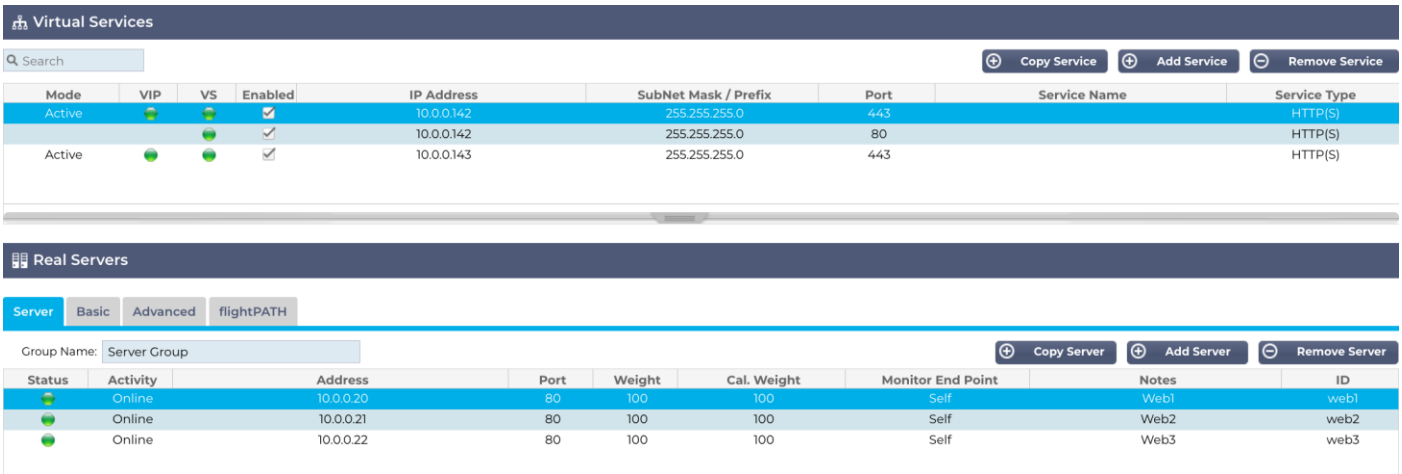
Vous pouvez maintenant appuyer sur le bouton "Update" pour enregistrer cette section et passer automatiquement à la section "Real Server" détaillée ci-dessous :



Champ d'application	Description
Activité	Le champ Activité permet d'afficher et de modifier l'état du serveur réel à équilibrage de charge. En ligne - Indique que le serveur est actif et qu'il reçoit des demandes d'équilibrage de charge. Hors ligne - Le serveur est hors ligne et ne reçoit pas de demandes. Drain - Le serveur a été placé en mode drain afin que la persistance puisse être vidée et que le serveur soit déplacé vers un état hors ligne sans affecter les utilisateurs. Standby - Le serveur a été placé en état de veille.
Adresse IP	Cette valeur est l'adresse IP du serveur Real. Elle doit être exacte et ne doit pas être une adresse DHCP.
Port	Le port cible d'accès sur le serveur réel. En cas d'utilisation d'un proxy inverse, ce port peut être différent du port d'entrée spécifié sur le VIP.
Pondération	Ce paramètre est généralement configuré automatiquement par l'ADC. Vous pouvez le modifier si vous souhaitez changer la pondération de la priorité.
Cal. Poids	Si vous laissez la pondération à sa valeur par défaut, l'ADC calculera automatiquement la pondération en fonction des temps de réponse.
Point final du moniteur	La valeur par défaut est "Self". Vous pouvez toutefois la remplacer par une valeur de port ou par une adresse IP:port. Ce champ est utilisé pour surveiller un autre point de terminaison et déterminer si le trafic doit être transmis au service virtuel. VoirComment utiliser Monitor End Point ci-dessous.

- Cliquez sur le bouton "Mise à jour" ou appuyez sur "Entrée" pour enregistrer vos modifications.
- Le voyant d'état devient d'abord gris, puis vert si le contrôle de santé du serveur réussit. Il devient rouge si le Real Server Monitor échoue.
- Un serveur dont le voyant d'état est rouge n'est pas équilibré.

Exemple d'un service virtuel achevé

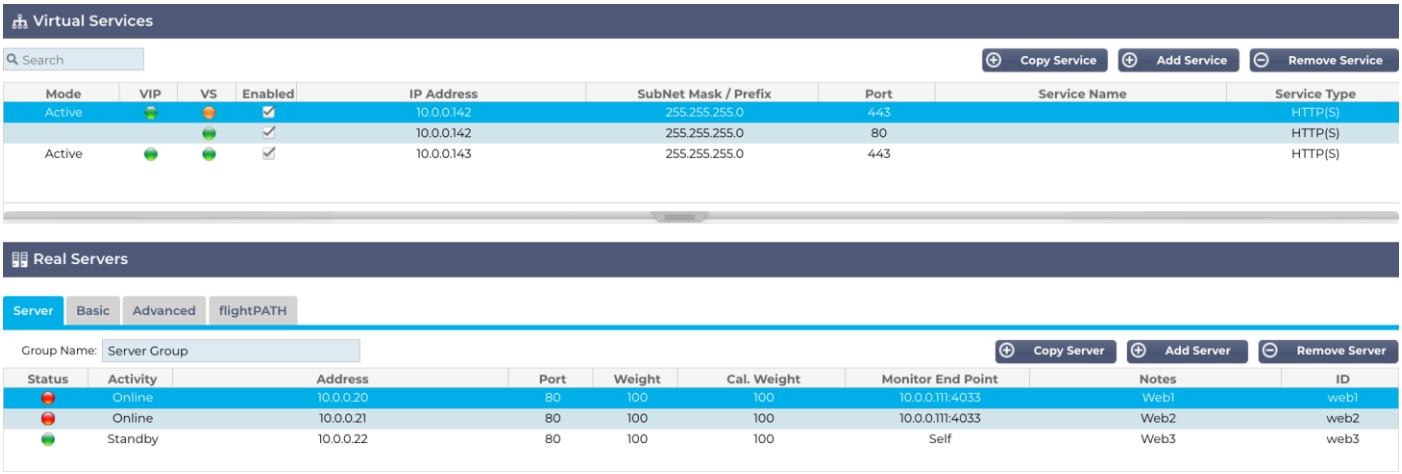


Comment utiliser Monitor End Point

Exemple 1

Prenons l'exemple d'une infrastructure comprenant deux serveurs web à charge équilibrée qui fournissent une application web à l'utilisateur final. L'application web est connectée à un serveur de base de données en arrière-plan. L'accès au serveur de base de données est interrompu, mais les serveurs d'application web restent opérationnels. Les utilisateurs essaient d'utiliser l'application web et reçoivent des erreurs.

La solution consiste à utiliser Monitor End Point.



- L'exemple montre deux serveurs web, 10.0.0.20 et 10.0.0.21, ainsi qu'un troisième serveur web 10.0.0.22. Le serveur 10.0.0.22 a été placé en mode veille.
- Les deux serveurs web actifs ont été configurés avec une valeur de point final de surveillance de 10.0.0.111:4033, qui est l'adresse IP et le port de connexion du serveur de base de données.
- Si la connexion au serveur de base de données devait être interrompue, les deux serveurs actifs seraient mis hors ligne et le serveur de secours serait mis en ligne, affichant une page web qui pourrait informer le client que les systèmes sont en cours de maintenance.

Exemple 2

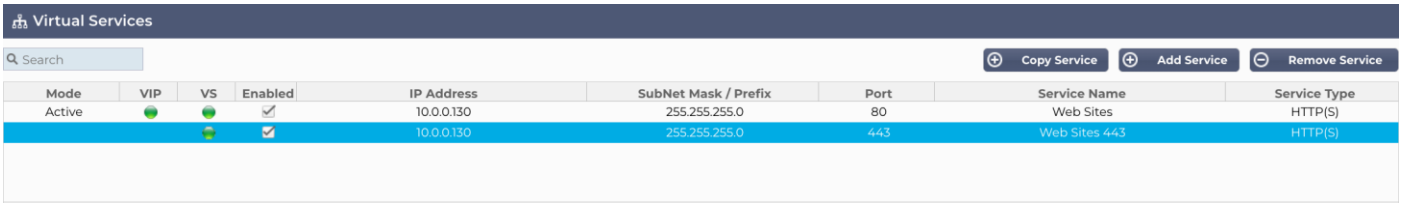
Un autre exemple d'utilisation de Monitor End Point est celui de l'équilibrage de charge des serveurs de protocole UDP, tels que Always-On-VPN. Comme vous le savez peut-être, les ports UDP ne sont pas surveillés de manière fiable, et il est donc nécessaire de surveiller un port TCP.

L'utilisation de Monitor End Point nous permet justement de le faire. Le port principal utilisé par les serveurs Always-on-VPN sera 53/udp, mais vous surveillerez, par exemple, 8433/tcp. Dans ce cas, il vous suffit de saisir la valeur du port dans le champ Monitor End Point.

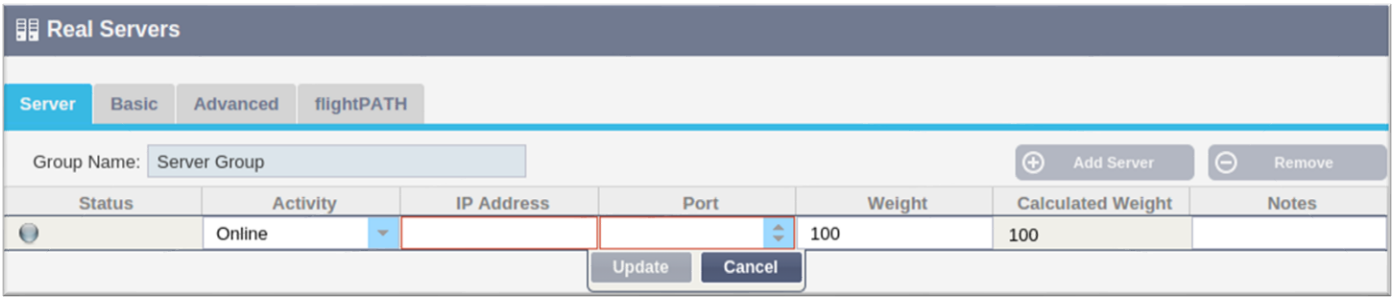
Création de sous-services virtuels

Vous pouvez également avoir des services sous-virtuels dans les cas où vous avez besoin d'équilibrer la charge en utilisant différents ports sur le même VIP. Par exemple, vous pouvez avoir des serveurs accédés par la même IP virtuelle sur les ports 80, 8088 et 443, et vous devrez donc créer des services sous-virtuels pour répondre à ce besoin.

- Mettez en surbrillance le service virtuel que vous souhaitez copier.
- Cliquez sur Add Virtual Service (Ajouter un service virtuel) pour entrer dans le mode d'édition des rangées.



- L'adresse IP et le masque de sous-réseau sont copiés automatiquement.
- Saisissez le numéro de port de votre service.
- Saisir un nom de service facultatif
- Sélectionnez un type de service.
- Vous pouvez maintenant appuyer sur le bouton "Update" pour enregistrer cette section et passer automatiquement à la section "Real Server" ci-dessous.

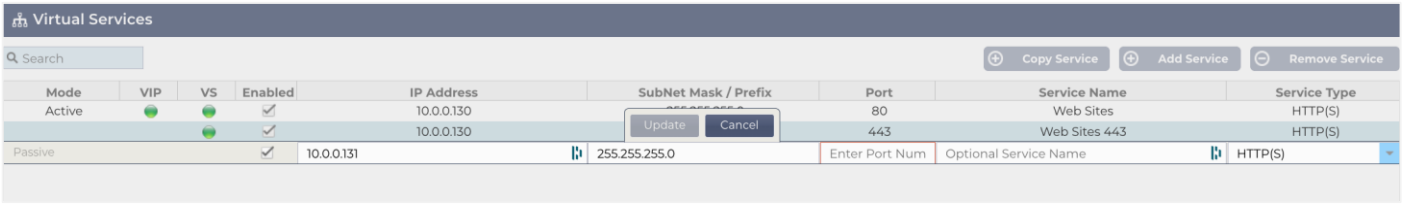


- Laissez l'option Activité du serveur sur Online - cela signifie qu'il sera équilibré en charge s'il passe le contrôle de santé par défaut de TCP Connect. Ce paramètre peut être modifié ultérieurement si nécessaire.
- Entrez une adresse IP pour le Real Server
- Saisir un numéro de port pour le serveur réel
- Entrez un nom facultatif pour le serveur réel dans le champ Notes. N'oubliez pas que ce champ de notes est utilisé à d'autres fins spécifiques, par exemple dans les variables flightPATH, etc.
- Cliquez sur Mettre à jour pour enregistrer vos modifications.
- Le voyant d'état devient d'abord gris, puis vert si le Real Server Monitor réussit. Il devient rouge si le Real Server Monitor échoue.
- Un serveur dont le voyant d'état est rouge ne sera pas équilibré.

Changer l'adresse IP d'un service virtuel

Vous pouvez à tout moment modifier l'adresse IP d'un service virtuel ou d'un VIP existant.

- Mettez en surbrillance le service virtuel dont vous souhaitez modifier l'adresse IP.
- Cliquez sur le champ de l'adresse IP de ce service pour le rendre modifiable.



- Remplacer l'adresse IP par celle que vous souhaitez utiliser
- Cliquez sur le bouton Mettre à jour pour enregistrer les modifications.

Remarque : La modification de l'adresse IP d'un service virtuel entraîne la modification de l'adresse IP de tous les services associés au VIP.

Création d'un nouveau service virtuel à l'aide de Copy Service

- Le bouton Copier le service permet de copier un service entier, y compris tous les serveurs réels, les paramètres de base, les paramètres avancés et les règles flightPATH qui lui sont associés.
- Mettez en évidence le service que vous souhaitez dupliquer et cliquez sur Copier le service.
- L'éditeur de ligne apparaît avec un curseur clignotant sur la colonne Adresse IP.
- Vous devez modifier l'adresse IP pour qu'elle soit unique ou, si vous souhaitez conserver l'adresse IP, vous devez modifier le port pour qu'il soit unique à cette adresse IP.

N'oubliez pas de modifier chaque onglet si vous changez un paramètre tel qu'une stratégie d'équilibrage de charge, le moniteur Real Server ou si vous supprimez une règle flightPATH.

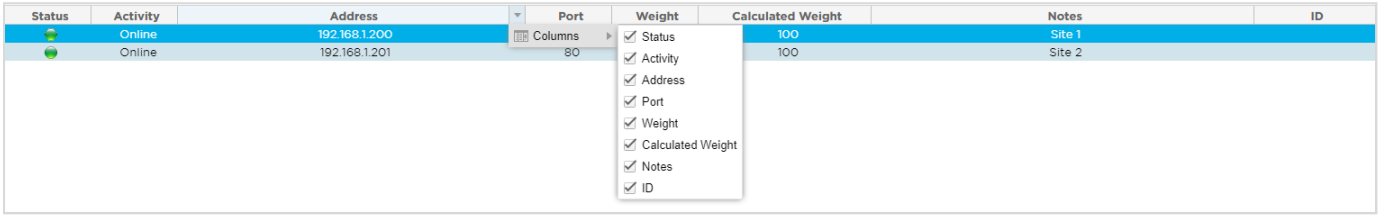
Filtrage des données affichées

Recherche d'un terme spécifique

La boîte de recherche vous permet d'effectuer une recherche dans le tableau en utilisant n'importe quelle valeur, comme les octets de l'adresse IP ou le nom du service.

Sélection de la visibilité des colonnes

Vous pouvez également sélectionner les colonnes que vous souhaitez afficher dans le tableau de bord.



- Déplacez la souris sur l'une des colonnes
- Une petite flèche apparaît sur le côté droit de la colonne.
- En cliquant sur les cases à cocher, vous sélectionnez les colonnes que vous souhaitez voir apparaître dans le tableau de bord.

Comprendre les colonnes de services virtuels

Primaire/Mode

La colonne Mode indique le rôle de haute disponibilité sélectionné pour le VIP actuel. Pour connaître les modes, voir Système > Clustering>Rôles.

Option	Description
Actif	En mode Cluster, la valeur de ce champ est Active. Lorsque vous avez une paire d'appliances ADC HA dans votre centre de données, l'une d'entre elles indiquera Active et l'autre Passive. Si l'appliance actuelle
Passif	Lorsque l'ADC agit en tant que membre secondaire d'un cluster, la colonne Mode indique Passif.
Manuel	Le rôle manuel permet à la paire de CDA de fonctionner en mode actif-actif pour différentes adresses IP virtuelles. Dans ce cas, la colonne Primaire contient une case à côté de chaque adresse IP virtuelle unique qui peut être sélectionnée pour le mode actif ou laissée décochée pour le mode passif.
Autonome	L'ADC agit en tant que dispositif autonome et n'est pas en mode haute disponibilité. La colonne Primaire indique donc "Autonome".

VIP

Cette colonne fournit des informations visuelles sur l'état de chaque service virtuel. Les indicateurs sont codés par couleur et sont les suivants :

LED	Signification
●	En ligne
●	Failover-Standby. Ce service virtuel est en attente à chaud
●	Indique qu'un "secondaire" attend un "primaire".
●	Le service a besoin d'attention. Cette indication peut résulter de l'échec d'un contrôle de santé d'un serveur réel ou d'un passage manuel à l'état hors ligne. Le trafic continuera à circuler mais avec une capacité réduite du serveur réel.
●	Hors ligne. Les serveurs de contenu sont inaccessibles ou aucun serveur de contenu n'est activé.
●	État des recherches
●	Pas de licence ou IP virtuelles sous licence dépassées

Activé

Cette option est activée par défaut et la case est cochée. Vous pouvez désactiver le service virtuel en double-cliquant sur la ligne, en décochant la case, puis en cliquant sur le bouton Mettre à jour.

Adresse IP

Ajoutez votre adresse IPv4 en notation décimale pointée ou une adresse IPv6. Cette valeur est l'adresse IP virtuelle (VIP) pour votre service. Exemple IPv4 "192.168.1.100". Exemple Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Masque de sous-réseau/Préfixe

Ajoutez votre masque de sous-réseau en notation décimale pointée. Exemple : "255.255.255.0". Vous pouvez également utiliser la valeur du sous-réseau telle que /24, ou pour IPv6, ajouter votre préfixe. Pour plus d'informations sur l'IPv6, veuillez consulter **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Port

Ajoutez le numéro de port associé à votre service. Le port peut être un numéro de port TCP ou UDP. Exemple : TCP "80" pour le trafic Web et TCP "443" pour le trafic Web sécurisé. Vous pouvez également spécifier une plage de valeurs telles que 80-87.

Actuellement, il n'est pas possible d'utiliser des valeurs séparées par des virgules pour spécifier des valeurs de port non contiguës.

Nom du service

Ajoutez un nom convivial pour identifier votre service. Exemple : "Serveurs Web de production". Ce champ est également utilisé lors de l'utilisation de GSLB.

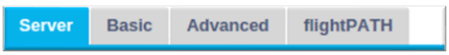
Type de service

Veuillez noter qu'avec tous les types de services de "couche 4", l'ADC n'interagit pas et ne modifie pas le flux de données, de sorte que flightPATH n'est pas disponible avec les types de services de couche 4. Les services de la couche 4 se contentent d'équilibrer le trafic en fonction de la politique d'équilibrage de la charge :

Type de service	Port/Protocole	Couche service	Commentaire
Couche 4 TCP	N'importe quel port TCP	Couche 4	L'ADC ne modifie aucune information dans le flux de données et procède à l'équilibrage standard du trafic conformément à la politique d'équilibrage de la charge.
Couche 4 UDP	N'importe quel port UDP	Couche 4	Comme pour le TCP de couche 4, l'ADC ne modifie aucune information dans le flux de données et effectue un équilibrage de charge standard du trafic conformément à la politique d'équilibrage de charge.
Couche 4 TCP/UDP	N'importe quel port TCP ou UDP	Couche 4	L'idéal est que votre service ait un protocole primaire tel que UDP, mais qu'il se rabatte sur TCP. L'ADC ne modifie aucune information dans le flux de données et effectue un équilibrage de charge standard du trafic conformément à la politique d'équilibrage de charge.
DNS	TCP/UDP	Couche 4	Utilisé pour équilibrer la charge des serveurs DNS.
HTTP(S)	Protocole HTTP ou HTTPS	Couche 7	L'ADC peut interagir, manipuler et modifier le flux de données à l'aide de flightPATH.
FTP	Protocole de transfert de fichiers	Couche 7	Utilisation de connexions de contrôle et de données séparées entre le client et le serveur
SMTP	Protocole de transfert de courrier simple	Couche 4	À utiliser lors de l'équilibrage de la charge des serveurs de messagerie
POP3	Protocole de la poste	Couche 4	À utiliser lors de l'équilibrage de la charge des serveurs de messagerie
IMAP	Protocole d'accès aux messages Internet	Couche 4	À utiliser lors de l'équilibrage de la charge des serveurs de messagerie
RDP	Protocole de bureau à distance	Couche 4	À utiliser lors de l'équilibrage de charge des serveurs Terminal Services
RPC	Appel de procédure à distance	Couche 4	À utiliser lors de l'équilibrage de la charge des systèmes utilisant des appels RPC
RPC/ADS	Exchange 2010 RPC statique pour le service de carnet d'adresses	Couche 4	A utiliser lors de l'équilibrage de charge des serveurs Exchange
RPC/CA/PF	Exchange 2010 RPC statique pour l'accès client et les dossiers publics	Couche 4	A utiliser lors de l'équilibrage de charge des serveurs Exchange
DICOM	Imagerie numérique et communications en médecine	Couche 4	À utiliser lors de l'équilibrage de la charge des serveurs utilisant des protocoles DICOM

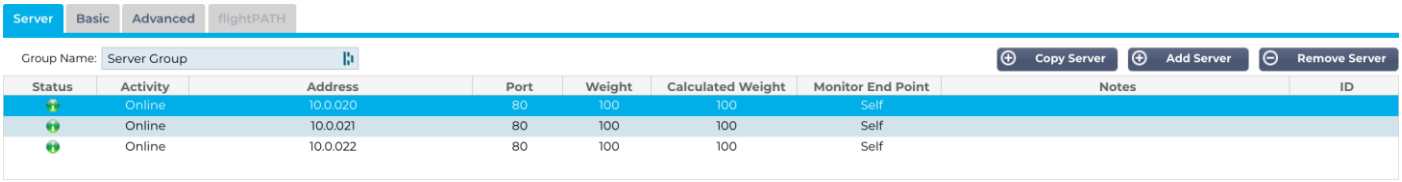
Serveurs réels

Il y a plusieurs onglets dans la section Serveurs réels du tableau de bord : Serveur, Basique, Avancé et flightPATH.



Serveur

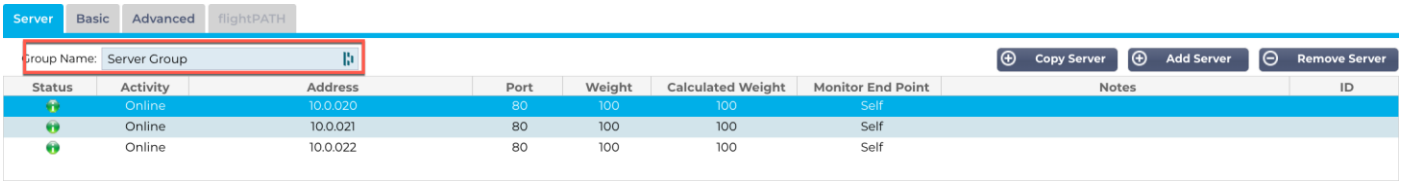
L'onglet Serveur contient les définitions des serveurs back-end réels associés au service virtuel sélectionné. Vous devez ajouter au moins un serveur à la section Serveurs réels.



Ajouter un serveur

- Sélectionnez le VIP approprié que vous avez défini précédemment.
- Cliquez sur Ajouter un serveur
- Une nouvelle ligne apparaît avec le curseur clignotant dans la colonne Adresse IP.
- Entrez l'adresse IPv4 de votre serveur en notation décimale pointée. Le serveur réel peut se trouver sur le même réseau que votre service virtuel, sur n'importe quel réseau local directement connecté ou sur n'importe quel réseau que votre CDA peut acheminer. Exemple "10.1.1.1".
- Passez à la colonne Port et entrez le numéro de port TCP/UDP de votre serveur. Le numéro de port peut être le même que le numéro de port du service virtuel ou un autre numéro de port pour la connectivité Reverse Proxy. L'ADC traduira automatiquement ce numéro.
- Passez à la section Notes pour ajouter tout détail pertinent concernant le serveur. Exemple : "Serveur Web IIS 1"

Nom du groupe



Lorsque vous avez ajouté les serveurs composant l'ensemble équilibré, vous pouvez également attacher un nom de groupe. Une fois ce champ modifié, le contenu est enregistré sans qu'il soit nécessaire d'appuyer sur le bouton Mettre à jour.

Voyants d'état du serveur Real

Vous pouvez voir le statut d'un serveur réel par la couleur de la colonne Statut. Voir ci-dessous :

LED	Signification
●	Connecté
◎	Non surveillé
●	Drainage
●	Hors ligne

●	En attente
●	Non connecté
●	État de la recherche
●	Pas de licence ou licence Real Servers dépassée

Activité

Vous pouvez à tout moment modifier l'activité d'un serveur réel en utilisant le menu déroulant. Pour ce faire, double-cliquez sur la ligne d'un serveur réel pour la mettre en mode édition.

Option	Description
En ligne	Tous les serveurs réels assignés en ligne recevront du trafic selon la politique d'équilibrage de charge définie dans l'onglet Basique.
Drainage	Tous les serveurs réels affectés à la vidange continueront à desservir les connexions existantes mais n'accepteront pas de nouvelles connexions. Le voyant d'état clignote en vert/bleu pendant la durée de la vidange. Une fois que les connexions existantes sont naturellement fermées, les serveurs réels sont mis hors ligne et le voyant d'état devient bleu fixe. Vous pouvez également visualiser ces connexions en vous rendant dans la section Navigation > Monitor > Status. Le comportement de vidange peut être modifié dans l'onglet Paramètres avancés.
Hors ligne	Tous les serveurs réels mis hors ligne seront immédiatement mis hors ligne et ne recevront aucun trafic.
En attente	Tous les serveurs réels définis comme étant en attente resteront hors ligne jusqu'à ce que **TOUS les** serveurs du groupe en ligne échouent à leurs contrôles de santé du serveur. Le trafic est reçu par le groupe en attente conformément à la politique d'équilibrage de la charge lorsque cela se produit. Si un serveur du groupe en ligne réussit le contrôle de santé du serveur, ce serveur en ligne recevra tout le trafic et le groupe en attente cessera de recevoir du trafic.

Adresse IP

Ce champ correspond à l'adresse IP de votre Real Server. Exemple "192.168.1.200".

Port

Numéro du port TCP ou UDP que le Real Server écoute pour le service. Exemple "80" pour le trafic Web.

Poids

Cette colonne devient modifiable lorsqu'une politique d'équilibrage de la charge appropriée est spécifiée.

Le poids par défaut d'un serveur réel est de 100, et vous pouvez entrer des valeurs comprises entre 1 et 100. Une valeur de 100 correspond à une charge maximale et une valeur de 1 à une charge minimale.

Un exemple pour trois serveurs peut ressembler à ceci :

- Serveur 1 Poids = 100
- Serveur 2 Poids = 50
- Serveur 3 Poids = 50

Si nous considérons que la politique d'équilibrage de la charge est définie sur Moins de connexions, et qu'il y a 200 connexions clients au total ;

- Le serveur 1 recevra 100 connexions simultanées
- Le serveur 2 recevra 50 connexions simultanées

- Le serveur 3 recevra 50 connexions simultanées

Si nous devions utiliser Round Robin comme méthode d'équilibrage de la charge, qui fait tourner les demandes à travers l'ensemble des serveurs équilibrés, la modification des poids affecte la fréquence à laquelle les serveurs sont choisis comme cible.

Si nous pensons que la politique d'équilibrage de la charge la plus rapide utilise le temps le plus court pour obtenir une réponse, l'ajustement des pondérations modifie le biais de la même manière que la politique des moindres connexions.

Poids calculé

Le poids calculé de chaque serveur peut être visualisé dynamiquement. Il est calculé automatiquement et n'est pas modifiable. Ce champ indique la pondération réelle qu'ADC utilise en tenant compte de la pondération manuelle et de la politique d'équilibrage de la charge.

Point final du moniteur

Cette fonction vous permet de spécifier des points d'extrémité particuliers à surveiller et de déterminer ainsi l'état de santé de l'entrée Real Server. Vous pouvez laisser la valeur par défaut "Self", ce qui lui permet de s'appuyer sur les moniteurs de serveur réel spécifiés pour le service virtuel. Vous pouvez également spécifier une adresse IP, un port ou une adresse IP:port, ce qui vous permet de surveiller un autre point d'extrémité sur votre réseau. Il peut s'agir, par exemple, d'un serveur de base de données dont les services dépendent.

Notes

Saisissez dans le champ Notes toute note particulière utile à la description de l'entrée définie. Exemple : "IIS Server1 - London DC". Ce champ peut être utilisé pour des besoins spécifiques dans les règles flightPATH et GSLB.

ID

Ce paramètre peut être utilisé de différentes manières.

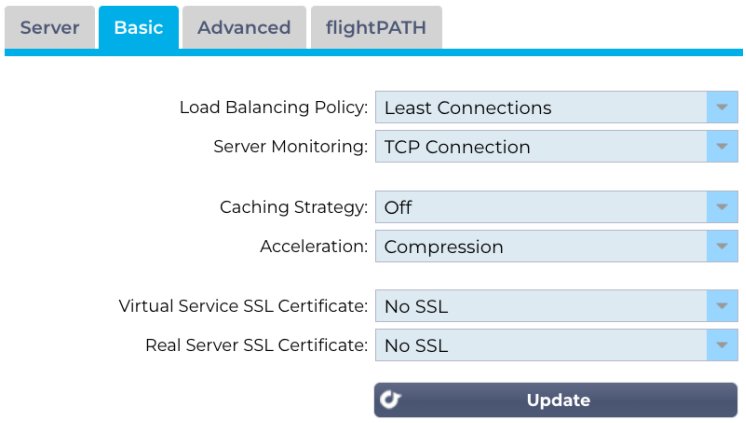
Persistance

La valeur peut être utilisée en conjonction avec la méthode de persistance basée sur l'ID du cookie. Cette méthode ressemble beaucoup à la persistance basée sur la session PHP, mais elle utilise une nouvelle technique appelée Cookie ID Based et cookie RegEx h=[^ ;]+. La méthode de persistance Cookie ID Based utilise la valeur du champ ID pour générer un cookie.

Utilisation de flightPATH

Vous pouvez également utiliser la valeur de ce champ pour diriger le trafic, etc.

De base



Politique d'équilibrage de la charge

La liste déroulante indique les politiques d'équilibrage de la charge actuellement prises en charge et disponibles. Vous trouverez ci-dessous une liste des politiques d'équilibrage de charge, ainsi qu'une explication.

Least Connections
Fastest
Persistent Cookie
Round Robin
IP-Bound
IP List Based
Shared IP List Based
Classic ASP Session Cookie
ASP.NET Session Cookie
JSP Session Cookie
JAX-WS Session Cookie
PHP Session Cookie
RDP Cookie Persistence
Cookie ID Based

Option	Description
Le moins de connexions	L'équilibreur de charge tient compte du nombre de connexions actuelles à chaque serveur réel. Le serveur réel qui a le moins de connexions reçoit la nouvelle demande suivante.
Le plus rapide	La politique d'équilibrage de charge la plus rapide calcule automatiquement le temps de réponse pour toutes les requêtes par serveur, lissé dans le temps. La colonne Poids calculé contient la valeur calculée automatiquement. La saisie manuelle n'est possible qu'avec cette politique de répartition de la charge.
Cookie persistant	Couche 7 Affinité/Persistance de la session Le mode d'équilibrage de la charge basé sur la liste IP est utilisé pour chaque première demande. L'ADC insère un cookie dans les en-têtes de la première réponse HTTP. Ensuite, l'ADC utilise le cookie du client pour acheminer le trafic vers le même serveur final. Ce cookie est utilisé à des fins de persistance lorsque le client doit se rendre à chaque fois sur le même serveur dorsal. Le cookie expire au bout de deux heures et la connexion est équilibrée en fonction d'un algorithme basé sur une liste d'adresses IP. Ce délai d'expiration est configurable à l'aide d'un jetPACK.
Tour de table	La méthode Round Robin est couramment utilisée dans les pare-feu et les équilibreurs de charge de base et est la plus simple. Chaque serveur réel reçoit une nouvelle demande dans l'ordre. Cette méthode n'est appropriée que lorsqu'il s'agit d'équilibrer la charge des requêtes vers les serveurs de manière uniforme, comme c'est le cas pour les serveurs web de recherche. Cependant, lorsque vous devez équilibrer la charge en fonction de la charge de l'application ou de la charge du serveur, ou même vous assurer que vous utilisez le même serveur pour la session, la méthode Round Robin n'est pas appropriée.
Liaison IP	Cookie d'affinité de session/de persistance de la couche 3. Dans ce mode, l'adresse IP du client sert de base à la sélection du Real Server qui recevra la demande. Cette action assure la persistance. Les protocoles HTTP et de couche 4 peuvent utiliser ce mode. Cette méthode est utile pour les réseaux internes dont la topologie est connue, et vous pouvez être sûr qu'il n'y a pas de "super proxies" en amont. Avec la couche 4 et les proxys, toutes les demandes peuvent sembler provenir d'un seul client et la charge n'est donc pas uniforme. Avec HTTP, les informations de l'en-tête (X-Forwarder-For) sont utilisées lorsqu'elles sont présentes pour faire face aux proxies.

Basé sur une liste d'adresses IP	La connexion au serveur Real s'initie en utilisant "Least connections", puis l'affinité de session est réalisée sur la base de l'adresse IP du client. Une liste est maintenue pendant 2 heures par défaut, mais cette durée peut être modifiée à l'aide d'un jetPACK.
Basé sur une liste d'adresses IP partagées	Ce type de service n'est disponible que lorsque le mode de connectivité est défini sur Retour direct au serveur. Il a été ajouté principalement pour la prise en charge de l'équilibrage de charge VMware.
Cookie persistant	Couche 7 Affinité/Persistance de la session Le mode d'équilibrage de la charge basé sur la liste IP est utilisé pour chaque première demande. L'ADC insère un cookie dans les en-têtes de la première réponse HTTP. Ensuite, l'ADC utilise le cookie du client pour acheminer le trafic vers le même serveur final. Ce cookie est utilisé à des fins de persistance lorsque le client doit se rendre à chaque fois sur le même serveur dorsal. Le cookie expire au bout de deux heures et la connexion est équilibrée en fonction d'un algorithme basé sur une liste d'adresses IP. Ce délai d'expiration est configurable à l'aide d'un jetPACK.
Cookie de session ASP classique	Active Server Pages (ASP) est une technologie côté serveur de Microsoft. Lorsque cette option est sélectionnée, le CDA maintient la persistance de la session sur le même serveur si un cookie ASP est détecté et trouvé dans sa liste de cookies connus. Lors de la détection d'un nouveau cookie ASP, la charge sera équilibrée à l'aide de l'algorithme "Least Connections".
Cookie de session ASP.NET	Ce mode s'applique à **ASP.net.** Lorsque ce mode est sélectionné, l'ADC maintient la persistance de la session sur le même serveur si un cookie ASP.NET est détecté et trouvé dans sa liste de cookies connus. Lors de la détection d'un nouveau cookie ASP, la charge sera équilibrée à l'aide de l'algorithme Least Connections.
Cookie de session JSP	Java Server Pages (JSP) est une technologie Oracle côté serveur. Lorsque ce mode est sélectionné, le CDA maintient la persistance de la session sur le même serveur si un cookie JSP est détecté et trouvé dans sa liste de cookies connus. Lorsqu'un nouveau cookie JSP est détecté, la charge est équilibrée à l'aide de l'algorithme "Least Connections".
Cookie de session JAX-WS	Les services web Java (JAX-WS) sont une technologie Oracle côté serveur. Lorsque ce mode est sélectionné, le CDA maintient la persistance de la session sur le même serveur si un cookie JAX-WS est détecté et trouvé dans sa liste de cookies connus. Lors de la détection d'un nouveau cookie JAX-WS, la charge est équilibrée à l'aide de l'algorithme "Least Connections".
Cookie de session PHP	Personal Home Page (PHP) est une technologie open-source côté serveur. Lorsque ce mode est sélectionné, l'ADC maintient la persistance de la session sur le même serveur lorsqu'un cookie PHP est détecté.
Persistance des cookies RDP	Cette méthode d'équilibrage de la charge utilise le cookie RDP créé par Microsoft et basé sur le nom d'utilisateur/domaine pour assurer la persistance d'un serveur. L'avantage de cette méthode est qu'il est possible de maintenir une connexion à un serveur même si l'adresse IP du client change.
Basé sur l'identification par cookie	Une nouvelle méthode très semblable à "PhpCookieBased" et à d'autres méthodes d'équilibrage de charge, mais qui utilise CookieIDBased et le cookie RegEx h=[^ ;]+. Cette méthode utilisera la valeur définie dans le champ de notes du serveur réel "ID=X ;" comme valeur de cookie pour identifier le serveur. Il s'agit donc d'une méthode similaire à CookieListBased, mais qui utilise un nom de cookie différent et stocke une valeur de cookie unique, non pas l'IP brouillée, mais l'ID du serveur réel (lue au moment du chargement). La valeur par défaut est CookieIDName="h" ; cependant, s'il existe une valeur de remplacement dans la configuration des paramètres avancés du serveur virtuel, utilisez-la à la place. **NOTE** : Nous écrasons l'expression du cookie ci-dessus

	pour remplacer h= par la nouvelle valeur si cette valeur est définie. Enfin, si une valeur de cookie inconnue arrive et correspond à l'un des identifiants de serveur réel, il convient de sélectionner ce serveur ; dans le cas contraire, il convient d'utiliser la méthode suivante (déléguer).

Surveillance du serveur

Votre ADC contient plusieurs méthodes prédéfinies de surveillance des serveurs réels.

Choisissez la méthode de surveillance que vous souhaitez appliquer au service virtuel (VIP)

Il est essentiel de choisir le bon moniteur pour le service. Par exemple, si le Real Server est un serveur RDP, un moniteur 200OK n'est pas pertinent. De même, choisir TCP Connection et 200OK n'a pas de sens, car vous avez besoin d'une connexion TCP opérationnelle pour que 200OK fonctionne. Si vous ne savez pas quel moniteur choisir, la connexion TCP par défaut est un excellent point de départ

Vous pouvez choisir plusieurs moniteurs en cliquant tour à tour sur chaque moniteur que vous souhaitez appliquer au service. Les moniteurs sélectionnés s'exécutent dans l'ordre dans lequel vous les avez sélectionnés ; commencez donc les moniteurs des couches inférieures. Par exemple, la configuration des moniteurs Ping/ICMP Echo, TCP Connection, et 200OK s'affichera dans les événements du tableau de bord comme dans l'image ci-dessous :

Nous pouvons voir que les couches 3 Ping et 4 TCP Connect ont réussi si nous regardons la ligne du haut, mais que la couche 7 200OK a échoué. Ces résultats de surveillance fournissent suffisamment d'informations pour indiquer que le routage est correct et qu'un service fonctionne sur le port correspondant, mais que le site web ne répond pas correctement à la page demandée. Il est maintenant temps d'examiner le serveur web et la section Bibliothèque > Real Server Monitor pour voir les détails du moniteur défaillant.

Option	**Description**
Aucun	Dans ce mode, le serveur réel n'est pas surveillé et fonctionne toujours correctement. Le paramètre Aucun est utile dans les situations où la surveillance perturbe un serveur et pour les services qui ne doivent pas participer à l'action de basculement de l'ADC. C'est un moyen d'héberger des systèmes peu fiables ou anciens qui ne sont pas essentiels aux opérations de H/A. Utilisez cette méthode de surveillance avec n'importe quel type de service.
Ping/ICMP Echo	Dans ce mode, l'ADC envoie une demande d'écho ICMP à l'IP du serveur de contenu. Si une réponse valide est reçue, l'ADC considère que le serveur réel est opérationnel et le trafic vers le serveur continue. Il maintiendra également le service disponible sur une paire H/A. Cette méthode de surveillance est utilisable avec n'importe quel type de service.
Connexion TCP	Une connexion TCP est établie avec le Real Server et immédiatement interrompue sans envoyer de données dans ce mode. Si la connexion réussit, l'ADC considère que le serveur réel est opérationnel. Cette méthode de surveillance est utilisable avec n'importe quel type de service, et les services UDP ne sont actuellement pas appropriés pour la surveillance de la connexion TCP.
ICMP inaccessible	L'ADC enverra un contrôle de santé UDP au serveur et marquera le Real Server comme étant indisponible s'il reçoit un message ICMP de port inaccessible. Cette méthode peut être utile lorsque vous devez vérifier si un port de service UDP est disponible sur un serveur, tel que le port DNS 53.

RDP	Dans ce mode, une connexion TCP est initialisée comme expliqué dans la méthode ICMP Unreachable. Après l'initialisation de la connexion, une connexion RDP de niveau 7 est demandée. Si la liaison est confirmée, l'ADC considère que le Real Server est opérationnel. Cette méthode de surveillance est utilisable avec n'importe quel serveur de terminal Microsoft.
200 OK	Dans cette méthode, une connexion TCP est initialisée avec le serveur réel. Une fois la connexion établie, l'ADC envoie au Real Server une requête HTTP. Une réponse HTTP est attendue et le code de réponse "200 OK" est vérifié. L'ADC considère que le serveur réel est opérationnel si le code de réponse "200 OK" est reçu. Si l'ADC ne reçoit pas de code de réponse "200 OK" pour quelque raison que ce soit, y compris les dépassements de délai, l'échec de la connexion et d'autres raisons, l'ADC considère que le serveur réel n'est pas disponible. Cette méthode de surveillance n'est valable que pour les types de service HTTP et HTTP accéléré. Si un type de service de couche 4 est utilisé pour un serveur HTTP, il est utilisable si SSL n'est pas utilisé sur le serveur réel ou traité de manière appropriée par la fonction "Content SSL".
DICOM	Une connexion TCP s'initialise avec le serveur Real en mode DICOM, et une "demande d'association" Echoscu est faite au serveur Real lors de la connexion. Une conversation comprenant une "Acceptation d'association" de la part du serveur de contenu, un transfert d'une petite quantité de données suivi d'une "Demande de libération", puis d'une "Réponse de libération" conclut le moniteur avec succès. Si le moniteur ne se termine pas avec succès, le serveur réel est considéré comme hors service pour quelque raison que ce soit.
Défini par l'utilisateur	Tout moniteur configuré dans la section Surveillance du serveur réel apparaît dans la liste.

Stratégie de mise en cache

Par défaut, la stratégie de mise en cache est désactivée et définie comme Off. Si votre type de service est HTTP, vous pouvez appliquer deux types de stratégie de mise en cache.

Veuillez consulter la page Configurer le cache pour configurer les paramètres détaillés du cache. Notez que lorsque la mise en cache est appliquée à un VIP avec le type de service "HTTP" accéléré, les objets compressés ne sont pas mis en cache.

Option	**Description**
Par l'hôte	La mise en cache par hôte est basée sur l'application par nom d'hôte. Un cache séparé existera pour chaque domaine/nom d'hôte. Ce mode est idéal pour les serveurs web qui peuvent servir plusieurs sites web en fonction du domaine.
Par le service virtuel	La mise en cache par service virtuel est disponible lorsque vous choisissez cette option. Il n'y aura qu'un seul cache pour tous les domaines/noms d'hôtes qui passent par le service virtuel. Cette option est un paramètre spécialisé à utiliser avec plusieurs clones d'un même site.

Accélération

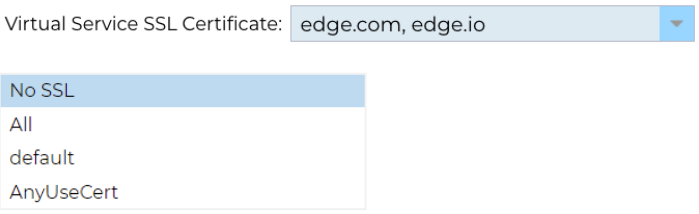
Option	**Description**
Arrêt	Désactiver la compression pour le service virtuel
Compression	Lorsqu'elle est sélectionnée, cette option active la compression pour le service virtuel sélectionné. L'ADC compresse dynamiquement le flux de données transmis au client sur demande. Ce processus ne s'applique qu'aux objets qui contiennent l'en-tête content-encoding : gzip. Un exemple de contenu est HTML, CSS ou JavaScript. Vous pouvez également exclure certains types de contenu à l'aide de la section Exclusions globales.

Remarque : si l'objet peut être mis en cache, le CDA stockera une version compressée et la servira de manière statique (à partir de la mémoire) jusqu'à ce que le contenu expire et soit revalidé.

Certificat SSL du service virtuel (cryptage entre le client et l'ADC)

Par défaut, le paramètre est Pas de SSL. Si votre type de service est "HTTP", vous pouvez sélectionner un certificat dans la liste déroulante pour l'appliquer au service virtuel. Les certificats qui ont été créés ou importés apparaissent dans cette liste.

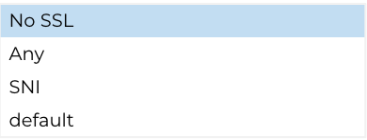
Vous pouvez également mettre en évidence plusieurs certificats à appliquer à un service. Cette opération activera automatiquement l'extension SNI pour autoriser un certificat basé sur le "nom de domaine" demandé par le client.



Option	**Description**
Pas de SSL	Le trafic entre la source et le CDA n'est pas crypté.
Tous	Charge tous les certificats disponibles pour utilisation
Défaut	Cette option a pour effet d'appliquer un certificat créé localement, appelé "Default", au côté navigateur du canal. Utilisez cette option pour tester SSL lorsqu'aucun certificat n'a été créé ou importé.

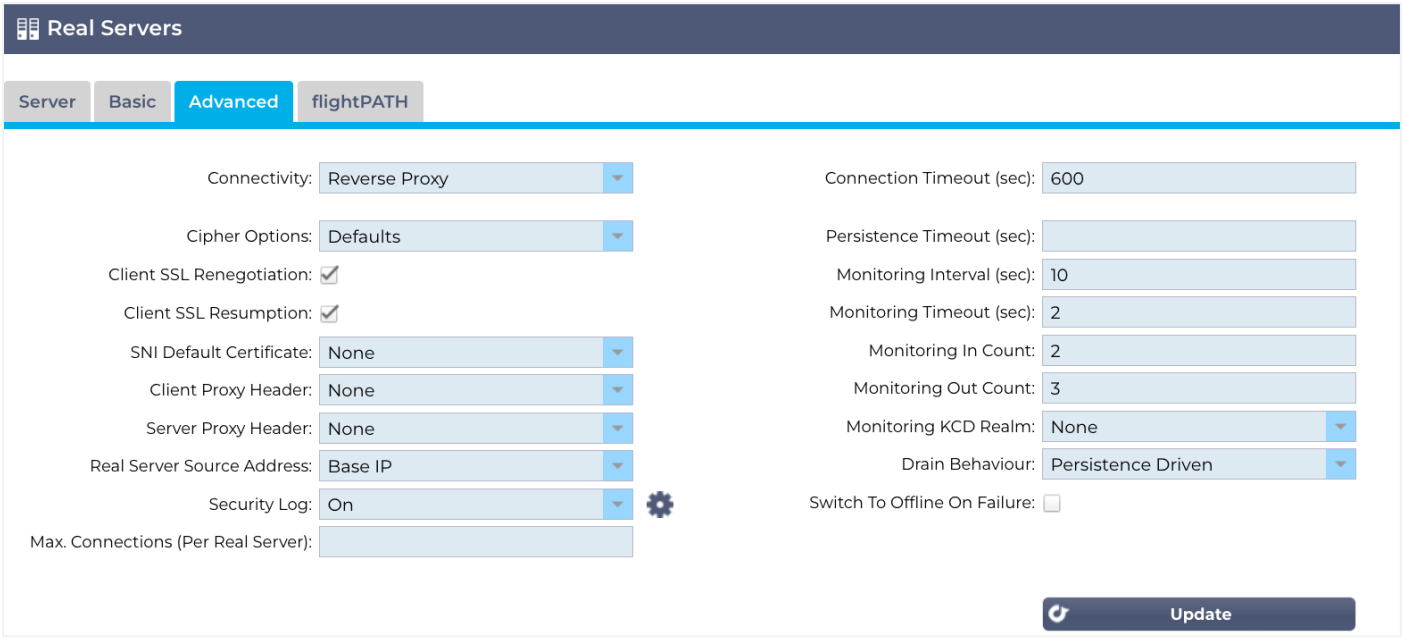
Certificat SSL du serveur réel (cryptage entre l'ADC et le serveur réel)

Le paramètre par défaut de cette option est Pas de SSL. Si votre serveur nécessite une connexion cryptée, cette valeur doit être différente de Pas de SSL. Les certificats qui ont été créés ou importés apparaissent dans cette liste.



Option	**Description**
Pas de SSL	Le trafic entre l'ADC et le serveur réel n'est pas crypté. La sélection d'un certificat du côté du navigateur signifie que l'option "Pas de SSL" peut être choisie du côté du client pour fournir ce qui est connu sous le nom de "SSL Offload".
Tous	L'ADC agit en tant que client et accepte tout certificat présenté par le serveur réel. Le trafic entre l'ADC et le serveur réel est crypté lorsque cette option est sélectionnée. Utilisez l'option "Any" lorsqu'un certificat est spécifié du côté du service virtuel, ce qui permet d'obtenir ce que l'on appelle un "pontage SSL" ou un "recryptage SSL".
SNI	SNI (Server Name Indication) est une extension du protocole de réseau TLS qui permet au client d'indiquer le nom d'hôte auquel il tente de se connecter au début du processus d'échange de données ( ). Ce paramètre permet au CDA de présenter plusieurs certificats sur la même adresse IP virtuelle et le même port TCP.
Défaut	Les certificats auto-signés que vous avez générés apparaissent ici.

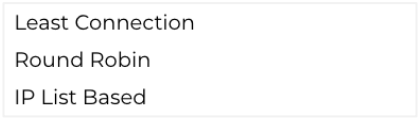
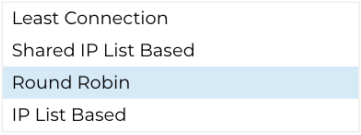
Avancé



Connectivité

Votre service virtuel peut être configuré avec différents types de connectivité. Veuillez sélectionner le mode de connectivité à appliquer au service.

Option	Description
Proxy inversé	Reverse Proxy est la valeur par défaut et utilise la compression et la mise en cache lorsqu'il est utilisé avec la couche 7. Au niveau 4, le proxy inverse fonctionne sans cache ni compression. Dans ce mode, votre CDA agit comme un proxy inverse et devient l'adresse source vue par les serveurs réels.
Retour direct du serveur	Direct Server Return ou DSR, également connu sous le nom de DR - Direct Routing, permet au serveur situé derrière l'équilibreur de charge de répondre directement au client en contournant l'ADC sur la réponse. Le DSR ne peut être utilisé qu'avec l'équilibrage de charge de la couche 4. Par conséquent, la mise en cache et la compression ne sont pas disponibles avec cette option. **Ce mode ne peut être utilisé qu'avec les types de services TCP, UDP et TCP/UDP.** Les politiques de persistance de l'équilibrage de charge sont également limitées à Least Connections, Shared IP List Based, Round Robin et IP List Based.  L'utilisation du DSR nécessite également que des modifications soient apportées au serveur réel. Veuillez vous référer à la section Modifications du serveur réel.
NAT	Par défaut, l'ADC utilise l'adresse IP de l'ADC comme adresse IP source, et les serveurs réels renvoient alors la réponse à l'ADC pour qu'elle soit renvoyée au client. Cela convient dans la plupart des cas, mais il existe des scénarios dans lesquels le serveur réel doit voir l'adresse IP source du client et non celle de l'ADC. Lorsque le mode NAT est appliqué, l'ADC reçoit la requête entrante, puis l'envoie au serveur réel après avoir modifié l'adresse IP source pour la remplacer par celle du service virtuel (adresse VIP). **Ce mode ne peut être utilisé qu'avec les politiques d'équilibrage de charge suivantes :**

	
Passerelle	Le mode passerelle vous permet d'acheminer tout le trafic via l'ADC, ce qui permet aux serveurs réels d'être acheminés via l'ADC vers d'autres réseaux par le biais des services virtuels ou des interfaces matérielles de l'ADC. L'utilisation de l'appareil en tant que passerelle pour les serveurs réels est idéale en mode multi-interface. Les politiques de persistance de l'équilibrage de charge sont également limitées à Least Connections, Shared IP List Based, Round Robin et IP List Based.  Cette méthode nécessite que le Real Server définisse sa passerelle par défaut sur l'adresse de l'interface locale de l'ADC (eth0, eth1, etc.). Veuillez vous reporter à la section Modifications du serveur réel. ***Veuillez noter que le mode passerelle ne prend pas en charge le basculement dans un environnement en grappe.***

Options de chiffrement

Les codes constituent la base de la cryptographie SSL et sont extrêmement importants pour assurer la réussite et la sécurité du contenu web et de la diffusion des applications.

L'ADC contient un ensemble intégré de codes par défaut, comprenant les codes les plus récents et les plus sûrs disponibles.

Il arrive que l'utilisateur souhaite annoncer la disponibilité d'un ensemble particulier de Ciphers, et l'ADC permet la création de tels Ciphers par le biais de jetPACKS rédigés par l'utilisateur. Les jetPACKS rédigés par les utilisateurs peuvent être importés dans l'ADC par le biais de Configuration > Logiciel, puis mis à disposition pour être choisis dans le menu Options de Cipher.

Les options de chiffrement sont spécifiques à chaque VIP et offrent une grande flexibilité et une grande sécurité.

Pour plus d'informations sur les options de chiffrement, voir : *Cipher*

Renégociation SSL du client

Cochez cette case si vous souhaitez autoriser la renégociation SSL à l'initiative du client. Désactivez la renégociation SSL à l'initiative du client pour prévenir toute attaque DDOS éventuelle contre la couche SSL en décochant cette option.

Reprise du SSL par le client

Cochez cette case si vous souhaitez activer les sessions du serveur de reprise SSL ajoutées au cache de session. Lorsqu'un client propose la réutilisation d'une session, le serveur essaiera de réutiliser la session si elle est trouvée. Si la case Reprise n'est pas cochée, aucune session n'est mise en cache pour le client ou le serveur.

Certificat SNI par défaut

Lors d'une connexion SSL avec le SNI côté client activé, si le domaine demandé ne correspond à aucun des certificats attribués au service, l'ADC présentera le certificat SNI par défaut. Le paramètre par défaut est Aucun, ce qui aurait pour effet d'interrompre la connexion s'il n'y a pas de correspondance exacte.

Choisissez l'un des certificats installés dans le menu déroulant à présenter en cas d'échec de la correspondance exacte du certificat SSL.

Le protocole Proxy

Le protocole Proxy est conçu pour permettre aux proxys de réseau de transmettre les informations de connexion du client (telles que l'adresse IP d'origine et le numéro de port) au serveur de réception. Ce protocole est particulièrement utile dans les scénarios où l'adresse IP réelle de l'utilisateur final doit être préservée lorsque le trafic est acheminé via un équilibreur de charge ou un proxy inverse. Il permet de conserver l'adresse IP d'origine du client à des fins de journalisation, de statistiques ou de sécurité, ce qui renforce la capacité à prendre des décisions éclairées sur la base de la véritable source du trafic.

En-tête du proxy du client

Le Client Proxy Header est un en-tête ajouté à la requête du client par l'ADC, encapsulant les informations de connexion originales (telles que l'adresse IP et le port du client). Ceci est crucial dans les environnements où l'ADC agit comme un proxy, et où le serveur a besoin de connaître les détails originaux du client à des fins telles que la journalisation, les évaluations de sécurité, et le maintien d'un comportement spécifique au client. L'en-tête Client Proxy garantit que, malgré le rôle d'intermédiaire de l'ADC, le serveur peut identifier avec précision les données de connexion originales du client et interagir avec elles.

Les options comprennent

Option	Description
Aucun	Lorsqu'il n'y a pas d'en-tête Proxy ou qu'il n'est pas pris en charge par le type de service actuel
Retirer	Supprime l'en-tête Proxy du paquet TCP
En avant	Renvoie l'en-tête Proxy au serveur

En-tête Proxy du serveur

Il existe deux versions de Server Proxy Headers : Version 1 et Version 2.

Option	Description
Version 1	• Format texte, facile à mettre en œuvre et à déboguer. • Fournit des informations de base sur la connexion du client, notamment l'IP source, l'IP de destination, le port source et le port de destination. • La ligne de protocole est ajoutée au début de la connexion TCP, ce qui la rend lisible par l'homme mais légèrement moins efficace en termes de performances que les formats binaires.
Version 2	• Format binaire, conçu pour améliorer les performances et l'efficacité. • Étend les informations qui peuvent être transmises au sujet de la connexion, en prenant en charge des données supplémentaires telles que la famille d'adresses et les informations spécifiques au protocole. • Assure une meilleure compatibilité avec les protocoles et les fonctionnalités des réseaux modernes, y compris la prise en charge de l'IPv6 et des protocoles de transport autres que TCP.

Les options d'en-tête Proxy client et Proxy serveur ne sont disponibles que pour les types de services HTTP de couche 4 et 7.

Adresse source du serveur réel

Ce paramètre fonctionne avec le Reverse Proxy et les services TCP de couche 4, UDP de couche 4 ou HTTP(S). Ce paramètre propose trois options parmi lesquelles vous pouvez choisir.

Option	Description
IP de base (par défaut)	Utilise l'adresse eth0 ou l'adresse IP de base de l'ADC comme IP source de la requête.
IP virtuel	Utilise l'IP virtuelle du service.
<Adresse IP>	Permet de spécifier une adresse IP qui fait partie de l'ADC. Il peut s'agir d'une interface réseau différente ou d'un VIP différent.

Journal de sécurité

La valeur par défaut est "On". Elle s'applique à chaque service et permet au service d'enregistrer les informations d'authentification dans les journaux du W3C. En cliquant sur l'icône Cog, vous accéderez à la page Système > Journalisation, où vous pourrez vérifier les paramètres de la journalisation W3C.

Max. Connexions

Limite le nombre de connexions simultanées au Real Server et est défini par service. Par exemple, si vous configurez cette limite à 1 000 et que vous disposez de deux serveurs réels, l'ADC limite **chaque** serveur réel à 1 000 connexions simultanées. Vous pouvez également choisir d'afficher une page "Serveur trop occupé" lorsque cette limite est atteinte sur tous les serveurs, afin d'aider les utilisateurs à comprendre la raison d'une absence de réponse ou d'un retard. Laissez ce champ vide pour des connexions illimitées. Ce que vous définissez ici dépend des ressources de votre système.

Délai de connexion

Le délai de connexion par défaut est de 600 secondes ou 10 minutes. Ce paramètre permet d'ajuster le délai d'expiration de la connexion en cas d'absence d'activité. Réduisez ce délai pour le trafic web sans état de courte durée, qui est généralement de 90s ou moins. Augmentez ce chiffre pour les connexions avec état, telles que RDP, à quelque chose comme 7200 secondes (2 heures) ou plus, en fonction de votre infrastructure. L'exemple du délai d'attente RDP signifie que si un utilisateur a une période d'inactivité de 2 heures ou moins, les connexions resteront ouvertes.

Délai de persistance

Le paramètre Persistence Timeout des équilibreurs de charge spécifie la durée pendant laquelle un équilibreur de charge conserve les informations de session d'un client. Cela permet de s'assurer que les demandes ultérieures du même client sont dirigées vers le même serveur dorsal, ce qui favorise la cohérence des sessions et la communication avec état. Une fois que le délai spécifié s'est écoulé sans nouvelle activité du client, les informations de session sont supprimées et les nouvelles demandes peuvent être acheminées vers un autre serveur.

Intervalle de surveillance

L'intervalle est le temps en secondes entre les moniteurs. L'intervalle par défaut est de 1 seconde. Bien que 1 seconde soit acceptable pour la plupart des applications, il peut être utile d'augmenter ce délai pour d'autres applications ou lors de tests.

Délai de surveillance

La valeur du délai d'attente correspond à la durée pendant laquelle l'ADC attend qu'un serveur réponde à une demande de connexion. La valeur par défaut est de 2 secondes. Augmentez cette valeur pour les serveurs occupés.

Suivi du nombre d'entrées

La valeur par défaut de ce paramètre est 2. La valeur 2 indique que le Real Server doit réussir deux contrôles de surveillance de la santé avant d'être mis en ligne. En augmentant ce chiffre, vous augmentez la probabilité que le serveur puisse servir le trafic, mais il faudra plus de temps pour le mettre en service, en fonction de l'intervalle. En diminuant cette valeur, le serveur sera mis en service plus rapidement.

Surveillance du nombre de sorties

La valeur par défaut de ce paramètre est 3, ce qui signifie que le moniteur Real Server doit échouer trois fois avant que l'ADC n'arrête d'envoyer du trafic au serveur, qui est alors marqué RED et Unreachable (inaccessible). En augmentant ce chiffre ( ), vous obtiendrez un service de meilleure qualité et plus fiable, au détriment du temps nécessaire à l'ADC pour cesser d'envoyer du trafic à ce serveur.

Surveillance du domaine KCD

Ce paramètre vous permet d'activer la surveillance du domaine de délégation restreinte Kerberos que vous avez configuré dans les définitions Kerberos. Voir Authentification > Kerberos.

Comportement en matière de vidange

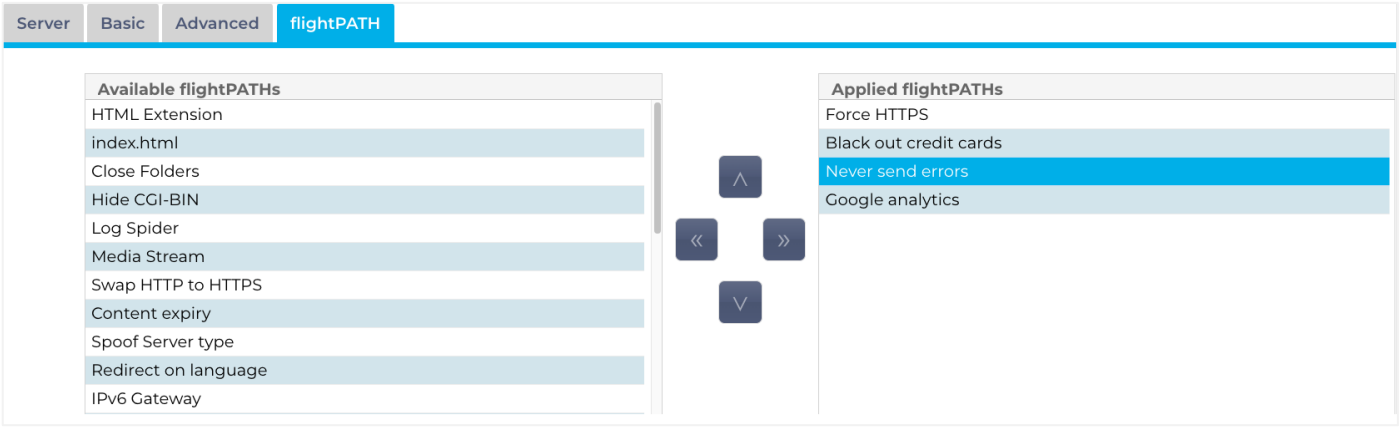
Lorsqu'un serveur réel est placé en mode vidange, il est toujours préférable de pouvoir contrôler le comportement du trafic qui lui est envoyé. Le menu Drain Behaviour permet de sélectionner le comportement du trafic pour chaque service virtuel. Les options sont les suivantes :

Option	Description
Axé sur la persistance	Il s'agit de la sélection par défaut. Chaque fois que l'utilisateur utilise la session de persistance, celle-ci est prolongée. En cas d'utilisation 24 heures sur 24, il est possible que la vidange ne se produise jamais. Toutefois, si le nombre de connexions au serveur réel atteint 0, le drainage s'arrête, les sessions de persistance sont supprimées et tous les visiteurs sont rééquilibrés lors de leur prochaine connexion.
Migrer les visiteurs	Session persistante ignorée lors de la reconnexion - (comportement hérité avant 2022) Les nouvelles connexions TCP (qu'elles fassent partie d'une session existante ou non) sont toujours établies avec un serveur réel en ligne. Si la session de persistance était liée à un serveur réel épuisé, elle est écrasée. Le service virtuel ignorera effectivement la persistance pour toutes les nouvelles connexions, et celles-ci seront réparties sur un nouveau serveur.
Sessions de retraite	Les sessions persistantes ne sont pas prolongées. Les connexions d'utilisateurs entrantes seront attribuées au serveur de leur choix, mais leur session de persistance n'est pas prolongée. Par conséquent, une fois la durée de la session de persistance dépassée, elles seront traitées comme de nouvelles connexions et déplacées vers un autre serveur.

Passage à l'état hors ligne en cas d'échec

Lorsque cette option est cochée, les serveurs réels dont le bilan de santé n'est pas satisfaisant sont mis hors ligne et ne peuvent être remis en ligne que manuellement.

chemin d'accès au vol



flightPATH est une technologie de gestion du trafic conçue par Edgenexus et exclusivement disponible au sein de l'ADC. Contrairement aux moteurs basés sur des règles d'autres fournisseurs, flightPATH ne fonctionne pas par le biais d'une ligne de commande ou d'une console d'entrée de script. Il utilise plutôt une interface graphique pour sélectionner les différents paramètres, conditions et actions à effectuer pour obtenir ce dont ils ont besoin. Ces caractéristiques rendent flightPATH extrêmement puissant et permettent aux administrateurs de réseau de manipuler le trafic HTTPS de manière très efficace.

flightPATH n'est disponible que pour les connexions HTTPS, et cette section n'est pas visible lorsque le type de service virtuel n'est pas HTTP.

Comme le montre l'image ci-dessus, la liste des règles disponibles se trouve à gauche et les règles appliquées au service virtuel se trouvent à droite.

Appliquez une règle disponible en la faisant glisser du côté gauche vers le côté droit ou en la mettant en surbrillance et en cliquant sur la flèche droite pour la déplacer vers le côté droit.

L'ordre d'exécution est essentiel et commence par la règle du haut. Pour modifier l'ordre d'exécution, mettez la règle en surbrillance et déplacez-la vers le haut ou vers le bas à l'aide des flèches.

Il est important de comprendre que les règles flightPATH de cette section de l'ADC fonctionnent sur la base d'un **OU** booléen, alors que les conditions et les actions de la zone de définition flightPATH fonctionnent sur la base d'un **ET.**

Pour supprimer une règle, faites-la glisser et déposez-la dans l'inventaire des règles sur la gauche ou mettez la règle en surbrillance et cliquez sur la flèche gauche.

Vous pouvez ajouter, supprimer et modifier les règles flightPATH dans la section Configurer flightPATH de ce guide.

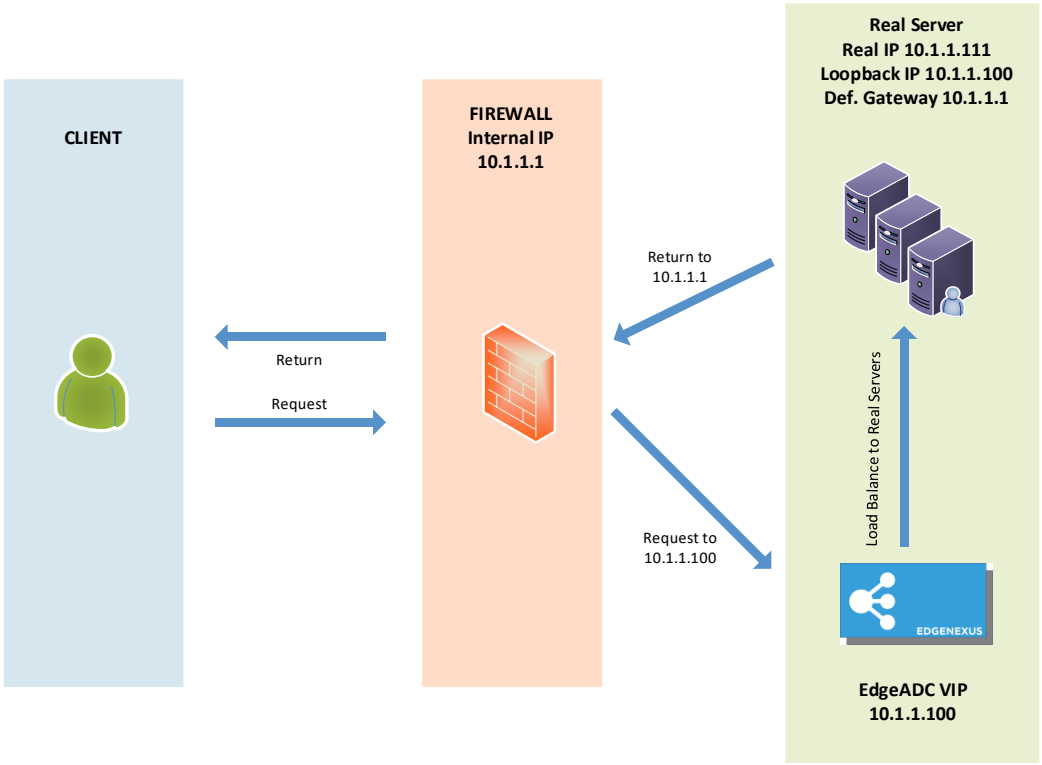
Changements dans le serveur réel pour le retour du serveur direct

Le retour direct du serveur ou DSR (DR - Direct Routing dans certains cercles) permet au serveur situé derrière l'ADC de répondre directement au client, en contournant l'ADC dans la réponse. Le DSR ne peut être utilisé qu'avec l'équilibrage de charge de la couche 4. La mise en cache et la compression ne sont pas disponibles lorsqu'elles sont activées.

L'équilibrage de charge de la couche 7 avec cette méthode ne fonctionnera pas car il n'y a pas de support de persistance autre que l'IP source. L'équilibrage de charge SSL/TLS avec cette méthode n'est pas idéal car il n'y a qu'une prise en charge de la persistance de l'IP source.

Comment cela fonctionne-t-il ?

- Le client envoie une demande à l'EdgeADC VIP
- Demande reçue par EdgeADC
- Demande acheminée vers les serveurs de contenu
- Réponse envoyée directement au client sans passer par EdgeADC



Configuration requise du serveur de contenu

Général

- La passerelle par défaut du serveur de contenu doit être configurée normalement. (Pas via l'ADC)
- Le serveur de contenu et l'équilibreur de charge doivent se trouver dans le même sous-réseau.

Fenêtres

- Le serveur de contenu doit avoir un loopback ou un alias configuré avec l'adresse IP du canal ou du VIP. avec l'adresse IP du canal ou du VIP
    - La métrique du réseau doit être de 254 pour empêcher la réponse aux requêtes ARP.
    - Ajouter un adaptateur loopback dans Windows Server 2012 - Cliquez ici

    - Ajouter un adaptateur de bouclage dans Windows Server 2003/2008 - Cliquez ici
- Exécutez les opérations suivantes dans une invite de commande pour chaque interface réseau que vous avez configurée sur les serveurs Windows Real

netsh interface ipv4 set interface "Nom de l'interface réseau Windows" weakhostreceive=enable

netsh interface ipv4 set interface "Nom de l'interface de boucle Windows" weakhostreceive=enable

netsh interface ipv4 set interface "Nom de l'interface de bouclage Windows" weakhostsend=enable

Linux

- Ajouter une interface de bouclage permanente
- Modifier "/etc/sysconfig/network-scripts"

ifcfg-lo:1
DEVICE=lo:1
IPADDR=x.x.x.x
NETMASK=255.255.255.255
BROADCAST=x.x.x.x.x
ONBOOT=yes

- Modifier "/etc/sysctl.conf"

net.ipv4.conf.all.arp_ignore = 1
net.ipv4.conf.eth0.arp_ignore = 1
net.ipv4.conf.eht1.arp_ignore = 1
net.ipv4.conf.all.arp_announce = 2
net.ipv4.conf.eth0.arp_announce = 2
net.ipv4.conf.eth1.arp_announce = 2

- Exécutez "sysctl - p"

Changements dans Real Server - Mode passerelle

Le mode passerelle vous permet d'acheminer tout le trafic via le CDA, ce qui permet au trafic provenant des serveurs de contenu d'être acheminé via le CDA vers d'autres réseaux par l'intermédiaire des interfaces de l'unité CDA. L'utilisation de l'appareil en tant que passerelle pour les serveurs de contenu doit se faire en mode multi-interface.

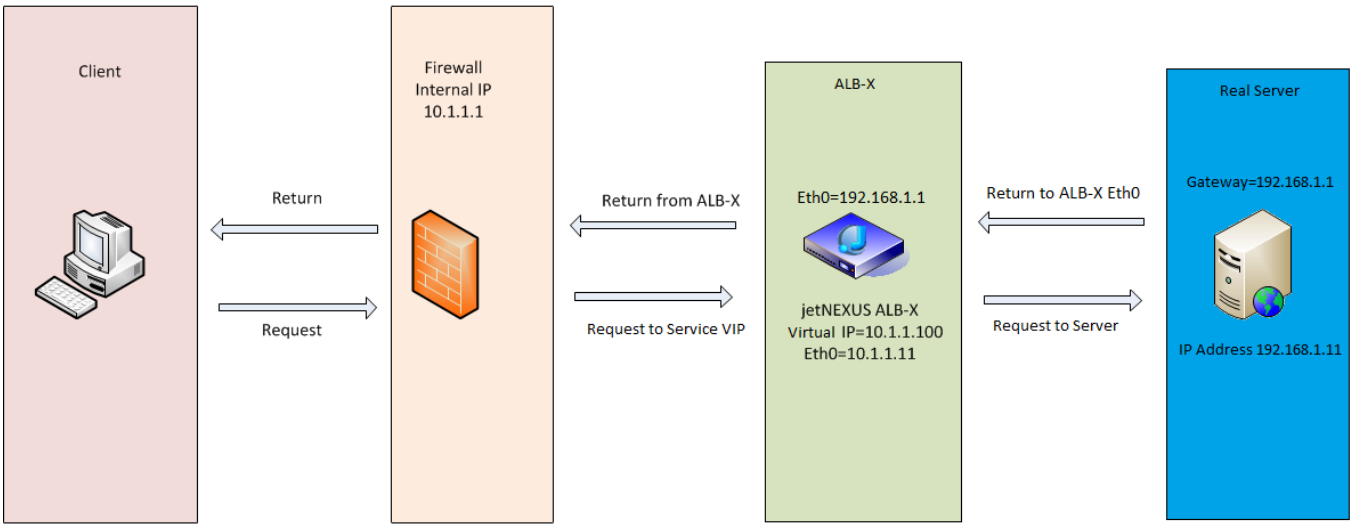
Comment cela fonctionne-t-il ?

- Le client envoie une demande à l'EdgeADC
- Une demande est reçue par EdgeADC
- Demande envoyée aux serveurs de contenu
- Réponse envoyée à EdgeADC
- L'ADC achemine la réponse vers le client

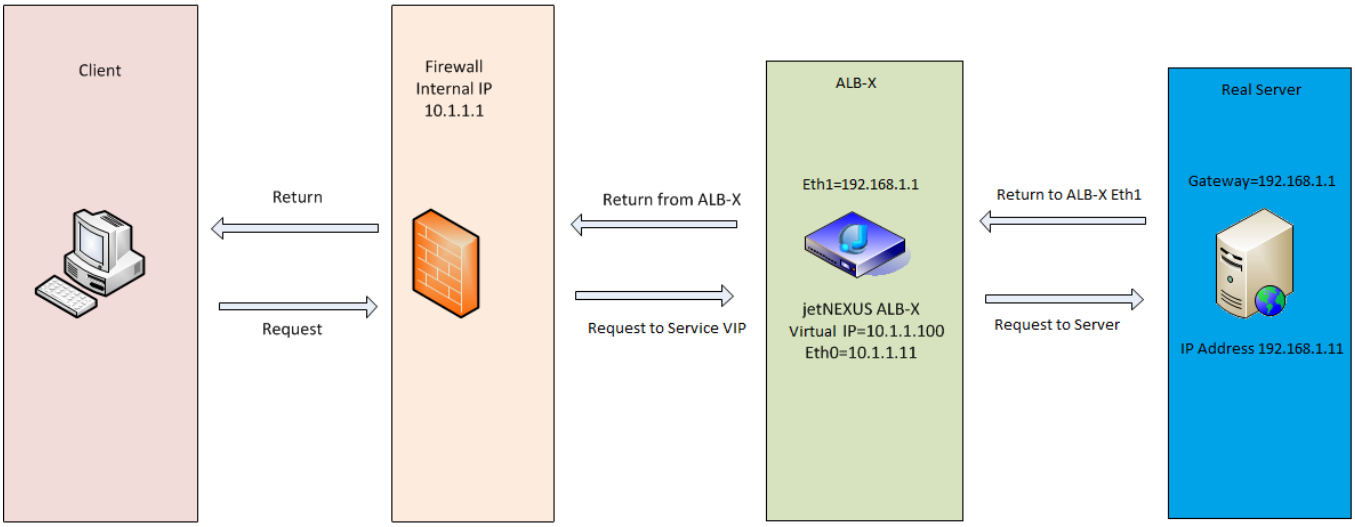
Configuration requise du serveur de contenu

- Single Arm Mode - une interface est utilisée, mais le service VIP et les serveurs réels doivent se trouver sur des sous-réseaux différents.
- Dual Arm Mode - deux interfaces sont utilisées, mais le service VIP et les serveurs réels doivent se trouver sur des sous-réseaux différents.
- Dans chaque cas, bras simple ou double, les serveurs réels doivent configurer leur passerelle par défaut à l'adresse de l'interface du CDA sur le sous-réseau concerné.

Exemple de bras unique



Exemple de bras double

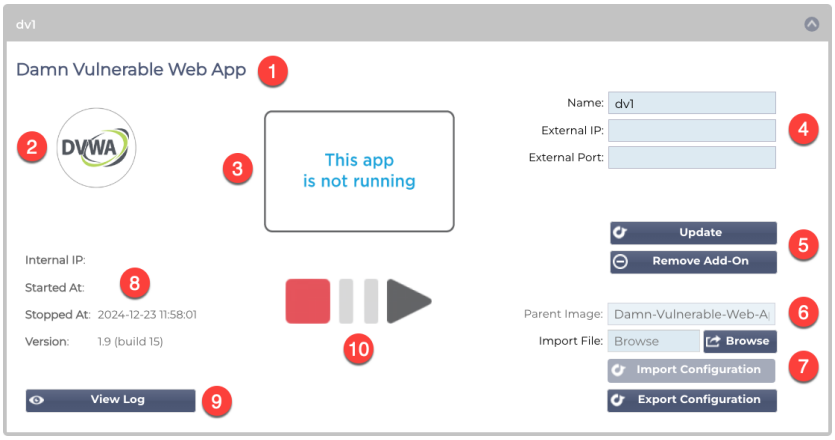


Bibliothèque

Compléments

Les add-ons sont des applications qui sont chargées dans des conteneurs et fonctionnent dans un mode isolé au sein de l'ADC. Il peut s'agir par exemple d'un pare-feu applicatif ou même d'une micro-instance de l'ADC lui-même.

Une application est déployée dans la section Add-Ons à l'aide de la page Apps, comme décrit dans ce guide. Une fois déployée, une application apparaît comme suit.



Comme vous pouvez le voir sur l'image ci-dessus, plusieurs éléments sont mis en évidence.

Objet	Description
❶	Titre de l'application
❷	Icône de l'application
❸	Affichage de l'application en cours d'exécution. Si l'application est en cours d'exécution, une miniature de l'écran s'affiche.
❹	Détails d'accès : **Nom** : Il s'agit d'un nom interne que vous utilisez pour faire référence à l'application à partir de la section Services virtuels. Il n'est pas possible de référencer une application en utilisant son adresse IP. Le nom doit être alphanumérique, sans espace. **IP externe** : Il s'agit de l'adresse IP que vous devez fournir pour l'application. Elle fera partie du sous-réseau de votre réseau. **Port externe** : Il s'agit d'un champ important. Vous devrez spécifier les ports qui seront utilisés pour accéder à l'application. Lorsque le trafic externe à l'application y accède, vous devez le spécifier en utilisant la notation suivante : 53/tcp ou 53/udp. En plus de cela, vous devrez spécifier le port de l'interface utilisateur pour l'application. Ceux-ci sont indiqués dans l'infobulle du champ pour chaque application.
❺	Bouton de mise à jour : Une fois que vous avez rempli les détails spécifiés dans❸ , cliquez sur ce bouton pour confirmer les entrées et configurer l'application. Le bouton "Supprimer le complément" permet de le retirer de la section "Applications". Pour supprimer une application, veuillez vous assurer que toutes les références à l'application sont également supprimées avant de procéder à la suppression.
❻	L'image des parents est un champ informatif et n'est pas utilisé du point de vue de l'utilisateur.
❼	L'importation et l'exportation d'une configuration sont importantes pour conserver une copie de sauvegarde des paramètres. Cette option permet d'exécuter les fonctions d'importation et d'exportation.
❽	Les détails de l'exécution fournissent des informations sur l'adresse IP de l'API interne, l'heure de début et de fin, et le numéro de version de l'application.
❾	Ce bouton vous permet de télécharger et d'afficher le journal. Il est principalement utilisé lorsque vous avez besoin d'ouvrir un ticket d'assistance.
❿	Le fonctionnement de l'application s'effectue à l'aide de ces boutons. Rouge=Arrêté, Or=Enclenché et Vert=En marche.

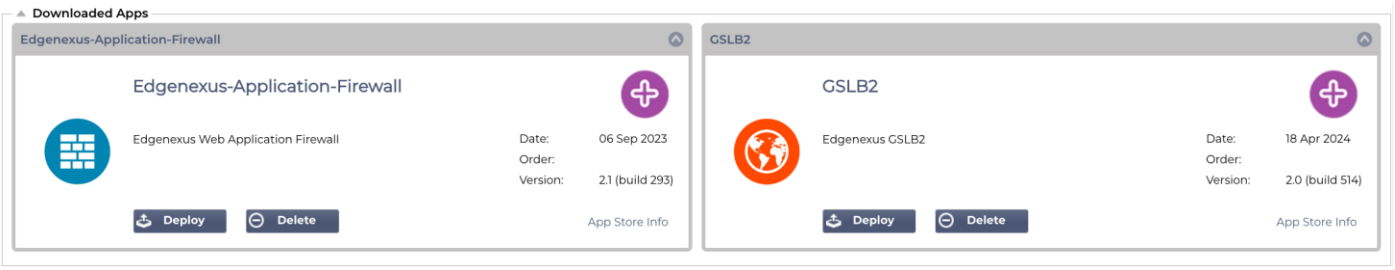
Applications

La section Apps comporte plusieurs sous-sections qui traitent des applications disponibles sur l'ADC. Il s'agit du filtre, des applications téléchargées et des applications achetées.

Le filtre

Le filtre vous permet de filtrer les applications/outils en fonction de leur type.

Applications téléchargées

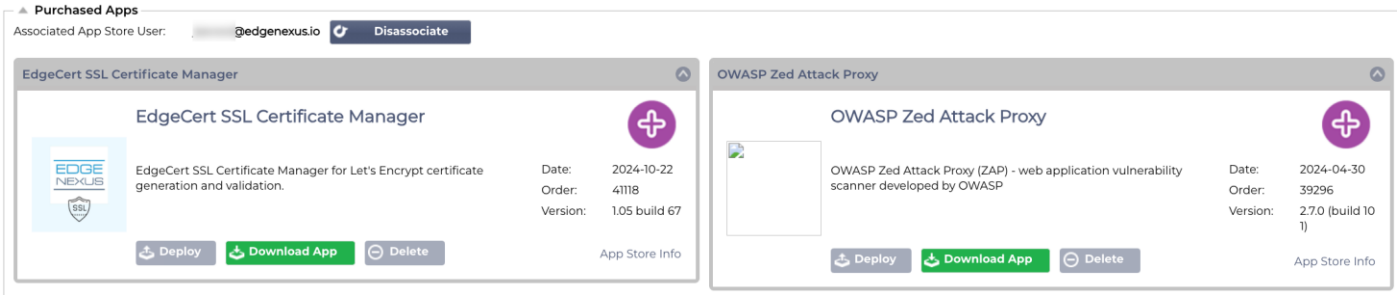


Cette section contient les applications qui ont été téléchargées sur le CDA. Vous pouvez les avoir téléchargées sur votre bureau local, puis téléchargées sur le CDA, ou vous pouvez les avoir téléchargées via le portail App Store intégré.

Chaque application est dotée de deux boutons, ainsi que de données qui indiquent son numéro de version et sa date de sortie.

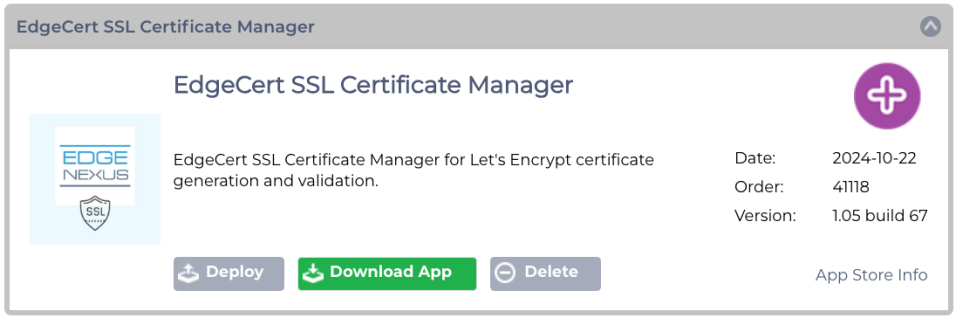
Le bouton Déployer permet de déployer l'application en tant que conteneur sécurisé, tandis que le bouton Supprimer permet de supprimer l'application au sein de l'ADC.

Application achetée



La première chose que vous remarquerez est l'utilisateur associé à l'App Store et le bouton qui lui est associé. Vous devrez vous connecter à l'aide de vos identifiants App Store pour que l'ADC soit associé à l'App Store. En dessous, vous trouverez les applications associées à votre compte.

Lorsque vous vous connectez à l'App Store, soit directement, soit via le portail intégré, vous pouvez acheter des applications. Celles-ci sont indiquées dans cette section et peuvent être téléchargées sur le CDA, prêtes à être déployées.



Chaque application dispose d'un certain nombre de boutons : Déployer, Télécharger l'application et Supprimer. En outre, un lien "App Store Info" se trouve sur le côté droit. Il permet d'accéder à la page de l'App Store concernée et d'afficher des informations sur l'addon.

Déployer

La section Apps dans Add-Ons détaille les applications que vous avez achetées, téléchargées et déployées. Une fois déployée, l'application apparaît dans la section Téléchargée.

Télécharger l'application

L'application peut être téléchargée à partir de l'App Store en cliquant sur ce bouton.

Supprimer

Si vous souhaitez supprimer une application qui a été téléchargée.

Authentification

La page Bibliothèque> Authentification permet de configurer des serveurs d'authentification et de créer des règles d'authentification.

Mise en place de l'authentification - Un flux de travail

Veuillez au moins suivre les étapes suivantes pour appliquer l'authentification à votre service.

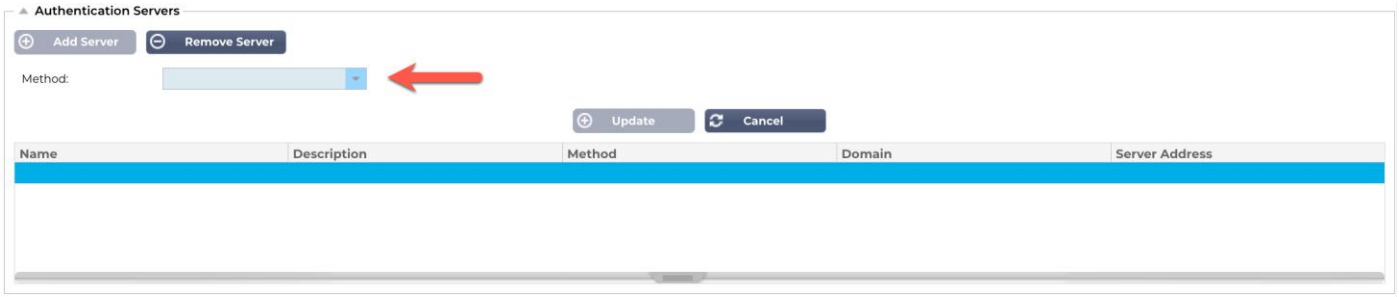
1. Créer un serveur d'authentification.
2. Créez une règle d'authentification qui utilise un serveur d'authentification.
3. Créer une règle flightPATH qui utilise une règle d'authentification.
4. Appliquer la règle flightPATH à un service

Serveurs d'authentification

Pour mettre en place une méthode d'authentification efficace, nous devons d'abord configurer un serveur d'authentification.

La première étape consiste à sélectionner la méthode d'authentification dont vous avez besoin.

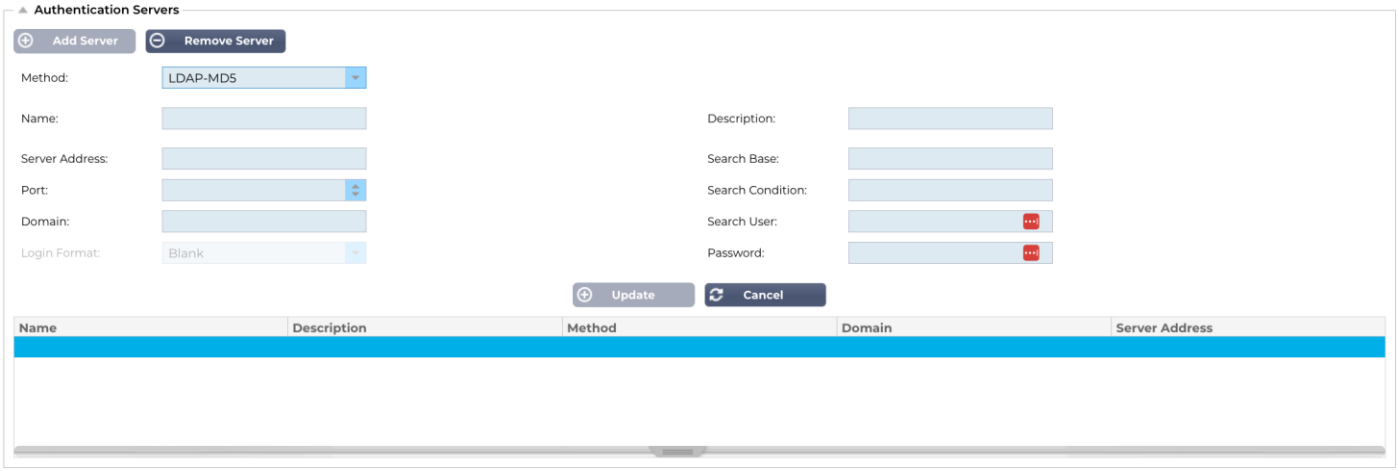
- Cliquez sur Ajouter un serveur.
- Sélectionnez la méthode dans le menu déroulant.



La fonction Serveur d'authentification est dynamique et n'affiche que les champs nécessaires à la méthode d'authentification choisie.

- Remplissez les champs avec précision afin d'assurer une connexion correcte aux serveurs.

Options pour LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius et SAML

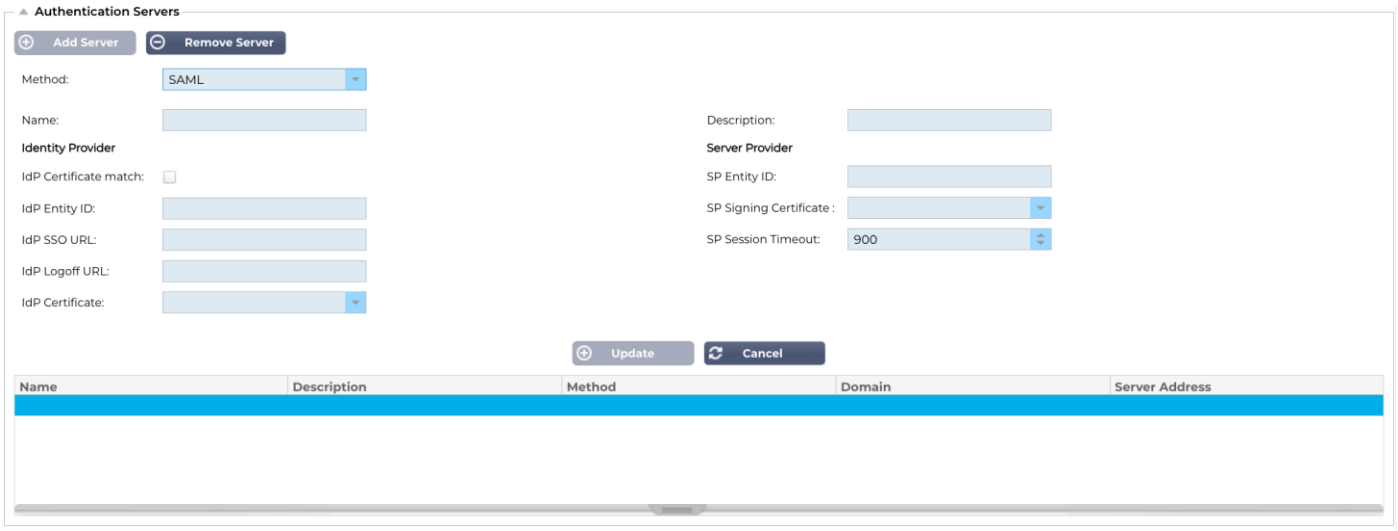


Option	Description

Méthode	Choisir une méthode d'authentification LDAP - LDAP de base avec des noms d'utilisateur et des mots de passe envoyés en texte clair au serveur LDAP. LDAP-MD5 - LDAP de base avec nom d'utilisateur en texte clair et mot de passe haché au MD5 pour une sécurité accrue. LDAPS - LDAP sur SSL. Envoie le mot de passe en clair dans un tunnel crypté entre l'ADC et le serveur LDAP. LDAPS-MD5 - LDAP sur SSL. Le mot de passe est haché par MD5 pour plus de sécurité dans un tunnel crypté entre l'ADC et le serveur LDAP.
Nom	Donnez un nom à votre serveur à des fins d'identification - ce nom est utilisé dans toutes les règles.
Adresse du serveur	Ajouter l'adresse IP ou le nom d'hôte du serveur d'authentification
Port	Pour LDAP et LDAPS, les ports sont définis par défaut sur 389 et 636. Pour Radius, le port est généralement 1812. Pour SAML, les ports sont définis dans l'ADC.
Domaine	Ajoutez le nom de domaine du serveur LDAP.
Format de connexion	Utilisez le format de connexion dont vous avez besoin. Nom d'utilisateur - avec ce format choisi, vous ne devez saisir que le nom d'utilisateur. Toutes les informations relatives à l'utilisateur et au domaine saisies par l'utilisateur sont supprimées et les informations relatives au domaine provenant du serveur sont utilisées. Nom d'utilisateur et domaine - L'utilisateur doit saisir la syntaxe complète du domaine et du nom d'utilisateur. Exemple : *mycompany\jdoe OR jdoe@mycompany*. Les informations relatives au domaine saisies au niveau du serveur sont ignorées. Blank - le CDA accepte tout ce que l'utilisateur saisit et l'envoie au serveur d'authentification. Cette option est utilisée lors de l'utilisation de MD5.
Description	Ajouter une description
Base de recherche	Cette valeur est le point de départ de la recherche dans la base de données LDAP. Exemple *dc=mycompany,dc=local*
Conditions de recherche	Les conditions de recherche doivent être conformes à la RFC 4515. Exemple : (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Recherche d'un utilisateur	Effectuez une recherche pour un utilisateur administrateur de domaine dans le serveur d'annuaire.
Mot de passe	Mot de passe de l'utilisateur administrateur du domaine.
Temps mort	Délai après lequel un serveur inactif est marqué comme étant à nouveau actif.

Options pour l'authentification SAML

IMPORTANT : Lorsque vous configurez l'authentification via SAML, vous devez créer une application d'entreprise pour Entra ID Authentication. Les instructions pour ce faire sont disponibles dans le chapitreConfiguration de l'application d'authentification Entra ID dans Microsoft Entra

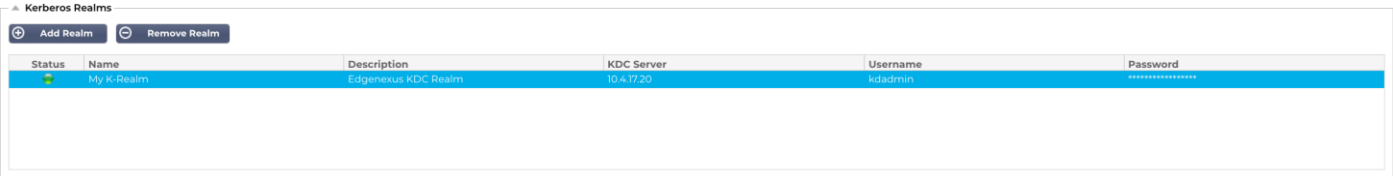


Option	Description
Méthode	Choisir une méthode d'authentification LDAP - LDAP de base avec des noms d'utilisateur et des mots de passe envoyés en texte clair au serveur LDAP. LDAP-MD5 - LDAP de base avec nom d'utilisateur en texte clair et mot de passe haché au MD5 pour une sécurité accrue. LDAPS - LDAP sur SSL. Envoie le mot de passe en clair dans un tunnel crypté entre l'ADC et le serveur LDAP. LDAPS-MD5 - LDAP sur SSL. Le mot de passe est haché par MD5 pour plus de sécurité dans un tunnel crypté entre l'ADC et le serveur LDAP.
Nom	Donnez un nom à votre serveur à des fins d'identification - ce nom est utilisé dans toutes les règles.
Fournisseur d'identité	
Correspondance des certificats IdP	La correspondance des certificats IdP fait référence au processus de vérification que le certificat numérique utilisé par un fournisseur d'identité (IdP) pour signer les assertions SAML correspond au certificat auquel le fournisseur de services (SP) fait confiance. Cette validation garantit que le fournisseur d'identité est légitime et que les assertions qu'il envoie sont authentiques et non modifiées. Le fournisseur de services stocke généralement le certificat de l'IdP dans ses métadonnées et compare le certificat intégré dans les assertions SAML à celui stocké pour déterminer une correspondance.
ID de l'entité IdP	Un identifiant d'entité SAML IdP est un identifiant unique au monde qui sert d'adresse définitive à un fournisseur d'identité (IdP) au sein de l'écosystème SAML (Security Assertion Markup Language). Cet identifiant est généralement une URL ou un URI qui distingue de manière unique l'IdP des autres entités impliquées dans les processus d'authentification et d'autorisation basés sur SAML. Il joue un rôle crucial dans l'établissement de la confiance et la facilitation d'une communication sécurisée entre les IdP, les fournisseurs de services (SP) et les utilisateurs.
IdP SSO URL	Une URL IdP SSO, abréviation de Single Sign-On URL, est une URL d'extrémité spécifique fournie par un fournisseur d'identité (IdP) qui sert de passerelle d'authentification pour initier des sessions d'authentification unique (SSO). Lorsqu'un utilisateur est redirigé vers cette URL, le fournisseur d'identité l'invite à s'authentifier à l'aide de ses données d'identification et, si l'authentification est réussie, il le redirige vers le fournisseur de services avec une assertion contenant les informations relatives à son identité. Cette assertion est ensuite validée par le fournisseur de services, ce qui permet à l'utilisateur d'accéder aux ressources du fournisseur de services sans avoir à s'authentifier à nouveau.
IdP Log off URL	L'URL de déconnexion SAML IdP est un point d'extrémité spécifique du fournisseur d'identité (IdP) qui lance et gère le processus de déconnexion pour les sessions d'authentification unique (SSO). Lorsqu'un utilisateur clique sur le bouton de déconnexion d'une application, celle-ci le redirige vers l'URL de déconnexion de l'IdP. L'IdP invalide alors la session de l'utilisateur auprès de toutes les parties utilisatrices associées à l'authentification SSO et renvoie une réponse de déconnexion à l'application, déconnectant ainsi l'utilisateur de toutes les applications connectées.
Certificat IdP	Un certificat SAML IdP est un certificat numérique X.509 délivré par une autorité de confiance à un fournisseur d'identité (IdP) qui participe aux protocoles d'authentification SAML (Security Assertion Markup Language). Ce certificat constitue un moyen sûr de vérifier l'identité du fournisseur d'identité et d'authentifier l'intégrité et la confidentialité des messages SAML échangés entre le fournisseur d'identité et les fournisseurs de services. Vous pouvez sélectionner le certificat IdP que vous aurez installé dans l'ADC en utilisant le menu déroulant.
Description	Une description de la définition.
Recherche d'un utilisateur	Effectuer une recherche pour un utilisateur administrateur de domaine.
Mot de passe	Pour spécifier le mot de passe de l'utilisateur admin.

Fournisseur de serveur	
ID de l'entité SP	Un SP Entity ID est un identifiant unique qui sert d'adresse globale pour un fournisseur de services spécifique (SP) dans le contexte du protocole SAML. Il s'agit d'un moyen normalisé d'identifier un fournisseur de services et il s'agit généralement d'une URL ou d'un autre URI qui indique les métadonnées SAML du fournisseur de services, lesquelles contiennent des informations essentielles telles que les certificats de cryptage et les points d'extrémité d'authentification.
Certificat de signature SP	Un certificat de signature SAML SP est un certificat X.509 utilisé par un fournisseur de services (SP) pour signer les réponses SAML, garantissant l'authenticité et l'intégrité des messages échangés entre le SP et le fournisseur d'identité (IdP) lors de l'authentification SSO (Single Sign-On). Le fournisseur de services signe la réponse à l'aide de sa clé privée et le fournisseur d'identité vérifie la signature à l'aide de la clé publique associée au certificat, confirmant ainsi l'identité de l'expéditeur et le fait que le contenu du message n'a pas été modifié.
SP Délai d'attente de la session	Le délai de session SP désigne la durée maximale pendant laquelle la session d'authentification d'un utilisateur est considérée comme valide du côté du fournisseur de services (SP) après une ouverture de session unique (SSO) réussie par l'intermédiaire d'un fournisseur d'identité (IdP). Passé ce délai, le fournisseur de services met fin à la session et demande à l'utilisateur de s'authentifier à nouveau pour retrouver l'accès aux ressources protégées. Ce mécanisme contribue à la protection contre les accès non autorisés et garantit que les sessions des utilisateurs ne restent pas inactives pendant de longues périodes.

KDC Realms

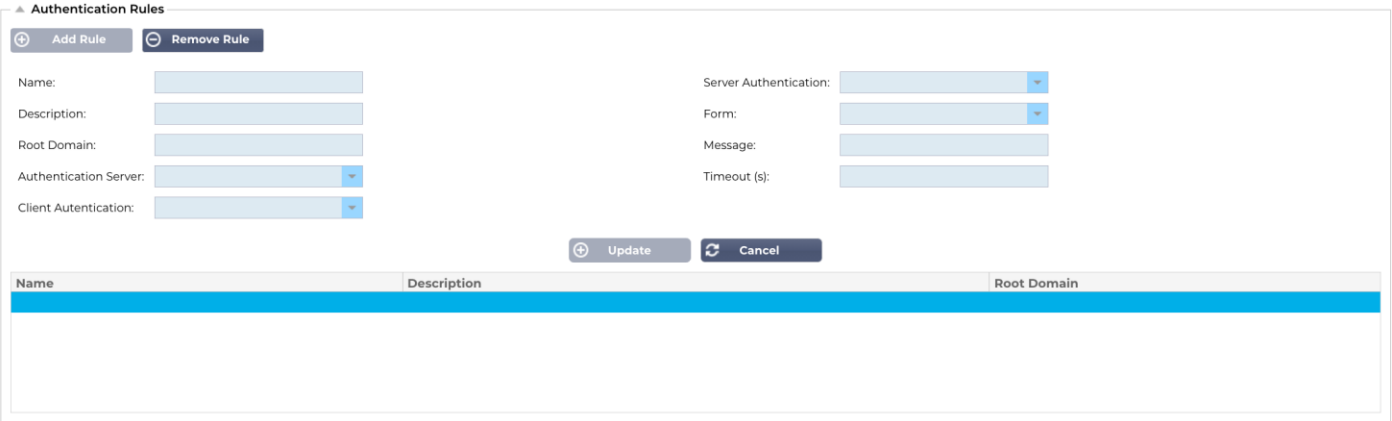
Les domaines KDC font référence aux configurations du protocole d'authentification Kerberos, où chaque domaine est essentiellement un domaine ou un réseau qui fonctionne sous un seul centre de distribution de clés (KDC). Cette configuration délimite un groupe de systèmes gérés par le même KDC principal, ce qui facilite l'authentification sécurisée et les mécanismes d'attribution de tickets à travers le réseau. Les domaines peuvent être hiérarchiques ou non, avec la possibilité d'établir des relations de confiance entre eux pour une authentification sécurisée entre domaines.



L'interface utilisateur de l'ADC, comme le montre l'image ci-dessus, vous permet de définir vos domaines Kerberos. Ces informations peuvent ensuite être utilisées dans les règles d'authentification.

Règles d'authentification

L'étape suivante consiste à créer les règles d'authentification à utiliser avec la définition du serveur.



Champ d'application	Description
Nom	Ajoutez un nom approprié à votre règle d'authentification.
Description	Ajoutez une description appropriée.
Domaine racine	Ce champ doit être laissé vide, sauf si vous avez besoin d'une connexion unique pour les sous-domaines.
Serveur d'authentification	Il s'agit d'une liste déroulante contenant les serveurs que vous avez configurés.
Authentification du client :	Choisissez la valeur correspondant à vos besoins : Basic (401) - Cette méthode utilise la méthode d'authentification standard 401. Formulaires - ce formulaire présente à l'utilisateur le formulaire par défaut de l'ADC. Dans le formulaire, vous pouvez ajouter un message. Vous pouvez sélectionner un formulaire que vous avez téléchargé en utilisant la section ci-dessous.
Authentification du serveur	Choisissez la valeur appropriée. Aucun - si votre serveur n'a pas d'authentification existante, sélectionnez ce paramètre. Ce paramètre signifie que vous pouvez ajouter des capacités d'authentification à un serveur qui n'en avait pas auparavant. Basic - si l'authentification de base (401) est activée sur votre serveur, sélectionnez BASIC. NTLM - si l'authentification NTLM est activée sur votre serveur, sélectionnez NTLM.
Formulaire	Choisir la valeur appropriée Défaut - En sélectionnant cette option, l'ADC utilisera sa forme intégrée. Personnalisé - vous pouvez ajouter un formulaire que vous avez conçu et le sélectionner ici.
Message	Ajouter un message personnel au formulaire.
Délai d'attente	Ajoutez un délai d'attente à la règle, après lequel l'utilisateur devra s'authentifier à nouveau. Notez que le paramètre Délai d'attente n'est valable que pour l'authentification basée sur les formulaires.

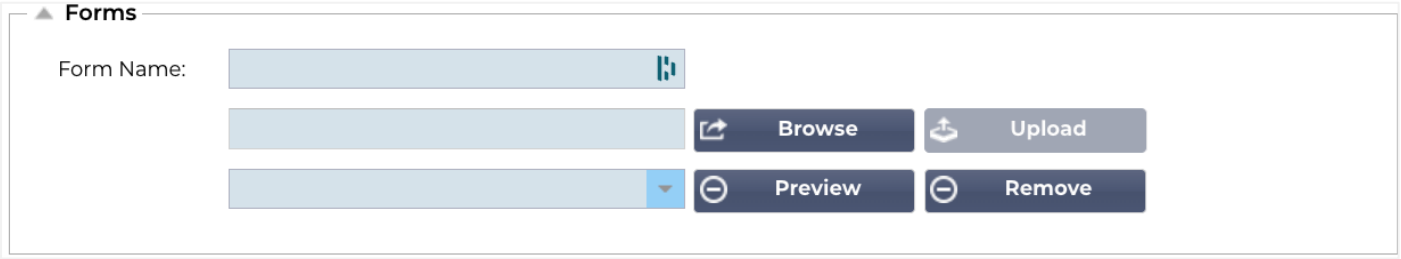
Si vous souhaitez fournir une connexion unique aux utilisateurs, complétez le champ Domaine racine avec votre domaine. Dans cet exemple, mycompany.com. Nous pouvons maintenant avoir plusieurs services qui utiliseront edgenexus.io comme domaine racine, et vous n'aurez à vous connecter qu'une seule fois. Si nous considérons les services suivants :

- SharePoint.monentreprise.com
- usercentral.mycompany.com
- App Store.mycompany.com

Ces services peuvent résider sur un seul VIP ou être répartis sur 3 VIP. Un utilisateur accédant à usercentral.mycompany.com pour la première fois se verra présenter un formulaire lui demandant de se connecter en fonction de la règle d'authentification utilisée. Le même utilisateur peut ensuite se connecter à

App Store.mycompany.com et sera automatiquement authentifié par l'ADC. Vous pouvez définir le délai d'attente, qui forcera l'authentification une fois cette période d'inactivité atteinte.

Formulaires



Cette section vous permet de télécharger un formulaire personnalisé.

Comment créer votre formulaire personnalisé

Bien que le formulaire de base fourni par l'ADC soit suffisant dans la plupart des cas, il peut arriver que les entreprises souhaitent présenter leur propre identité à l'utilisateur. Vous pouvez créer votre propre formulaire personnalisé que les utilisateurs devront remplir dans de tels cas. Ce formulaire doit être au format HTM ou HTML.

Option	Description
Nom	nom du formulaire = loginform action = %JNURL% Méthode = POST
Nom d'utilisateur	Syntaxe : name = "JNUSER"
Mot de passe :	name="JNPASS"
Message facultatif1 :	%JNMESSAGE%
Message facultatif2 :	%JNAUTHMESSAGE%
Images	Si vous souhaitez ajouter une image, veuillez l'ajouter en ligne en utilisant le codage Base64.

Exemple de code html d'un formulaire très simple et basique

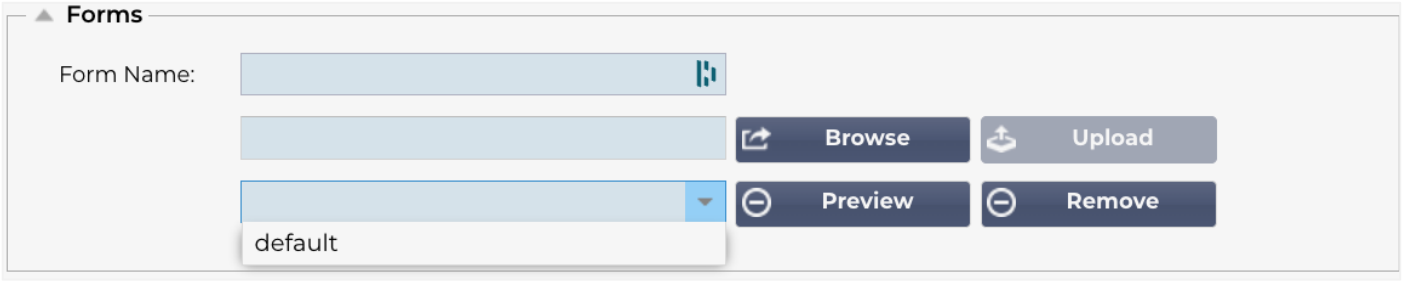
```
<HTML>
<HEAD>
<TITLE>EXEMPLE DE FORMULAIRE D'AUTHENTIFICATION</TITLE>
</HEAD>
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USER : <input type="text" name="JNUSER" size="20" value=""></br>
PASS : <input type="password" name="JNPASS" size="20" value=""></br>
<input type="submit" name="submit" value="OK">
</form>
</BODY>
</HTML>
```

Ajouter un formulaire personnalisé

Une fois que vous avez créé un formulaire personnalisé, vous pouvez l'ajouter en utilisant la section Formulaires.

1. Choisissez un nom pour votre formulaire
2. Rechercher localement votre formulaire
3. Cliquez sur Télécharger

Prévisualisation de votre formulaire personnalisé



Pour visualiser le formulaire personnalisé que vous venez de télécharger, sélectionnez-le et cliquez sur Aperçu. Vous pouvez également utiliser cette section pour supprimer les formulaires qui ne sont plus nécessaires

Note : Lorsque vous utilisez des produits de filtrage des cookies tels qu'AdGuard, vous pouvez obtenir un message d'erreur 404. Pour éviter cela, mettez l'adresse IP de l'ADC sur liste blanche.

Cache

L'ADC est capable de mettre en cache des données dans sa mémoire interne et d'améliorer la fourniture de services web. Les paramètres qui gèrent cette fonctionnalité sont décrits dans cette section.

Paramètres globaux du cache

Taille maximale du cache (Mo)

Cette valeur détermine la RAM maximale que le cache peut consommer. Le cache de l'ADC est un cache en mémoire qui est aussi périodiquement vidé sur le support de stockage afin de maintenir la persistance du cache après les redémarrages, les redémarrages et les opérations d'arrêt. Cette fonctionnalité signifie que la taille maximale du cache doit s'inscrire dans l'empreinte mémoire de l'appliance (plutôt que dans l'espace disque) et ne doit pas dépasser la moitié de la mémoire disponible.

Taille du cache souhaitée (Mo)

Cette valeur indique la RAM optimale à laquelle le cache sera réduit. Alors que la taille maximale du cache représente la limite supérieure absolue du cache, la taille souhaitée du cache est conçue comme la taille optimale que le cache doit tenter d'atteindre chaque fois qu'une vérification automatique ou manuelle de la taille du cache est effectuée. L'écart entre la taille maximale et la taille souhaitée de la mémoire cache existe pour tenir compte de l'arrivée et du chevauchement de nouveaux contenus entre les vérifications périodiques de la taille de la mémoire cache afin d'éliminer les contenus périmés. Une fois encore, il peut être plus efficace d'accepter la valeur par défaut (30 Mo) et de vérifier périodiquement la taille du cache dans "Moniteur -> Statistiques" pour déterminer la taille appropriée.

Temps de mise en cache par défaut (J/HH:MM)

La valeur saisie ici représente la durée de vie du contenu sans valeur d'expiration explicite. La durée de mise en cache par défaut est la période pendant laquelle le contenu sans directive "no-store" ou sans délai d'expiration explicite dans l'en-tête de trafic est stocké.

L'entrée du champ prend la forme "D/HH:MM" - ainsi, une entrée de "1/01:01" (la valeur par défaut est 1/00:00) signifie que l'ADC conservera le contenu pendant un jour, "01:00" pendant une heure et "00:01" pendant une minute.

Codes de réponse HTTP pouvant être mis en cache

Les réponses HTTP constituent l'un des ensembles de données mis en cache. Les codes de réponse HTTP mis en cache sont les suivants :

- 200 - Réponse standard pour les requêtes HTTP réussies
- 203 - Les en-têtes ne sont pas définitifs mais proviennent d'une copie locale ou d'un tiers.
- 301 - Une nouvelle URL permanente a été attribuée à la ressource demandée.

- 304 - N'a pas été modifié depuis la dernière demande et une copie mise en cache localement doit être utilisée à la place.
- 410 - La ressource n'est plus disponible sur le serveur et aucune adresse de réacheminement n'est connue.

Ce champ doit être modifié avec prudence, car les codes de réponse les plus courants sont déjà répertoriés.

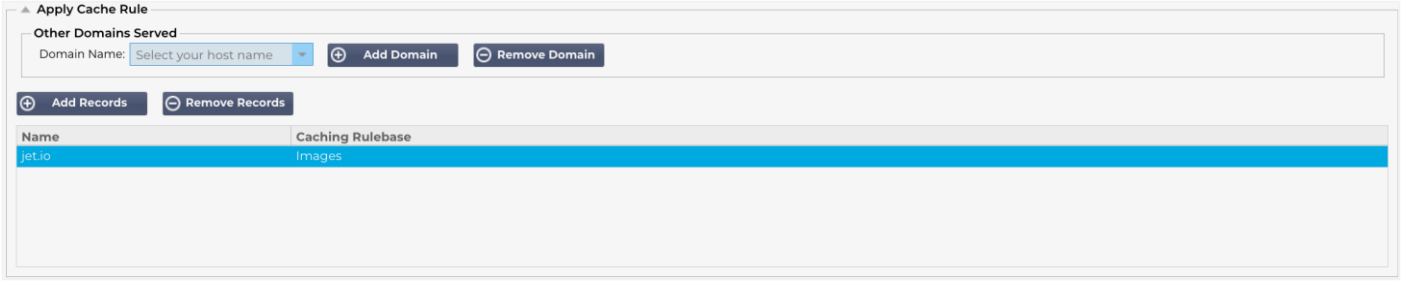
Minuterie de vérification de la mémoire cache (J/HH:MM)

Ce paramètre détermine l'intervalle de temps entre les opérations de découpage du cache.

Compte de remplissage du cache

Ce paramètre est une fonction d'aide qui permet de remplir le cache lorsqu'un certain nombre de 304 ont été détectés.

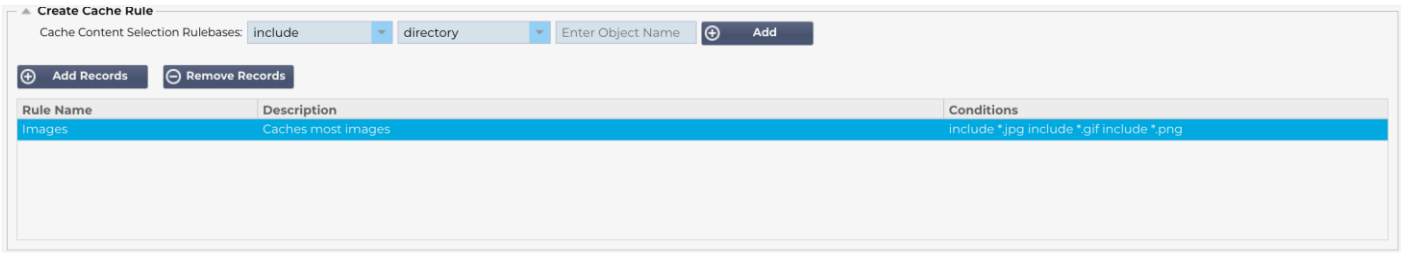
Appliquer la règle de mise en cache



Cette section permet d'appliquer une règle de cache à un domaine :

- Ajoutez le domaine manuellement à l'aide du bouton Ajouter des enregistrements. Vous devez utiliser un nom de domaine entièrement qualifié ou une adresse IP en notation décimale pointée. Exemple www.mycompany.com ou 192.168.3.1:80
- Cliquez sur la flèche du menu déroulant et choisissez votre domaine dans la liste.
- La liste sera alimentée tant que le trafic aura transité par un service virtuel et qu'une stratégie de mise en cache aura été appliquée au service virtuel.
- Choisissez votre règle de cache en double-cliquant sur la colonne Caching Rulebase et en sélectionnant dans la liste

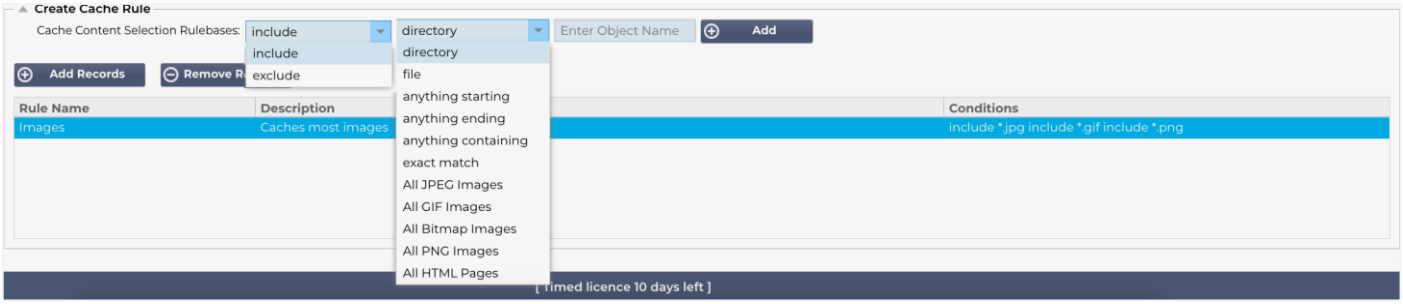
Créer une règle de mise en cache



Cette section vous permet de créer plusieurs règles de mise en cache différentes qui peuvent ensuite être appliquées à un domaine :

- Cliquez sur Ajouter des enregistrements et donnez un nom et une description à votre règle.
- Vous pouvez saisir vos conditions manuellement ou utiliser la fonction Ajouter une condition

Pour ajouter une condition à l'aide de la base de règles de sélection :



- Choisissez Inclure ou Exclure.
- Choisissez un critère de sélection, par exemple, Toutes les images JPEG
- Cliquez sur le symbole + Ajouter.
- Vous constaterez que l'expression "inclure *.jpg" a été ajoutée aux conditions.
- Vous pouvez ajouter d'autres conditions. Si vous choisissez de le faire manuellement, vous devez ajouter chaque condition sur une NOUVELLE ligne. Veuillez noter vos règles s'afficheront sur la même ligne jusqu'à ce que vous cliquiez dans la case Conditions, après quoi elles s'afficheront sur une ligne distincte.

chemin d'accès au vol

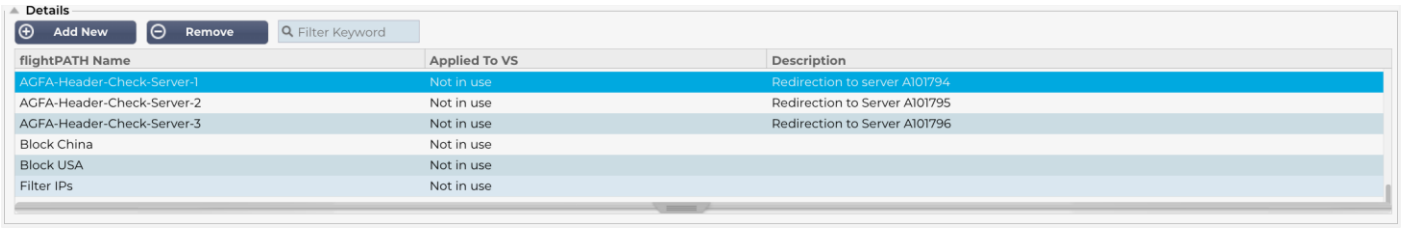
flightPATH est la technologie de gestion du trafic intégrée à l'ADC. Elle permet d'inspecter le trafic HTTP et HTTPS en temps réel et d'effectuer des actions en fonction des conditions.

Pour utiliser les règles flightPATH, il faut les appliquer à un service virtuel en utilisant l'onglet flightPATH dans la section Real Servers.

Une règle de trajectoire de vol se compose de quatre éléments :

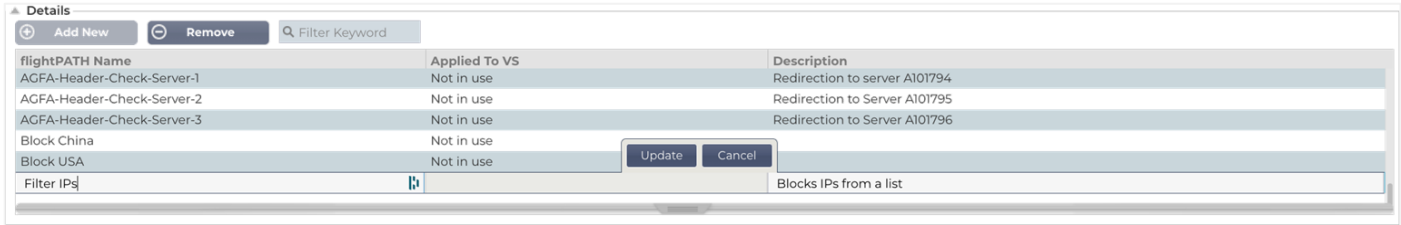
1. Détails, où vous définissez le nom de flightPATH et le service auquel il est rattaché.
2. Condition(s) pouvant être définie(s) qui entraîne(nt) le déclenchement de la règle.
3. Évaluation qui permet de définir des variables pouvant être utilisées dans les actions.
4. Actions utilisées pour gérer ce qui doit se passer lorsque des conditions sont remplies.

Détails



La section Détails présente les règles flightPATH disponibles. Vous pouvez ajouter de nouvelles règles flightPATH et supprimer celles qui sont définies dans cette section.

Ajout d'une nouvelle règle flightPATH



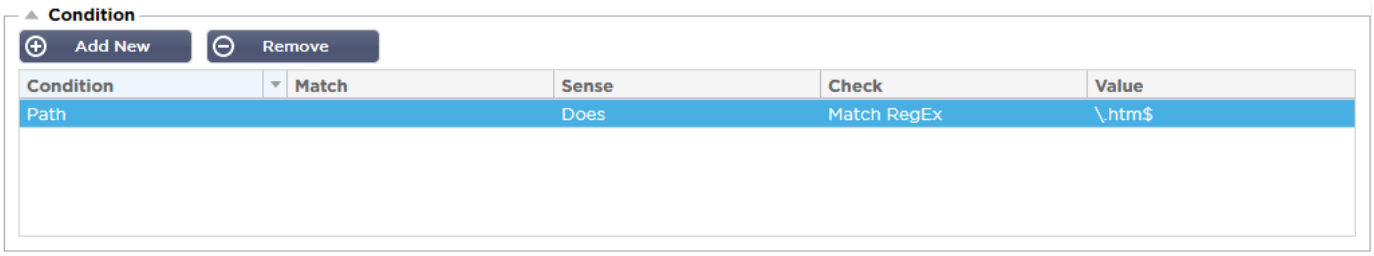
Champ d'application	Description
Nom de FlightPATH	Ce champ contient le nom de la règle flightPATH. Le nom que vous indiquez ici apparaît et est référencé dans d'autres parties de l'ADC.
Appliqué au VS	Cette colonne est en lecture seule et indique le VIP auquel la règle flightPATH est appliquée.
Description	Valeur représentant une description fournie à des fins de lisibilité.

Étapes à suivre pour ajouter une règle flightPATH

1. Tout d'abord, cliquez sur le bouton Ajouter un nouveau situé dans la section Détails.
2. Saisissez un nom pour votre règle. Exemple Auth2
3. Saisissez une description de votre règle
4. Une fois que la règle a été appliquée à un service, la colonne Appliqué à se remplit automatiquement d'une adresse IP et d'une valeur de port.
5. N'oubliez pas de cliquer sur le bouton "Mettre à jour" pour enregistrer vos modifications. Si vous faites une erreur, il vous suffit de cliquer sur "Annuler" pour revenir à l'état précédent.

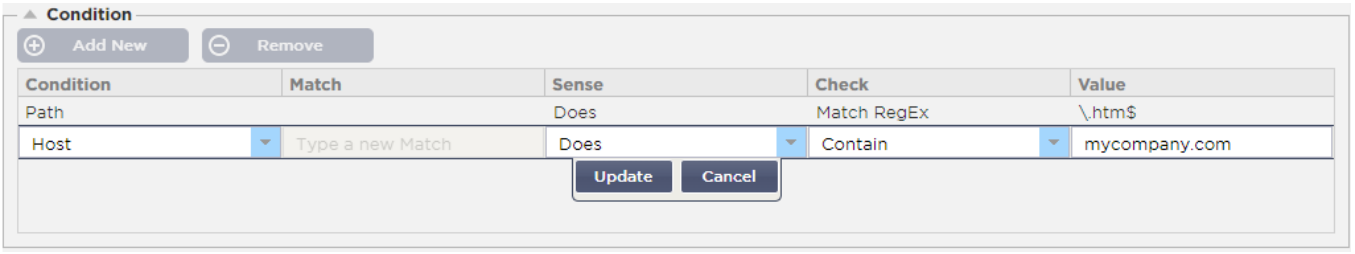
Condition

Une règle flightPATH peut comporter un nombre illimité de conditions. Les conditions fonctionnent sur une base **ET**, ce qui vous permet de définir la condition de déclenchement de l'action. Si vous souhaitez utiliser une condition **OR**, créez des règles flightPATH supplémentaires et appliquez-les au VIP dans le bon ordre.



Vous pouvez également utiliser RegEx en sélectionnant Match RegEx dans le champ Check et la valeur RegEx dans le champ Value. L'inclusion de l'évaluation RegEx élargit considérablement les possibilités de flightPATH.

Création d'une nouvelle condition flightPATH



Vous devez d'abord sélectionner une valeur dans la colonne Condition.

Nous fournissons plusieurs conditions dans la liste déroulante et couvrons tous les scénarios prévus. Lorsque de nouvelles conditions seront ajoutées, elles seront disponibles via les mises à jour de Jetpack.

Les choix possibles sont les suivants :

CONDITION	DESCRIPTION	EXEMPLE
<form>	Les formulaires HTML sont utilisés pour transmettre des données à un serveur	Exemple "le formulaire n'a pas la longueur 0".
Localisation du GEO	Compare l'adresse IP source aux codes pays ISO 3166	GEO Location est égal à GB, OU GEO Location est égal à Germany
Hôte	Hôte extrait de l'URL	www.mywebsite.com ou 192.168.1.1
Langue	Langue extraite de l'en-tête HTTP langue	Cette condition produira un menu déroulant avec une liste de langues.
Méthode	Liste déroulante des méthodes HTTP	Liste déroulante comprenant GET, POST, etc.
Origine IP	Si le proxy en amont prend en charge X-Forwarded-for (XFF), il utilisera la véritable adresse d'origine.	IP du client. Il peut également utiliser plusieurs IP ou sous-réseaux. 10.1.2.* est le sous-réseau 10.1.2.0 /24 10\N- 1\N- 2\N- 3|10\N- 1\N- 2\N- 4 Utiliser | pour des IP multiples
Chemin d'accès	Chemin d'accès au site web	/mon site web/index.asp
POST	Méthode de requête POST	Vérifier les données téléchargées sur un site web

Demande de renseignements	Nom et valeur d'une requête, et peut accepter soit le nom de la requête, soit une valeur également.	"Best=jetNEXUS" Lorsque la correspondance est Best et la valeur est edgeNEXUS
Chaîne de requête	Toute la chaîne de requête après le caractère ?	
Demande de cookie	Nom d'un cookie demandé par un client	MS-WSMAN=afYfn1CDqqCDqUD: :
En-tête de la demande	Tout en-tête HTTP	Referrer, User-Agent, From, Date
Demande de version	La version HTTP	HTTP/1.0 OU HTTP/1.1
Organe de réponse	Une chaîne définie par l'utilisateur dans le corps de la réponse	Serveur UP
Code de réponse	Le code HTTP de la réponse	200 OK, 304 Non modifié
Cookie de réponse	Le nom d'un cookie envoyé par le serveur	MS-WSMAN=afYfn1CDqqCDqUD: :
En-tête de réponse	Tout en-tête HTTP	Referrer, User-Agent, From, Date
Version de la réponse	La version HTTP envoyée par le serveur	HTTP/1.0 OU HTTP/1.1
Source IP	Soit l'adresse IP d'origine, soit l'adresse IP du serveur proxy, soit une autre adresse IP agrégée.	IP du client, IP du proxy, IP du pare-feu. Il est également possible d'utiliser plusieurs IP et sous-réseaux. Les points doivent être échappés car il s'agit de RegEX. Exemple 10.1.2.3 est 10.1.2.3

Correspondance

Le champ Correspondance peut être une liste déroulante ou une valeur textuelle et peut être défini en fonction de la valeur du champ Condition. Par exemple, si la condition est définie sur Hôte, le champ Correspondance n'est pas disponible. Si la condition est <form>, le champ de concordance est affiché sous forme de texte et si la condition est POST, le champ de concordance est présenté sous forme de liste déroulante contenant des valeurs pertinentes.

Les choix possibles sont les suivants :

MATCH	DESCRIPTION	EXEMPLE
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodages acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>
Acceptation de la langue	Langues acceptables pour la réponse	Accept-Language : en-US
Plages d'acceptation	Types de plages de contenu partiel pris en charge par ce serveur	Accept-Ranges : bytes
Autorisation	Données d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==.
Charge-To	Contient des informations comptables relatives aux coûts de l'application de la méthode demandée.	

Content-Encoding	Le type d'encodage utilisé	Content-Encoding : gzip
Longueur du contenu	Longueur du corps de la réponse en octets (octets de 8 bits)	Content-Length : 348
Content-Type	Le type de mime du corps de la requête (utilisé avec les requêtes POST et PUT)	Content-Type : application/x-www-form-urlencoded
Cookie	Un cookie HTTP précédemment envoyé par le serveur avec Set-Cookie (ci-dessous)	Cookie : $Version=1 ; Skin=new ;
Date	Date et heure d'émission du message	Date = "Date" " :" HTTP-date
ETag	Identifiant d'une version spécifique d'une ressource, souvent un condensé de message.	ETag : "aed6bdb8e090cd1:0"
De	L'adresse électronique de l'utilisateur qui fait la demande	De : user@example.com
Si modifié depuis	Permet de renvoyer un message 304 Non modifié si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	Date de la dernière modification de l'objet demandé, au format RFC 2822	Dernière modification : Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Mise en œuvre : En-têtes spécifiques qui peuvent avoir divers effets tout au long de la chaîne demande-réponse.	Pragma : no-cache
Référent	Adresse de la page web précédente à partir de laquelle un lien vers la page actuellement demandée a été suivi	Référent : HTTP://www.edgenexus.io
Serveur	Un nom pour le serveur	Serveur : Apache/2.4.1 (Unix)
Set-Cookie	Un cookie HTTP	Set-Cookie : UserID=JohnDoe ; Max-Age=3600 ; Version=1
User-Agent	Chaîne de caractères de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Variable	Indique aux mandataires en aval comment faire correspondre les futurs en-têtes de requête pour décider si la réponse mise en cache peut être utilisée plutôt que de demander une nouvelle réponse. si la réponse mise en cache peut être utilisée plutôt que d'en demander une nouvelle au au serveur d'origine	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple ASP.NET, PHP, JBoss) qui supporte l'application web.	X-Powered-By : PHP/5.4.0

Sens

Le champ Sens est un champ booléen déroulant qui contient des choix de type "Fait" ou "Ne fait pas".

Vérifier

Le champ Contrôle permet de définir des valeurs de contrôle par rapport à la condition.

Les choix possibles sont les suivants : Contenir, Terminer, Égal, Exister, Avoir une longueur, Correspondre à RegEx, Correspondre à la liste, Commencer, Dépasser la longueur

VÉRIFIER	DESCRIPTION	EXEMPLE

Exister	Cela ne concerne pas les détails de la condition, mais seulement le fait qu'elle existe ou n'existe pas.	Hôte> Existe-t-il> ?
Démarrage	La chaîne commence par la valeur	Chemin d'accès> Fait> Commence /secure>
Fin	La chaîne se termine par la valeur	Le chemin> se termine par> - .jpg
Contenir	La chaîne contient bien la valeur	Request Header> Accept> Does> Contain> image
Égalité	La chaîne est égale à la valeur	Hôte> Est-ce que> est égal à> www.edgenexus.io
Avoir de la longueur	La chaîne a une longueur de la valeur	Hôte> Est-ce que> a la longueur> 16 www.edgenexus.io = VRAI www.edgenexus.com = FAUX
Match RegEx	Permet de saisir une expression régulière complète compatible avec Perl	Origin IP> Does> Match Regex
Liste des matches	Permet de comparer la valeur à une liste de valeurs. Ceci est utile lorsqu'il y a, par exemple, des adresses IP spécifiques qui doivent être comparées. Les valeurs sont séparées par des virgules (,) ou des points (|).	Source IP> Does > Match List > 10.10.10.1, 10.10.10.2, 10.10.10.3 etc.
Dépasser la longueur	Permet de vérifier si la valeur dépasse la longueur spécifiée.	Chemin > Does > Exceed Length > 200

Étapes à suivre pour ajouter une condition

Il est très facile d'ajouter une nouvelle condition flightPATH. Un exemple est présenté ci-dessus.

1. Cliquez sur le bouton Ajouter un nouveau dans la zone Condition.
2. Choisissez une condition dans la liste déroulante. Prenons l'exemple de l'hôte. Vous pouvez également taper dans le champ et l'ADC affichera la valeur dans une liste déroulante.
3. Choisissez un sens. Par exemple, est-ce que
4. Choisissez un contrôle. Par exemple, Contenir
5. Choisissez une valeur. Par exemple, monentreprise.com

L'exemple ci-dessus montre qu'il existe deux conditions qui doivent toutes deux être VRAIES pour que la règle soit appliquée

- La première consiste à vérifier que l'objet demandé est une image
- La seconde vérifie si l'hôte dans l'URL est www.imagepool.com

L'évaluation

La possibilité d'ajouter des variables définissables est une capacité convaincante. D'autres CDA offrent cette possibilité en utilisant des options de script ou de ligne de commande qui ne sont pas idéales pour tout le monde. L'EdgeADC vous permet de définir un nombre illimité de variables à l'aide d'une interface graphique facile à utiliser, comme illustré et décrit ci-dessous.

La définition de la variable flightPATH comprend quatre entrées à effectuer.

- Variable - il s'agit du nom de la variable
- Source - une liste déroulante de points sources possibles

- Détail - sélectionner des valeurs dans une liste déroulante ou les saisir manuellement.
- Valeur - la valeur que la variable contient et qui peut être une valeur alphanumérique ou un RegEx pour un réglage plus fin.

Variables intégrées :

Les variables intégrées ont déjà été codées en dur, il n'est donc pas nécessaire de créer une entrée d'évaluation pour celles-ci.

Vous pouvez utiliser n'importe laquelle des variables énumérées ci-dessous dans la section Action.

- $sourceip$ - L'adresse IP source de la requête
- $sourceport$ - Le port source qui a été utilisé
- $clientip$ - L'adresse IP du client
- $clientport$ - Le port utilisé par le client
- $host$ - L'hôte nommé dans la demande
- $method$ - La méthode utilisée : GET, POST, etc.
- $path$ - Le chemin d'accès spécifié dans la demande
- $querystring$ - La chaîne de requête utilisée dans la demande
- $version$ - La version de la requête HTTP dans le REQUEST (seules les versions 1 et 1.1 sont autorisées à l'heure actuelle).
- $resp$ - La RÉPONSE du serveur, par exemple 200OK, 404, etc.
- $geolocation$ - L'emplacement GEO d'où provient la demande.

ACTION	CIBLE
Action = Redirection 302	Cible = HTTPs://$host$/404.html
Action = Enregistrer	Cible = Un client de $sourceip$:$sourceport$ vient de faire une requête $path$ page

Explication :

- Un client accédant à une page qui n'existe pas se verrait normalement présenter la page d'erreur 404 du navigateur.
- Au lieu de cela, l'utilisateur est redirigé vers le nom d'hôte original qu'il a utilisé, mais le chemin incorrect est remplacé par 404.html.
- Une entrée est ajoutée au Syslog, disant : "Un client de 154.3.22.14:3454 vient de demander la page wrong.html".

Action

L'étape suivante consiste à ajouter une action associée à la règle et à la condition flightPATH.

Dans cet exemple, nous voulons réécrire la partie chemin de l'URL pour refléter l'URL tapée par l'utilisateur.

- Cliquez sur Ajouter nouveau
- Choisissez Réécrire le chemin dans le menu déroulant Action
- Dans le champ Cible, tapez $path$/myimages
- Cliquez sur Mise à jour

Cette action ajoutera /myimages au chemin, de sorte que l'URL finale devienne www.imagepool.com/myimages

Action	Description	Exemple
Ajouter un cookie de demande	Ajouter le cookie de demande détaillé dans la section Cible avec la valeur dans la section Données	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter un en-tête de demande	Ajouter un en-tête de requête de type Target avec une valeur dans la section Data	Target= Accept Data= image/png
Ajouter un cookie de réponse	Ajouter le cookie de réponse détaillé dans la section Cible avec la valeur dans la section Données	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter un en-tête de réponse	Ajouter l'en-tête de la demande détaillé dans la section Target avec la valeur dans la section Data	Target= Cache-Control Data= max-age=8888888
Corps Remplacer tout	Rechercher dans le corps de la réponse et remplacer toutes les instances	Target= http:// (chaîne de recherche) Data= https:// (chaîne de remplacement)
Remplacer le corps d'abord	Rechercher l'élément de réponse et remplacer la première instance uniquement	Target= http:// (chaîne de recherche) Data= https:// (chaîne de remplacement)
Corps Remplacer le dernier	Rechercher le corps de la réponse et remplacer la dernière instance uniquement	Target= http:// (chaîne de recherche) Data= https:// (chaîne de remplacement)
Chute	La connexion sera interrompue	Objectif= N/A Données= N/A
Courriel	Permet d'envoyer un courrier électronique à l'adresse configurée dans les événements de courrier électronique. Vous pouvez utiliser une variable comme adresse ou comme message.	Target= "flightPATH a envoyé cet événement par e-mail" Data= N/A

Événement de journal	Cela permet d'enregistrer un événement dans le journal du système	Target= "flightPATH a enregistré ceci dans le syslog" Data= N/A
Redirection 301	Cette opération entraînera une redirection permanente	Objectif= http://www.edgenexus.io Données= N/A
Redirection 302	Cette opération entraîne une redirection temporaire	Objectif= http://www.edgenexus.io Données= N/A
Supprimer le cookie de demande	Supprimer le cookie de demande détaillé dans la section Cible	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Supprimer l'en-tête de la demande	Supprimer l'en-tête de la demande détaillé dans la section Cible	Cible=Serveur Données=N/A
Supprimer la réponse	Supprimer le cookie de réponse détaillé dans la section Cible Cookie	Cible=jnAccel
Supprimer la réponse	Supprimer l'en-tête de réponse détaillé dans la section Cible En-tête	Cible= Etag Données= N/A
Remplacer le cookie de demande	Remplacer le cookie de demande détaillé dans la section Cible par la valeur indiquée dans la section Données	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remplacer l'en-tête de la demande	Remplacer l'en-tête de la requête dans la cible par la valeur des données	Cible= Connexion Données= keep-alive
Remplacer la	Remplacer le cookie de réponse indiqué dans la section Cible par la valeur indiquée dans la section Données Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
Remplacer la réponse	Remplacer l'en-tête de la réponse indiqué dans la section "Cible" par la valeur indiquée dans la section "Données" En-tête	Target= Server Data= Withheld for Security (Cible = Serveur - Données non divulguées pour des raisons de sécurité)

Chemin de réécriture	Cela vous permettra de rediriger la demande vers une nouvelle URL en fonction de la condition suivante	Target= /test/path/index.html$querystring$ Data= N/A
Utiliser un serveur sécurisé	Sélectionner le serveur sécurisé ou le service virtuel à utiliser	Target=192.168.101:443 Data=N/A
Utiliser le	Sélectionner le serveur ou le service virtuel à utiliser	Cible= 192.168.101:80 Données= N/A
Cryptage du cookie	Cela permet de crypter les cookies en 3DES et de les encoder en base64.	Target= Saisir le nom du cookie à crypter, vous pouvez utiliser * comme joker à la fin Data= Saisir une phrase de passe pour le cryptage

Scénario d'une règle flightPATH

Un client possède un site de commerce électronique et rencontre des problèmes avec les cookies qui sont bloqués par les dernières versions d'un navigateur.

Le client retrace les problèmes et découvre que la cause première est l'absence de marquage "sécurisé" et "sur le même site" pour les cookies en question.

Voyons comment flightPATH peut vous aider.

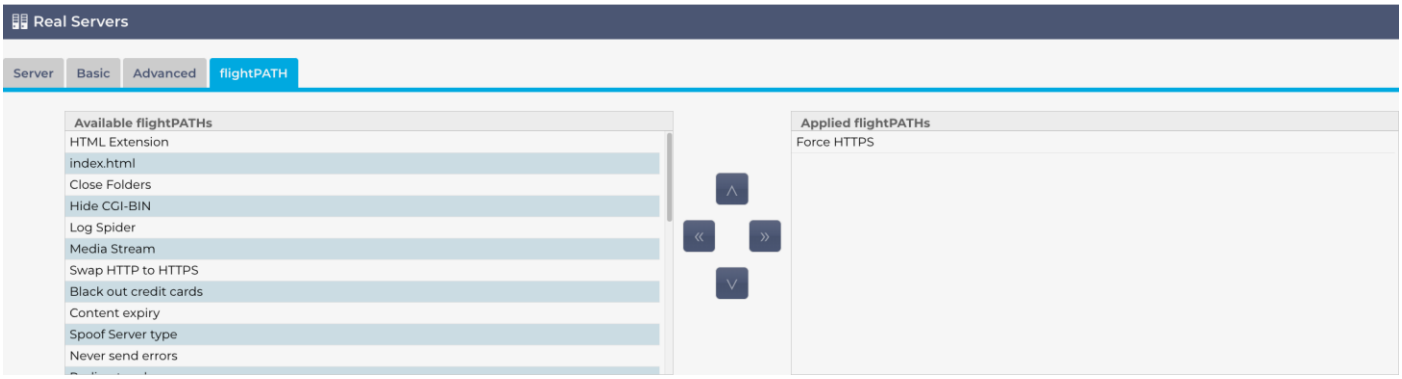
- Nous avons un cookie nommé 'wp_woocommerce_session_97929973749972642'
- Le nom du cookie est "wp_woocommerce_session_" avec une valeur d'identification unique aléatoire de "97929973749972642" générée par le système de commerce électronique.
- Les balises "same-site" et "secure" semblent être vides, ce qui signifie que le cookie est bloqué par les nouvelles restrictions de sécurité du navigateur.
- Pour éviter cela, nous pouvons créer les règles flightPATH suivantes.
- **flightPATH Règle pour l'identifiant de session**
    - **Condition** :
      Laisser en blanc
    - **Évaluation** :
      Variable = $variable_1$
      Source = cookie de réponse
      Détail = wp_woocommerce_session_*
    - Action
      Action = Remplacer le cookie de la réponse
      Cible = wp_woocommerce_session_*
      Données = $variable_1$
- **Règle flightPATH pour les étiquettes**
    - **Condition :**
      Condition = Cookie de réponse
      Correspondance = woocommerce_cart_hash
      Sense = Fait
      Check = Existe
      Valeur = Laisser vide

- **Évaluation :**
  Variable = $variable_2$
  Source = Cookie de réponse
  Détail = woocommerce_cart_hash
  Valeur = Laisser vide
- **Action :**
  Action = Remplacer le cookie de réponse
  Cible = woocommerce_cart_hash
  Données = $variable_2$,SameSite=None,Secure

Vous pouvez maintenant appliquer les règles au(x) service(s) virtuel(s) qui le nécessite(nt).

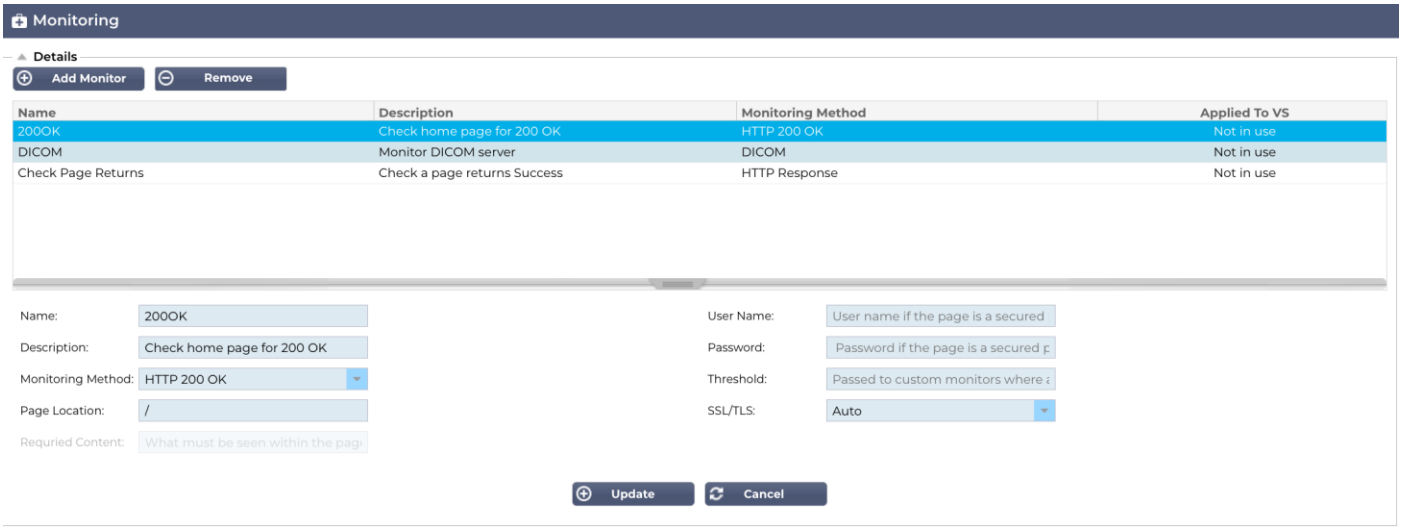
Application de la règle flightPATH

L'application d'une règle flightPATH se fait dans l'onglet flightPATH de chaque VIP/VS.



- Naviguez vers Services > IP Services et choisissez le VIP auquel vous souhaitez assigner la règle flightPATH.
- La liste des serveurs réels s'affiche comme suit
- Cliquer sur l'onglet flightPATH
- Sélectionnez la règle flightPATH que vous avez configurée ou l'une des règles prédéfinies prises en charge. Vous pouvez sélectionner plusieurs règles flightPATH si nécessaire.
- Glissez-déposez l'ensemble sélectionné dans la section Applied flightPATHs ou cliquez sur le bouton fléché >>.
- La règle sera déplacée vers la droite et appliquée automatiquement.

Moniteurs de serveur réels



La surveillance de serveurs réels est importante dans un scénario d'équilibrage de charge pour détecter et répondre aux problèmes des serveurs, assurer une distribution équilibrée de la charge, optimiser l'utilisation des ressources, donner la priorité aux services critiques, et identifier et traiter les vulnérabilités des logiciels.

La page Library> Real Server Monitors vous permet d'ajouter, d'afficher et de modifier une surveillance personnalisée. Il s'agit de "bilans de santé" du serveur de couche 7, que vous pouvez sélectionner dans le champ Surveillance du serveur de l'onglet Basique du service virtuel que vous définissez.

Types de moniteurs Real Server

Plusieurs moniteurs de Real Server sont disponibles, et le tableau ci-dessous les explique. Vous pouvez, bien sûr, écrire des moniteurs supplémentaires en utilisant PERL.

Méthode de contrôle	Description	Exemple
HTTP 200 OK	Une connexion TCP est établie avec le Real Server. Une fois la connexion établie, une brève requête HTTP est envoyée au Real Server. Lorsque la réponse est reçue, la chaîne "200 OK" est vérifiée. Si elle est présente, le serveur est considéré comme opérationnel. Veuillez noter que l'utilisation de ce moniteur permet de récupérer la page entière avec son contenu. Cette méthode de surveillance ne peut vraiment être utilisée qu'avec les types de service HTTP et HTTP accéléré. Toutefois, si un type de service de couche 4 est utilisé pour un serveur HTTP, il peut toujours être utilisé si SSL n'est pas utilisé sur le serveur réel ou géré de manière appropriée par la fonction "Content SSL".	**Demande** GET / HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Content-Type : text/html Dernière modification : Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges : bytes ETag : "0dd3253a59ad31:0" Serveur : Microsoft-IIS/10.0 Date : Tue, 13 Jul 2021 15:55:47 GMT Contenu-Longueur : 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml">

		<b>En-tête> <meta http-equiv="Content-Type" content="text/html ; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- corps { couleur:#FFFFFF ; ... </body> </html>
HTTP 200 En-tête	Une connexion TCP est établie avec le serveur Real, le champ PATH spécifiant l'emplacement à vérifier. L'en-tête de la réponse est extrait du serveur, le contenu étant écarté. La réponse est vérifiée pour 200 OK. Si c'est le cas, le serveur est considéré comme opérationnel. Veuillez noter que l'utilisation de ce moniteur ne permet de récupérer que la partie tête. Cette méthode de surveillance ne peut vraiment être utilisée qu'avec les types de service HTTP et HTTP accéléré. Toutefois, si un type de service de couche 4 est utilisé pour un serveur HTTP, il peut toujours être utilisé si SSL n'est pas utilisé sur le serveur réel ou géré de manière appropriée par la fonction "Content SSL".	**Demande** HEAD / HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Contenu-Longueur : 1364 Content-Type : text/html Dernière modification : Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges : bytes ETag : "0dd3253a59ad31:0" Serveur : Microsoft-IIS/10.0 Date : Tue, 13 Jul 2021 15:49:19 GMT
Options HTTP 200	Une connexion TCP est établie avec le serveur Real et une demande d'options est formulée. Les options sont renvoyées et le contenu 200 OK est vérifié. Si le contenu 200 OK est trouvé, le serveur est considéré comme disponible.	**Demande** OPTIONS / HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Autoriser : OPTIONS, TRACE, GET, HEAD, POST Serveur : Microsoft-IIS/10.0 Public : OPTIONS, TRACE, GET, HEAD, POST Date : Tue, 13 Jul 2021 16:23:39 GMT Contenu-Longueur : 0
Tête HTTP	Le moniteur HTTP Head nous permet de vérifier la présence d'une valeur spécifique dans la partie Head du flux HTTP. Nous pouvons saisir un chemin et une réponse requise dans les champs appropriés, puis vérifier la présence de cette valeur dans la réponse. Si la valeur Required Response est trouvée dans l'en-tête, le serveur est considéré comme opérationnel et disponible. Nous pouvons également l'utiliser sur des pages spécialement protégées qui nécessitent un nom d'utilisateur et un mot de passe. De cette manière, le résultat du moniteur peut être considéré comme exact.	**Demande** HEAD /ispagethere.htm HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Contenu-Longueur : 1364 Content-Type : text/html Dernière modification : Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges : bytes ETag : "0dd3253a59ad31:0"

	Par exemple, la fourniture de **/ispagethere.html** et de valeurs **200 OK** dans les champs Chemin et Réponse requise renverra un résultat positif si le serveur est opérationnel, si la page est disponible et si elle répond à la demande. Cette méthode de surveillance ne peut vraiment être utilisée qu'avec les types de service HTTP et HTTP accéléré. Toutefois, si un type de service de couche 4 est utilisé pour un serveur HTTP, il peut toujours être utilisé si SSL n'est pas utilisé sur le serveur réel ou géré de manière appropriée par la fonction "Content SSL".	Serveur : Microsoft-IIS/10.0 Date : Wed, 14 Jul 2021 08:28:18 GMT
Options HTTP	Le moniteur d'options HTTP vous permet de vérifier la présence d'une valeur spécifique dans les données d'options renvoyées. Nous saisissons un chemin d'accès et une réponse requise dans les champs appropriés, puis nous vérifions la réponse. Si la réponse requise est trouvée dans les données des options, le serveur est disponible et fonctionne. Les valeurs de la réponse requise peuvent être l'une des suivantes : OPTIONS, TRACE, GET, HEAD et POST. Par exemple, la fourniture de **/ispagethere.html** et de valeurs **GET** dans les champs Chemin et Réponse requise renverra un résultat positif si le serveur est opérationnel, si la page est disponible et si elle répond à la demande. Cette méthode de surveillance ne peut vraiment être utilisée qu'avec les types de service HTTP et HTTP accéléré. Toutefois, si un type de service de couche 4 est utilisé pour un serveur HTTP, il peut toujours être utilisé si SSL n'est pas utilisé sur le serveur réel ou géré de manière appropriée par la fonction "Content SSL".	**Demande** OPTIONS /ispagethere.htm HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Autoriser : OPTIONS, TRACE, GET, HEAD, POST Serveur : Microsoft-IIS/10.0 Public : OPTIONS, TRACE, GET, HEAD, POST Date : Wed, 14 Jul 2021 09:47:27 GMT Contenu-Longueur : 0
Réponse HTTP	Une connexion et une requête/réponse HTTP sont établies avec le serveur réel et vérifiées comme expliqué dans les exemples précédents. Mais plutôt que de vérifier un code de réponse "200 OK", l'en-tête de la réponse HTTP est vérifié pour son contenu textuel personnalisé. Le texte peut être un en-tête complet, une partie d'en-tête, une ligne d'une partie de la page ou juste un mot. Par exemple, dans l'exemple ci-contre, nous avons spécifié **/ispagethere.htm** comme chemin d'accès et **Microsoft-IIS** comme réponse requise. Si le texte est trouvé, le Real Server est considéré comme opérationnel. Cette méthode de surveillance ne peut vraiment être utilisée qu'avec les types de services HTTP et HTTP accéléré.	**Demande** GET /ispagethere.htm HTTP/1.1 Hôte : 192.168.159.200 Accepter : */* Accept-Language : en-gb User-Agent : Edgenexus-ADC/4.0 Connexion : Keep-Alive Cache-Control : no-cache **Réponse** HTTP/1.1 200 OK Content-Type : text/html Dernière modification : Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges : bytes ETag : "0dd3253a59ad31:0" Serveur : Microsoft-IIS/10.0 Date : Wed, 14 Jul 2021 10:07:13 GMT Contenu-Longueur : 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN"

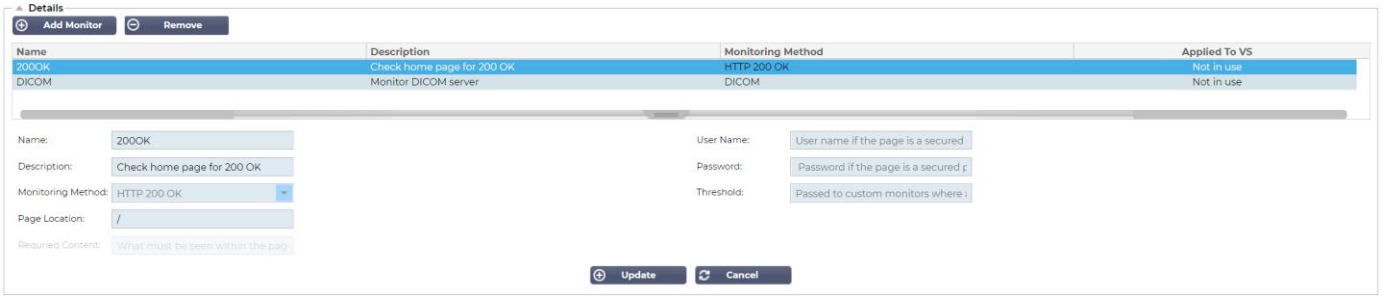
	Toutefois, si un type de service de couche 4 est utilisé pour un serveur HTTP, il peut encore être utilisé si SSL n'est pas utilisé sur le serveur réel ou s'il est traité de manière appropriée par la fonction "Content SSL".	"http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <b>En-tête> <meta http-equiv="Content-Type" content="text/html ; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- corps { couleur:#FFFFFF ; ...
Moniteur TCP multiport	Cette méthode est similaire à la précédente, sauf que vous pouvez avoir plusieurs ports différents. Le moniteur n'est considéré comme réussi que si tous les ports spécifiés dans la section du contenu requis répondent correctement.	Nom : Moniteur multiport Description : Surveiller plusieurs ports pour assurer le succès de l'opération Emplacement de la page : N/A Contenu requis : 135,59534,59535
TCP hors bande	La méthode TCP hors bande est semblable à une connexion TCP, à ceci près que vous pouvez spécifier le port que vous souhaitez surveiller dans la colonne du contenu requis. Ce port n'est généralement pas le même que le port de trafic et est utilisé lorsque vous souhaitez relier des services entre eux.	Nom : TCP hors bande Description : Surveillance du port hors bande/trafic Emplacement de la page : N/A Contenu requis : 555
DICOM	Nous envoyons un écho DICOM en utilisant la valeur du titre AE "Source Calling" dans la colonne de contenu requise. Vous pouvez également définir la valeur "Destination Called" AE Title dans la section Notes de chaque serveur. Vous trouverez la colonne Notes dans la section IP Services- -Services virtuels - Page Serveur.	Nom : DICOM Description : Contrôle de santé L7 pour le service DICOM Méthode de surveillance : DICOM Emplacement de la page : N/A Contenu requis : Valeur de l'EFA
LDAPS	Ce nouveau contrôle de santé est utilisé pour vérifier la santé et la réponse d'un serveur LDAP/AD.	Nom : LDAPS Description : Contrôle de l'état du serveur LDAP/AD Les paramètres d'utilisation sont les suivants : **Nom d'utilisateur** : cn=username,cn=users,dc=domainname, dc=local **Mot de passe** : DomainUserPassword **Contenu** : 200OK
SNMP v2	Cette méthode de surveillance vous permet de vérifier l'état de disponibilité d'un serveur à l'aide de la réponse SNMP MIB du serveur. La valeur Require Response doit contenir le nom de la communauté.	
Vérification du serveur DNS	Lors de l'équilibrage de la charge des serveurs DNS, il est utile de vérifier si le serveur répond aux requêtes DNS. Le moniteur peut être utilisé comme suit : • Le champ Chemin est utilisé pour le FQDN que vous interrogez. Par exemple, si vous souhaitez interroger www.edgenexus.io, entrez ce nom dans le champ Chemin. • Si vous laissez ce champ vide, le moniteur utilisera sa recherche par défaut pour effectuer la requête. • Le champ Réponse requise peut être laissé vide et le moniteur considérera que toute réponse est valide. Dans le cas contraire, vous devez saisir l'adresse IP attendue dans le champ Réponse requise. Par exemple, il peut s'agir de 101.10.10.100. Si la requête renvoie cette valeur, le moniteur signale un succès ; dans le cas contraire, il signale un échec.	

	Un résultat positif indique que le serveur DNS dont vous assurez l'équilibrage de charge est opérationnel.

La page Real Server Monitors est divisée en trois sections.

Détails

La section Détails permet d'ajouter de nouveaux moniteurs et de supprimer ceux dont vous n'avez pas besoin. Vous pouvez également modifier un moniteur existant en double-cliquant dessus.



Nom

Nom de votre choix pour votre moniteur.

Description

Description textuelle de ce moniteur. Nous recommandons de la rendre aussi descriptive que possible.

Méthode de contrôle

Choisissez la méthode de surveillance dans la liste déroulante. Les choix disponibles sont les suivants :

- HTTP 200 OK
- HTTP 200 En-tête
- Options HTTP 200
- Tête HTTP
- Options HTTP
- Réponse HTTP
- Moniteur TCP multiport
- TCP hors bande
- DICOM
- SNMP v2
- Vérification du serveur DNS
- LDAPS

Emplacement de la page

URL Emplacement de la page pour un moniteur HTTP. Cette valeur peut être un lien relatif tel que /dossier1/dossier2/page1.html. Vous pouvez également utiliser un lien absolu où le site web est lié au nom d'hôte.

Contenu obligatoire

Cette valeur contient tout contenu que le moniteur doit détecter et utiliser. La valeur représentée ici changera en fonction de la méthode de surveillance choisie.

Appliqué au VS

Ce champ est automatiquement rempli avec l'IP/Port du service virtuel auquel le moniteur est appliqué. Vous ne pourrez pas supprimer un moniteur qui a été utilisé avec un service virtuel.

Utilisateur

Certains moniteurs personnalisés peuvent utiliser cette valeur ainsi que le champ du mot de passe pour se connecter à un Real Server.

Mot de passe

Certains moniteurs personnalisés peuvent utiliser cette valeur ainsi que le champ Utilisateur pour se connecter à un Real Server.

Seuil

Le champ Threshold est un nombre entier général utilisé dans les moniteurs personnalisés lorsqu'un seuil tel que le niveau de CPU est requis.

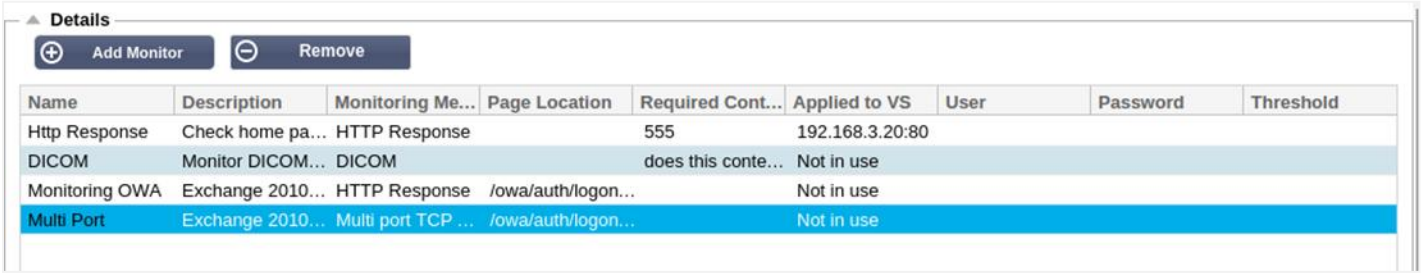
REMARQUE : Assurez-vous que la réponse du serveur d'application n'est pas une réponse groupée ("Chunked").

SSL/TLS

Ce champ vous permet d'imposer l'utilisation ou non de SSL. Les paramètres sont les suivants :

- Activé - Cette option force le protocole SSL
- Désactivé - Désactive le protocole SSL
- Auto - Cette option laisse l'état actuel

Exemples de Real Server Monitor



Moniteur de téléchargement

Il y aura de nombreuses occasions où les utilisateurs souhaiteront créer leurs propres moniteurs personnalisés et cette section leur permet de les télécharger vers l'ADC.

Les moniteurs personnalisés sont écrits à l'aide de scripts PERL et ont une extension de fichier .pl.

- Donnez un nom à votre moniteur afin de pouvoir l'identifier dans la liste des méthodes de surveillance.
- Rechercher le fichier .pl
- Cliquez sur Télécharger un nouveau moniteur
- Votre fichier sera téléchargé au bon endroit et sera visible en tant que nouvelle méthode de surveillance.

Moniteurs personnalisés

Dans cette section, vous pouvez visualiser les moniteurs personnalisés téléchargés et les supprimer s'ils ne sont plus nécessaires.

- Cliquez sur la liste déroulante
- Sélectionnez le nom du moniteur personnalisé
- Cliquez sur Supprimer
- Votre moniteur personnalisé ne sera plus visible dans la liste des méthodes de surveillance.

Création d'un script Perl de surveillance personnalisé

ATTENTION : Cette section est destinée aux personnes ayant une expérience de l'utilisation et de l'écriture en Perl

Cette section présente les commandes que vous pouvez utiliser dans votre script Perl.

La commande #Monitor-Name : est le nom utilisé pour le script Perl stocké sur l'ADC. Si vous n'incluez pas cette ligne, votre script ne sera pas trouvé !

Les éléments suivants sont obligatoires :

- #Nom du moniteur
- utiliser strict ;
- avertissement sur l'utilisation ;

Les scripts Perl sont exécutés dans un environnement CHROOTED. Ils appellent souvent une autre application telle que WGET ou CURL. Parfois, ces dernières doivent être mises à jour pour une fonctionnalité spécifique, telle que SNI.

Valeurs dynamiques

- my $host = $_[0] ; ### IP ou nom de l'hôte (provient des détails du RS ou de l'OOB s'il est utilisé)
- my $port = $_[1] ; ### Port de l'hôte (provient des détails du RS ou de l'OOB s'il est utilisé)
- my $content = $_[2] ; ### Contenu requis dans les paramètres du moniteur (ce qui doit être vu dans la réponse)
- my $notes = $_[3] ; ### notes à partir des détails du RS dans les services IP (à utiliser pour personnaliser chaque moniteur de RS de manière unique)
- my $page = $_[4] ; ### emplacement de la page dans les paramètres du moniteur
- my $user = $_[5] ; ### nom d'utilisateur des paramètres du moniteur
- my $password = $_[6] ; ### mot de passe des paramètres du moniteur
- my $threshold = $_[7] ; ### paramètre de seuil des paramètres du moniteur
- my $rsaddr = $_[8] ; ### RS IP (différent de _[0] si surveillance hors bande)
- my $rsport = $_[9] ; ### Port RS (différent de _[1] si surveillance hors bande)
- my $timeout = $_[10] ; ### surveiller le délai de contact en secondes depuis IP Services > Real Server > Advanced > Monitoring Timeout

Les bilans de santé personnalisés ont deux résultats

- Réussi
  Valeur de retour 1

Imprimer un message de réussite dans Syslog
Marquer le serveur réel en ligne (à condition que IN COUNT corresponde)

- Échec
  Valeur de retour 2
  Imprimer un message disant Unsuccessful dans Syslog
  Marquer le serveur réel hors ligne (à condition que le compte OUT corresponde)

Exemple de moniteur de santé personnalisé

```
#Nom du moniteur HTTPS_SNI
utiliser strict :
les avertissements relatifs à l'utilisation ;
# Le nom du moniteur est affiché dans la liste déroulante des contrôles de santé disponibles.
# Il y a 6 valeurs passées à ce script (voir ci-dessous)
# Le script renvoie les valeurs suivantes
# 1 si le test est réussi
# 2 si le test n'est pas concluant sub monitor
{
my Shost        = $_[0] ; ### IP ou nom de l'hôte
my Sport        = $_[1] ; ### Port de l'hôte
my Scontent     = $_[2] ; ### Contenu à rechercher (dans la page web et les en-têtes HTTP)
my Snotes       = $_[3] ; ### Nom d'hôte virtuel
my Spage        = $_[4] ; ### La partie de l'URL après l'adresse de l'hôte
my Suser        = $_[5] : ### domaine/nom d'utilisateur (optionnel)
mon mot de passe          = $_[6] ; ### mot de passe (optionnel)
mon $resolve ;
mon $auth       = ;
si ($port)
{
        $resolve = "$notes:$port:$host" :
}
else {
        $resolve = "$notes:$host" ;
}
if ($user && $password) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1' ;
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} looking for - $content - Health check successful.\n" ;
        retour(1) ;
        }
autre
        {
```

```
        print "HTTPs://${notes}${page} looking for - $content - Health check failed.\n" ;
        retour(2)
        }
}
monitor(@ARGV) :
```

NOTE :

Surveillance personnalisée - L'utilisation de variables globales n'est pas possible. Utiliser uniquement des variables locales, c'est-à-dire des variables définies à l'intérieur de fonctions

Utilisation de RegEx - Toutes les expressions régulières doivent utiliser une syntaxe d'instruction compatible avec Perl.

Certificats SSL

Pour utiliser avec succès l'équilibrage de charge de couche 7 avec des serveurs utilisant des connexions cryptées à l'aide de SSL, l'ADC doit être équipé des certificats SSL utilisés sur les serveurs cibles. Cette exigence permet de décrypter le flux de données, de l'examiner, de le gérer et de le recrypter avant de l'envoyer au serveur cible.

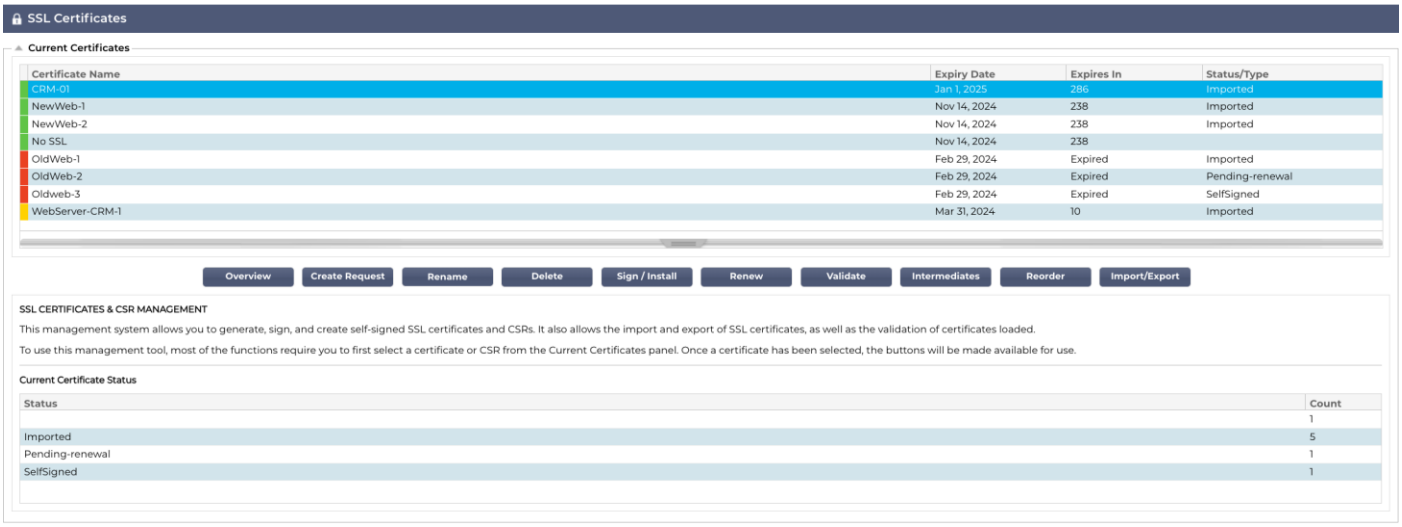
Les certificats SSL peuvent aller des certificats auto-signés que l'ADC peut générer aux certificats traditionnels (joker inclus) disponibles auprès de fournisseurs de confiance. Vous pouvez également utiliser des certificats signés par le domaine qui sont générés à partir d'Active Directory.

Que fait l'ADC avec le certificat SSL ?

L'ADC peut appliquer des règles de gestion du trafic (flightPATH) en fonction du contenu des données. Cette gestion ne peut pas être effectuée sur des données cryptées par SSL. Lorsque l'ADC doit inspecter les données, il doit d'abord les décrypter, et pour cela, il doit disposer du certificat SSL utilisé par le serveur. Une fois les données décryptées, l'ADC pourra examiner et appliquer les règles flightPATH. Les données seront ensuite recryptées à l'aide du certificat SSL et envoyées au serveur Real final.

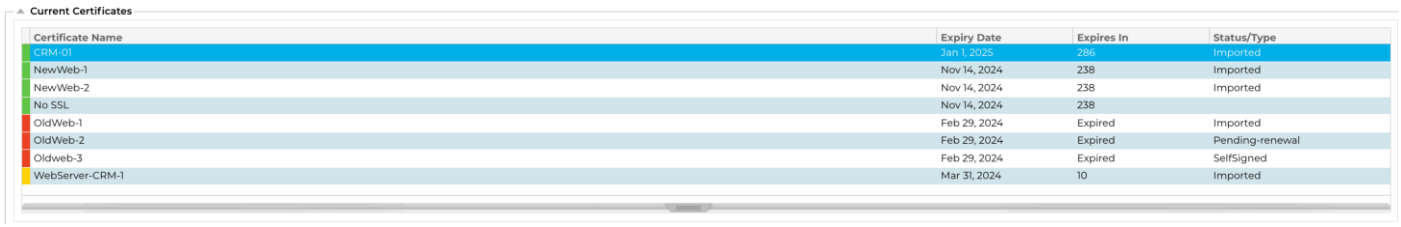
Le gestionnaire de configuration SSL

La version 196X et les suivantes proposent une nouvelle méthode plus simple pour configurer et gérer les certificats SSL et les demandes de certificats.



Le gestionnaire de configuration SSL comporte trois sections principales.

La zone de listage des certificats



La partie supérieure du gestionnaire affiche les certificats SSL disponibles ou en attente d'activation auprès d'une autorité de confiance.

Les certificats sont affichés dans une fenêtre à quatre colonnes, indiquant le nom du certificat, la date d'expiration, Expires In (nombre de jours avant l'expiration) et le statut/type du certificat.

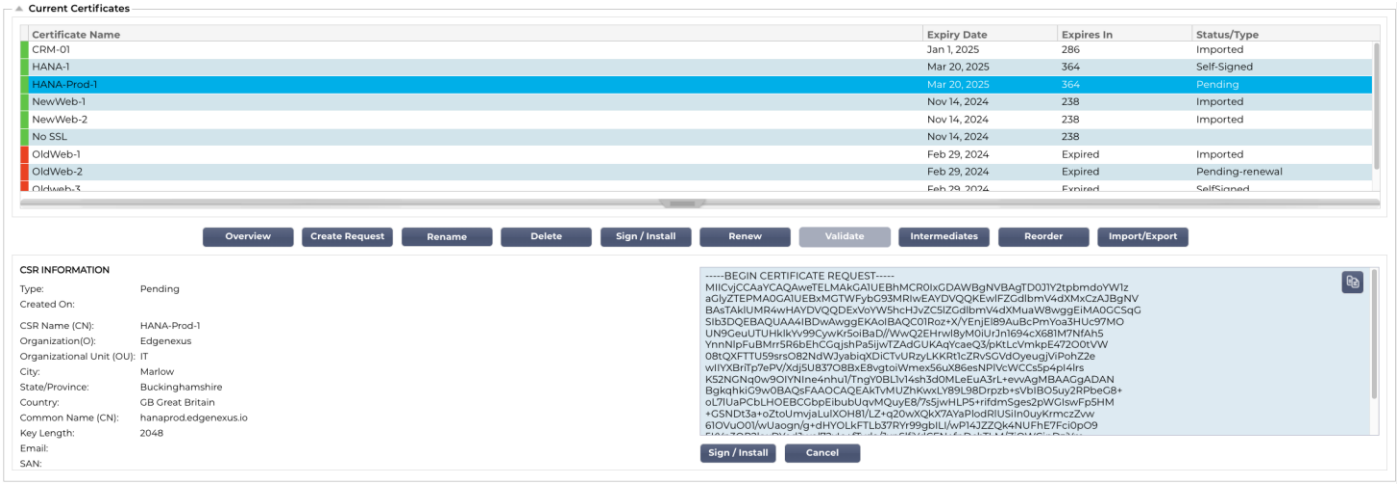
Codes de couleur

Comme vous pouvez le voir, chaque ligne présente un certificat accompagné d'un bloc de couleur. Le tableau ci-dessous présente les différents blocs de couleur et leur signification.

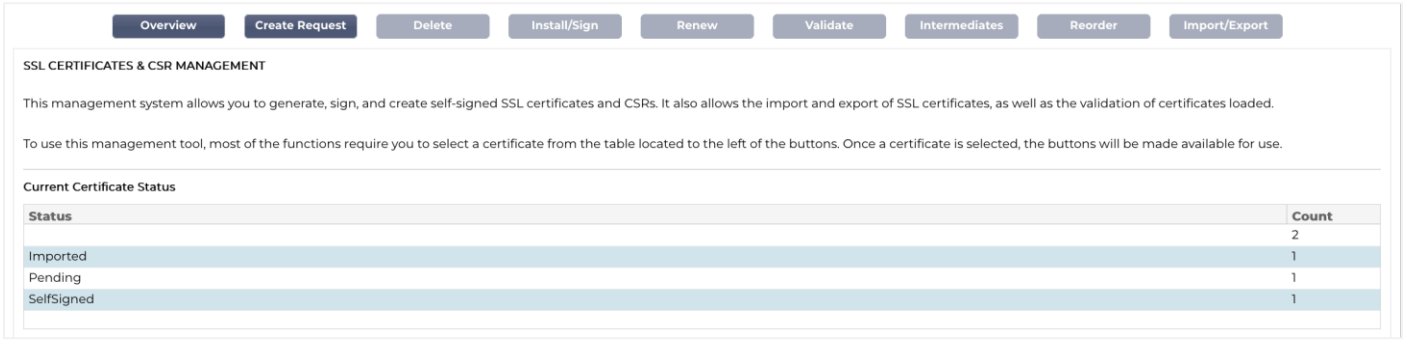
Code couleur	Signification
	Le certificat est à jour et il reste plus de 60 jours avant son expiration.
	Le certificat expirera dans moins de 30 jours
	Il reste entre 30 et 60 jours pour le certificat
	Le certificat est sur le point d'expirer à moins d'un jour de la fin.
	Le certificat a expiré

Affichage de l'information sur le certificat/DSR

En cliquant sur un certificat ou une CSR, les informations le concernant s'affichent dans le panneau inférieur. Voir l'image ci-dessous.



Les boutons d'action et les zones de configuration



Un certain nombre de boutons d'action sont disponibles et entrent en jeu lorsqu'un certificat est sélectionné dans la zone de listage.

Vue d'ensemble

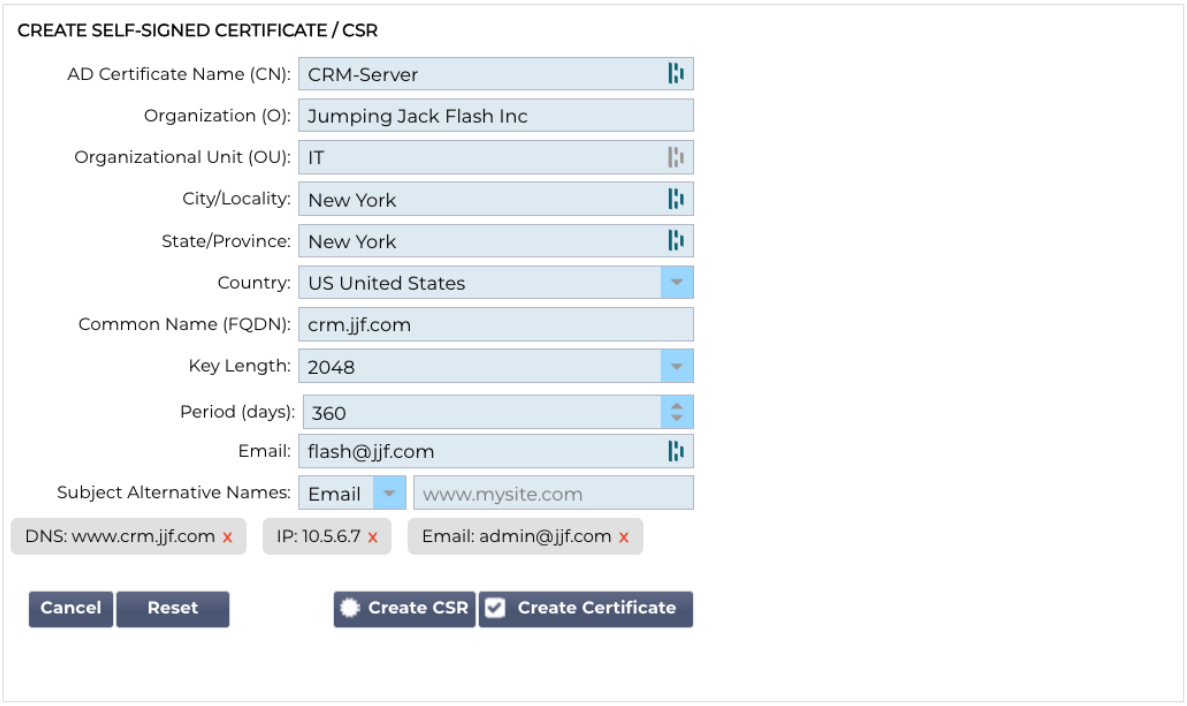

Current Certificate Status

Status	Count
	1
Imported	5
Pending	1
Pending-renewal	1
Self-Signed	1
SelfSigned	1

Le bouton Vue d'ensemble permet d'afficher une situation globale des certificats dans la partie inférieure. Contrairement à d'autres actions, le bouton Aperçu est indépendant et ne nécessite pas la sélection d'un certificat.

Créer une demande

Si vous souhaitez créer un certificat auto-signé ou une CSR, vous devez cliquer sur le bouton Créer une demande. Vous verrez apparaître un panneau de saisie commun qui vous permettra de fournir tous les détails nécessaires.



Nom du certificat AD (CN)

Il s'agit d'un champ descriptif utilisé pour afficher le nom du certificat dans le CDA. L'entrée du champ doit être alphanumérique, sans espace.

Organisation (O)

Ce champ est utilisé pour spécifier le nom de l'organisation qui va utiliser le certificat.

Unité d'organisation (OU)

Normalement utilisé pour spécifier le département ou l'unité organisationnelle, ce champ est facultatif.

Ville/Localité

Comme son nom l'indique, les utilisateurs ont généralement tendance à spécifier l'endroit où se trouve l'organisation.

État/Province

Spécifiez l'état, le comté ou la province dans ce champ.

Pays

Ce champ est obligatoire et doit être complété en sélectionnant le pays dans lequel le certificat sera utilisé. Veuillez vous assurer que les informations fournies ici sont exactes.

Nom commun (FQDN)

Il s'agit d'un champ critique qui sert à spécifier le nom de domaine complet (FQDN) du ou des serveurs qui doivent être protégés à l'aide du certificat. Il peut s'agir de quelque chose comme www.edgenexus.io, ou **edgenexus.io**, ou même d'un caractère générique ***.edgenexus.io**. Vous pouvez également utiliser une adresse IP si vous souhaitez lier le certificat à cette adresse.

Longueur de la clé

Permet de spécifier la longueur de la clé de cryptage pour le certificat SSL.

Période (jours)

La durée de validité du certificat en jours. Une fois la période écoulée, le certificat devient non opérationnel.

Courriel

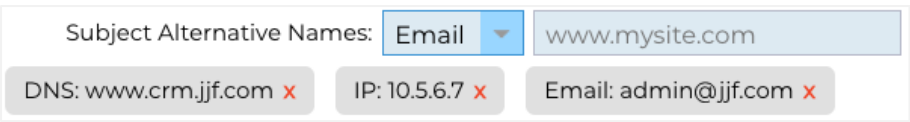
Il s'agit de l'adresse électronique de l'administration utilisée pour le certificat.

Noms alternatifs du sujet (SAN)

Subject Alternative Name (SAN) est une extension des certificats SSL qui permet de protéger plusieurs noms de domaine avec un seul certificat. Cette fonctionnalité est particulièrement utile pour sécuriser les sites web avec plusieurs sous-domaines ou différents noms de domaine, ce qui permet une approche plus rationnelle et plus rentable de la gestion SSL. En incluant les SAN, un seul certificat SSL peut couvrir une variété de noms de domaine et de sous-domaines, éliminant ainsi le besoin de certificats individuels pour chaque adresse web, ce qui simplifie le processus de sécurisation des communications web et garantit le cryptage des données à travers divers domaines.

Ce champ comprend deux éléments, une liste déroulante permettant de sélectionner le type de SAN et un champ de texte pour spécifier la valeur.

L'EdgeADC dispose des SAN suivants : DNS, adresse IP, adresse électronique et URI. Vous pouvez sélectionner et spécifier plusieurs SAN pour un certificat ou une CSR.



Les SAN qui ont été spécifiés peuvent être supprimés en cliquant sur le **x** rouge situé dans chaque valeur de SAN.

- **DNS** - Le champ Subject Alternate Name (SAN) vous permet de spécifier des noms de domaine supplémentaires pour lesquels le certificat est valide. Contrairement au champ Common Name (CN), qui n'autorise qu'un seul domaine, le champ SAN peut inclure plusieurs noms de domaine, ce qui offre souplesse et évolutivité dans la gestion des certificats. Ceci est particulièrement utile pour les organisations hébergeant plusieurs services à travers différents domaines et sous-domaines, car cela leur permet de sécuriser les

communications pour toutes ces entités sous un seul certificat SSL/TLS, ce qui simplifie l'administration et améliore la sécurité.

- **Adresse IP** - Le nom alternatif du sujet IP (SAN) permet d'inclure les adresses IP aux côtés des noms de domaine en tant qu'entités protégées par le certificat. Cette fonctionnalité est essentielle pour sécuriser l'accès direct aux services via les adresses IP, en garantissant que des connexions cryptées peuvent également être établies lorsque l'on accède à un serveur non pas via son nom de domaine, mais directement via son adresse IP. En incorporant des SAN IP, les organisations peuvent améliorer la sécurité de leur réseau en activant le cryptage SSL/TLS pour les communications basées sur le domaine et sur l'adresse IP, ce qui le rend polyvalent pour les environnements où les noms de domaine peuvent ne pas être utilisés ou préférés pour accéder à des ressources internes ou à des services spécifiques.
- **Adresse électronique** - Le nom alternatif du sujet de l'adresse électronique (SAN) vous permet de spécifier des adresses électroniques supplémentaires à associer au certificat, en plus du domaine principal ou de l'entité pour laquelle il a été délivré. Cela permet au certificat de valider l'identité de l'émetteur pour plusieurs adresses électroniques, et non pour un seul domaine ou nom commun (CN). Il est particulièrement utile dans les scénarios où une communication sécurisée par courrier électronique est nécessaire pour plusieurs adresses électroniques appartenant à la même organisation ou entité, en garantissant que les échanges de courrier électronique cryptés sont authentifiés et liés à l'identité de l'émetteur vérifiée par le certificat. Le SAN d'adresses électroniques est donc une fonctionnalité essentielle pour renforcer la sécurité et la fiabilité des communications électroniques dans un cadre crypté.
- **URI** - Le SAN URI (Uniform Resource Identifier) est utilisé pour spécifier des identités supplémentaires représentées par des URI pour une seule entité sécurisée par le certificat. Contrairement aux entrées SAN traditionnelles qui comprennent généralement des noms de domaine (noms DNS) ou des adresses IP, un SAN URI permet au certificat d'associer l'entité à des URI spécifiques, tels qu'une URL vers une ressource spécifique ou un point de terminaison de service. Cela permet une identification plus souple et plus précise, permettant d'établir des connexions sécurisées avec des ressources ou des services spécifiques au sein d'un domaine, plutôt que de sécuriser le domaine lui-même, améliorant ainsi la granularité et la portée des certificats SSL/TLS.

Une fois le formulaire correctement rempli, vous pouvez choisir de créer une demande de signature de certificat (CSR) et de l'envoyer pour signature à une autorité de certification ou de créer un certificat auto-signé pour une utilisation immédiate.

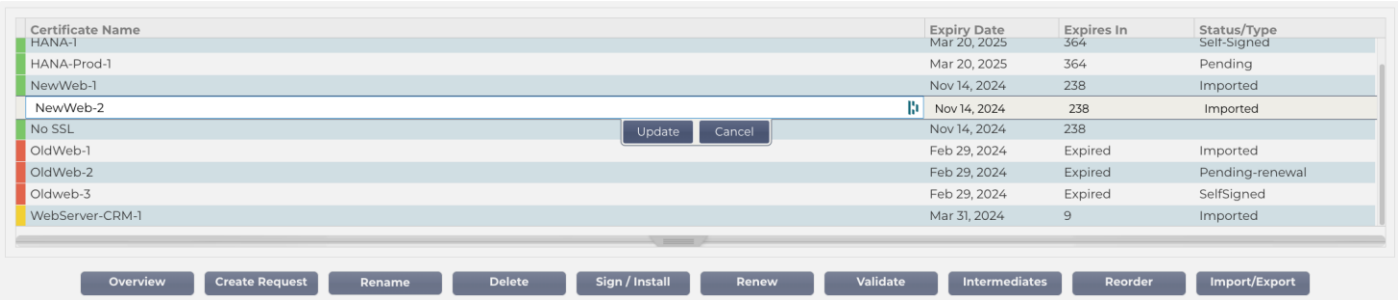
Le bouton Annuler annule toute la demande, tandis que le bouton Réinitialiser réinitialise tous les champs.

Renommer

Le bouton Renommer permet de renommer les certificats qui ne sont pas utilisés par les services virtuels.

Pour utiliser cette fonction :

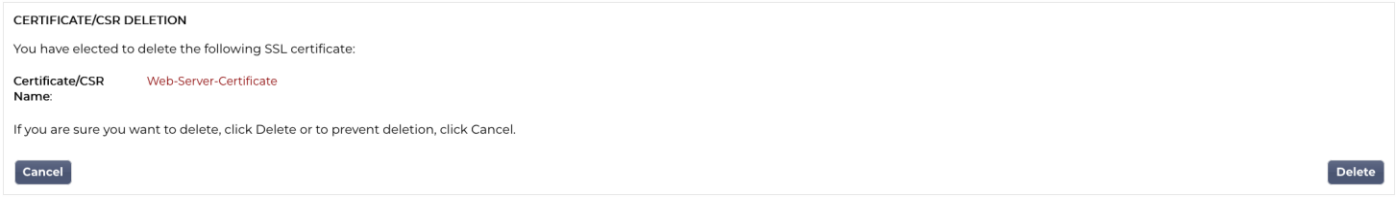
- Cliquez sur le certificat que vous souhaitez renommer et cliquez sur le bouton Renommer.
- La ligne du certificat change et vous pouvez modifier son nom.



- Une fois que vous avez terminé, cliquez sur le bouton Mettre à jour.
- Vous pouvez également double-cliquer sur le certificat pour le renommer.

Supprimer

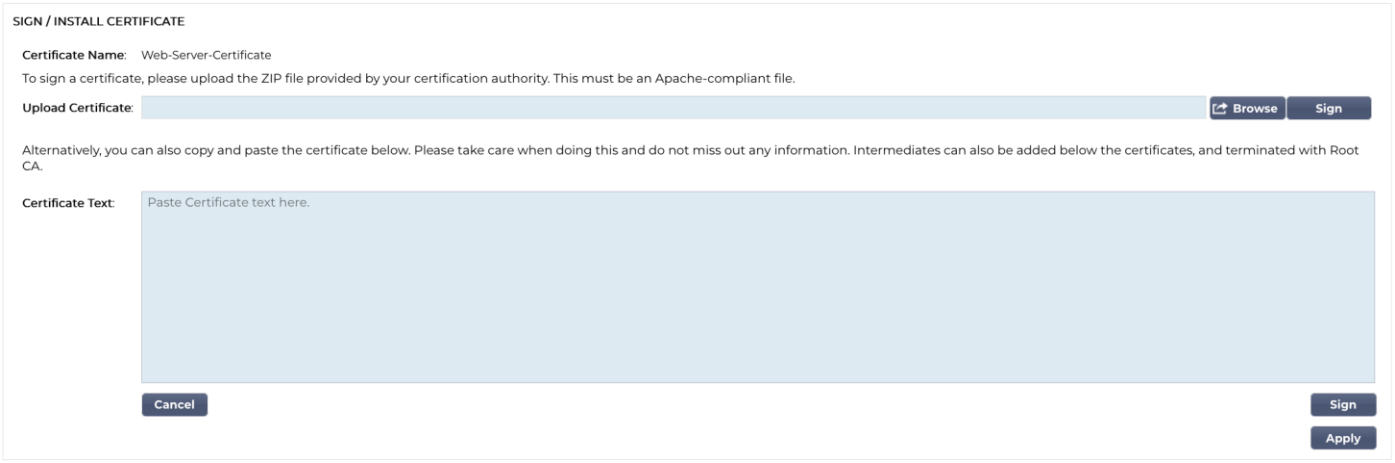
Le bouton Supprimer n'est disponible que lorsqu'un certificat est sélectionné. Lorsqu'il est cliqué, il affiche le contenu suivant



Le volet inférieur affiche la demande de suppression ainsi que le nom du certificat pour lequel la suppression a été demandée.

Cliquez sur le bouton Supprimer en bas à droite du volet pour procéder à la suppression.

Installation/Signature



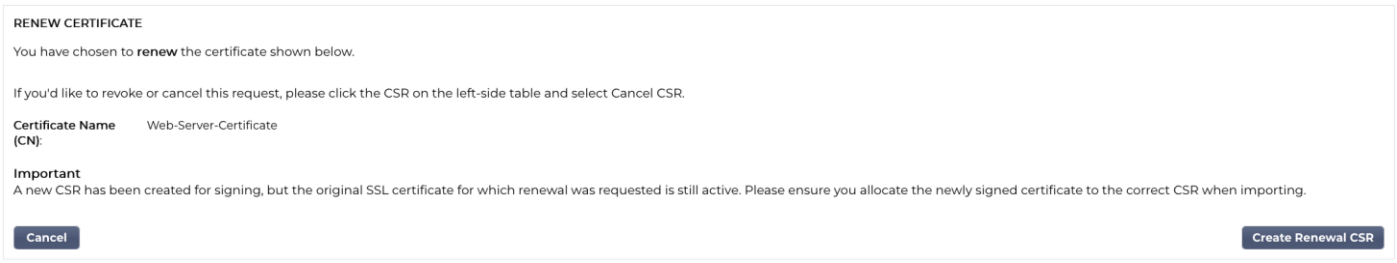
Lorsque vous créez une RSC et que vous souhaitez que la demande soit signée par une autorité de certification (AC), vous envoyez la RSC à l'AC. En retour, l'autorité de certification enverra le certificat signé avec le fichier de la clé privée et tous les intermédiaires nécessaires au bon fonctionnement du certificat.

Il se peut qu'ils vous envoient un fichier ZIP contenant tous les éléments requis, qui peut être téléchargé dans la partie supérieure du volet de droite.

Vous pouvez également construire le jeu de certificats dans un éditeur de texte et coller le contenu dans le champ Texte du certificat dans la partie inférieure du volet.

Une fois que vous avez utilisé l'une ou l'autre méthode, cliquez sur le bouton Signer, puis sur le bouton Appliquer. Le certificat signé s'affiche alors dans le volet de gauche.

Renouveler



Lorsqu'un certificat arrive à expiration après ses données de validité, le bouton Renouveler vous permet de prolonger et de renouveler le certificat. Il existe deux types de renouvellement.

Certificats auto-signés

Contrairement aux certificats de confiance, les certificats auto-signés ne peuvent pas être renouvelés à l'aide d'une CSR. Au lieu de cela, le certificat auto-signé est renouvelé en présentant une nouvelle configuration utilisant les données existantes. L'utilisateur est alors autorisé à spécifier un nouveau nom pour le certificat ainsi qu'une nouvelle valeur d'expiration pour le certificat.

Une fois cette opération effectuée, le nouveau certificat auto-signé sera créé et enregistré dans le magasin de certificats. Il incombe alors à l'administrateur de veiller à ce que les services virtuels qui utilisent le certificat soient reconfigurés à temps.

Certificats signés de confiance

Lorsqu'il s'agit de certificats fiables et signés par une autorité de certification, l'utilisation de CSR est adoptée.

Lorsque vous cliquez sur un certificat arrivant à expiration dans le panneau supérieur et que vous cliquez sur Renouveler, vous obtenez une nouvelle RSC utilisant les détails du certificat actuel. La CSR peut alors être téléchargée et présentée à l'autorité de certification pour signature, après quoi le certificat signé peut être installé.

Le certificat que vous aviez demandé de renouveler aura un nouveau statut, Renouvellement. Une fois le certificat signé installé, il vous sera demandé d'attribuer un nouveau nom au certificat. Ce nom sera alors "Trusted" (de confiance). Le certificat original sera conservé et tous les services qui l'utilisent devront être configurés pour utiliser le nouveau certificat dès que possible.

Valider le certificat

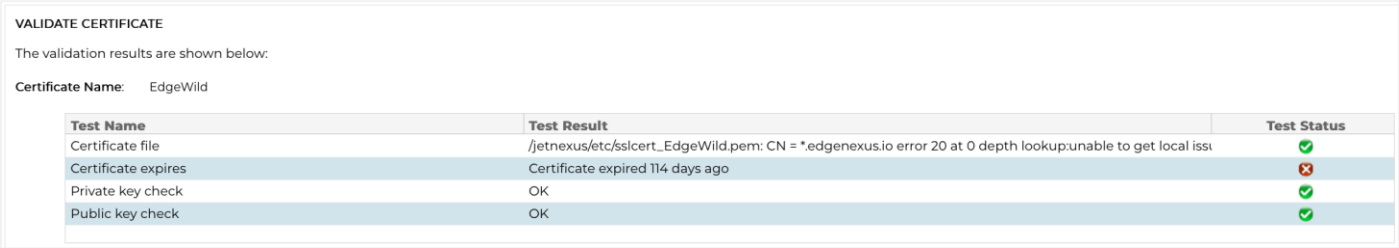
Un certificat SSL se compose de plusieurs éléments, et il est essentiel que ces éléments soient non seulement présents, mais aussi dans le bon ordre. Les raisons de valider les certificats SSL obtenus auprès d'organisations tierces sont énumérées ci-dessous.

- **L'authentification** : La validation garantit que le certificat provient d'une autorité de confiance et vérifie l'identité du site web ou du serveur. Cela permet d'éviter les attaques de type "man-in-the-middle", où un pirate peut intercepter la communication entre un client et un serveur.
- **Intégrité** : En validant un certificat SSL, vous pouvez vous assurer que le certificat n'a pas été altéré ou modifié. C'est essentiel pour maintenir l'intégrité de la connexion sécurisée.
- **Vérification de la chaîne de confiance** : Les certificats SSL sont émis par des autorités de certification (AC). La validation d'un certificat consiste à vérifier qu'il renvoie à une autorité de certification racine de confiance. Ce processus garantit que le certificat est légitime et qu'il est digne de confiance.
- **Statut de révocation** : Lors de la validation, il est également important de vérifier si le certificat SSL a été révoqué par l'autorité de certification émettrice. Un certificat peut être révoqué s'il a été émis par erreur, si la clé privée du site web a été compromise ou si le site n'a plus besoin du certificat. L'importation d'un certificat révoqué peut entraîner des failles de sécurité.
- **Vérification de l'expiration** : Les certificats SSL sont valables pour une période spécifique. La validation d'un certificat à l'importation inclut la vérification de sa date d'expiration pour s'assurer qu'il est toujours valide. L'utilisation d'un certificat expiré peut entraîner des vulnérabilités et amener les navigateurs ou les clients à rejeter la connexion sécurisée.
- **Configuration et compatibilité** : La validation garantit que la configuration du certificat est compatible avec les politiques de sécurité du client et les exigences techniques du serveur ou de l'application. Il s'agit notamment de vérifier les algorithmes utilisés, l'objet du certificat et d'autres détails techniques.
- **Conformité** : Dans certains secteurs, la réglementation peut exiger la validation de certificats SSL pour garantir le traitement sécurisé d'informations sensibles. Cela est particulièrement important dans des secteurs comme la finance, les soins de santé et le commerce électronique.

Le système de gestion SSL de l'ADC permet de valider un certificat SSL importé.

- Sélectionnez un certificat SSL que vous avez importé.
- Cliquez sur le bouton Valider.

- Les résultats sont visibles dans le panneau inférieur, comme le montre l'image ci-dessous.

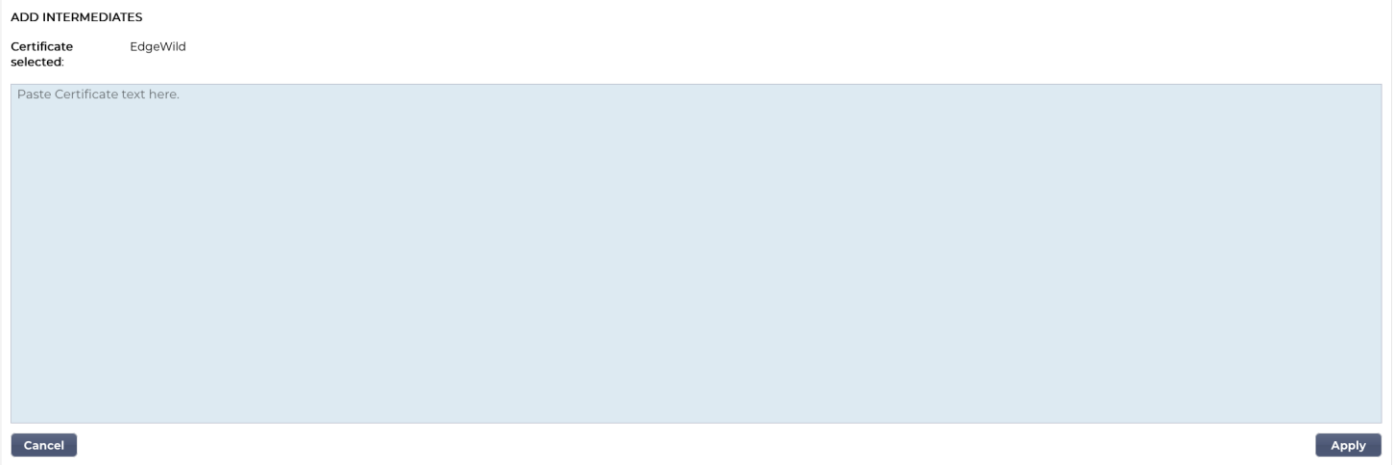


Ajouter des intermédiaires

Comme indiqué précédemment, les certificats SSL se composent de plusieurs éléments, dont les certificats intermédiaires qui constituent la chaîne complète.

Le gestionnaire SSL de l'ADC vous permet d'ajouter les certificats intermédiaires manquants.

- Cliquez sur le SSL auquel vous souhaitez ajouter le certificat intermédiaire.
- Cliquez sur le bouton Intermédiaires.
- Un panneau s'affiche, comme dans l'image ci-dessous.



- Collez le contenu du certificat intermédiaire.
- Cliquez sur Appliquer.

Il se peut que vous deviez modifier l'ordre des certificats intermédiaires, afin que le certificat SSL soit validé correctement. Pour ce faire, utilisez le bouton Réorganiser.

Réorganiser

Pour qu'un certificat SSL fonctionne correctement, il doit être placé dans le bon ordre.

La règle d'or est que le certificat de l'expéditeur doit venir en premier, et le certificat racine final en dernier dans la chaîne. En général, cela ressemble à la représentation ci-dessous :

```
Émetteur original > Intermédiaire 1 > Racine finale.
```

La racine finale est un certificat racine de confiance fourni par une autorité de certification.

Dans certains cas, il existe plusieurs certificats intermédiaires, qui doivent également être placés dans la bonne position. En fait, chaque certificat suivant doit certifier celui qui le précède. Cela pourrait donc ressembler à ce qui suit.

```
Émetteur original > Intermédiaire 1 > Racine finale
```

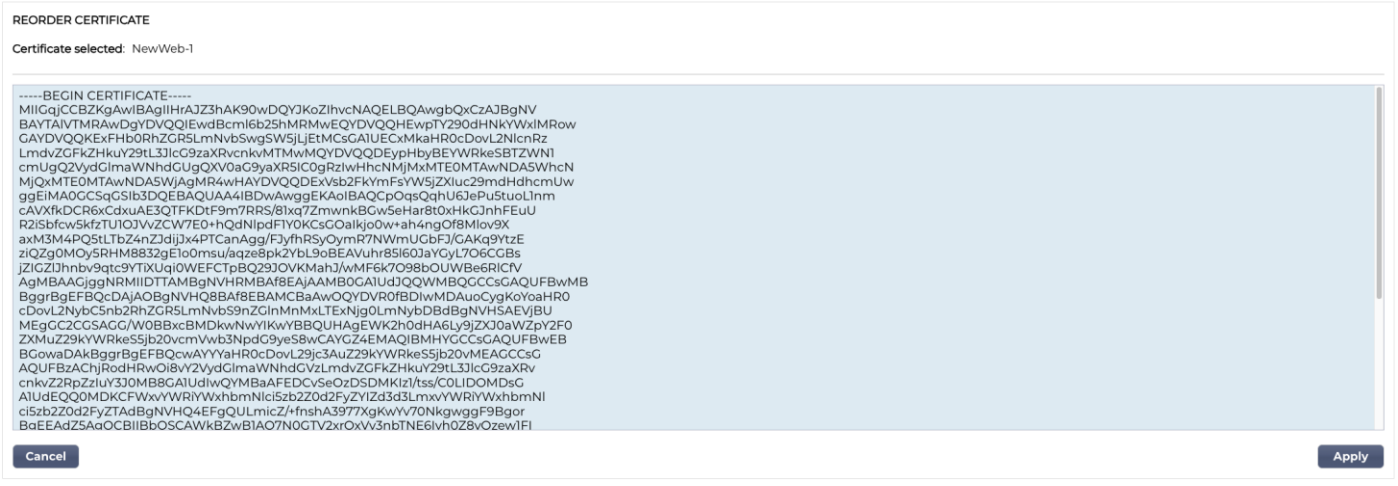
Lorsque vous importez, disons, l'intermédiaire 2, celui-ci pourrait être placé à la fin de la chaîne, ce qui signifierait que la certification n'est pas valide. D'où la nécessité de réorganiser la chaîne et de placer l'intermédiaire 2 à sa place (en rouge).

Le résultat final serait donc le suivant :

Émetteur original > Intermédiaire 1 > Intermédiaire 2 > Racine finale

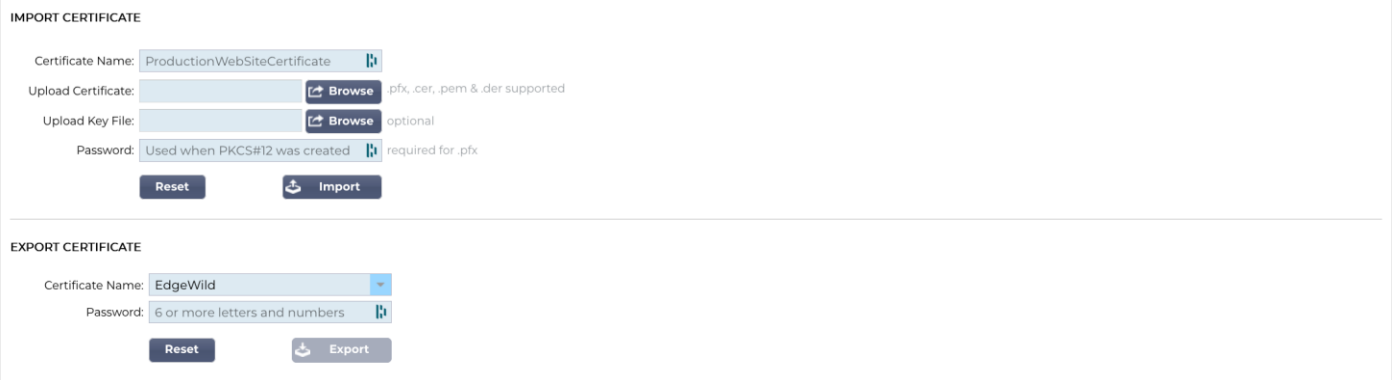
```
----- DÉBUT DU CERTIFICAT-----
MIIFKTCCBBGgAwIBAgISA/UyBjJ71fucZuvpiLsdfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfdsfsdfw=
-----END CERTIFICAT-----
----- DÉBUT DU CERTIFICAT-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinsdfsdfsdfdsfsdfsdd
....
nLRbwHqsdqD7hHwg====.
-----END CERTIFICAT-----
----- DÉBUT DU CERTIFICAT-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICAT-----
----- DÉBUT DU CERTIFICAT-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICAT-----
```

La section Réorganiser ressemble à l'image ci-dessous une fois que vous avez sélectionné un certificat et appuyé sur le bouton Réorganiser.



Pour réorganiser les sections du certificat, vous pouvez copier le texte dans la boîte, modifier et réorganiser le contenu dans un éditeur de texte, puis le recoller pour remplacer le contenu existant. Une fois que vous avez terminé, cliquez sur le bouton Appliquer.

Importation/Exportation



Lorsque vous recevez un certificat de votre fournisseur de certificats SSL, il se présente sous la forme d'un fichier ZIP ou d'un ensemble de fichiers. Ceux-ci contiennent le certificat SSL, le fichier clé et le fichier racine, ainsi que tous les fichiers intermédiaires

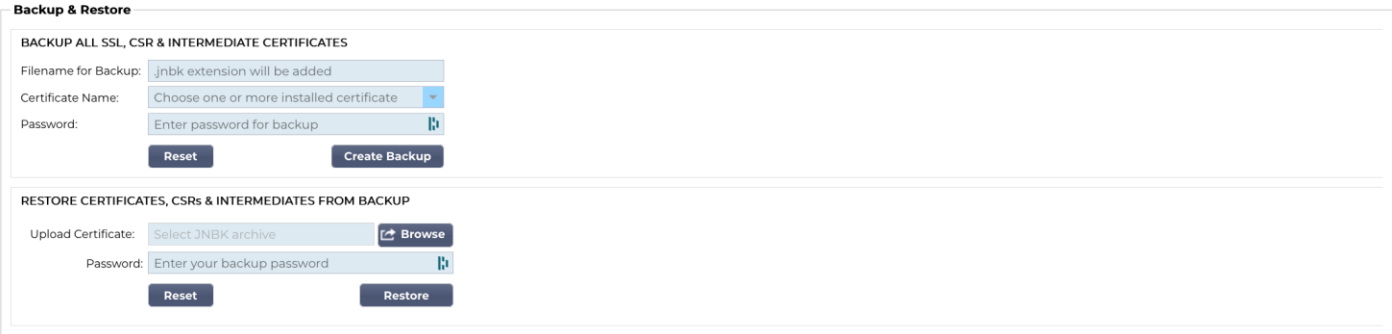
Vous devrez les importer dans l'ADC, et nous avons donc fourni une méthode pour les importer.

Il existe un certain nombre de formats pour les certificats SSL, tels que CER, DER, PEM et PFX. Certains formats nécessitent l'ajout d'un fichier KEY à la procédure d'importation. Les fichiers PFX nécessitent un mot de passe pour pouvoir importer le certificat PFX.

Nous avons également prévu la possibilité d'exporter un certificat à partir de l'ADC si nécessaire. Une fois exporté, le fichier sera au format PFX et nécessitera donc un mot de passe pour la création de l'exportation.

Sauvegarde et restauration

Sauvegarde



Afin de sauvegarder les certificats dans le magasin de certificats de l'ADC :

- Ajouter un nom de fichier à utiliser pour la sauvegarde.
- Utilisez le menu déroulant pour sélectionner un seul certificat ou TOUS pour sauvegarder tous les certificats.
- Ajouter un mot de passe
- Cliquez sur le bouton Créer une sauvegarde.
- Le fichier créé est un fichier JNBK qui est crypté.

IMPORTANT

La sauvegarde ne fonctionnera qu'avec les certificats de confiance qui ont été importés.

Restaurer

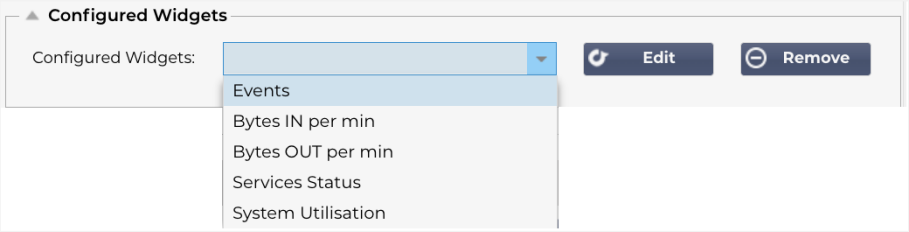
Lorsque vous souhaitez restaurer la sauvegarde, utilisez la partie inférieure de la section Sauvegarde et restauration.

- Recherchez et localisez le fichier de sauvegarde.
- Saisissez le mot de passe.
- Cliquez sur le bouton Restaurer.
- Les certificats contenus dans le fichier de sauvegarde seront restaurés.

Widgets

La page Bibliothèque > Widgets vous permet de configurer divers composants visuels légers affichés dans votre tableau de bord personnalisé.

Widgets configurés

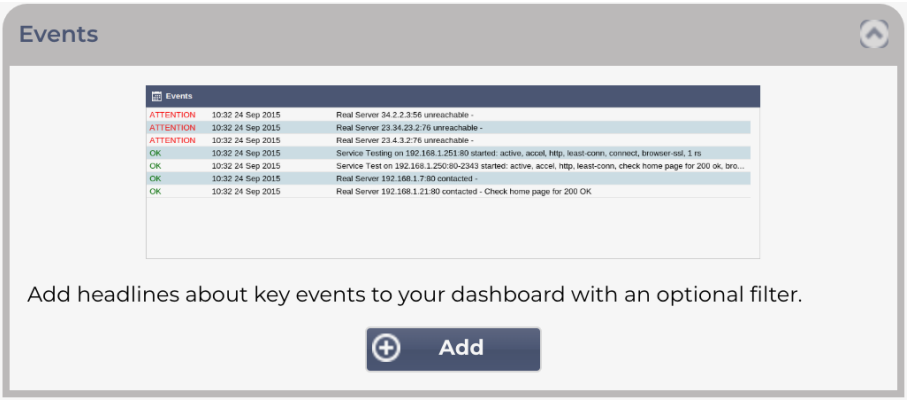


La section Widgets configurés vous permet d'afficher, de modifier ou de supprimer tout widget créé à partir de la section des widgets disponibles.

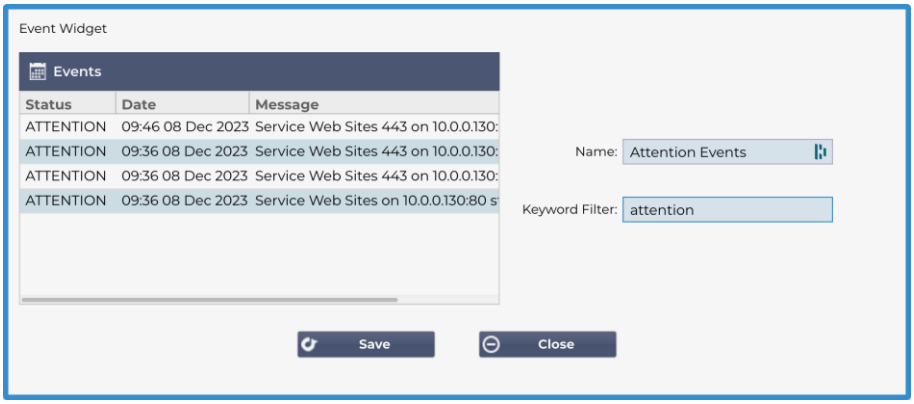
Widgets disponibles

L'ADC propose cinq widgets différents, que vous pouvez configurer en fonction de vos besoins.

Le widget des événements

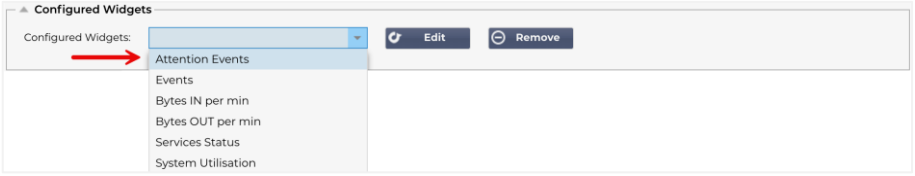


- Pour ajouter un événement au widget Événements, cliquez sur le bouton Ajouter.
- Donnez un nom à votre événement. Dans notre exemple, nous avons ajouté Attention Events comme nom d'événement.
- Ajouter un filtre de mots-clés. Nous avons également ajouté la valeur de filtre Attention



- Cliquez sur Enregistrer, puis sur Fermer

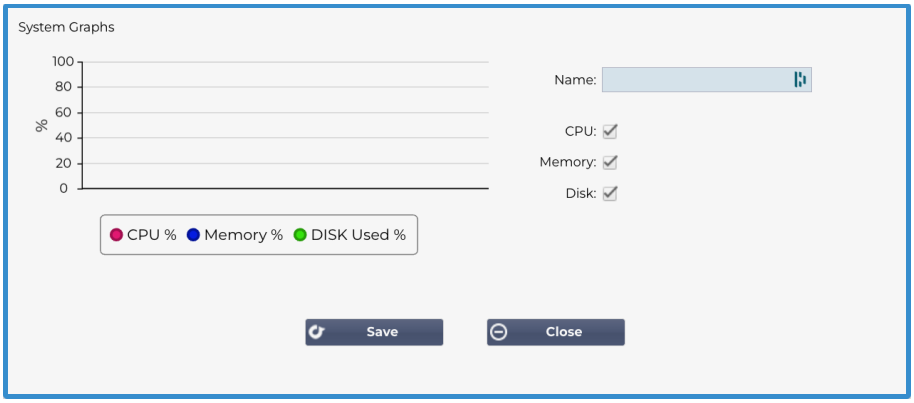
- Vous verrez maintenant un widget supplémentaire appelé Événements d'attention dans le menu déroulant des widgets configurés.



- Vous pouvez voir que nous avons ajouté ce widget dans la section Affichage > Tableau de bord.
- Sélectionnez le widget Attention Events pour l'afficher dans le tableau de bord. Voir ci-dessous.

Vous pouvez également interrompre et redémarrer le flux de données en direct en cliquant sur le bouton Pause Live Data (Interrompre les données en direct). En outre, vous pouvez à tout moment revenir au tableau de bord par défaut en cliquant sur le bouton Tableau de bord par défaut.

Le widget des graphiques du système

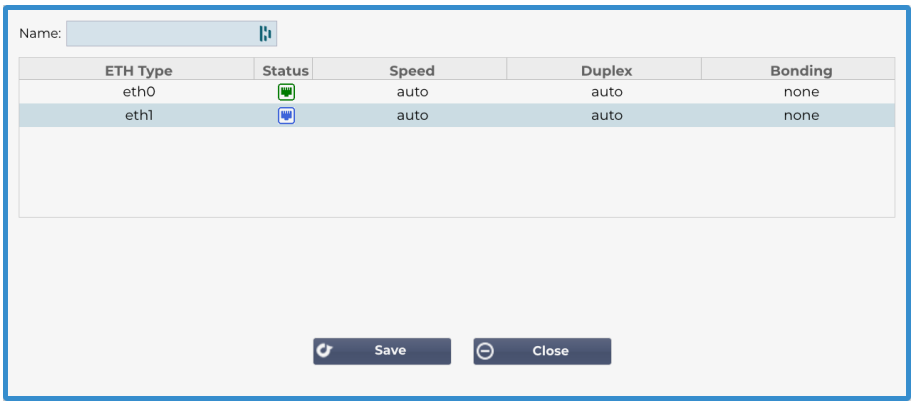


L'ADC dispose d'un widget System Graph configurable. En cliquant sur le bouton Ajouter du widget, vous pouvez ajouter les graphiques de surveillance suivants à afficher.

- UNITÉ CENTRALE
- MÉMOIRE
- DISQUE

Une fois ajoutés, ils seront disponibles individuellement dans le menu des widgets du tableau de bord.

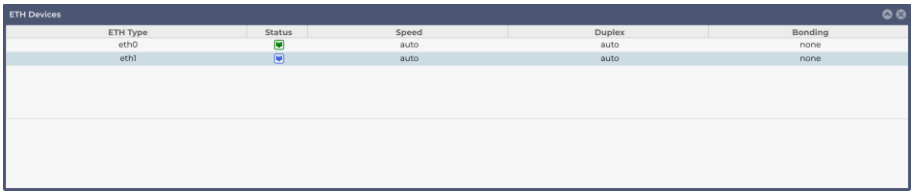
Widget d'interface



Le widget Interface vous permet d'afficher les données de l'interface réseau choisie, telle que ETH0, ETH1, etc. Le nombre d'interfaces disponibles pour l'ajout dépend du nombre d'interfaces réseau que vous avez définies pour l'appliance virtuelle ou provisionnées dans l'appliance matérielle.

Une fois que vous avez terminé, cliquez sur le bouton Enregistrer, puis sur le bouton Fermer.

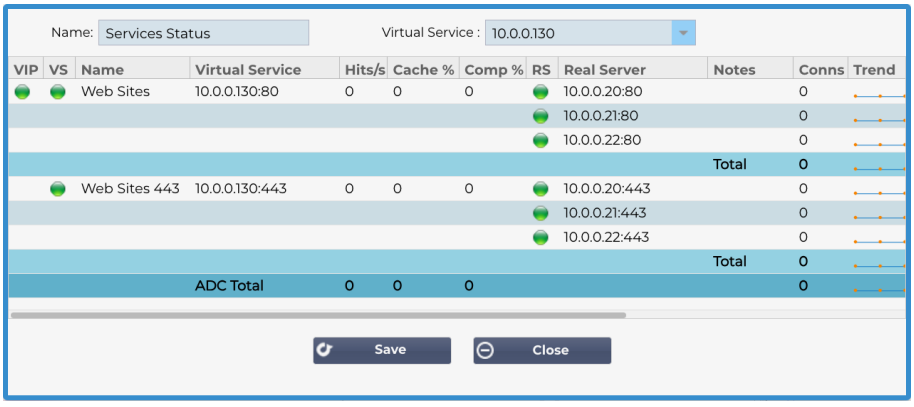
Sélectionnez le widget que vous venez de personnaliser dans le menu déroulant du tableau de bord. Vous verrez un écran comme celui ci-dessous.



Widget d'état

Le widget d'état vous permet de voir l'équilibrage de charge en action. Vous pouvez également filtrer la vue pour afficher des informations spécifiques.

- Cliquez sur Ajouter.



- Saisissez un nom pour le service que vous souhaitez surveiller
- Vous pouvez également choisir les colonnes que vous souhaitez afficher dans le widget en cliquant sur l'en-tête de la colonne.
- Lorsque vous êtes satisfait, cliquez sur Enregistrer, puis sur Fermer.
- Le widget Statut choisi sera disponible dans la section Tableau de bord.

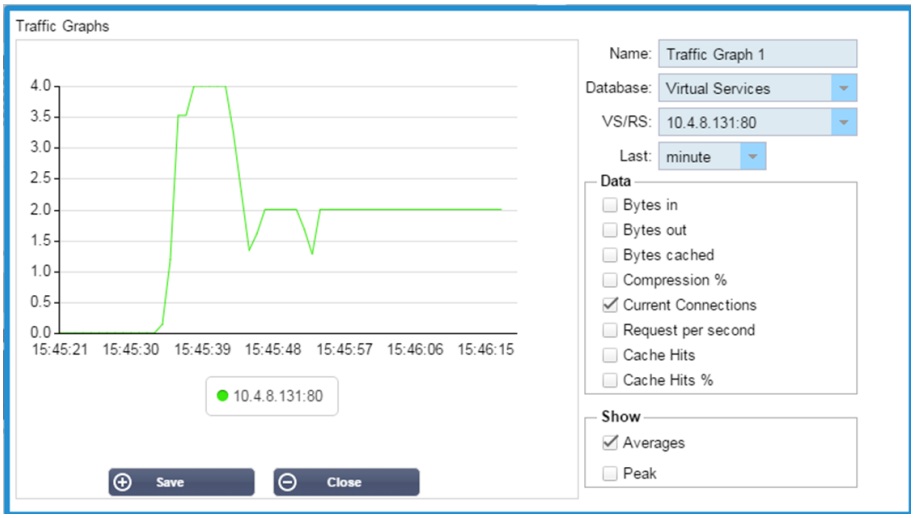
Widget graphique de trafic

Ce widget peut être configuré pour afficher les données actuelles et historiques du trafic par services virtuels et serveurs réels. En outre, vous pouvez voir les données actuelles et historiques du trafic global.

- Cliquez sur le bouton Ajouter
- Nommez votre widget.
- Choisissez une base de données parmi les services virtuels, les serveurs réels ou le système.
- Si vous choisissez Services virtuels, vous pouvez sélectionner un service virtuel dans la liste déroulante VS/RS.
- Choisissez une période dans la liste déroulante Dernière.
    - Minute - derniers 60s
    - Heure - données agrégées de chaque minute pour les 60 dernières minutes
    - Jour - données agrégées de chaque heure pour les 24 heures précédentes
    - Semaine - données agrégées pour chaque jour des sept jours précédents
    - Mois - données agrégées de chaque semaine pour les sept derniers jours
    - Année - données agrégées pour chaque mois des 12 derniers mois
- Sélectionnez les données disponibles en fonction de la base de données que vous avez choisie.
    - Base de données des services virtuels
    - Octets en
    - Octets sortants
    - Octets mis en cache
    - Compression %
    - Connexions actuelles
    - Demandes par seconde
    - Cache Hits
    - Hits du cache %
- Serveurs réels
    - Octets en
    - Octets sortants
    - Connexions actuelles
    - Demande par seconde
    - Temps de réponse
- Système
    - % DE L'UNITÉ CENTRALE
    - Services CPU
    - Mémoire %
    - % de disque libre
    - Octets en
    - Octets sortants

- Choix de l'affichage des valeurs moyennes ou des valeurs maximales
- Une fois que vous avez choisi toutes les options, cliquez sur Enregistrer et fermer.

Exemple de graphique de trafic



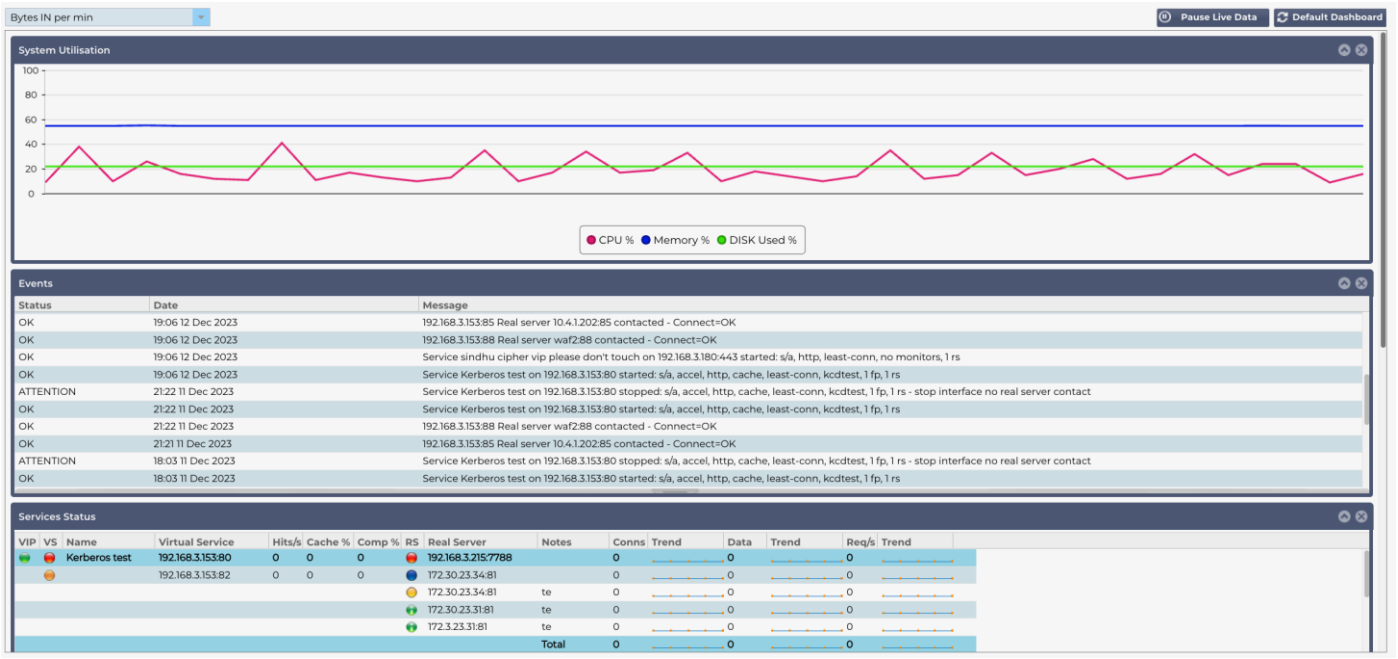
Vous pouvez maintenant ajouter votre widget Traffic Graph au tableau de bord View>

Voir

Tableau de bord

Comme pour toutes les interfaces de gestion des systèmes informatiques, il est souvent nécessaire de consulter les mesures de performance et les données gérées par l'ADC. Nous fournissons un tableau de bord personnalisable pour vous permettre de le faire de manière simple et significative.

Le tableau de bord est accessible en utilisant le segment Vue du panneau du navigateur. Lorsqu'il est sélectionné, il affiche plusieurs widgets par défaut et vous permet de choisir les widgets personnalisés que vous avez définis.



Utilisation du tableau de bord

Le tableau de bord U comporte quatre éléments : le menu des widgets, le bouton Pause/Lecture et le bouton Tableau de bord par défaut.

Le menu Widgets

Le menu Widgets situé en haut à gauche du tableau de bord vous permet de sélectionner et d'ajouter tout widget standard ou personnalisé que vous avez défini. Pour l'utiliser, sélectionnez le widget dans le menu déroulant.

Bouton de mise en pause des données en direct

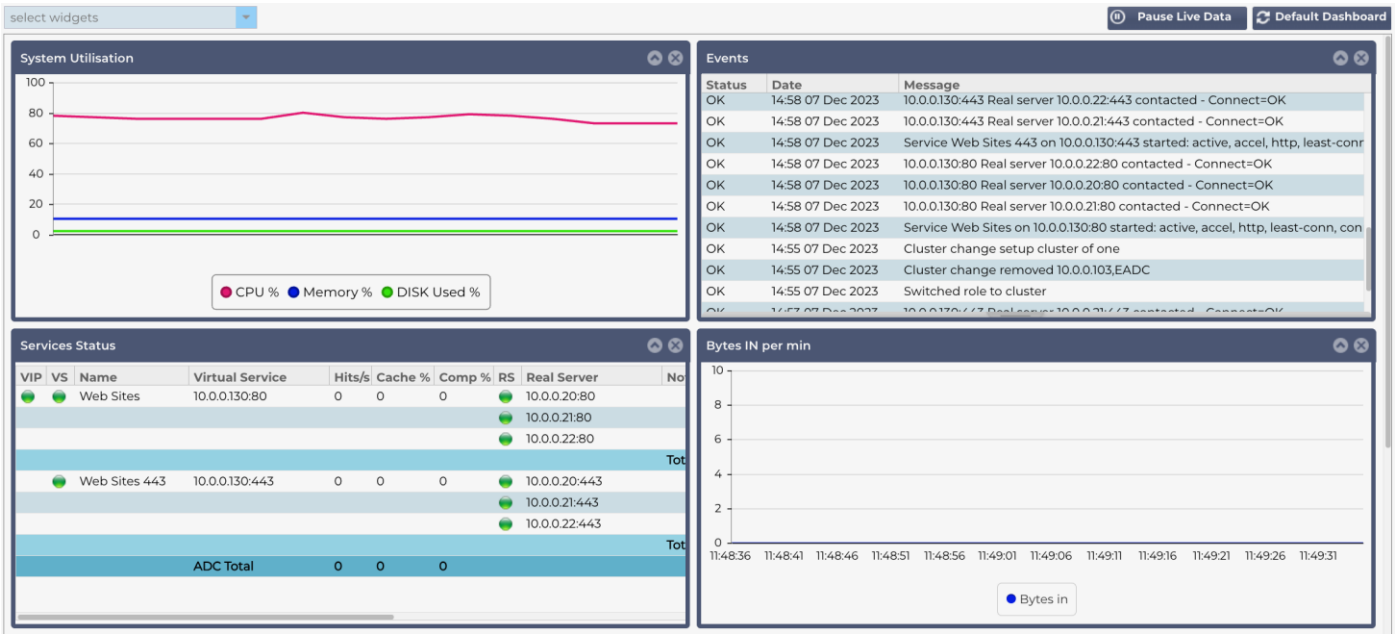
Ce bouton vous permet de choisir si le CDA doit mettre à jour le tableau de bord en temps réel. En cas de pause, aucun widget du tableau de bord n'est mis à jour, ce qui vous permet d'examiner le contenu à votre guise. Le bouton change d'état et affiche Play Live Data dès qu'une pause est initiée.

Lorsque vous avez terminé, il vous suffit de cliquer sur le bouton Lire les données en direct pour relancer la collecte des données et mettre à jour le tableau de bord.

Bouton par défaut du tableau de bord

Il se peut que vous souhaitiez rétablir la présentation par défaut du tableau de bord. Dans ce cas, cliquez sur le bouton Tableau de bord par défaut. Une fois ce bouton cliqué, toutes les modifications apportées au tableau de bord seront perdues.

Redimensionner, minimiser, réorganiser et supprimer les widgets de



Redimensionnement d'un widget

Vous pouvez redimensionner un widget très facilement. Cliquez sur la barre de titre du widget et maintenez-la enfoncée, puis faites-la glisser vers la gauche ou la droite de la zone du tableau de bord. Vous verrez apparaître un rectangle en pointillés qui représente la nouvelle taille du widget. Déposez le widget dans le rectangle et relâchez le bouton de la souris. Si vous souhaitez déposer un widget redimensionné à côté d'un widget précédemment redimensionné, vous verrez le rectangle apparaître à côté du widget que vous souhaitez déposer.

Réduire un widget

Vous pouvez réduire les widgets à tout moment en cliquant sur la barre de titre du widget. Cette action réduira le widget et n'affichera que la barre de titre.

Déplacement de l'ordre des widgets

Pour déplacer un widget, vous pouvez effectuer un glisser-déposer en cliquant sur la barre de titre et en la maintenant enfoncée, puis en déplaçant la souris.

Suppression d'un widget

Vous pouvez supprimer un widget en cliquant sur l'icône⊗ dans la barre de titre du widget.

L'histoire

L'option Historique, sélectionnable dans le navigateur, permet à l'administrateur d'examiner les performances historiques de l'ADC. Des vues historiques peuvent être générées pour les services virtuels, les serveurs réels et le système.

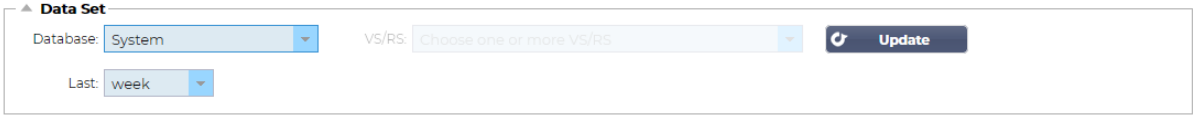
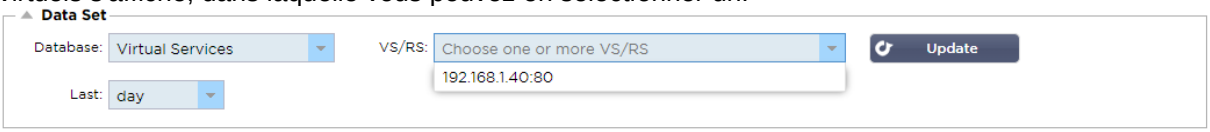
Cela vous permet également de voir l'équilibrage de la charge en action et de détecter les erreurs ou les schémas qui doivent être examinés. Notez que vous devez activer la journalisation historique dans Système > Historique pour utiliser cette fonctionnalité.

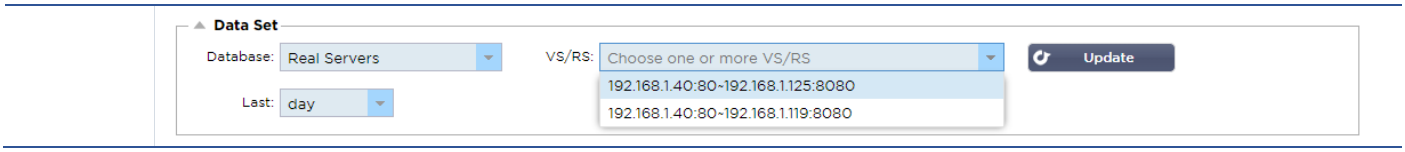
Visualisation de données graphiques

Ensemble de données

Pour visualiser les données historiques sous forme de graphiques, veuillez procéder comme suit :

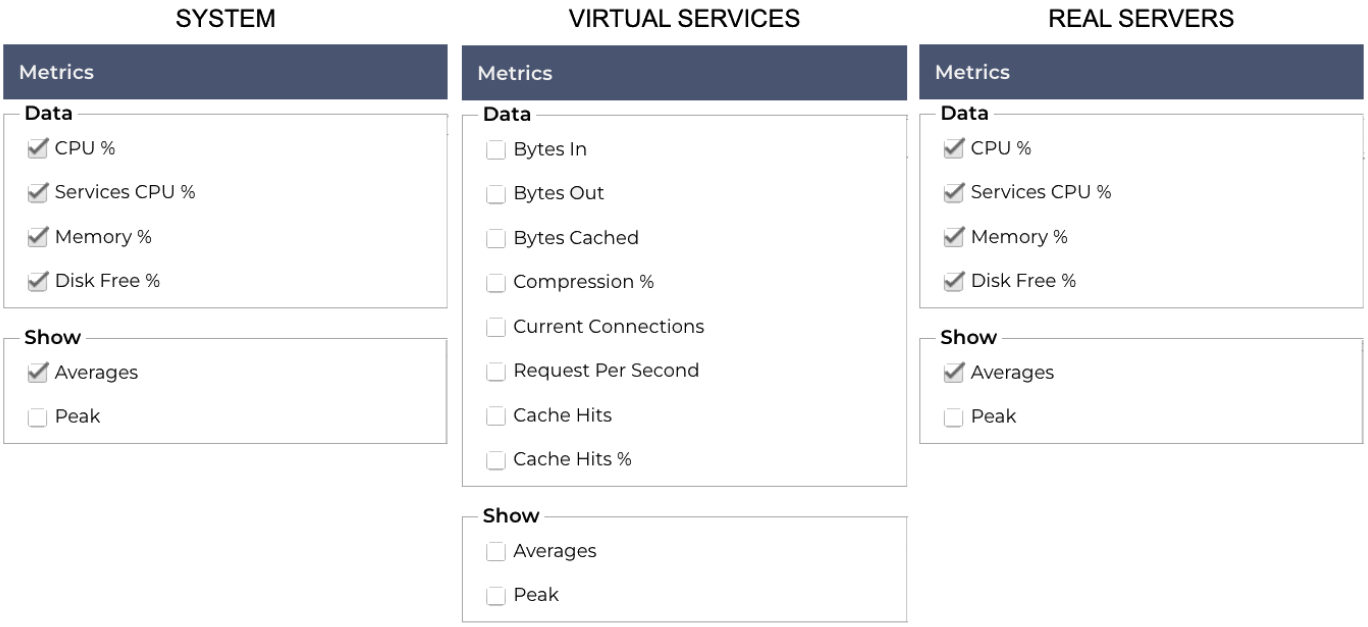
La première étape consiste à choisir la base de données et la période correspondant aux informations que vous souhaitez consulter. La période que vous pouvez sélectionner dans le menu déroulant Dernière est la minute, l'heure, le jour, la semaine, le mois et l'année.

Base de données	Description
Système	En sélectionnant cette base de données, vous pourrez voir l'évolution de l'unité centrale, de la mémoire et de l'espace disque. 
Services virtuels	En sélectionnant cette base de données, vous pourrez choisir tous les services virtuels de la base de données à partir du moment où vous avez commencé à enregistrer des données. Une liste de services virtuels s'affiche, dans laquelle vous pouvez en sélectionner un. 
Services réels	En sélectionnant cette base de données, vous pourrez choisir tous les serveurs réels de la base de données à partir du moment où vous avez commencé à enregistrer les données. Une liste de serveurs réels s'affiche, dans laquelle vous pouvez en sélectionner un.

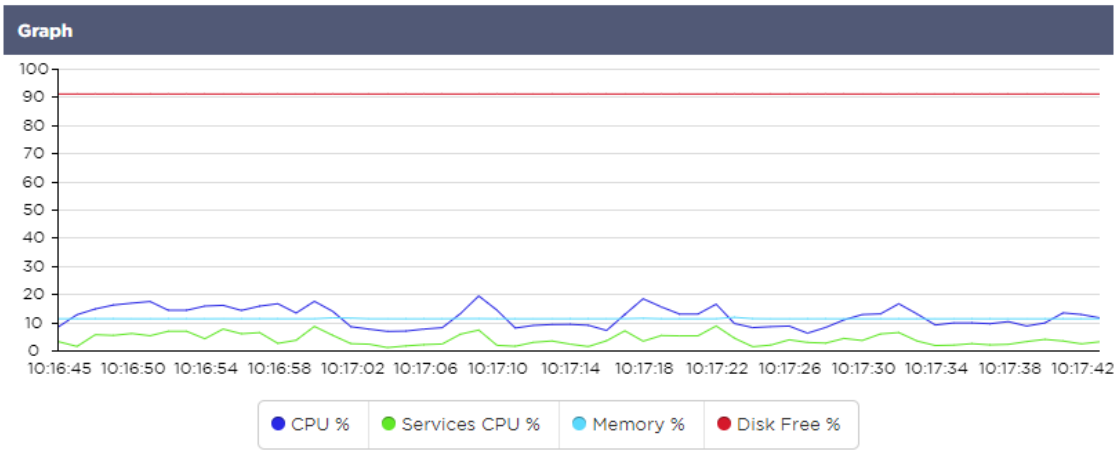


Métriques

Une fois que vous avez sélectionné l'ensemble de données que vous allez utiliser, il est temps de choisir les mesures que vous souhaitez afficher. L'image ci-dessous illustre les mesures que l'administrateur peut sélectionner : ces sélections correspondent au système, aux services virtuels et aux serveurs réels (de gauche à droite).



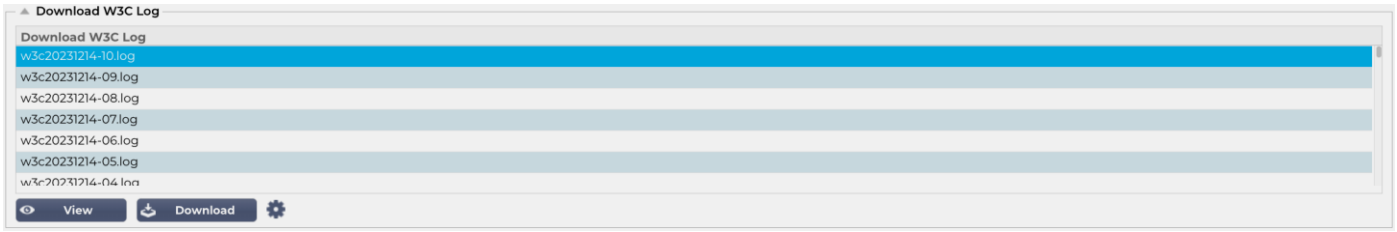
Exemple de graphique



Journaux

La page Journaux de la section Affichage vous permet de prévisualiser et de télécharger les journaux du W3C et du système. La page est organisée en deux sections, comme indiqué ci-dessous.

Journaux du W3C



La journalisation W3C est activée dans la section Système > Journalisation. Un journal W3C est un journal d'accès pour les serveurs Web dans lequel sont générés des fichiers texte contenant des données sur chaque demande d'accès, notamment l'adresse IP (Internet Protocol) source, la version HTTP, le type de navigateur, la page de référence et l'horodatage. Les journaux du W3C peuvent devenir très volumineux en fonction de la quantité de données et de la catégorie de journalisation enregistrée.

Dans la section W3C, vous pouvez sélectionner le journal dont vous avez besoin, puis le consulter ou le télécharger.

Voir le bouton

Le bouton Visualiser vous permet de visualiser le journal choisi dans la fenêtre d'un éditeur de texte, tel que le Bloc-notes.

Bouton de téléchargement

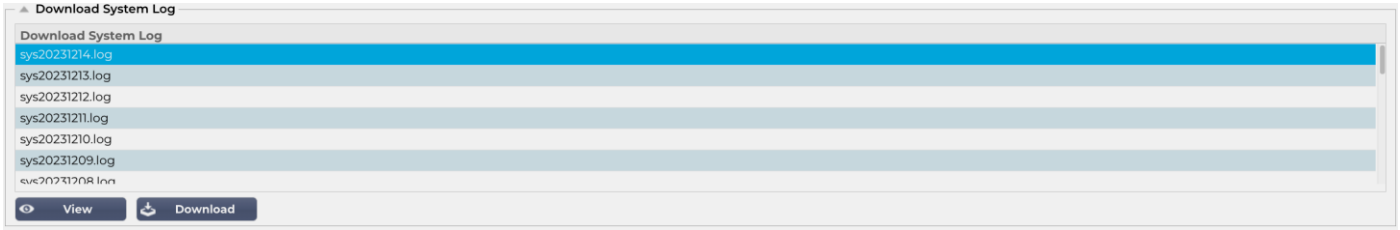
Ce bouton vous permet de télécharger le journal sur votre espace de stockage local pour le consulter ultérieurement.

L'icône du rouage

En cliquant sur cette icône, vous accédez à la section Paramètres de journalisation du W3C, située dans Système > Journalisation. Nous en parlerons en détail dans la section Journalisation de ce guide.

Journal du système

Le journal du système est essentiel pour déboguer ou examiner ce qui s'est passé avec l'ADC. Il est destiné à des personnes assez expérimentées au sein du service informatique.



Voir le bouton

Le bouton Visualiser vous permet de visualiser le journal choisi dans la fenêtre d'un éditeur de texte, tel que le Bloc-notes.

Bouton de téléchargement

Ce bouton vous permet de télécharger le journal sur votre espace de stockage local pour le consulter ultérieurement.

Statistiques

La section Statistiques de l'ADC est une zone très utilisée par les administrateurs système qui veulent s'assurer que les performances de l'ADC sont conformes à leurs attentes.

Compression

L'objectif principal de l'ADC est de contrôler les données et de les diriger vers les serveurs réels configurés pour les recevoir. La fonction de compression est fournie par l'ADC pour augmenter ses performances. Dans certains cas, les administrateurs souhaiteront tester et vérifier les informations de compression des données de l'ADC ; ces données sont fournies par le panneau Compression dans les Statistiques.

Compression de contenu à ce jour

Content Compression To Date	
Compression	0%
Throughput Before Compression	0
Throughput After Compression	0

Les données présentées dans cette section détaillent le niveau de compression atteint par l'ADC sur le contenu compressible. Une valeur de 60-80% est ce que nous qualifierions de typique.

Compression globale à ce jour

Overall Compression To Date			Current Values
Compression	0%		0%
Throughput Before Compression	0		0.00 Mbps (data)
Throughput After Compression	0		0.00 Mbps (data)
Throughput From Cache	0		0.00 Mbps (data)
		Total	0.00 Mbps (data)

Les valeurs fournies dans cette section indiquent le niveau de compression atteint par l'ADC sur l'ensemble du contenu. Le pourcentage type dépend du nombre d'images précompressées contenues dans vos services. Plus le nombre d'images est élevé, plus le pourcentage de compression global est susceptible d'être faible.

Total des entrées/sorties

Total Input	345.9 MB	Input/s	12.7 kbps
Total Output	296.8 MB	Output/s	25.7 kbps

Les chiffres du total des entrées/sorties représentent la quantité de données brutes qui entrent et sortent de l'ADC. L'unité de mesure change au fur et à mesure que la taille augmente, passant de kbps à Mbps puis à Gbps.

Coups d'éclat et connexions

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

La section Hits et Connections contient les statistiques globales des hits et des transactions qui passent par l'ADC. Que signifient les hits et les connexions ?

- Un Hit est défini comme une transaction de la couche 7. Généralement utilisé pour les serveurs web, il s'agit d'une requête GET pour un objet tel qu'une image.
- Une connexion est définie comme une connexion TCP de niveau 4. Plusieurs transactions peuvent avoir lieu sur une seule connexion TCP.

Nombre total de visites comptabilisées

Les chiffres de cette section indiquent le nombre cumulé d'accès non mis en cache depuis la dernière réinitialisation. Sur le côté droit, la figure indique le nombre actuel de résultats par seconde.

Total des connexions

La valeur Total Connections représente le nombre cumulé de connexions TCP depuis la dernière réinitialisation. Le chiffre de la deuxième colonne indique les connexions TCP établies par seconde avec l'ADC. Le chiffre de la colonne de droite est le nombre de connexions TCP par seconde avec les serveurs réels. Exemple 6/8 connexions/sec. Dans l'exemple présenté, nous avons 6 connexions TCP par seconde vers le service virtuel et 6 connexions TCP par seconde vers les serveurs réels.

Connexions de pointe

La valeur "peak Connections" représente le nombre maximum de connexions TCP effectuées vers l'ADC. Le nombre dans la colonne de droite indique le nombre actuel de connexions TCP actives.

Mise en cache

Comme vous vous en souvenez, l'ADC est équipé à la fois de la compression et de la mise en cache. Cette section présente les statistiques globales relatives à la mise en cache lorsqu'elle est appliquée à un canal. Si la mise en cache n'a pas été appliquée à un canal et configurée correctement, vous verrez 0 contenu de cache.

Content Caching	Hits	Bytes
From Cache	0 / -	0 / -
From Server	0 / -	0 / -
Cache Contents	0 entries	0 / 0.0%

Depuis le cache

Hits : La première colonne indique le nombre total de transactions servies par la mémoire cache de l'ADC depuis la dernière réinitialisation. Un pourcentage du total des transactions est également fourni.

octets : La deuxième colonne indique la quantité totale de données en kilo-octets servies par la mémoire cache de l'ADC. Un pourcentage des données totales est également indiqué.

Du serveur

Hits : La colonne 1 indique le nombre total de transactions servies par les serveurs réels depuis la dernière réinitialisation. Un pourcentage du total des transactions est également fourni.

Octets : La deuxième colonne indique la quantité totale de données en kilo-octets servies par les serveurs réels. Un pourcentage des données totales est également indiqué.

Contenu du cache

Hits : Ce chiffre indique le nombre total d'objets contenus dans la mémoire cache du CDA.

Octets : Le premier chiffre indique la taille globale en mégaoctets des objets mis en cache par l'ADC. Un pourcentage de la taille maximale du cache est également indiqué.

Tampon d'application

Buffer Type	Connections Used/Free	Memory Used/Free	Average Buffer Fill Size
Low	0/5k(0%)	0/655MB(0%)	0
Medium	0/5k(0%)	0/30MB(0%)	0
High	0/10k(0%)	0/20MB(0%)	0

L'utilisation de tampons d'application dans l'ADC permet d'optimiser les performances, d'améliorer le débit et de garantir un flux de données fiable et efficace entre les clients et les serveurs. La taille des tampons, les politiques de traitement et d'autres paramètres sont optimisés par l'ADC pour ajuster la charge en fonction des exigences spécifiques des applications et de l'infrastructure.

Avec l'EdgeADC, nous faisons le travail à votre place et ajustons automatiquement les paramètres des tampons en fonction des besoins.

Persistance de la session

Total current sessions	0
% used (of max)	0
New sessions this min	0
Revalidations this min	0
Expired sessions this min	0

La section Persistance de la session fournit des informations sur plusieurs paramètres.

Total des sessions en cours

Elle indique le nombre de sessions de persistance en cours - mise à jour toutes les minutes.

% utilisé (du maximum)

Cela montre l'utilisation de l'espace total autorisé pour les informations de session.

Nouvelle session ce matin

Cela montre, au cours de la dernière minute, combien de nouvelles sessions de persistance ont été ajoutées.

Revalider cette minute

Cela montre, au cours de la dernière minute, combien de sessions de persistance existantes ont été revalidées par un trafic plus important.

Sessions expirées ce mois-ci

Cela montre, au cours de la dernière minute, combien de sessions de persistance existantes ont expiré parce qu'il n'y avait plus de trafic dans le délai imparti.

Matériel

Que vous utilisiez l'ADC dans un environnement virtuel ou matériel, cette section vous fournira des informations précieuses sur les performances de l'appareil.

Disk Usage	2%
Memory Usage	10.1%(185.4MB of 1832.7MB)
CPU Usage	76.0%

Utilisation du disque

La valeur fournie dans la colonne 2 indique le pourcentage d'espace disque actuellement utilisé et inclut des informations sur les fichiers journaux et les données de cache, qui sont périodiquement stockées sur le disque.

Utilisation de la mémoire

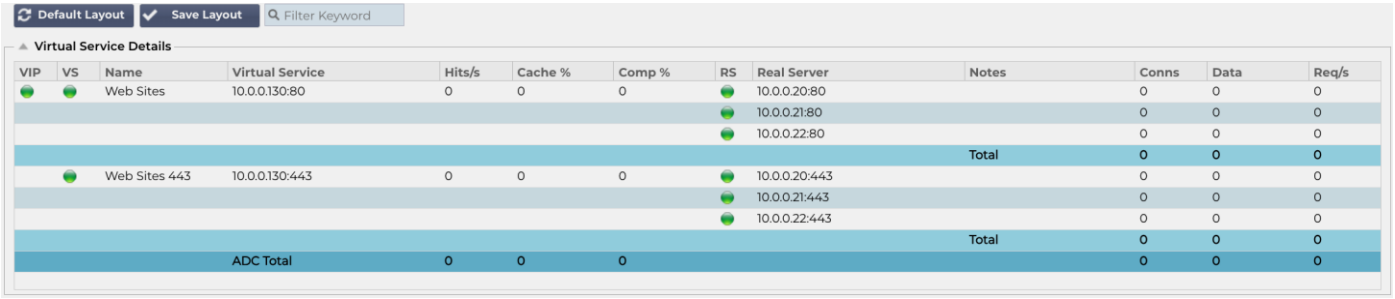
La deuxième colonne indique le pourcentage de mémoire actuellement utilisé. Le chiffre le plus important entre parenthèses est la quantité totale de mémoire allouée à l'ADC. Il est recommandé d'allouer au CDA un minimum de 2 Go de RAM.

Utilisation de l'unité centrale

L'une des valeurs critiques fournies est le pourcentage de CPU actuellement utilisé par l'ADC. Il est naturel que ce pourcentage fluctue.

Statut

La page View > Status affiche le trafic en direct qui traverse l'ADC pour les services virtuels que vous avez définis. Elle indique également le nombre de connexions et de données vers chaque serveur réel afin que vous puissiez constater l'équilibrage de la charge en temps réel.



VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s
		Web Sites	10.0.0.130:80	0	0	0		10.0.0.20:80		0	0	0
								10.0.0.21:80		0	0	0
								10.0.0.22:80		0	0	0
									Total	0	0	0
		Web Sites 443	10.0.0.130:443	0	0	0		10.0.0.20:443		0	0	0
								10.0.0.21:443		0	0	0
								10.0.0.22:443		0	0	0
									Total	0	0	0
			ADC Total	0	0	0				0	0	0

Détails du service virtuel

Colonne VIP

La couleur du voyant indique l'état de l'adresse IP virtuelle associée à un ou plusieurs services virtuels.

Statut	Description
●	En ligne
●	Failover-Standby. Ce service virtuel est en attente à chaud
●	Indique qu'un "passif" attend un "actif"
●	Hors ligne. Les serveurs réels sont inaccessibles ou aucun serveur réel n'est activé.
●	État des recherches
●	Pas de licence ou IP virtuelles sous licence dépassées

Colonne d'état VS

La couleur du voyant indique l'état du service virtuel.

Statut	Description
●	En ligne
●	Failover-Standby. Ce service virtuel est en attente à chaud
●	Indique qu'un "passif" attend un "actif"
●	Le service a besoin d'attention. Cette indication d'état peut résulter de l'échec d'un contrôle de santé d'un serveur réel ou d'un passage manuel à l'état hors ligne. Le trafic continuera à circuler mais avec une capacité réduite du serveur réel.
●	Hors ligne. Les serveurs réels sont inaccessibles ou aucun serveur réel n'est activé.
●	État des recherches
●	Pas de licence ou IP virtuelles sous licence dépassées

Nom

Le nom du service virtuel

Service virtuel (VIP)

L'adresse IP virtuelle et le port pour le service et l'adresse que les utilisateurs ou les applications utiliseront.

Hit/Sec

Couche 7 transactions par seconde côté client.

Cache%

Le chiffre fourni ici représente le pourcentage d'objets qui ont été servis à partir du cache RAM de l'ADC.

Compression%.

Ce chiffre représente le pourcentage d'objets qui ont été compressés entre le client et le CDA.

État RS (serveur distant)

Le tableau ci-dessous indique la signification de l'état des serveurs réels liés au VIP.

Statut	Description
●	Connecté
●	Non contrôlé
●	Drainage ou hors ligne
●	En attente
●	Non connecté
●	État des recherches
●	Pas de licence ou IP virtuelles sous licence dépassées

Serveur réel

L'adresse IP et le port du serveur réel.

Notes

Cette valeur peut être toute note utile pour faire comprendre aux autres l'objet de l'entrée.

Conns (Connexions)

La représentation du nombre de connexions à chaque serveur Real vous permet de voir l'équilibrage de la charge en action. C'est très utile pour vérifier que votre politique de répartition de charge fonctionne correctement.

Données

La valeur de cette colonne indique la quantité de données envoyées à chaque Real Server.

Req/Sec (Requêtes par seconde)

Nombre de requêtes par seconde envoyées à chaque serveur réel.

Système

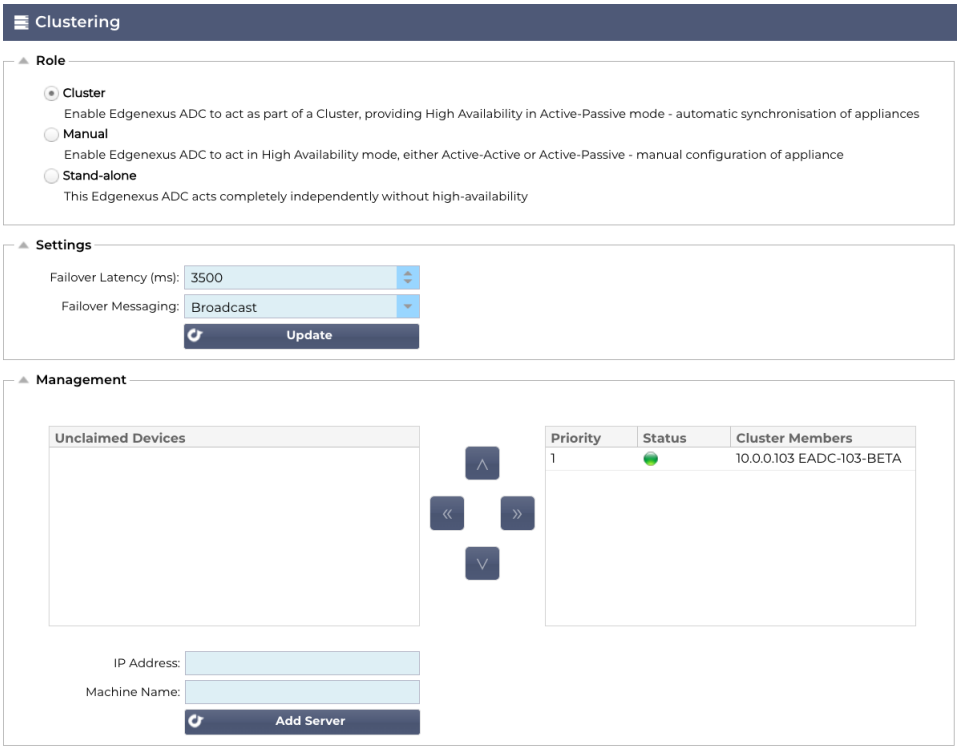
Regroupement

L'ADC peut être utilisé en tant que dispositif autonome, et il fonctionnera parfaitement bien dans ce cas. Cependant, si l'on considère que le but de l'ADC est d'équilibrer la charge d'ensembles de serveurs, la nécessité de mettre l'ADC en cluster devient évidente. L'interface utilisateur de l'ADC, facilement navigable, rend la configuration du système de clustering très simple.

La page Système > Clustering vous permet de configurer la haute disponibilité de vos appliances ADC. Cette section est organisée en plusieurs parties.

Note importante

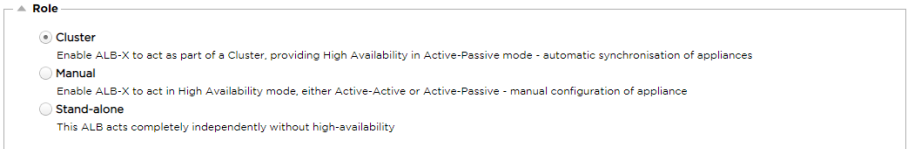
- Il n'est pas nécessaire d'avoir un câble dédié entre la paire d'ADC pour maintenir un rythme cardiaque de haute disponibilité.
- Le battement de cœur a lieu sur le même réseau que le service virtuel qui nécessite la mise en place d'une haute disponibilité.
- Il n'y a pas de basculement entre les appliances ADC.
- Lorsque la haute disponibilité est activée sur deux ADC ou plus, chaque boîtier diffuse via UDP les services virtuels qu'il est configuré pour fournir.
- Le basculement à haute disponibilité utilise la messagerie monodiffusion et l'ARP gratuit pour informer les nouveaux commutateurs d'équilibrage de charge actifs.



Rôle

Trois rôles de cluster sont disponibles lorsque vous configurez l'ADC pour la haute disponibilité.

Groupement d'entreprises



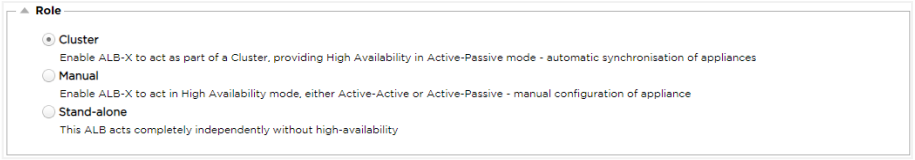
- Par défaut, un nouvel ADC est mis sous tension en utilisant le rôle Cluster. Dans ce rôle, chaque membre de la grappe a la même "configuration de travail" et, par conséquent, un seul CDA de la grappe est actif à la fois.
- Par "configuration de travail", on entend tous les paramètres de configuration, à l'exception des éléments qui doivent être uniques, tels que l'adresse IP de gestion, le nom de l'ALB, les paramètres réseau, les détails de l'interface, etc.
- L'ADC en priorité 1, la position la plus élevée, de la boîte Membres du cluster est le propriétaire du cluster et l'équilibreur de charge actif, tandis que tous les autres ADC sont des membres passifs.
- Vous pouvez modifier n'importe quel CDA du cluster et les modifications seront synchronisées avec tous les membres du cluster.
- Lorsque vous supprimez un ADC du cluster, tous les services virtuels sont supprimés de cet ADC.
- Vous ne pouvez pas supprimer le dernier membre du cluster dans les dispositifs non réclamés. Pour supprimer le dernier membre, veuillez changer le rôle en Manuel ou Autonome.
- Les objets suivants ne sont pas synchronisés :
    - Section date et heure manuelle - (la section NTP est synchronisée)
    - Latence de basculement (ms)
    - Section du matériel
    - Section appareils
    - Section réseau

Défaillance du propriétaire du cluster

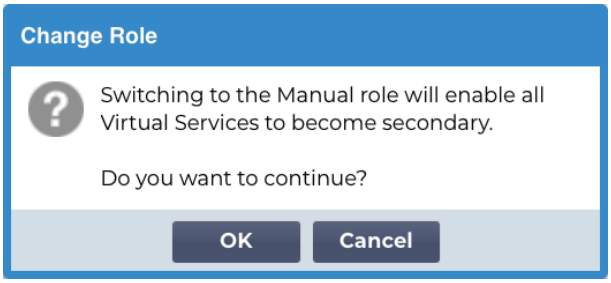
- En cas de défaillance du propriétaire d'une grappe, l'un des membres restants prend automatiquement le relais et assure l'équilibrage du trafic.
- Lorsque le propriétaire de la grappe revient, il reprend le trafic d'équilibrage de la charge et reprend le rôle de propriétaire.
- Supposons que le propriétaire ait échoué et qu'un membre ait pris en charge l'équilibrage de la charge. Si vous souhaitez que le membre qui a pris en charge l'équilibrage du trafic devienne le nouveau propriétaire, mettez-le en surbrillance et cliquez sur la flèche vers le haut pour le placer en position de priorité 1.
- Si vous modifiez l'un des membres restants de la grappe et que le propriétaire est en panne, le membre modifié sera automatiquement promu au propriétaire sans perte de trafic.

Changer le rôle de Cluster en rôle Manuel

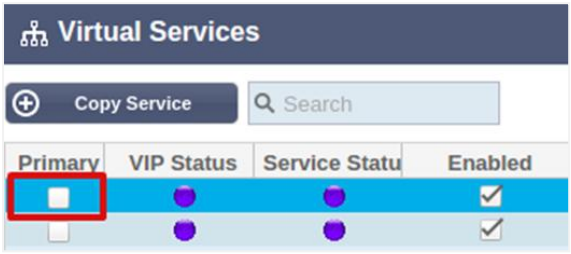
- Si vous souhaitez modifier le rôle de Cluster en Manuel, cliquez sur le bouton radio situé à côté de l'option de rôle Manuel.



- Après avoir cliqué sur le bouton radio, vous verrez le message suivant :



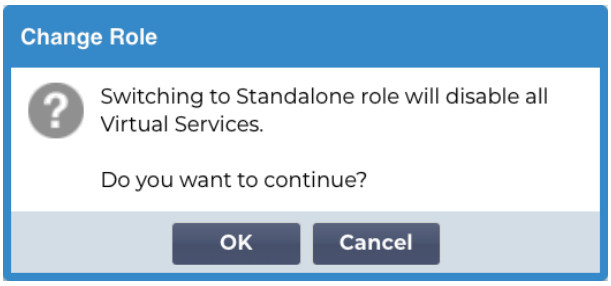
- Cliquez sur le bouton OK
- Vérifiez la section Services virtuels. Vous constaterez que la colonne Primaire affiche désormais une case décochée.



- Il s'agit d'une fonction de sécurité qui signifie que si vous avez un autre CDA avec les mêmes services virtuels, il n'y aura pas d'interruption du flux de trafic.

Passer d'un rôle de groupe à un rôle autonome

- Si vous souhaitez changer le rôle de Cluster à Autonome, cliquez sur le bouton radio à côté de l'option Autonome.
- Le message suivant s'affiche :



- Cliquez sur OK pour modifier les rôles.
- Vérifiez vos services virtuels. Vous verrez que la colonne Primaire a changé de nom et est devenue Autonome.
- Vous verrez également que tous les services virtuels sont désactivés (décochés) pour des raisons de sécurité.
- Une fois que vous êtes sûr qu'aucun autre ADC sur le même réseau n'a de services virtuels en double, vous pouvez activer chacun d'entre eux à tour de rôle.

Rôle manuel

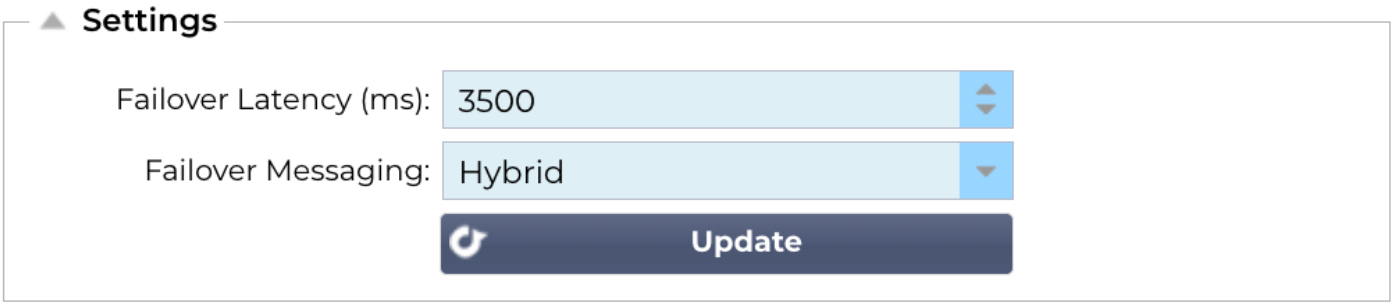
Un CDA dans le rôle manuel travaillera avec d'autres CDA dans le rôle manuel pour fournir une haute disponibilité. Le principal avantage par rapport au rôle Cluster est la possibilité de définir quel CDA est actif pour une IP virtuelle. L'inconvénient est qu'il n'y a pas de synchronisation de la configuration entre les CDA. Tout changement doit être répliqué manuellement sur chaque boîte via l'interface graphique, ou pour de nombreux changements, vous pouvez créer un jetPACK à partir d'un ADC et l'envoyer à l'autre.

- Pour rendre une adresse IP virtuelle "active", cochez la case dans la colonne principale (page Services IP).
- Pour rendre une adresse IP virtuelle "passive", laissez la case à cocher vide dans la colonne primaire (page Services IP).
- En cas de défaillance d'un service actif sur le service passif :
    - Si les deux colonnes primaires sont cochées, un processus d'élection a lieu et l'adresse MAC la plus basse est active.
    - Si les deux ne sont pas cochés, le même processus d'élection a lieu. En outre, si les deux cases ne sont pas cochées, il n'y a pas de retour automatique à l'ADC actif d'origine.

Rôle autonome

Un CDA autonome ne communique pas avec les autres CDA au sujet de ses services et, par conséquent, tous les services virtuels restent dans l'état vert et connectés. Vous devez vous assurer que tous les services virtuels ont des adresses IP uniques, sinon il y aura un conflit sur votre réseau.

Paramètres

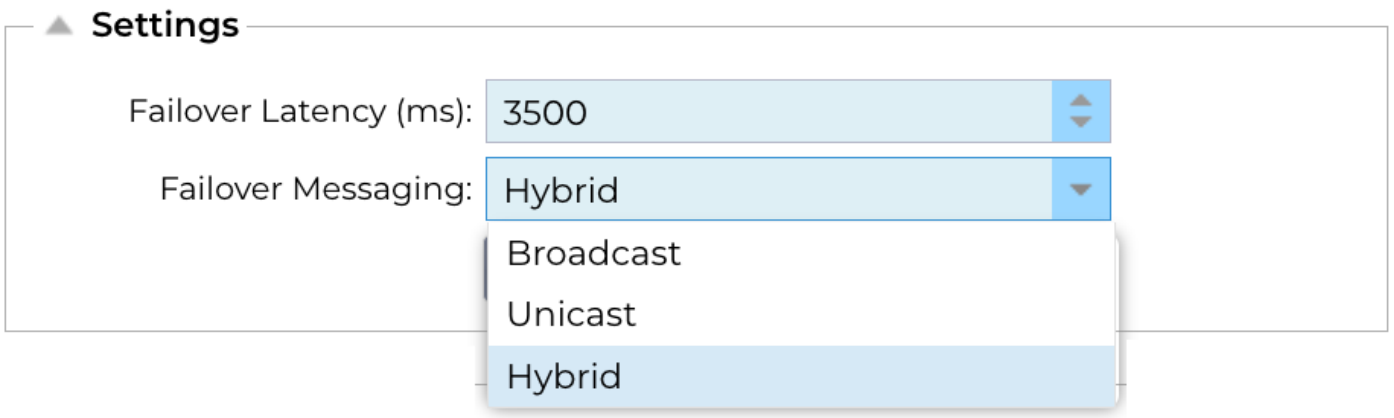


Latence de basculement (ms)

Vous pouvez définir la latence de basculement en millisecondes. Il s'agit du temps qu'un ADC passif attendra avant de reprendre les services virtuels après la défaillance de l'ADC actif.

Nous recommandons de régler cette valeur sur 10000ms ou 10 secondes, mais vous pouvez la diminuer ou l'augmenter en fonction de votre réseau et de vos besoins. Les valeurs acceptables se situent entre 1500ms et 20000ms. Si vous constatez une instabilité dans le cluster avec une latence plus faible, vous devez augmenter cette valeur.

Messagerie de basculement

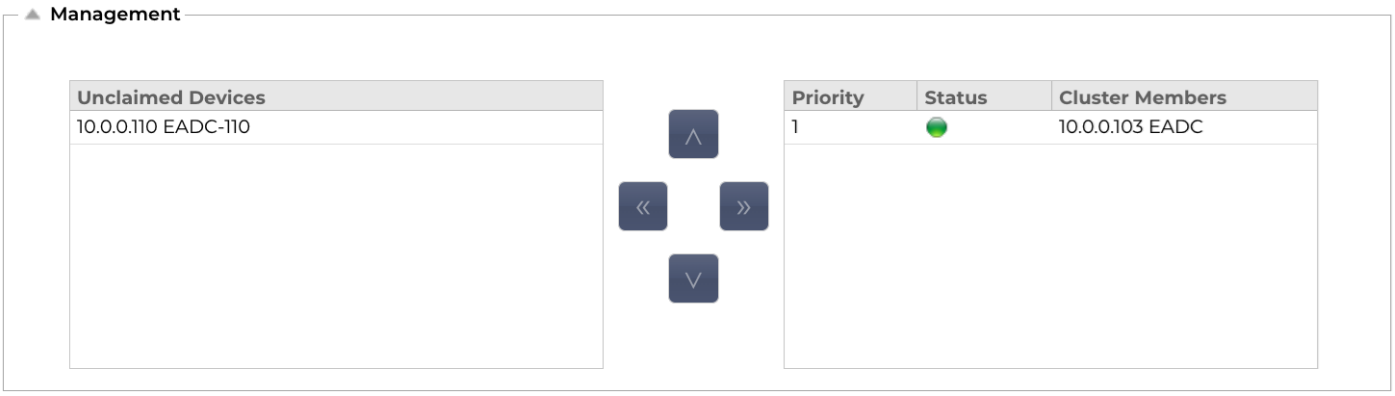


Par défaut, l'ADC utilise la diffusion pour sa messagerie de basculement. Cependant, certains réseaux bloquent la diffusion, c'est pourquoi nous avons prévu les options Unicast et Hybrid, un mélange d'Unicast et de Broadcast.

En mode diffusion par défaut, les dispositifs non réclamés sont automatiquement répertoriés et les messages de diffusion sont utilisés pour le basculement. En mode hybride, les dispositifs non réclamés continueront à faire de la publicité en mode diffusion, mais la communication de basculement se fera en mode monodiffusion (Unicast). Le mode Unicast ne diffuse pas les messages en tant que tels et vous devrez peut-être entrer manuellement les membres du cluster.

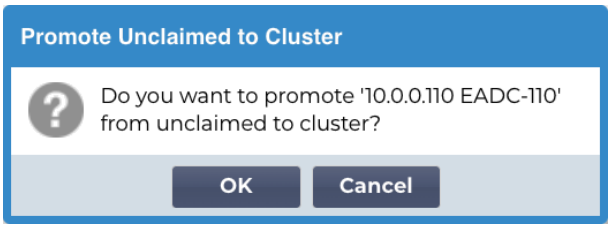
Gestion

Dans cette section, vous pouvez ajouter et supprimer des membres de la grappe et modifier la priorité d'un CDA dans la grappe. La section se compose de deux panneaux et d'un ensemble de touches fléchées entre les deux. La zone de gauche correspond aux dispositifs non réclamés, tandis que la zone de droite correspond à la grappe elle-même.

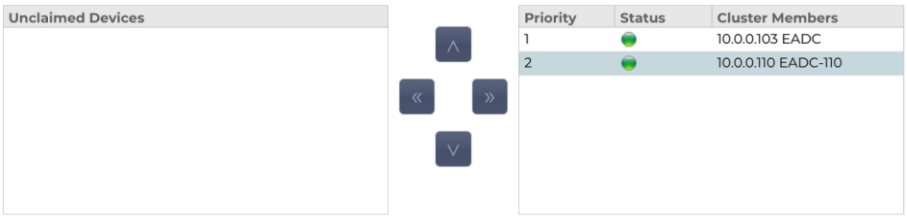


Ajout d'un ADC à la grappe

- Avant d'ajouter l'ADC au cluster, vous devez vous assurer que toutes les appliances ADC ont reçu un jeu de noms unique dans la section Système > Réseau.
- Vous devriez voir l'ADC en tant que priorité 1 avec un statut vert et son nom dans la colonne Membres du cluster dans la section de gestion. Cet ADC est l'appliance primaire par défaut.
- Tous les autres CDA disponibles apparaîtront dans la fenêtre Unclaimed Devices (Appareils non réclamés) de la section de gestion. Un appareil non réclamé est un CDA qui a été assigné dans le rôle de cluster mais qui n'a pas de services virtuels configurés.
- Mettez l'ADC en surbrillance dans la fenêtre Unclaimed Devices et cliquez sur la flèche droite.
- Le message suivant s'affiche :

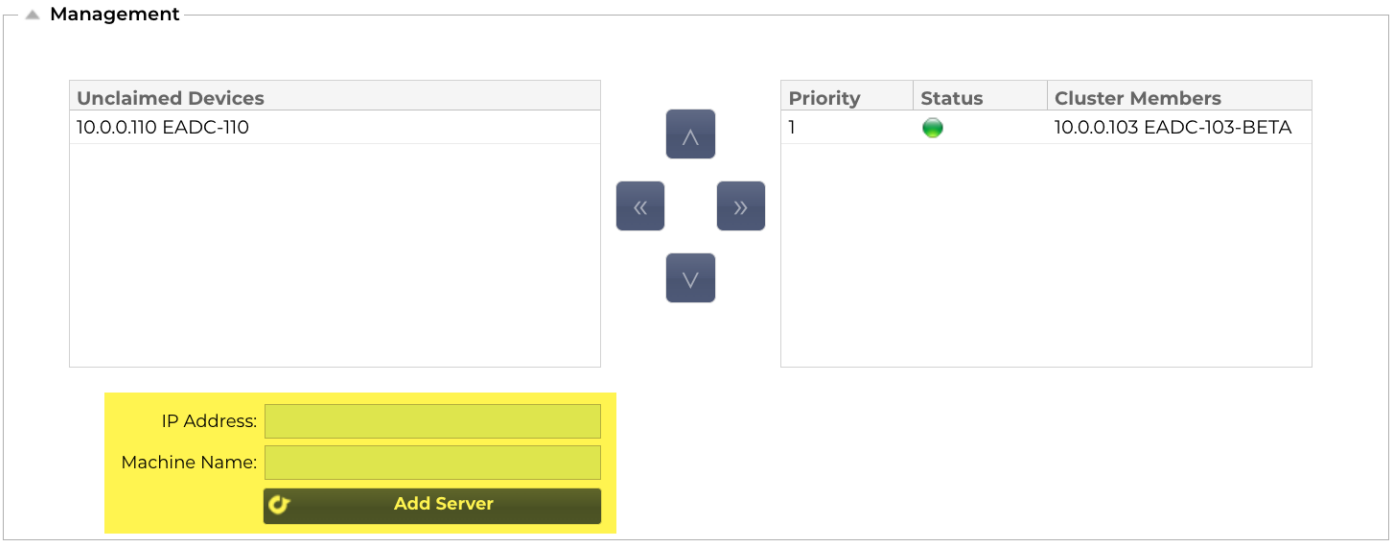


- Cliquez sur OK pour promouvoir l'ADC dans le cluster.
- Votre ADC devrait maintenant apparaître en tant que Priorité 2 dans la liste des membres du cluster.



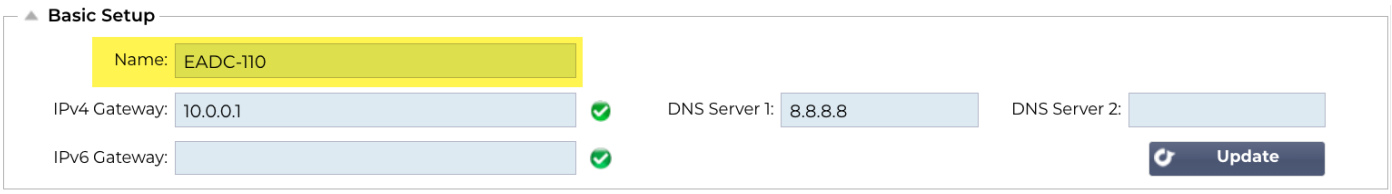
Ajout manuel d'un ADC à la grappe

Dans les systèmes où la diffusion est bloquée, vous devrez choisir le mode Unicast ou Hybrid pour ajouter un ADC au cluster.



Pour ajouter manuellement un ADC au cluster :

1. Fournir son adresse IP
2. Indiquez le nom de la machine - ce nom est disponible dans la section Système > Mise en réseau.



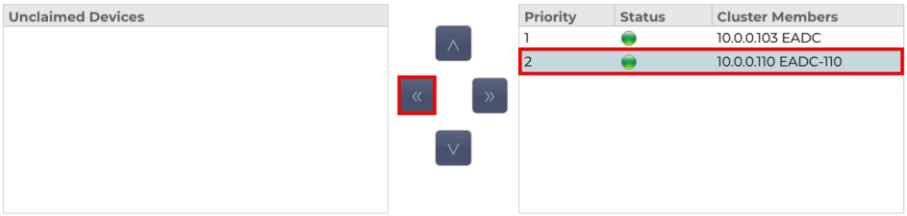
3. Cliquez sur Ajouter un serveur

L'ADC sera alors ajouté à la grappe.

Si l'ADC que vous essayez d'ajouter fait déjà partie d'un cluster, vous en serez informé par un message d'erreur.

Suppression d'un membre d'une grappe

- Mettez en surbrillance le membre du cluster que vous souhaitez supprimer du cluster.
- Cliquez sur la flèche gauche.



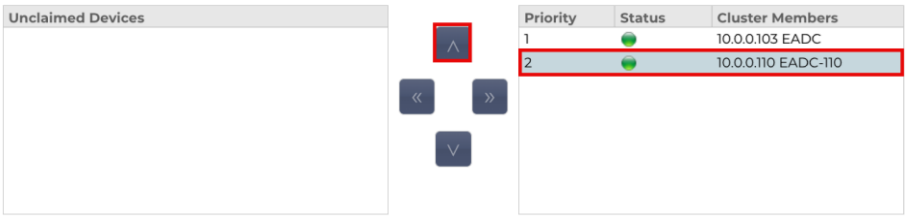
- Vous recevrez une demande de confirmation.
- Cliquez sur OK pour confirmer.
- Votre CDA sera supprimé et apparaîtra du côté des appareils non réclamés.

Modification de la priorité d'un ADC

Il peut arriver que vous souhaitiez modifier la priorité d'un CDA dans la liste des membres.

- L'ADC situé en haut de la liste des membres du cluster se voit attribuer la priorité 1 et est l'ADC actif pour tous les services virtuels.
- L'ADC qui vient en deuxième position dans la liste se voit attribuer la priorité 2 et est l'ADC passif pour tous les services virtuels.

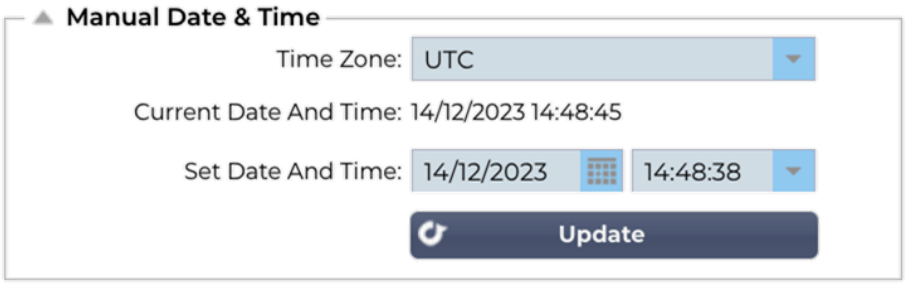
- Pour modifier l'ADC actif, il suffit de mettre en évidence et de cliquer sur la flèche vers le haut jusqu'à ce qu'il se trouve en haut de la liste.



Date et heure

La section date et heure permet de définir les caractéristiques date/heure de l'ADC, y compris le fuseau horaire dans lequel l'ADC est situé. Avec le fuseau horaire, la date et l'heure jouent un rôle essentiel dans les processus cryptographiques associés au cryptage SSL.

Date et heure manuelles



Fuseau horaire

La valeur que vous définissez dans ce champ représente le fuseau horaire dans lequel se trouve l'ADC.

- Cliquez sur la liste déroulante du fuseau horaire et commencez à saisir votre emplacement.
- Par exemple Londres
- Lorsque vous commencez à taper, l'ADC affiche automatiquement les emplacements contenant la lettre L.
- Continuez à taper "Lon", et ainsi de suite - les lieux listés seront réduits à ceux contenant "Lon".
- Si vous vous trouvez, par exemple, à Londres, choisissez Europe/Londres pour définir votre emplacement.

Si la date et l'heure sont toujours incorrectes après la modification ci-dessus, veuillez modifier la date manuellement.

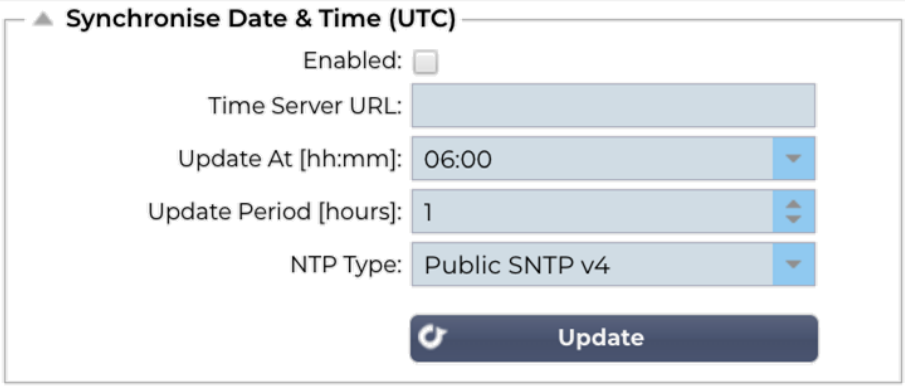
Régler la date et l'heure

Ce paramètre représente la date et l'heure réelles.

- Choisissez la date correcte dans la première liste déroulante ou,
  vous pouvez également saisir la date dans le format suivant : JJ/MM/AAAA
- Ajoutez l'heure dans le format suivant hh : mm : ss, par exemple, 06:00:10 pour 6 heures et 10 secondes.
- Une fois que vous l'avez saisi correctement, cliquez sur Mettre à jour pour postuler.
- La nouvelle date et l'heure s'affichent alors en caractères gras.

Synchroniser la date et l'heure (UTC)

Vous pouvez utiliser des serveurs NTP pour synchroniser votre date et votre heure avec précision. Les serveurs NTP sont situés dans le monde entier, et vous pouvez également disposer de votre propre serveur NTP interne lorsque votre infrastructure impose des limites à l'accès externe.



URL du serveur de temps

Saisissez une adresse IP valide ou un nom de domaine entièrement qualifié (FQDN) pour le serveur NTP. Si le serveur est situé au niveau mondial sur Internet, il est recommandé d'utiliser un FQDN.

Mise à jour à [hh:mm]

Sélectionnez l'heure programmée à laquelle vous souhaitez que l'ADC se synchronise avec le serveur NTP.

Période de mise à jour [heures] :

Sélectionnez la fréquence à laquelle vous souhaitez que la synchronisation ait lieu.

NTP Type :

- Public SNTP V4 - Il s'agit de la méthode actuelle et préférée pour la synchronisation avec un serveur NTP. **RFC 5905**
- NTP v1 Over TCP - Version héritée de NTP sur TCP. **RFC 1059**
- NTP v1 Over UDP - Version ancienne de NTP sur UDP. **RFC 1059**

Note : Veuillez noter que la synchronisation se fait uniquement en UTC. Si vous souhaitez régler l'heure locale, vous ne pouvez le faire que manuellement. Cette limitation sera modifiée dans les versions ultérieures afin de permettre la sélection d'un fuseau horaire.

Événements par courriel

L'ADC est un appareil critique et, comme tout système essentiel, il est doté de la capacité d'informer l'administrateur des systèmes de tout problème susceptible de nécessiter une attention particulière.

La page Système > Événements de messagerie vous permet de configurer une connexion à un serveur de messagerie et d'envoyer des notifications aux administrateurs du système. La page est organisée selon les sections ci-dessous.

Adresse

Envoi d'événements par courriel à des adresses électroniques

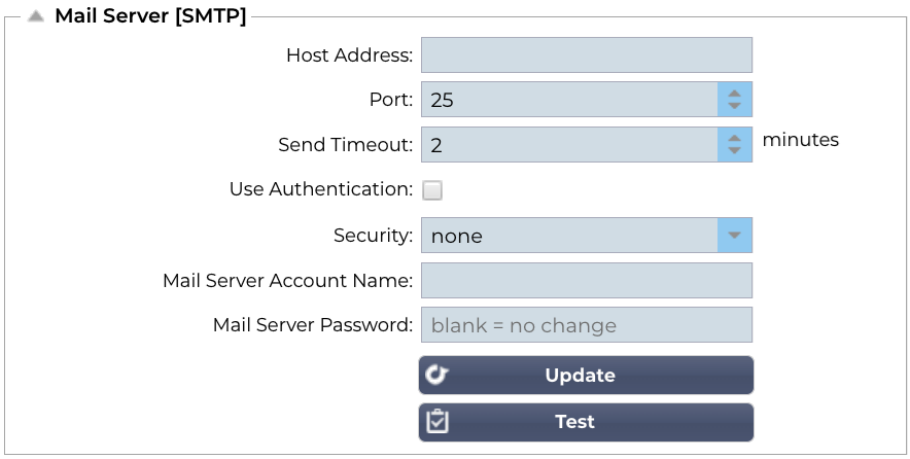
Ajoutez une adresse électronique valide à laquelle envoyer les alertes, les notifications et les événements. Exemplesupport@domain.com . Vous pouvez également ajouter plusieurs adresses électroniques en utilisant une virgule comme séparateur.

Adresse électronique de retour :

Ajoutez une adresse électronique qui apparaîtra dans la boîte de réception. Exemple . adc@domain.com

Serveur de messagerie (SMTP)

Dans cette section, vous devez ajouter les détails du serveur SMTP à utiliser pour envoyer les courriels. Veillez à ce que l'adresse électronique que vous utilisez pour l'envoi soit autorisée à le faire.



Adresse de l'hôte

Ajoutez le FQDN ou l'adresse IP de votre serveur SMTP.

Port

Ajoutez le port de votre serveur SMTP. Le port par défaut pour SMTP est 25 ou 587 si vous utilisez SSL.

Délai d'envoi

Ajoutez un délai d'attente SMTP. La valeur par défaut est de 2 minutes.

Utiliser l'authentification

Cochez la case si votre serveur SMTP nécessite une authentification.

Sécurité

- Aucun
- Le réglage par défaut est aucun.
- SSL - Utilisez ce paramètre si votre serveur SMTP nécessite une authentification Secure Sockets Layer.
- TLS - Utilisez ce paramètre si votre serveur SMTP nécessite une authentification par Transport Layer Security.

Nom du compte du serveur principal

Ajoutez le nom d'utilisateur requis pour l'authentification.

Mot de passe du serveur de messagerie

Ajoutez le mot de passe requis pour l'authentification.

Notifications et alertes

Il existe plusieurs types de notifications d'événements que l'ADC enverra aux personnes configurées pour les recevoir. Vous pouvez cocher et activer les notifications et les alertes qui doivent être envoyées. Les notifications se produisent lorsque les serveurs réels sont contactés ou que les canaux sont démarrés. Les alertes se produisent lorsque les serveurs réels ne peuvent pas être contactés ou que les canaux cessent de fonctionner.

Avis du service IP

L'avis de service IP vous informe lorsqu'une adresse IP virtuelle est en ligne ou a cessé de fonctionner. Cette action est effectuée pour tous les services virtuels qui appartiennent au VIP.

Avis sur le service virtuel

Informe le destinataire qu'un service virtuel est en ligne ou a cessé de fonctionner.

Avis de Real Server

Lorsqu'un serveur réel et un port sont connectés ou ne sont pas joignables, l'ADC envoie une notification au serveur réel.

chemin d'accès au vol

Cet avis est un courrier électronique envoyé lorsqu'une condition est remplie et qu'une action est configurée pour demander à l'ADC d'envoyer l'événement par courrier électronique.

Notifications groupées Ensemble

Cochez cette case pour regrouper les notifications. Si cette case est cochée, toutes les notifications et alertes seront regroupées dans un seul courriel.

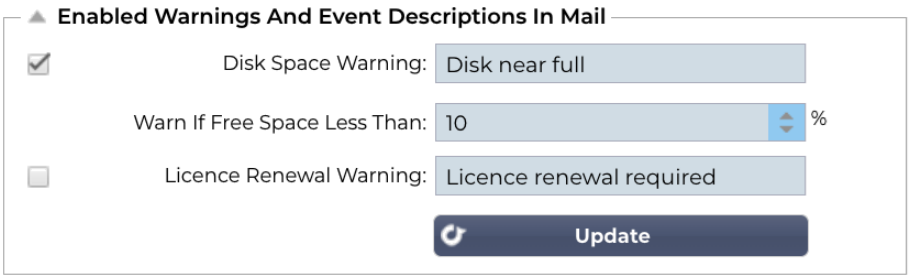
Description du courrier collectif

Spécifiez l'objet du courriel d'avis de groupe.

Intervalle d'envoi groupé

Indiquez le délai d'attente avant l'envoi d'un courriel de notification de groupe. Le délai minimum est de 2 minutes. La valeur par défaut est de 30 minutes.

Activation des avertissements et des descriptions d'événements dans le courrier électronique



Il existe deux types de messages d'avertissement, et aucun ne doit être ignoré.

Espace disque

Définissez le pourcentage d'espace disque libre avant lequel l'avertissement est envoyé. Lorsque ce pourcentage est atteint, un message électronique vous est envoyé.

Avertir si l'espace libre est inférieur à

Vous pouvez définir ici une valeur en pourcentage afin que l'ADC puisse envoyer un e-mail d'avertissement si l'espace disque passe en dessous de ce seuil.

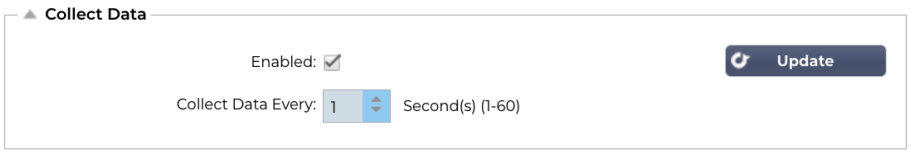
Expiration de la licence

Ce paramètre vous permet d'activer ou de désactiver l'e-mail d'avertissement d'expiration de licence envoyé à l'administrateur du système. Lorsque ce seuil est atteint, vous recevez un courriel.

L'histoire

Dans la section Système, l'option Historique du système permet de fournir des données historiques pour des éléments tels que l'unité centrale, la mémoire, les requêtes par seconde et d'autres caractéristiques. Une fois cette option activée, vous pouvez visualiser les résultats sous forme de graphiques via la page Affichage > Historique. Cette page vous permet également de sauvegarder ou de restaurer vos fichiers d'historique sur l'ADC local.

Collecte des données



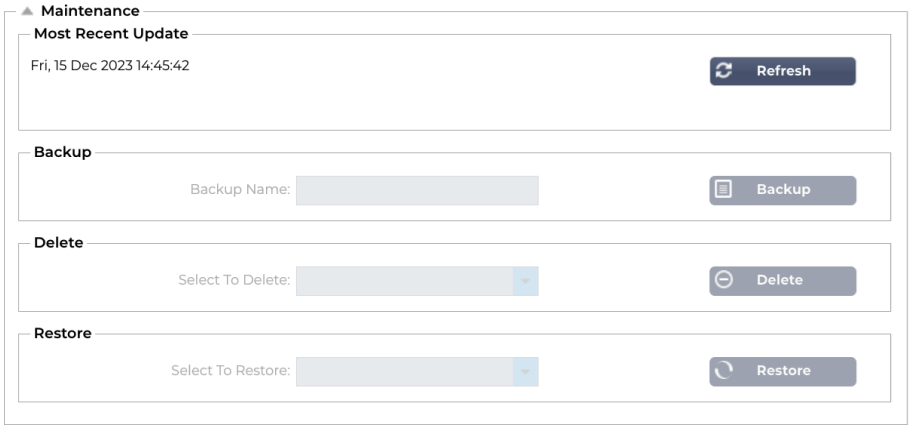
Activer

Pour permettre la collecte de données, veuillez cocher la case.

Collecter des données tous les

Ensuite, définissez l'intervalle de temps auquel vous souhaitez que l'ADC collecte les données. Cette valeur peut être comprise entre 1 et 60 secondes.

Maintenance



Dernière mise à jour

Ceci indique quand les dernières données d'historique ont été collectées à partir de l'ADC.

Cette section sera grisée si vous avez activé l'enregistrement historique. Décochez la case Activé dans la section Collecte des données et cliquez sur Mise à jour pour autoriser la maintenance des journaux historiques.

ADC basés sur HP Enterprise

Cette section de fonctionnalités n'est valable que pour les CDA installés sur des serveurs HPE ProLiant bare metal et qui utilisent ILO.

Sauvegarde

Donnez un nom descriptif à votre sauvegarde. Cliquez sur Sauvegarde pour sauvegarder tous les fichiers sur l'ADC.

Supprimer

Sélectionnez un fichier de sauvegarde dans la liste déroulante. Cliquez sur Supprimer pour supprimer le fichier de sauvegarde de l'ADC.

Restaurer

Sélectionnez un fichier de sauvegarde précédemment enregistré. Cliquez sur Restaurer pour compléter les données de ce fichier de sauvegarde.

Licence

L'ADC est autorisé à être utilisé selon l'un des modèles suivants, qui dépend des paramètres d'achat et du type de client.

Type de licence	Description
Perpétuelle	En tant que client, vous avez le droit d'utiliser l'ADC et les autres logiciels à perpétuité. Cela ne vous empêche pas d'acheter un service d'assistance pour recevoir de l'aide et des mises à jour.
SaaS	SaaS ou Software-as-a-Service (logiciel en tant que service) signifie que vous louez essentiellement le logiciel sur une base continue ou de paiement à l'utilisation. Dans ce modèle, vous payez un loyer annuel pour le logiciel. Vous ne disposez pas de droits perpétuels d'utilisation du logiciel.
MSP	Les fournisseurs de services gérés peuvent proposer l'ADC en tant que service et acheter la licence par VIP, facturée et payée annuellement.

Détails de la licence

Chaque licence comporte des détails spécifiques concernant la personne ou l'organisation qui l'achète.

ID de la licence

L'identifiant de licence est directement lié à l'identifiant de machine et à d'autres détails spécifiques à votre achat et à votre appareil ADC. Ces informations sont essentielles et sont requises lorsque vous souhaitez récupérer des mises à jour et d'autres éléments de l'App Store.

ID de la machine

L'identifiant de la machine est généré à partir de l'adresse IP eth0 de l'appliance ADC. Si vous changez l'adresse IP de l'appliance ADC, la licence ne sera plus valide. Vous devrez contacter le support pour obtenir de l'aide. Nous recommandons que votre ou vos appliances ADC aient des adresses IP fixes et que votre personnel informatique reçoive l'instruction de ne pas les modifier. Le support technique est disponible en créant un ticket à l'adresse https://www.edgenexus.io/support.

Remarque : vous ne devez pas modifier l'adresse IP de vos appareils ADC. Si vous êtes dans un environnement virtualisé, fixez le MAC ID et utilisez une adresse IP statique.

Délivré à

Cette valeur contient le nom de l'acheteur associé à l'ID machine de l'ADC.

Personne de contact

Cette valeur contient la personne à contacter dans l'entreprise du client associée à l'identifiant de la machine.

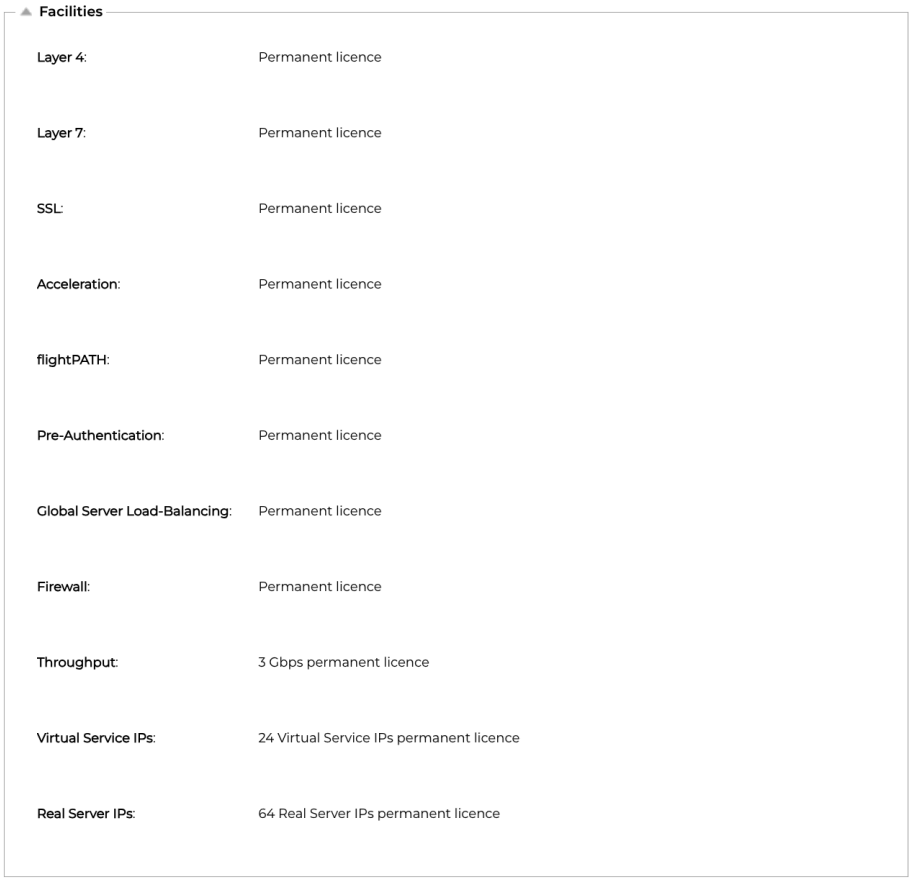
Date Émission d

La date à laquelle la licence a été délivrée.

Nom

Cette valeur indique le nom descriptif de l'appareil ADC que vous avez fourni dans Système > Mise en réseau.

Installations



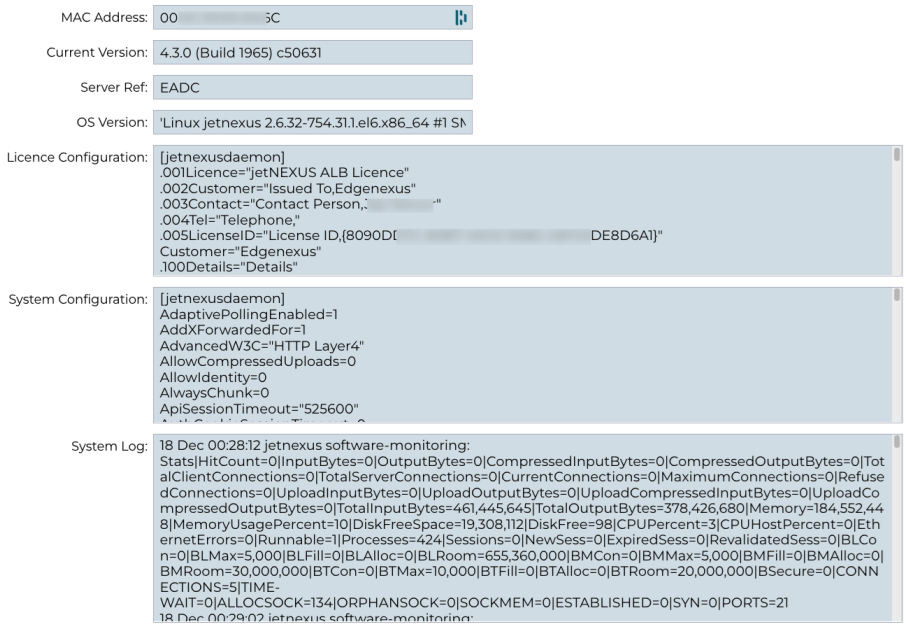
La section des installations vous fournit des informations sur les fonctions de l'ADC qui ont fait l'objet d'une licence d'utilisation et sur la validité de la licence. Le débit autorisé pour l'ADC et le nombre de serveurs réels sont également affichés. Ces informations dépendent de la licence que vous avez achetée.

Installer les licences e

- L'installation d'une nouvelle licence est très simple. Lorsque vous recevez votre nouvelle licence ou votre licence de remplacement d'Edgenexus, elle vous est envoyée sous la forme d'un fichier texte. Vous pouvez ouvrir le fichier et ensuite copier et coller le contenu dans le champ "Coller la licence".
- Vous pouvez également le télécharger vers le CDA si le copier/coller n'est pas une option pour vous.
- Une fois que vous avez fait cela, veuillez cliquer sur le bouton de mise à jour.
- La licence est maintenant installée.

Informations sur le service des licences

En cliquant sur le bouton Informations sur le service de la licence, toutes les informations relatives à la licence s'affichent. Cette fonction peut être utilisée pour envoyer les détails au personnel d'assistance.

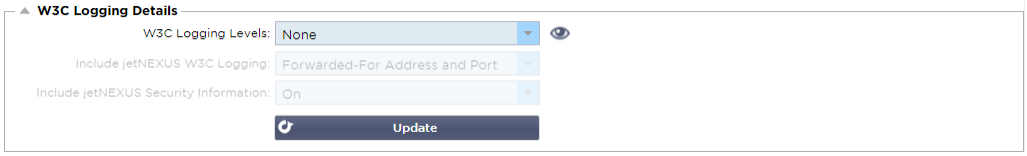


Enregistrement

La page Système > Journalisation permet de définir les niveaux de journalisation du W3C et de spécifier le serveur distant vers lequel les journaux seront automatiquement exportés. La page est organisée selon les quatre sections ci-dessous.

Détails de l'enregistrement du W3C

L'activation de la journalisation W3C permet à l'ADC de commencer à enregistrer un fichier journal compatible avec le W3C. Un journal W3C est un journal d'accès pour les serveurs Web dans lequel sont générés des fichiers texte contenant des données sur chaque demande d'accès, notamment l'adresse IP (Internet Protocol) source, la version HTTP, le type de navigateur, la page de référence et l'horodatage. Le format a été développé par le World Wide Web Consortium (W3C), une organisation qui promeut des normes pour l'évolution du Web. Le fichier est un texte ASCII dont les colonnes sont délimitées par des espaces. Le fichier contient des lignes de commentaires commençant par le caractère #. L'une de ces lignes de commentaire est une ligne indiquant les champs (en fournissant des noms de colonnes) afin que les données puissent être extraites. Il existe des fichiers distincts pour les protocoles HTTP et FTP.



Niveaux de journalisation du W3C

Il existe différents niveaux de journalisation et les données fournies varient en fonction du type de service.

Le tableau ci-dessus décrit les niveaux de journalisation pour W3C HTTP.

Valeur	Description
Aucun	La journalisation du W3C est désactivée.
Brève	Les champs présents sont les suivants : #Fields : time c-ip c-port s-ip method uri x-c-version x-r-version sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x- round-trip-time cs(User-Agent) x-sc(Content-Type).
Complet	Il s'agit d'un format plus compatible avec les processeurs, avec des champs séparés pour la date et l'heure. Voir le résumé des champs ci-dessous pour plus d'informations sur la signification des champs. Les champs présents sont les suivants : #Fields : date time c-ip c-port cs-username s-ip s-port cs-method cs-uri-stem cs-ur- -query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-roun-trip-time x-sc(Content-Type).
Site	Ce format est très similaire au format "complet", mais il comporte un champ supplémentaire. Voir le résumé des champs ci-dessous pour plus d'informations sur la signification des champs. Les champs présents sont les suivants : #Fields : date time x-mil c-ip c-port cs-username s-ip s-port cs-host cs-method cs-uri-stem cs-ur--query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round--trip-time x-sc(Content-Type).
Diagnostic	Ce format contient toutes sortes d'informations pertinentes pour le personnel de développement et de soutien. Voir le résumé des champs ci-dessous pour plus d'informations sur la signification des champs. Les champs présents sont : #Champs : date heure c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-host x-r-ip x-r-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent) referer x-c-version x-r-version cs-bytes sr-bytes rs-bytes sc-bytes x-percent time-taken x-round-trip-time x-trip-times(new,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-closed-by x- compress-action x-sc(Content-Type) x-cache-action X-finish

Le tableau ci-dessous décrit les niveaux de journalisation pour W3C FTP.

Valeur	Description
Brève	#Champs : date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param sc-status sc-param sr-method sr-param rs-status rs-param
Complet	#Champs : date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
Diagnostic	#Champs : date time c-ip c-port s-ip s-port r-ip r-port cs-method cs-param cs-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Inclure la journalisation du W3C

Cette option vous permet de définir les informations relatives à l'ADC qui doivent être incluses dans les journaux du W3C.

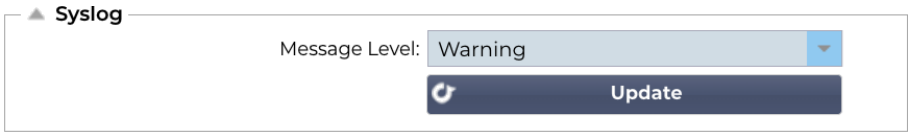
Valeur	Description
Adresse et port du réseau du client	La valeur indiquée ici affiche l'adresse IP réelle du client ainsi que le port.
Adresse du réseau du client	Cette option permet d'inclure et d'afficher uniquement l'adresse IP réelle du client.
Adresse et port du destinataire	Cette option affiche les détails contenus dans l'en-tête XFF, y compris l'adresse et le port.
Adresse du destinataire	Cette option permet d'afficher les détails contenus dans l'en-tête XFF, y compris l'adresse uniquement.

Inclure des informations sur la sécurité

Ce menu se compose de deux options :

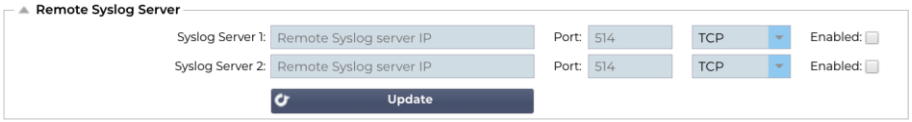
Valeur	Description
Sur	Ce paramètre est global. Lorsqu'il est activé, le nom d'utilisateur est ajouté au journal W3C lorsqu'un service virtuel utilise l'authentification et que la journalisation W3C est activée.
Arrêt	Cela désactivera la possibilité d'enregistrer le nom d'utilisateur dans le journal du W3C à un niveau global.

Serveur Syslog



Cette section permet de définir le niveau d'enregistrement des messages sur le serveur SYSLOG. Les options disponibles sont les suivantes.

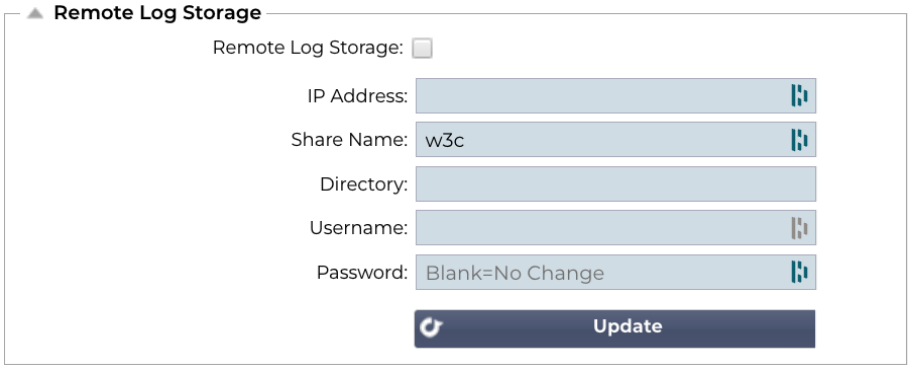
Serveur Syslog distant



Dans cette section, vous pouvez configurer deux serveurs Syslog externes pour envoyer tous les journaux du système.

- Ajouter l'adresse IP de votre serveur Syslog
- Ajouter le port
- Choisissez si vous souhaitez utiliser TCP ou UDP
- Cochez la case Activé pour commencer l'enregistrement.
- Cliquez sur Mise à jour

Stockage à distance des journaux



Tous les journaux du W3C sont stockés sous forme compressée sur l'ADC toutes les heures. Les fichiers les plus anciens sont supprimés lorsqu'il ne reste plus que 30 % d'espace disque. Si vous souhaitez les exporter vers un serveur distant pour les conserver, vous pouvez le faire en utilisant un partage SMB. Veuillez noter que le journal du W3C ne sera pas transféré vers l'emplacement distant tant que le fichier n'aura pas été complété et compressé. Comme les journaux sont écrits toutes les heures, cela peut prendre jusqu'à deux heures pour un appareil à machine virtuelle et cinq heures pour un appareil matériel.

Col1	**Col2**
Stockage à distance des journaux	Cochez la case pour activer le stockage des journaux à distance
Adresse IP	Indiquez l'adresse IP de votre serveur SMB. Cette adresse doit être indiquée en notation décimale pointée. Exemple : 10.1.1.23
Nom de l'action	Indiquez le nom du partage sur le serveur SMB. Exemple : w3c.
Annuaire	Indiquez le répertoire sur le serveur SMB. Exemple : /log.
Nom d'utilisateur	Spécifiez le nom d'utilisateur pour le partage SMB.
Mot de passe	Spécifier le mot de passe pour le partage SMB

Résumé du champ

Condition	**Description**
Date	Non localisé = toujours AAAA-MM-JJ (GMT/UTC)
L'heure	Non localisé = HH:MM:SS ou HH:MM:SS.ZZZ (GMT/UTC) * Note : il existe malheureusement deux formats (Site

	n'a pas de .ZZZ millisecondes)
x-mil	Format site uniquement = milliseconde de l'horodatage
c-ip	IP du client, tel qu'il peut être déduit du réseau ou de l'en-tête X-Forwarded-For
c-port	Port du client tel qu'il peut être déduit du réseau ou de l'en-tête X-Forwarded-For
cs-nom d'utilisateur	Champ de la demande du nom d'utilisateur du client
s-ip	Port d'écoute de l'ALB
s-port	L'écoute VIP de l'ALB
x-xff	Valeur de l'en-tête X-Forwarded-For
x-xffcustom	Valeur de l'en-tête de requête de type X-Forwarded-For configuré-nommé
cs-host	Nom d'hôte dans la demande
x-r-ip	Adresse IP du serveur réel utilisé
x-r-port	Port du serveur réel utilisé
cs-méthode	Méthode de requête HTTP * sauf format bref
méthode	* Seul le format court utilise ce nom pour cs-method
cs-uri-stem	Chemin de la ressource demandée * sauf format bref
cs-uri-query	Requête pour la ressource demandée * sauf format bref
uri	* Le format bref enregistre un chemin d'accès et une chaîne de requête combinés.
sc-status	Code de réponse HTTP
cs(User-Agent)	Chaîne User-Agent du navigateur (telle qu'envoyée par le client)
référent	Page de référence (telle qu'envoyée par le client)
x-c-version	Demande du client Version HTTP
x-r-version	Contenu-Réponse du serveur Version HTTP
cs-octets	Octets provenant du client, dans la demande
sr-octets	Octets transmis au Real Server, dans la requête
rs-octets	Octets du Real Server, dans la réponse
sc-octets	Octets envoyés au client dans la réponse
x-pourcentage	Pourcentage de compression * = 100 * (1 - sortie / entrée) y compris les en-têtes
temps pris	Durée de l'intervention du serveur réel (en secondes)
x-trip-times nouveau pcon	milliseconde entre la connexion et l'affichage dans la "liste des débutants". milliseconde entre la connexion et l'établissement de la connexion au serveur réel
acon	milliseconde entre la connexion et la fin de la mise en place de la connexion au Real Server
rcon	milliseconde entre la connexion et l'établissement de la connexion avec le serveur réel
rqf	milliseconde entre la connexion et la réception du premier octet de la requête du client
rql	milliseconde entre la connexion et la réception du dernier octet de la requête du client
tqf	milliseconde entre la connexion et l'envoi du premier octet de la requête au Real Server
tql	milliseconde entre la connexion et l'envoi du dernier octet de la requête au Real Server
rsf	milliseconde entre la connexion et la réception du premier octet de réponse du Real Server
rsl	milliseconde entre la connexion et la réception du dernier octet de réponse du Real Server
tsf	milliseconde entre la connexion et l'envoi du premier octet de réponse au client

tsl	milliseconde entre la connexion et l'envoi du dernier octet de réponse au client
dis	milliseconde entre la connexion et la déconnexion (des deux côtés - le dernier à se déconnecter)
journal	milliseconde de la connexion à cet enregistrement généralement suivi de (politique d'équilibrage de la charge et raisonnement)
x-round-trip-time	Durée de l'ALB en secondes
x-clos-by	Quelle action a provoqué la fermeture (ou le maintien) de la connexion ?
x-compress-action	Comment la compression a été effectuée ou empêchée
x-sc(Content-Type)	Type de contenu de la réponse
x-cache-action	Comment la mise en cache a réagi ou a été empêchée
x-finish	Déclencheur à l'origine de cette ligne de journal

Effacer les fichiers journaux

Cette fonction vous permet d'effacer les fichiers journaux de l'ADC. Vous pouvez sélectionner le type de journal que vous souhaitez supprimer dans le menu déroulant, puis cliquer sur le bouton Effacer.

Réseau

La section Réseau de la bibliothèque permet de configurer les interfaces réseau de l'ADC et leur comportement.

IMPORTANT

Gestion des interfaces réseau virtuelles dans un environnement virtuel

Lors du déploiement de machines virtuelles dans un environnement virtualisé tel que ESXi, les interfaces réseau (par exemple, eth0, eth1) sont automatiquement créées et mises en correspondance avec les adaptateurs réseau de configuration de l'hôte (par exemple, adaptateur réseau 1, adaptateur réseau 2). Cependant, ces mappages ne sont pas toujours cohérents en raison des règles du système d'exploitation qui lient les interfaces à des adresses MAC spécifiques. Cette section décrit les étapes à suivre pour gérer les interfaces réseau sur l'hôte afin d'éviter les interruptions de services lorsque l'utilisateur ne peut pas accéder à la VM.

Principales considérations

1. **Persistance de l'adresse MAC** :
    a. Le système d'exploitation attribue des noms d'interface (par exemple, eth0, eth1) sur la base de règles qui associent un nom à une adresse MAC spécifique.
    b. La suppression et la recréation d'une interface réseau VM sans réutiliser l'adresse MAC d'origine peut entraîner une configuration réseau incohérente ou non fonctionnelle.
2. **Mappages internes dans l'ADC (EdgeOS**) :
    a. Les interfaces réseau virtuelles sont automatiquement reconnues par l'ADC (Application Delivery Controller) et mappées en interne.
    b. La suppression d'une interface réseau de l'hôte de la VM peut laisser des mappages périmés dans l'ADC, ce qui peut perturber l'accès à la gestion ou les services réseau.

Étapes recommandées pour la configuration de l'hôte

1. **Avant de retirer une carte d'interface réseau** :
    a. Enregistrez l'adresse MAC de l'interface que vous avez l'intention de supprimer. Cette adresse peut être consultée dans les paramètres de la VM dans l'hôte ESXi.
2. **Lors de l'ajout d'un NIC de remplacement** :
    a. Attribuez l'adresse MAC précédemment enregistrée à la nouvelle carte réseau afin de garantir la cohérence des mappages d'interface de la VM.
3. **Empêcher la suppression accidentelle des NIC critiques** :
    a. Identifiez les cartes réseau qui sont mappées sur des interfaces ADC critiques (par exemple, ETH0 (Greenside) pour l'accès à la gestion). Évitez de supprimer ces cartes à moins que cela ne soit absolument nécessaire.
4. **Vérifier la cohérence des adresses MAC** :
    a. Assurez-vous que les adresses MAC attribuées aux interfaces réseau de la VM correspondent à la configuration attendue dans l'ADC. Utilisez les outils de l'hôte ESXi pour confirmer cette correspondance.
5. **Assurer la coordination avec les administrateurs VM** :
    a. Si des changements susceptibles d'affecter la configuration interne de la VM sont nécessaires, informez les administrateurs de la VM afin qu'ils se préparent à d'éventuelles perturbations et qu'ils veillent à ce que les mappages appropriés soient maintenus.

Exemple de scénario

1. **Configuration initiale** :
    a. La VM ADC possède deux cartes d'interface réseau : NIC1 (MAC : 00:11:22:33:44:55) et NIC2 (MAC : 00:11:22:33:44:66).
2. **Action** : Supprimez la carte NIC1 et ajoutez une nouvelle carte NIC (NIC3).

   a. Attribuez l'adresse MAC d'origine (00:11:22:33:44:55) à NIC3 lors de la création sur l'hôte ESXi.
3. **Évitement de l'impact** :
   a. En réutilisant l'adresse MAC d'origine, les mappages internes de l'ADC (par exemple, ETH0) restent cohérents, ce qui évite toute perturbation de l'accès à la gestion ou des services de réseau.

Lors de la gestion des interfaces réseau dans un environnement virtualisé, il est essentiel de maintenir la cohérence des attributions d'adresses MAC. Si l'accès à la VM n'est pas disponible, toutes les mesures nécessaires doivent être prises du côté de l'hôte pour garantir un fonctionnement sans faille et éviter les interruptions de service. Il faut toujours se coordonner avec les administrateurs concernés pour traiter efficacement les impacts potentiels.

Éviter les vMotions fréquentes pour les appareils critiques

vMotion est une fonctionnalité puissante de VMware qui permet la migration en direct des machines virtuelles (VM) entre les hôtes ESXi sans temps d'arrêt. Cependant, bien que vMotion soit très utile pour maintenir la flexibilité et la disponibilité de l'infrastructure, il n'est pas recommandé de migrer fréquemment des appareils critiques, tels que les équilibreurs de charge, en particulier lorsqu'ils gèrent activement un volume élevé de connexions.

Il peut exister d'autres technologies similaires fournies par d'autres fournisseurs, mais pour cette section, nous partirons du principe qu'il s'agit de VMware.

Pourquoi il n'est pas recommandé d'effectuer des vMotions fréquentes

1. **Perturbations de la session** :
   a. Les équilibreurs de charge gèrent les sessions actives entre les clients et les serveurs dorsaux. Lors d'une opération de vMotion, l'état du réseau est réinitialisé pendant une brève période, ce qui peut perturber ces sessions.
   b. La perturbation peut entraîner des interruptions de connexion, obligeant les clients à rétablir leur session, ce qui peut nuire à l'expérience de l'utilisateur.
2. **Latence et perte de paquets** :
   a. Le processus de migration d'une VM implique la mise en pause temporaire et la synchronisation de sa mémoire et de son état. Pour les appareils gérant un trafic en temps réel, cette pause peut entraîner une latence, voire une perte de paquets.
   b. Les applications qui dépendent de réponses à faible latence peuvent subir une dégradation des performances ou des dépassements de délai.
3. **Augmentation de l'utilisation des ressources** :
   a. vMotion nécessite des ressources en CPU, mémoire et bande passante réseau pour la synchronisation des données entre les hôtes source et destination.
   b. Les migrations fréquentes peuvent solliciter les ressources de l'infrastructure et avoir un impact potentiel sur les autres machines virtuelles et les services hébergés dans le même environnement.
4. **Impact sur les configurations de haute disponibilité** :
   a. Dans les environnements avec des configurations de haute disponibilité (HA), les vMotion fréquents peuvent entrer en conflit avec les mécanismes de basculement, entraînant un comportement inattendu ou des retards dans les actions de basculement.
5. **Complexité opérationnelle** :
   a. Le déplacement constant des machines virtuelles critiques accroît la complexité des configurations réseau, y compris les mappages VLAN et les règles de pare-feu, ce qui peut entraîner des erreurs de configuration.

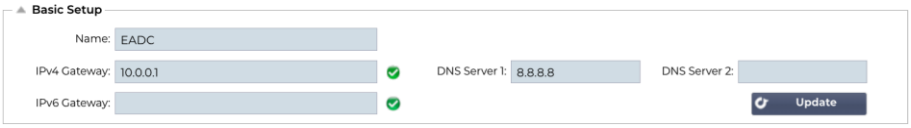
Recommandations pour la gestion des appareils critiques

1. **Planifier les opérations de vMotion pendant les fenêtres de maintenance** :
   a. Planifiez les migrations pendant les périodes de faible trafic afin de minimiser l'impact sur les sessions actives.
2. **Mise en place d'un clustering d'équilibreurs de charge** :

   a. Utilisez des configurations de clustering ou de haute disponibilité pour les équilibreurs de charge afin de garantir la redondance. Cela permet de rediriger le trafic de manière transparente vers un autre nœud lors des opérations de vMotion.
3. **Contrôler les ressources de l'infrastructure** :
   a. Assurez-vous que l'unité centrale, la mémoire et la bande passante du réseau sont disponibles en quantité suffisante avant d'initier le vMotion afin d'éviter la contention des ressources.
4. **Réduire la fréquence des migrations** :
   a. Limiter le vMotion des appliances critiques aux scénarios où il est absolument nécessaire, comme la maintenance des hôtes ou la reprise sur panne.
5. **Test avant production** :
   a. Tester les opérations de vMotion dans un environnement d'essai pour comprendre leur impact sur les sessions actives et s'assurer que les configurations sont optimisées.

Si vMotion est un outil précieux pour la gestion des machines virtuelles, il doit être utilisé à bon escient pour les équipements critiques tels que les répartiteurs de charge. Des migrations fréquentes peuvent perturber les services, augmenter la latence et solliciter les ressources. En planifiant soigneusement les opérations de vMotion et en employant des stratégies telles que le clustering et la planification de la maintenance, vous pouvez garantir une prestation de services fiable et minimiser le risque d'interruptions.

Configuration de base



Nom de l'ALB

Spécifiez un nom pour votre appliance ADC. Veuillez noter que ce nom ne peut pas être modifié s'il y a plus d'un membre dans le cluster. Veuillez consulter la section sur le clustering.

Passerelle IPv4

Spécifiez l'adresse de la passerelle IPv4. Cette adresse doit se trouver dans le même sous-réseau qu'un adaptateur existant. Si vous ajoutez une passerelle incorrecte, vous verrez une croix blanche dans un cercle rouge. Si vous ajoutez une passerelle correcte, vous verrez une bannière verte de réussite en bas de la page et une coche blanche dans un cercle vert à côté de l'adresse IP.

Passerelle IPv6

Spécifiez l'adresse de la passerelle IPv6. Cette adresse doit se trouver dans le même sous-réseau qu'un adaptateur existant. Si vous ajoutez une passerelle incorrecte, vous verrez une croix blanche dans un cercle rouge. Si vous ajoutez une passerelle correcte, vous verrez une bannière verte de réussite en bas de la page et une coche blanche dans un cercle vert à côté de l'adresse IP.

Serveur DNS 1 & Serveur DNS 2

Ajoutez l'adresse IPv4 de votre premier et de votre deuxième serveur DNS (facultatif).

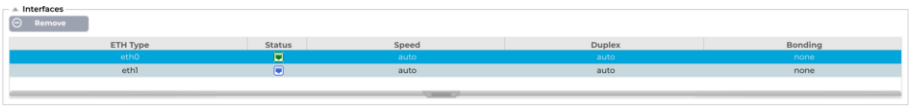
Détails de l'adaptateur

Cette section du panneau Réseau montre les interfaces réseau qui sont installées dans votre appliance ADC. Vous pouvez ajouter et supprimer des adaptateurs selon vos besoins.

Colonne	**Description**
Adaptateur	Cette colonne affiche les adaptateurs physiques installés sur votre appliance. Choisissez un adaptateur dans la liste des adaptateurs disponibles en cliquant dessus - un double-clic placera la ligne de liste en mode édition.
VLAN	Double-cliquez pour ajouter l'ID VLAN de l'adaptateur. Un VLAN est un réseau local virtuel qui crée un domaine de diffusion distinct. Un VLAN a les mêmes attributs qu'un réseau local physique, mais il permet de regrouper plus facilement les stations finales qui ne se trouvent pas sur le même commutateur réseau.
Adresse IP	Double-cliquez pour ajouter l'adresse IP associée à l'interface de l'adaptateur. Vous pouvez ajouter plusieurs adresses IP à la même interface. Il doit s'agir d'un nombre IPv4 de 32 bits en notation décimale pointée. Exemple 192.168.101.2
Masque de sous-réseau	Double-cliquez pour ajouter le masque de sous-réseau attribué à l'interface de l'adaptateur. Il doit s'agir d'un nombre IPv4 de 32 bits en notation décimale pointée. Exemple 255.255.255.0
Passerelle	Ajouter une passerelle pour l'interface. Lorsque cette passerelle est ajoutée, le CDA met en place une politique simple qui permet aux connexions initiées à partir de cette interface d'être renvoyées via cette interface vers le routeur de la passerelle spécifiée. Cela permet à l'ADC d'être installé dans des environnements réseau plus complexes sans avoir à configurer manuellement un routage complexe basé sur une politique.
Description	Double-cliquez pour ajouter une description de votre adaptateur. Exemple d'interface publique. Note : L'ADC nomme automatiquement la première interface côté vert, la deuxième interface côté rouge et la troisième interface côté 3, etc. N'hésitez pas à modifier ces conventions de dénomination à votre guise.
Console Web	Double-cliquez sur la colonne, puis cochez la case pour attribuer l'interface comme adresse de gestion pour la console Web de l'interface utilisateur graphique. Soyez très prudent lorsque vous modifiez l'interface sur laquelle la console Web écoutera. Vous devrez disposer du routage correct ou être dans le même sous-réseau que la nouvelle interface afin d'atteindre la console Web après la modification. La seule façon de revenir en arrière est d'accéder à la ligne de commande et de lancer la commande set greenside. Cette commande supprimera toutes les interfaces à l'exception de eth0.

Interfaces

La section Interfaces du panneau Réseau permet de configurer certains éléments relatifs à l'interface réseau. Vous pouvez également supprimer une interface réseau de la liste en cliquant sur le bouton Supprimer. Lorsque vous utilisez une appliance virtuelle, les interfaces que vous voyez ici sont limitées par le cadre de virtualisation sous-jacent.



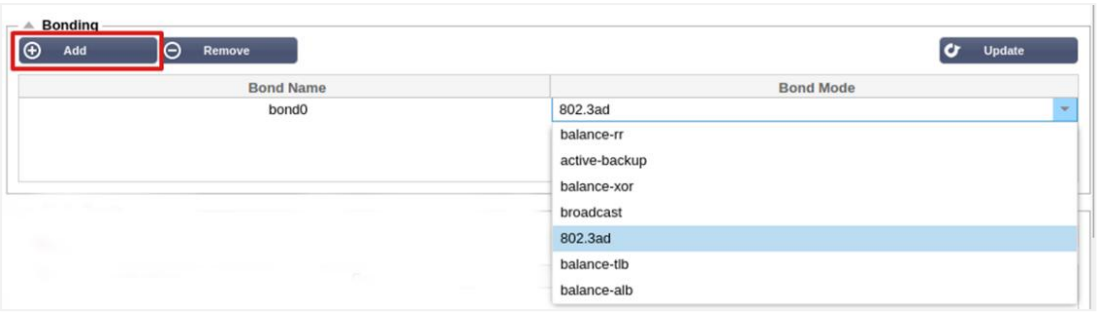
Colonne	Description
Type d'EPF	Cette valeur indique la référence interne du système d'exploitation à l'interface réseau. Ce champ ne peut pas être personnalisé. Les valeurs commencent par ETH0 et se poursuivent dans l'ordre en fonction du nombre d'interfaces réseau.
Statut	Cette indication graphique montre l'état actuel de l'interface réseau. Un état vert indique que l'interface est connectée et en service. D'autres indicateurs d'état sont présentés ci-dessous.  **Adaptateur UP**  Adaptateur vers le bas  Adaptateur débranché  Adaptateur manquant
Vitesse	Par défaut, cette valeur est réglée sur la négociation automatique de la vitesse. Mais vous pouvez changer la vitesse réseau de l'interface pour toute valeur disponible dans le menu déroulant (10/100/1000/AUTO).
Duplex	La valeur de ce champ est personnalisable et vous pouvez choisir entre Auto (par défaut), Full-Duplex et Half-Duplex.
Collage	Vous pouvez choisir l'un des types de liaison que vous avez définis. Voir la section sur le collage pour plus de détails.

Collage

De nombreux noms sont utilisés pour désigner la liaison des interfaces réseau : Port Trunking, Channel Bonding, Link Aggregation, NIC teaming, etc. Le bonding combine ou agrège plusieurs connexions réseau en une interface bondée à canal unique. Le bonding permet à deux interfaces réseau ou plus d'agir comme une seule, d'augmenter le débit et d'assurer la redondance ou le basculement.

Le noyau de l'ADC dispose d'un pilote Bonding intégré permettant d'agréger plusieurs interfaces réseau physiques en une seule interface logique (par exemple, agréger eth0 et eth1 en bond0). Pour chaque interface bondée, vous pouvez définir le mode et les options de surveillance des liens. Il existe sept options de mode différentes, chacune offrant des caractéristiques spécifiques d'équilibrage de la charge et de tolérance aux pannes. Elles sont illustrées dans l'image ci-dessous.

Remarque : la liaison ne peut être configurée que pour les appareils ADC matériels.

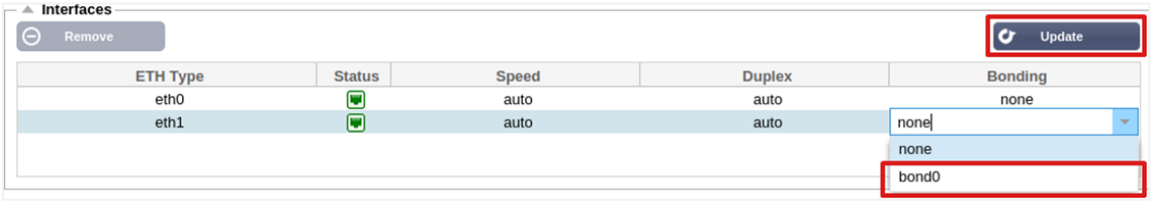


Création d'un profil de cautionnement

- Cliquez sur le bouton Ajouter pour ajouter une nouvelle obligation
- Fournir un nom pour la configuration du bonding
- Choisissez le mode de collage que vous souhaitez utiliser

Ensuite, dans la section Interfaces, sélectionnez le mode de liaison que vous souhaitez utiliser dans le champ déroulant Liaison pour l'interface réseau.

Dans l'exemple ci-dessous, eth0, eth1 et eth2 font désormais partie de bond0. Eth0 reste quant à lui l'interface de gestion.

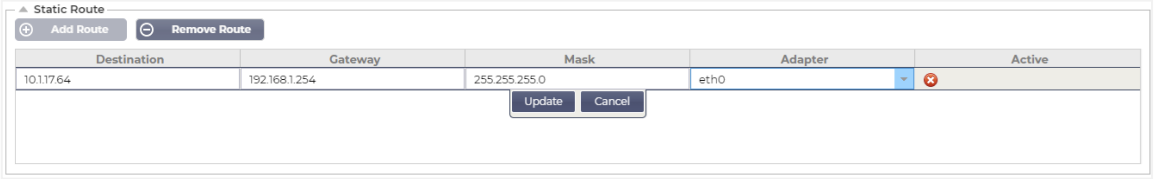


Modes de liaison

Mode de liaison	Description
équilibre-rr :	Les paquets sont transmis/reçus séquentiellement par chaque interface, un par un.
sauvegarde active :	Dans ce mode, une interface est active et la seconde est en attente. Cette interface secondaire ne devient active que si la connexion active de la première interface échoue.
balance-xor :	Transmet en fonction de l'adresse MAC source XOR's avec l'adresse MAC de destination. Cette option sélectionne le même esclave pour chaque adresse MAC de destination.
diffusion :	Ce mode transmet toutes les données sur toutes les interfaces esclaves.
802.3ad :	Crée des groupes d'agrégation qui partagent les mêmes paramètres de vitesse et de duplex et utilise tous les esclaves de l'agrégateur actif conformément à la spécification 802.3ad.
balance-tlb :	Mode de liaison par équilibrage adaptatif de la charge de transmission : Fournit une liaison de canal qui ne nécessite pas de support spécial de la part du commutateur. Le trafic sortant est distribué en fonction de la charge actuelle (calculée par rapport à la vitesse) sur chaque esclave. L'esclave actuel reçoit le trafic entrant. Si l'esclave récepteur tombe en panne, un autre esclave prend en charge l'adresse MAC de l'esclave récepteur en panne.
équilibre-alb :	Le mode de liaison Adaptive load balancing : comprend également balance-tlb plus receive load balancing (rlb) pour le trafic IPV4 et ne nécessite pas de support spécial de la part du commutateur. L'équilibrage de la charge en réception est réalisé par négociation ARP. Le pilote de liaison intercepte les réponses ARP envoyées par le système local et remplace l'adresse matérielle source par l'adresse matérielle unique de l'un des esclaves de la liaison, de sorte que les différents pairs utilisent des adresses matérielles différentes pour le serveur.

Route statique

Il peut arriver que vous ayez besoin de créer des routes statiques pour des sous-réseaux spécifiques de votre réseau. L'ADC vous offre la possibilité de le faire en utilisant le module Routes statiques.



Ajout d'une route statique

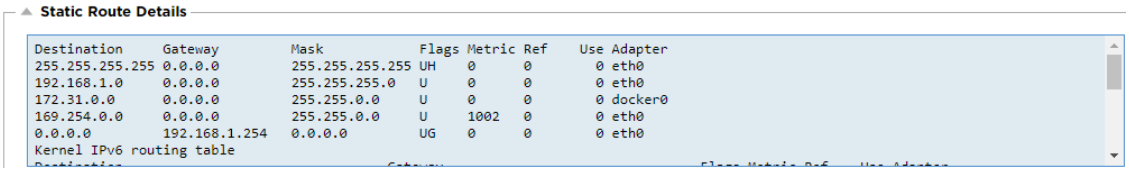
- Cliquez sur le bouton Ajouter un itinéraire
- Remplissez le champ en vous aidant des informations figurant dans le tableau ci-dessous.

- Cliquez sur le bouton "Mise à jour" lorsque vous avez terminé.

Champ d'application	Description
Destination	Entrez l'adresse du réseau de destination en notation décimale pointée. Exemple 123.123.123.5
Passerelle	Entrez l'adresse IPv4 de la passerelle en notation décimale pointée. Exemple 10.4.8.1
Masque	Saisissez le masque de sous-réseau de destination en notation décimale pointée. Exemple 255.255.255.0
Adaptateur	Entrez l'adaptateur sur lequel la passerelle peut être atteinte. Exemple eth1.
Actif	Une case à cocher verte indique que la passerelle est accessible. Une croix rouge indique que la passerelle n'est pas accessible sur cette interface. Assurez-vous d'avoir configuré une interface et une adresse IP sur le même réseau que la passerelle.

Détails de la route statique

Cette section fournit des informations sur toutes les routes configurées sur l'ADC.



Paramètres réseau avancés

Qu'est-ce que Nagle ?

L'algorithme de Nagle, également connu sous le nom d'algorithme TCP No Delay, est une technique utilisée dans la communication en réseau pour réduire le nombre de paquets retransmis en raison de données non ordonnées. Il retarde l'envoi de petits paquets si aucun accusé de réception n'a été reçu pour les paquets précédents. Cela permet de s'assurer que les données arrivent dans le bon ordre et de réduire la charge sur le réseau.

Voir l'ARTICLE DE WIKIPEDIA SUR NAGLE

Serveur Nagle

Cochez cette case pour activer le paramètre Server Nagle. Le Server Nagle est un moyen d'améliorer l'efficacité des réseaux TCP/IP en réduisant le nombre de paquets qui doivent être envoyés sur le réseau. Ce paramètre s'applique au côté serveur de la transaction. Il convient d'être prudent avec les paramètres du serveur, car le Nagle et l'ACK retardé peuvent avoir un impact important sur les performances.

Client Nagle

Cochez la case pour activer le paramètre Client Nagle. Comme ci-dessus, mais appliqué au côté client de la transaction.

SNAT

SNAT est l'abréviation de Source Network Address Translation (traduction d'adresse de réseau source), et les différents fournisseurs ont de légères variations dans la mise en œuvre de SNAT. Une explication simple du SNAT de l'EdgeADC serait la suivante.

Dans des circonstances normales, les demandes entrantes sont dirigées vers le VIP qui voit l'adresse IP source de la demande. Ainsi, par exemple, si un navigateur a une adresse IP de 81.71.61.51, celle-ci sera visible par le VIP.

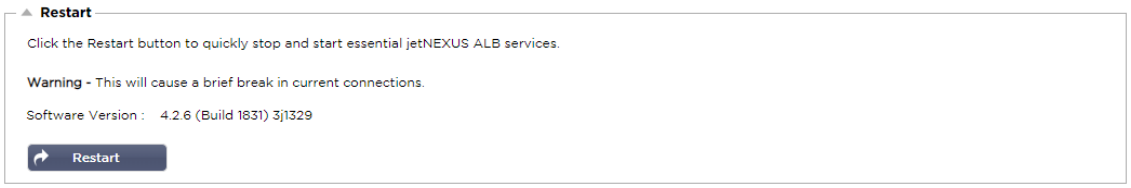
Lorsque la règle SNAT est en vigueur, l'adresse IP source originale de la requête est cachée au VIP, qui voit à la place l'adresse IP fournie dans la règle SNAT. Ainsi, le SNAT peut être utilisé dans les modes d'équilibrage de charge des couches 4 et 7.

Champ d'application	**Description**
Source IP	L'adresse IP source est facultative et peut être une adresse IP réseau (avec /mask) ou une adresse IP ordinaire. Le masque peut être soit un masque de réseau, soit un simple nombre, spécifiant le nombre de 1 à gauche du masque de réseau. Ainsi, un masque de /24 équivaut à 255.255.255.0.
IP de destination	L'adresse IP de destination est facultative et peut être une adresse IP de réseau (avec /mask) ou une adresse IP ordinaire. Le masque peut être soit un masque de réseau, soit un nombre simple, spécifiant le nombre de 1 à gauche du masque de réseau. Ainsi, un masque de /24 équivaut à 255.255.255.0.
Port source	Le port source est facultatif. Il peut s'agir d'un seul chiffre, auquel cas il ne spécifie que ce port, ou il peut inclure deux points, ce qui spécifie une série de ports. Exemples : 80 ou 5900:5905.
Port de destination	Le port de destination est facultatif. Il peut s'agir d'un seul chiffre, auquel cas il ne spécifie que ce port, ou il peut inclure deux points, ce qui permet de spécifier une série de ports. Exemples : 80 ou 5900:5905.
Protocole	Vous pouvez choisir d'utiliser SNAT sur un seul protocole ou sur tous les protocoles. Nous vous suggérons d'être spécifique pour être plus précis.
SNAT vers IP	SNAT to IP est une adresse IP obligatoire ou une plage d'adresses IP. Exemples : 10.0.0.1 ou 10.0.0.1-10.0.0.3.
SNAT à Port	Le port SNAT to est facultatif. Il peut s'agir d'un seul chiffre, auquel cas il ne spécifie que ce port, ou il peut inclure un tiret, ce qui permet de spécifier une série de ports. Exemples : 80 ou 5900-5905.
Notes	Utilisez ceci pour mettre un nom amical afin de vous rappeler pourquoi les règles existent. Ceci est également utile pour le débogage dans le Syslog.

Puissance

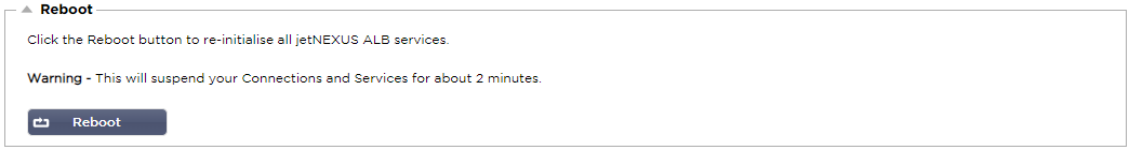
Cette fonction du système ADC vous permet également d'effectuer plusieurs tâches liées à l'alimentation sur votre ADC.

Redémarrage



Ce paramètre déclenche un redémarrage global de tous les services et interrompt par conséquent toutes les connexions actuellement actives. Tous les services reprendront automatiquement après une courte période, mais le délai dépendra du nombre de services configurés. Une fenêtre contextuelle s'affiche pour demander la confirmation de l'action de redémarrage.

Reboot



En cliquant sur le bouton Reboot, l'ADC est mis hors tension et revient automatiquement à l'état actif. Une fenêtre contextuelle s'affiche pour demander la confirmation de l'action de redémarrage.

Mise hors tension

Cliquer sur le bouton "Power Off" éteint l'ADC. S'il s'agit d'un appareil matériel, vous devrez accéder physiquement à l'appareil pour le remettre sous tension. Une fenêtre contextuelle s'affiche pour demander la confirmation de l'action d'arrêt.

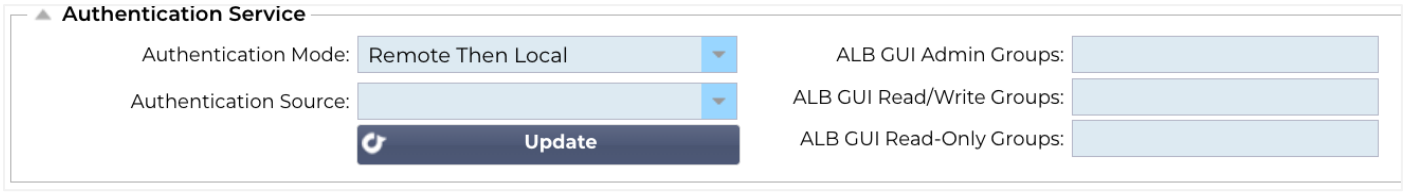
Sécurité

Cette section permet de modifier le mot de passe de la console web et d'activer ou de désactiver l'accès Secure Shell. Elle permet également d'activer la capacité de l'API REST.

SSH

Option	Description
Connexion à distance par Secure Shell	Veuillez cocher la case si vous souhaitez accéder à l'ADC en utilisant SSH. "Putty" est une excellente application pour ce faire.

Service d'authentification



Dans la plupart des organisations, l'accès à l'interface de gestion de l'ADC doit se faire via les propres services d'authentification de l'entreprise.

Pour de tels scénarios, nous avons fourni la fonction de service d'authentification décrite ici. Cette fonctionnalité fonctionne avec des services d'annuaire locaux, ainsi qu'avec des services externes tels que SAML.

Option	Description
Mode d'authentification	Local Only : Il s'agit du mode par défaut qui utilise la base de données locale de l'ADC, par exemple pour l'utilisateur admin. Distant puis Local : L'ADC tente de valider l'utilisateur par rapport au serveur d'authentification distant spécifié dans le champ Source d'authentification. En cas d'échec, il utilisera la base de données locale comme source de validation.
Source d'authentification	Ce menu déroulant vous permet de sélectionner l'un des serveurs d'authentification que vous avez définis dans Bibliothèque > Authentification.
Groupes d'administrateurs de l'interface graphique de l'ALB	Spécifiez les groupes d'administrateurs autorisés.
Groupes de lecture/écriture de l'interface graphique de l'ALB	Spécifier les groupes de lecture/écriture autorisés
GUI ALB Groupes en lecture seule	Spécifiez les groupes en lecture seule autorisés.

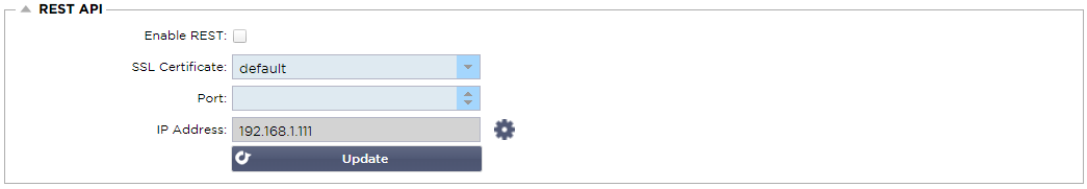
Console Web

Certificat SSL Choisissez un certificat dans la liste déroulante. Le certificat que vous choisissez sera utilisé pour sécuriser votre connexion à l'interface utilisateur web de l'ADC. Vous pouvez créer un certificat auto-signé dans le CDA ou en importer un depuis la section **CERTIFICATS SSL.**

Option	**Description**
Port sécurisé	Le port par défaut de la console web est TCP 443. Si vous souhaitez utiliser un autre port pour des raisons de sécurité, vous pouvez le modifier ici.

API REST

L'API REST, également connue sous le nom d'API RESTful, est une interface de programmation d'applications conforme au style architectural REST qui permet de configurer le CDA ou d'extraire des données du CDA. Le terme REST (representational state transfer) a été créé par l'informaticien Roy Fielding.



Option	**Description**
Activer REST	Cochez cette case pour activer l'accès via l'API REST. Notez que vous devrez également configurer l'adaptateur sur lequel REST est activé. Voir la note sur le lien Cog ci-dessous.
Certificat SSL	Choisissez un certificat pour le service REST. La liste déroulante affiche tous les certificats installés sur l'ADC.
Port	Définissez le port du service REST. Il est conseillé d'utiliser un port autre que 443.
Adresse IP	Ceci affichera l'adresse IP à laquelle le service REST est lié. Vous pouvez cliquer sur le lien Cog pour accéder à la page Réseau et modifier l'adaptateur sur lequel le service REST est activé.
Lien Cog	En cliquant sur ce lien, vous accéderez à la page Réseau où vous pourrez configurer un adaptateur pour le REST.

Documentation pour l'API REST

La documentation sur l'utilisation de l'API REST est disponible : **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Remarque : si vous obtenez des erreurs sur la page Swagger, c'est parce qu'ils ont un problème de prise en charge des chaînes de requête.
Passez les erreurs pour accéder à l'API REST de jetNEXUS

Exemples

GUID en utilisant CURL :

- Commandement

```
curl -k HTTPs://<rest ip>/POST/32 -H "Content-Type : application/json" -X POST -d '{"<rest username>" :"<password>"}'
```

- renverra

```
{"Loginstatus" : "OK", "Username" : "<rest username>", "GUID" : "<guid>"}.
```

- Validité
    - Le GUID est valable pendant 24 heures

Détails de la licence

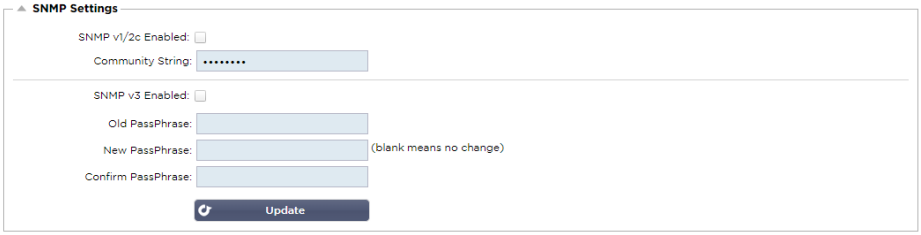
- Commandement

```
curl -k HTTPs://<rest ip>/GET/39 -GET -b 'GUID=<guid;>
```

SNMP

La section SNMP permet de configurer le MIB SNMP résidant dans l'ADC. Le MIB peut ensuite être interrogé par des logiciels tiers capables de communiquer avec des appareils équipés de SNMP.

Paramètres SNMP



Option	Description
SNMP v1 / V2C	Cochez la case pour activer la MIB V1/V2C. SNMP v1 est conforme à la RFC-1157. SNMP V2c est conforme à la RFC-1901-1908.
SNMP v3	Cochez la case pour activer la MIB V3. RFC-3411-3418. Le nom d'utilisateur pour v3 est admin. Exemple:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Chaîne communautaire	Il s'agit de la chaîne en lecture seule définie sur l'agent et utilisée par le gestionnaire pour récupérer les informations SNMP. La chaîne de communauté par défaut est jetnexus
Phrase de passe	Il s'agit du mot de passe nécessaire lorsque SNMP v3 est activé. Il doit être composé d'au moins 8 caractères et contenir uniquement les lettres Aa-Zz et les chiffres 0-9. La phrase de passe par défaut est **jetnexus.**

MIB SNMP

Les informations consultables via SNMP sont définies par la base d'informations de gestion (MIB). Les MIB décrivent la structure des données de gestion et utilisent des identificateurs d'objets hiérarchiques (OID). Chaque OID peut être lu par une application de gestion SNMP.

Téléchargement des MIB

Le MIB peut être téléchargé ici :

ADC OID

ROOT OID

```
iso.org.dod.internet.private.enterprise = .1.3.6.1.4.1
```

Nos OID

```
.38370 jetnexusMIB
      .1 jetnexusData   (1.3.6.1.4.1.38370.1)
            .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
            .2 jetnexusVirtualServices   (1.3.6.1.4.1.38370.1.2)
            .3 jetnexusServers   (1.3.6.1.4.1.38370.1.3)
                  .1 jetnexusGlobal   (1.3.6.1.4.1.38370.1.1)
                        .1 jetnexusOverallInputBytes   (1.3.6.1.4.1.38370.1.1.1.0)
                        .2 jetnexusOverallOutputBytes   (1.3.6.1.4.1.38370.1.1.2.0)
                        .3 jetnexusCompressedInputBytes   (1.3.6.1.4.1.38370.1.1.3.0)
                        .4 jetnexusCompressedOutputBytes   (1.3.6.1.4.1.38370.1.1.4.0)
                        .5 jetnexusVersionInfo   (1.3.6.1.4.1.38370.1.1.5.0)
                        .6 jetnexusTotalClientConnections   (1.3.6.1.4.1.38370.1.1.6.0)
```

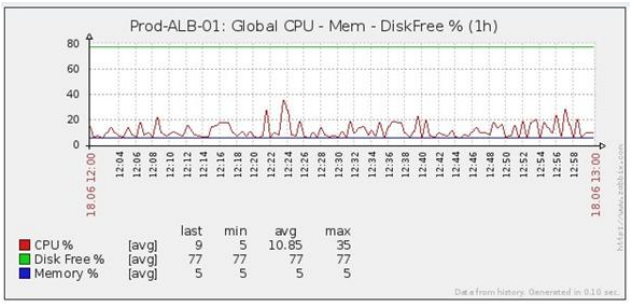
.7 **jetnexusCpuPercent** (1.3.6.1.4.1.38370.1.1.7.0)
.8 **jetnexusDiskFreePercent** (1.3.6.1.4.1.38370.1.1.8.0)
.9 **jetnexusMemoryPercent** (1.3.6.1.4.1.38370.1.1.9.0)
.10 **jetnexusCurrentConnections** (1.3.6.1.4.1.38370.1.1.10.0)

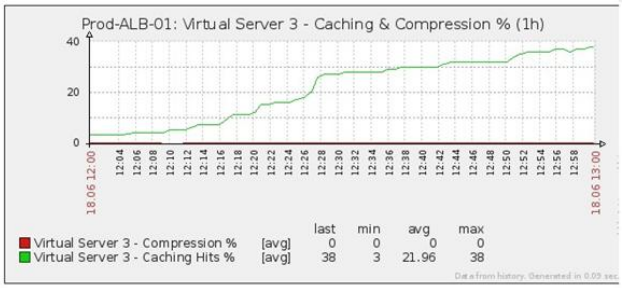
.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry** (1.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice** (1.3.6.1.4.1.38370.1.2.1.1)
.2 **jnvirtualserviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.2)
.3 **jnvirtualserviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.3)
.4 **jnvirtualserviceOverallOutputBytes** (1.3.6.1.4.1.38370.1.2.1.4)
.5 **jnvirtualserviceCacheBytes** (1.3.6.1.4.1.38370.1.2.1.5)
.6 **jnvirtualserviceCompressionPercent** (1.3.6.1.4.1.38370.1.2.1.6)
.7 **jnvirtualservicePresentClientConnections** (1.3.6.1.4.1.38370.1.2.1.7)
.8 **jnvirtualserviceHitCount** (1.3.6.1.4.1.38370.1.2.1.8)
.9 **jnvirtualserviceCacheHits** (1.3.6.1.4.1.38370.1.2.1.9)
.10 **jnvirtualserviceCacheHitsPercent** (1.3.6.1.4.1.38370.1.2.1.10)
.11 **jnvirtualserviceVSStatus** (1.3.6.1.4.1.38370.1.2.1.11)

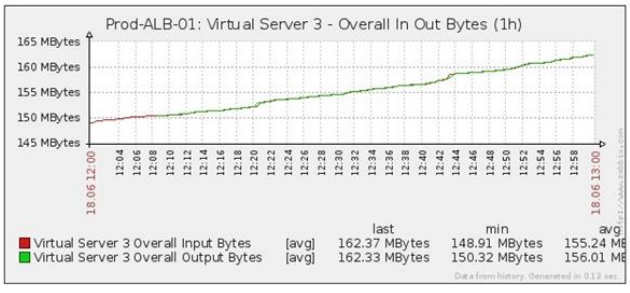
.3 **jetnexusRealServers** (1.3.6.1.4.1.38370.1.3)
.1 **jnrealserverEntry** (1.3.6.1.4.1.38370.1.3.1)
.1 **jnrealserverIndexVirtualService** (1.3.6.1.4.1.38370.1.3.1.1)
.2 **jnrealserverIndexRealServer** (1.3.6.1.4.1.38370.1.3.1.2)
.3 **jnrealserverChAddrPort** (1.3.6.1.4.1.38370.1.3.1.3)
.4 **jnrealserverCSAddrPort** (1.3.6.1.4.1.38370.1.3.1.4)
.5 **jnrealserverOverallInputBytes** (1.3.6.1.4.1.38370.1.3.1.5)
.6 **jnrealserverOverallOutputBytes** (1.3.6.1.4.1.38370.1.3.1.6)
.7 **jnrealserverCompressionPercent** (1.3.6.1.4.1.38370.1.3.1.7)
.8 **jnrealserverPresentClientConnections** (1.3.6.1.4.1.38370.1.3.1.8)
.9 **jnrealserverPoolUsage** (1.3.6.1.4.1.38370.1.3.1.9)
.10 **jnrealserverHitCount** (1.3.6.1.4.1.38370.1.3.1.10)
.11 **jnrealserverRSStatus** (1.3.6.1.4.1.38370.1.3.1.11)

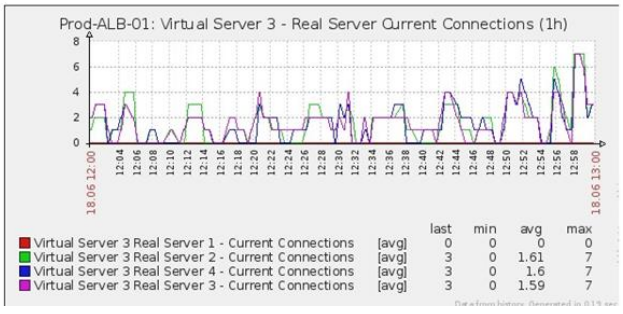
Graphique historique

La meilleure utilisation de la MIB SNMP personnalisée de l'ADC est la possibilité de décharger les graphiques historiques vers une console de gestion de votre choix. Vous trouverez ci-dessous quelques exemples de Zabbix qui interroge un ADC sur les différentes valeurs OID énumérées ci-dessus.









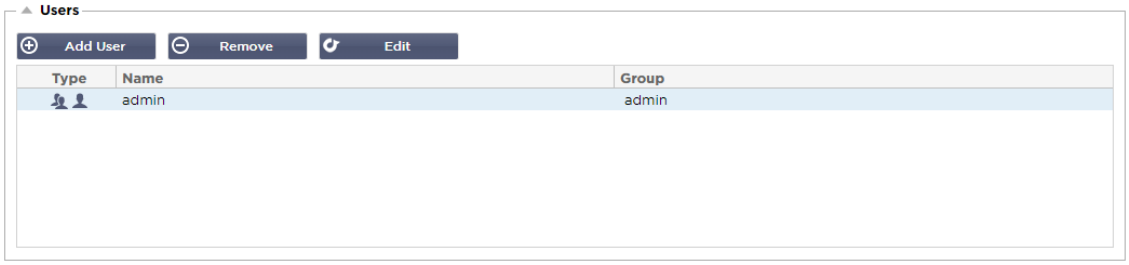
Utilisateurs et journaux d'audit

Le CDA permet d'avoir un ensemble d'utilisateurs internes pour configurer et définir ce que fait le CDA. Les utilisateurs définis dans le CDA peuvent effectuer diverses opérations en fonction du rôle qui leur est attribué.

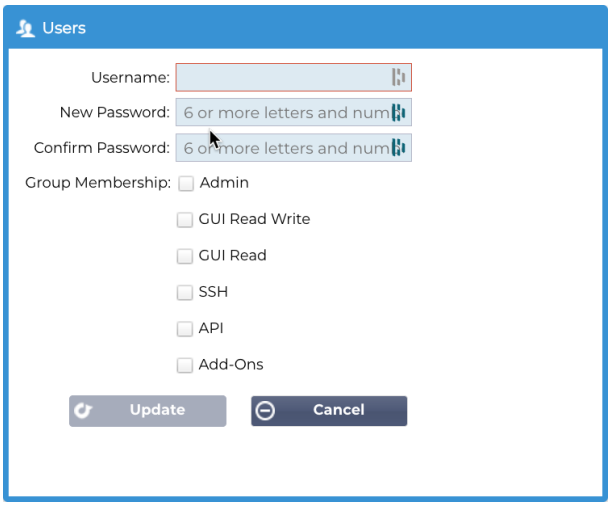
Il existe un utilisateur par défaut appelé **admin** que vous utilisez lors de la première configuration de l'ADC. Le mot de passe par défaut pour admin est **jetnexus**.

Utilisateurs

La section Utilisateurs vous permet de créer, de modifier et de supprimer des utilisateurs du CDA.



Ajouter un utilisateur



Cliquez sur le bouton Ajouter un utilisateur illustré dans l'image ci-dessus pour afficher la boîte de dialogue Ajouter un utilisateur.

Paramètres	Description/Utilisation
Nom d'utilisateur	Entrez un nom d'utilisateur de votre choix. Le nom d'utilisateur doit être conforme à ce qui suit : • Nombre minimum de caractères 1 • Nombre maximal de caractères 32 • Les lettres peuvent être majuscules ou minuscules. • Des chiffres peuvent être utilisés. • Les symboles ne sont pas autorisés
Mot de passe	Saisissez un mot de passe **fort**, conforme aux exigences ci-dessous. • Nombre minimum de caractères 6 • Nombre maximal de caractères 32 • Doit utiliser au moins une combinaison de lettres et de chiffres. • Les lettres peuvent être majuscules ou minuscules. • Les symboles sont autorisés, à l'exception de ceux figurant dans l'exemple ci-dessous **£**, **%**, &, **<** , **>**
Confirmer le mot de passe	Confirmez à nouveau le mot de passe pour vous assurer qu'il est correct
Membres du groupe	Cochez le groupe auquel vous souhaitez que l'utilisateur appartienne. • Admin - Ce groupe peut tout faire. • GUI Read Write - Les utilisateurs de ce groupe peuvent accéder au GUI et y apporter des modifications. • Lecture de l'interface graphique - Les utilisateurs de ce groupe peuvent accéder à l'interface graphique pour consulter des informations uniquement. Aucune modification ne peut être apportée. • SSH - Les utilisateurs de ce groupe peuvent accéder à l'ADC via Secure Shell. Ce choix permet d'accéder à la ligne de commande, qui dispose d'un ensemble minimal de commandes. • API - Les utilisateurs de ce groupe auront accès aux interfaces programmables SOAP et REST. REST sera disponible à partir de la version 4.2.1 du logiciel. • Add-Ons - L'autorisation est accordée pour accéder aux configurations Add-On.

Type d'utilisateur

	Utilisateur local L'ADC dans le rôle autonome ou manuel H/A ne créera que des utilisateurs locaux. Par défaut, un utilisateur local appelé "admin" est membre du groupe admin. Pour des raisons de compatibilité ascendante, cet utilisateur ne peut jamais être supprimé. Vous pouvez modifier le mot de passe de cet utilisateur ou le supprimer, mais vous ne pouvez pas supprimer le dernier administrateur local.
	Utilisateur de la grappe Le rôle ADC in Cluster permet de créer uniquement des utilisateurs de cluster. Les utilisateurs du cluster sont synchronisés sur tous les ADC du cluster. Toute modification apportée à un utilisateur de la grappe sera répercutée sur tous les membres de la grappe. Si vous êtes connecté en tant qu'utilisateur de la grappe, vous ne pourrez pas passer du rôle de grappe à celui de manuel ou d'autonome.
	Cluster et utilisateur local Tous les utilisateurs créés dans le cadre du rôle autonome ou manuel seront copiés dans le cluster. Si l'ADC quitte ensuite le cluster, seuls les utilisateurs locaux seront conservés. Le dernier mot de passe configuré pour l'utilisateur sera valide.

Suppression d'un utilisateur

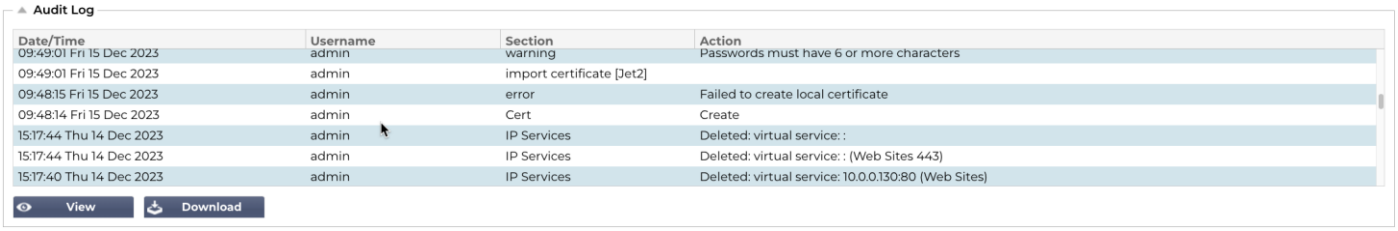
- Mettre en évidence un utilisateur existant.
- Cliquez sur Supprimer.
- Vous ne pourrez pas supprimer l'utilisateur qui est actuellement connecté.
- Vous ne pourrez pas supprimer le dernier utilisateur local du groupe d'administrateurs.
- Vous ne pourrez pas supprimer le dernier utilisateur de cluster restant dans le groupe d'administration.
- Vous ne pourrez pas supprimer l'utilisateur admin pour des raisons de compatibilité ascendante.
- Si vous supprimez l'ADC du cluster, tous les utilisateurs, à l'exception des utilisateurs locaux, seront supprimés.

Modification d'un utilisateur

- Mettez en évidence un utilisateur existant.
- Cliquez sur Modifier
- Vous pouvez modifier l'appartenance de l'utilisateur à un groupe en cochant les cases appropriées et en mettant à jour.
- Vous pouvez également modifier le mot de passe d'un utilisateur, à condition de disposer des droits d'administrateur.

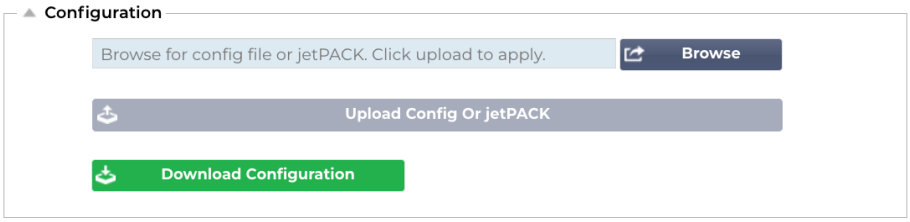
Journal d'audit

L'ADC enregistre les modifications apportées à la configuration de l'ADC par les différents utilisateurs. Le journal d'audit fournit les 50 dernières actions effectuées par tous les utilisateurs. Vous pouvez également voir TOUTES les entrées dans la section **LOGS**. Par exemple :



Avancé

Configuration



Il est toujours préférable de télécharger et de sauvegarder la configuration de l'ADC une fois qu'il est entièrement configuré et qu'il fonctionne comme il se doit. Vous pouvez utiliser le module de configuration pour télécharger une configuration.

Les Jetpacks sont des fichiers de configuration pour des applications standard et sont fournis par Edgenexus pour vous simplifier la tâche. Ils peuvent également être téléchargés vers l'ADC à l'aide du module de configuration.

Un fichier de configuration est essentiellement un fichier texte et, en tant que tel, peut être édité à l'aide d'un éditeur de texte tel que Notepad++, Nano ou VI. Une fois édité, le fichier de configuration peut être téléchargé dans l'ADC.

ATTENTION :

La modification du fichier de configuration de l'EdgeADC est réservée à des experts qualifiés. Si vous décidez de modifier vous-même le fichier de configuration et qu'un problème technique survient, l'assistance technique d'Edgenexus ne sera plus en mesure de prendre en charge le produit.

Téléchargement d'une configuration

- Pour télécharger la configuration actuelle de l'ADC, appuyez sur le bouton Download Configuration.
- Une fenêtre contextuelle s'affiche pour vous demander d'ouvrir ou d'enregistrer le fichier .conf.
- Sauvegarder dans un endroit pratique.
- Vous pouvez l'ouvrir avec n'importe quel éditeur de texte, tel que Notepad++.

Téléchargement d'une configuration

- Vous pouvez télécharger un fichier de configuration enregistré en recherchant le fichier .conf enregistré.
- Cliquez sur le bouton "Upload Config or Jetpack".
- L'ADC téléchargera et appliquera la configuration, puis rafraîchira le navigateur. Si le navigateur n'est pas actualisé automatiquement, cliquez sur l'icône d'actualisation du navigateur.
- Vous serez redirigé vers la page du tableau de bord une fois que vous aurez terminé.

Critique : Il est essentiel de ne pas tenter de copier la configuration d'un CDA vers un autre sans avoir consulté au préalable l'assistance d'Edgenexus. Cela pourrait rendre votre CDA irrécupérable.

Télécharger un JetPACK

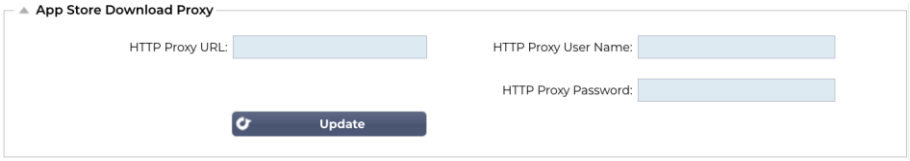
- Un JetPACK est un ensemble de mises à jour de la configuration existante.
- Un JetPACK peut être aussi simple qu'une modification de la valeur du délai d'attente TCP ou une configuration complète d'une application spécifique telle que Microsoft Exchange ou Microsoft Lync.
    - Vous pouvez obtenir un JetPACK à partir du portail d'assistance indiqué à la fin de ce guide.
- Recherchez le fichier jetPACK.txt.
- Cliquez sur télécharger.
- Le navigateur se rafraîchira automatiquement après le téléchargement.
- Vous serez redirigé vers la page du tableau de bord une fois que vous aurez terminé.

- L'importation peut prendre plus de temps pour des déploiements plus complexes tels que Microsoft Lync, etc.

Paramètres globaux

La section Paramètres globaux permet de modifier divers éléments, notamment la bibliothèque cryptographique SSL.

Proxy de téléchargement de l'App Store



Les réseaux sécurisés n'autorisent généralement pas l'accès à Internet, à moins que les données ne soient envoyées via les serveurs proxy de l'organisation. L'EdgeADC est un appareil de périmètre et doit pouvoir accéder aux serveurs d'Edgenexus afin de s'assurer de la validité de l'assistance et d'accéder à l'App Store pour télécharger des mises à jour et des applications.

URL du proxy HTTP

Ce champ est utilisé pour spécifier le nom d'hôte ou l'adresse IP de votre serveur proxy.

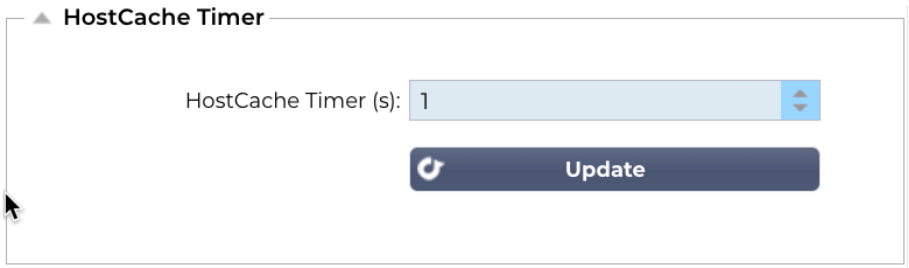
Nom d'utilisateur du proxy HTTP

Entrez le nom d'utilisateur spécifiquement utilisé pour autoriser les appareils et les utilisateurs qui utilisent le serveur proxy.

Mot de passe du proxy HTTP

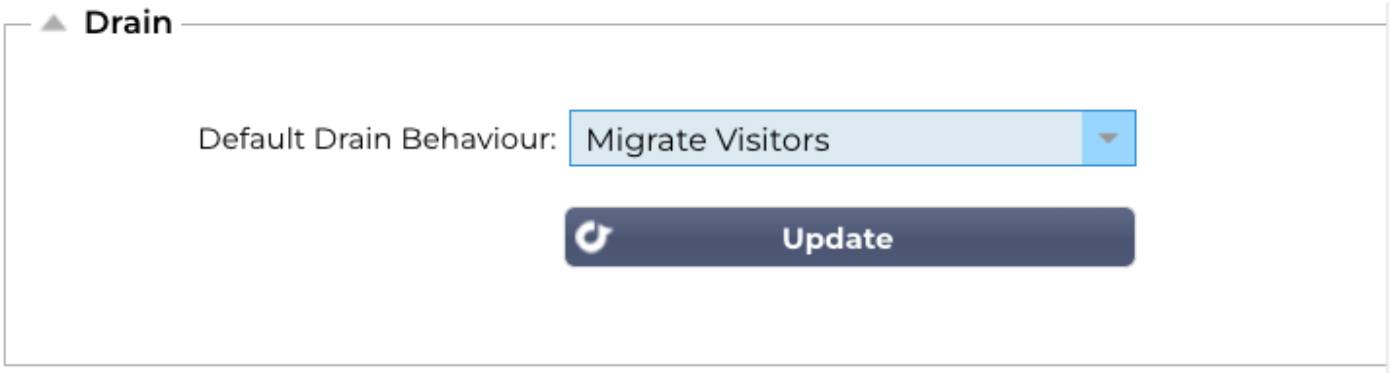
Le nom d'utilisateur spécifié dans le champ Nom d'utilisateur du proxy HTTP sera un nom sécurisé. Vous devrez saisir le mot de passe associé dans ce champ.

Temporisation du cache de l'hôte



La temporisation du cache de l'hôte est un paramètre qui stocke l'adresse IP d'un serveur réel pendant une période donnée lorsque le nom de domaine a été utilisé au lieu d'une adresse IP. Le cache est vidé en cas de défaillance d'un serveur réel. Si cette valeur est fixée à zéro, le cache ne sera pas vidé. Il n'y a pas de valeur maximale pour ce paramètre.

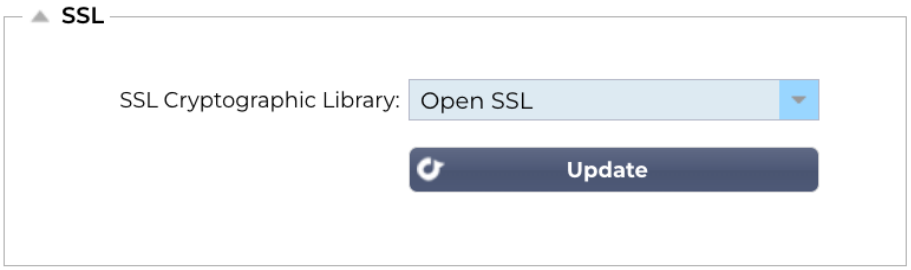
Drainage



Lorsqu'un serveur réel est placé en mode vidange, il est toujours préférable de pouvoir contrôler le comportement du trafic qui lui est envoyé. Le menu Drain Behaviour permet de sélectionner le comportement du trafic pour chaque service virtuel. Les options sont les suivantes :

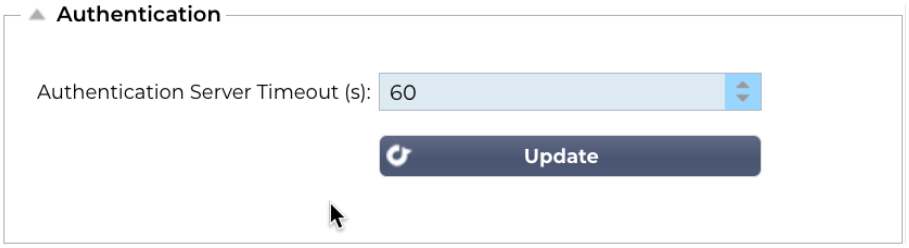
Option	Description
Axé sur la persistance	Il s'agit de la sélection par défaut. Chaque fois que l'utilisateur utilise la session de persistance, celle-ci est prolongée. En cas d'utilisation 24 heures sur 24, il est possible que la vidange ne se produise jamais. Toutefois, si le nombre de connexions au serveur réel atteint 0, le drainage s'arrête, les sessions de persistance sont supprimées et tous les visiteurs sont rééquilibrés lors de leur prochaine connexion.
Migrer les visiteurs	Session persistante ignorée lors de la reconnexion - (comportement hérité avant 2022) Les nouvelles connexions TCP (qu'elles fassent partie d'une session existante ou non) sont toujours établies avec un serveur réel en ligne. Si la session de persistance était liée à un serveur réel épuisé, elle est écrasée. Le service virtuel ignorera effectivement la persistance pour toutes les nouvelles connexions, et celles-ci seront réparties sur un nouveau serveur.
Sessions de retraite	Les sessions persistantes ne sont pas prolongées. Les connexions d'utilisateurs entrantes seront attribuées au serveur de leur choix, mais leur session de persistance n'est pas prolongée. Ainsi, une fois la durée de la session de persistance dépassée, elles seront traitées comme une nouvelle connexion et déplacées vers un autre serveur.

SSL



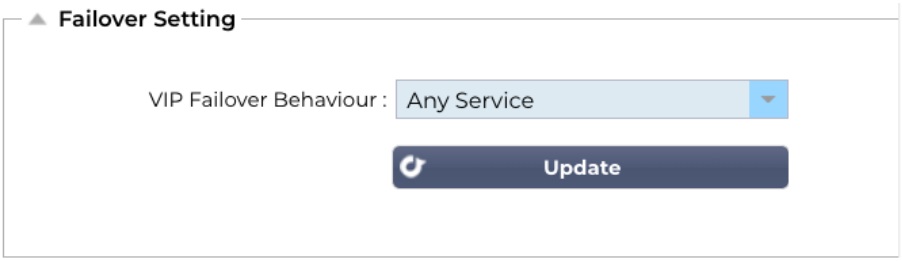
Ce paramètre global permet de modifier la bibliothèque SSL en fonction des besoins. La bibliothèque cryptographique SSL utilisée par défaut par l'ADC est OpenSSL. Si vous souhaitez utiliser une autre bibliothèque cryptographique, vous pouvez la modifier ici.

Authentification



Cette valeur définit le délai d'attente pour l'authentification, après lequel la tentative d'authentification sera considérée comme ayant échoué.

Paramètres de basculement



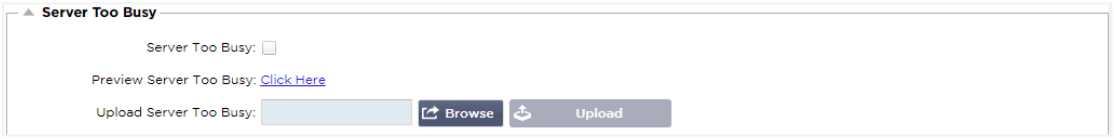
Lorsqu'un ensemble d'ADC en cluster est créé, il existe désormais deux méthodes pour spécifier comment un service virtuel sera basculé.

Option	Description
Tout service	Lorsque cette option est choisie, la défaillance d'un service au sein du VIP entraînera le basculement de l'ensemble du VIP et de ses services virtuels vers le partenaire du cluster. Par exemple, vous pouvez avoir un VIP 10.0.100.101, avec des services virtuels utilisant chacun les ports 443, 8080, 4399, 2020, etc. En cas de défaillance de l'un de ces sous-services, l'ensemble du VIP est basculé.
Tous les services	Lorsque cette option est choisie, si un ou plusieurs sous-services tombent en panne, le VIP reste sur le membre actuel du cluster. Le VIP ne basculera vers le partenaire de cluster que si **tous les** services tombent en panne. Cette option est utile lorsque vous souhaitez désactiver un service particulier, mais que vous ne souhaitez pas que le VIP soit basculé.

Protocole

La section Protocole permet de définir les nombreux paramètres avancés du protocole HTTP.

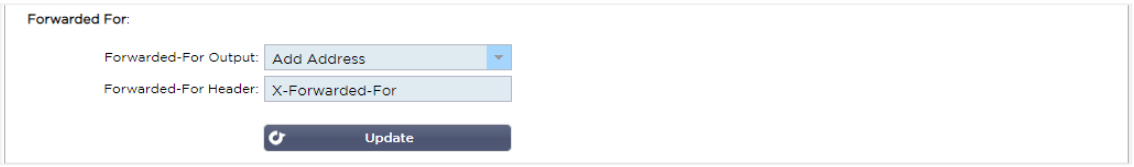
Serveur trop occupé



Supposons que vous ayez limité le nombre maximal de connexions à vos serveurs réels ; vous pouvez choisir d'afficher une page web conviviale lorsque cette limite est atteinte.

- Créez une page web simple avec votre message. Vous pouvez inclure des liens externes vers des objets situés sur d'autres serveurs et sites web. Si vous souhaitez ajouter des images à votre page web, utilisez des images codées en ligne (base64).
- Recherchez le fichier HTM(L) de la page web que vous venez de créer.
- Cliquez sur Télécharger
- Si vous souhaitez prévisualiser la page, vous pouvez le faire en cliquant sur le lien Cliquez ici.

Transmis pour



Forwarded For est la norme de facto pour identifier l'adresse IP d'origine d'un client qui se connecte à un serveur web par l'intermédiaire de répartiteurs de charge et de serveurs proxy de la couche 7.

Sortie de Forwarded-For

Option	**Description**
Arrêt	L'ADC ne modifie pas l'en-tête Forwarded-For.
Ajouter une adresse et un port	Ce choix ajoutera l'adresse IP et le port de l'appareil ou du client connecté à l'ADC à l'en-tête Forwarded-For.
Ajouter une adresse	Ce choix ajoutera l'adresse IP de l'appareil ou du client connecté à l'ADC à l'en-tête Forwarded-For.
Remplacer l'adresse et le port	Ce choix remplacera la valeur de l'en-tête Forwarded-For par l'adresse IP et le port de l'appareil ou du client connecté à l'ADC.
Remplacer l'adresse	Ce choix remplacera la valeur de l'en-tête Forwarded-For par l'adresse IP de l'appareil ou du client connecté à l'ADC.

En-tête Forwarded-For

Ce champ vous permet de spécifier le nom donné à l'en-tête Forwarded-For. Généralement, il s'agit de "X-Forwarded-For", mais ce nom peut être modifié dans certains environnements.

Journalisation avancée pour IIS - Journalisation personnalisée

Vous pouvez obtenir les informations X-Forwarded-For en installant l'application IIS Advanced logging 64-bit. Une fois téléchargée, créez un champ de journalisation personnalisé appelé X-Forwarded-For avec les paramètres ci-dessous.

Sélectionnez Default dans la liste Source Type dans la liste Category, sélectionnez Request Header dans la case Source Name et tapez X-Forwarded-For.

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

Changements dans le fichier HTTPd.conf d'Apache

Vous devrez apporter plusieurs modifications au format par défaut afin d'enregistrer l'adresse IP du client X-Forwarded-For ou l'adresse IP réelle du client si l'en-tête X-Forwarded-For n'existe pas.

Ces changements sont présentés ci-dessous :

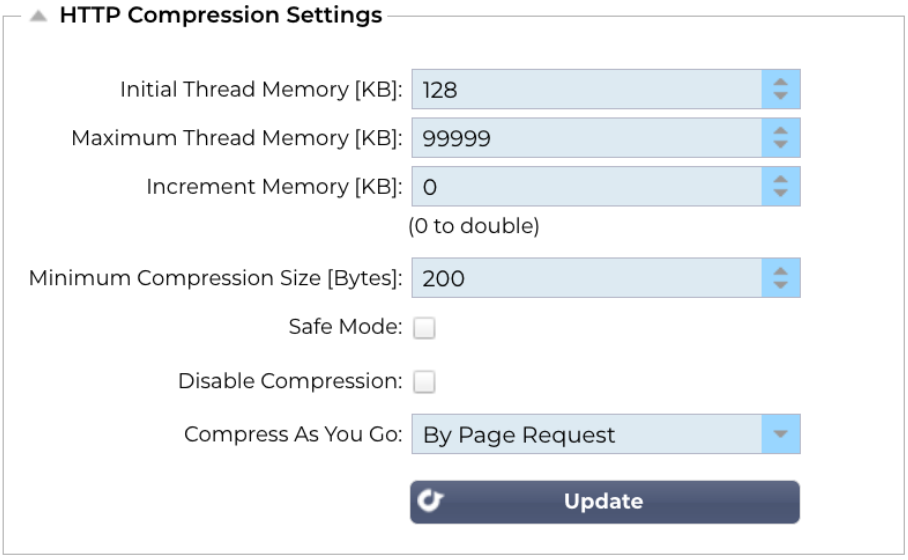
Type	Valeur
LogFormat :	"%h %l %u %t \N- "%r\N" %>s %b \N- "%{Referer}i\N" \N- "%{User-Agent}i\N"" combiné
LogFormat :	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \N- "%{User-Agent}i\N"" proxy SetEnvIf X- Forwarded-For "^.*\N..*\N..*\N..*" forwarded
CustomLog :	"logs/access_log" combiné env=!forwarded
CustomLog :	"logs/access_log" proxy env=forwarded

Ce format tire parti du support intégré d'Apache pour la journalisation conditionnelle basée sur des variables d'environnement.

- La ligne 1 est la chaîne formatée standard du journal combiné par défaut.
- La ligne 2 remplace le champ %h (hôte distant) par les valeurs extraites de l'en-tête X-Forwarded-For et définit le nom de ce modèle de fichier journal comme étant "proxy".
- La ligne 3 est un réglage de la variable d'environnement "forwarded" qui contient une expression régulière libre correspondant à une adresse IP, ce qui est acceptable dans ce cas puisque nous nous soucions davantage de savoir si une adresse IP existe dans l'en-tête X-Forwarded-For.
- De même, la ligne 3 pourrait être lue comme suit : "S'il existe une valeur X-Forwarded-For, utilisez-la : "S'il existe une valeur X-Forwarded-For, utilisez-la."
- Les lignes 4 et 5 indiquent à Apache le modèle de journal à utiliser. Si une valeur X-Forwarded-For existe, utilisez le modèle "proxy", sinon utilisez le modèle "combined" pour la requête. Pour des raisons de lisibilité, les lignes 4 et 5 ne tirent pas parti de la fonction de journalisation par rotation (piped) d'Apache, mais nous supposons que presque tout le monde l'utilise.

Ces modifications permettront d'enregistrer une adresse IP pour chaque demande.

Paramètres de compression HTTP



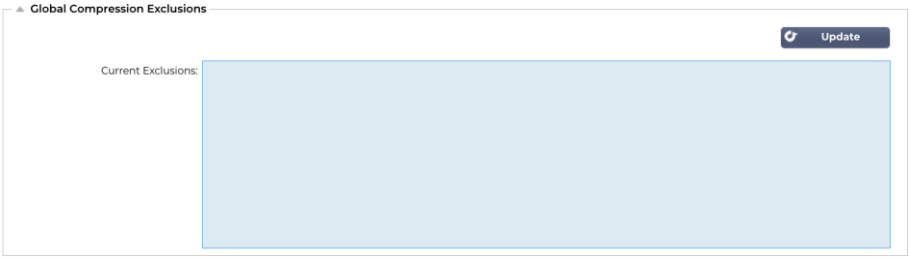
La compression est une fonction d'accélération et est activée pour chaque service sur la page Services IP.

AVERTISSEMENT - Soyez extrêmement prudent lorsque vous réglez ces paramètres, car des réglages inappropriés peuvent affecter négativement les performances de l'ADC.

Option	**Description**
Mémoire initiale des threads [KB]	Cette valeur correspond à la quantité de mémoire que chaque requête reçue par ADC peut initialement allouer. Pour des performances optimales, cette valeur doit être fixée à une valeur juste supérieure au plus grand fichier HTML non compressé que les serveurs web sont susceptibles d'envoyer.
Mémoire maximale des threads [KB]	Cette valeur correspond à la quantité maximale de mémoire que l'ADC allouera à une demande. Pour une performance maximale, l'ADC stocke et compresse normalement tout le contenu en mémoire. Si un fichier de contenu exceptionnellement volumineux dépassant cette valeur est traité, le CDA écrira sur le disque et y compressera les données.
Mémoire incrémentale [KB]	Cette valeur définit la quantité de mémoire ajoutée à l'allocation initiale de la mémoire des threads lorsque davantage de mémoire est nécessaire. La valeur par défaut est zéro. Cela signifie que l'ADC doublera l'allocation lorsque les données dépasseront l'allocation actuelle (par exemple 128 Ko, puis 256 Ko, puis 512 Ko, etc.) jusqu'à la limite fixée par l'utilisation maximale de la mémoire par thread. Cette méthode est efficace lorsque la majorité des pages sont de taille constante, mais qu'il y a occasionnellement des fichiers plus volumineux. (par exemple, la majorité des pages ont une taille de 128 Ko ou moins, mais les réponses occasionnelles ont une taille de 1 Mo). Dans le cas de fichiers de taille variable, il est plus efficace de définir un incrément linéaire d'une taille significative (par exemple, les réponses ont une taille comprise entre 2 et 10 Mo, un réglage initial de 1 Mo avec des incréments de 1 Mo serait plus efficace).
Taille minimale de compression [octets]	Cette valeur est la taille, en octets, en dessous de laquelle l'ADC n'essaiera pas de compresser. Ceci est utile car tout ce qui est inférieur à 200 octets n'est pas bien compressé et peut même augmenter en taille à cause des frais généraux des en-têtes de compression.
Mode sans échec	Cochez cette option pour empêcher ADC d'appliquer la compression aux feuilles de style et au JavaScript. La raison en est que même si ADC sait quels navigateurs individuels peuvent gérer du contenu compressé, certains autres serveurs proxy, même s'ils prétendent être conformes à la norme HTTP/1.1, sont incapables de transporter correctement des feuilles de style et du JavaScript compressés. Si des problèmes surviennent avec des feuilles de style ou du JavaScript via un serveur

	proxy, utilisez cette option pour désactiver la compression de ces types de contenu. Toutefois, cela réduira le niveau global de compression du contenu.
Désactiver la compression	Cochez cette case pour empêcher l'ADC de comprimer toute réponse.
Compresser au fur et à mesure	ON - Utiliser Compresser au fur et à mesure sur cette page. Cela permet de compresser chaque bloc de données reçu du serveur en un morceau discret qui est entièrement décompressible. OFF - Ne pas utiliser la compression au fur et à mesure sur cette page. By Page Request - Utiliser la compression à la demande de la page.

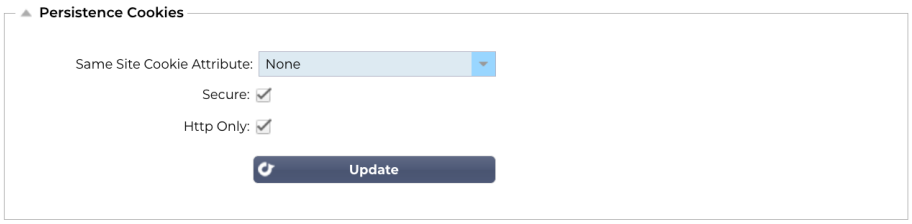
Exclusions de la compression globale



Les pages dont l'extension figure dans la liste d'exclusion ne seront pas compressées.

- Tapez le nom du fichier individuel.
- Cliquez sur mettre à jour.
- Si vous souhaitez ajouter un type de fichier, tapez simplement "*.css" pour exclure toutes les feuilles de style en cascade.
- Chaque fichier ou type de fichier doit être ajouté à une nouvelle ligne.

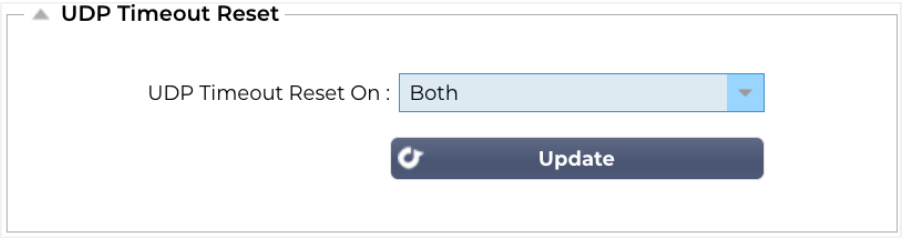
Cookies de persistance



Ce paramètre vous permet de spécifier comment les cookies de persistance sont gérés.

Champ d'application	Description
Même site Attribut Cooke	**Aucun** : Tous les cookies sont accessibles aux scripts **Laxiste** : Empêche l'accès des cookies à d'autres sites, mais ils sont stockés pour devenir accessibles et soumis au site propriétaire s'il est visité. **Strict** : empêche l'accès ou le stockage d'un cookie destiné à un autre site. **Désactivé** : retour au comportement par défaut du navigateur
Sécurisé	Cette case, lorsqu'elle est cochée, applique la persistance au trafic sécurisé.
HTTP uniquement	Si cette case est cochée, les cookies persistants ne sont autorisés que pour le trafic HTTP.

Réinitialisation du délai UDP



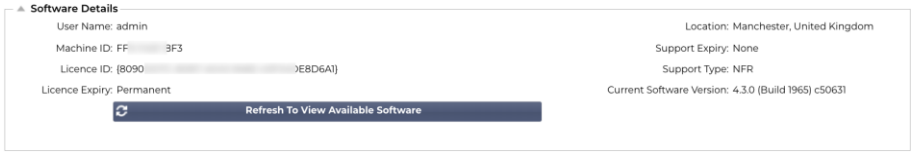
La réinitialisation du délai d'attente UDP est un mécanisme utilisé dans les communications réseau qui permet de redémarrer le délai d'attente relatif à une session UDP (User Datagram Protocol). La réinitialisation permet de maintenir la session active, ce qui garantit un flux de données continu sans interruption.

Option	Description
Les deux	Réinitialise le délai d'attente UDP sur le serveur et le client.
Serveur	Réinitialise le délai d'attente UDP sur le serveur.
Client	Réinitialise le délai d'attente UDP sur le client.

Logiciel

La section Logiciel vous permet de mettre à jour la configuration et le micrologiciel de votre ADC.

Détails de la mise à jour du logiciel



Les informations contenues dans cette section seront complétées si vous disposez d'une connexion Internet opérationnelle. Si votre navigateur n'a pas de lien avec l'internet, cette section sera vide. Une fois connecté, vous recevrez le message ci-dessous.

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

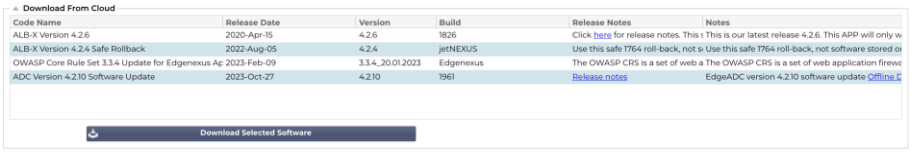
La section Télécharger à partir du nuage illustrée ci-dessous sera complétée par des informations indiquant les mises à jour disponibles dans le cadre de votre plan d'assistance. Vous devez prêter attention au type de support et à la date d'expiration du support.

Note : Nous utilisons la connexion internet de votre navigateur pour afficher ce qui est disponible dans le nuage Edgenexus. Vous ne pourrez télécharger les mises à jour logicielles que si l'ADC dispose d'une connexion internet.

Pour le vérifier :

- Avancé--Dépannage--Ping
- Adresse IP - App Store.edgenexus.io
- Cliquez sur Ping
- Si le résultat indique "ping : unknown host App Store.edgenexus.io".
- L'ADC ne sera PAS en mesure de télécharger quoi que ce soit à partir du nuage.

Télécharger à partir du nuage



Si votre navigateur est connecté à l'internet, vous verrez les détails des logiciels disponibles dans le nuage.

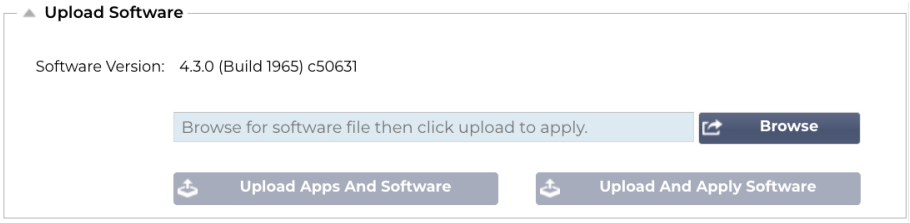
- Mettez en évidence la ligne qui vous intéresse et cliquez sur le bouton "Télécharger le logiciel sélectionné dans l'ALB".
- Le logiciel sélectionné sera téléchargé sur votre ALB lorsque vous cliquerez dessus, et pourra être appliqué dans la section "Appliquer le logiciel stocké sur l'ALB" ci-dessous.

Note : Si le CDA n'a pas d'accès direct à l'internet, vous recevrez un message d'erreur comme celui ci-dessous :

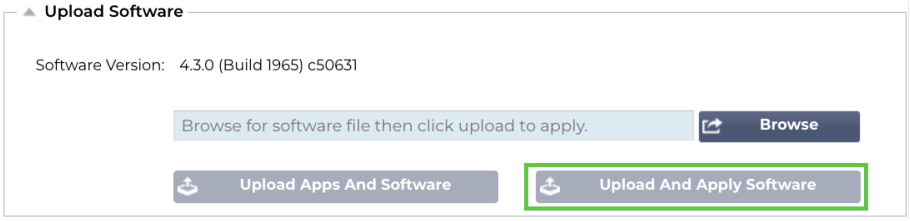
Erreur de téléchargement, ALB n'a pas pu accéder à ADC Cloud Services pour le fichier build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Si votre réseau est protégé par un serveur proxy, veuillez consulterProxy de téléchargement de l'App Store

Logiciel de téléchargement



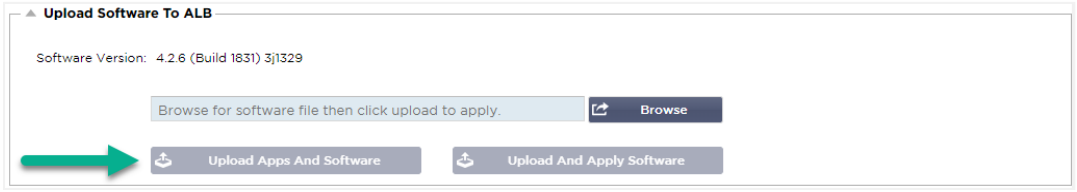
Téléchargement d'applications



Si vous avez un fichier d'application qui se termine par <appname> .<apptype>.alb, vous pouvez utiliser cette méthode pour le télécharger.

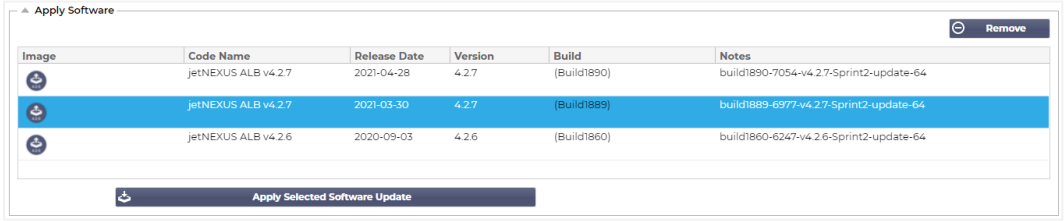
- Il existe cinq types d'applications
  - <nom de l'application>flightpath.alb
  - <appname>.monitor.alb
  - <appname>.jetpack.alb
  - <appname>.addons.alb
  - <appname>.featurepack.alb
- Une fois téléchargée, chaque application se trouve dans la section Bibliothèque>Applications.
- Vous devez ensuite déployer chaque application de cette section individuellement.

Logiciel /Mises à jour du micrologiciel



- Si vous souhaitez télécharger un logiciel sans l'appliquer, utilisez le bouton en surbrillance.
- Le fichier logiciel est <nom du logiciel>.software.alb.
- Il apparaîtra alors dans la section "Logiciels stockés sur l'ALB", d'où vous pourrez l'appliquer à votre convenance.

Appliquer le logiciel stocké sur ADC



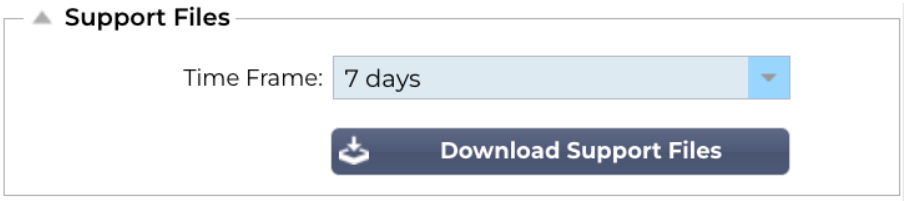
Cette section affiche tous les fichiers logiciels stockés sur l'ALB et disponibles pour le déploiement. La liste comprendra les signatures mises à jour du Web Application Firewall (WAF).

- Mettez en surbrillance la ligne du logiciel que vous souhaitez utiliser.
- Cliquez sur "Appliquer le logiciel de la sélection"
- S'il s'agit d'une mise à jour du logiciel de l'ALB, sachez qu'elle sera téléchargée et que l'ALB sera redémarré pour l'appliquer.
- Si la mise à jour que vous appliquez est une mise à jour de signature OWASP, elle s'appliquera automatiquement sans redémarrage.

Dépannage

Il y a toujours des problèmes qui nécessitent un dépannage pour trouver la cause première et la solution. Cette section vous permet de le faire.

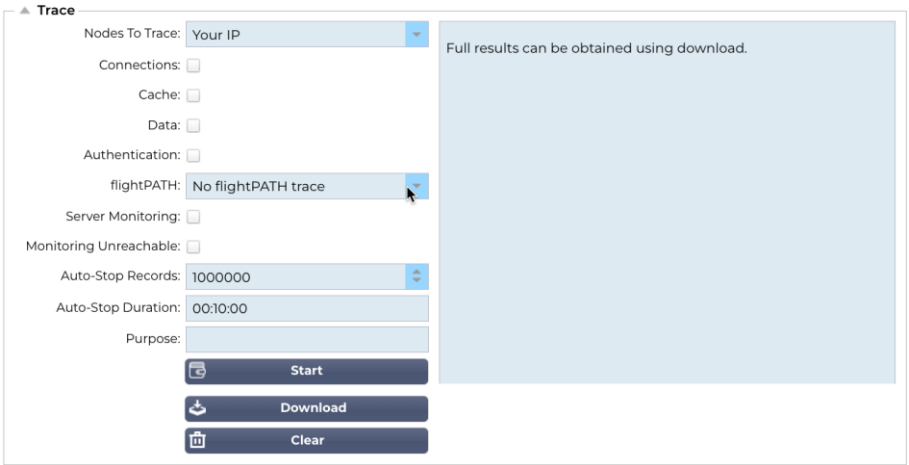
Fichiers de soutien



Si vous avez un problème avec l'ADC et que vous devez ouvrir un ticket d'assistance, le support technique demandera souvent plusieurs fichiers différents à partir de l'appliance ADC. Ces fichiers ont été regroupés en un seul fichier .dat qui peut être téléchargé via cette section.

- Sélectionnez une période dans le menu déroulant : Vous avez le choix entre 3, 7, 14 et Tous les jours.
- Cliquez sur "Télécharger les fichiers de support"
- Un fichier sera téléchargé au format Support-jetNEXUS-yyymmddhh-NAME.dat
- Créer un ticket d'assistance sur le portail d'assistance, dont les détails sont disponibles à la fin de ce document.
- Veillez à bien décrire le problème et à joindre le fichier .dat au ticket.

Trace



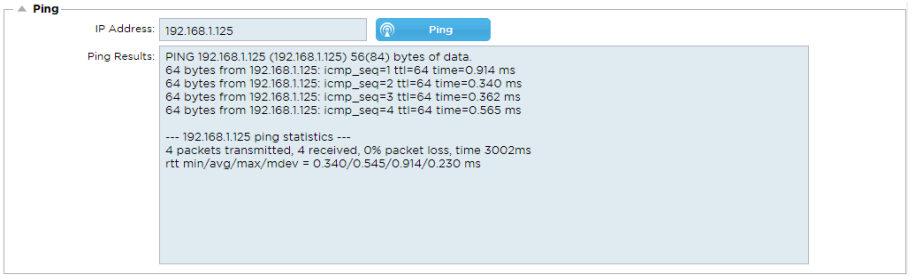
La section Trace vous permet d'examiner les informations permettant de déboguer le problème. Les informations fournies dépendent des options que vous choisissez dans les menus déroulants et les cases à cocher.

Option	**Description**
Nœuds à suivre	**Your IP** : Ceci filtrera la sortie pour utiliser l'adresse IP à partir de laquelle vous accédez à l'interface graphique (Note : ne pas choisir cette option pour la surveillance car la surveillance utilisera l'adresse de l'interface ADC). **Toutes les adresses IP** : aucun filtre ne sera appliqué. Il convient de noter que sur une boîte occupée, cela affectera négativement les performances.
Connexions	Cette case, lorsqu'elle est cochée, affiche des informations sur les connexions côté client et côté serveur.

Cache	Si vous cochez cette case, vous obtiendrez des informations sur les objets mis en cache.
Données	Lorsque cette case est cochée, elle inclut les octets de données brutes traités en entrée et en sortie par l'ADC.
chemin d'accès au vol	Le menu flightPATH vous permet de sélectionner une règle flightPATH particulière à surveiller ou toutes les règles flightPATH.
Surveillance du serveur	Cette case, lorsqu'elle est cochée, affiche les moniteurs de santé du serveur actifs sur l'ADC et leurs résultats respectifs.
Surveillance de l'inaccessibilité	Lorsque cette option est sélectionnée, le comportement est très similaire à celui de la surveillance des serveurs, sauf qu'elle n'affiche que les surveillances qui ont échoué et agit donc comme un filtre pour ces messages uniquement.
Dossiers Auto-Stop	La valeur par défaut est de 1 000 000 d'enregistrements, après quoi la fonction Trace s'arrête automatiquement. Ce réglage est une précaution de sécurité pour éviter que la fonction Trace ne reste accidentellement activée et n'affecte les performances de l'ADC.
Durée de l'arrêt automatique	La durée par défaut est fixée à 10 minutes, après quoi la fonction Trace s'arrête automatiquement. Cette fonction est une précaution de sécurité pour éviter que la fonction Trace ne reste accidentellement activée et n'affecte les performances de l'ADC.
Démarrage	Cliquez sur ce bouton pour lancer manuellement la fonction Trace.
Arrêter	Cliquez sur ce bouton pour arrêter manuellement la fonction Trace avant que l'enregistrement automatique ou la durée ne soit atteint.
Télécharger	Bien que vous puissiez voir le visualiseur en direct sur le côté droit, les informations risquent d'être affichées trop rapidement. Au lieu de cela, vous pouvez télécharger le fichier Trace.log pour visualiser toutes les informations recueillies au cours des différentes traces de la journée. Cette fonction est une liste filtrée d'informations sur les traces. Si vous souhaitez consulter les informations de traçage des jours précédents, vous pouvez télécharger le Syslog de ce jour-là, mais vous devrez alors procéder à un filtrage manuel.
Clair	Efface le journal des traces

Ping

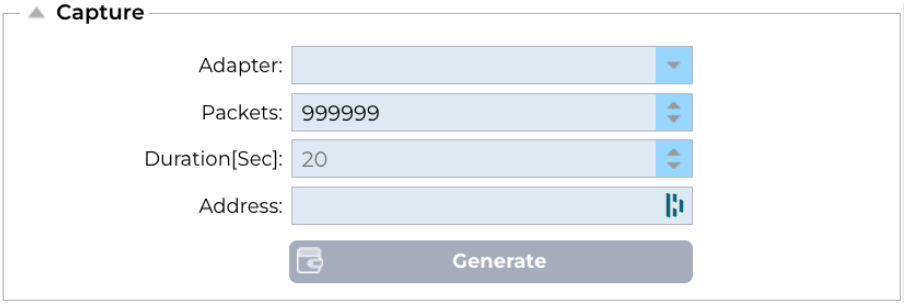
Vous pouvez vérifier la connectivité du réseau avec les serveurs et les autres objets du réseau dans votre infrastructure à l'aide de l'outil Ping.



Saisissez l'adresse IP de l'hôte que vous souhaitez tester, par exemple la passerelle par défaut en utilisant la notation décimale pointée ou une adresse IPv6. Il se peut que vous deviez attendre quelques secondes avant d'obtenir un résultat après avoir appuyé sur le bouton "Ping".

Si vous avez configuré un serveur DNS, vous pouvez saisir le nom de domaine complet. Vous pouvez configurer un serveur DNS dans la section **Serveur DNS 1 & Serveur DNS 2.** Il se peut que vous deviez attendre quelques secondes avant d'obtenir un résultat une fois que vous avez appuyé sur le bouton "Ping".

Capture



Pour capturer le trafic réseau, suivez les instructions simples ci-dessous.

- Complétez les options du formulaire
- Cliquez sur Générer
- Une fois la capture exécutée, votre navigateur s'affichera et vous demandera où vous souhaitez enregistrer le fichier. Il se présentera sous le format "jetNEXUS.cap.gz".
- Créer un ticket d'assistance sur le portail d'assistance, dont les détails sont disponibles à la fin de ce document.
- Veillez à bien décrire le problème et à joindre le fichier au ticket.
- Vous pouvez également visualiser le contenu à l'aide de Wireshark

Option	**Description**
Adaptateur	Choisissez votre adaptateur dans la liste déroulante, généralement eth0 ou eth1. Vous pouvez également capturer toutes les interfaces avec "any"
Paquets	Cette valeur correspond au nombre maximum de paquets à capturer. Typiquement, 99999
Durée de l'accord	Choisissez une durée maximale pour la capture. Une durée typique est de 15 secondes pour les sites à fort trafic. L'interface graphique sera inaccessible pendant la période de capture.
Adresse	Cette valeur permet de filtrer toute adresse IP saisie dans la case. Laissez ce champ vide pour ne pas filtrer.

Pour maintenir les performances, nous avons limité le fichier de téléchargement à 10 Mo. Si vous estimez que ce n'est pas suffisant pour capturer toutes les données nécessaires, nous pouvons augmenter ce chiffre.

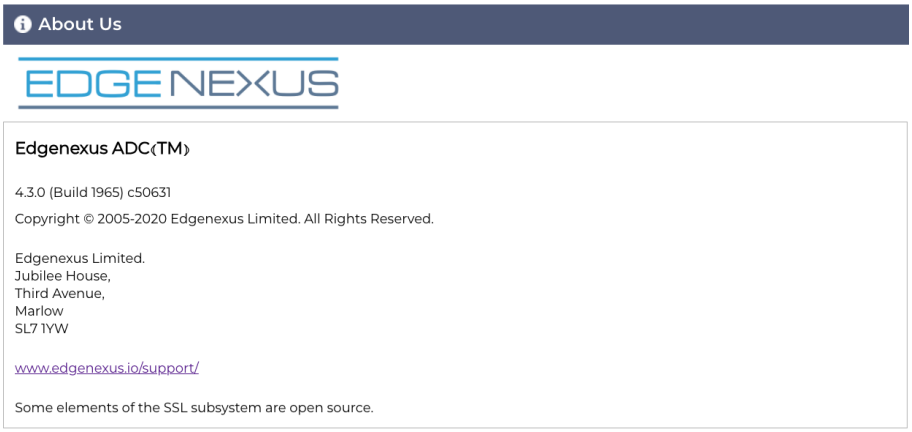
Remarque : cette mesure aura un impact sur les performances des sites en direct. Pour augmenter la taille de capture disponible, veuillez appliquer un paramètre global jetPACK pour augmenter la taille de capture.

Aide

La section Aide permet d'accéder aux informations sur Edgenexus, aux guides d'utilisation et à d'autres informations utiles.

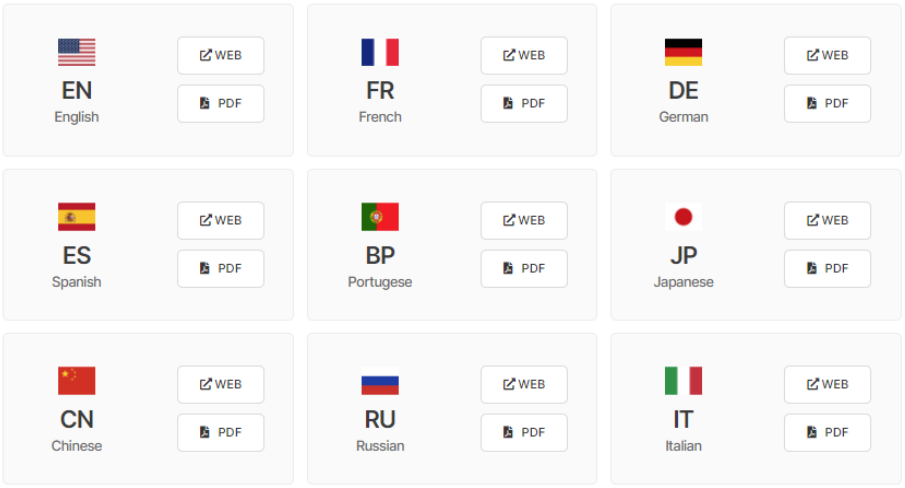
A propos de nous

En cliquant sur l'option À propos de nous, vous obtiendrez des informations sur Edgenexus et son siège social.



Référence

L'option de référence ouvrira la page web contenant les guides d'utilisation et d'autres documents utiles. La page web peut également être trouvée en utilisant https://www.edgenexus.io/documentation.



Si vous ne trouvez pas ce que vous cherchez, veuillez contacter .support@edgenexus.io

JetPACKs

Edgenexus jetPACK s

Les jetPACKs sont une méthode unique pour configurer instantanément votre ADC pour des applications spécifiques. Ces modèles faciles à utiliser sont préconfigurés et entièrement réglés avec tous les paramètres spécifiques à l'application dont vous avez besoin pour bénéficier d'une prestation de services optimisée de la part de votre CDA. Certains jetPACKs utilisent flightPATH pour manipuler le trafic, et vous devez disposer d'une licence flightPATH pour que cet élément fonctionne. Pour savoir si vous disposez d'une licence pour flightPATH, veuillez consulter la page **LICENCE.**

Télécharger un jetPACK

- Chaque jetPACK ci-dessous a été créé avec une adresse IP virtuelle unique contenue dans le titre du jetPACK. Par exemple, le premier jetPACK ci-dessous a une adresse IP virtuelle de 1.1.1.1.
- Vous pouvez soit télécharger ce jetPACK tel quel et changer l'adresse IP dans l'interface graphique, soit éditer le jetPACK avec un éditeur de texte tel que Notepad++ et rechercher et remplacer 1.1.1.1 par votre adresse IP virtuelle.
- De plus, chaque jetPACK a été créé avec 2 serveurs réels dont les adresses IP sont 127.1.1.1 et 127.2.2.2. Là encore, vous pouvez modifier ces adresses dans l'interface graphique après le téléchargement ou au préalable à l'aide de Notepad++.
- Cliquez sur un lien jetPACK ci-dessous et enregistrez le lien en tant que fichier jetPACK-VIP-Application.txt à l'emplacement de votre choix.

Microsoft Exchange

Application	Lien de téléchargement	Que fait-il ?	Qu'est-ce qui est inclus ?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	Ce jetPACK ajoutera les paramètres de base pour équilibrer la charge de Microsoft Exchange 2010. Une règle flightPATH est incluse pour rediriger le trafic du service HTTP vers HTTPS, mais il s'agit d'une option. Si vous n'avez pas de licence pour flightPATH, ce jetPACK fonctionnera quand même.	Paramètres globaux : Délai d'attente de service 2 heures Moniteurs : Moniteur de couche 7 pour l'application web Outlook et moniteur hors bande de couche 4 pour le service d'accès client. Service virtuel IP : 1.1.1.1 Ports de service virtuels : 80, 443, 135, 59534, 59535 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP à HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Même chose que ci-dessus, mais cela ajoutera un service SMTP sur le port 25 en connectivité proxy inverse. Le serveur SMTP verra l'adresse de l'interface ALB-X comme l'IP source.	Paramètres globaux : Délai d'attente de service 2 heures Moniteurs : Moniteur de couche 7 pour l'application web Outlook. Moniteur hors bande de la couche 4 pour le service d'accès au client. Service virtuel IP : 1.1.1.1 Ports du service virtuel : 80, 443, 135, 59534, 59535, 25 (reverse proxy) Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP à HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Identique au précédent, sauf que ce jetPACK configurera le service SMTP pour qu'il utilise la connectivité de retour	Paramètres globaux : Délai d'attente de service 2 heures

		direct du serveur. Ce jetPACK est nécessaire si votre serveur SMTP a besoin de voir l'adresse IP réelle du client.	Moniteurs : Moniteur de couche 7 pour l'application web Outlook. Moniteur hors bande de la couche 4 pour le service d'accès au client. Service virtuel IP : 1.1.1.1 Ports du service virtuel : 80, 443, 135, 59534, 59535, 25 (retour direct du serveur) Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP vers HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Cette configuration ajoute 1 VIP et deux services pour le trafic HTTP et HTTPS et nécessite le moins de CPU. Il est possible d'ajouter plusieurs contrôles de santé au VIP afin de vérifier que chacun des services individuels est opérationnel.	Paramètres globaux : Moniteurs : Moniteur de couche 7 pour OWA, EWS, OA, EAS, ECP, OAB et ADS Service virtuel IP : 2.2.2.1 Ports de service virtuels : 80, 443 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP à HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Cette configuration utilise une adresse IP unique pour chaque service et consomme donc plus de ressources que la précédente. Vous devez configurer chaque service comme une entrée DNS individuelle Exemple owa.edgenexus.com, ews.edgenexus.com, etc. Un moniteur pour chaque service sera ajouté et appliqué au service concerné.	Paramètres globaux : Moniteurs : Surveillance de la couche 7 pour OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI et PowerShell Service virtuel IP : 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 Ports de service virtuels : 80, 443 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP vers HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Ce jetPACK ajoute une adresse IP unique et plusieurs services virtuels sur différents ports. flightPATH effectue alors un changement de contexte en fonction du chemin de destination vers le service virtuel approprié. Ce jetPACK nécessite la plus grande quantité de CPU pour effectuer le changement de contexte.	Paramètres globaux : Moniteurs : Surveillance de la couche 7 pour OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI et PowerShell Service virtuel IP : 2.2.2.3 Ports de service virtuels : 80, 443, 1, 2, 3, 4, 5, 6, 7 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : ajoute une redirection de HTTP à HTTPS

Microsoft Lync 2010/2013

Proxy inversé	Front-end	Bord interne	Bord externe
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

Services Web

HTTP normal	Déchargement SSL	Recryptage SSL	SSL Passthrough

jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Web-SSL Offload	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Microsoft Remote Desktop

Normal
jetPACK-5.5.5.1-Remote-Desktop

DICOM - Imagerie numérique et communication en médecine

HTTP normal
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

Déchargement SSL	
jetPACK-7.7.7..1-Oracle-EBS	

VMware Horizon View

Serveurs de connexion - SSL Offload	**Serveurs de sécurité - Recryptage SSL**
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

Paramètres globaux

- GUI Secure Port 443 - ce jetPACK changera votre port GUI sécurisé de 27376 à 443. HTTPs://x.x.x.x
- Délai d'attente de l'interface graphique 1 jour - l'interface graphique vous demande de saisir votre mot de passe toutes les 20 minutes. Ce paramètre portera ce délai à 1 jour.
- ARP Refresh 10 - lors d'un basculement entre appliances HA, ce paramètre augmente le nombre d'**ARP gratuits** pour aider les commutateurs pendant la transition.
- Taille de la capture 16MB - la taille de la capture par défaut est de 2MB. Cette valeur permet d'augmenter la taille jusqu'à un maximum de 16 Mo.

Cipher s et Cipher jetPACKs

L'EdgeADC est équipé en standard des meilleurs algorithmes de chiffrement. Ces codes sont associés à leurs protocoles TLS respectifs, ce qui facilite la tâche des utilisateurs.

Nous avons fourni un ensemble de codes supplémentaires que vous pouvez utiliser si vous en avez besoin.

Chiffres forts

Ajoute la possibilité de choisir "Strong Ciphers" dans la liste des options de chiffrement :

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
```

Anti-bête

Ajoute la possibilité de choisir "Anti Beast" dans la liste des options de chiffrement :

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

Pas de SSLv3

Ajoute la possibilité de choisir "Pas de SSLv3" dans la liste des options de chiffrement :

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

Pas de SSLv3 pas de TLSv1 pas de RC4

Ajoute la possibilité de choisir "No-TLSv1 No-SSLv3 No-RC4" dans la liste des options de chiffrement :

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

NO_TLSv1.1

Ajoute la possibilité de choisir "NO_TLSv1.1" dans la liste des options de chiffrement :

```
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128 :
DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4
```

Activer les codes TLS-1.0-1.1

À partir de la version 4.2.10, la prise en charge du chiffrement pour les protocoles TLS1.0 et TLS 1.1 a été supprimée. Cependant, certains clients continuent d'utiliser ces anciens protocoles pour leurs serveurs internes. Le Cipher ci-dessous ajoute la possibilité d'activer TLS v1.0 et TLS v1.1.

```
AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-
SHA :EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-
SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-
SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-
AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Exemple Chiffre jetPACK

Les codes sont importés dans l'ADC à l'aide de jetPACKs. Un jetPACK est un simple fichier texte qui contient des paramètres que l'ADC reconnaîtra. L'exemple ci-dessous montre un jetPACK utilisant le chiffrement Enable TLS-1.0-1.1.

```
#!update

[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]

Cipher="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-
AES256-SHA :EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-
SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-
AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-
SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"

Cipher1=""

Cipher2=""

CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"

Description=" TLS v1.0 - v1.1 activé "
```

- X-Content-Type-Options - ajoutez cet en-tête s'il n'existe pas et donnez-lui la valeur "nosniff" - pour empêcher le navigateur de "renifler" automatiquement les données MIME.
- X-Frame-Options - ajoutez cet en-tête s'il n'existe pas et donnez-lui la valeur "SAMEORIGIN" - les pages de votre site web peuvent être incluses dans des cadres, mais seulement sur d'autres pages du même site web.
- X-XSS-Protection - ajoutez cet en-tête s'il n'existe pas et définissez-le à "1 ; mode=block" - pour activer les protections contre les scripts intersites dans le navigateur.
- Strict-Transport-Security - ajouter un en-tête s'il n'existe pas et le définir à "max-age=31536000 ; includeSubdomains" - garantit que le client doit respecter le fait que tous les liens doivent être HTTPs:// pour l'âge maximum.

Application d'un jetPACK

Vous pouvez appliquer n'importe quel jetPACK dans n'importe quel ordre, mais veillez à ne pas utiliser un jetPACK avec la même adresse IP virtuelle. Cette action entraînera une adresse IP en double dans la configuration. Si vous faites cela par erreur, vous pouvez le modifier dans l'interface graphique.

- Naviguer vers Avancé > Mise à jour du logiciel
- Section Configuration
- Télécharger une nouvelle configuration ou un nouveau jetPACK
- Parcourir pour jetPACK
- Cliquez sur Télécharger
- Une fois que l'écran du navigateur devient blanc, cliquez sur rafraîchir et attendez que la page du tableau de bord apparaisse.

Création d'un jetPACK

L'un des grands avantages de jetPACK est que vous pouvez créer votre propre configuration. Il se peut que vous ayez créé la configuration parfaite pour une application et que vous souhaitiez l'utiliser pour plusieurs autres boîtes indépendamment.

- Commencez par copier la configuration actuelle de votre ALB-X existant.
  - Avancé
  - Mise à jour du logiciel
  - Télécharger la configuration actuelle
- Modifier ce fichier avec Notepad++
- Ouvrez un nouveau document txt et appelez-le "yourname-jetPACK1.txt".
- Copiez toutes les sections pertinentes du fichier de configuration dans "yourname-jetPACK1.txt".
- Sauvegarder une fois terminé

IMPORTANT : Chaque jetPACK est divisé en différentes sections, mais tous les jetPACKs doivent avoir #!jetpack en haut de la page.

Les sections qu'il est recommandé d'éditer/copier sont énumérées ci-dessous.

Section 0 :

```
#!jetpack
```

Cette ligne doit se trouver en haut du jetPACK, sinon votre configuration actuelle sera écrasée.

Section 1 :

```
[jetnexusdaemon]
```

Cette section contient des paramètres globaux qui, une fois modifiés, s'appliquent à tous les services. Certains de ces paramètres peuvent être modifiés à partir de la console web, mais d'autres ne sont disponibles qu'ici.

Exemples :

```
ConnectionTimeout=600000
```

Cet exemple représente la valeur du délai d'attente TCP en millisecondes. Ce paramètre signifie qu'une connexion TCP sera fermée après 10 minutes d'inactivité.

```
ContentServerCustomTimer=20000
```

Cet exemple indique le délai en millisecondes entre les contrôles de santé du serveur de contenu pour les moniteurs personnalisés tels que DICOM.

```
jnCookieHeader="MS-WSMAN"
```

Cet exemple modifiera le nom de l'en-tête de cookie utilisé dans l'équilibrage de charge persistant de la valeur par défaut "jnAccel" à "MS-WSMAN". Ce changement particulier est nécessaire pour le proxy inverse Lync 2010/2013.

Section 2 :

```
[jetnexusdaemon-Csm-Rules]
```

Cette section contient les règles personnalisées de surveillance des serveurs qui sont généralement configurées à partir de la console Web.

Exemple :

```
[jetnexusdaemon-Csm-Rules-0]
Content="Serveur en place"
Desc="Moniteur 1″ (en anglais)
Method="CheckResponse"
Name="Bilan de santé - Le serveur est-il opérationnel ?
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Section 3 :

```
[jetnexusdaemon-LocalInterface]
```

Cette section contient tous les détails de la section Services IP. Chaque interface est numérotée et comprend des sous-interfaces pour chaque canal. Si une règle flightPATH est appliquée à votre canal, celui-ci contiendra également une section Path.

Exemple :

```
[jetnexusdaemon-LocalInterface1]
1.1="443″
1.2="104″
1.3="80″
1.4="81″
Activé=1
Netmask=”255.255.255.0″
PrimaryV2=”{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}”
[jetnexusdaemon-LocalInterface1.1]
1=">,""Groupe sécurisé"",2000,"".
2="192.168.101.11:80,Y,""IIS WWW Server 1″""
3="192.168.101.12:80,Y,""IIS WWW Server 2″""
AddressResolution=0
CachePort=0
CertificateName="default" (nom du certificat)
ClientCertificateName="Pas de SSL"
Compress=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
```

```
Activé=1
LoadBalancePolicy="CookieBased" (Politique d'équilibre de charge)
MaxConnections=10000
MonitoringPolicy="1″ (Politique de surveillance)
PassThrough=0
Protocol="Accélérer HTTP"
ServiceDesc="Serveurs sécurisés VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1="6″
Section 4 :
[jetnexusdaemon-Path]
```

Cette section contient toutes les règles flightPATH. Les numéros doivent correspondre à ce qui a été appliqué à l'interface. Dans l'exemple ci-dessus, nous voyons que la règle flightPATH "6" a été appliquée au canal.

Exemple :

```
[jetnexusdaemon-Path-6]
Desc="Forcer l'utilisation de HTTPS pour certains répertoires"
Name="Gary - Forcer HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contain"
Condition="path"
Match=
Sens="fait"
Valeur="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Détail=
Source="host"
Valeur=
Variable="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="redirect"
Target="HTTPs://$host$$path$$querystring$"
Valeur=
```

chemin d'accès au vol

Introduction à flightPATH

Qu'est-ce que flightPATH ?

flightPATH est un moteur de règles intelligent développé par Edgenexus pour manipuler et acheminer le trafic HTTP et HTTPS. Il est hautement configurable, très puissant et pourtant très facile à utiliser.

Bien que certains composants de flightPATH soient des objets IP, tels que l'IP source, flightPATH ne peut être appliqué qu'à un type de service de couche 7 égal à HTTP(s). Si vous choisissez un autre type de service, l'onglet flightPATH des services IP sera vide.

Que peut faire flightPATH ?

flightPATH peut être utilisé pour modifier le contenu et les requêtes HTTP(s) entrantes et sortantes.

Outre l'utilisation de simples correspondances de chaînes telles que "Commence par" et "Se termine par" par exemple, il est possible de mettre en œuvre un contrôle complet à l'aide de puissantes expressions régulières (RegEx) compatibles avec Perl.

Pour en savoir plus sur RegEx, consultez ce site utile

En outre, des variables personnalisées peuvent être créées dans la section Évaluation et utilisées dans la zone Action, ce qui offre de nombreuses possibilités.

Une règle flightPATH comporte trois éléments :

Option	Description
Détails	Permet d'ajouter ou de supprimer un flightPATH et de dresser la liste de ceux qui sont disponibles.
Condition	Définir plusieurs critères pour déclencher la règle flightPATH.
L'évaluation	Permet d'utiliser des variables qui peuvent être utilisées dans la zone d'action.
Action	Le comportement à adopter une fois que la règle s'est déclenchée.

Condition

Dans cette section, vous pouvez spécifier cinq paramètres individuels qui s'appliquent à une condition. Ces paramètres sont présentés ci-dessous avec une description de chaque option et un exemple.

Condition	Description	Exemple
<form>	Les formulaires HTML sont utilisés pour transmettre des données à un serveur	Exemple "le formulaire n'a pas la longueur 0".
Emplacement du GEO	Cette fonction compare l'adresse IP source au code pays ISO 3166.	GEO Location est égal à GB OU GEO Location est égal à Germany
Hôte	Voici l'hôte extrait de l'URL	www.mywebsite.com ou 192.168.1.1
Langue	Voici la langue extraite de l'en-tête HTTP de la langue	Cette condition produira un menu déroulant avec une liste de langues.
Méthode	Il s'agit d'une liste déroulante de méthodes HTTP	Il s'agit d'une liste déroulante qui comprend GET, POST, etc.
Origine IP	Si le proxy en amont prend en charge X-Forwarded-for (XFF), il utilisera la véritable adresse d'origine.	IP du client. Il est également possible d'utiliser plusieurs IP ou sous-réseaux.

		10.1.2.* est le sous-réseau 10.1.2.0 /24 10\N- 1\N- 2\N- 3|10\N- 1\N- 2\N- 4 Utiliser | pour des IP multiples
Chemin d'accès	Voici le chemin d'accès au site web	/mywebsite/index.asp
POST	Méthode de requête POST	Vérifier les données téléchargées sur un site web
Demande de renseignements	Il s'agit du nom et de la valeur d'une requête, qui peut donc accepter soit le nom de la requête, soit une valeur.	"Best=edgeNEXUS" Lorsque la correspondance est Best et que la valeur est edgeNEXUS
Chaîne de requête	Toute la chaîne de requête après le caractère ?	
Demande de cookie	Il s'agit du nom d'un cookie demandé par un client.	MS-WSMAN=afYfn1CDqqCDqUD: :
En-tête de la demande	Il peut s'agir de n'importe quel en-tête HTTP	Referrer, User-Agent, From, Date
Demande de version	Voici la version HTTP	HTTP/1.0 OU HTTP/1.1
Organe de réponse	Une chaîne définie par l'utilisateur dans le corps de la réponse	Serveur UP
Code de réponse	Le code HTTP de la réponse	200 OK, 304 Non modifié
Cookie de réponse	Il s'agit du nom d'un cookie envoyé par le serveur.	MS-WSMAN=afYfn1CDqqCDqUD: :
En-tête de réponse	Il peut s'agir de n'importe quel en-tête HTTP	Referrer, User-Agent, From, Date
Version de la réponse	La version HTTP envoyée par le serveur	HTTP/1.0 OU HTTP/1.1
Source IP	Il s'agit de l'adresse IP d'origine, de l'adresse IP du serveur proxy ou d'une autre adresse IP agrégée.	IP client IP, IP du proxy, IP du pare-feu. Il est également possible d'utiliser plusieurs IP et sous-réseaux. Les points doivent être échappés car il s'agit de RegEX. Vous devez échapper aux points, car il s'agit de RegEX. Exemple 10.1.2.3 est 10.1.2.3

Correspondance

Le paramètre Match est sensible au contexte en fonction de la valeur du paramètre Condition.

Correspondance	Description	Exemple
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodages acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>
Acceptation de la langue	Langues acceptables pour la réponse	Accept-Language : en-US
Plages d'acceptation	Types de plages de contenu partiel pris en charge par ce serveur	Accept-Ranges : bytes
Autorisation	Données d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==.

Charge-To	Contient des informations comptables relatives aux coûts de l'application de la méthode demandée.	
Content-Encoding	Le type d'encodage utilisé pour les données.	Content-Encoding : gzip
Longueur du contenu	Longueur du corps de la réponse en octets (octets de 8 bits)	Content-Length : 348
Content-Type	Le type de mime du corps de la requête (utilisé avec les requêtes POST et PUT)	Content-Type : application/x-www-form-urlencoded
Cookie	Un cookie HTTP précédemment envoyé par le serveur avec Set-Cookie (ci-dessous)	Cookie : $Version=1 ; Skin=new ;
Date	Date et heure d'émission du message	Date = "Date" " :" HTTP-date
ETag	Identifiant d'une version spécifique d'une ressource, souvent un condensé de message.	ETag : "aed6bdb8e090cd1:0"
De	L'adresse électronique de l'utilisateur qui fait la demande	De : user@example.com
Si modifié depuis	Permet de renvoyer un message 304 Non modifié si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	Date de la dernière modification de l'objet demandé, au format RFC 2822	Dernière modification : Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Les en-têtes spécifiques à la mise en œuvre peuvent avoir divers effets tout au long de la chaîne demande-réponse.	Pragma : no-cache
Référent	Il s'agit de l'adresse de la page web précédente à partir de laquelle un lien vers la page actuellement demandée a été suivi	Référent : HTTP://www.edgenexus.io
Serveur	Un nom pour le serveur	Serveur : Apache/2.4.1 (Unix)
Set-Cookie	Un cookie HTTP	Set-Cookie : UserID=JohnDoe ; Max-Age=3600 ; Version=1
User-Agent	Chaîne de caractères de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Variable	Indique aux mandataires en aval comment faire correspondre les futurs en-têtes de requête pour décider si la réponse mise en cache peut être utilisée plutôt que de demander une nouvelle réponse. si la réponse mise en cache peut être utilisée plutôt que d'en demander une nouvelle au au serveur d'origine	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple ASP.NET, PHP, JBoss) qui supporte l'application web.	X-Powered-By : PHP/5.4.0

Vérifier

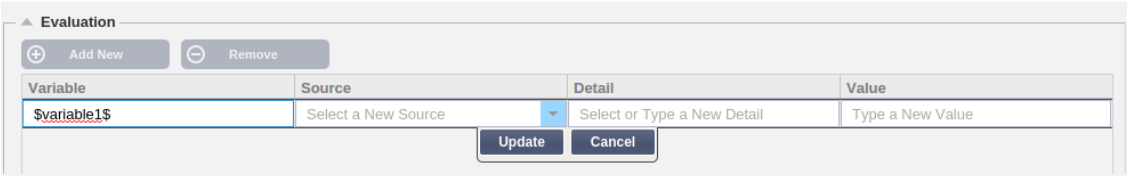
Vérifier	Description	Exemple
Exister	Cela ne concerne pas les détails de la condition, mais seulement le fait qu'elle existe ou n'existe pas.	Hôte> Existe-t-il> ?
Démarrage	La chaîne commence par la valeur	Chemin d'accès> Fait> Commence /secure>

Fin	La chaîne se termine par la valeur	Chemin d'accès> Does> End> .jpg
Contenir	La chaîne contient bien la valeur	Request Header> Accept> Does> Contain> Image
Égalité	La chaîne est égale à la valeur	Hôte> Est-ce que> est égal à> www.edgenexus.io
Avoir de la longueur	La chaîne a la longueur de la valeur	Hôte> Est-ce que> a la longueur> 16 www.edgenexus.io = VRAI www.edgenexus.com = FAUX
Dépasser la longueur	Vérifier que la valeur ne dépasse pas la longueur spécifiée.	Chemin > Faits > Dépasser la longueur - 10
Match RegEx	Cela vous permet de saisir une expression régulière complète compatible avec Perl	Origine IP> Correspond à> Regex> 10\..* | 11\..*
Liste des matches	Permet de fournir une liste de valeurs délimitée par PIPE (|) que vous pouvez vérifier.	Source IP > Does > Match List > 10.0.0.1 | 10.0.0.100 | 192.178.28.32

Exemple

- L'exemple comporte deux conditions, et les **DEUX** doivent être remplies pour que l'action soit exécutée.
- La première consiste à vérifier que l'objet demandé est une image
- La seconde consiste à rechercher un nom d'hôte spécifique

L'évaluation



L'ajout d'une variable est une fonctionnalité intéressante qui vous permettra d'extraire des données de la demande et de les utiliser dans les actions. Par exemple, vous pouvez enregistrer le nom d'un utilisateur ou envoyer un courrier électronique en cas de problème de sécurité.

- Variable : Elle doit commencer et se terminer par le symbole $. Par exemple $variable1$
- Source : Sélectionnez dans la liste déroulante la source de la variable.
- Détail : Sélectionner dans la liste le cas échéant. Si la source est l'en-tête de la requête, les détails peuvent être User-Agent.
- Valeur : Saisissez le texte ou l'expression régulière permettant d'affiner la variable.

Variables intégrées :

- Les variables intégrées ont déjà été codées en dur, il n'est donc pas nécessaire de créer une entrée d'analyse pour celles-ci.
- Vous pouvez utiliser l'une des variables énumérées ci-dessous dans votre action
- L'explication de chaque variable se trouve dans le tableau "Condition" ci-dessus.
    - Méthode = $method$
    - Chemin = $path$
    - Chaîne de requête = $querystring$

- Sourceip = $sourceip$
- Code de réponse (le texte comprend également "200 OK") = $resp$
- Hôte = $host$
- Version = $version$
- Clientport = $clientport$
- Clientip = $clientip
- Géolocalisation = $geolocation$"

Exemple d'action :

- Action = Redirection 302
  - Cible = HTTPs://$host$/404.html
- Action = Enregistrer
  - Cible = Un client de $sourceip$:$sourceport$ vient de faire une requête $path$ page

Explication :

- Un client accédant à une page qui n'existe pas se verrait normalement présenter une page 404 du navigateur.
- Dans ce cas, l'utilisateur est redirigé vers le nom d'hôte original qu'il a utilisé, mais le mauvais chemin est remplacé par 404.html.
- Une entrée est ajoutée au syslog disant "Un client de 154.3.22.14:3454 vient de faire une requête à la page wrong.html"

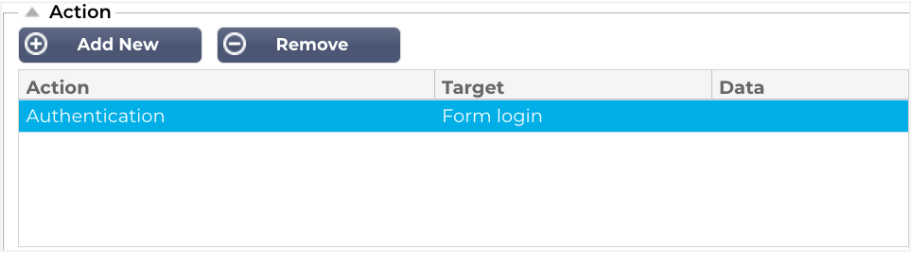
Source	Description	Exemple
Cookie	Il s'agit du nom et de la valeur de l'en-tête du cookie.	MS-WSMAN=afYfn1CDqqCDqUD::Où le nom est MS-WSMAN et la valeur est afYfn1CDqqCDqUD: :
Hôte	Il s'agit du nom d'hôte extrait de l'URL	www.mywebsite.com ou 192.168.1.1
Langue	Voici la langue extraite de l'en-tête HTTP Langue	Cette condition produira une liste déroulante avec une liste de langues.
Méthode	Il s'agit d'une liste déroulante de méthodes HTTP	La liste déroulante comprendra GET, POST
Trajectoire	Voici le chemin d'accès au site web	/mon site web/index.html
POST	Méthode de requête POST	Vérifier les données téléchargées sur un site web
Élément de la requête	Il s'agit du nom et de la valeur d'une requête. En tant que tel, il peut accepter soit le nom de la requête, soit une valeur.	"Best=jetNEXUS" Lorsque la correspondance est Best et la valeur est edgeNEXUS
Chaîne de requête	Il s'agit de la chaîne entière après le caractère ?	HTTP://server/path/program?query_string
En-tête de la demande	Il peut s'agir de n'importe quel en-tête envoyé par le client	Referrer, User-Agent, From, Date...
En-tête de réponse	Il peut s'agir de n'importe quel en-tête envoyé par le serveur	Referrer, User-Agent, From, Date...
Version	Voici la version HTTP	HTTP/1.0 ou HTTP/1.1

Détail	Description	Exemple
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodages acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>

Acceptation de la langue	Langues acceptables pour la réponse	Accept-Language : en-US
Plages d'acceptation	Types de plages de contenu partiel pris en charge par ce serveur	Accept-Ranges : bytes
Autorisation	Données d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==.
Charge-To	Contient des informations comptables relatives aux coûts de l'application de la méthode demandée.	
Content-Encoding	Le type d'encodage utilisé pour les données.	Content-Encoding : gzip
Longueur du contenu	Longueur du corps de la réponse en octets (octets de 8 bits)	Content-Length : 348
Content-Type	Le type de mime du corps de la requête (utilisé avec les requêtes POST et PUT)	Content-Type : application/x-www-form-urlencoded
Cookie	un cookie HTTP précédemment envoyé par le serveur avec Set-Cookie (ci-dessous)	Cookie : $Version=1 ; Skin=new ;
Date	Date et heure auxquelles le message a été émis	Date = "Date" " :" HTTP-date
ETag	Identifiant d'une version spécifique d'une ressource, souvent un condensé de message.	ETag : "aed6bdb8e090cd1:0"
De	L'adresse électronique de l'utilisateur qui fait la demande	De : user@example.com
Si modifié depuis	Permet de renvoyer un message 304 Non modifié si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	Date de la dernière modification de l'objet demandé, au format RFC 2822	Dernière modification : Tue, 15 Nov 1994 12:45:26 GMT
Pragma	En-têtes spécifiques à la mise en œuvre qui peuvent avoir divers effets tout au long de la chaîne demande-réponse.	Pragma : no-cache
Référent	Il s'agit de l'adresse de la page web précédente à partir de laquelle un lien vers la page actuellement demandée a été suivi	Référent : HTTP://www.edgenexus.io
Serveur	Un nom pour le serveur	Serveur : Apache/2.4.1 (Unix)
Set-Cookie	un cookie HTTP	Set-Cookie : UserID=JohnDoe ; Max-Age=3600 ; Version=1
User-Agent	Chaîne de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Variable	Indique aux aux serveurs mandataires en aval comment faire correspondre les futurs en-têtes de requête pour décider si la réponse mise en cache peut être utilisée plutôt que d'en demander une nouvelle au serveur d'origine. au serveur d'origine	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple ASP.NET, PHP, JBoss) qui supporte l'application web.	X-Powered-By : PHP/5.4.0

Action

L'action est la ou les tâches qui sont activées lorsque la ou les conditions sont remplies.



Action

Double-cliquez sur la colonne Action pour afficher la liste déroulante.

Cible

Double-cliquez sur la colonne Cible pour afficher la liste déroulante. La liste change en fonction de l'action.

Vous pouvez également taper manuellement avec certaines actions.

Données

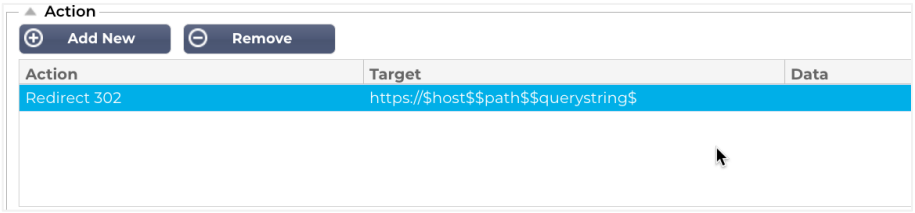
Double-cliquez sur la colonne Données pour ajouter manuellement les données que vous souhaitez ajouter ou remplacer.

La liste de toutes les actions est détaillée ci-dessous :

Action	Description	Exemple
Ajouter un cookie de demande	Ajouter le cookie de demande détaillé dans la section Cible avec la valeur dans la section Données	Cible= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter un en-tête de demande	Ajouter un en-tête de requête de type Target avec une valeur dans la section Data	Cible= Accepter Données= image/png
Ajouter un cookie de réponse	Ajouter le cookie de réponse détaillé dans la section Cible avec la valeur dans la section Données	Cible= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter un en-tête de réponse	Ajouter l'en-tête de la demande détaillé dans la section Target avec la valeur dans la section Data	Target= Cache-Control Données= max-age=8888888
Corps Remplacer tout	Rechercher dans le corps de la réponse et remplacer toutes les instances	Cible= HTTP:// (Chaîne de recherche) Data= HTTPs:// (chaîne de remplacement)
Remplacer le corps d'abord	Rechercher l'élément de réponse et remplacer la première instance uniquement	Cible= HTTP:// (Chaîne de recherche) Data= HTTPs:// (chaîne de remplacement)
Corps Remplacer le dernier	Rechercher le corps de la réponse et remplacer la dernière instance uniquement	Cible= HTTP:// (Chaîne de recherche) Data= HTTPs:// (chaîne de remplacement)
Chute	La connexion sera interrompue	Objectif= N/A Données= N/A
Courriel	Permet d'envoyer un courrier électronique à l'adresse configurée dans les événements de courrier électronique.	Target= "flightPATH a envoyé cet événement par courriel" Données= N/A

	Vous pouvez utiliser une variable comme adresse ou comme message.	
Événement de journal	Cela permet d'enregistrer un événement dans le journal du système	Target= "flightPATH a enregistré ceci dans le syslog" Données= N/A
Redirection 301	Cette opération entraînera une redirection permanente	Cible= HTTP://www.edgenexus.io Données= N/A
Redirection 302	Cette opération entraîne une redirection temporaire	Cible= HTTP://www.edgenexus.io Données= N/A
Supprimer le cookie de demande	Supprimer le cookie de demande détaillé dans la section Cible	Cible= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Supprimer l'en-tête de la demande	Supprimer l'en-tête de la demande détaillé dans la section Cible	Cible=Serveur Données=N/A
Supprimer le cookie de réponse	Supprimer le cookie de réponse décrit dans la section Cible	Cible=jnAccel
Supprimer l'en-tête de réponse	Supprimer l'en-tête de réponse détaillé dans la section Target	Cible= Etag Données= N/A
Remplacer le cookie de demande	Remplacer le cookie de demande détaillé dans la section Cible par la valeur indiquée dans la section Données	Cible= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remplacer l'en-tête de la demande	Remplacer l'en-tête de la requête dans la cible par la valeur des données	Cible= Connexion Données= keep-alive
Remplacer le cookie de réponse	Remplacer le cookie de réponse indiqué dans la section "Cible" par la valeur indiquée dans la section "Données".	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
Remplacer l'en-tête de la réponse	Remplacer l'en-tête de réponse détaillé dans la section "Target" par la valeur de la section "Data".	Cible= Serveur Données= non divulguées pour des raisons de sécurité
Chemin de réécriture	Cela vous permettra de rediriger la demande vers une nouvelle URL en fonction de la condition suivante	Target= /test/path/index.html$querystring$ (Cible= /test/path/index.html$querystring$) Données= N/A
Utiliser un serveur sécurisé	Sélectionner le serveur sécurisé ou le service virtuel à utiliser	Target=192.168.101:443 Données=N/A
Utiliser le serveur	Sélectionner le serveur ou le service virtuel à utiliser	Cible= 192.168.101:80 Données= N/A
Cryptage du cookie	Cela permet de crypter les cookies en 3DES et de les encoder en base64.	Target= Entrez le nom du cookie à crypter, vous pouvez utiliser * comme joker à la fin. Data= Saisir une phrase de passe pour le cryptage

Exemple :



L'action ci-dessous redirige temporairement le navigateur vers un service virtuel HTTPS sécurisé. Elle utilisera le même nom d'hôte, le même chemin d'accès et la même chaîne de requête que la demande.

Utilisations courantes

Pare-feu et sécurité des applications

- Bloquer les IP indésirables
- Obliger l'utilisateur à utiliser HTTPS pour un contenu spécifique (ou pour l'ensemble du contenu)
- Bloquer ou rediriger les spiders
- Prévenir et alerter les scripts intersites
- Prévenir et alerter les injections SQL
- Masquer la structure interne des répertoires
- Réécriture des cookies
- Répertoire sécurisé pour des utilisateurs particuliers

Caractéristiques

- Rediriger les utilisateurs en fonction du chemin d'accès
- Fournir une signature unique sur plusieurs systèmes
- Segmenter les utilisateurs en fonction de l'identifiant ou du cookie
- Ajouter des en-têtes pour le délestage de SSL
- Détection des langues
- Réécrire la demande de l'utilisateur
- Corriger les URL cassés
- Enregistrement et alerte par courrier électronique des codes de réponse 404
- Empêcher l'accès aux répertoires/la navigation
- Envoyer un contenu différent aux robots d'indexation

Règles préétablies

Extension HTML

Remplace toutes les requêtes .htm par des requêtes .html

État :

- Condition = Chemin
- Sens = Fait
- Check = Match RegEx
- Valeur = \.htm$

Évaluation :

- Blanc

Action :

- Action = Réécrire le chemin
- Cible = $path$l

Index.html

Oblige à utiliser index.html dans les requêtes vers les dossiers.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = Hôte
- Sens = Fait
- Vérifier = Exister

Évaluation :

- Blanc

Action :

- Action = Redirection 302
- Cible = HTTP://$host$$path$index.html$querystring$

Fermer les dossiers

Refuser les demandes de dossiers.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = cela nécessite une réflexion approfondie
- Sens =
- Vérifier =

Évaluation :

- Blanc

Action :

- Action =
- Cible =

Masquer CGI-BBIN :

Cache le catalogue cgi-bin dans les requêtes adressées aux scripts CGI.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = Hôte
- Sens = Fait
- Check = Correspondance RegEX
- Valeur = \.cgi$

Évaluation :

- Blanc

Action :

- Action = Réécrire le chemin
- Cible = /cgi-bin$chemin$

Araignée de mer

Enregistrer les requêtes des moteurs de recherche les plus populaires.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = En-tête de la demande
- Correspondance = User-Agent

- Sens = Fait
- Check = Correspondance RegEX
- Valeur = Googlebot|Slurp|bingbot|ia_archiver

Évaluation :

- Variable = $crawler$
- Source = En-tête de la demande
- Détail = User-Agent

Action :

- Action = Enregistrer l'événement
- Cible = [$crawler$] $host$$path$$querystring$

Forcer HTTPS

Oblige à utiliser HTTPS pour certains répertoires. Dans ce cas, si un client accède à quelque chose contenant le répertoire /secure/, il sera redirigé vers la version HTTPs de l'URL demandée.

État :

- Condition = Chemin
- Sens = Fait
- Vérifier = Contenir
- Valeur = /secure/

Évaluation :

- Blanc

Action :

- Action = Redirection 302
- Cible = HTTPs://$host$$path$$querystring$ (en anglais)

Media Stream :

Redirige le flux multimédia Flash vers le service approprié.

État :

- Condition = Chemin
- Sens = Fait
- Vérification = Fin
- Valeur = .flv

Évaluation :

- Blanc

Action :

- Action = Redirection 302
- Cible = HTTP://$host$:8080/$path$

Passer de HTTP à HTTPS

Remplacer les codes en dur HTTP:// par HTTPS://

État :

- Condition = Code de réponse
- Sens = Fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- Blanc

Action :

- Action = Corps Remplacer tout
- Cible = HTTP://
- Données = HTTPs://

Effacer les cartes de crédit

Vérifiez qu'il n'y a pas de carte de crédit dans la réponse et, si c'est le cas, effacez-la.

État :

- Condition = Code de réponse
- Sens = Fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- Blanc

Action :

- Action = Corps Remplacer tout
- Target = [0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+-[0-9]+[0-9]+[0-9]+[0-9]+
- Données = xxxx-xxxx-xxxx-xxxx

Expiration du contenu

Ajoutez une date d'expiration raisonnable au contenu de la page pour réduire le nombre de requêtes et de 304.

Condition : il s'agit d'une condition générique qui sert de fourre-tout. Il est recommandé d'axer cette condition sur votre

- Condition = Code de réponse
- Sens = Fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- Blanc

Action :

- Action = Ajouter un en-tête de réponse
- Cible = Cache-Control
- Données = max-age=3600

Type de serveur d'espionnage

Obtenez le type de serveur et changez-le en quelque chose d'autre.

Condition : il s'agit d'une condition générique qui sert de fourre-tout. Il est recommandé d'axer cette condition sur votre

- Condition = Code de réponse
- Sens = Fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- Blanc

Action :

- Action = Remplacer l'en-tête de la réponse
- Cible = Serveur
- Données = Secrètes

Ne jamais envoyer d'erreurs

Le client ne reçoit jamais d'erreurs de votre site.

Condition

- Condition = Code de réponse
- Sens = Fait
- Vérifier = Contenir
- Valeur = 404

L'évaluation

- Blanc

Action

- Action = Redirection 302
- Cible = HTTP//$host$/

Redirection sur la langue

Trouvez le code de la langue et redirigez vers le domaine du pays concerné.

Condition

- Condition = Langue
- Sens = Fait
- Vérifier = Contenir
- Valeur = allemand (standard)

L'évaluation

- Variable = $host_template$
- Source = Hôte
- Valeur = .*\.

Action

- Action = Redirection 302
- Cible = HTTP//$host_template$de$path$$querystring$ (en anglais)

Google Analytics

Insérez le code requis par Google pour l'analyse - Remplacez la valeur MYGOOGLECODE par votre Google UA ID.

Condition

- Condition = Code de réponse
- Sens = Fait
- Contrôle = égal
- Valeur = 200 OK

L'évaluation

- vierge

Action

- Action = Corps Remplacer le dernier
- Cible = </body>
- Données = <script type='text/javascript'> var _gaq = _gaq || [] ; _gaq.push(['_setAccount', 'MY GOOGLE CODE']) ; _gaq.push(['_trackPageview']) ; (function() { var ga = document.createElement('script') ; ga.type = 'text/javascript' ; ga.async = true ; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js' ; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s) ; })() ; </script> </body>

Passerelle IPv6

Ajuster l'en-tête de l'hôte pour les serveurs IIS IPv4 sur les services IPv6. Les serveurs IIS IPv4 n'apprécient pas de voir une adresse IPV6 dans la requête du client hôte. Cette règle remplace donc cette adresse par un nom générique.

Condition

- vierge

L'évaluation

- vierge

Action

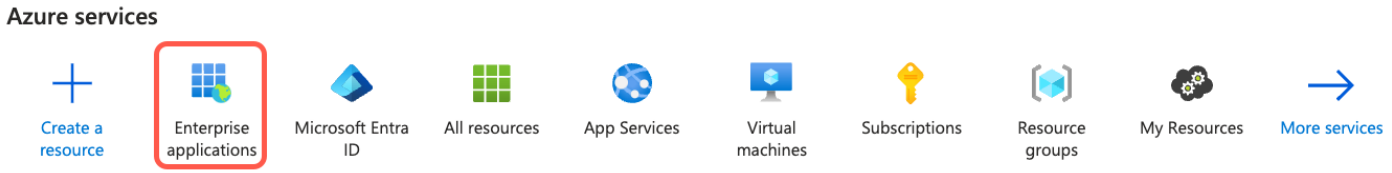
- Action = Remplacer l'en-tête de la demande
- Cible = hôte
- Données =ipv4.host.header

SAML et Entra ID

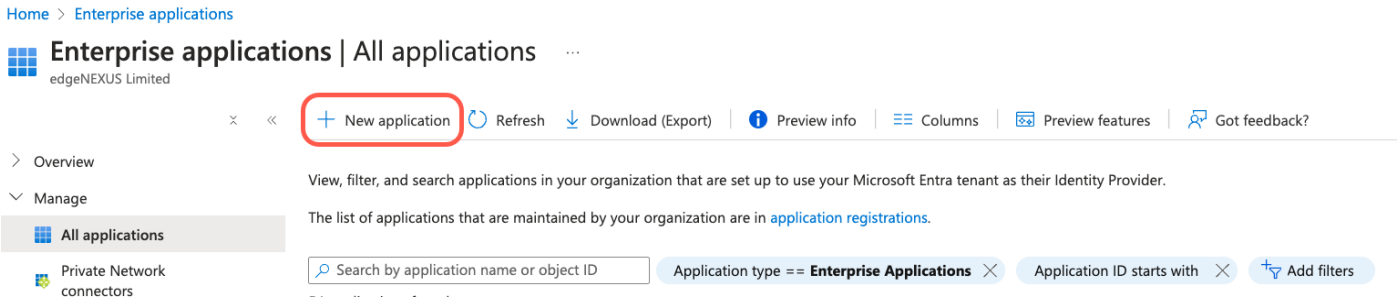
Configuration de l'application d'authentification Entra ID dans Microsoft Entra

Pour que l'authentification SAML fonctionne correctement, vous devez configurer une application d'entreprise dans votre portail Microsoft Entra Admin. Il s'agit d'une tâche simple qui permet de fournir le certificat de signature nécessaire pour les demandes d'authentification SAML et les jetons, ainsi que les données XML de configuration.

Pour ce faire, vous devez d'abord vous connecter à votre portail Microsoft Entra (https://portal.azure.com) et vous assurer que vous êtes sur la page Azure Services où vous trouverez une liste d'icônes en haut de la page (voir ci-dessous).

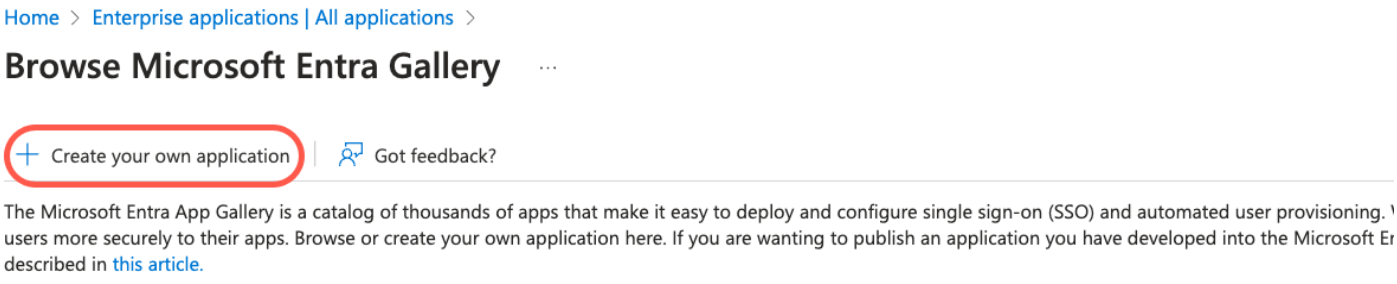


- Cliquez sur Applications d'entreprise. Si vous ne voyez pas Enterprise Applications dans la liste des icônes, vous pouvez saisir le nom dans la barre de recherche en haut. Une page s'affiche alors, comme indiqué ci-dessous.

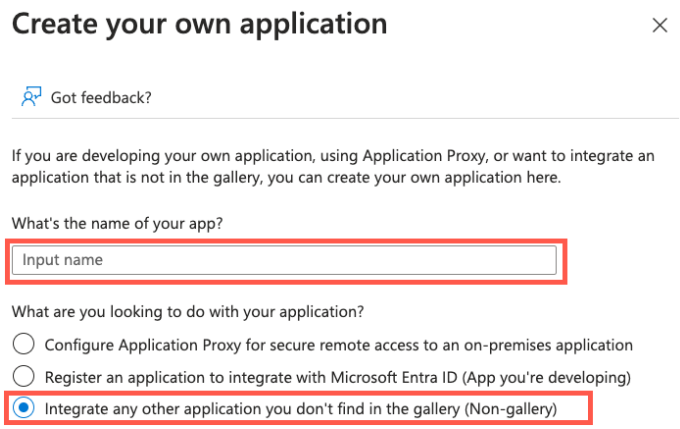


Cliquez sur *Nouvelle demande*

Dans la page suivante, cliquez sur *Créer votre propre application*.

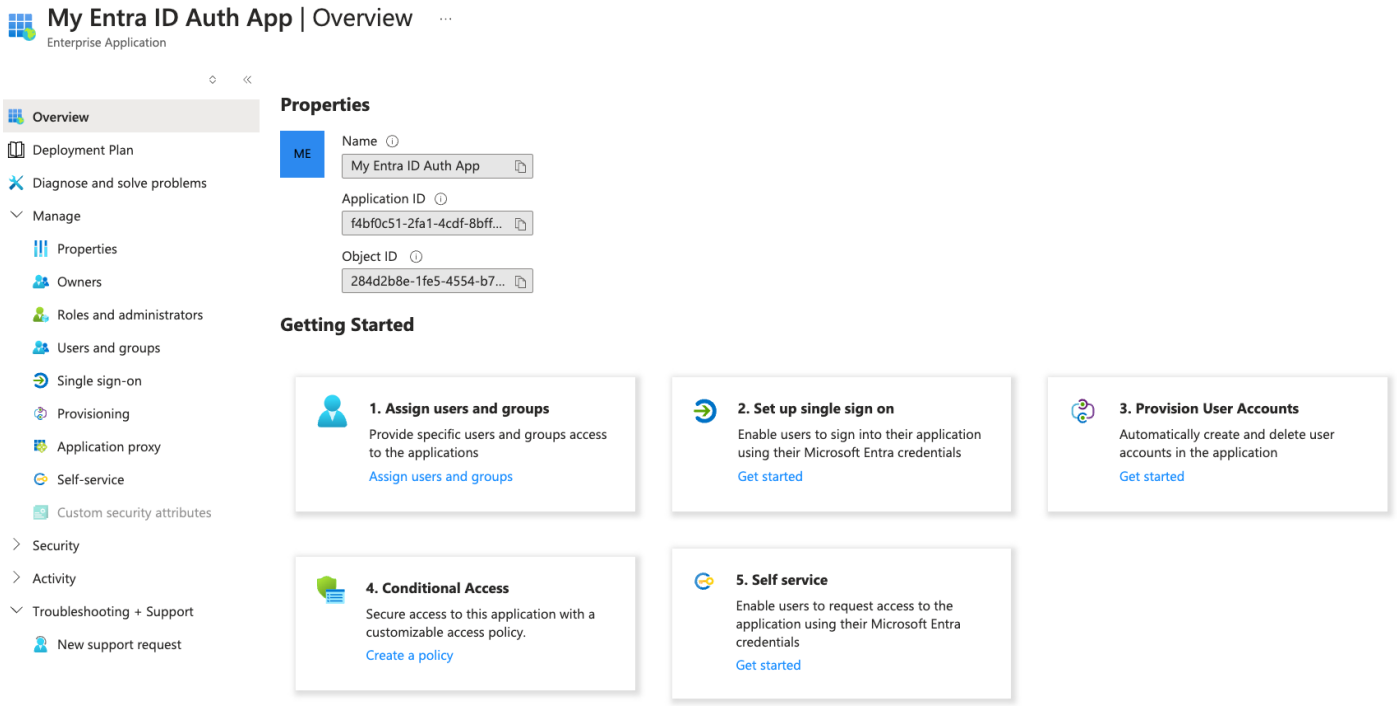


- Une section intitulée "*Créez votre propre application*" s'ouvre sur le côté droit de la page.

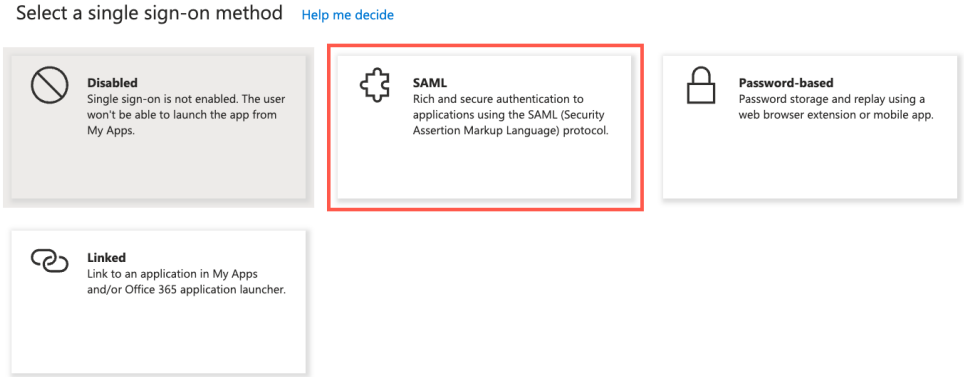


- Donnez un nom à votre application, par exemple "My Entra ID Auth App". Vous pouvez choisir le nom que vous souhaitez.
- Cliquez sur le bouton radio *Intégrer toute autre application que vous ne trouvez pas dans la galerie (Non-galerie).*
- Cliquez sur le bouton *Créer.*

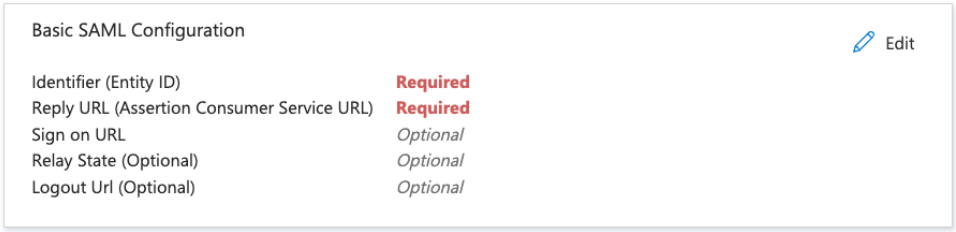
Une page ressemblant à celle ci-dessous s'affiche.



- Cliquez sur l'option Single Sign-on située dans la barre de navigation de gauche.
- Sélectionnez la case SAML



- Vous verrez maintenant une page contenant la section pour la configuration de base de SAML.



- Dans la zone Configuration SAML de base, remplissez :
  - Identifiant (ID de l'entité)
  - URL de réponse (URL du service consommateur d'assertion)
  - URL de connexion
  - URL de déconnexion (facultatif)
- Sauvegardez votre configuration et testez l'application.

Pour des conseils plus détaillés, vous pouvez vous référer à la documentation Enable single sign-on for an enterprise application (Activer l'authentification unique pour une application d'entreprise) sur le site de Microsoft.

Support technique

Nous fournissons une assistance technique à tous nos utilisateurs conformément aux conditions de service standard de l'entreprise.

Nous vous fournirons une assistance technique si vous avez un contrat d'assistance et de maintenance actif pour l'EdgeADC, l'EdgeWAF ou l'EdgeGSLB.

Pour déposer un ticket d'assistance, veuillez visiter le site :

https://www.edgenexus.io/support/