EdgeADC

GUIDE DE L'ADMINISTRATION

Table des matières

Propriétés du document

Numéro du document : 2.0.5.20.21.12.05

Date de création du document : 30 avril 2021

Dernière modification du document : 20 mai 2021

Auteur du document : Jay Savoor

Document Dernière modification par :

Renvoi du document : EdgeADC - Version 4.2.7.1890

Avis de non-responsabilité

Les captures d'écran et les graphiques de ce manuel peuvent différer légèrement de votre produit en raison des différences de version de votre produit. Edgenexus assure qu'il fait tous les efforts raisonnables pour s'assurer que les informations contenues dans ce document sont complètes et précises. Edgenexus n'assume aucune responsabilité en cas d'erreur. Edgenexus apportera des modifications et des corrections aux informations contenues dans ce document dans les prochaines versions lorsque le besoin s'en fera sentir.

Droits d'auteur

Marques commerciales

Le logo Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS sont tous des marques 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 créer un ticket d'assistance à l'adresse suivante : support@edgenexus.io.

Installation de l'EdgeADC

Le produit EdgeADC (appelé ADC à partir de maintenant) peut être installé de plusieurs manières. Chaque plateforme cible nécessite son propre installateur, et ceux-ci sont tous à votre disposition.

Voici les différents modèles d'installation disponibles.

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oracle VM
- 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.

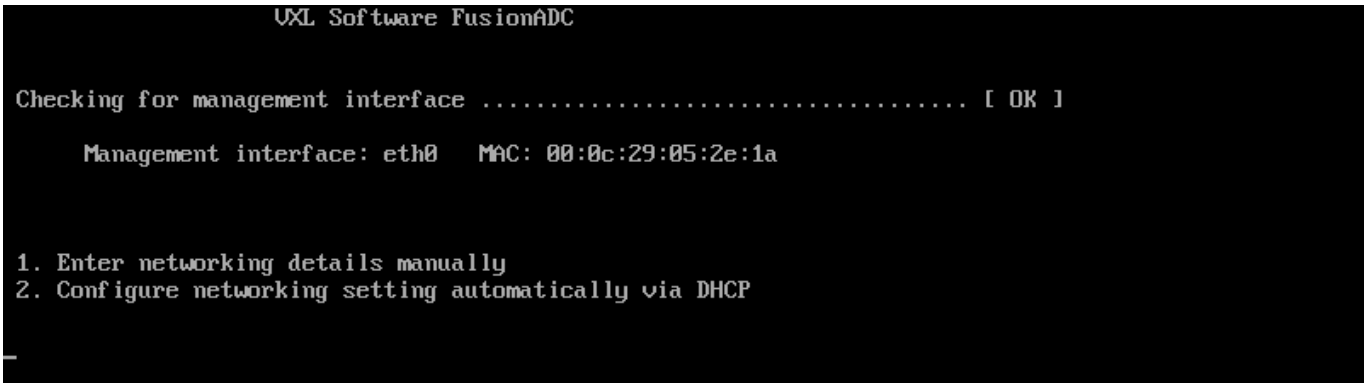
VMware ESXi

ADC est disponible pour une installation sur VMware ESXi are 5.x et plus.

- Téléchargez le dernier paquet OVA d'installation de l'ADC en utilisant le lien approprié fourni avec l'email de téléchargement.
- Une fois téléchargé, veuillez le décompresser dans un répertoire approprié sur votre hôte ESXi ou SAN.
- Dans votre client vSphere, sélectionnez Fichier : Déployer un modèle OVA/OVF.
- Parcourez et sélectionnez l'emplacement où vous avez sauvegardé vos fichiers ; choisissez le fichier OVF et cliquez sur **NEXT.**
- Le serveur ESX demande le nom de l'appliance. Tapez un nom approprié et cliquez sur **NEXT**
- Sélectionnez le datastore à partir duquel votre appliance ADC sera exécutée.
- Sélectionnez un datastore avec suffisamment d'espace et cliquez sur **NEXT.**
- Vous obtiendrez alors des informations sur le produit ; cliquez sur **SUIVANT.**
- Cliquez sur **NEXT.**
- Une fois que vous avez copié les fichiers sur le datastore, 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 allez à Power > Power-On.
- Votre VA démarrera alors, et l'écran de démarrage de l'ADC s'affichera sur la console.



Veuillez vous reporter à la section **CONFIGURATION DU PREMIER DÉMARRAGE** pour poursuivre.

Installation de l'interface VMXNET3

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

***Remarque** - Ne mettez PAS à niveau le logiciel VMware-tools*

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

1. Supprimez les deux NICs de la VM
2. Mettre à niveau le matériel de la VM - -Cliquez avec le bouton droit de la souris sur le VA 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. Ajoutez deux NICs et sélectionnez-les pour être VMXNET3.
4. Démarrez le VA en utilisant la méthode standard. Il fonctionnera avec le VMXNET3

Activation de l'interface VMXNET3 sur un VA déjà en fonctionnement

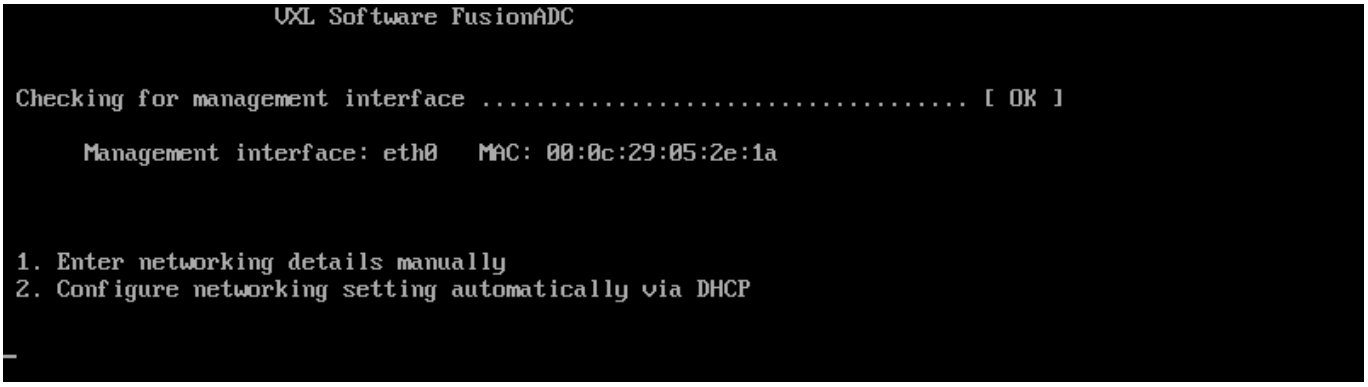
1. Arrêter la VM (commande CLI shutdown ou GUI power-off)
2. Obtenez les adresses MAC des deux cartes réseau (n'oubliez pas l'ordre des cartes dans la liste !).
3. Supprimez les deux NICs de la VM
4. Mettez à niveau le matériel de la VM (ne lancez pas l'installation ou la mise à jour des outils VMware, effectuez **uniquement la** mise à niveau du matériel).
5. Ajouter deux NICs et les sélectionner pour être VMXNET3
6. Définissez les adresses MAC pour les nouvelles cartes réseau conformément à l'étape 2.
7. Redémarrer le VA

Nous prenons en charge VMware ESXi comme plate-forme de production. À des fins d'évaluation, vous pouvez utiliser VMware Workstation et Player.

Microsoft Hyper-V

L'appliance virtuelle ADC est compatible avec une installation sur un serveur Microsoft Hyper-V.

- Extrayez le fichier zip Hyper-V ADC VA sur votre machine ou serveur local.
- Ouvrez le gestionnaire Hyper-V.
- Dans votre gestionnaire Hyper-V, cliquez avec le bouton droit de la souris sur le serveur et sélectionnez **"Importer une machine virtuelle".**
- Naviguez jusqu'au dossier contenant les fichiers ADC Hyper-V.
- Cliquez sur **"Copier la machine virtuelle (créer un nouvel identifiant unique)".**
- Cochez la case pour **"Dupliquer tous les fichiers afin que la même machine virtuelle puisse être importée à nouveau".**
- Cliquez sur **"Importer".**
- Votre machine importe avec le nom **"ADC ADC VA pour Hyper-V".**
- Assurez-vous que vous sélectionnez le bon réseau sur la carte réseau.
- Si vous installez plus d'un appareil virtuel, vous devrez configurer chaque appareil avec une adresse MAC unique.
- Cliquez à droite sur la machine virtuelle que vous venez de créer et cliquez sur **"Connecter".**
- Cliquez sur le bouton vert Démarrer ou cliquez sur **"ActionStart".**
- Votre VA va démarrer, et l'écran de la console ADC va s'afficher.



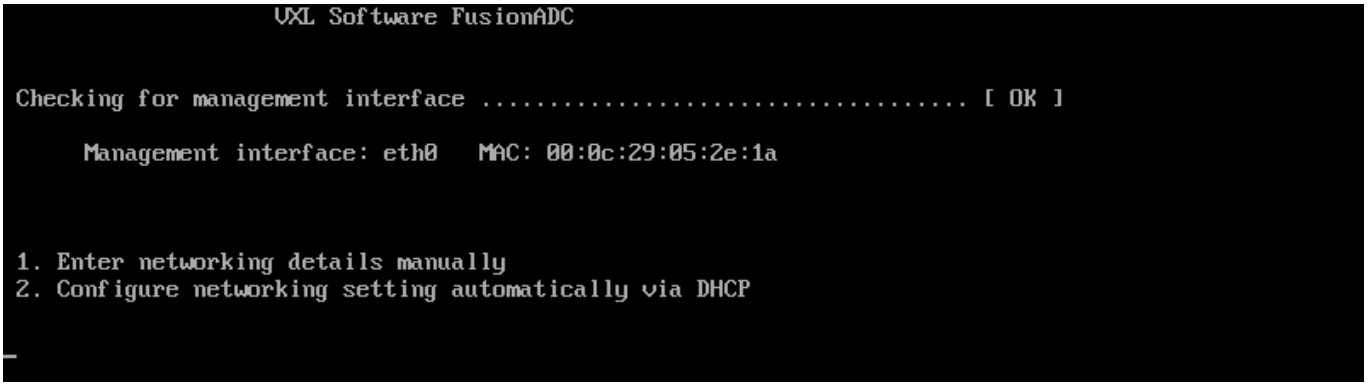
- Une fois que vous avez configuré les propriétés du réseau, le VA redémarre et présente la connexion à la console du VA.

Veuillez vous reporter à la section **CONFIGURATION DU PREMIER DÉMARRAGE** pour poursuivre.

Citrix XenServer

L'appliance virtuelle ADC est installable 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".**
- Naviguez jusqu'au fichier **OVA** et sélectionnez-le, puis cliquez sur "**Open Next".**
- Sélectionnez l'emplacement de création de la VM lorsqu'on vous le demande.
- Choisissez le XenServer que vous souhaitez installer et cliquez sur "**SUIVANT".**
- Sélectionnez le référentiel de stockage (SR) pour le placement du disque virtuel lorsqu'on vous le demande.
- Sélectionnez un SR avec suffisamment d'espace et cliquez sur "**SUIVANT".**
- Mettez en correspondance vos interfaces de réseau virtuel. Les deux interfaces porteront la mention Eth0 ; cependant, notez que l'interface du bas est Eth1.
- Sélectionnez le réseau cible pour chaque interface et cliquez sur **NEXT.**
- **NE PAS** cocher la case "Utiliser le correcteur de 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 détails d'adresse IP statiques si vous ne disposez pas d'un serveur DHCP fonctionnel pour le transfert. Si vous ne le faites pas, l'importation indiquera "Connecting continuously" puis "failed". Cliquez sur "**SUIVANT".**
- Revoyez toutes les informations et vérifiez ensuite les paramètres corrects. Cliquez sur "**FINISH".**
- Votre VM commencera à transférer le disque virtuel "ADC ADC" et, une fois terminé, il apparaîtra sous votre XenServer.
- Dans votre client XenCenter, vous pourrez maintenant voir la nouvelle machine virtuelle. Cliquez avec le bouton droit de la souris sur la VA et cliquez sur "**START**".
- Votre VM démarrera alors, et l'écran de démarrage de l'ADC s'affichera.



- Une fois configuré, la connexion au VA se présente.

Veuillez vous reporter à la section **CONFIGURATION DU PREMIER DÉMARRAGE** pour poursuivre.

Configuration du premier démarrage

Au premier démarrage, l'ADC VA affiche l'écran suivant demandant la configuration pour les opérations de production.

Premier démarrage - Détails du réseau manuel

Au premier démarrage, vous aurez 10 secondes pour interrompre l'attribution automatique des coordonnées IP via DHCP

Pour interrompre ce processus, cliquez dans la fenêtre de la console et appuyez sur n'importe quelle touche. Vous pouvez alors entrer les détails suivants manuellement.

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

Ces changements sont persistants et survivront à un redémarrage. Il n'est pas nécessaire de les configurer à nouveau sur le VA.

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 ne pas utiliser le VA ADC en utilisant une adresse DHCP à moins que cette adresse IP ne soit liée de façon permanente à l'adresse MAC du VA dans le serveur DHCP. Nous vous conseillons toujours d'utiliser une **ADRESSE IP FIXE** lorsque vous utilisez le VA. 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 - DHCP échoue

Si vous ne disposez pas d'un 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 le VA trouve une adresse IP libre. De même, le VA

vérifiera si l'adresse IP est actuellement utilisée et, si c'est le cas, il l'incrémentera à nouveau et vérifiera à nouveau.

Changement de l'adresse IP de gestion

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

```
Command:set greenside=192.168.101.1_
```

Changer le 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 net peut être modifié à l'aide de la commande **set mask eth0 n.n.n.n**. Vous pouvez voir un exemple ci-dessous.

```
Command:set mask eth0 255.255.255.0_
```

Attribution d'une passerelle par défaut

Le VA a besoin d'une passerelle par défaut pour ses opérations. Pour définir la passerelle par défaut, utilisez la commande **route add default gw n.n.n.n** comme indiqué dans l'exemple ci-dessous.

```
Command:route add default gw 192.168.101.254_
```

Vérification de la valeur de la passerelle par défaut

Pour vérifier si la passerelle par défaut est ajoutée et si elle est correcte, utilisez la commande **route**. Cette commande affiche les routes 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 l'ADC pour 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 utilisation opérationnelle.

Dans le champ URL du navigateur, tapez soit **HTTPS://{ADRESSEIP}, soit HTTPS://{FQDN}.**

Par défaut, le CDA utilise un certificat SSL auto-signé. Vous pouvez modifier le CDA pour utiliser 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 :

Nom d'utilisateur par défaut = **admin** / Mot de passe par défaut = **jetnexus**

Tableau de référence des commandes

Commande	Paramètre1	Paramètre2	Description	Exemple
date			Indique la date et l'heure actuellement configurées	Mar Sept 3 13:00 UTC 2013
Valeurs par défaut			Attribuez les paramètres d'usine par défaut à votre appareil	
quitter			Se déconnecter de l'interface de ligne de commande	
aide			Affiche toutes les commandes valides	
ifconfig	[blanc]		Visualiser la configuration de l'interface pour toutes les interfaces	ifconfig
	eth0		Visualisez la configuration de l'interface de eth0 uniquement	ifconfig eth0
numéro de machine			Cette commande fournira l'identifiant de la machine utilisée pour l'autorisation de l'ADC ADC	EF4-3A35-F79
quitter			Se déconnecter de l'interface de ligne de commande	
redémarrer			Terminer toutes les connexions et redémarrer l'ADC ADC	redémarrer
redémarrer			Redémarrer les services virtuels de l'ADC	
itinéraire	[blanc]		Afficher la table de routage	itinéraire
	ajouter	gw par défaut	Ajouter l'adresse IP de la passerelle par défaut	route add default gw 192.168.100.254
set	greenside		Définir l'adresse IP de gestion pour l'ADC	set greenside=192.168.101.1
	masque		Définit le masque de sous-réseau pour une interface. Les noms d'interface sont eth0, eth1....	set mask eth0 255.255.255.0
montrer			Affiche les paramètres de configuration globale	
arrêt			Terminer toutes les connexions et éteindre l'ADC ADC	
statut			Affiche les statistiques de données actuelles	
top			Voir les informations sur les processus, comme le CPU et la mémoire	
journal	messages		Affiche les messages syslog bruts	Afficher les messages du

d'affichage	journal

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

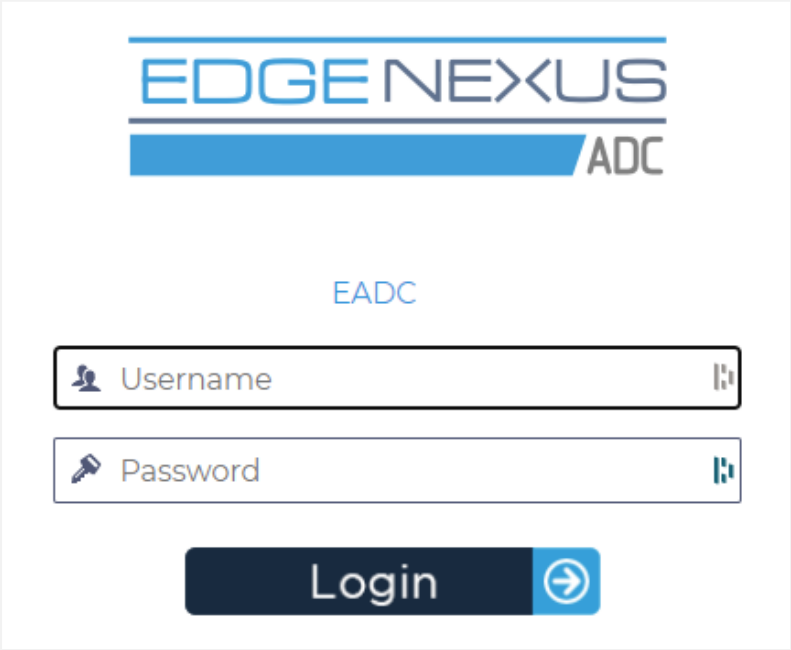
Lancement de la console Web de l'ADC

Toutes les opérations sur le CDA (également appelé CDA) sont configurées et exécutées 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 utiliserons l'exemple de adc.company.com à titre d'exemple :

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.



Identifiants de connexion par défaut

Les identifiants de connexion par défaut sont :

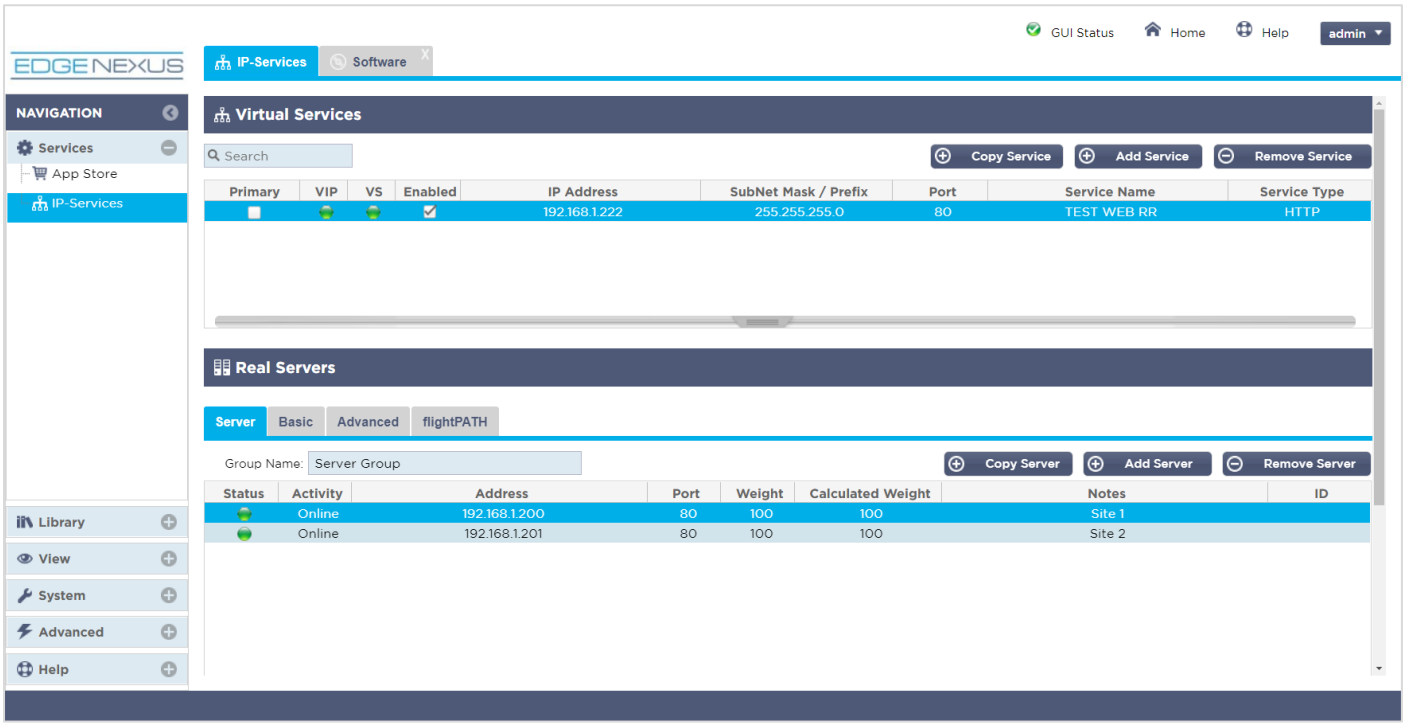
- Nom d'utilisateur : admin
- Mot de passe : jetnexus

Vous pouvez changer cela à tout moment en utilisant les capacités de configuration des utilisateurs situées dans *Système > Utilisateurs*.

Une fois que vous vous êtes connecté avec succès, le tableau de bord principal du CDA s'affiche.

Le tableau de bord principal

L'image ci-dessous illustre l'aspect du tableau de bord principal ou "page d'accueil" du CDA. Nous pouvons apporter quelques changements de temps en temps pour des raisons d'amélioration, mais toutes les fonctions seront conservées.



Pour être aussi concis que possible, nous supposerons que cette première introduction aux sections de l'écran prouvera que vous connaissez suffisamment les différentes sections de la zone de configuration de l'ADC, nous ne les décrirons donc pas en détail au fur et à mesure que nous avancerons mais nous nous concentrerons plutôt sur les éléments de configuration.

En allant de gauche à droite, nous avons d'abord la section Navigation. La section Navigation comprend les différentes zones du CDA. Lorsque vous cliquez sur un choix particulier dans la section Navigation, la section correspondante s'affiche sur le côté droit de l'écran. Vous pouvez également voir la section de configuration choisie sous forme d'onglet en haut de l'écran, à côté du logo du produit. Les onglets permettent une navigation plus rapide vers des zones déjà utilisées de la configuration du CDA.

Services

La section des services du CDA comporte plusieurs domaines. Lorsque vous cliquez sur l'élément Service, celui-ci s'agrandit pour afficher les choix disponibles.

Services IP

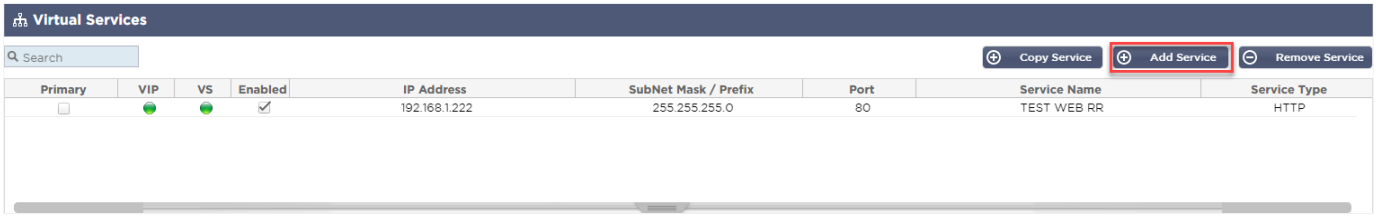
La section Services IP de l'ADC vous permet d'ajouter, de supprimer et de configurer les différents services IP virtuels dont vous avez besoin pour votre cas d'utilisation particulier. Les paramètres et les options sont regroupés dans les sections ci-dessous. Ces sections se trouvent sur le côté droit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

Services virtuels

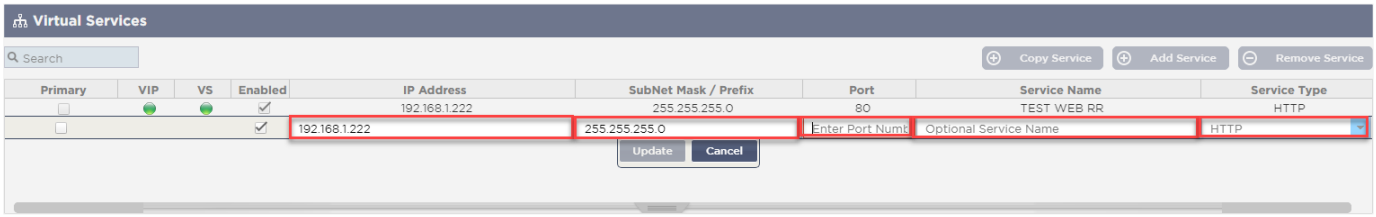
Un service virtuel combine une IP virtuelle (VIP) et un port TCP/UDP sur lequel le CDA écoute. Le trafic arrivant à l'IP du service virtuel est redirigé vers l'un des serveurs réels associés à ce service. L'adresse IP du Service Virtuel ne peut pas être la même que l'adresse de gestion de l'ADC. i.e.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

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

Créer un nouveau service virtuel en utilisant un nouveau VIP



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

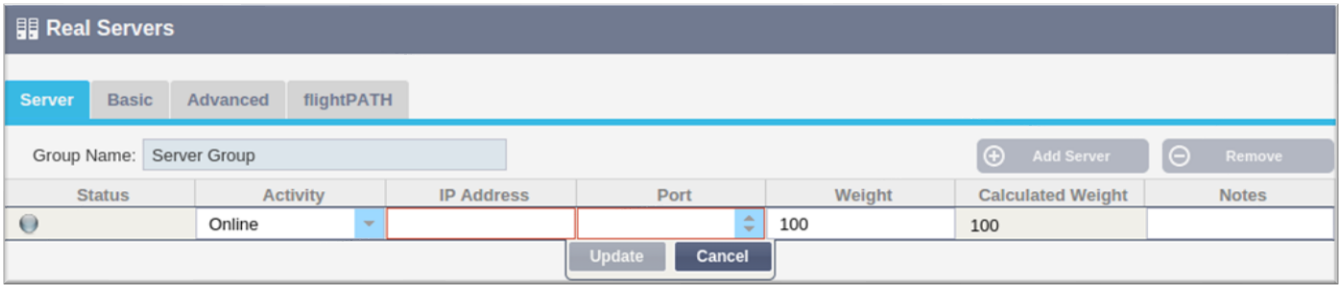


- Vous entrerez alors dans le mode de **modification de la ligne**.
- Remplissez les quatre champs mis en évidence pour continuer, puis cliquez sur le bouton de mise à jour.

Veuillez utiliser la touche TAB pour naviguer dans les champs.

Champ	Description
Adresse IP	Saisissez une nouvelle adresse IP virtuelle qui sera le point d'entrée cible pour accéder au serveur réel. Cette adresse IP est celle vers laquelle les utilisateurs ou les applications se dirigeront pour accéder à l'application équilibrée en termes de charge.
Masque de sous-réseau/Préfixe	Ce champ est réservé au 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 PIV. Il est facultatif, mais nous vous recommandons de le fournir pour plus de clarté.
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.

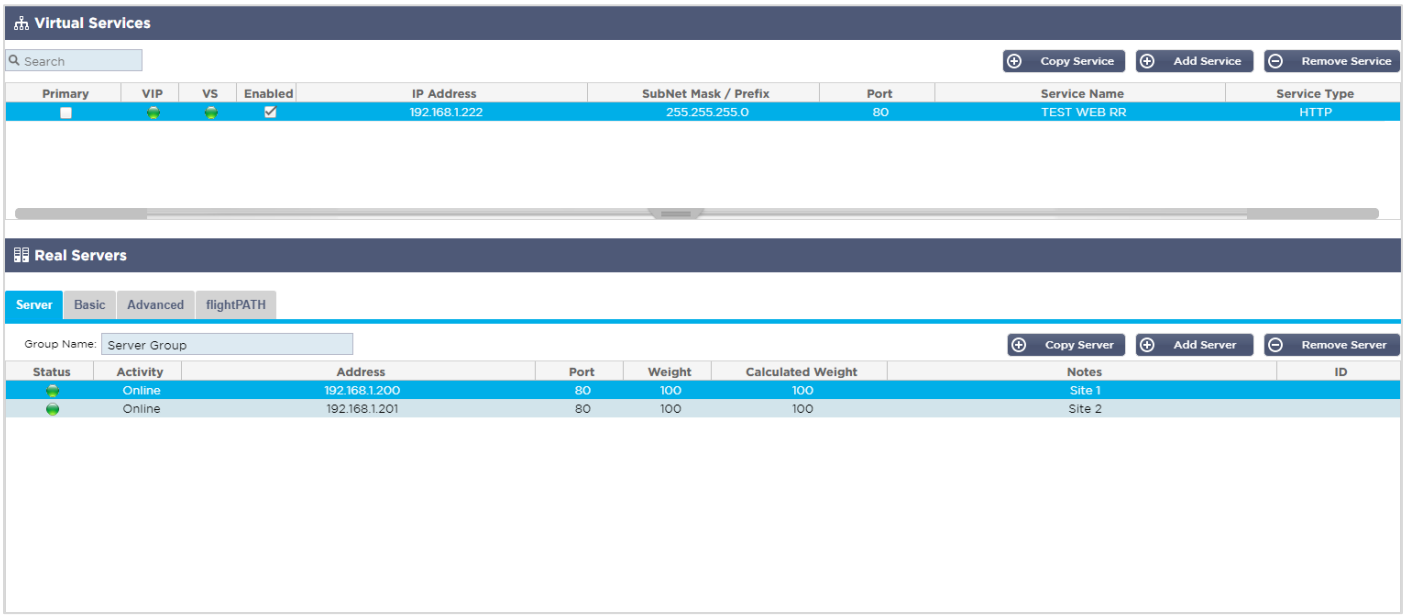
Vous pouvez maintenant appuyer sur le bouton "Update" pour sauvegarder cette section et passer automatiquement à la section "Real Server" détaillée ci-dessous :



Champ	Description
Activité	Le champ Activité peut être utilisé pour afficher et modifier l'état du serveur réel équilibré en charge. En ligne - Indique que le serveur est actif et qu'il reçoit des demandes d'équilibrage de la charge. Hors ligne - Le serveur est hors ligne et ne reçoit pas de demandes. Drain - Le serveur a été placé en mode drain pour que la persistance puisse être vidée et que le serveur passe à un état hors ligne sans affecter les utilisateurs. Standby - Le serveur a été placé dans un état de veille.
Adresse IP	Cette valeur est l'adresse IP du serveur réel. 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 des priorités.

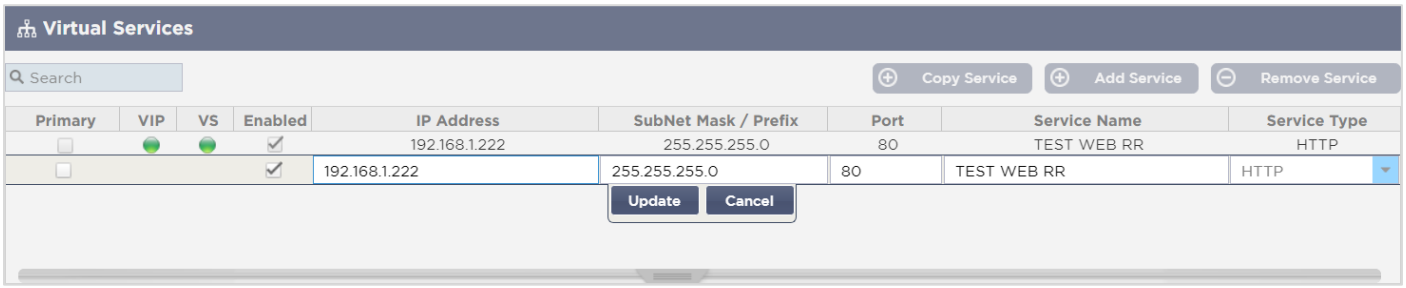
- Cliquez sur le bouton "Update" ou appuyez sur "Enter" pour enregistrer vos modifications.
- Le voyant d'état devient d'abord gris, puis vert si le contrôle de santé du serveur réussit. Il devient rouge si le Real Server Monitor échoue.
- Un serveur dont le voyant d'état est rouge ne sera pas équilibré en termes de charge.

Exemple d'un service virtuel terminé

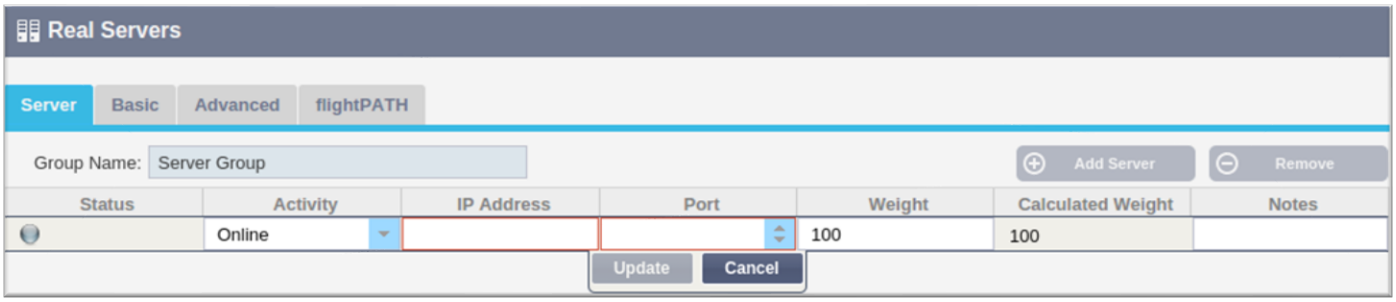


Créer un nouveau service virtuel en utilisant un VIP existant

- Mettez en surbrillance un service virtuel que vous souhaitez copier
- Cliquez sur Add Virtual Service pour entrer dans le mode d'édition de la rangée



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

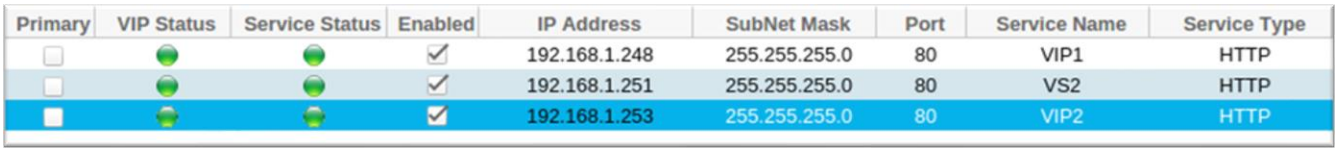


- Laissez l'option Activité du serveur en ligne, ce qui signifie qu'il sera équilibré en charge s'il passe le contrôle de santé par défaut de TCP Connect. Ce paramètre peut être modifié ultérieurement si nécessaire.
- Entrez une adresse IP du serveur réel
- Entrez un numéro de port pour le serveur réel
- Saisissez un nom facultatif pour le serveur réel
- Cliquez sur Mettre à jour 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 ne sera pas équilibré en termes de charge.

Changement de l'adresse IP d'un service virtuel

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

- Mettez en surbrillance le service virtuel dont vous souhaitez modifier l'adresse IP.



- Double-cliquez sur le champ de l'adresse IP de ce service

- Changez l'adresse IP pour 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

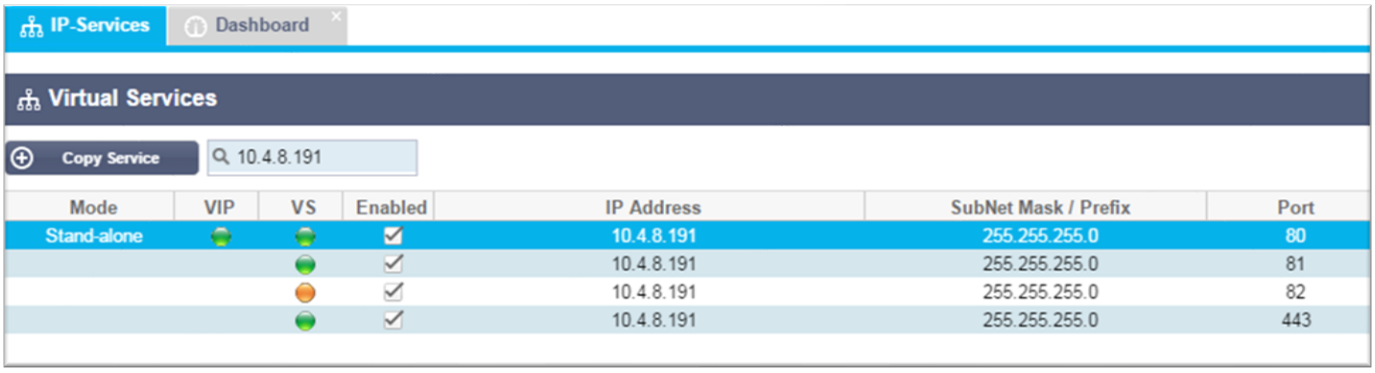
- Le bouton Copier le service permet de copier un service entier, y compris tous les serveurs réels, les paramètres de base, les paramètres avancés et les règles du chemin de vol qui lui sont associés.
- Mettez en surbrillance le service que vous souhaitez dupliquer et cliquez sur "Copier le service".
- 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 politique d'équilibrage de charge, le moniteur Real Server ou si vous supprimez une règle flightPATH.

Filtrage des données affichées

Recherche d'un terme spécifique

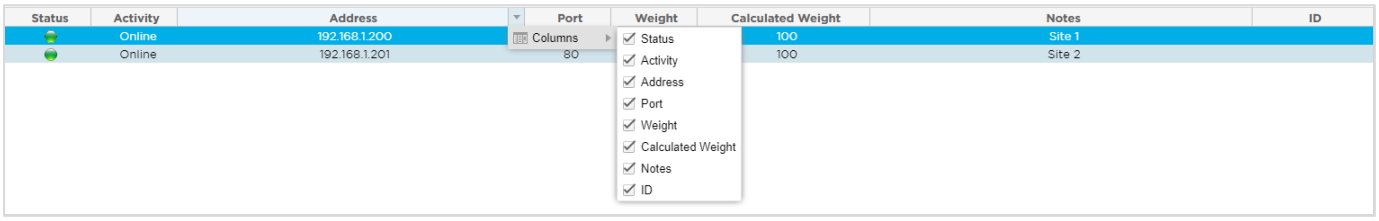
La boîte de recherche vous permet d'effectuer une recherche dans la table en utilisant n'importe quelle valeur, comme les octets de l'adresse IP ou le nom du service.



L'exemple ci-dessus montre le résultat de la recherche d'une adresse IP spécifique de 10.4.8.191.

Sélection de la visibilité des colonnes

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

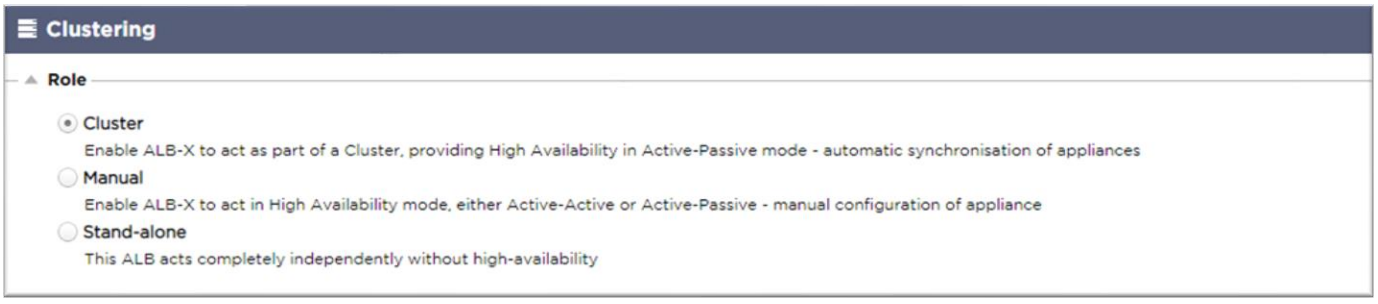


- Déplacez la souris sur l'une des colonnes
- Vous verrez apparaître une petite flèche sur le côté droit de la colonne.
- En cliquant sur les cases à cocher, vous sélectionnez les colonnes que vous souhaitez voir apparaître dans le tableau de bord.

Comprendre les colonnes de services virtuels

Primaire/Mode

La colonne Primary/Mode indique le rôle de haute disponibilité sélectionné pour le VIP actuel. Utilisez les options disponibles dans Système > Clustering pour configurer cette option.



Option	Description
Cluster	Cluster est le rôle par défaut de l'ADC lors de l'installation, et la colonne Primary/Mode indique le mode dans lequel il fonctionne actuellement. Lorsque vous avez une paire d'appareils ADC HA dans votre centre de données, l'un d'entre eux affichera Active et l'autre Passive.
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 Primary contient une case à côté de chaque adresse IP virtuelle unique qui peut être cochée pour Active ou non cochée pour Passive.
Stand-Alone	L'ADC agit comme un dispositif autonome et n'est pas en mode haute disponibilité. En tant que tel, la colonne Primary indiquera Stand-alone.

VIP

Cette colonne fournit un retour visuel 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".

●	Service Needs attention. Cette indication peut être due au fait qu'un serveur réel a échoué à un contrôle de santé ou qu'il a été mis manuellement 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.
●	Statut de la recherche
●	Pas de licence ou des IP virtuelles sous licence dépassées

Activé

La valeur par défaut de cette option est Activé, et la case à cocher est cochée. Vous pouvez désactiver le service virtuel en double-cliquant sur la ligne, en décochant la case, puis en cliquant sur le bouton Actualiser.

Adresse IP

Ajoutez votre adresse IPv4 en notation décimale pointée ou une adresse IPv6. Cette valeur est l'adresse IP virtuelle (VIP) de 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". Ou pour IPv6, ajoutez votre préfixe. Pour plus d'informations sur 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.

Nom du service

Ajoutez un nom convivial pour identifier votre service. Exemple : "Serveurs Web de production".

Type de service

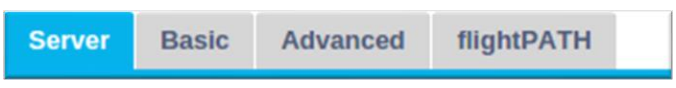
Veuillez noter qu'avec tous les types de services de "couche 4", le CDA n'interagit pas avec le flux de données et ne le modifie pas. flightPATH n'est donc pas disponible avec les types de services de couche 4. Les services de couche 4 équilibrent simplement le trafic en fonction de la politique d'équilibrage de la charge :

Type de service	**Port/Protocole**	**Couche de service**	**Commentaire**
Couche 4 TCP	Tout port TCP	Couche 4	L'ADC ne modifiera aucune information dans le flux de données et effectuera un équilibrage de charge standard du trafic conformément à la politique d'équilibrage de charge.
Couche 4 UDP	Tout port UDP	Couche 4	Comme pour le TCP de la couche 4, l'ADC ne modifiera aucune information dans le flux de données et effectuera un équilibrage de charge standard du trafic selon la politique d'équilibrage de charge.

Couche 4 TCP/UDP	Tout port TCP ou UDP	Couche 4	C'est l'idéal si votre service a un protocole primaire tel que UDP mais qu'il se rabat sur TCP. L'ADC ne modifiera aucune information dans le flux de données et effectuera un équilibrage de charge standard du trafic conformément à la politique d'équilibrage de charge.
HTTP	Protocole HTTP ou HTTPS	Couche 7	Le CDA 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 distinctes 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 la 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 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 les protocoles DICOM.

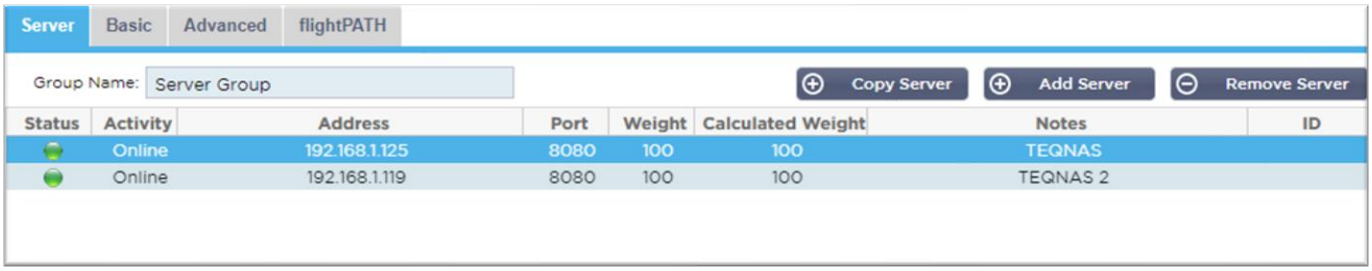
Serveurs réels

Il y a plusieurs onglets dans la section Real Servers du tableau de bord : Server, Basic, Advanced et flightPATH.



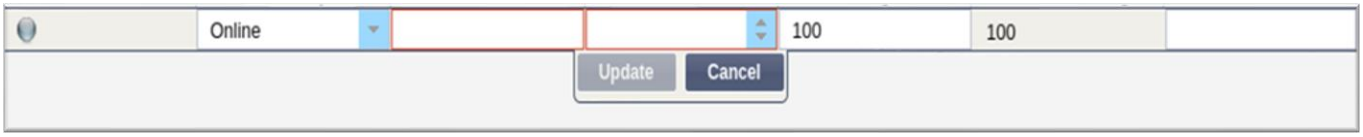
Serveur

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



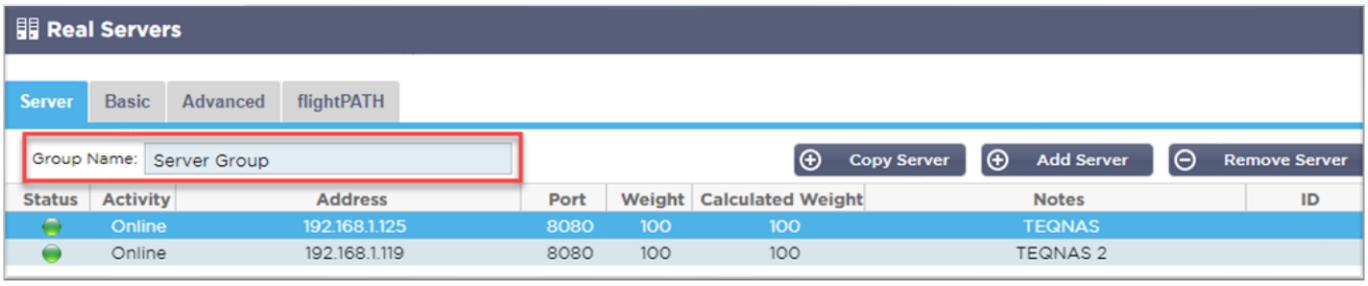
Ajouter un serveur

- Sélectionnez le VIP approprié que vous avez précédemment défini.
- Cliquez sur Ajouter un serveur
- Une nouvelle ligne apparaît avec le curseur clignotant dans la colonne Adresse IP.



- Saisissez l'adresse IPv4 de votre serveur en notation décimale pointillée. Le serveur réel peut se trouver sur le même réseau que votre service virtuel, sur tout réseau local directement attaché ou sur tout réseau que votre CDA peut acheminer. Exemple "10.1.1.1".
- Passez à la colonne Port et saisissez le numéro de port TCP/UDP de votre serveur. Ce numéro de port peut être le même que celui du service virtuel ou un autre numéro de port pour la connectivité par proxy inverse. Le CDA effectuera automatiquement la conversion vers ce numéro.
- Passez à la section Notes pour ajouter tout détail pertinent concernant le serveur. Exemple : "IIS Web Server 1"

Nom du groupe



Lorsque vous avez ajouté les serveurs qui composent l'ensemble équilibré en charge, vous pouvez également leur attribuer un nom de groupe. Une fois que vous avez modifié ce champ, le contenu est enregistré sans qu'il soit nécessaire d'appuyer sur le bouton Update.

Voyants d'état du serveur réel

Vous pouvez voir l'état d'un serveur réel par la couleur claire dans la colonne État. Voir ci-dessous :

LED	Signification
●	Connecté
◎	Non surveillé

●	Drainage
●	Hors ligne
●	Standby
●	Non connecté
●	État des constatations
●	Serveurs réels non licenciés ou licenciés dépassés

Activité

Vous pouvez modifier l'activité d'un serveur réel à tout moment en utilisant le menu déroulant. Pour ce faire, double-cliquez sur une ligne de serveur réel pour la placer 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 Basic.
Drainage	Tous les serveurs réels affectés au drainage continueront à servir les connexions existantes mais n'accepteront pas de nouvelles connexions. Le voyant d'état clignote en vert/bleu pendant la durée de la purge. Une fois que les connexions existantes sont naturellement fermées, les serveurs réels sont mis hors ligne et le voyant d'état est bleu fixe. Vous pouvez également visualiser ces connexions en accédant à la section Navigation > Monitor > Status.
Hors ligne	Tous les serveurs réels définis comme hors ligne seront immédiatement mis hors ligne et ne recevront aucun trafic.
Standby	Tous les serveurs réels définis comme étant en attente resteront hors ligne jusqu'à ce que **TOUS les** serveurs du groupe en ligne échouent dans leurs vérifications du Server Health Monitor. Le trafic est reçu par le groupe Standby conformément à la politique d'équilibrage de charge lorsque cela se produit. Si l'un des serveurs du groupe en ligne passe 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 est l'adresse IP de votre serveur réel. Exemple "192.168.1.200".

Port

Numéro du port TCP ou UDP sur lequel le serveur Real écoute le service. Exemple "80" pour le trafic Web.

Poids

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

Le poids par défaut d'un serveur réel est de 100, et vous pouvez entrer des valeurs de 1 à 100. Une valeur de 100 signifie une charge maximale, et 1 signifie 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 l'on considère que la politique d'équilibrage de la charge est définie sur le principe des moindres 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 le Round Robin comme méthode d'équilibrage de la charge, qui fait tourner les demandes à travers l'ensemble des serveurs équilibrés, la modification des pondérations 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 pour les connexions les plus faibles.

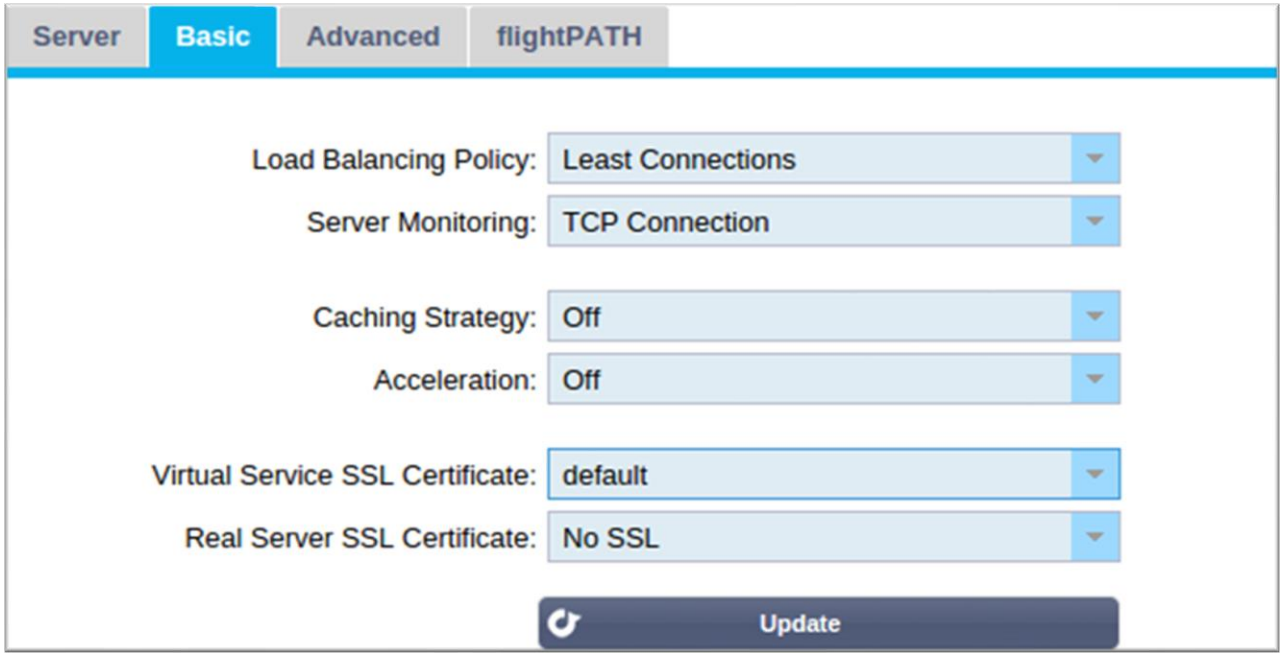
Poids calculé

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 que le CDA utilise en tenant compte de la pondération manuelle et de la politique d'équilibrage de la charge.

Notes

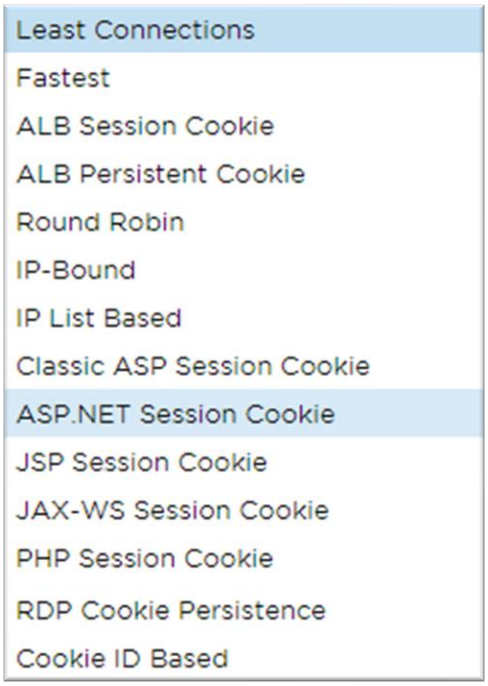
Saisissez dans le champ Notes toute note particulière utile à la description de l'entrée définie. Exemple : "IIS Server1 - London DC".

Base



Politique d'équilibrage des charges

La liste déroulante vous indique les politiques d'équilibrage de charge actuellement prises en charge et disponibles. Une liste des politiques d'équilibrage de charge, accompagnée d'une explication, est présentée ci-dessous.



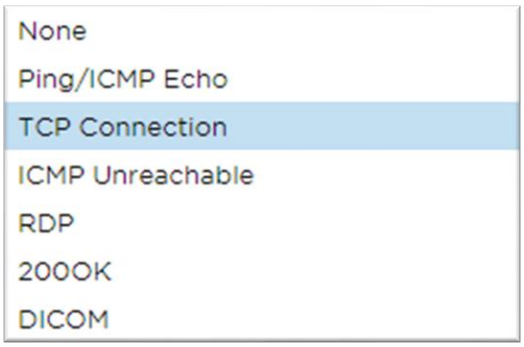
Option	Description
Le plus rapide	La politique d'équilibrage de charge la plus rapide calcule automatiquement le temps de réponse de toutes les demandes par serveur, lissé dans le temps. La colonne Poids calculé contient la valeur calculée automatiquement. La saisie manuelle n'est possible qu'en utilisant cette politique d'équilibrage de charge.

Round Robin	La méthode Round Robin, couramment utilisée dans les pare-feu et les équilibreurs de charge de base, est la plus simple. Chaque serveur réel reçoit une nouvelle demande dans l'ordre. Cette méthode n'est appropriée que lorsque vous devez équilibrer la charge des demandes vers les serveurs de manière uniforme ; un exemple serait les serveurs Web de recherche. Cependant, lorsque vous devez équilibrer la charge en fonction de la charge de l'application ou du serveur, ou même vous assurer que vous utilisez le même serveur pour la session, la méthode Round Robin est inappropriée.
Le moins de connexions	L'équilibreur de charge garde la trace du nombre de connexions actuelles à chaque serveur réel. Le serveur réel ayant le moins de connexions reçoit la nouvelle demande suivante.
Affinité/persistance des sessions de couche 3 - Liaison IP	Dans ce mode, l'adresse IP du client sert de base pour sélectionner le serveur réel 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 proxies, toutes les requêtes peuvent sembler provenir d'un seul client et, de ce fait, la charge n'est pas uniforme. Avec HTTP, l'information de l'en-tête (X-Forwarder-For) est utilisée lorsqu'elle est présente pour faire face aux proxies.
Affinité/persistance des sessions de couche 3 - basée sur une liste d'adresses IP	La connexion au serveur réel 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 cela peut être modifié en utilisant un jetPACK.
Affinité/Persistance de session de la couche 7 - Cookie de session ALB	Ce mode est la méthode de persistance la plus populaire pour l'équilibrage de charge HTTP. Dans ce mode, l'ADC utilise l'équilibrage de charge basé sur la liste d'IP pour chaque première demande. Il 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 dorsal. Ce cookie est utilisé pour la persistance lorsque le client doit se rendre chaque fois sur le même serveur dorsal. Le cookie expire lorsque la session est fermée.
Affinité/Persistance des sessions de la couche 7 - Cookie persistant de l'ALB	Le mode d'équilibrage de charge basé sur la liste d'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 back-end. Ce cookie est utilisé pour la persistance lorsque le client doit se rendre chaque fois sur le même serveur dorsal. Le cookie expire au bout de 2 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 - Cookie de session ASP classique	Active Server Pages (ASP) est une technologie Microsoft côté serveur. Si 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 - Cookie de session ASP.NET	Ce mode s'applique à **ASP.net.** Lorsque ce mode est sélectionné, le CDA 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 - Cookie de session JSP	Java Server Pages (JSP) est une technologie Oracle côté serveur. Lorsque ce mode est sélectionné, l'ADC maintient la persistance de la session sur le même serveur si un cookie JSP est détecté et trouvé dans sa liste de cookies connus. Lors de la détection d'un nouveau cookie JSP, la charge sera équilibrée à l'aide de l'algorithme Least Connections.
Cookie de session - Cookie de session JAX-WS	Java web services (JAX-WS) 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 JAX-WS est détecté et trouvé dans sa liste de cookies connus. Lors de la détection d'un nouveau cookie JAX-WS, il équilibrera la charge à l'aide de l'algorithme Least Connections.
Cookie de session - Cookie de session PHP	Personal Home Page (PHP) est une technologie open-source côté serveur. Lorsque ce mode est sélectionné, le CDA maintient la persistance de la session sur le même serveur lorsqu'un cookie PHP est détecté.
Cookie de session - Persistance du cookie 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 de la connexion à un serveur. L'avantage de cette méthode est que le maintien d'une connexion à un serveur est possible même si l'adresse IP du client change.
Basé sur le Cookie-ID	Une nouvelle méthode très semblable à "PhpCookieBased" et aux autres méthodes d'équilibrage de charge, mais utilisant CookieIDBased et le cookie RegEx h=[^ ;]+. Cette méthode utilisera la valeur définie dans le champ notes du serveur réel "ID=X ;" comme valeur de cookie pour identifier le serveur. Cela signifie donc qu'il s'agit d'une méthode similaire à CookieListBased, mais qu'elle utilise un nom de cookie différent et stocke une valeur de cookie unique, non pas l'IP brouillée, mais l'ID du serveur réel (lu au moment du chargement). La valeur par défaut est CookieIDName="h" ; toutefois, s'il existe une valeur prioritaire dans la configuration des paramètres avancés du serveur virtuel, utilisez-la à la place. **REMARQUE** : Si cette valeur est définie, nous écrasons l'expression du cookie ci-dessus pour remplacer h= par la nouvelle valeur. Enfin, si une valeur de cookie inconnue arrive et correspond à l'un des ID de serveur réel, il faut sélectionner ce serveur ; sinon, il faut utiliser la méthode suivante (déléguer).

Surveillance des serveurs

Votre ADC contient six méthodes standard de surveillance du serveur réel, énumérées ci-dessous.



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 serveur réel est un serveur RDP, un moniteur 200OK n'est pas pertinent. Si vous n'êtes pas sûr du moniteur à 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 par les moniteurs des couches inférieures. Par exemple, la définition des moniteurs Ping/ICMP Echo, Connexion TCP et 200OK s'affichera dans les événements du tableau de bord comme l'image ci-dessous :

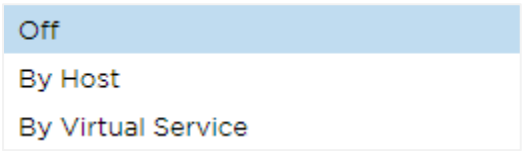
Nous pouvons voir que la couche 3 Ping et la couche 4 TCP Connect ont réussi si nous regardons la ligne supérieure, mais que la couche 7 200OK a échoué. Ces résultats de surveillance fournissent suffisamment d'informations pour indiquer que le routage est correct et qu'un service fonctionne sur le port correspondant, mais le site Web ne répond pas correctement à la page demandée. Il est maintenant temps de regarder le serveur Web et la section Library > 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. Il s'agit d'une voie pour héberger des systèmes non fiables ou anciens qui ne sont pas essentiels aux opérations 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 d'écho valide est reçue, l'ADC considère que le serveur réel est opérationnel et le trafic vers le serveur continue. Il maintient également le service disponible sur une paire H/A. Cette méthode de surveillance est utilisable avec n'importe quel type de service.
Connexion TCP	Dans ce mode, une connexion TCP est établie avec le serveur réel et immédiatement interrompue sans envoyer de données. Si la connexion réussit, le CDA considère que le serveur réel est opérationnel. Cette méthode de surveillance est utilisable avec tout type de service. Les services UDP sont les seuls qui ne conviennent pas actuellement à la surveillance des connexions TCP.

ICMP non atteignable	L'ADC enverra un contrôle de santé UDP au serveur et marquera le serveur réel comme indisponible s'il reçoit un message ICMP port unreachable. Cette méthode peut être utile lorsque vous devez vérifier si un port de service UDP est disponible sur un serveur, comme le port DNS 53.
RDP	Dans ce mode, une connexion TCP s'initialise comme expliqué dans la méthode ICMP Unreachable. Après l'initialisation de la connexion, une connexion RDP de couche 7 est demandée. Si la liaison est confirmée, l'ADC considère que le serveur réel est opérationnel. Cette méthode de surveillance est utilisable avec n'importe quel serveur terminal Microsoft.
200 OK	Dans cette méthode, une connexion TCP s'initialise avec le serveur réel. Une fois la connexion établie, le CDA envoie une demande HTTP au serveur réel. Une réponse HTTP est attendue et le code de réponse "200 OK" est vérifié. Si le code de réponse "200 OK" est reçu, le CDA considère que le serveur réel est opérationnel. Si l'ADC ne reçoit pas de code de réponse "200 OK" pour une raison quelconque, y compris les délais d'attente, l'échec de la connexion et d'autres raisons, l'ADC marque le serveur réel comme étant indisponible. Cette méthode de surveillance est uniquement valable pour une utilisation avec 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 s'il est géré de manière appropriée par la fonction "Content SSL".
DICOM	Une connexion TCP s'initialise avec le serveur réel en mode DICOM, et une "demande d'association" Echoscu est envoyée au serveur réel lors de la connexion. Une conversation comprenant une "acceptation d'association" 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, pour une raison quelconque, le moniteur ne se termine pas avec succès, le serveur réel est considéré comme hors service.
Défini par l'utilisateur	Tout moniteur configuré dans la section Surveillance du serveur réel apparaîtra dans la liste.

Stratégie de mise en cache

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



Veuillez vous reporter à 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 distinct 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 Service Virtuel	La mise en cache par service virtuel est disponible lorsque vous choisissez cette option. Un seul cache existera 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
Off	Désactiver la compression pour le service virtuel
Compression	Lorsqu'elle est sélectionnée, cette option active la compression pour le service virtuel sélectionné. Le CDA compresse dynamiquement le flux de données vers le client sur demande. Ce processus s'applique uniquement aux objets qui contiennent l'en-tête content-encoding : gzip. Les exemples de contenu incluent HTML, CSS ou Javascript. Vous pouvez également exclure certains types de contenu à l'aide de la section Exclusions globales.

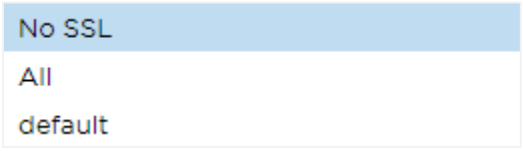
Remarque : Si l'objet peut être mis en cache, le CDA stocke une version compressée et la sert de manière statique (à partir de la mémoire) jusqu'à ce que le contenu expire et soit revalidé.

Certificat SSL de service virtuel (chiffrement entre le client et l'ADC)

Par défaut, le paramètre est No SSL. Si votre type de service est "HTTP" ou "Layer4 TCP", vous pouvez sélectionner un certificat dans la liste déroulante pour l'appliquer au service virtuel. Les certificats qui ont été créés ou importés apparaîtront dans cette liste. Vous pouvez 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.

Indication du nom du serveur

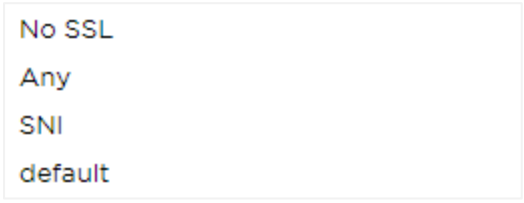
Cette option est une extension du protocole de réseau TLS grâce à laquelle le client indique le nom d'hôte auquel il tente de se connecter au début du processus d'établissement de la liaison. Ce paramètre permet au CDA de présenter plusieurs certificats sur la même adresse IP virtuelle et le même port TCP.



Option	Description
Pas de SSL	Le trafic de la source vers le CDA n'est pas crypté.
Défaut	Cette option a pour effet d'appliquer un certificat créé localement, appelé "Default", au côté navigateur du canal. Utilisez cette option pour tester le SSL lorsqu'il n'a pas été créé ou importé.
Certificats SSL importés par l'utilisateur	Tous les certificats que vous avez importés dans le CDA sont affichés ici.

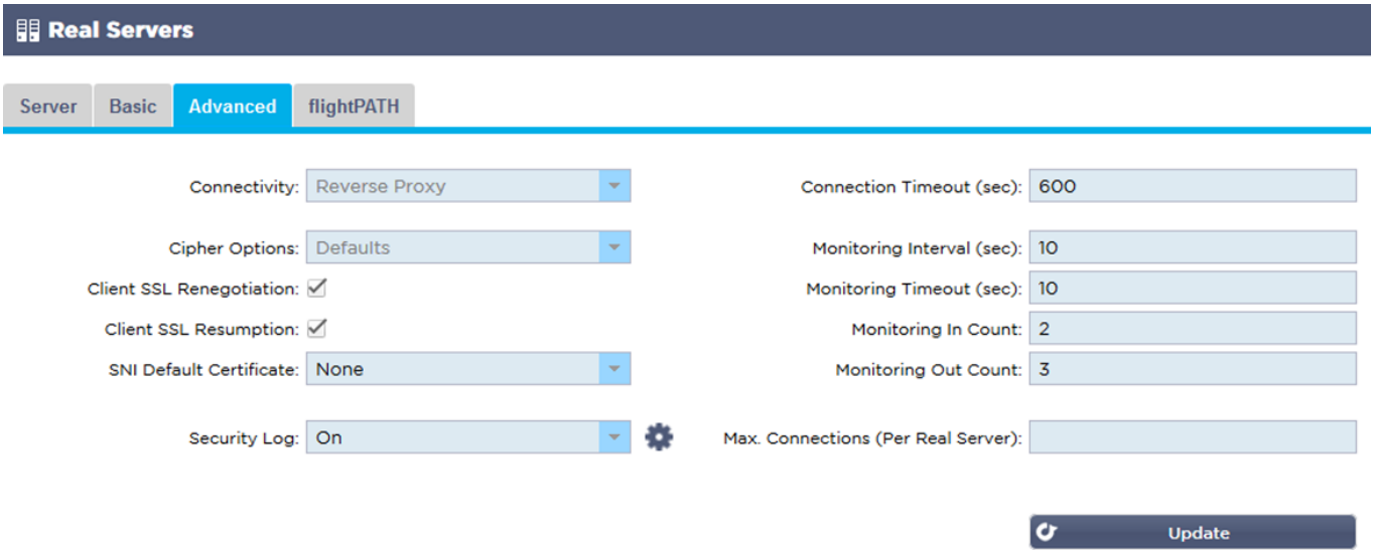
Certificat SSL du serveur réel (cryptage entre l'ADC et le serveur réel)

Le paramètre par défaut de cette option est No SSL. Si votre serveur nécessite une connexion cryptée, cette valeur doit être différente de No SSL. Les certificats qui ont été créés ou importés apparaissent dans cette liste.



Option	Description
Pas de SSL	Le trafic entre le CDA et le serveur réel n'est pas crypté. La sélection d'un certificat du côté du navigateur signifie que "No SSL" peut être choisi du côté du client pour fournir ce qui est connu comme "SSL Offload".
Tout	L'ADC agit comme un 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, fournissant ce que l'on appelle un "pontage SSL" ou un "re-cryptage SSL".
SNI	L'ADC agit comme un client et accepte tout certificat présenté par le serveur réel. Le trafic entre l'ADC et le serveur réel est crypté si cette option est sélectionnée. Utilisez l'option "Any" lorsqu'un certificat est spécifié du côté du service virtuel, fournissant ce que l'on appelle un "pontage SSL" ou un "re-cryptage SSL". Choisissez cette option pour activer SNI du côté du serveur.
Certificats SSL importés par l'utilisateur	Tous les certificats que vous avez importés dans le CDA apparaissent ici.

Avancé



Connectivité

Votre service virtuel est configurable avec quatre types de connectivité différents. Veuillez sélectionner le mode de connectivité à appliquer au service.

Option	Description
Proxy inversé	Reverse Proxy est la valeur par défaut et fonctionne au niveau de la couche 7 avec compression et mise en cache. Et au niveau de la couche 4 sans mise en cache ni compression. Dans ce mode, votre ADC agit comme un proxy inverse et devient

	l'adresse source vue par les serveurs réels.
Retour direct du serveur	Le Direct Server Return ou DSR (DR - Direct Routing dans certains milieux) permet au serveur situé derrière l'équilibreur de charge de répondre directement au client en contournant l'ADC de la réponse. Le DSR ne peut être utilisé qu'avec l'équilibrage de charge de couche 4. Par conséquent, la mise en cache et la compression ne sont pas disponibles avec cette option choisie. L'équilibrage de charge de la couche 7 ne fonctionne pas avec ce DSR. De plus, il n'y a pas de support de persistance autre que celui basé sur la liste d'IP. L'équilibrage de charge SSL/TLS avec cette méthode n'est pas idéal car le support de la persistance de l'IP source est le seul type disponible. Le DSR exige également que des modifications soient apportées au serveur réel. Veuillez vous reporter à la section Modifications du serveur réel.
Passerelle	Le mode passerelle vous permet d'acheminer tout le trafic à travers l'ADC, ce qui permet au trafic des serveurs réels d'être acheminé par l'ADC vers d'autres réseaux via les machines virtuelles ou les interfaces matérielles de l'ADC. L'utilisation de l'appareil en tant que dispositif de passerelle pour les serveurs réels est idéale lorsqu'il fonctionne en mode multi-interface. L'équilibrage de charge de couche 7 avec cette méthode ne fonctionne pas car il n'y a pas de support de persistance autre que celui basé sur la liste d'IP. Cette méthode exige que le serveur réel définisse sa passerelle par défaut à l'adresse de l'interface locale (eth0, eth1, etc.) de l'ADC. Veuillez vous référer à la section Modifications du serveur réel.

Options de chiffrement

Vous pouvez définir les ciphers au niveau de chaque service et cela ne concerne que les services pour lesquels SSL/TLS est activé. Le CDA effectue un choix automatique du chiffrement, et vous pouvez ajouter différents chiffrement en utilisant des jetPACKS. En ajoutant le jetPACK approprié, vous pouvez définir les options de chiffrement par service. L'avantage de cette méthode est que vous pouvez créer plusieurs services avec différents niveaux de sécurité. Sachez que les anciens clients ne sont pas compatibles avec les nouveaux ciphers ; plus le service est sécurisé, plus le nombre de clients est réduit.

Renégociation SSL du client

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

Reprise SSL du client

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

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 en l'absence de correspondance exacte. Choisissez l'un des certificats installés dans la liste déroulante pour le présenter en cas d'échec de la correspondance exacte du certificat SSL.

Journal de sécurité

La valeur par défaut est 'On'. Elle permet au service de consigner les informations d'authentification dans les journaux du W3C. En cliquant sur l'icône de la roue dentée, vous accédez à la page Système > Journalisation, où vous pouvez vérifier les paramètres de la journalisation du W3C.

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 l'absence d'activité. Réduisez cette valeur pour le trafic Web sans état de courte durée, qui est généralement de 90 secondes 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.

Paramètres de surveillance

Ces paramètres concernent les moniteurs de serveur réel dans l'onglet Basic. Il existe des entrées globales dans la configuration pour compter le nombre de surveillances réussies ou échouées avant que le statut d'un serveur soit marqué en ligne ou en échec.

Intervalle

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

Délai de surveillance

La valeur du délai d'attente est le temps pendant lequel l'ADC attendra qu'un serveur réponde à une demande de connexion. La valeur par défaut est de 2s. 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 serveur Real doit passer deux contrôles de santé réussis avant d'être mis en ligne. En augmentant ce chiffre, vous augmentez la probabilité que le serveur puisse servir le trafic, mais la mise en service prendra plus de temps en fonction de l'intervalle. En diminuant cette valeur, le serveur sera mis en service plus rapidement.

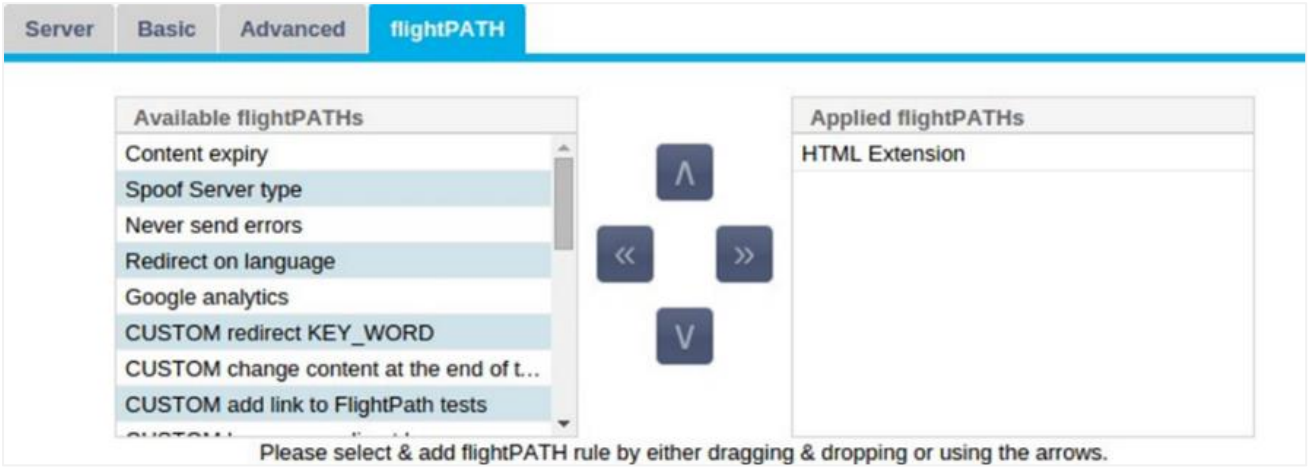
Surveillance du nombre de sorties

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 et que celui-ci soit marqué RED et Unreachable. En augmentant ce chiffre, vous obtiendrez un service meilleur et plus fiable, au détriment du temps nécessaire à l'ADC pour arrêter d'envoyer du trafic à ce serveur.

Max. Connexions

Limite le nombre de connexions simultanées du serveur réel et est défini par service. Par exemple, si vous configurez cette limite à 1000 et que vous avez deux serveurs réels, l'ADC limite **chaque** serveur réel à 1000 connexions simultanées. Vous pouvez également choisir de présenter une page "Server too busy" (Serveur trop occupé) une fois que cette limite est atteinte sur tous les serveurs, afin d'aider les utilisateurs à comprendre pourquoi une absence de réponse ou un retard s'est produit. Laissez ce champ vide pour des connexions illimitées. Ce que vous définissez ici dépend des ressources de votre système.

flightPATH



flightPATH est un système conçu par Edgenexus et disponible exclusivement au sein de l'ADC. Contrairement aux moteurs à base de règles d'autres fournisseurs, flightPATH ne fonctionne pas via une ligne de commande ou une console de saisie de script. Au lieu de cela, il utilise une interface graphique pour sélectionner les différents paramètres, conditions et actions à exécuter pour obtenir ce dont ils ont besoin. Ces caractéristiques rendent flightPATH extrêmement puissant et permettent aux administrateurs 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.

Vous pouvez voir sur l'image ci-dessus ; il y a une liste des règles disponibles sur la gauche et les règles appliquées au service virtuel sur la droite.

Ajoutez une règle disponible en la faisant glisser et en la déposant du côté gauche vers le côté droit ou en mettant en surbrillance une règle 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 supérieure exécutée en premier. Pour modifier l'ordre d'exécution, mettez la règle en surbrillance et déplacez-vous vers le haut et le bas à l'aide des flèches.

Pour supprimer une règle, faites-la glisser et déposez-la à nouveau 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.

Bibliothèque

Add-Ons

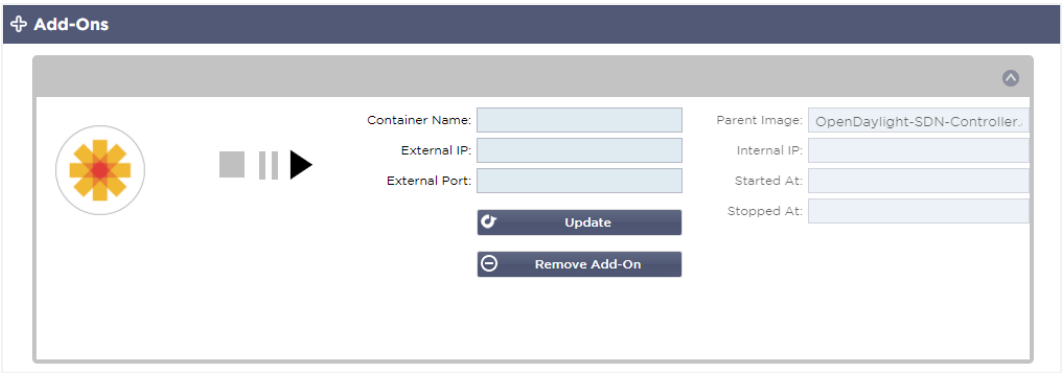
Les modules complémentaires sont des conteneurs basés sur Docker qui peuvent fonctionner en mode isolé au sein de l'ADC. Il peut s'agir, par exemple, d'un pare-feu d'application ou même d'une micro-instance de l'ADC lui-même.

Apps

La section Apps de la rubrique Add-Ons détaille les Apps que vous avez achetées, téléchargées et déployées.

Si aucune application n'est présente, cette section affichera un message vous invitant à passer à la section des applications et à télécharger et déployer une application.

Une fois que vous avez déployé une application, elle apparaît dans la zone des applications.



Achat d'un complément

Pour acheter une application, vous devez vous inscrire sur l'App Store. L'achat est effectué en utilisant le CDA lui-même. Vous trouverez

Accédez à la page Bibliothèque > Apps du tableau de bord du CDA.

Vous pouvez y sélectionner l'application que vous souhaitez télécharger et installer.

Si vous effectuez cette opération à partir du tableau de bord ADC, veuillez ne sélectionner qu'un seul élément. Vous pouvez posséder plusieurs ensembles ADC, et les applications doivent être associées à l'ADC sur lequel elles sont déployées.

Si vous accédez à l'App Store via votre bureau et votre navigateur, vous pouvez en télécharger autant que vous le souhaitez. Par exemple, quatre instances du WAF ou du GSLB. Elles apparaîtront dans la zone des applications achetées de votre CDA pour que vous puissiez les télécharger.

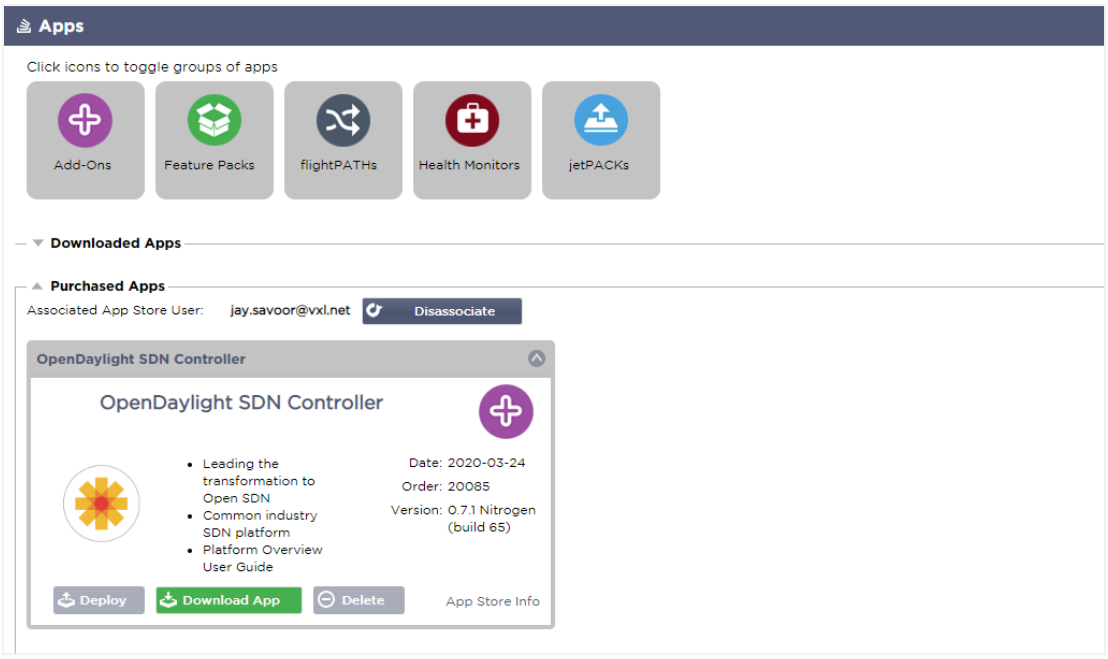
Les applications sont associées aux CDA que vous possédez et que vous avez enregistrés.

Lorsque vous choisissez de télécharger une application, l'ID de la machine vous est demandé, après quoi l'application est cryptée et liée à l'ID de la machine ADC.

Les liens vers l'App Store sont les suivants :

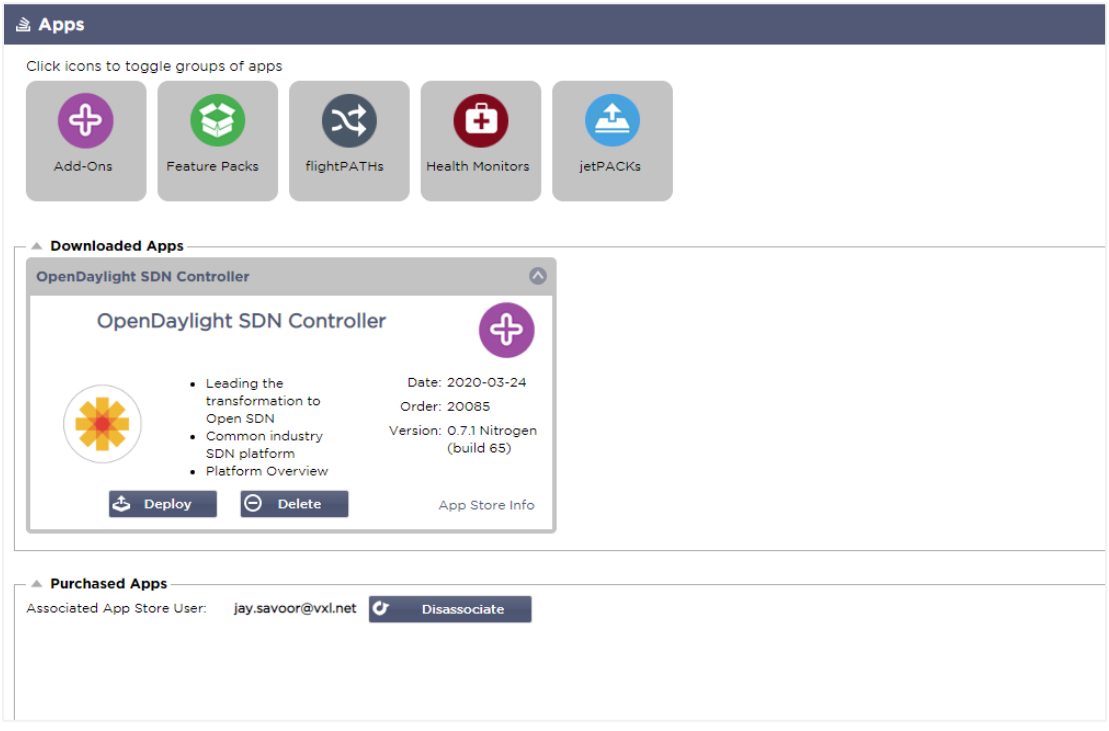
- Add-Ons : **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Moniteurs de santé : **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**

- jetPACKS : HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/
- Packs de fonctionnalités : HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/
- Règles de flightPATH : HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/
- Mises à jour des logiciels : HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/



Déploiement d'une application

Une fois téléchargée sur le CDA, l'application sera déplacée dans la section Applications téléchargées et déployée sur le CDA à l'aide du bouton Déployer. Ce processus prend un certain temps en fonction des ressources disponibles pour le CDA. Une fois déployée, l'application apparaît dans la section des applications téléchargées.



Authentification

La page Bibliothèque > Authentification vous permet de configurer des serveurs d'authentification et de créer des règles d'authentification avec des options pour Basic ou Forms côté client et NTLM ou BASIC côté serveur.

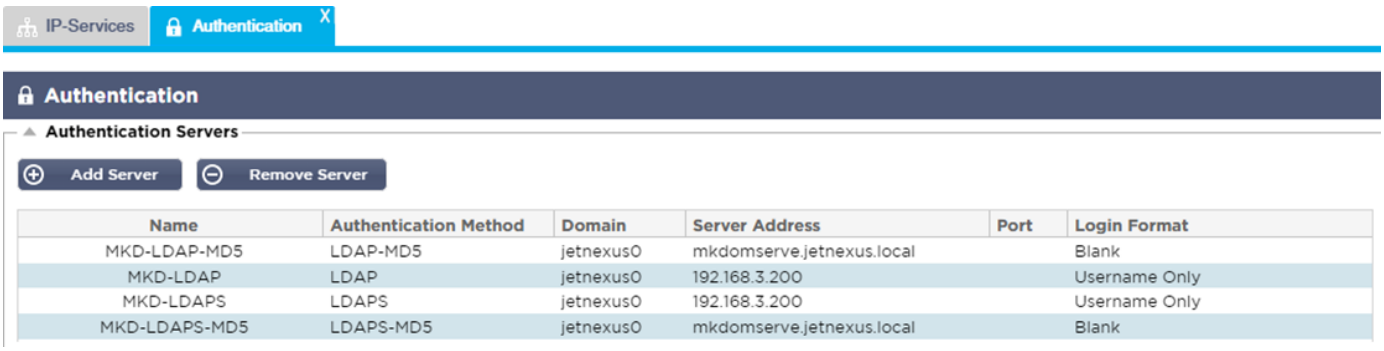
Configuration de l'authentification - un flux de travail

Veuillez effectuer les étapes suivantes au minimum 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. Créez 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 fonctionnelle, nous devons d'abord configurer un serveur d'authentification.



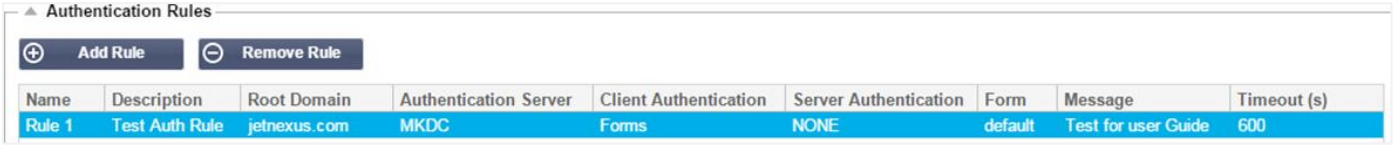
- Cliquez sur le bouton Ajouter un serveur.
- Cette action produira une ligne vierge prête à être complétée.

Option	Description
Nom	Donnez un nom à votre serveur à des fins d'identification - ce nom est utilisé dans les règles.
Description	Ajouter une description
Méthode d'authentification	Choisissez 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 le nom d'utilisateur en clair et le mot de passe haché en 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 en MD5 pour plus de sécurité dans un tunnel crypté entre l'ADC et le serveur LDAP.
Domaine	Ajoutez le nom de domaine du serveur LDAP.
Adresse du serveur	Ajoutez l'adresse IP ou le nom d'hôte du serveur d'authentification. LDAP - Adresse IPv4 ou nom d'hôte. LDAP-MD5 - nom d'hôte uniquement (l'adresse IPv4 ne fonctionne pas) LDAPS - adresse IPv4 ou nom d'hôte. LDAPS-MD5 - nom d'hôte uniquement (l'adresse IPv4 ne fonctionne pas).
Port	Utilisez le port 389 pour LDAP et le port 636 pour LDAPS par défaut. Il n'est pas nécessaire d'ajouter le numéro de port pour LDAP et LDAPS. Lorsque d'autres méthodes seront disponibles, vous pourrez les configurer ici.

Conditions de recherche	Les conditions de recherche doivent être conformes à la norme RFC 4515. Exemple : (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Base de recherche	Cette valeur est le point de départ de la recherche dans la base de données LDAP. Exemple *dc=mycompany,dc=local*
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 d'utilisateur et de domaine saisies par l'utilisateur sont supprimées et les informations de domaine 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\gchristie OR someone@mycompany*. Les informations relatives au domaine saisies au niveau du serveur sont ignorées. Blanc - le CDA accepte tout ce que l'utilisateur saisit et l'envoie au serveur d'authentification. Cette option est utilisée lorsque vous utilisez MD5.
Phrase de passe	Cette option n'est pas utilisée dans cette version.
Temps mort	Non utilisé dans cette version

Règles d'authentification

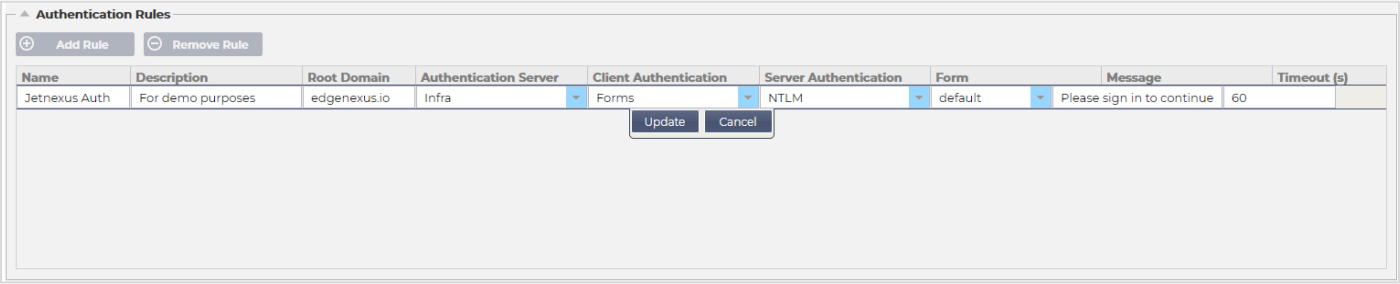
L'étape suivante consiste à créer les règles d'authentification à utiliser avec la définition du serveur.



Champ	Description
Nom	Ajoutez un nom approprié pour votre règle d'authentification.
Description	Ajoutez une description appropriée.
Domaine de la racine	Ce champ doit être laissé vide, sauf si vous avez besoin d'une authentification unique pour les sous-domaines.
Serveur d'authentification	Il s'agit d'une boîte déroulante contenant les serveurs que vous avez configurés.
Authentification du client :	Choisissez la valeur appropriée à vos besoins : Basic (401) - Cette méthode utilise la méthode d'authentification standard 401. Formulaires - ce formulaire présente le formulaire par défaut du CDA à l'utilisateur. 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 aucune 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	Choisissez la valeur appropriée Défaut - En sélectionnant cette option, le CDA utilisera sa forme intégrée. Personnalisé - vous pouvez ajouter un formulaire que vous avez conçu et le sélectionner ici.
Message	Ajoutez 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 Timeout n'est valable que pour l'authentification basée sur les formulaires.

Ouverture de session unique



Si vous souhaitez fournir une authentification unique aux utilisateurs, remplissez la colonne Domaine racine avec votre domaine. Dans cet exemple, nous avons utilisé edgenexus.io. Nous pouvons maintenant avoir plusieurs services qui utiliseront edgenexus.io comme domaine racine, et vous ne devrez vous connecter qu'une seule fois. Si nous considérons les services suivants :

- Sharepoint.monentreprise.com
- usercentral. mycompany.com
- appstore. 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 appstore. mycompany.com et sera authentifié automatiquement par le CDA. Vous pouvez définir le délai d'attente, qui forcera l'authentification une fois cette période d'inactivité atteinte.

Formulaires

Cette section vous permettra de télécharger un formulaire personnalisé.

Comment créer votre formulaire personnalisé

Bien que le formulaire de base fourni par le CDA soit suffisant dans la plupart des cas, il y aura des occasions où les entreprises souhaiteront 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"

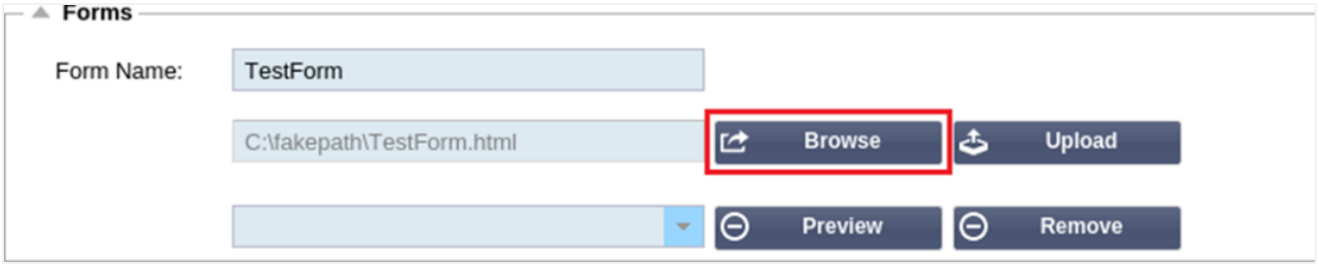
Message facultatif1 :	%JNMESSAGE
Message facultatif2 :	%JNAUTHMESSAGE%
Images	Si vous souhaitez ajouter une image, veuillez l'ajouter en ligne en utilisant le codage Base64.

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

```
<HTML>
<HEAD>
<TITLE>SAMPLE AUTH FORM</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>
```

Ajout d'un formulaire personnalisé

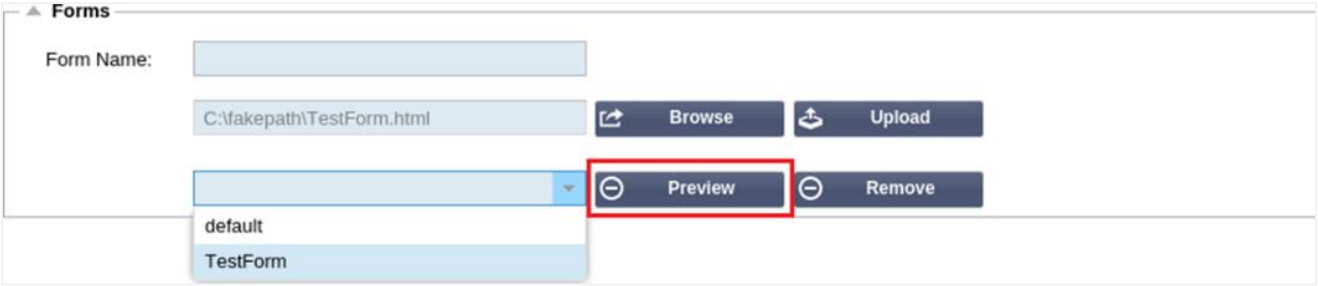
Une fois que vous avez créé un formulaire personnalisé, vous pouvez l'ajouter en utilisant la section Formulaires.



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

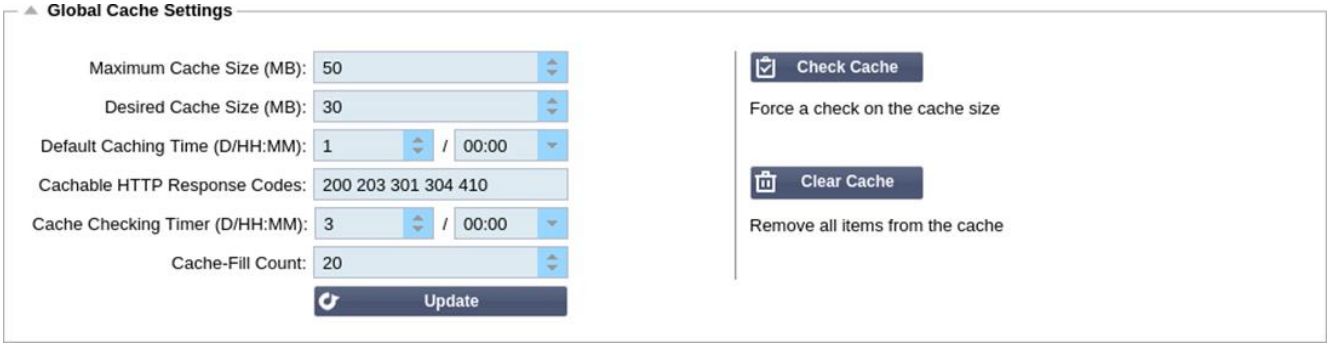
Prévisualisation de votre formulaire personnalisé

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



Cache

L'ADC est capable de mettre en cache des données dans sa mémoire interne et de vider périodiquement ce cache vers le stockage interne de l'ADC. Les paramètres qui gèrent cette fonctionnalité sont fournis 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 pour 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'appareil (plutôt que dans l'espace disque) et ne doit pas dépasser la moitié de la mémoire disponible.

Taille souhaitée du cache (Mo)

Cette valeur indique la RAM optimale à laquelle le cache sera réduit. Alors que la taille maximale de l'antémémoire représente la limite supérieure absolue de l'antémémoire, la taille souhaitée de l'antémémoire est conçue comme la taille optimale que l'antémémoire doit essayer d'atteindre à chaque fois qu'une vérification automatique ou manuelle de la taille de l'antémémoire est effectuée. L'écart entre la taille maximale et la taille souhaitée de l'antémémoire existe pour tenir compte de l'arrivée et du chevauchement de nouveaux contenus entre les vérifications périodiques de la taille de l'antémémoire pour 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 sous "Moniteur -> Statistiques" pour un dimensionnement approprié.

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 est stocké le contenu sans directive "no-store" ou délai d'expiration explicite dans l'en-tête de trafic.

L'entrée du champ prend la forme "J/HH:MM" - ainsi, une entrée de "1/01:01" (par défaut, 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 cachables

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

- 200 - Réponse standard pour les demandes HTTP réussies
- 203 - Les en-têtes ne sont pas définitifs mais proviennent d'une copie locale ou d'une tierce partie.
- 301 - Une nouvelle URL permanente a été attribuée à la ressource demandée.
- 304 - Non modifié depuis la dernière demande et la copie en cache locale doit être utilisée à la place.
- 410 - La ressource n'est plus disponible sur le serveur et aucune adresse de transfert n'est connue.

Ce champ doit être édité avec précaution, car les codes de réponse cachables les plus courants sont déjà répertoriés.

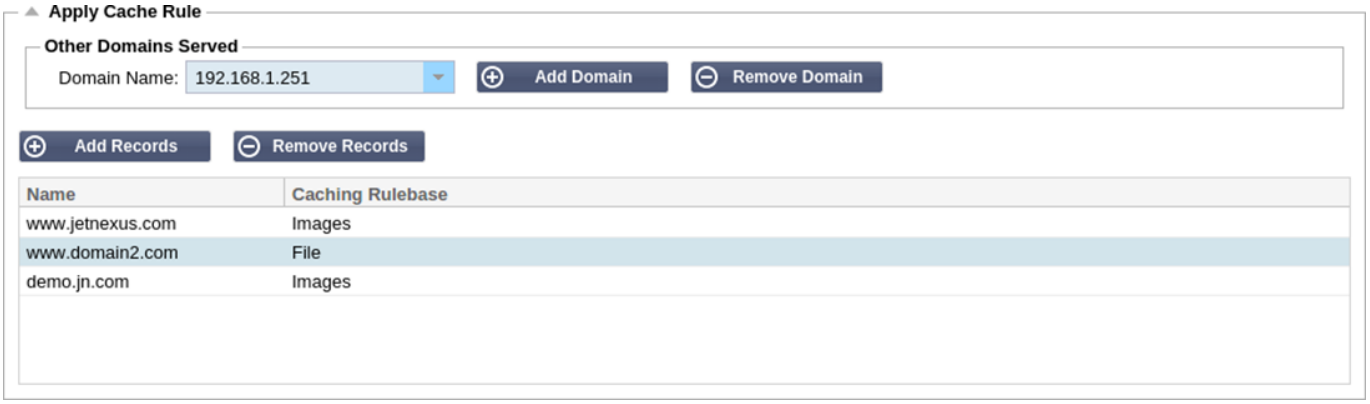
Temps de vérification du cache (J/HH:MM)

Ce paramètre détermine l'intervalle de temps entre les opérations d'ajustement 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 a été détecté.

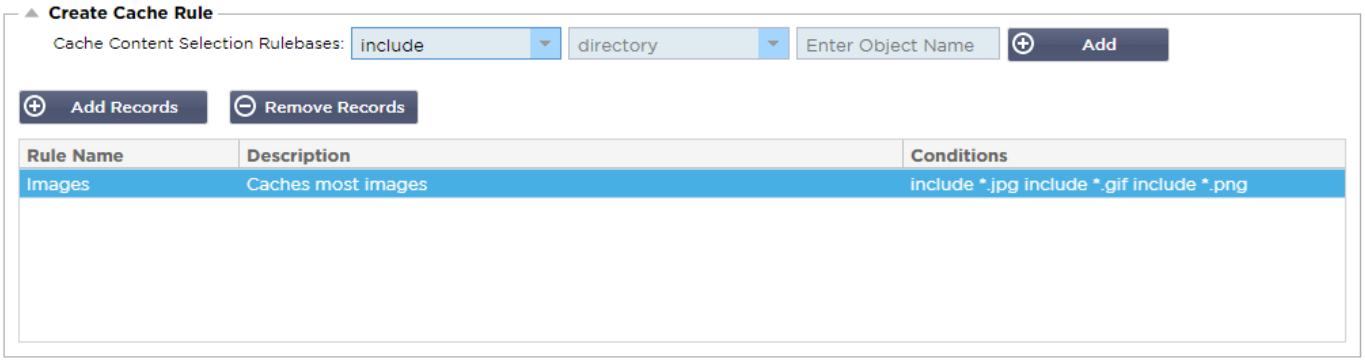
Appliquer une règle de mise en cache



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

- Ajouter le domaine manuellement avec le bouton Ajouter des enregistrements. Vous devez utiliser un nom de domaine entièrement qualifié ou une adresse IP en notation décimale en pointillés. Exemple www. mycompany.com ou 192.168.3.1:80
- Cliquez sur la flèche déroulante et choisissez votre domaine dans la liste.
- La liste sera remplie 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 mise en cache en double-cliquant sur la colonne Base de règles de mise en cache et en la 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 soit taper vos conditions manuellement, soit utiliser la fonction "Ajouter une condition".

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

- Choisissez Inclure ou Exclure
- Choisir toutes les images JPEG
- Cliquez sur le symbole + Ajouter
- Vous verrez que 'include *.jpg' a été ajouté 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 que vos règles s'afficheront sur la même ligne jusqu'à ce que vous cliquiez dans la case Conditions, puis elles s'afficheront sur une ligne distincte.

flightPATH

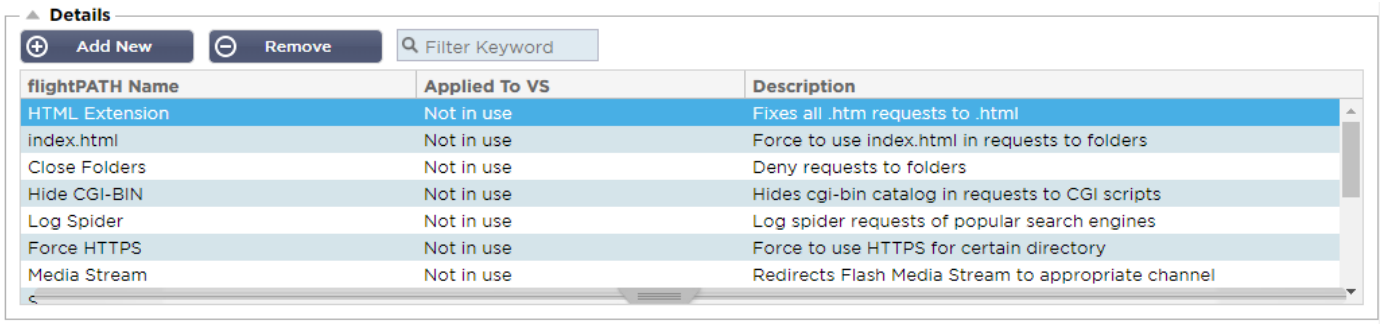
flightPATH est la technologie de gestion du trafic intégrée à l'ADC. flightPATH vous permet d'inspecter le trafic HTTP et HTTPS en temps réel et d'effectuer des actions en fonction des conditions.

Les règles flightPATH doivent être appliquées à un VIP lorsque des objets IP sont utilisés dans les règles.

Une règle de trajectoire de vol est constituée de quatre éléments :

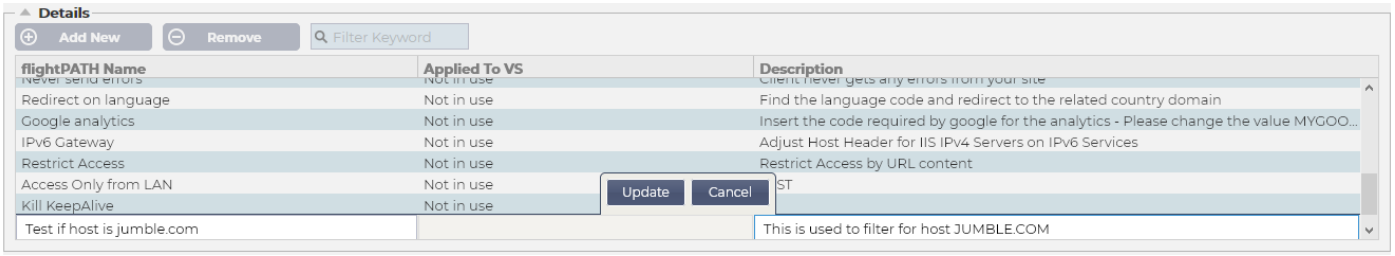
1. Détails, où vous définissez le nom du flightPATH et le service auquel il est rattaché.
2. Condition(s) pouvant être définie(s) et entraînant le déclenchement de la règle.
3. Évaluation qui permet de définir des variables qui peuvent être utilisées dans les actions
4. Les actions qui sont utilisées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

Détails



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

Ajout d'une nouvelle règle flightPATH



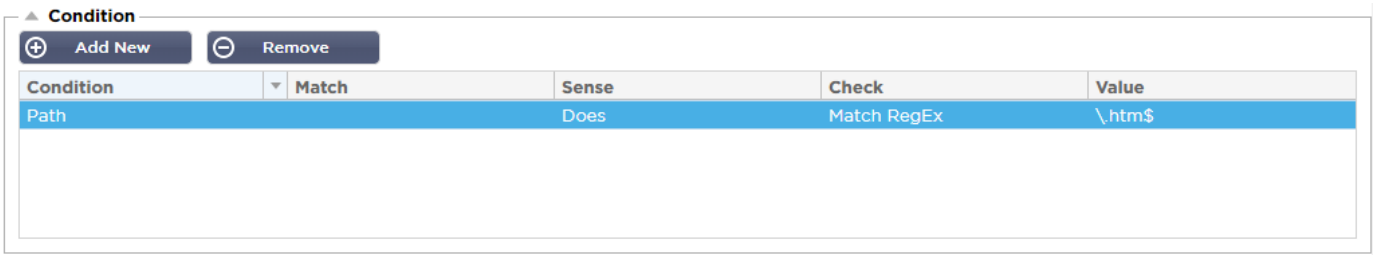
Champ	Description
Nom de FlightPATH	Ce champ est réservé au nom de la règle flightPATH. Le nom que vous indiquez ici apparaît et est référencé dans d'autres parties du CDA.
Appliqué à VS	Cette colonne est en lecture seule et indique le VIP auquel la règle flightPATH est appliquée.
Description	Valeur 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 nouveau situé dans la section Détails.
2. Saisissez un nom pour votre règle. Exemple Auth2
3. Entrez une description de votre règle
4. Une fois que la règle a été appliquée à un service, vous verrez la colonne Applied To se remplir automatiquement avec une adresse IP et une valeur de port.
5. N'oubliez pas d'appuyer sur le bouton Mettre à jour pour enregistrer vos modifications. Si vous faites une erreur, appuyez simplement sur Annuler pour revenir à l'état précédent.

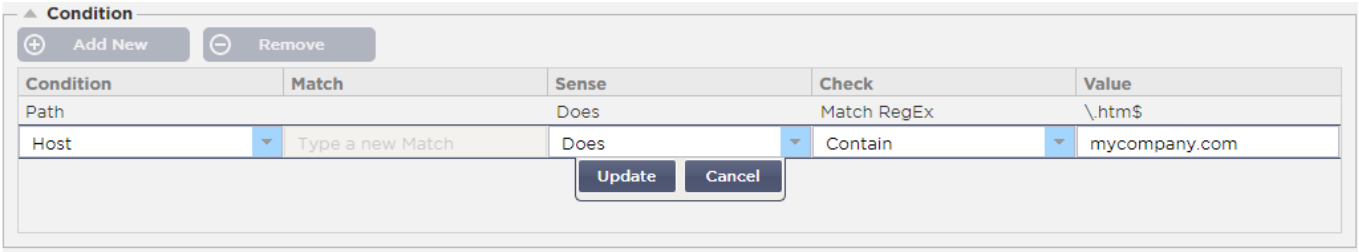
Condition

Une règle FlightPATH peut comporter un nombre quelconque de conditions. Les conditions fonctionnent sur la base d'un ET, ce qui vous permet de définir la condition à partir de laquelle l'action est déclenchée. Si vous souhaitez utiliser une condition OR, créez une règle flightPATH supplémentaire et appliquez-la au VIP dans l'ordre correct.



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 étend considérablement les capacités de flightPATH.

Création d'une nouvelle condition flightPATH



Condition

Nous fournissons plusieurs conditions prédéfinies dans le menu déroulant et couvrent tous les scénarios prévus. Lorsque de nouvelles conditions seront ajoutées, elles seront disponibles via les mises à jour de Jetpack.

Les choix disponibles 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 de GEO	Compare l'adresse IP source aux codes de pays ISO 3166.	GEO Location est égal à GB, OU GEO Location est égal à Allemagne
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 une liste déroulante avec une liste de langues.
Méthode	Liste déroulante des méthodes HTTP	Liste déroulante qui inclut GET, POST, etc.
IP d'origine	Si le proxy en amont prend en charge X-Forwarded-for (XFF), il utilisera l'adresse d'origine réelle.	IP du client. Il peut également utiliser plusieurs IP ou sous-réseaux. 10\.1\.2\.* est 10.1.2.0 /24 sous-réseau10\ .1\.2\.3|10\.1\.2\.4 Utilisez | pour plusieurs adresses IP
Chemin d'accès	Chemin du site web	/mywebsite/index.asp
POST	Méthode de demande POST	Vérifier les données téléchargées sur un site web
Requête	Nom et valeur d'une requête, et peut accepter soit le nom de la requête soit une valeur également	"Best=jetNEXUS" où la correspondance est Best et la valeur est edgeNEXUS
Chaîne de requête	La chaîne de requête complète après le caractère ?	
Demande de cookie	Nom d'un cookie demandé par un client	MS-WSMAN=afYfn1CDqCDqUD: :
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 pour la réponse	200 OK, 304 Non modifié
Cookie de réponse	Le nom d'un cookie envoyé par le serveur	MS-WSMAN=afYfn1CDqCDqUD: :
En-tête de réponse	Tout en-tête HTTP	Referrer, User-Agent, From, Date
Version de réponse	La version HTTP envoyée par le serveur	HTTP/1.0 OU HTTP/1.1
Source IP	Soit l'IP d'origine, l'IP du serveur proxy ou une autre adresse IP agrégée.	ClientIP , Proxy IP, Firewall IP. Vous pouvez également utiliser plusieurs IP et sous-réseaux. Vous devez échapper les points car il s'agit de RegEX. Exemple 10\.1\.2\.3 est 10.1.2.3

Match

Le champ "Match" peut être une liste déroulante ou une valeur de texte et il est définissable 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 définie sur <form>, le champ Correspondance est présenté comme un champ de texte, et si la Condition est POST, le champ Correspondance est présenté comme un menu déroulant contenant des valeurs pertinentes.

Les choix disponibles sont les suivants :

MATCH	DESCRIPTION	EXEMPLE
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodements acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>
Accept-Language	Langues acceptables pour la réponse	Accept-Language : en-US
Accept-Ranges	Quels types de plages de contenu partiel ce serveur supporte-t-il ?	Accept-Ranges : bytes
Autorisation	Références d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contient des informations comptables sur les coûts de l'application de la méthode demandée.	
Content-Encoding	Le type d'encodage utilisé	Content-Encoding : gzip
Content-Length	La longueur du corps de la réponse en octets (octets de 8 bits).	Content-Length : 348
Content-Type	Le type mime du corps de la demande (utilisé avec les demandes 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'origine du message	Date = "Date" " :" HTTP-date
ETag	Un identifiant pour une version spécifique d'une ressource, souvent un résumé 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 304 Not Modified si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	La date de 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 des effets divers 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.	Referrer : 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	La chaîne de l'agent utilisateur de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Varier	Indique aux mandataires en aval comment faire correspondre les futurs en-têtes de demande pour décider si la réponse mise en cache peut être utilisée plutôt que de demander une nouvelle réponse au serveur d'origine.	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple, ASP.NET, PHP, JBoss) qui prend en charge l'application Web.	X-Powered-By : PHP/5.4.0

Sense

Le champ Sense est un champ booléen déroulant qui contient les choix Does ou Doesn't.

Vérifiez

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

Les choix disponibles sont les suivants : Contient, Fin, Egal, Existe, A une longueur, Correspond à RegEx, Correspond à une liste, Début, Dépasse la longueur.

CHECK	DESCRIPTION	EXEMPLE
Existe	Le détail de la condition n'a pas d'importance, il suffit de savoir qu'elle existe ou n'existe pas.	L'hôte - existe - existe
Début	La chaîne de caractères commence par la valeur	Chemin - Does - Start - /secure
Fin	La chaîne se termine par la valeur	Chemin - Fait - Fin - .jpg

Contenir	La chaîne contient bien la valeur	En-tête de la demande - Accepter - Ne - Contenir - image
Equal	La chaîne est égale à la valeur	Hôte - Fait - Égale - www.jetnexus.com
Avoir la longueur	La chaîne de caractères a une longueur de la valeur	L'hôte - a - une longueur - 16www.jetnexus.com = VRAIwww.jetnexus.co.uk = FAUX
Match RegEx	Permet de saisir une expression régulière complète compatible avec Perl.	IP d'origine - Correspond - Regex - 10\..* | 11\..*

Étapes pour ajouter une condition

L'ajout d'une nouvelle condition flightPATH est très simple. Un exemple est montré ci-dessus.

1. Cliquez sur le bouton Ajouter un nouveau dans la zone des conditions.
2. Choisissez une condition dans la liste déroulante. Prenons l'exemple de l'hôte. Vous pouvez également taper dans le champ, et le CDA affichera la valeur dans une liste déroulante.
3. Choisissez un sens. Par exemple, est-ce que
4. Choisissez une vérification. Par exemple, Container
5. Choisissez une valeur. Par exemple, mycompany.com

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

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

Évaluation

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

La définition de la variable flightPATH comprend quatre entrées qui doivent être effectuées.

- Variable - c'est le nom de la variable
- Source - une liste déroulante de points sources possibles
- Détail - sélectionnez les valeurs dans une liste déroulante ou saisissez-les manuellement.
- Valeur - la valeur que la variable contient et peut être une valeur alphanumérique ou un RegEx pour un réglage plus fin.

Variables intégrées :

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

Vous pouvez utiliser l'une des variables énumérées ci-dessous dans la section Action.

L'explication de chaque variable se trouve dans le tableau "Condition" ci-dessus.

- Méthode = $method
- Chemin = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Code de réponse (le texte inclut également "200 OK") = $resp$.
- Hôte = $host$
- Version = $version$
- Port du client = $clientport
- Clientip = $clientip$.
- Géolocalisation = $geolocation$"

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

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 du processus consiste à ajouter une action associée à la règle et à la condition flightPATH.

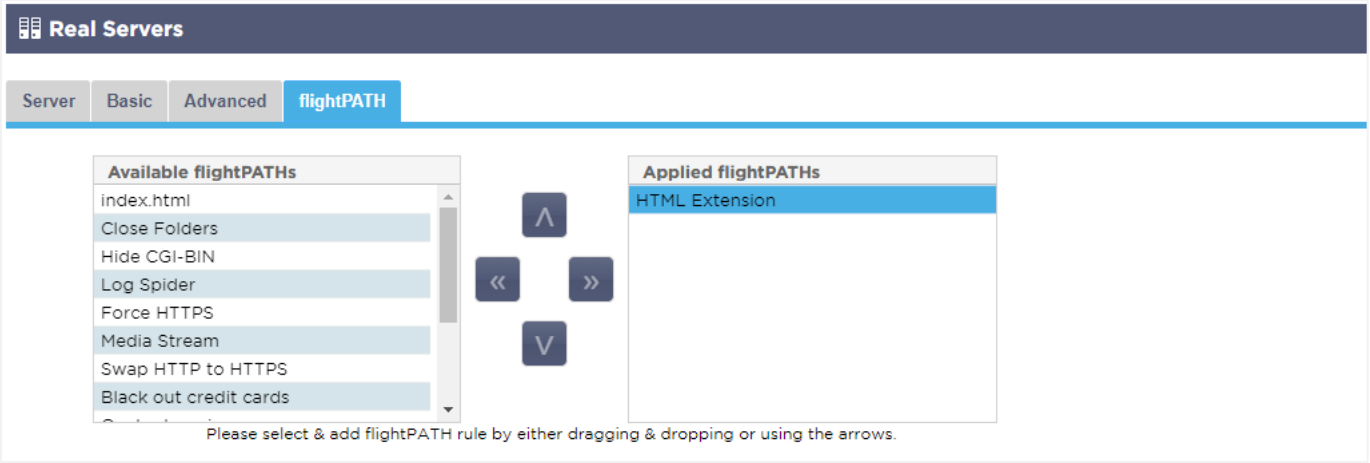
Dans cet exemple, nous voulons réécrire la partie chemin d'accès de l'URL pour refléter l'URL tapée par l'utilisateur.

- Cliquez sur Ajouter un 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 final devienne www.imagepool.com/myimages.

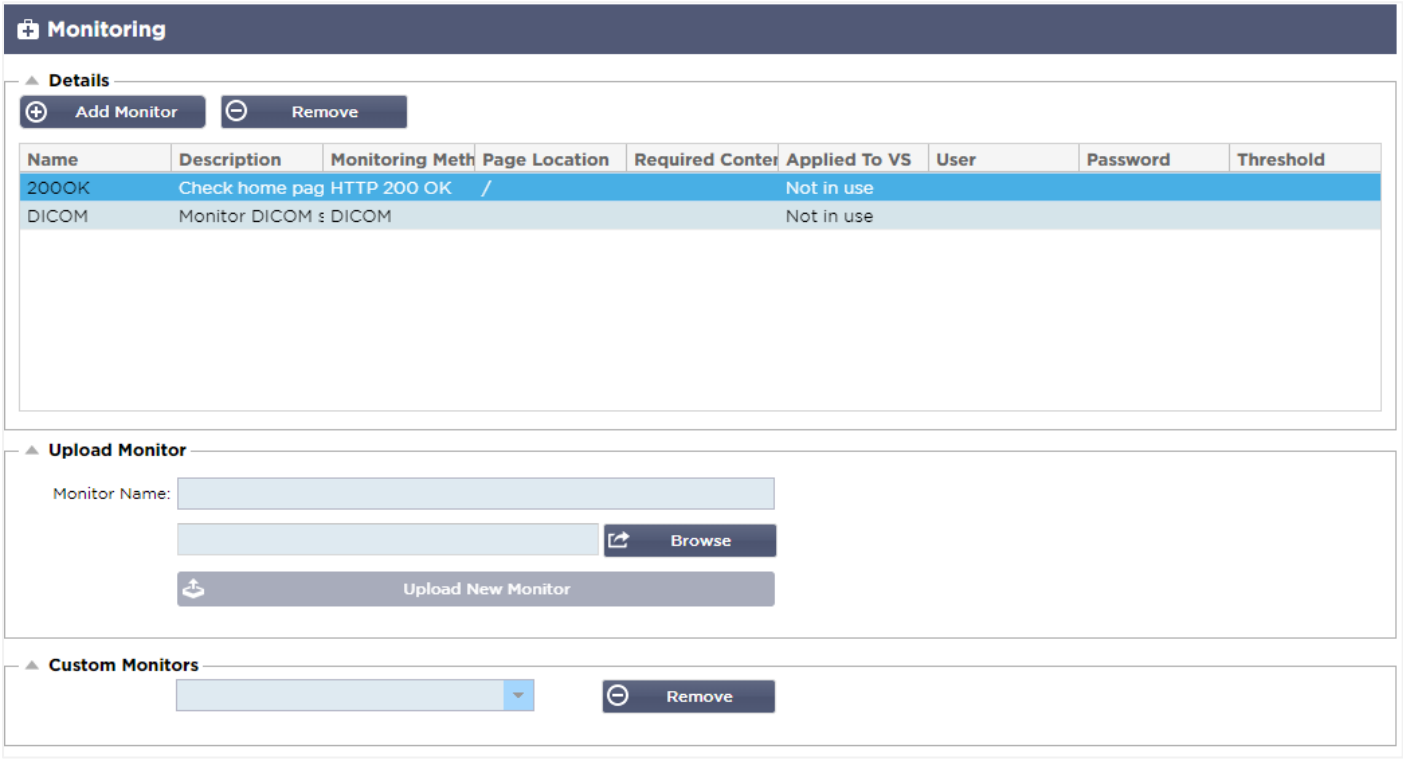
Application de la règle flightPATH

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



- Accédez à Services > Services IP et choisissez le VIP auquel vous souhaitez affecter la règle flightPATH.
- Vous verrez la liste des serveurs réels ci-dessous
- Cliquez sur l'onglet flightPATH
- Sélectionnez la règle flightPATH que vous avez configurée ou l'une des règles préétablies prises en charge. Vous pouvez sélectionner plusieurs règles flightPATH si nécessaire.
- Faites glisser et déposez l'ensemble sélectionné dans la section Applied flightPATHs ou cliquez sur le bouton fléché >>.
- La règle sera déplacée vers le côté droit et appliquée automatiquement.

Moniteurs pour serveurs réels



Lorsque l'équilibrage des charges est mis en place, il est utile de surveiller l'état des serveurs réels et des applications qui y sont exécutées. Par exemple, pour les serveurs web, vous pouvez configurer une page spécifique que vous pouvez utiliser pour surveiller l'état ou utiliser l'un des autres systèmes de surveillance dont dispose l'ADC.

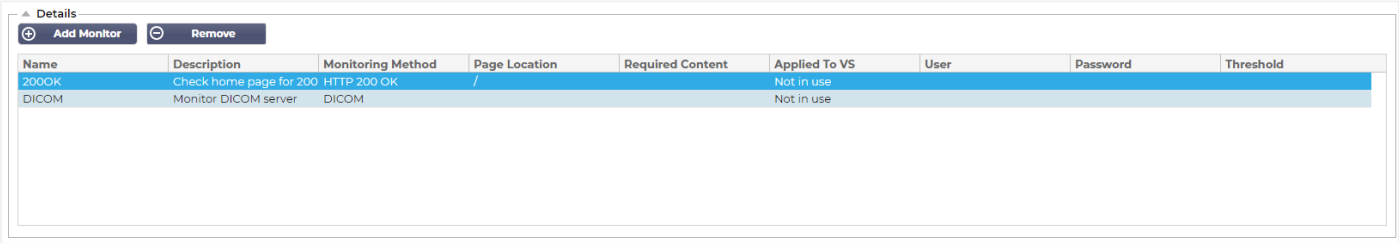
La page Library > Real Server Monitors vous permet d'ajouter, d'afficher et de modifier des surveillances personnalisées. Il s'agit de "contrôles de santé" du serveur de la couche 7. Vous pouvez les sélectionner dans le champ "Server Monitoring" de l'onglet Basic du service virtuel que vous définissez.

La page des moniteurs du serveur réel est divisée en trois sections.

- Détails
- Télécharger
- Moniteurs personnalisés

Détails

La section Détails est utilisée pour ajouter de nouveaux moniteurs et pour 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 pour ce moniteur, et nous recommandons qu'il est préférable de le rendre aussi descriptif que possible.

Méthode de contrôle

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

Méthode de contrôle	Description	Exemple
HTTP 200 OK	Une connexion TCP est établie avec le serveur réel. Une fois la connexion établie, une brève requête HTTP est envoyée au serveur réel. Une réponse HTTP du serveur est attendue, puis le code de réponse "200 OK" est vérifié. Si le code de réponse "200 OK" est reçu, le serveur réel est considéré comme opérationnel. Si, pour une raison quelconque, le code de réponse "200 OK" n'est pas reçu, y compris les délais d'attente ou l'échec de la connexion, le serveur réel est considéré comme hors service et indisponible. Cette méthode de surveillance ne peut vraiment	Nom : 200OK Description : Vérifier le site web de la production Méthode de surveillance : HTTP 200 OK Emplacement de la page : /main/index.html OU HTTP://www.edgenexus.io/main/index.html Contenu obligatoire : N/A

	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 s'il est géré de manière appropriée par la fonction "Content SSL".	
Réponse HTTP	Une connexion et une demande/réponse HTTP sont établies avec le serveur réel et vérifiées comme expliqué dans l'exemple précédent. Mais plutôt que de vérifier le code de réponse "200 OK", l'en-tête de la réponse HTTP est vérifié pour y trouver un contenu textuel personnalisé. Il peut s'agir d'un en-tête complet, d'une partie d'en-tête, d'une ligne d'une partie de page ou d'un seul mot. Si le texte est trouvé, le serveur réel est considéré comme opérationnel. 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 s'il est géré de manière appropriée par la fonction "Content SSL".	Nom : Serveur en place Description : Vérifier le contenu de la page pour "Server Up. " Méthode de surveillance : Réponse HTTP Emplacement de la page : /main/index.html OU HTTP://www.edgenexus.io/main/index.html Contenu obligatoire : Serveur en place
DICOM	Nous envoyons un écho DICOM en utilisant la valeur "Source Calling" AE Title dans la colonne de contenu requise. Vous pouvez également définir la valeur AE Title "Destination Calling" dans la section Notes de chaque serveur. Vous pouvez trouver la colonne Notes dans la section IP Services- -Virtual Services--Server page.	Nom : DICOM Description : Contrôle de santé L7 pour le service DICOM Méthode de surveillance : DICOM Emplacement de la page : N/A Contenu obligatoire : Valeur AET
TCP hors bande	La méthode TCP Out of Band est semblable à une connexion TCP, sauf 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 obligatoire : 555
Moniteur TCP multiport	Cette méthode est semblable à la précédente, sauf que vous pouvez avoir plusieurs ports différents. Le moniteur est considéré comme réussi uniquement si tous les ports spécifiés dans la section du contenu requis répondent correctement.	Nom : Moniteur Multi-Port Description : Surveiller le succès de plusieurs ports Emplacement de la page : N/A Contenu obligatoire : 135,59534,59535

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 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 à 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 serveur Real.

Mot de passe

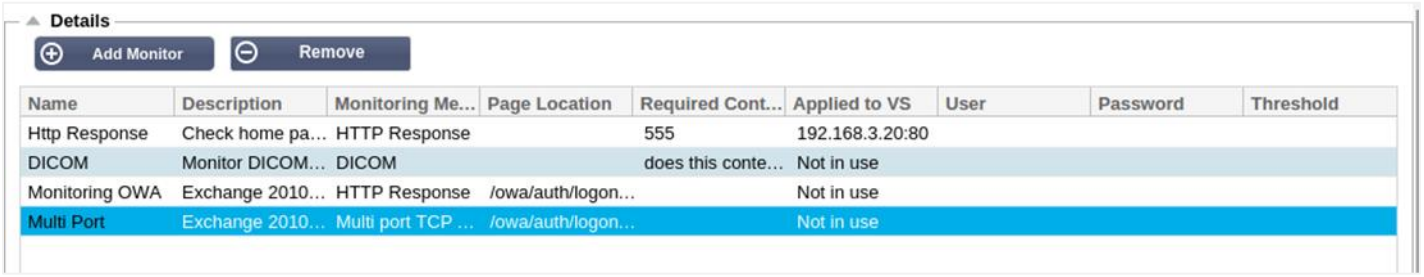
Certains moniteurs personnalisés peuvent utiliser cette valeur avec le champ Utilisateur pour se connecter à un serveur réel.

Seuil

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

NOTE : Assurez-vous que la réponse du serveur d'application n'est pas une réponse "Chunked".

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.
- Recherchez 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 le menu déroulant
- 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 vous 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 le CDA. Si vous n'incluez pas cette ligne, votre script ne sera pas trouvé !

Les éléments suivants sont obligatoires :

- #Moniteur-Nom
- utiliser strictement ;
- avertissement d'utilisation ;

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

Valeurs dynamiques

- my $host = $_[0] ; - Ceci utilise l'"Adresse" de la section IP Services--Real Server.
- my $port = $_[1] ; - Ceci utilise le "Port" de la section IP Services--Real Server.
- my $content = $_[2] ; - Ceci utilise la valeur "Required Content" de la section Library--Real Server Monitoring de la bibliothèque.
- my $notes = $_[3] ; - Cette opération utilise la colonne "Notes" de la section Real Server des Services IP.
- my $page = $_[4] ; - Ceci utilise les valeurs "Page Location" de la section Library--Real Server Monitor.
- my $user = $_[5] ; - Ceci utilise la valeur "User" de la section Library--Real Server Monitor.
- my $password = $_[6] ; - Ceci utilise la valeur "Password" de la section Library--Real Server Monitor.

Les bilans de santé personnalisés ont deux résultats

- Succès
  Valeur de retour 1Imprime
  un message de réussite à SyslogMarque
  le serveur réel en ligne (si IN COUNT correspond)

- Échec
  Valeur de retour 2Imprime
  un message indiquant Unsuccessful à SyslogMark
  the Real Server Offline (à condition que OUT Count corresponde)

Exemple d'un moniteur de santé personnalisé

```
#Moniteur-Nom HTTPS_SNI
utiliser strictement :
les avertissements d'utilisation ;
Le nom du moniteur comme ci-dessus 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 retournera les valeurs suivantes
# 1 si le test est réussi
# 2 si le test est infructueux sub monitor
{
my $host=       $_[0] ; ### IP ou nom de l'hôte
my $port=       $_[1] ; ### Port de l'hôte
my $content=    $_[2] ; ### Contenu à rechercher (dans la page web et les en-têtes HTTP)
my $notes=      $_[3] ; ### Nom d'hôte virtuel
my $page=       $_[4] ; ### La partie de l'URL après l'adresse de l'hôte
my $user=       $_[5] : ### domaine/nom d'utilisateur (facultatif)
my $password=           $_[6] ; ### mot de passe (facultatif)
mon $resolve ;
mon $auth       = ;
if ($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 $auth HTTPs://${notes}${page} 2>&1' ; if(join(""@lines)=~/$content/)
        {
        imprimez "HTTPs://$notes}${page} looking for - $content - Health check successful.\n" ;
        retour(1) ;
        }
sinon
        {
        imprimez "HTTPs://${notes}${page} looking for - $content - Health check failed.\n" ;
        retour(2)
```

```
        }
    }
    moniteur(@ARGV) :
```

NOTE : Surveillance personnalisée - L'utilisation de variables globales n'est pas possible. Utilisez uniquement les variables locales - les variables définies à l'intérieur des fonctions

Certificats SSL

Pour utiliser avec succès l'équilibrage de charge de couche 7 avec des serveurs utilisant des connexions cryptées par SSL, l'ADC doit être équipé des certificats SSL utilisés sur les serveurs cibles. Cette condition est nécessaire pour que le flux de données puisse être décrypté, examiné, géré, puis ré-encrypté avant d'être envoyé au serveur cible.

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

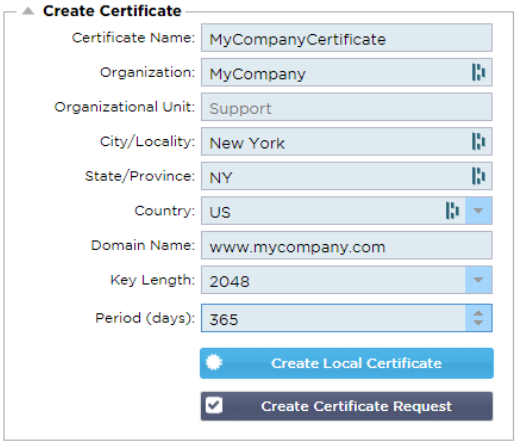
Que fait le CDA avec le certificat SSL ?

L'ADC peut effectuer des règles de gestion du trafic (flightPATH) en fonction de ce que contiennent les 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 déchiffrer, et pour cela, il doit disposer du certificat SSL utilisé par le serveur. Une fois décrypté, l'ADC pourra alors examiner et exécuter les règles flightPATH. Ensuite, les données seront ré-encryptées à l'aide du certificat SSL et envoyées sur le serveur réel final.

Créer un certificat

Bien que l'ADC puisse utiliser un certificat SSL de confiance globale, il peut générer un certificat SSL auto-signé. Le certificat SSL auto-signé est parfait pour les exigences d'équilibrage de charge interne. Cependant, vos politiques informatiques peuvent exiger un certificat d'autorité de certification de confiance ou de domaine.

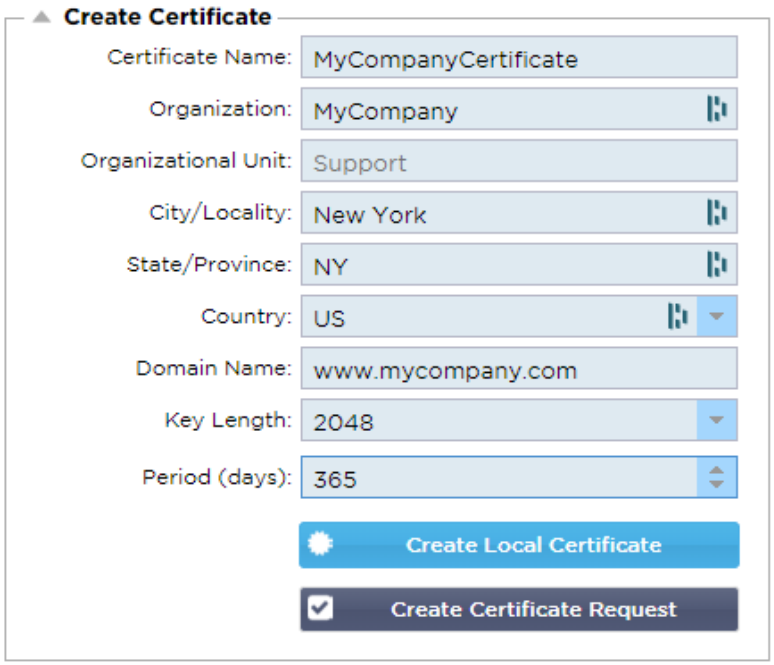
Comment créer un certificat SSL local



- Remplissez tous les détails comme dans l'exemple ci-dessus.
- Cliquez sur Créer un certificat local
- Une fois que vous avez cliqué sur ce bouton, vous pouvez appliquer le certificat à un **SERVICE VIRTUEL.**

Créer une demande de certificat (CSR)

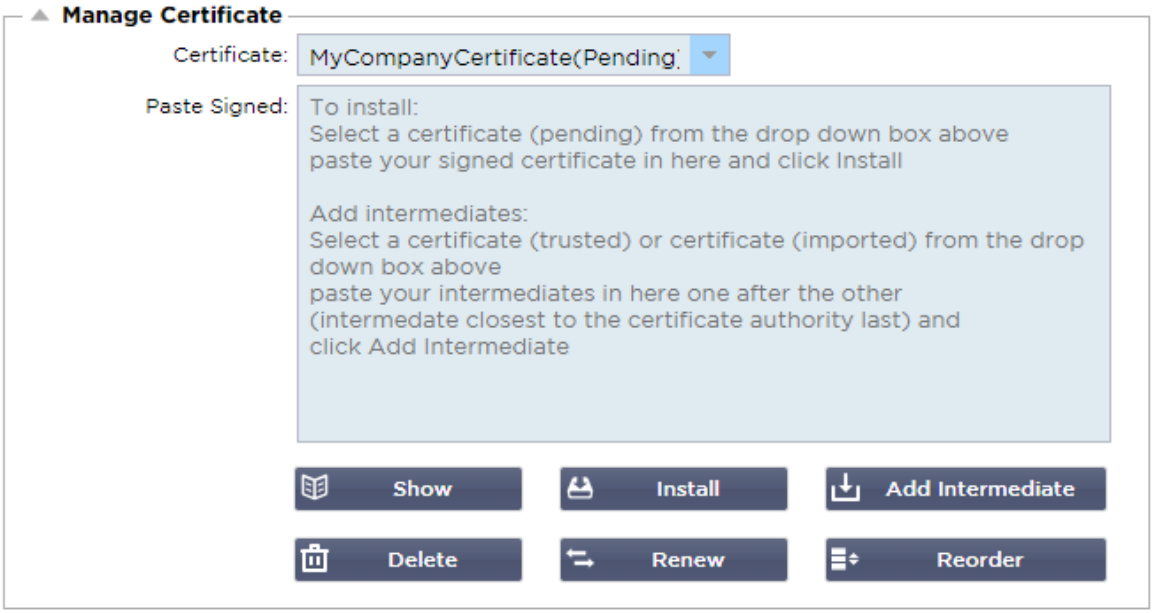
Lorsque vous devez obtenir un SSL de confiance globale auprès d'un fournisseur externe, vous devez générer un CSR pour générer le certificat SSL.



Remplissez le formulaire comme indiqué ci-dessus avec toutes les données pertinentes, puis cliquez sur le bouton Demande de certificat. Le popup correspondant aux données que vous avez fournies vous sera présenté.

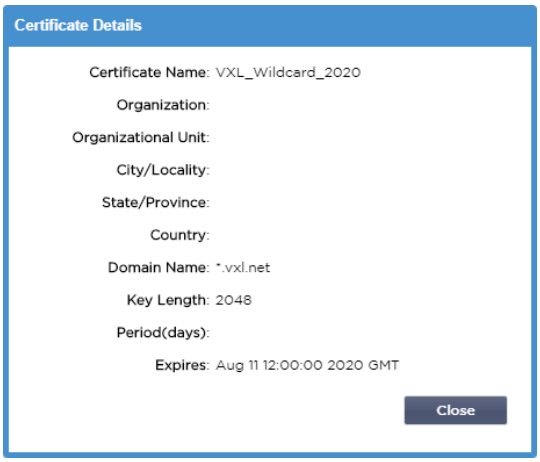
Vous devrez couper et coller le contenu dans un fichier TEXTE et le nommer avec une extension de fichier CSR, par exemple, *mycert.csr*. Ce fichier CSR devra ensuite être fourni à votre autorité de certification pour créer le certificat SSL.

Gérer le certificat



Cette sous-section contient divers outils permettant de gérer les certificats SSL que vous avez dans l'ADC.

Afficher

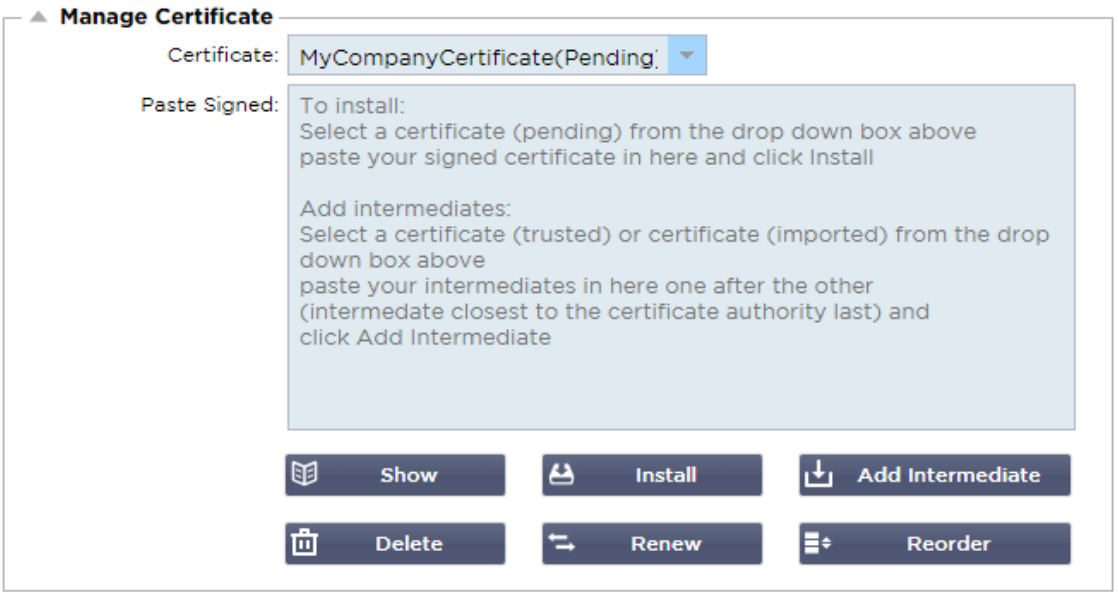


Il peut arriver que vous souhaitiez consulter les détails d'un certificat SSL installé.

- Sélectionnez le certificat dans le menu déroulant
- Cliquez sur le bouton Afficher
- La fenêtre popup ci-dessous sera présentée avec les détails du certificat.

Installation d'un certificat

Une fois que vous avez obtenu le certificat de l'autorité de certification de confiance, vous devez le faire correspondre à la RSC générée et l'installer dans l'ADC.



- Sélectionnez un certificat que vous avez généré dans les étapes ci-dessus. Un statut (Pending) sera fixé au poste. Dans l'exemple, MyCompanyCertificate est montré dans l'image ci-dessus.
- Ouvrez le fichier de certificat dans un éditeur de texte
- Copier l'intégralité du contenu du fichier dans le presse-papiers
- Collez le contenu du certificat SSL signé que vous avez reçu de l'autorité de confiance dans le champ marqué "Paste Signed".
- Vous pouvez également coller les intermédiaires en dessous, en prenant soin de suivre l'ordre correct :
    1. (TOP) Votre certificat signé
    2. (2ème en partant du haut) Intermédiaire 1
    3. (3ème en partant du haut) Intermédiaire 2
    4. (En bas) Intermédiaire 3
    5. Autorité de certification racine Il n'est pas nécessaire de les ajouter car ils existent sur les machines clientes.
       (l'ADC contient également un bundle racine pour le re-cryptage lorsqu'il agit comme un client d'un serveur réel).
- Cliquez sur Installer
- Une fois que vous avez installé le certificat, vous devriez voir le statut (Trusted) à côté de votre certificat.

Si vous avez fait une erreur ou si vous avez saisi le mauvais ordre intermédiaire, sélectionnez le certificat (de confiance) et ajoutez à nouveau les certificats (y compris le certificat signé) dans le bon ordre, puis cliquez sur Installer.

Ajouter un intermédiaire

Il est parfois nécessaire d'ajouter les certificats intermédiaires séparément. Par exemple, vous avez peut-être importé un certificat qui ne comporte pas les certificats intermédiaires.

- Mettre en évidence un certificat (de confiance) ou un certificat (importé)
- Coller les intermédiaires l'un après l'autre en veillant à ce que l'intermédiaire le plus proche de l'autorité de certification soit collé en dernier.
- Cliquez sur Ajouter un intermédiaire.

Si vous faites une erreur dans la commande, vous pouvez répéter le processus et ajouter à nouveau les intermédiaires. Cette action ne fera qu'écraser les intermédiaires précédents.

Supprimer un certificat

Vous pouvez supprimer un certificat en utilisant le bouton Supprimer. Une fois supprimé, le certificat sera entièrement retiré du CDA et devra être remplacé, puis réappliqué aux services virtuels si nécessaire.

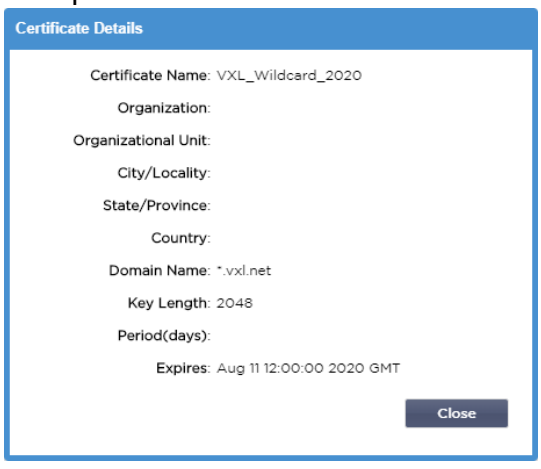
Note : Veuillez vous assurer que le certificat n'est pas attaché à un VIP opérationnel avant de le supprimer.

Renouveler un certificat

Le bouton Renouveler vous permet d'obtenir une nouvelle demande de signature de certificat. Cette action est nécessaire lorsque le certificat arrive à expiration et doit être renouvelé.

- Sélectionnez un certificat dans la liste déroulante ; vous pouvez choisir n'importe quel certificat ayant le statut (Pending), (Trusted) ou (Imported).
- Cliquez sur Renouveler
- Copiez les détails du nouveau CSR afin d'obtenir un nouveau certificat.

- Lorsque vous obtenez le nouveau certificat, suivez les étapes détaillées dans le document SHOW



- Il peut arriver que vous souhaitiez consulter les détails d'un certificat SSL installé.
- Sélectionnez le certificat dans le menu déroulant
- Cliquez sur le bouton Afficher
- La fenêtre popup ci-dessous sera présentée avec les détails du certificat.

- Installation d'un certificat.
- Le certificat nouveau et renouvelé sera maintenant installé dans le CDA.

Importation d'un certificat

Dans de nombreux cas, les entreprises devront utiliser les certificats signés par leur domaine dans le cadre de leur régime de sécurité interne. Les certificats doivent être au format PKCS#12, et des mots de passe protègent invariablement ces certificats.

L'image ci-dessous montre la sous-section pour l'importation d'un seul certificat SSL.

- Donnez à votre certificat un nom convivial. Ce nom permet de l'identifier dans les listes déroulantes utilisées dans le CDA. Il ne doit pas nécessairement être identique au nom de domaine du certificat, mais doit être alphanumérique et sans espace. Aucun caractère spécial autre que _ et - n'est autorisé.
- Saisissez le mot de passe que vous avez utilisé pour créer le certificat PKCS#12.
- Recherchez le fichier {nom du certificat}.pfx
- Cliquez sur Importer.
- Votre certificat sera maintenant dans les menus déroulants SSL appropriés dans le CDA.

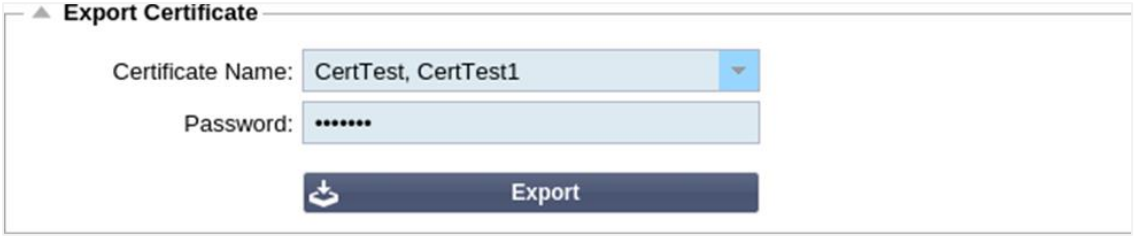
Importation de plusieurs certificats

Cette section vous permet d'importer un fichier JNBK qui contient plusieurs certificats. Un fichier JNBK est crypté et produit par ADC lors de l'exportation de plusieurs certificats.

- Recherchez votre fichier JNBK - vous pouvez en créer un en exportant plusieurs certificats.
- Saisissez le mot de passe que vous avez utilisé pour créer le fichier JNBK.
- Cliquez sur Importer.
- Vos certificats seront maintenant dans les menus déroulants SSL appropriés dans le CDA.

Exportation d'un certificat

De temps en temps, vous pouvez souhaiter exporter l'un des certificats détenus dans le CDA. Le CDA a été doté de la capacité de le faire.



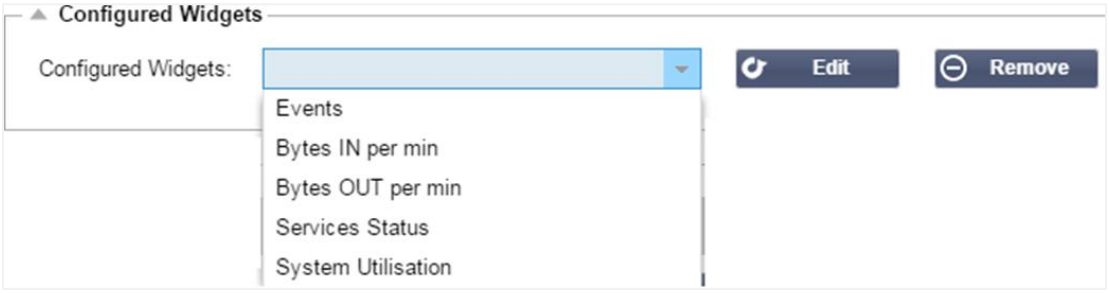
- Cliquez sur le ou les certificats que vous souhaitez installer. Vous pouvez cliquer sur l'option Tous pour sélectionner tous les certificats répertoriés.
- Saisissez un mot de passe pour protéger le fichier exporté. Le mot de passe doit comporter au moins six caractères. Vous pouvez utiliser des lettres, des chiffres et certains symboles. Les caractères suivants **ne** sont **pas** acceptés : < > " ' ( ) ; \ | \A3 % &
- Cliquez sur Exporter
- Si vous exportez un seul certificat, le fichier résultant sera nommé sslcert_{certname}.pfx. Par exemple sslcert_Test1Cert.pfx
- Dans le cas d'une exportation de plusieurs certificats, le fichier résultant sera un fichier JNBK. Le nom du fichier sera sslcert__pack.jnbk.

Note : Un fichier JNBK est un fichier conteneur crypté produit par le CDA et valable uniquement pour l'importation dans le CDA.

Widgets

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

Widgets configurés

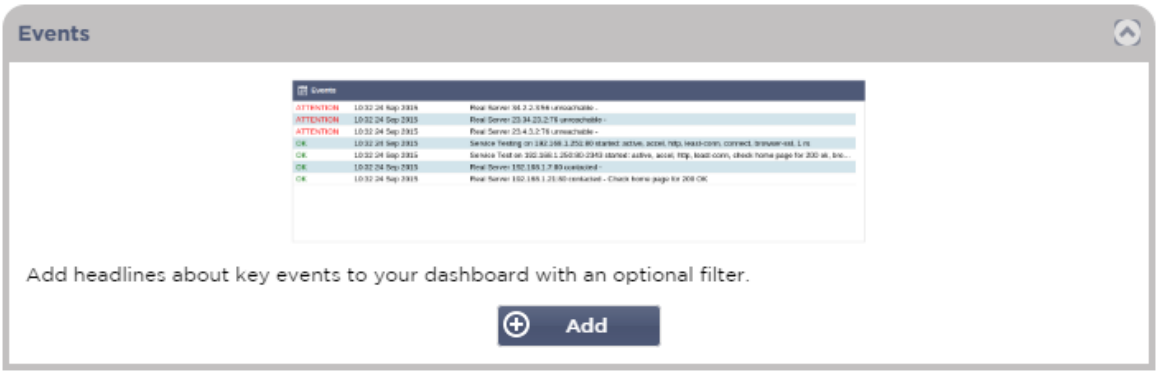


La section Widgets configurés vous permet d'afficher, de modifier ou de supprimer tout widget créé à partir de la section des widgets disponibles.

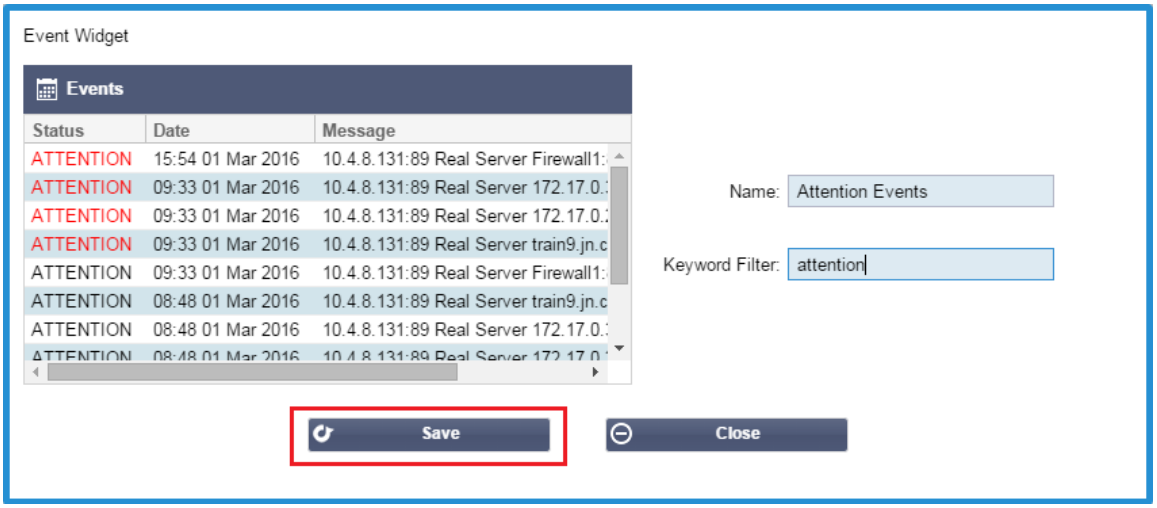
Widgets disponibles

Cinq widgets différents sont fournis dans le CDA, et vous pouvez les configurer selon vos besoins.

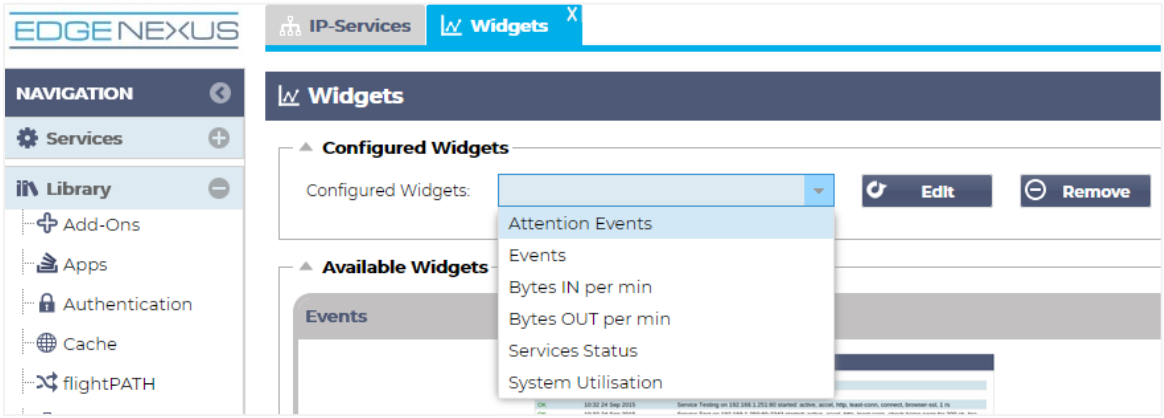
Le widget Événements



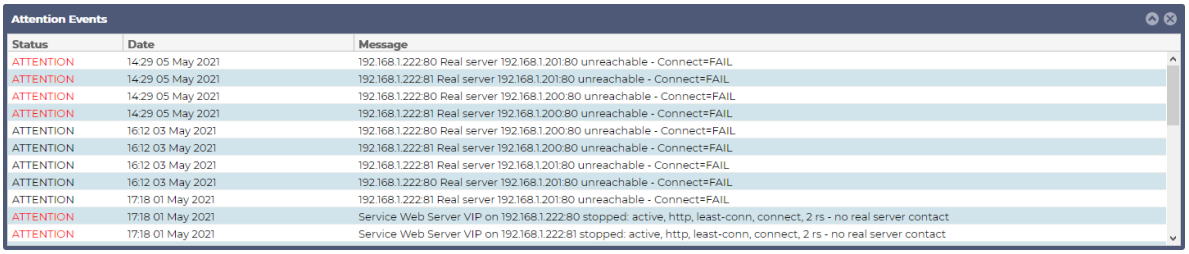
- Pour ajouter un événement au widget Événements, cliquez sur le bouton Ajouter.
- Donnez un nom à votre événement. Dans notre exemple, nous avons ajouté Attention Events comme nom d'événement.
- Ajout d'un filtre de mots-clés. Nous avons également ajouté la valeur de filtre de Attention



- Cliquez sur Enregistrer, puis sur Fermer
- Vous verrez maintenant un widget supplémentaire appelé Événements d'attention dans la liste déroulante des widgets configurés.

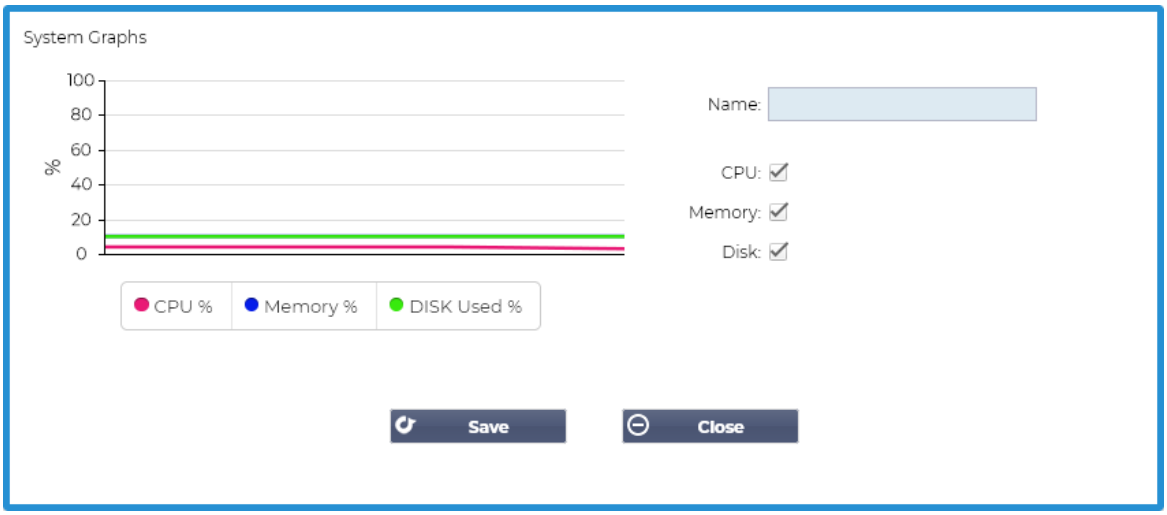


- Vous pouvez voir que nous avons maintenant ajouté ce widget dans la section Affichage > Tableau de bord.
- Sélectionnez le widget Événements Attention pour l'afficher dans le tableau de bord. Voir ci-dessous.



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

Le widget Graphiques du système

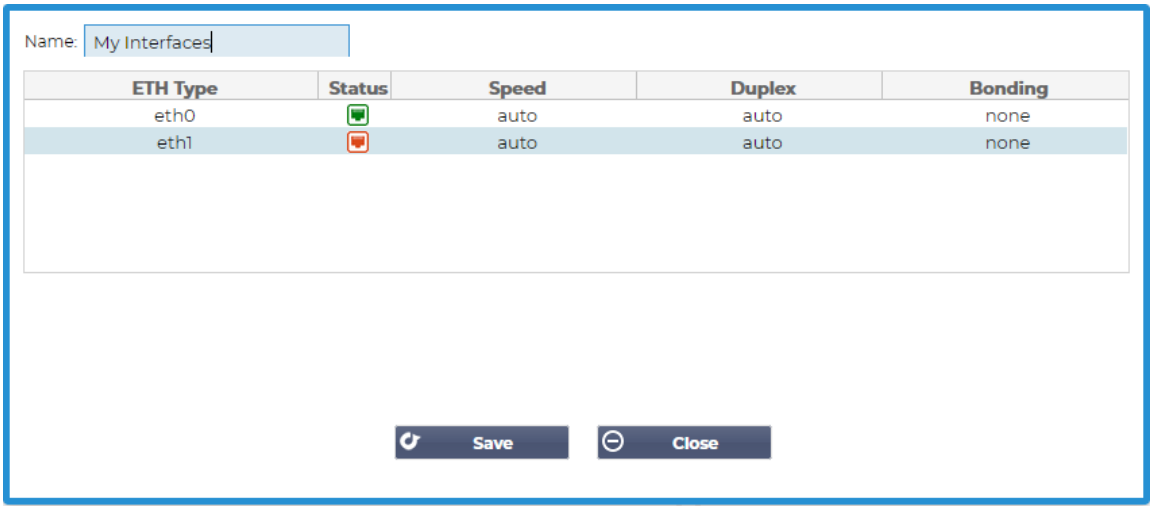


L'ADC dispose d'un widget graphique système configurable. En cliquant sur le bouton Ajouter du widget, vous pouvez ajouter les graphiques de surveillance suivants à afficher.

- CPU
- MEMOIRE
- DISQUE

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

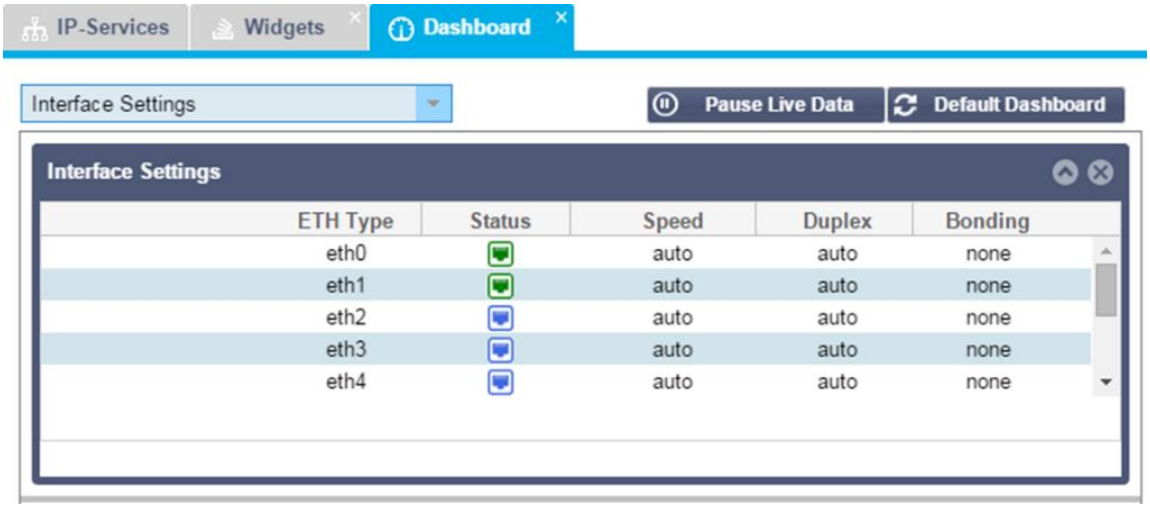
Widget d'interface



Le widget Interface vous permet d'afficher les données de l'interface réseau choisie, comme 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.

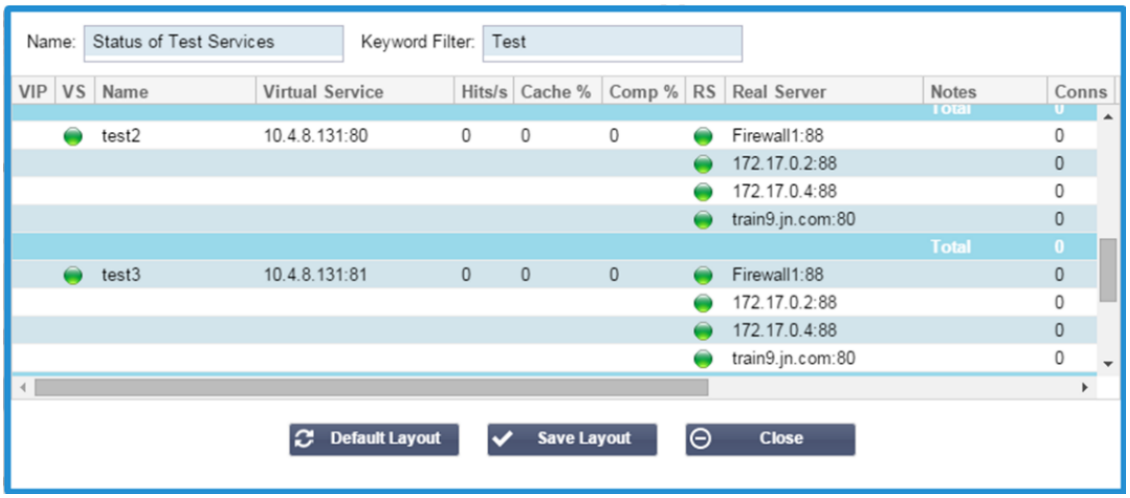
Sélectionnez le widget que vous venez de personnaliser dans le menu déroulant des widgets du tableau de bord. Vous verrez un écran comme celui ci-dessous.



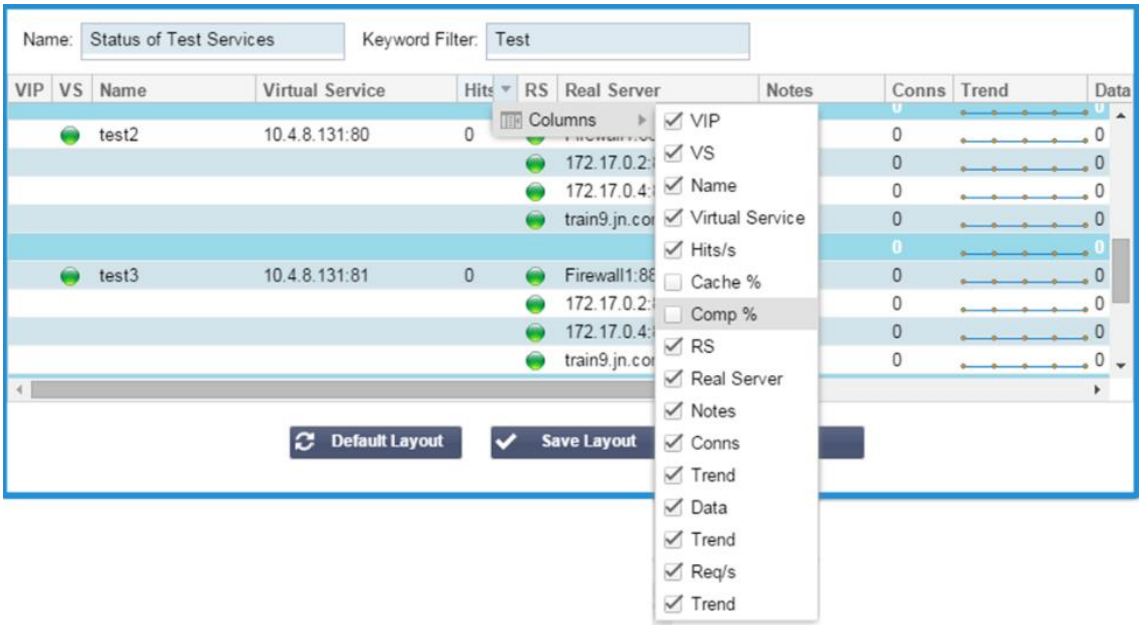
Widget d'état

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

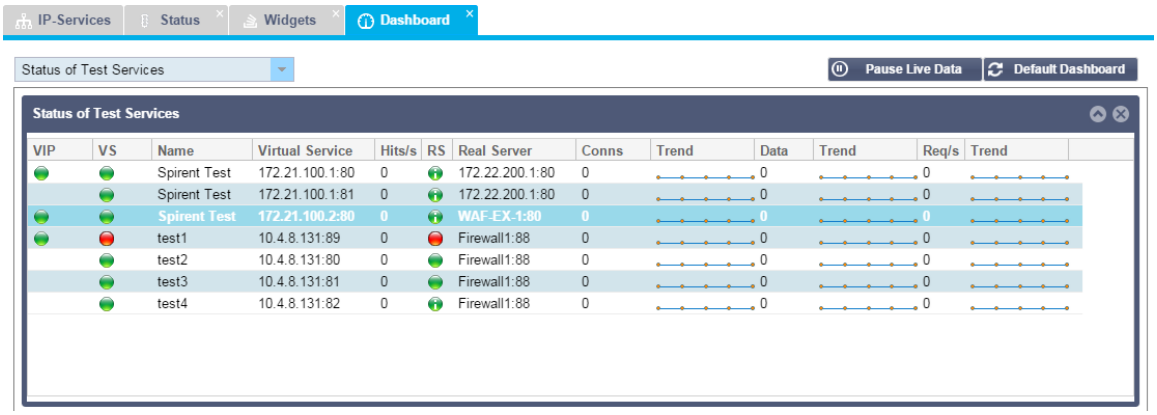
- Cliquez sur Ajouter.



- Saisissez un nom pour le service que vous souhaitez surveiller.
- Vous pouvez également choisir les colonnes que vous souhaitez afficher dans le widget.

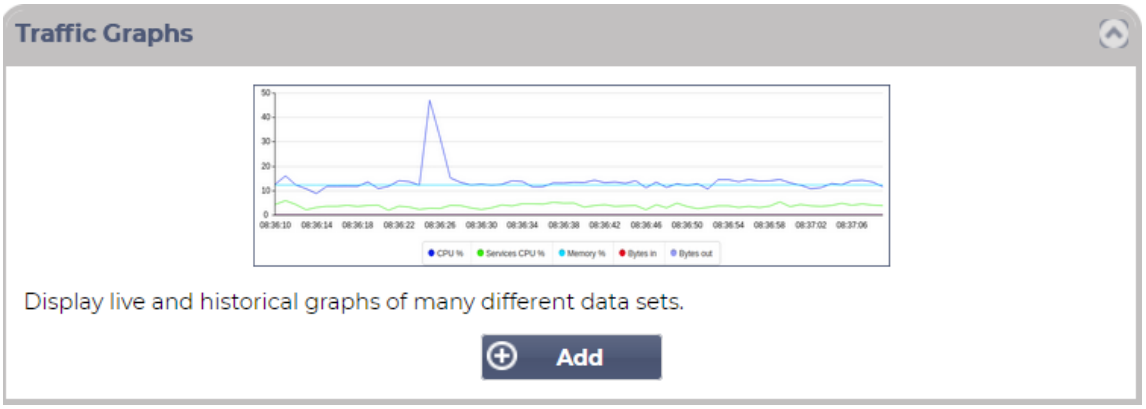


- Une fois que vous êtes satisfait, cliquez sur Enregistrer, puis sur Fermer.
- Le widget "Statut" choisi sera disponible dans la section "Tableau de bord".



Widget graphique de trafic

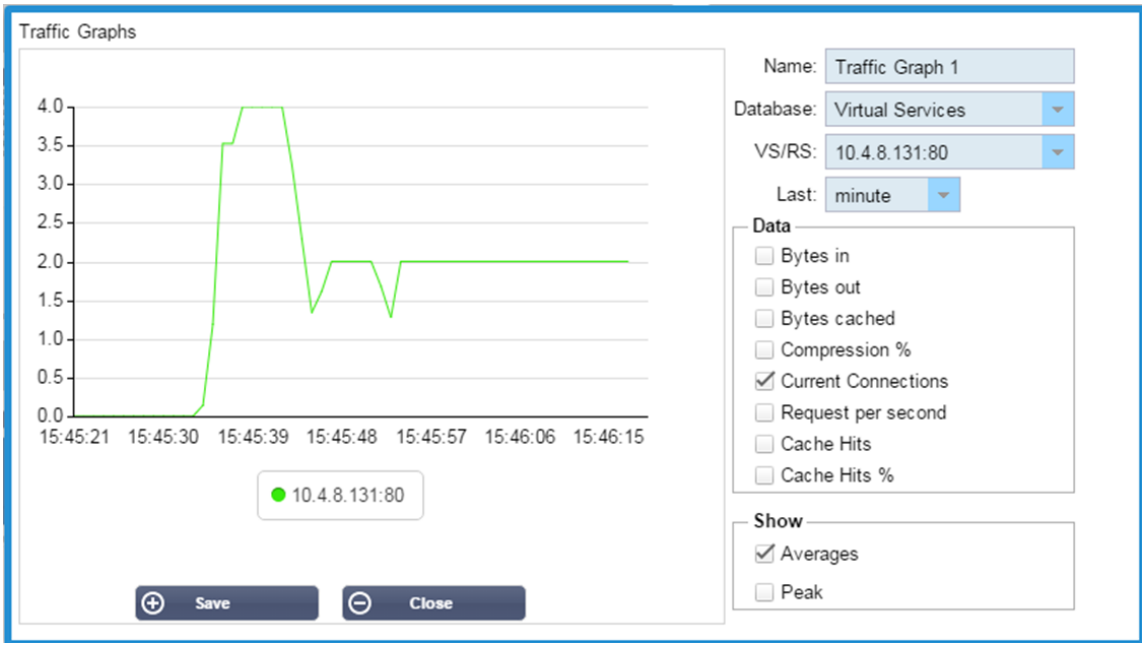
Ce widget peut être configuré pour afficher les données de trafic actuelles et historiques par services virtuels et serveurs réels. En outre, vous pouvez voir les données globales actuelles et historiques du trafic global.



- 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 de temps dans la liste déroulante Dernier.
    - Minute - dernières 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 de chaque jour au cours des sept jours précédents
    - Mois - données agrégées de chaque semaine pour les sept derniers jours
    - Année - données agrégées de chaque mois au cours des 12 mois précédents
- Choisissez les données disponibles en fonction de la base de données que vous avez choisie.
    - Base de données des services virtuels
    - Octets dans
    - Octets sortis
    - Octets mis en cache
    - % de compression
    - Connexions actuelles
    - Demandes par seconde
    - Cache Hits
    - Cache Hits (%)
- Serveurs réels
    - Octets dans
    - Octets sortis
    - Connexions actuelles
    - Demande par seconde
    - Temps de réponse
- Système
    - % DE CPU
    - Services CPU
    - % de mémoire
    - % de disque libre
    - Octets dans
    - Octets sortis
- Choisissez d'afficher les valeurs moyennes ou les valeurs de pointe.
- Une fois que vous avez choisi toutes les options, cliquez sur Enregistrer et fermer.

Exemple de graphique de trafic



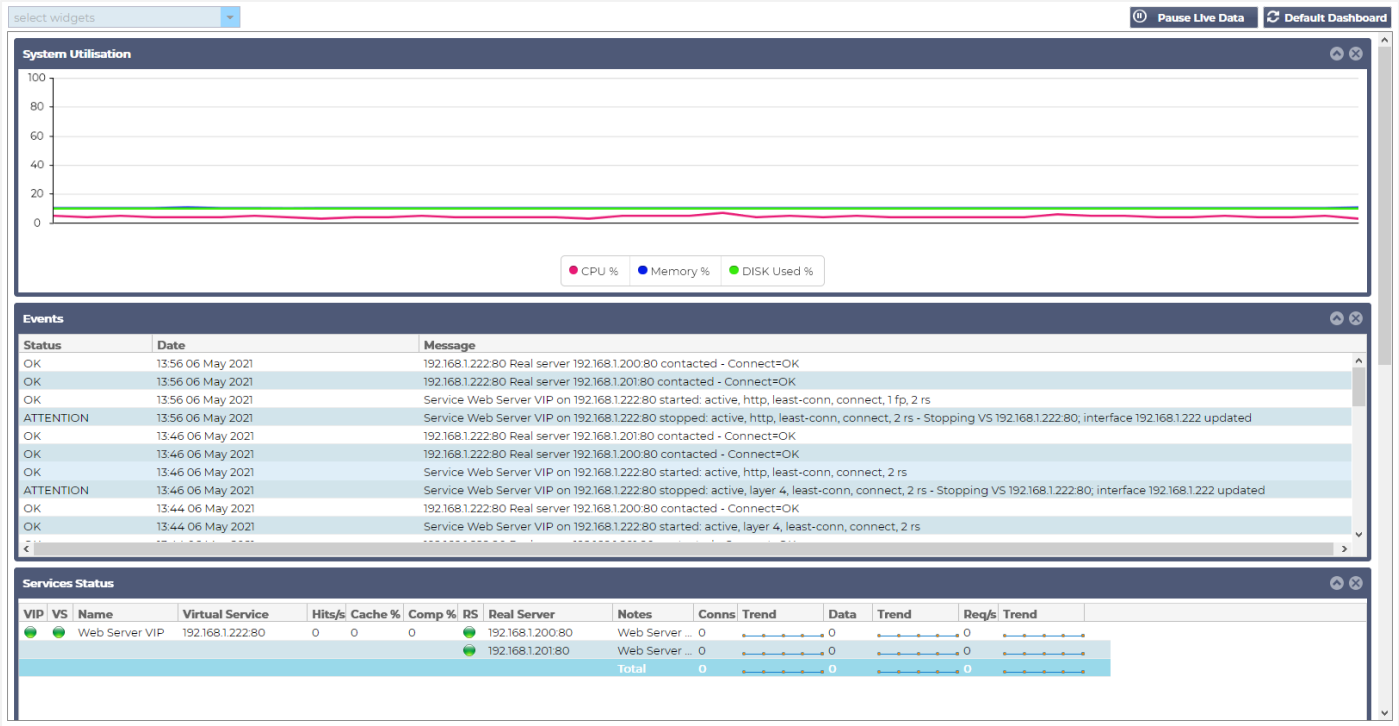
Vous pouvez maintenant ajouter votre widget Traffic Graph à la section Affichage > Tableau de bord.

Voir

Tableau de bord

Comme toutes les interfaces de gestion des systèmes informatiques, il est souvent nécessaire d'examiner les mesures de performance et les données traitées par le CDA. Nous fournissons un tableau de bord personnalisable pour que vous puissiez le faire de manière simple et significative.

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



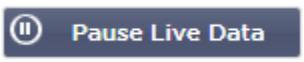
Utilisation du tableau de bord

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

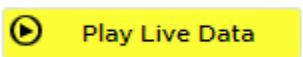
Le menu Widgets

Le menu Widgets situé en haut à gauche du tableau de bord vous permet de sélectionner et d'ajouter les widgets standard ou personnalisés que vous avez définis. Pour l'utiliser, sélectionnez le widget dans la liste déroulante.

Bouton 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. Une fois en pause, aucun widget du tableau de bord ne sera mis à jour, ce qui vous permet d'examiner le contenu à votre guise. Le bouton change d'état pour afficher Lire les données en direct dès qu'une pause est initiée.



Lorsque vous avez terminé, il suffit de cliquer sur le bouton "Play Live Data" 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 disposition par défaut du tableau de bord. Dans ce cas, cliquez sur le bouton Tableau de bord par défaut. Une fois le bouton cliqué, toutes les modifications apportées au tableau de bord seront perdues.

Redimensionnement, réduction, réorganisation et suppression des widgets

Redimensionnement d'un widget

Vous pouvez redimensionner un widget très facilement. Cliquez et maintenez enfoncé la barre de titre du widget et faites-le 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 à côté.

Minimiser un widget

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

Déplacement de l'ordre des widgets

Pour déplacer un widget, vous pouvez le faire glisser 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.

Histoire

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

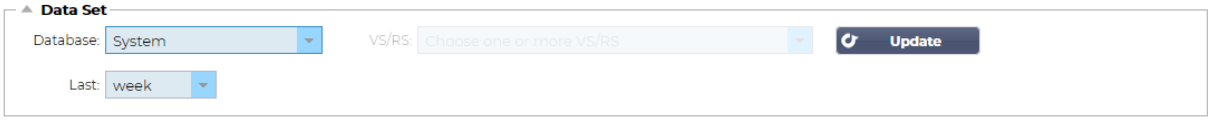
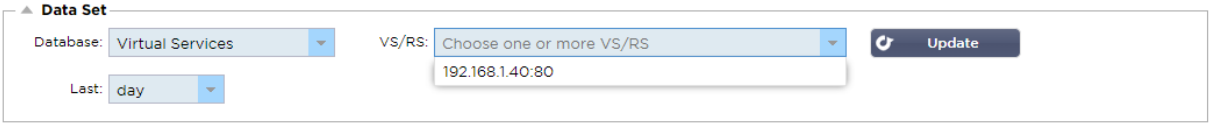
Cela vous permet également de voir l'équilibrage de la charge en action et de détecter les erreurs ou les modèles qui doivent être étudiés. Notez que vous devez activer la journalisation historique dans Système > Historique pour utiliser cette fonctionnalité.

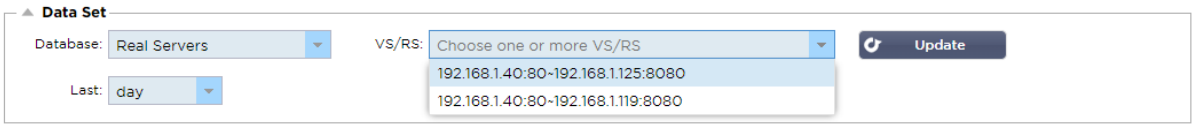
Visualisation des données graphiques

Ensemble de données

Pour visualiser les données historiques en format graphique, veuillez procéder comme suit :

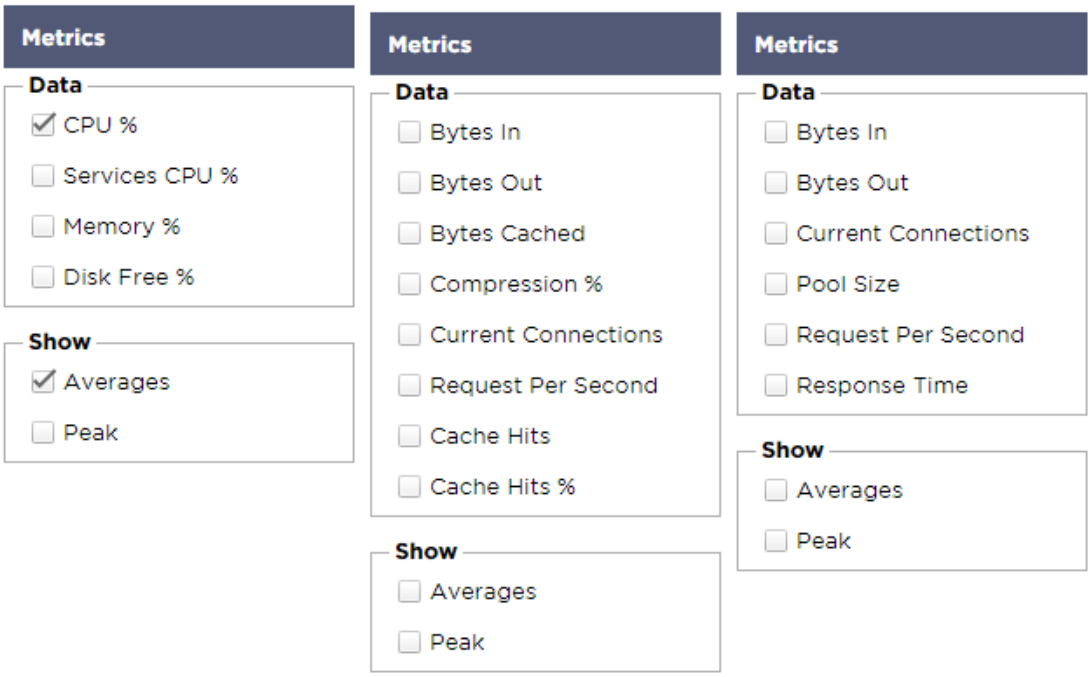
La première étape consiste à choisir la base de données et la période correspondant aux informations que vous souhaitez consulter. La période que vous pouvez sélectionner dans la liste déroulante Last est la suivante : Minute, Heure, Jour, Semaine, Mois et Année.

Base de données	Description
Système	En sélectionnant cette base de données, vous pourrez voir l'évolution du CPU, de la mémoire et de l'espace disque dans le temps. 
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. Vous verrez une liste de services virtuels 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. Vous verrez une liste de serveurs réels dans laquelle vous pouvez en sélectionner un.

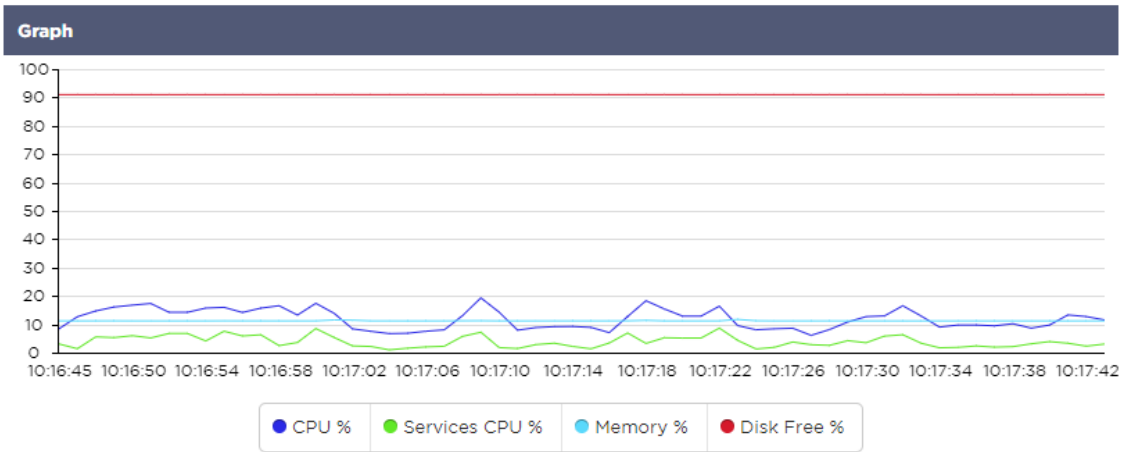


Métriques

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



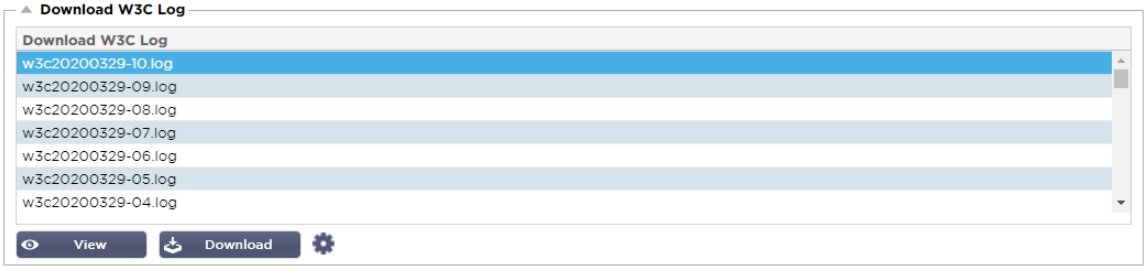
Exemple de graphique



Bûches

La page Logs de la section View vous permet de prévisualiser et de télécharger les logs du W3C et du système. La page est organisée en deux sections, comme détaillé ci-dessous.

Télécharger les 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 source, la version HTTP, le type de navigateur, la page de référence et l'horodatage. Les journaux du W3C peuvent devenir très volumineux selon la quantité de données et la catégorie de journalisation enregistrée.

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

Bouton d'affichage

Le bouton Afficher vous permet de visualiser le journal choisi dans la fenêtre d'un éditeur de texte, tel que Notepad.

Bouton de téléchargement

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

L'icône de la roue dentée

En cliquant sur cette icône, vous accédez à la section W3C Log Settings située dans System > Logging. Nous en parlerons en détail dans la section "Logging" du guide.

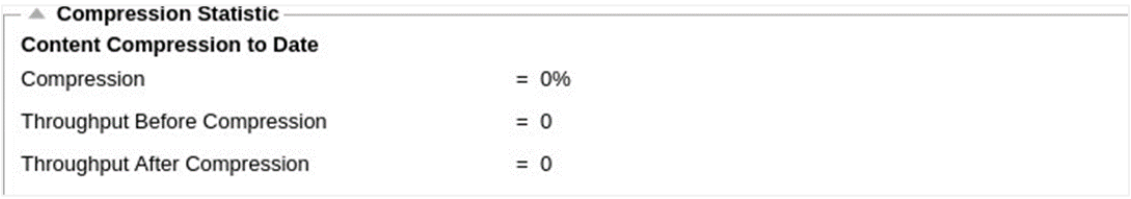
Statistiques

La section Statistiques du CDA est une zone très utilisée par les administrateurs système qui veulent s'assurer que les performances du CDA correspondent à leurs attentes.

Compression

L'objectif de l'ADC est de surveiller les données et de les diriger vers les serveurs réels configurés pour les recevoir. La fonction de compression est fournie dans l'ADC pour augmenter les performances de l'ADC. Il arrive que les administrateurs souhaitent tester et vérifier les informations relatives à la compression des données de l'ADC ; ces données sont fournies par le panneau Compression dans les statistiques.

Compression du contenu à ce jour



Les données présentées dans cette section détaillent le niveau de compression atteint par le CDA 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	= 1.93 GB		= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput From Cache	= 0		= 0.00 Mbps (data)
		Total	= 14.64 Mbps (data)

Les valeurs fournies dans cette section indiquent le niveau de compression atteint par le CDA sur l'ensemble du contenu. Le pourcentage typique dépend du nombre d'images pré-compressées 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	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

Les chiffres d'entrée/sortie totaux 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 passe de kbps à Mbps puis à Gbps.

Hits et Connexions

Hits and Connections

Overall Hits Counted	= 185033	95 Hits/sec
Total Connection	= 208194	94 / 42 connections/sec
Peak Connections	= 29	1 current connections

La section Hits et Connexions contient les statistiques globales des hits et des transactions qui passent par le CDA. Que signifient les hits et les connexions ?

- Un Hit est défini comme une transaction de la couche 7. Typiquement 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 couche 4. De nombreuses transactions peuvent avoir lieu sur une seule connexion TCP.

Nombre total de coups comptés

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 d'occurrences par seconde.

Total des connexions

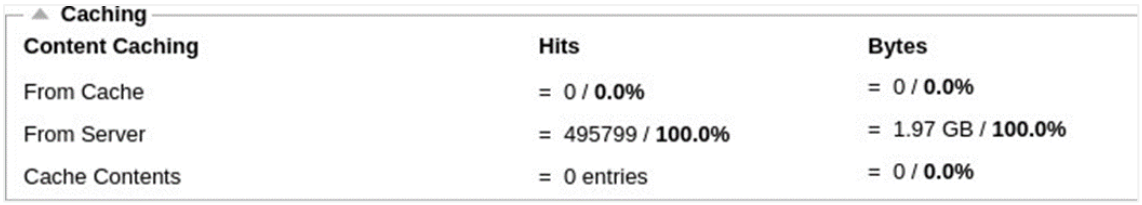
La valeur Total Connections représente le nombre cumulé de connexions TCP depuis la dernière réinitialisation. Le chiffre de la deuxième colonne indique le nombre de connexions TCP par seconde effectuées vers l'ADC. Le chiffre de la colonne de droite est le nombre de connexions TCP par seconde effectuées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

Connexions de pointe

La valeur maximale de Connexions représente le nombre maximum de connexions TCP effectuées vers l'ADC. Le chiffre de la colonne la plus à droite indique le nombre actuel de connexions TCP actives.

Mise en cache

Comme vous vous en souvenez, le CDA est équipé à la fois de la compression et de la mise en cache. Cette section présente les statistiques globales liées 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.



Depuis le cache

Hits : La première colonne donne le nombre total de transactions servies par le cache du CDA 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 le cache du CDA. Un pourcentage des données totales est également fourni.

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 du total des données est également fourni.

Contenu du cache

Hits : Ce nombre donne le nombre total d'objets contenus dans le cache du CDA.

Octets : Le premier nombre donne la taille globale en mégaoctets des objets mis en cache par le CDA. Un pourcentage de la taille maximale du cache est également indiqué.

Matériel informatique

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

Utilisation du disque

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

Utilisation de la mémoire

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

Utilisation du CPU

L'une des valeurs critiques fournies est le pourcentage du CPU actuellement utilisé par le CDA. Il est naturel qu'il fluctue.

Statut

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

Détails du service virtuel

Colonne VIP

La couleur de la lumière 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.
●	Statut de la recherche
●	Pas de licence ou des IP virtuelles sous licence dépassées

Colonne d'état VS

Statut	Description
●	En ligne
●	Failover-Standby. Ce service virtuel est en attente à chaud
●	Indique qu'un "passif" attend un "actif".
●	Service Needs attention. Cette indication d'état peut résulter d'un serveur réel qui échoue à un contrôle de santé ou qui a été changé manuellement en 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.
●	Statut de la recherche
●	Pas de licence ou des IP virtuelles sous licence dépassées

La couleur de la lumière indique l'état du service virtuel.

Nom

Le nom du service virtuel

Service virtuel (VIP)

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

Hit/Sec

Couche 7 transactions par seconde du 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 l'ADC.

Statut RS (serveur distant)

Statut	Description
●	Connecté
●	Non surveillé
●	Drainage ou hors ligne
●	Standby
●	Non connecté
●	Statut de la recherche
●	Pas de licence ou des IP virtuelles sous licence dépassées

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

Serveur réel

L'adresse IP et le port du serveur réel.

Notes

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

Conns (Connexions)

La représentation du nombre de connexions à chaque serveur réel vous permet de voir l'équilibrage de la charge en action. Très utile pour vérifier que votre politique d'équilibrage de charge fonctionne correctement.

Données

La valeur de cette colonne indique la quantité de données envoyées à chaque serveur réel.

Req/Sec (Demandes par seconde)

Le nombre de demandes par seconde envoyées à chaque serveur réel.

Système

Le segment Système de l'interface utilisateur de l'ADC vous permet d'accéder et de contrôler tous les aspects du système de l'ADC.

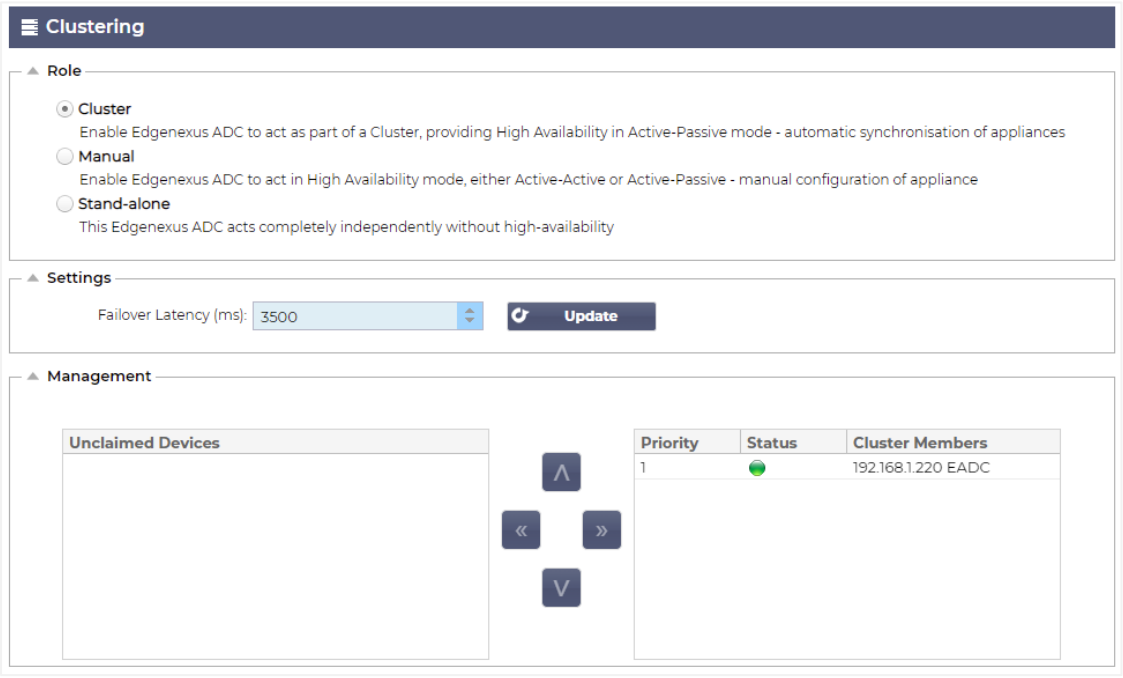
Regroupement

L'ADC peut être utilisé comme un dispositif autonome unique, et il fonctionnera parfaitement bien dans ce cas. Cependant, si l'on considère que l'objectif de l'ADC est d'équilibrer la charge des ensembles de serveurs, la nécessité de mettre l'ADC lui-même en cluster devient évidente. L'interface utilisateur de l'ADC est facile à naviguer, ce qui rend la configuration du système de mise en grappe très simple.

La page Système > Clustering est l'endroit où vous allez configurer la haute disponibilité de vos appliances ADC. Cette section est organisée en plusieurs parties.

Note importante

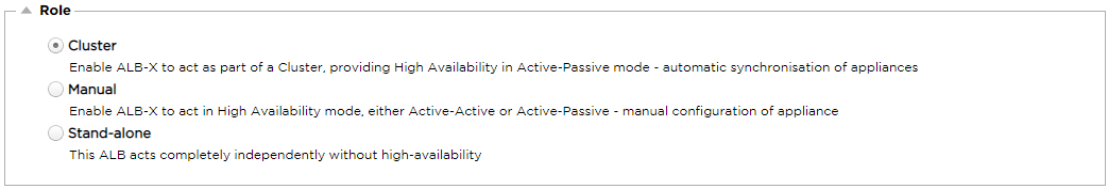
- Il n'est pas nécessaire de disposer d'un câble dédié entre la paire d'ADC pour maintenir un battement de cœur à haute disponibilité.
- Le heartbeat a lieu sur le même réseau que le service virtuel qui nécessite la mise en place de la haute disponibilité.
- Il n'y a pas de basculement d'état entre les appareils 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 unicast et le protocole ARP gratuit pour informer les nouveaux commutateurs de l'équilibreur de charge actif.



Rôle

Il y a trois rôles de cluster disponibles lorsque vous configurez l'ADC pour la haute disponibilité.

Cluster



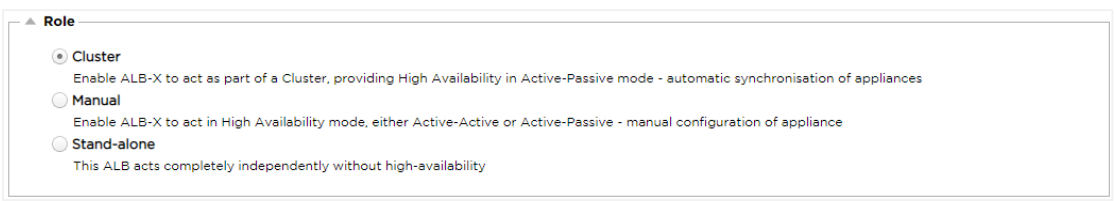
- Par défaut, un nouvel ADC sera mis sous tension en utilisant le rôle Cluster. Dans ce rôle, chaque membre du cluster aura la même "configuration de travail", et en tant que tel, un seul ADC dans le cluster sera actif à tout moment.
- Une "configuration de travail" désigne tous les paramètres de configuration, 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.
- Le CDA en priorité 1, la position la plus haute, de la boîte des membres du cluster est le propriétaire du cluster et l'équilibreur de charge actif, tandis que tous les autres CDA sont des membres passifs.
- Vous pouvez modifier n'importe quel ADC du Cluster, et les modifications seront synchronisées avec tous les membres du Cluster.
- Lorsque vous supprimez un ADC du Cluster, tous les Services Virtuels seront supprimés de cet ADC.
- Vous ne pouvez pas supprimer le dernier membre du Cluster dans les Périphériques non réclamés. Pour supprimer le dernier membre, veuillez changer le rôle en Manuel ou Autonome.
- Les objets suivants ne sont pas synchronisés :
    - Section Date & Heure manuelle - (la section NTP est synchronisée)
    - Latence de basculement (ms)
    - Section matériel
    - Section des appareils
    - Section réseau

Défaillance du propriétaire de la grappe

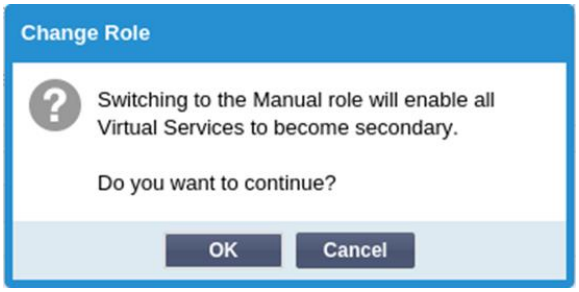
- Lorsqu'un propriétaire de cluster tombe en panne, l'un des membres restants prend automatiquement le relais et assure l'équilibrage du trafic.
- Lorsque le propriétaire du cluster revient, il reprend le trafic d'équilibrage de charge et reprend le rôle de propriétaire.
- Supposons que le propriétaire 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 le trafic d'équilibrage de charge devienne le nouveau propriétaire, mettez le membre en surbrillance et cliquez sur la flèche vers le haut pour le faire passer en position de priorité 1.
- Si vous modifiez l'un des membres restants du cluster et que le propriétaire est en panne, le membre modifié sera automatiquement promu au rang de propriétaire sans perte de trafic.

Changement de rôle du rôle Cluster au rôle Manuel

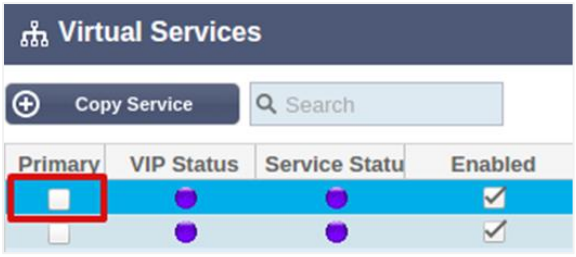
- Si vous souhaitez changer le rôle de Cluster à Manuel, cliquez sur le bouton radio à côté de l'option de rôle Manuel.



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



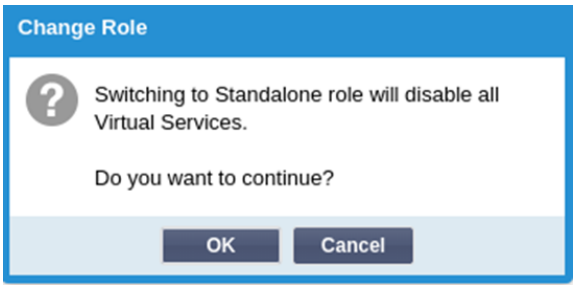
- Cliquez sur le bouton OK
- Vérifiez la section Services virtuels. Vous constaterez que la colonne Primary affiche désormais une case non cochée.



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

Changement de rôle d'un Cluster à un Stand-alone

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



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

Rôle manuel

Un ADC dans le rôle Manuel travaillera avec d'autres ADC dans le rôle Manuel pour fournir une haute disponibilité. Le principal avantage par rapport au rôle Cluster est la possibilité de définir quel ADC est actif pour une IP virtuelle. L'inconvénient est qu'il n'y a pas de synchronisation de la configuration entre les ADC. Tout changement doit être répliqué manuellement sur chaque boîtier 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 primaire (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 sera active.
    - Si les deux ne sont pas cochés, le même processus d'élection a lieu. De plus, si les deux sont décochés, il n'y a pas de retour automatique au CDA actif d'origine.

Rôle autonome

Un CDA dans le rôle autonome ne communiquera avec aucun autre CDA concernant ses services, et donc tous les services virtuels resteront dans le statut 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.

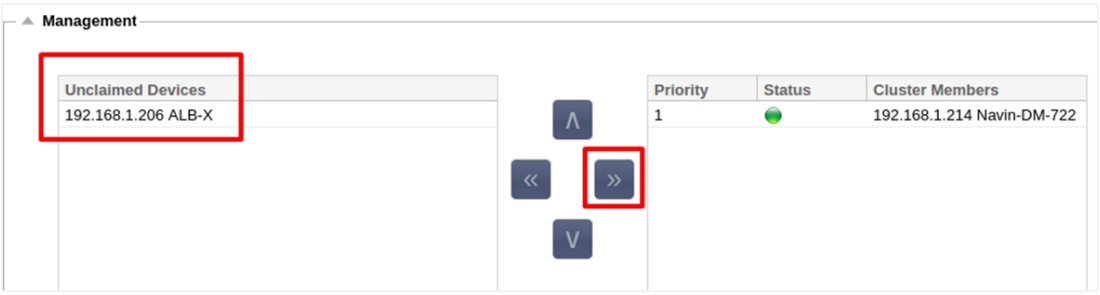
Paramètres

Dans la section Paramètres, vous pouvez définir la latence de basculement en millisecondes, le temps qu'un CDA passif attendra avant de prendre en charge les services virtuels après la défaillance du CDA 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 rencontrez une instabilité dans le cluster avec une latence inférieure, vous devez augmenter cette valeur.

Gestion

Dans cette section, vous pouvez ajouter et supprimer des membres du cluster tout en modifiant la priorité d'un ADC dans le cluster. La section se compose de deux panneaux et d'un ensemble de touches fléchées entre les deux. La zone de gauche est celle des dispositifs non réclamés, tandis que la zone la plus à droite est le cluster lui-même.

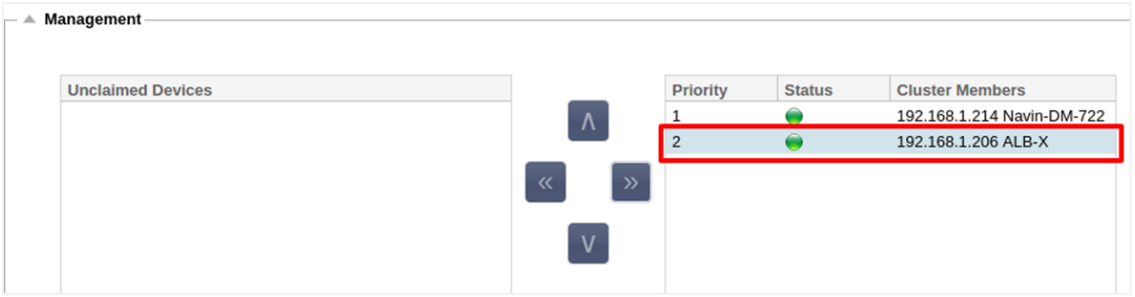


Ajout d'un ADC au cluster

- Avant d'ajouter l'ADC au cluster, vous devez vous assurer que tous les appareils ADC ont reçu un nom unique dans la section Système > Réseau.
- Vous devriez voir l'ADC en tant que Priorité 1 avec le Statut vert et son nom dans la colonne des Membres du Cluster dans la section de gestion. Cet ADC est l'appareil primaire par défaut.

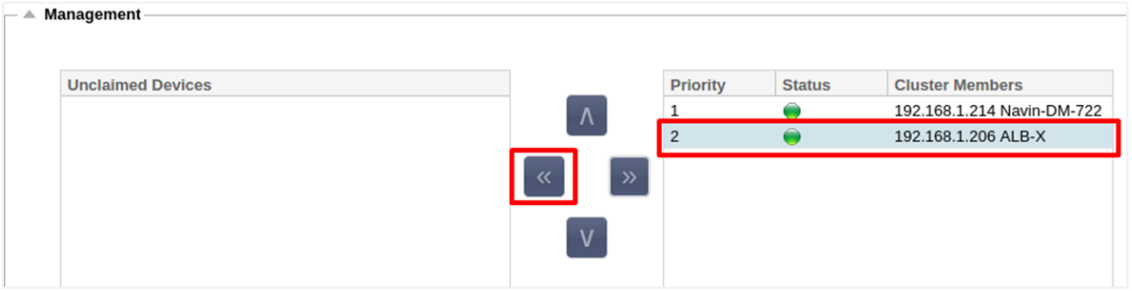
- Tous les autres ADC disponibles apparaîtront dans la fenêtre Dispositifs non réclamés de la section de gestion. Un dispositif non réclamé est l'ADC qui a été assigné dans le rôle de cluster mais qui n'a pas de services virtuels configurés.
- Mettez en surbrillance l'ADC de la fenêtre Unclaimed Devices et cliquez sur le bouton de la flèche droite.
- Vous verrez maintenant le message suivant :

- Cliquez sur OK pour promouvoir l'ADC sur le cluster.
- Votre CDA doit maintenant apparaître comme Priorité 2 dans la liste des membres du cluster.



Suppression d'un membre du cluster

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

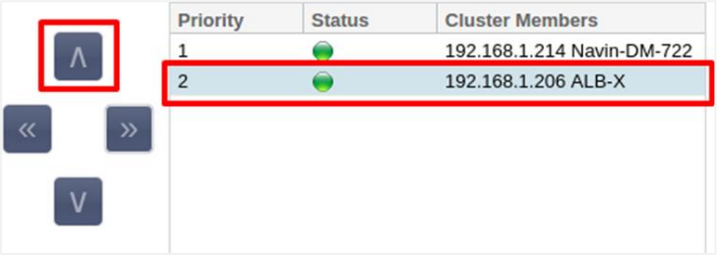


- Une demande de confirmation vous sera présentée.
- Cliquez sur OK pour confirmer.
- Votre CDA sera supprimé et apparaîtra du côté des dispositifs non réclamés.

Changement de la priorité d'un ADC

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

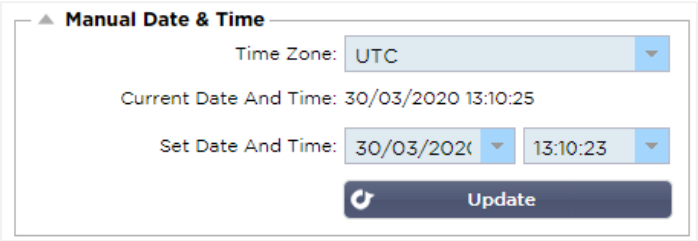
- L'ADC en haut de la liste des membres du cluster a la priorité 1 et est l'ADC actif pour tous les services virtuels.
- Le CDA qui est deuxième dans la liste reçoit la priorité 2 et est le CDA passif pour tous les services virtuels.
- Pour changer le CDA actif, il suffit de le mettre en évidence et de cliquer sur la flèche vers le haut jusqu'à ce qu'il soit en haut de la liste.



Date et heure

La section date et heure permet de définir les caractéristiques de la date et de l'heure du CDA, y compris le fuseau horaire dans lequel le CDA 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 le CDA est situé.

- Cliquez sur le menu déroulant du fuseau horaire et commencez à taper votre position.
  Par exemple, Londres
- Lorsque vous commencerez à taper, l'ADC affichera 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 à Londres, par exemple, 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.

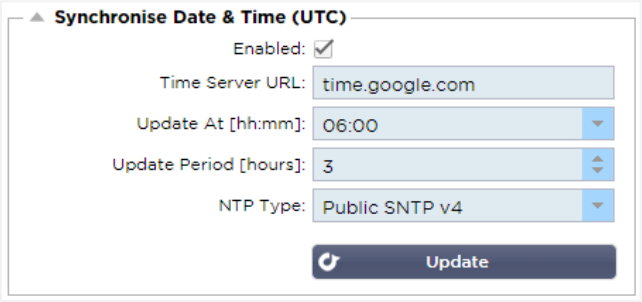
Définir la date et l'heure

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 au format suivant hh : mm : ss, par exemple, 06:00:10 pour 6 heures et 10 secondes.
- Une fois que vous l'avez saisie correctement, veuillez cliquer sur Mettre à jour pour postuler.
- Vous devriez alors voir la nouvelle date et heure 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 comporte des limitations d'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 un serveur situé dans le monde entier sur Internet, nous vous recommandons 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**

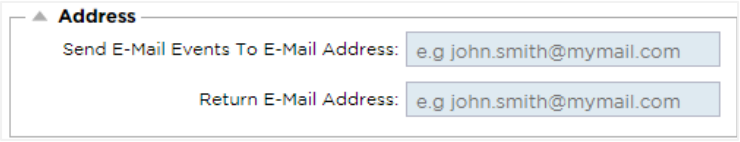
Remarque : Veuillez noter que la synchronisation se fait uniquement en UTC. Si vous souhaitez définir une heure locale, vous ne pouvez le faire que manuellement. Cette limitation sera modifiée dans les versions ultérieures afin de permettre la sélection d'un fuseau horaire.

Événements par courriel

L'ADC est un appareil critique, et comme tout système essentiel, il est équipé de la capacité d'informer l'administration des systèmes de tout problème qui pourrait 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 de courriel

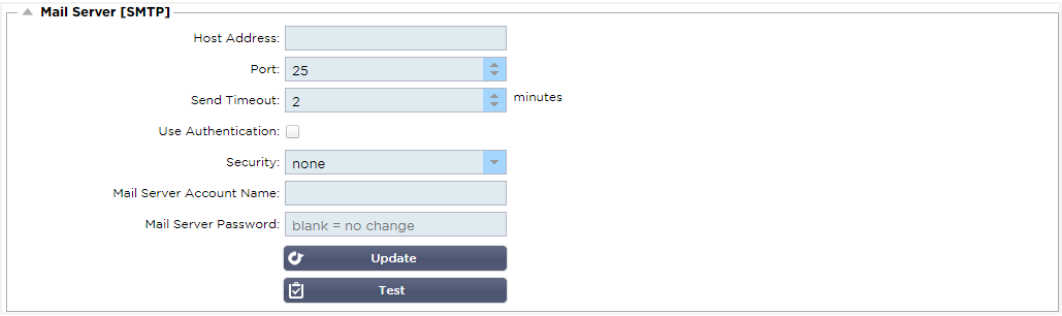
Ajoutez une adresse électronique valide à laquelle envoyer les alertes, les notifications et les événements. Exemple support@domain.com.

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 e-mails. Veuillez vous assurer que l'adresse électronique que vous utilisez pour l'envoi est autorisée à le faire.



Adresse de l'hôte

Ajoutez l'adresse IP de votre serveur SMTP.

Port

Ajoutez le port de votre serveur SMTP. Le port par défaut pour le 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 paramètre par défaut est aucun.
- SSL - Utilisez ce paramètre si votre serveur SMTP requiert une authentification Secure Sockets Layer.
- TLS - Utilisez ce paramètre si votre serveur SMTP requiert une authentification Transport Layer Security.

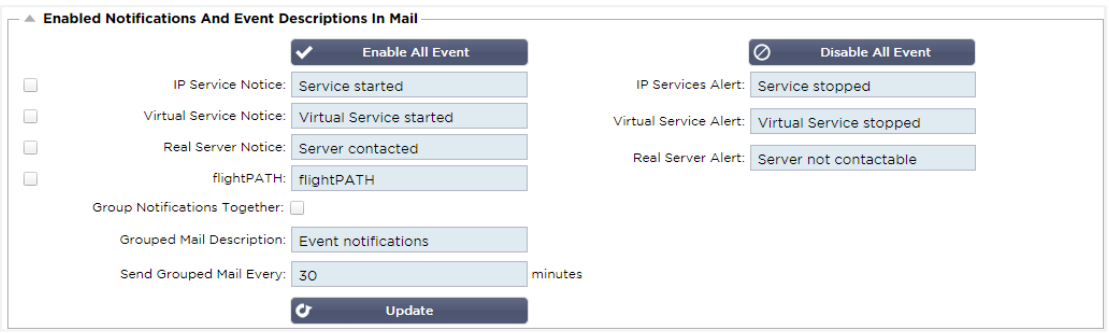
Nom du compte du serveur principal

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 le CDA 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 les canaux démarrés. Les alertes se produisent lorsque les serveurs réels ne peuvent pas être contactés ou que les canaux cessent de fonctionner.

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 exécutée pour tous les services virtuels qui appartiennent au VIP.

Service virtuel

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

Serveur réel

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

flightPATH

Cet avis est un courriel envoyé lorsqu'une condition a été remplie et qu'une action a été configurée pour demander au CDA d'envoyer un courriel sur l'événement.

Notifications de groupe

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

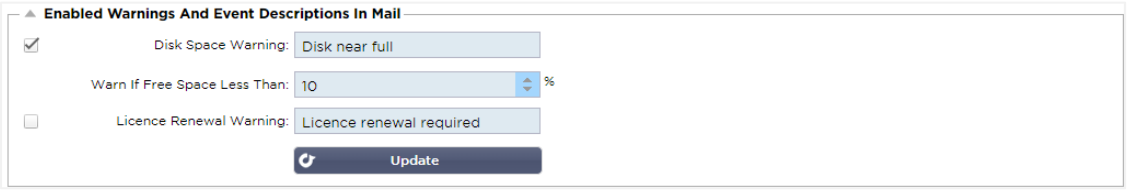
Description du courrier de groupe

Indiquez l'objet pertinent de l'e-mail de notification de groupe.

Intervalle d'envoi de groupe

Stipulez le temps que vous souhaitez attendre avant d'envoyer un e-mail de notification de groupe. Le délai minimum est de 2 minutes.

Avertissements



Il existe deux types de courriels 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 courriel vous est envoyé.

Expiration de la licence

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

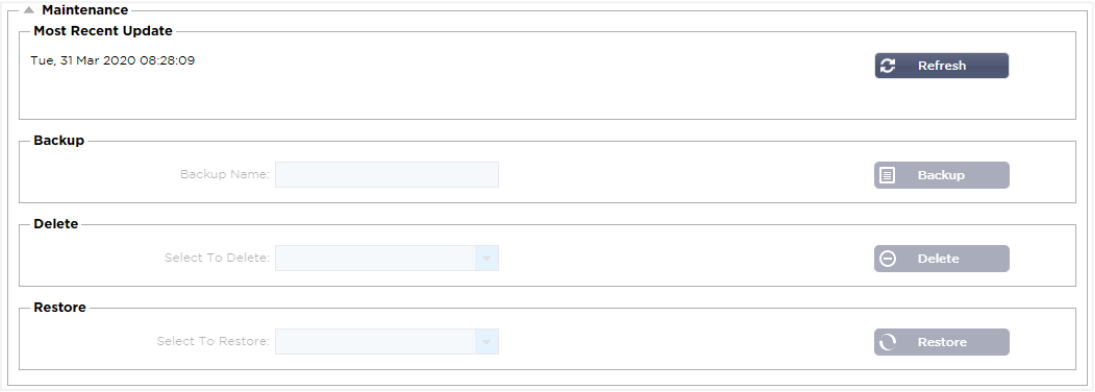
Historique du système

Dans la section Système, il y a l'option Historique du système, qui permet de fournir des données historiques pour des éléments tels que le CPU, la mémoire, les demandes par seconde et d'autres caractéristiques. Une fois cette option activée, vous pouvez visualiser les résultats sous forme de graphique via la page Affichage > Historique. Cette page vous permet également de sauvegarder ou de restaurer vos fichiers d'historique sur le CDA local.

Collecte des données

- Pour permettre la collecte de données, veuillez cocher la case.
- Ensuite, définissez l'intervalle de temps auquel vous souhaitez que l'ADC collecte les données. Cette valeur de temps peut être comprise entre 1 et 60 secondes.

Maintenance



Cette section sera grisée si vous avez activé la journalisation historique. Veuillez décocher la case Activé dans la section Collecte de données et cliquez sur Mettre à jour pour autoriser la maintenance des journaux historiques.

Sauvegarde

Donnez un nom descriptif à votre sauvegarde. Cliquez sur Sauvegarde pour sauvegarder tous les fichiers sur le CDA.

Supprimer

Sélectionnez un fichier de sauvegarde dans la liste déroulante. Cliquez sur Supprimer pour supprimer le fichier de sauvegarde du CDA.

Restaurer

Sélectionnez un fichier de sauvegarde précédemment stocké. Cliquez sur Restaurer pour remplir les données de ce fichier de sauvegarde.

Licence

L'utilisation de l'ADC est autorisée par l'un des modèles suivants, qui dépend des paramètres d'achat et du type de client.

Type de licence	Description
Perpétuel	Vous, le client, avez le droit d'utiliser le CDA et les autres logiciels à perpétuité. Cela ne vous empêche pas d'avoir à acheter un support pour recevoir de l'aide et des mises à jour.
SaaS	SaaS ou Software-as-a-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 pour utiliser le logiciel.
MSP	Les fournisseurs de services gérés peuvent offrir l'ADC en tant que service et acheter la licence sur une base par VIP, facturée et payée annuellement.

Détails de la licence

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

Numéro de licence

Cet ID de licence est directement lié à l'ID de la machine et à d'autres détails spécifiques à votre achat et à votre CDA. Ces informations sont essentielles et sont requises lorsque vous souhaitez récupérer des mises à jour et d'autres éléments sur l'App Store.

ID de la machine

L'ID de la machine est généré en utilisant l'adresse IP eth0 d'un appareil ADC virtuel et l'ID MAC d'un ADC matériel. Si vous changez l'adresse IP d'un appareil ADC virtuel, la licence ne sera plus valide. Vous devrez contacter le support technique pour obtenir de l'aide. Nous vous recommandons d'attribuer une adresse IP fixe à votre/vos appareil(s) ADC virtuel(s), avec l'instruction de ne pas la modifier. L'assistance technique est disponible en créant un ticket sur HTTPs://edgenexus.io.

Note : Vous ne devez pas changer l'adresse IP ou le MAC ID de vos appareils ADC. Si vous êtes dans une structure virtualisée, veuillez fixer l'ID MAC et l'adresse IP.

Délivré à

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

Personne de contact

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

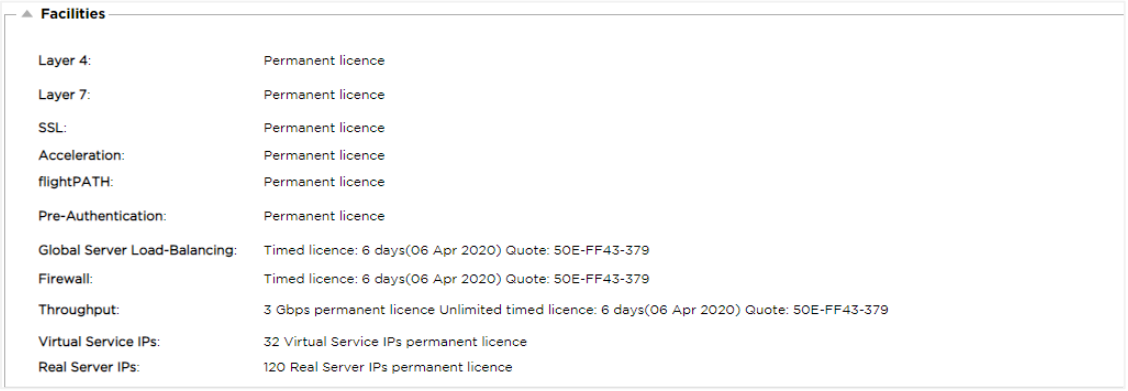
Questions de date

La date à laquelle la licence a été délivrée

Nom

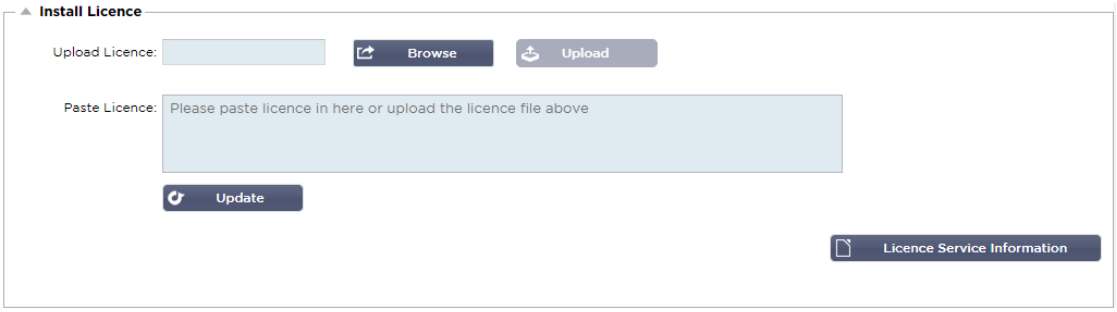
Cette valeur indique le nom descriptif de l'appareil ADC que vous avez fourni.

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 qui a été 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



- L'installation d'une nouvelle licence est très simple. Lorsque vous recevez votre nouvelle licence ou votre licence de remplacement d'Edgenexus, elle est envoyée sous la forme d'un fichier texte. Vous pouvez ouvrir le fichier, puis copier et coller le contenu dans le champ " Coller la licence ".
- Vous pouvez également le télécharger sur 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 de support.

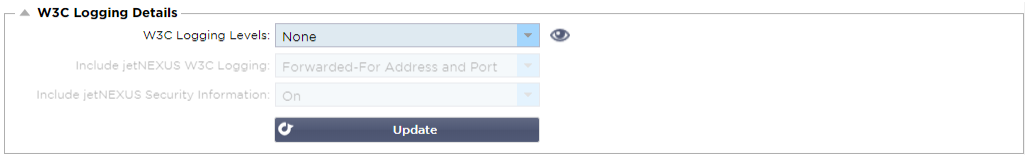
Enregistrement

La page Système > Journalisation vous 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 la journalisation du W3C

En activant la journalisation W3C, l'ADC commence à enregistrer un fichier journal compatible 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 en texte ASCII, avec des colonnes délimitées par des espaces. Le fichier contient des lignes de

commentaires commençant par le caractère #. L'une de ces lignes de commentaires est une ligne indiquant les champs (en fournissant des noms de colonnes) afin que les données puissent être exploitées. Il existe des fichiers séparés 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.

Valeur	Description
Aucun	La journalisation du W3C est désactivée.
Brief	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).
Full	Il s'agit d'un format plus compatible avec le processeur, avec des champs séparés pour la date et l'heure. Consultez le résumé des champs ci-dessous pour savoir ce qu'ils signifient. Les champs présents sont : #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 à "Complet" mais comporte un champ supplémentaire. Consultez le résumé des champs ci-dessous pour savoir ce qu'ils signifient. Les champs présents sont : #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 est rempli de toutes sortes d'informations pertinentes pour le personnel de développement et de soutien. Consultez le résumé des champs ci-dessous pour savoir ce qu'ils signifient. Les champs présents sont : #Fields : 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 le W3C HTTP.

Valeur	Description
Brief	#Fields : 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
Full	#Fields : 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	#Fields : 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

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

Inclure la journalisation W3C

Cette option vous permet de définir quelles informations sur le CDA doivent être incluses dans les journaux

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 réseau du client	Cette option inclut et affiche uniquement l'adresse IP réelle du client.
Adresse et port de l'expéditeur	Cette option montre les détails contenus dans l'en-tête XFF, y compris l'adresse et le port.
Adresse de l'expéditeur	Cette option permet d'afficher les détails contenus dans l'en-tête XFF, y compris l'adresse uniquement.

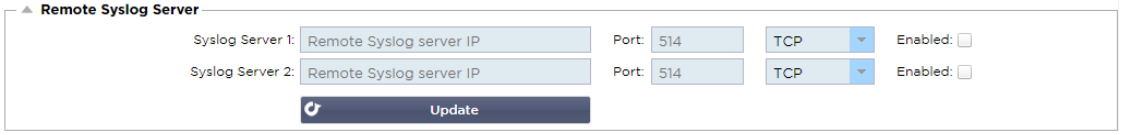
du W3C.

Inclure les informations de sécurité

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

Ce menu se compose de deux options :

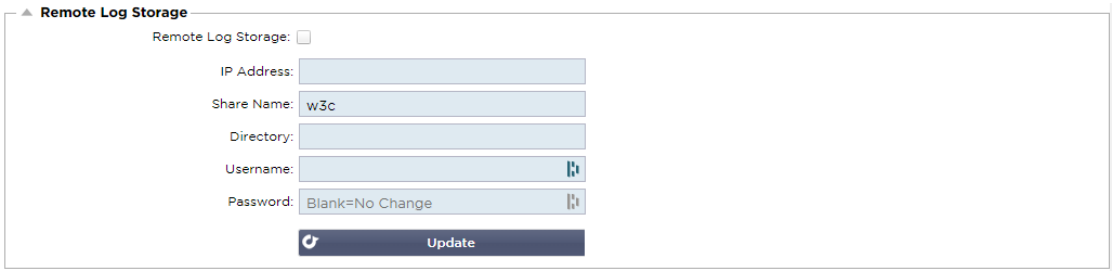
Serveur Syslog distant



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 TCP ou UDP
- Cochez la case
- Cliquez sur Mise à jour

Stockage des journaux à distance



Tous les journaux du W3C sont stockés sous forme comprimée sur le CDA toutes les heures. Les fichiers les plus anciens sont supprimés lorsqu'il reste 30 % d'espace disque. Si vous souhaitez les exporter vers un serveur distant pour les conserver, vous pouvez le configurer en utilisant un partage SMB. Veuillez noter que le journal 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 dans une appliance de machine virtuelle et cinq heures pour une appliance matérielle.

Nous inclurons un bouton de test dans les prochaines versions afin de vérifier que vos paramètres sont

Col1	Col2
Stockage des journaux à distance	Cochez la case pour activer le stockage des journaux à distance
Adresse IP	Indiquez l'adresse IP de votre serveur SMB. Celle-ci doit être en notation décimale pointillée. Exemple : 10.1.1.23
Nom de l'action	Spécifiez 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	Spécifiez le mot de passe pour le partage SMB

corrects.

Résumé du champ

Condition	Description
Date	Non localisé = toujours YYYY-MM-DD (GMT/UTC)
Temps	Non localisé = HH:MM:SS ou HH:MM:SS.ZZZ (GMT/UTC) * Remarque - malheureusement, il existe deux formats (Site
	n'a pas de .ZZZ millisecondes)
x-mil	Format site uniquement = milliseconde de l'horodatage
c-ip	L'adresse IP du client, telle qu'elle peut être déduite 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-username	Champ de demande du nom d'utilisateur du client
s-ip	Port d'écoute de l'ALB
s-port	L'écoute VIP d'ALB

x-xff	Valeur de l'en-tête X-Forwarded-For
x-xffcustom	Valeur de l'en-tête de la demande de type X-Forwarded-For configuré-nommé
cs-host	Nom de l'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 le format Brief
méthode	* Seul le format bref utilise ce nom pour cs-method
cs-uri-stem	Chemin de la ressource demandée * sauf format Brief
cs-uri-query	Requête pour la ressource demandée * sauf le format Brief
uri	Le format bref enregistre un chemin d'accès et une chaîne de recherche 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-bytes	Octets du client, dans la demande
sr-bytes	Octets transmis au serveur réel, dans la requête
rs-bytes	Octets du serveur réel, dans la réponse
sc-bytes	Octets envoyés au client, dans la réponse
x-percent	Pourcentage de compression * = 100 * (1 - output / input) y compris les en-têtes
temps pris	Combien de temps le serveur réel a pris en secondes
x-trip-times nouveau pcon	milliseconde entre la connexion et la publication dans la "liste des débutants". milliseconde entre la connexion et l'établissement de la connexion avec le serveur réel.
acon	milliseconde entre la connexion et la fin de l'établissement de la connexion avec le serveur réel.
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 demande du client.
rql	milliseconde entre la connexion et la réception du dernier octet de la demande du client.
tqf	milliseconde entre la connexion et l'envoi du premier octet de la demande au serveur réel.
tql	milliseconde entre la connexion et l'envoi du dernier octet de la demande au serveur réel.
rsf	milliseconde entre la connexion et la réception du premier octet de réponse du serveur réel.
rsl	milliseconde entre la connexion et la réception du dernier octet de réponse du serveur réel.
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 du journal 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 évitée
x-sc(Content-Type)	Type de contenu de la réponse
x-cache-action	Comment la mise en cache a répondu, ou a été empêchée
x-finish	Déclencheur qui a provoqué cette ligne de journal

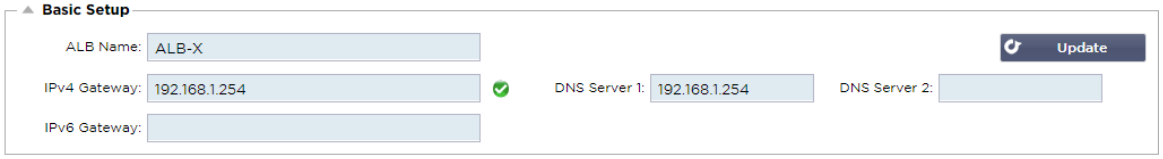
Effacer les fichiers journaux

Cette fonction vous permet d'effacer les fichiers journaux de l'appareil. 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.

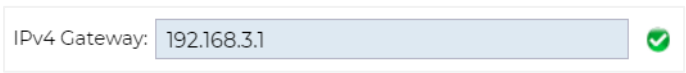
Configuration de base



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 la mise en grappe.

Passerelle IPv4



Indiquez l'adresse de la passerelle IPv4. Cette adresse devra être dans le même sous-réseau qu'un adaptateur existant. Si vous ajoutez une passerelle incorrecte, vous verrez une croix blanche dans un cercle rouge. Lorsque 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

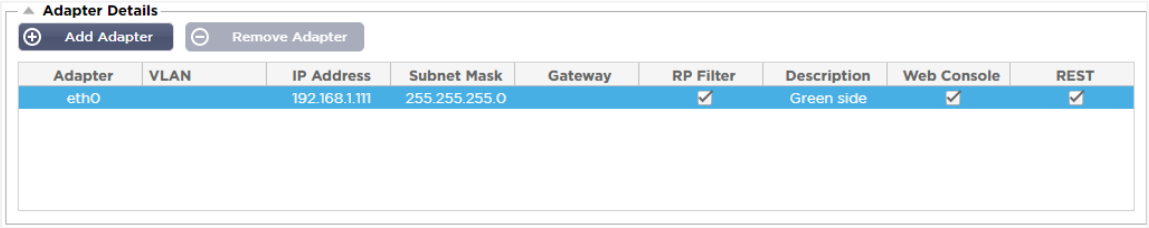
Indiquez l'adresse de la passerelle IPv6. Cette adresse devra être dans le même sous-réseau qu'un adaptateur existant. Si vous ajoutez une passerelle incorrecte, vous verrez une croix blanche dans un cercle rouge. Lorsque vous ajoutez une passerelle correcte, vous verrez une bannière verte de réussite 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 deuxième (facultatif) serveur DNS.

Détails de l'adaptateur

Cette section du panneau Réseau présente les interfaces réseau installées dans votre appareil ADC. Vous pouvez ajouter et supprimer des adaptateurs selon vos besoins.



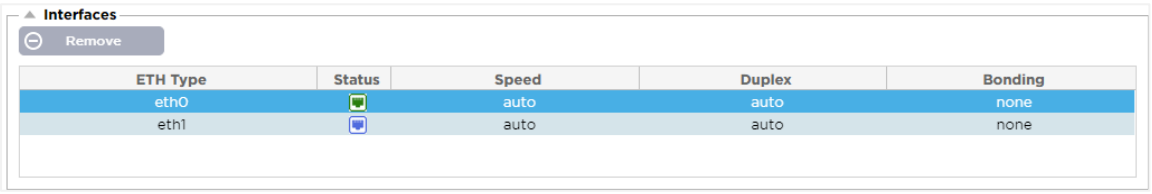
Colonne	Description
Adaptateur	Cette colonne affiche les adaptateurs physiques installés sur votre appliance. Choisissez un adaptateur dans la liste des adaptateurs disponibles en cliquant dessus - un double-clic placera la ligne de liste en mode édition.
VLAN	Double-cliquez pour ajouter l'ID du VLAN pour l'adaptateur. Un VLAN est un réseau local virtuel qui crée un domaine de diffusion distinct. Un VLAN possède les mêmes attributs qu'un réseau local physique, mais il permet de regrouper plus facilement les stations finales si elles ne sont 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 à quatre points. 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 à quatre points. Exemple 255.255.255.0
Passerelle	Ajouter une passerelle pour l'interface. Lorsque cela est ajouté, l'ADC configure une politique simple qui permet aux connexions initiées à partir de cette interface d'être renvoyées via cette interface vers le routeur passerelle spécifié. 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. Remarque : L'ADC nommera 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 selon votre propre choix.
Console Web	Double-cliquez sur la colonne puis cochez la case pour affecter l'interface comme adresse de gestion pour la console Web de l'interface utilisateur graphique. Faites très attention lorsque vous modifiez l'interface sur laquelle la console Web écoutera. Vous devrez avoir configuré le routage correct ou être dans le même sous-réseau

que la nouvelle interface afin d'atteindre la console Web après le changement. La seule façon de revenir en arrière est d'accéder à la ligne de commande et de lancer la commande set greenside. Cela 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 du système d'exploitation interne à l'interface réseau. Ce champ ne peut pas être personnalisé. Les valeurs commencent par ETH0 et se succèdent 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 opérationnelle. 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 l'auto-négociation de la vitesse. Mais vous pouvez changer la vitesse du réseau de l'interface à n'importe quelle valeur disponible dans la liste déroulante (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. Pour plus de détails, voir la section sur le collage.



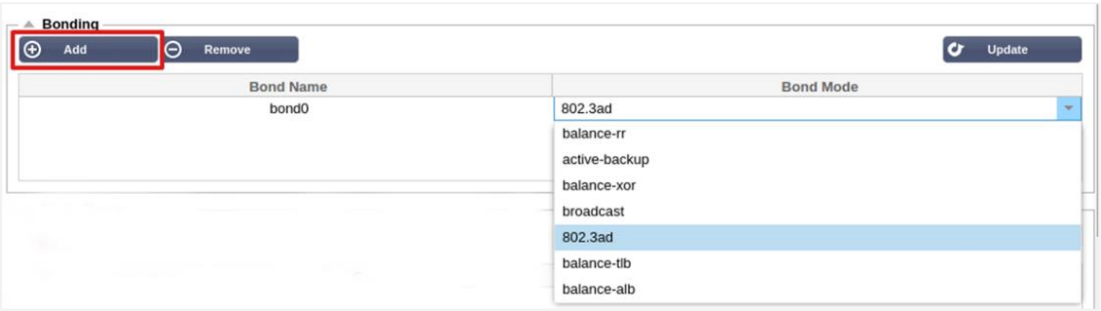
Collage

De nombreux noms sont utilisés pour désigner la liaison d'interface réseau : Port Trunking, Channel Bonding, Link Aggregation, NIC teaming, et autres. Le bonding combine ou agrège plusieurs connexions

réseau en une seule interface liée à un canal. Le bonding permet à deux ou plusieurs interfaces réseau d'agir comme une seule, d'augmenter le débit et de fournir une redondance ou un basculement.

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

REMARQUE : LE COLLAGE NE PEUT ÊTRE CONFIGURÉ QUE POUR LES APPAREILS ADC BASÉS SUR LE MATÉRIEL.

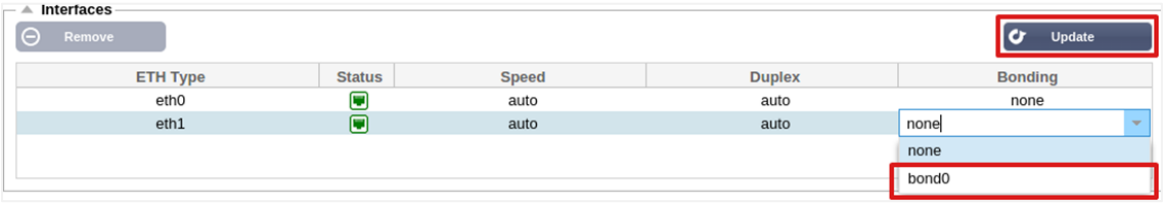


Création d'un profil de cautionnement

- Cliquez sur le bouton Ajouter pour ajouter un nouveau lien
- Fournir un nom pour la configuration de collage
- 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 maintenant partie de bond0. Alors que eth0 reste seul comme interface de gestion.



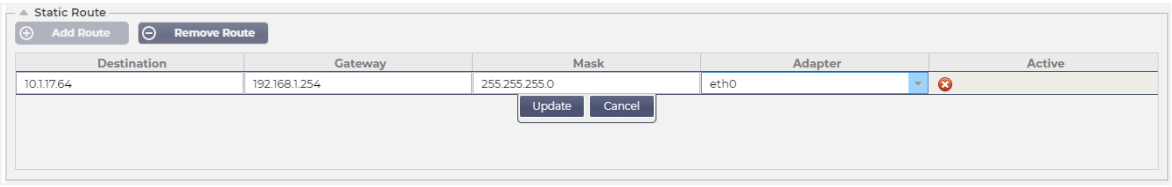
Modes de liaison

Mode de liaison	Description
balance-rr :	Les paquets sont séquentiellement transmis/reçus par chaque interface, un par un.
active-backup :	Dans ce mode, une interface sera active, et la seconde interface sera en veille. 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 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 utilisent tous les esclaves de l'agrégateur actif conformément à la spécification 802.3ad.
balance-tlb :	Le mode de liaison Adaptive transmit load balancing : Fournit un bonding de canal qui ne nécessite pas de support de commutateur spécial. 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 échoue, un autre esclave prend en charge l'adresse MAC de l'esclave récepteur défaillant.
équilibre-alb :	Le mode de liaison d'équilibrage de charge adaptatif : comprend également balance-tlb plus l'équilibrage de charge de réception (rlb) pour le trafic IPV4 et ne nécessite pas de prise en charge spéciale du commutateur. L'équilibrage de la charge de réception est réalisé par négociation ARP. Le pilote de liaison intercepte les réponses ARP envoyées par le système local à leur sortie et écrase l'adresse matérielle source avec l'adresse matérielle unique de l'un des esclaves de la liaison, de sorte que différents pairs utilisent différentes adresses matérielles pour le serveur.

Route statique

Il peut arriver que vous deviez créer des routes statiques pour des sous-réseaux spécifiques de votre réseau. L'ADC vous offre la possibilité de le faire à l'aide du module Static Routes.



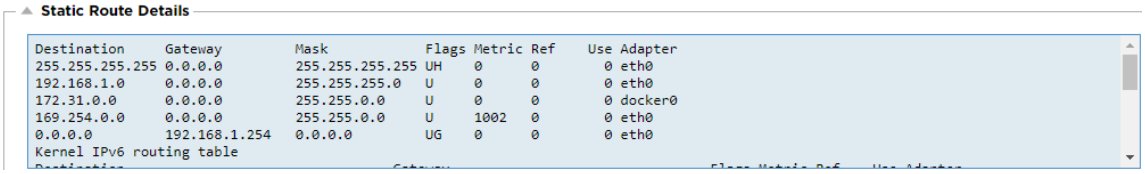
Ajout d'une route statique

- Cliquez sur le bouton Ajouter une route
- Remplissez le champ en utilisant les détails du tableau ci-dessous comme guide.
- Cliquez sur le bouton "Update" lorsque vous avez terminé.

Champ	Description
Destination	Saisissez l'adresse réseau de destination en notation décimale en pointillés. Exemple 123.123.123.5
Passerelle	Saisissez 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 en pointillés. 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 peut être atteinte. Une croix rouge indique que la passerelle ne peut pas être atteinte sur cette interface. Veuillez vous assurer que vous avez 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 le CDA.



Paramètres réseau avancés

Qu'est-ce que Nagle ?

L'algorithme de Nagle améliore l'efficacité des réseaux TCP/IP en réduisant le nombre de paquets qui doivent être envoyés sur le réseau. Voir l'ARTICLE DE WIKIPÉDIA SUR NAGLE

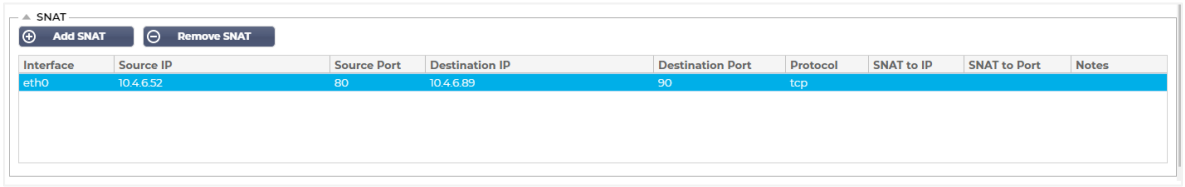
Serveur Nagle

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 est appliqué au côté serveur de la transaction. Il faut faire attention aux 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 Nagle du client. Comme ci-dessus, mais appliqué au côté client de la transaction.

SNAT



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

Dans des circonstances normales, les demandes entrantes sont dirigées vers le VIP qui voit l'IP source de la demande. Par exemple, si un terminal de 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 demande est cachée au VIP, qui voit alors l'adresse IP indiquée dans la règle SNAT. SNAT peut être utilisé dans les modes d'équilibrage de charge de la couche 4 et de la couche 7.

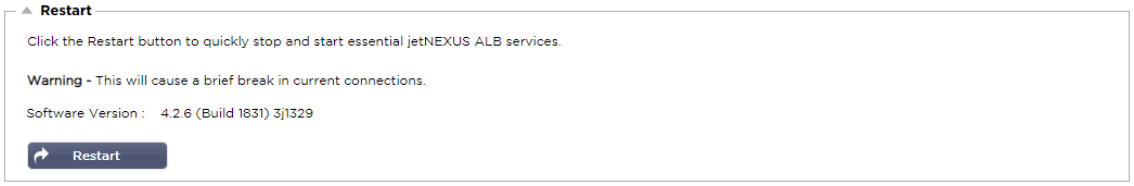
Champ	Description
Source IP	L'adresse IP source est facultative, il peut s'agir d'une adresse IP réseau (avec /mask) ou d'une adresse IP ordinaire. Le masque peut être un masque réseau ou un nombre simple, spécifiant le nombre de 1 à gauche du masque réseau. Ainsi, un masque de /24 est équivalent à 255.255.255.0.
IP de destination	L'adresse IP de destination est facultative, il peut s'agir d'une adresse IP réseau (avec /mask) ou d'une adresse IP ordinaire. Le masque peut être un masque réseau ou un nombre simple, spécifiant le nombre de 1 à gauche du masque réseau. Ainsi, un

	masque de /24 est équivalent à 255.255.255.0.
Port source	Le port source est facultatif, il peut être un nombre unique, auquel cas il ne spécifie que ce port, ou il peut inclure un deux-points, ce qui spécifie une gamme de ports. Exemples : 80 ou 5900:5905.
Port de destination	Le port de destination est facultatif, il peut être un nombre unique, auquel cas il ne spécifie que ce port, ou il peut inclure un deux-points, ce qui spécifie une gamme 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 à 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 SNAT à Port est facultatif, il peut être un seul nombre, auquel cas il ne spécifie que ce port, ou il peut inclure un tiret, ce qui spécifie une gamme de ports. Exemples : 80 ou 5900-5905.
Notes	Utilisez ceci pour mettre un nom amical pour vous rappeler pourquoi les règles existent ;-). Ceci est également utile pour le débogage dans le Syslog.

Puissance

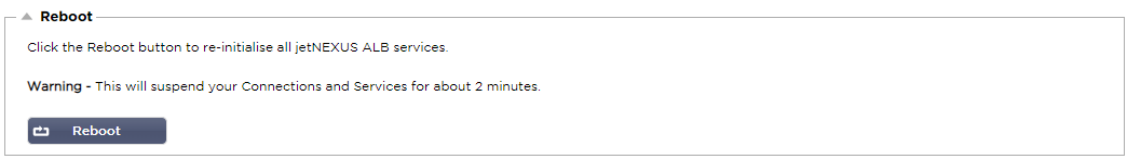
Cette fonction du système ADC vous permet également d'effectuer plusieurs tâches liées à l'alimentation sur votre ADC.

Redémarrer



Ce paramètre initie un redémarrage global de tous les services et, par conséquent, interrompt 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.

Redémarrer



En cliquant sur le bouton Reboot (redémarrage), l'appareil est mis sous tension et revient automatiquement à l'état actif. Une fenêtre pop-up s'affiche pour demander la confirmation de l'action de redémarrage.

Mise hors tension

En cliquant sur le bouton Power Off, l'ADC s'éteint. S'il s'agit d'un appareil matériel, vous devrez avoir un accès physique à l'appareil pour le remettre sous tension. Une fenêtre pop-up s'affiche pour demander la confirmation de l'action d'arrêt.

Sécurité

Cette section vous 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 fonctionnalité REST API.

SSH

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

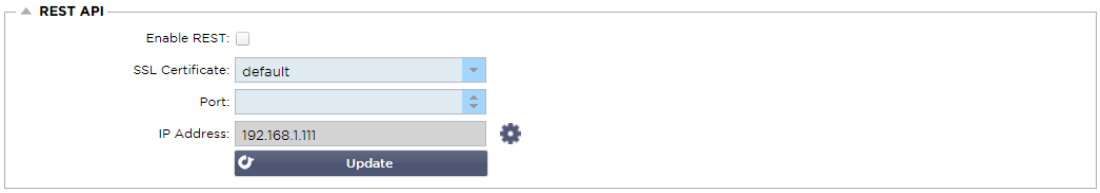
Console Web

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 qui se conforme au style architectural REST et permet la configuration du CDA ou l'extraction de données du CDA. Le terme REST signifie "representational state transfer" et a été créé par l'informaticien Roy Fielding.



Option	Description
Activer REST	Cochez cette case pour activer l'accès à l'aide de 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 affichera tous les certificats installés sur l'ADC.
Port	Définissez le port pour le service REST. Il est conseillé d'utiliser un port autre que 443.

Adresse IP	Cela 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 avec la roue dentée	En cliquant sur ce lien, vous accédez à la page Réseau où vous pouvez configurer un adaptateur pour le REST.

Documentation pour l'API REST

Une documentation sur la façon d'utiliser 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 :

- Commande

curl -k HTTPs://<rest ip>/POST/32 -H "Content-Type : application/json" -X POST -d'{"<nom d'utilisateurrest>" :"<mot de passe>"}''

- retournera

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

- Validité
  - Le GUID est valable pendant 24 heures

Détails de la licence

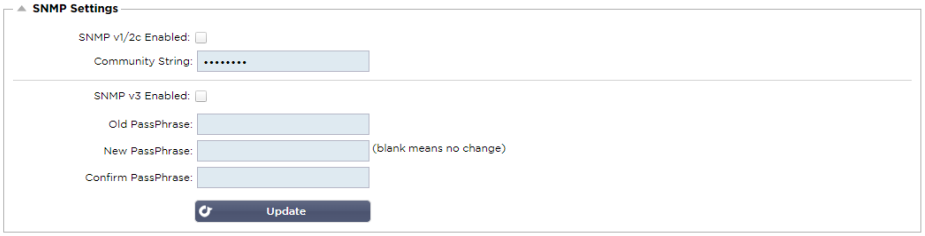
- Commande

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

SNMP

La section SNMP permet la configuration de la MIB SNMP résidant dans l'ADC. La MIB peut ensuite être interrogée par un logiciel tiers capable 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 norme 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
PassPhrase	Il s'agit du mot de passe nécessaire lorsque SNMP v3 est activé. Il doit comporter 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 visualisables par SNMP sont définies par la base d'informations de gestion (MIB). Les MIB décrivent la structure des données de gestion et utilisent des identifiants d'objets (OID) hiérarchiques. Chaque OID peut être lu via une application de gestion SNMP.

Téléchargement des MIB

La MIB peut être téléchargée 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 (octets de sortie globale)** (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 (connexions actuelles)** (1.3.6.1.4.1.38370.1.1.10.0)

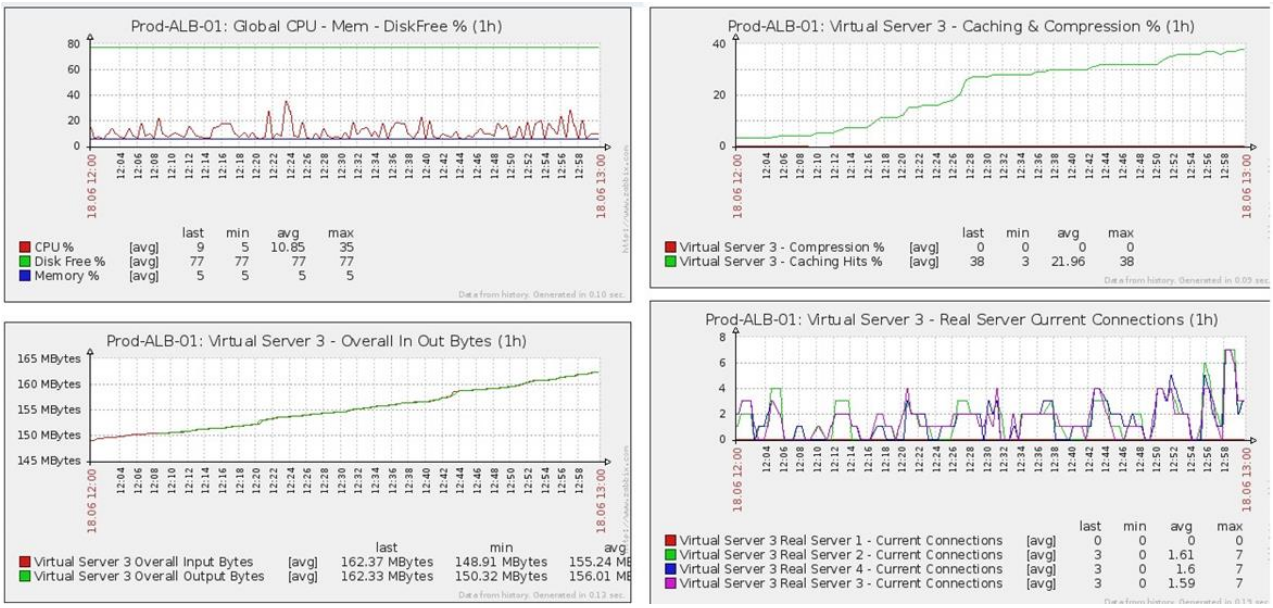
.2 **jetnexusVirtualServices** (1.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry** (1.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice** (1.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort** (1.3.6.1.4.1.38370.1.2.1.**2**)
.3 **jnvirtualserviceOverallInputBytes** (1.3.6.1.4.1.38370.1.2.1.**3**)
.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**)

Graphiques historiques

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 pour diverses valeurs OID énumérées ci-dessus.



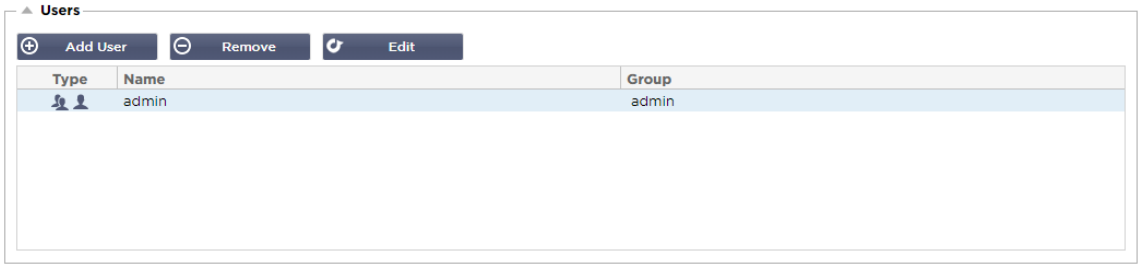
Utilisateurs et journaux d'audit

Le CDA offre la possibilité d'avoir un ensemble interne d'utilisateurs 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.

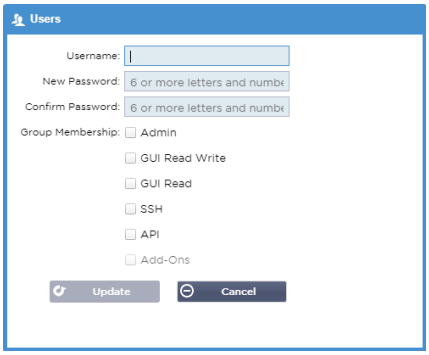
Il existe un utilisateur par défaut appelé **admin** que vous utilisez lors de la première configuration de l'ADC. Le mot de passe par défaut pour admin est **jetnexus**.

Utilisateurs

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



Ajouter un utilisateur



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

Paramètre	**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 minimal de caractères 1 • Nombre maximal de caractères 32 • Les lettres peuvent être en majuscules ou en minuscules • Les chiffres peuvent être utilisés • Les symboles ne sont pas autorisés
Mot de passe	Saisissez un mot de passe **fort**, conforme aux exigences suivantes • 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 en majuscules ou en minuscules • Les symboles sont autorisés, sauf ceux de l'exemple ci-dessous **£**, **%**, **& , <** , **>**
Confirmer le mot de passe	Confirmez à nouveau le mot de passe pour vous assurer qu'il est correct
Adhésion au 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 à l'interface graphique et effectuer des modifications via l'interface graphique. • GUI Read - 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 donne accès à la ligne de commande, qui dispose d'un ensemble minimal de commandes. • API - Les utilisateurs de ce groupe auront accès à l'interface programmable SOAP et REST. REST sera disponible à partir de la version 4.2.1 du logiciel.

Type d'utilisateur

Utilisateur local
Le CDA en 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 changer le mot de passe de cet utilisateur ou le supprimer, mais vous ne pouvez pas supprimer le dernier administrateur local.

Utilisateur du cluster
L'ADC dans le rôle de cluster créera uniquement des utilisateurs de cluster.
Les utilisateurs du cluster sont synchronisés sur tous les ADC du cluster.
Toute modification apportée à un utilisateur du cluster sera répercutée sur tous les membres du cluster.
Si vous êtes connecté en tant qu'utilisateur de cluster, vous ne pourrez pas changer de rôle de cluster à manuel ou à autonome.

Cluster et utilisateur local
Tous les utilisateurs créés dans le rôle Stand-Alone ou Manuel seront copiés dans le Cluster.
Si les CDA quittent ensuite le cluster, seuls les utilisateurs locaux resteront.
Le dernier mot de passe configuré pour l'utilisateur sera valide.

Suppression d'un utilisateur

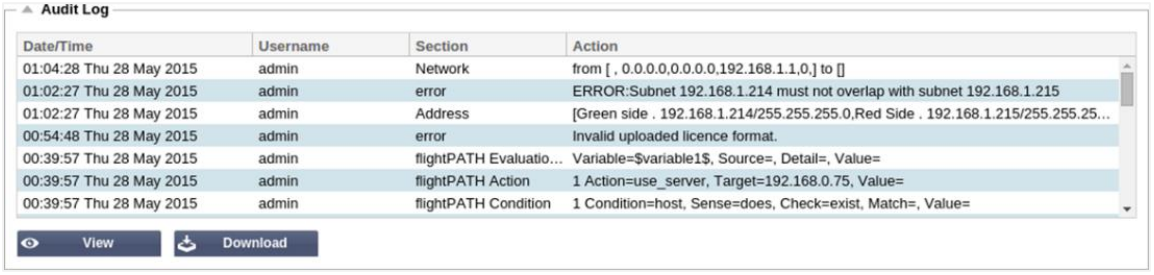
- Mettre en évidence un utilisateur existant
- Cliquez sur Supprimer
- Vous ne pourrez pas supprimer l'utilisateur qui est actuellement connecté.
- Vous ne serez pas en mesure de supprimer le dernier utilisateur local du groupe administrateur.
- Vous ne serez pas en mesure de supprimer le dernier utilisateur de cluster restant dans le groupe administrateur.
- 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.

Modifier un utilisateur

- Mettre 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 les informations suivantes
- Vous pouvez également modifier le mot de passe d'un utilisateur, à condition d'avoir les droits d'administrateur.

Journal d'audit

Le CDA enregistre les modifications apportées à la configuration du CDA par les utilisateurs individuels. Le journal d'audit fournit les 50 dernières actions effectuées par tous les utilisateurs. Vous pouvez également voir TOUTES les entrées dans la section **JOURNAUX**. Par exemple :


Audit Log
Date/Time
Username
Section
Action
01:04:28 Thu 28 May 2015
admin
Network
from [, 0.0.0.0,0.0.0.0,192.168.1.1,0,] to []
01:02:27 Thu 28 May 2015
admin
error
ERROR:Subnet 192.168.1.214 must not overlap with subnet 192.168.1.215
01:02:27 Thu 28 May 2015
admin
Address
[Green side . 192.168.1.214/255.255.255.0,Red Side . 192.168.1.215/255.255.25...
00:54:48 Thu 28 May 2015
admin
error
Invalid uploaded licence format.
00:39:57 Thu 28 May 2015
admin
flightPATH Evaluatio...
Variable=$variable1$, Source=, Detail=, Value=
00:39:57 Thu 28 May 2015
admin
flightPATH Action
1 Action=use_server, Target=192.168.0.75, Value=
00:39:57 Thu 28 May 2015
admin
flightPATH Condition
1 Condition=host, Sense=does, Check=exist, Match=, Value=
View
Download

Avancé

Configuration

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

Les Jetpacks sont des fichiers de configuration pour les applications standard et sont fournis par Edgenexus pour simplifier votre travail. Ils peuvent également être téléchargés sur le CDA à l'aide du module de configuration.

Un fichier de configuration est essentiellement un fichier texte, et en tant que tel, vous pouvez le modifier à l'aide d'un éditeur de texte tel que Notepad++ ou VI. Une fois modifié comme il se doit, le fichier de configuration peut être téléchargé dans l'ADC.

Téléchargement d'une configuration

- Pour télécharger la configuration actuelle de l'ADC, appuyez sur le bouton Télécharger la configuration.
- Une fenêtre pop-up apparaîtra pour vous demander d'ouvrir ou de sauvegarder le fichier .conf.
- Sauvegardez à 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 ne se rafraîchit pas automatiquement, cliquez sur le bouton "Rafraîchir" du navigateur.
- Vous serez redirigé vers la page du tableau de bord après avoir terminé.

Télécharger un jetPACK

- Un jetPACK est un ensemble de mises à jour de la configuration existante.
- Un jetPACK peut être aussi petit qu'une modification de la valeur de TCP Timeout jusqu'à 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 après avoir terminé.

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

Paramètres globaux

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

Temporisation du cache de l'hôte

Le délai de mise en 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. La mémoire cache est vidée en cas de défaillance d'un serveur réel. Si vous mettez cette valeur à zéro, le cache ne sera pas vidé. Il n'y a pas de valeur maximale pour ce paramètre.

Drainage

La fonction Drain est configurable pour chaque serveur réel lié à un service virtuel. Par défaut, le paramètre Drain Clears Persistence est activé, ce qui permet aux serveurs qui sont placés en mode Drain de mettre fin aux sessions de manière gracieuse afin qu'ils puissent être mis hors ligne pour la maintenance.

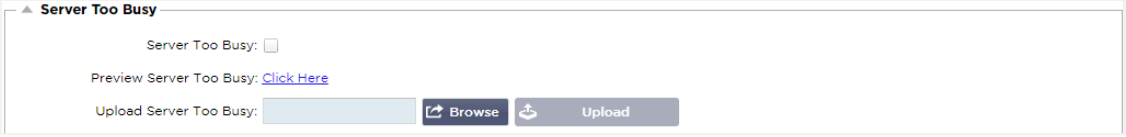
SSL

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

Protocole

La section Protocole est utilisée pour définir les nombreux paramètres avancés du protocole HTTP.

Le serveur est trop occupé



Supposons que vous ayez limité le nombre maximal de connexions à vos serveurs réels ; vous pouvez choisir de présenter 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 voulez avoir des images sur votre page Web, utilisez des images codées en ligne en base64.
- Recherchez le fichier HTM(L) de votre page Web nouvellement créée.
- Cliquez sur Télécharger
- Si vous souhaitez visualiser 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 le biais d'équilibreurs de charge et de serveurs proxy de couche 7.

Sortie de transfert

Option	Description
Off	L'ADC ne modifie pas l'en-tête Forwarded-For.
Ajouter l'adresse et le port	Ce choix ajoutera l'adresse IP et le port du dispositif ou du client connecté au CDA à l'en-tête Forwarded-For.
Ajouter une adresse	Ce choix ajoutera l'adresse IP du dispositif ou du client connecté au CDA 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 du périphérique 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 du périphérique ou du client connecté à l'ADC.

En-tête de transfert

Ce champ vous permet de spécifier le nom donné à l'en-tête Forwarded-For. En général, il s'agit de "X-Forwarded-For", mais il 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 téléchargé, créez un champ de journalisation personnalisé appelé X-Forwarded-For avec les paramètres ci-dessous.

Sélectionnez Défaut dans la liste Type de source dans la liste Catégorie, sélectionnez En-tête de la demande dans la zone Nom de la source, et tapez X-Forwarded-For.

HTTP://www.iis.net/learn/extensions/advanced-logging-module/advanced-logging-for-iis-custom-logging

Modifications du fichier HTTPd.conf d'Apache

Vous voudrez apporter plusieurs modifications au format par défaut pour 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 :

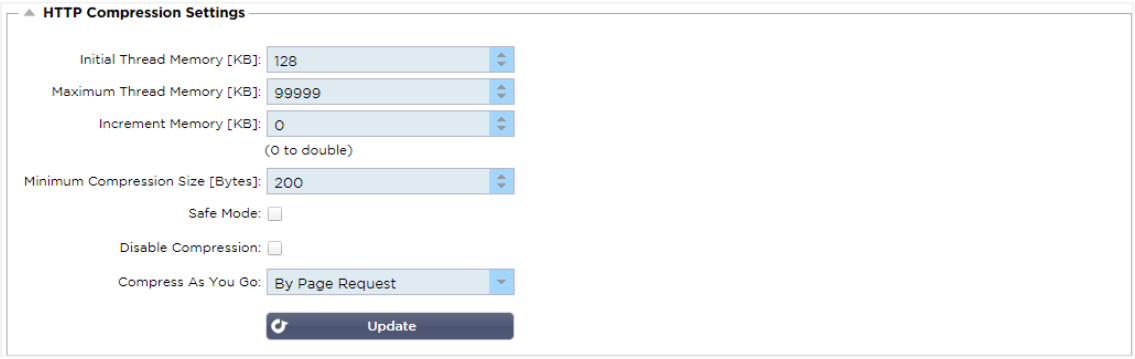
Type	Valeur
LogFormat :	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combinés
LogFormat :	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*" forwarded
CustomLog :	"logs/access_log" combiné env=!forwarded
CustomLog :	"logs/access_log" proxy env=forwarded

Ce format tire parti du support intégré d'Apache pour la journalisation conditionnelle basée sur des variables environnementales.

- La ligne 1 est la chaîne formatée standard du journal combiné par défaut.
- La ligne 2 remplace le champ %h (hôte distant) par la ou les valeurs extraites de l'en-tête X-Forwarded-For et définit le nom de ce modèle de fichier journal par "proxy".
- La ligne 3 est un paramètre pour la variable d'environnement "forwarded" qui contient une expression régulière libre correspondant à une adresse IP, ce qui est correct dans ce cas puisque nous nous soucions plus 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".
- 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 "combiné" pour la requête. Pour des raisons de lisibilité, les lignes 4 et 5 ne tirent pas parti de la fonction de journalisation d'Apache par rotation des journaux (piped), mais nous supposons que presque tout le monde l'utilise.

Ces changements auront pour effet d'enregistrer une adresse IP pour chaque demande.

Paramètres de compression HTTP



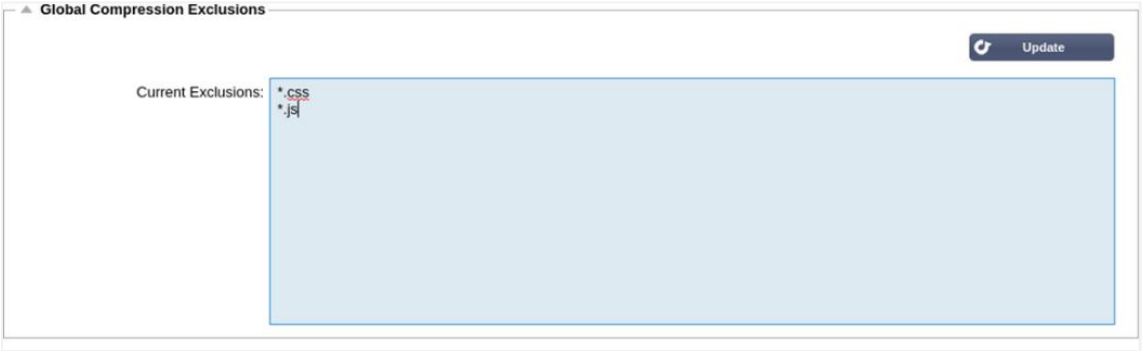
La compression est une fonction d'accélération et est activée pour chaque service sur la page Services IP.

AVERTISSEMENT - Faites preuve d'une extrême prudence lors du réglage de ces paramètres, car des réglages inappropriés peuvent nuire aux performances du CDA.

Option	Description
Mémoire initiale du thread [KB]	Cette valeur est la quantité de mémoire que chaque demande reçue par le CDA peut initialement allouer. Pour une performance optimale, 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	Cette valeur est la quantité maximale de mémoire que le CDA allouera sur

threads [KB]	une demande. Pour une performance maximale, le CDA stocke et compresse normalement tout le contenu en mémoire. Si un fichier exceptionnellement volumineux dépassant cette quantité est traité, l'ADC écrira sur le disque et y compressera les données.
Mémoire d'incrémentation [KB]	Cette valeur définit la quantité de mémoire ajoutée à l'allocation de mémoire initiale du fil lorsque celle-ci est nécessaire. Le paramètre par défaut est zéro. Cela signifie que le CDA doublera l'allocation lorsque les données dépassent 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 fil. 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 font 128 Ko ou moins, mais les réponses occasionnelles font 1 Mo). Dans le scénario où il y a de gros fichiers de taille variable, il est plus efficace de définir un incrément linéaire d'une taille significative (par exemple, les réponses ont une taille de 2 Mo à 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 le CDA ne tentera pas de compresser. C'est utile car tout ce qui est inférieur à 200 octets n'est pas bien compressé et peut même augmenter en taille en raison 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. En effet, bien qu'ADC sache quels navigateurs individuels peuvent traiter 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 les feuilles de style ou JavaScript via un serveur proxy, utilisez cette option pour désactiver la compression de ces types. Toutefois, cela réduira la quantité globale de compression du contenu.
Désactiver la compression	Cochez cette case pour empêcher l'ADC de compresser toute réponse.
Compresser au fur et à mesure	ON - Utilisez Compress as You Go sur cette page. Cela permet de compresser chaque bloc de données reçu du serveur dans un morceau discret qui est entièrement dé-compressible. OFF - Ne pas utiliser Compress As You Go sur cette page. Par demande de page - Utilise Compress as you go par demande de page.

Exclusions de la compression globale



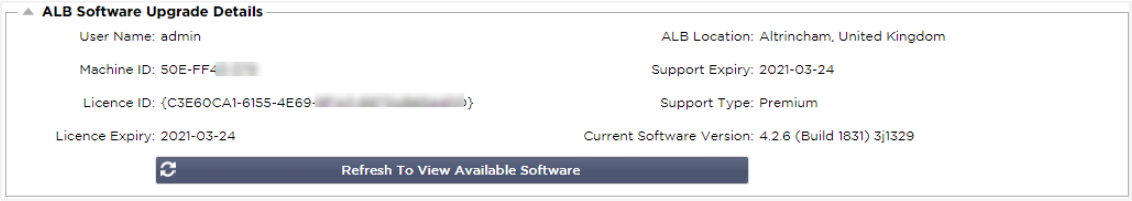
Toutes les pages avec l'extension ajoutée dans la liste d'exclusion ne seront pas compressées.

- Saisissez le nom du fichier individuel.
- Cliquez sur mettre à jour.
- Si vous souhaitez ajouter un type de fichier, tapez simplement "*.css" pour que toutes les feuilles de style en cascade soient exclues.
- Chaque fichier ou type de fichier doit être ajouté sur une nouvelle ligne.

Logiciel

La section Software vous permet de mettre à jour la configuration et le firmware de votre ADC.

Détails de la mise à jour du logiciel



L'information contenue dans cette section sera remplie si votre connexion Internet est fonctionnelle. Si votre navigateur n'a pas de lien avec Internet, cette section sera vide. Une fois connecté, vous recevrez le message de bannière ci-dessous.

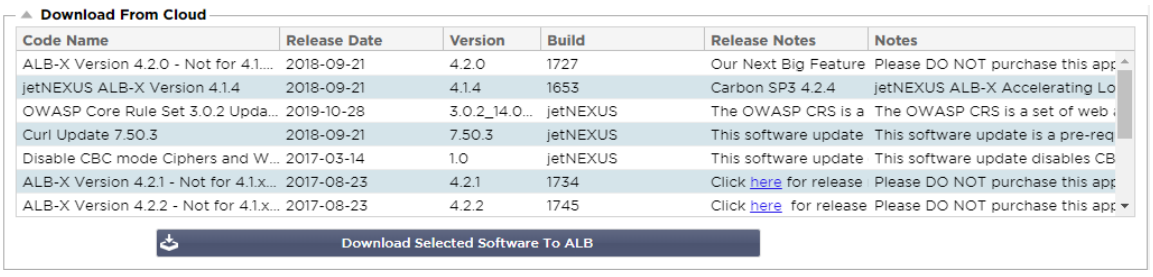
La section "Télécharger depuis le cloud" présentée ci-dessous sera remplie d'informations indiquant les mises à jour disponibles dans le cadre de votre plan d'assistance. Vous devez prêter attention au type d'assistance et à la date d'expiration de l'assistance.

Remarque : Nous utilisons la connexion Internet de votre navigateur pour afficher ce qui est disponible dans le nuage Edgenexus. Vous ne pourrez télécharger des mises à jour logicielles que si le CDA dispose d'une connexion Internet.

Pour vérifier cela :

- Avancé--Dépannage--Ping
- Adresse IP - appstore.edgenexus.io
- Cliquez sur Ping
- Si le résultat montre " ping : unknown host appstore.edgenexus.io. "
- Le CDA ne sera PAS en mesure de télécharger quoi que ce soit depuis le cloud.

Télécharger à partir de Cloud



Si votre navigateur est connecté à Internet, vous verrez les détails des logiciels disponibles dans le nuage.

- Mettez en surbrillance la ligne qui vous intéresse et cliquez sur le bouton "Download Selected Software to ALB. et cliquez sur le bouton "Télécharger le logiciel sélectionné vers ALB".

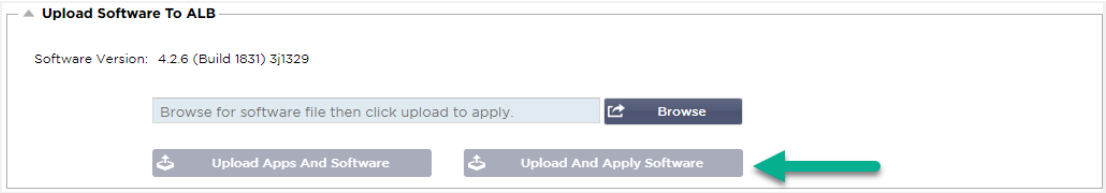
- Le logiciel sélectionné sera téléchargé sur votre ALB lorsque vous cliquez dessus. Vous pouvez l'appliquer dans la section "Appliquer le logiciel stocké sur l'ALB" ci-dessous.

Note : Si le CDA n'a pas d'accès direct à Internet, vous recevrez une erreur comme celle ci-dessous :

Erreur de téléchargement, ALB ne peut pas accéder aux ADC Cloud Services pour le fichier build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Télécharger des logiciels vers ALB

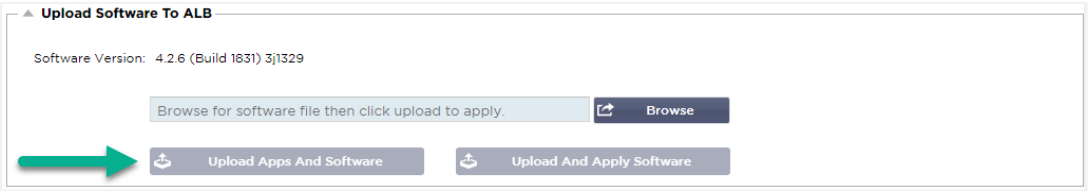
Téléchargement d'applications



Si vous avez un fichier App qui se termine par <apptype>.alb, vous pouvez utiliser cette méthode pour le télécharger.

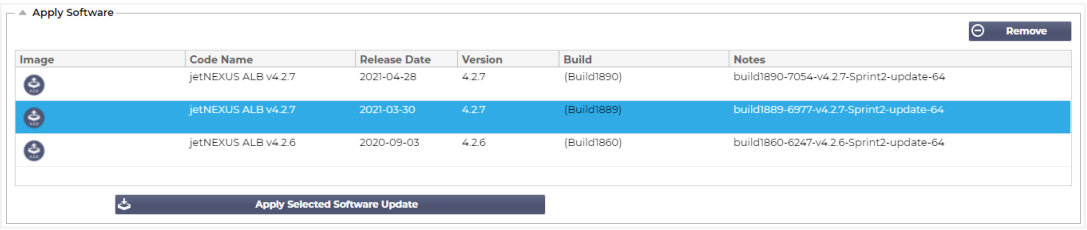
- Il existe cinq types d'App
  - <nom de l'application>flightpath.alb
  - <nom de l'application>.monitor.alb
  - <nom de l'application>.jetpack.alb
  - <nom de l'application>.addons.alb
  - <nom de l'application>.featurepack.alb
- Une fois téléchargée, chaque application se trouve dans la section Bibliothèque>Applications.
- Vous devez ensuite déployer chaque application de cette section individuellement.

Logiciel



- Si vous souhaitez télécharger un logiciel sans l'appliquer, utilisez le bouton en surbrillance.
- Le fichier du logiciel est <nom du logiciel>.software.alb.
- Il apparaîtra alors dans la section "Logiciels stockés sur ALB", d'où vous pourrez l'appliquer à votre convenance.

Appliquer les logiciels stockés sur l'ALB



Cette section montrera tous les fichiers logiciels stockés sur l'ALB et disponibles pour le déploiement. La liste comprendra les signatures mises à jour du pare-feu d'application Web (WAF).

- Mettez en surbrillance la ligne du logiciel que vous souhaitez utiliser.
- Cliquez sur "Appliquer le logiciel à partir de la sélection".
- S'il s'agit d'une mise à jour du logiciel ALB, sachez qu'elle sera téléchargée puis redémarrée par l'ALB pour être appliquée.
- Si la mise à jour que vous appliquez est une mise à jour de signature OWASP, elle s'appliquera automatiquement sans redémarrage.

Dépannage

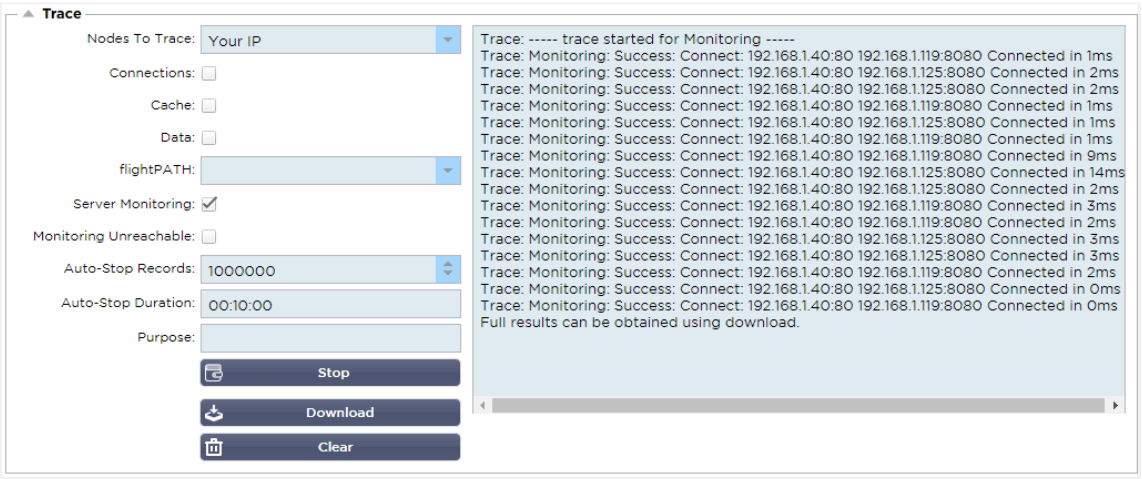
Il y a toujours des problèmes qui nécessitent un dépannage pour trouver une cause profonde et une solution. Cette section vous permet de le faire.

Fichiers de soutien

Si vous avez un problème avec l'ADC et que vous devez ouvrir un ticket de support, le support technique demandera souvent plusieurs fichiers différents de l'appareil ADC. Ces fichiers ont été regroupés en un seul fichier .dat qui peut être téléchargé via cette section.

- Sélectionnez un délai dans la liste déroulante : Un choix de 3, 7, 14, et Tous les jours vous est proposé.
- Cliquez sur "Télécharger les fichiers de support".
- Un fichier sera téléchargé au format Support-jetNEXUS-yyymmddhh-NAME.dat.
- Soulever un ticket de support sur le portail de support, 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



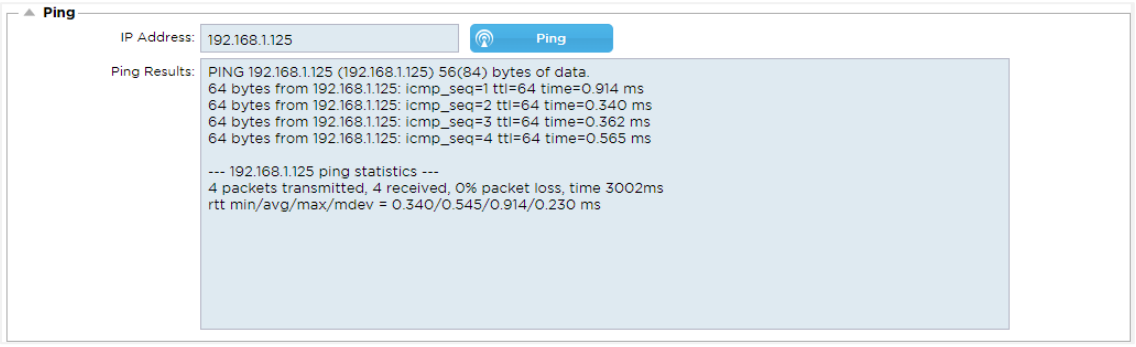
La section Trace vous permettra d'examiner les informations permettant de déboguer le problème. Les informations fournies dépendent des options que vous choisissez dans les menus déroulants et les cases à cocher.

Option	Description
Nœuds à tracer	**Your IP** : Ceci filtrera la sortie pour utiliser l'adresse IP à partir de laquelle vous accédez à l'interface graphique (Note : ne choisissez pas cette

	option pour la surveillance car celle-ci utilisera l'adresse de l'interface ADC). **All IP** : Aucun filtre ne sera appliqué. Il convient de noter que sur une boîte occupée, cela aura un effet négatif sur les performances.
Connexions	Cette case, lorsqu'elle est cochée, permet d'afficher 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.
flightPATH	Le menu flightPATH vous permet de sélectionner une règle flightPATH particulière à surveiller ou Toutes les règles flightPATH.
Surveillance des serveurs	Cette case, lorsqu'elle est cochée, affiche les moniteurs de santé du serveur actifs sur le CDA et leurs résultats respectifs.
Surveillance de l'inaccessibilité	Cette case cochée est comme ci-dessus, sauf qu'elle ne montrera que les moniteurs en échec et agira comme un filtre pour ces messages seulement.
Enregistrements d'arrêt automatique	La valeur par défaut est de 1 000 000 d'enregistrements, après quoi la fonction Trace s'arrête automatiquement. Il s'agit d'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. Il s'agit d'une précaution de sécurité pour éviter que la fonction Trace ne reste accidentellement activée et n'affecte les performances de l'ADC.
Début	Cliquez pour démarrer manuellement l'installation de traçage.
Stop	Cliquez pour arrêter manuellement l'installation Trace avant que l'enregistrement automatique ou le temps ne soit atteint.
Télécharger	Bien que vous puissiez voir le visualiseur en direct sur le côté droit, les informations peuvent s'afficher trop rapidement. Vous pouvez télécharger le fichier Trace.log pour visualiser toutes les informations recueillies lors des différentes traces de la journée. Il s'agit essentiellement d'une liste filtrée d'informations sur les traces. Si vous souhaitez afficher les informations des traces des jours précédents, vous pouvez télécharger le syslog de ce jour-là, mais vous devrez le filtrer manuellement.
Clair	Efface le journal de suivi

Ping

Vous pouvez vérifier la connectivité réseau des serveurs et des autres objets réseau de 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 notation décimale pointée ou une adresse IPv6. Il se peut que vous deviez attendre quelques secondes avant d'obtenir le résultat après avoir appuyé sur le bouton "Ping".

Si vous avez configuré un serveur DNS, vous pouvez alors saisir le nom de domaine entièrement qualifié. Vous pouvez configurer un serveur DNS dans la section **DNS Server 1 & DNS Server 2**. Il se peut que vous deviez attendre quelques secondes pour que le résultat vous soit renvoyé après avoir 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 sera au format "jetNEXUS.cap.gz".
- Soulever un ticket de support sur le portail de support, 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 en utilisant 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 est le nombre maximum de paquets à capturer. Généralement, 99999
Durée	Choisissez une durée maximale d'exécution de 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 cette case vide pour ne pas filtrer.

Pour maintenir les performances, nous avons limité le fichier à télécharger à 10 Mo. Si vous trouvez que ce n'est pas suffisant pour capturer toutes les données nécessaires, nous pouvons augmenter ce chiffre.

Note : Ceci aura un impact sur la performance des sites en direct. Pour augmenter la taille de capture disponible, veuillez appliquer un paramètre global jetPACK pour augmenter la taille de capture.

Qu'est-ce qu'un jetPACK

Les jetPACKs sont une méthode unique pour configurer instantanément votre CDA 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 des jetPACKs utilisent flightPATH pour manipuler le trafic, et vous devez disposer d'une licence flightPATH pour que cet élément fonctionne. Pour savoir si vous avez une licence pour flightPATH, veuillez vous référer à la page **LICENCE**.

Téléchargement d'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.
- En outre, chaque jetPACK a été créé avec 2 serveurs réels avec l'adresse IP de 127.1.1.1 et 127.2.2.2. Encore une fois, vous pouvez les modifier dans l'interface graphique après le téléchargement ou avant en utilisant Notepad++.
- Cliquez sur un lien jetPACK ci-dessous et enregistrez le lien sous forme de 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 sur le 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 du 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. IP du service virtuel : 1.1.1.1 Ports de services virtuels : 80, 443, 135, 59534, 59535 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : Ajoute une redirection de HTTP vers HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	Idem que ci-dessus, mais cela ajoutera un service SMTP sur le port 25 en connectivité reverse proxy. Le serveur SMTP verra l'adresse de l'interface ALB-X comme l'IP source.	Paramètres globaux : Délai d'attente du service 2 heures Moniteurs : Moniteur de couche 7 pour l'application web Outlook. Moniteur hors bande de couche 4 pour le service d'accès client. IP du service virtuel : 1.1.1.1 Ports de services virtuels : 80, 443, 135, 59534, 59535, 25 (reverse proxy) Serveurs réels : 127.1.1.1

			127.2.2.2 flightPATH : Ajoute une redirection de HTTP vers HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	Même chose que ci-dessus, sauf que ce jetPACK configurera le service SMTP pour utiliser la connectivité de retour direct du serveur. Ce jetPACK est nécessaire si votre serveur SMTP a besoin de voir l'adresse IP réelle du client.	Paramètres globaux : Délai d'attente du service 2 heures Moniteurs : Moniteur de couche 7 pour l'application web Outlook. Moniteur hors bande de couche 4 pour le service d'accès client. IP du service virtuel : 1.1.1.1 Ports de services virtuels : 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 à HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Cette configuration ajoute un 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 pour vérifier que chacun des services individuels est opérationnel.	Paramètres globaux : Surveille : Moniteur de couche 7 pour OWA, EWS, OA, EAS, ECP, OAB et ADS. IP du service virtuel : 2.2.2.1 Ports de services virtuels : 80, 443 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : Ajoute une redirection de HTTP vers HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Cette configuration utilise une adresse IP unique pour chaque service et utilise donc plus de ressources que ci-dessus. Vous devez configurer chaque service comme une entrée DNS individuelle Exemple owa.jetnexus.com, ews.jetnexus.com, etc. Un moniteur pour chaque service sera ajouté et appliqué au service concerné.	Paramètres globaux : Surveille : Surveillance de la couche 7 pour OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI et PowerShell. IP de service virtuel : 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 services virtuels : 80, 443 Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : Ajoute une redirection de HTTP à HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Ce jetPACK ajoutera une adresse IP unique et plusieurs services virtuels sur différents ports. flightPATH effectuera ensuite une commutation de contexte en fonction du chemin de destination vers le bon service virtuel. Ce jetPACK nécessite la plus grande quantité de CPU pour effectuer la commutation de	Paramètres globaux : Surveille : Surveillance de la couche 7 pour OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI et PowerShell. IP du service virtuel : 2.2.2.3 Ports de service virtuels : 80, 443, 1, 2, 3, 4, 5, 6, 7

	contexte.	Serveurs réels : 127.1.1.1 127.2.2.2 flightPATH : Ajoute une redirection de HTTP vers 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-Externe

Services Web

HTTP normal	Déchargement de SSL	Re-cryptage SSL	SSL Passthrough
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2 - Déchargement Web-SSL	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Bureau à distance Microsoft

jetPACK-5.5.5.1-Remote-Desktop

DICOM - Imagerie numérique et communication en médecine

jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

Déchargement de SSL
jetPACK-7.7.7..1-Oracle-EBS

VMware Horizon View

Serveurs de connexion - Déchargement de SSL	Serveurs de sécurité - Re-cryptage SSL
jetPACK-8.8.8.1-Vue-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.x
- GUI Timeout 1 day - le GUI vous demandera de saisir votre mot de passe toutes les 20 minutes. Ce paramètre augmentera cette demande à 1 jour
- ARP Refresh 10 - lors d'un basculement entre des appareils HA, ce paramètre augmentera 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.

Options de chiffrement

- Strong Ciphers - Ceci ajoutera la possibilité de choisir "Strong Ciphers" dans la liste des options de chiffrement :
  - Cipher = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Beast - Ceci ajoutera la possibilité de choisir "Anti-Beast" dans la liste des options du Cipher :
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Cela ajoutera la possibilité de choisir "No SSLv3" dans la liste des options de chiffrement :
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 No RC4 - Ceci ajoutera la possibilité de choisir "No-TLSv1 No-SSLv3 No-RC4" dans la liste des options de chiffrement :
  - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 - Cette option permet de choisir "NO_TLSv1.1" dans la liste des options de chiffrement :

- Cipher= 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

flightPATHs

- X-Content-Type-Options - ajoutez cet en-tête s'il n'existe pas et définissez-le à "nosniff" - empêche le navigateur de "renifler" automatiquement MIME.
- X-Frame-Options - ajoutez cet en-tête s'il n'existe pas et définissez-le sur "SAMEORIGIN" - les pages de votre site Web peuvent être incluses dans des cadres, mais uniquement sur d'autres pages du même site.
- X-XSS-Protection - ajoutez cet en-tête s'il n'existe pas et définissez-le à "1 ; mode=block" - activez les protections contre les scripts intersites du navigateur.
- Strict-Transport-Security - ajoutez l'en-tête s'il n'existe pas et définissez-le à "max-age=31536000 ; includeSubdomains" - garantit que le client doit respecter le fait que tous les liens doivent être HTTPs:// pour l'âge max.

Application d'un jetPACK

Vous pouvez appliquer n'importe quel jetPACK dans n'importe quel ordre mais faites attention à ne pas utiliser un jetPACK avec la même adresse IP virtuelle. Cette action entraînera un doublon d'adresse IP dans la configuration. Si vous le faites par erreur, vous pouvez le modifier dans l'interface graphique.

- Naviguez jusqu'à Advanced > Update Software
- Section de configuration
- Télécharger une nouvelle configuration ou un jetPACK
- Parcourir pour jetPACK
- Cliquez sur Télécharger
- Une fois que l'écran du navigateur devient blanc, veuillez cliquer sur rafraîchir et attendre que la page du tableau de bord apparaisse.

Créer un jetPACK

L'un des grands avantages de jetPACK est que vous pouvez créer vos propres configurations. 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 être en haut du jetPACK, ou votre configuration actuelle sera écrasée.

Section1 :

[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 est 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 changera le nom de l'en-tête de cookie utilisé dans l'équilibrage de charge persistant de "jnAccel" par défaut à "MS-WSMAN". Ce changement particulier est nécessaire pour le reverse proxy de Lync 2010/2013.

Section 2 :

[jetnexusdaemon-Csm-Rules]

Cette section contient les règles personnalisées de surveillance du serveur qui sont généralement configurées à partir de la console Web.

Exemple :

[jetnexusdaemon-Csm-Rules-0]

Content="Server Up"

Desc="Moniteur 1″

Méthode="CheckResponse"

Name="Bilan de santé - Le serveur est-il en marche ?"

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, il contient 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″"

Résolution d'adresse=0

CachePort=0

CertificateName="default"

ClientCertificateName="No SSL"

Compresser=1

Limitation de la connexion=0

DSR=0

DSRProto="tcp"

Activé=1

LoadBalancePolicy="CookieBased" (Politique d'équilibre de la charge)

MaxConnexions=10000

MonitoringPolicy="1″

PassThrough=0

Protocole="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 de 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, y compris à l'exemple ci-dessous.

Exemple :

[jetnexusdaemon-Path-6]

Desc="Forcer l'utilisation de HTTPS pour certains répertoires".

Name="Gary - Force HTTPS"

[jetnexusdaemon-Path-6-Condition-1]

Check="contain"

Condition="path"

Match=

Sense="does"

Valeur="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1]

Détail=

Source="hôte"

Valeur=

Variable="$host$" [jetnexusdaemon-Path-6-Function-1]

Action="redirect"

Target="HTTPs://$host$$path$$$querystring$"

Valeur=

Introduction à flightPATH

Qu'est-ce que le 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, comme l'IP source, flightPATH ne peut être appliqué qu'à un **type de service** égal à HTTP. Si vous choisissez un autre type de service, l'onglet flightPATH dans les services IP sera vide.

Une règle FlightPATH comporte trois éléments :

Option	Description
Condition	Définissez plusieurs critères pour déclencher la règle flightPATH.
Évaluation	Permet d'utiliser des variables qui peuvent être utilisées dans la zone d'action.
Action	Le comportement une fois que la règle s'est déclenchée.

Que peut faire FlightPATH ?

flightPATH peut être utilisé pour modifier le contenu et les demandes HTTP(s) entrants et sortants.

Outre l'utilisation de simples correspondances de chaînes de caractères telles que "Commence par" et "Finit par" par exemple, il est possible de mettre en œuvre un contrôle complet en utilisant de puissantes expressions régulières (RegEx) compatibles avec Perl.

Pour en savoir plus sur RegEx, veuillez consulter ce site utile https://www.regexbuddy.com/regex.html.

En outre, des variables personnalisées peuvent être créées et utilisées dans la zone d'**action**, ce qui permet de nombreuses possibilités différentes.

Condition

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 de GEO	Cela permet de comparer l'adresse IP source au code pays ISO 3166.	GEO Location est égal à GB OR 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 une liste déroulante 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.
IP d'origine	Si le proxy en amont prend en charge X-Forwarded-for (XFF), il utilisera l'adresse d'origine réelle.	IP du client. Peut également utiliser plusieurs IP ou sous-réseaux. 10\.1\.2\.* est 10.1.2.0 /24 sous-réseau10\ .1\.2\.3|10\.1\.2\.4 Utilisez | pour plusieurs adresses IP
Chemin	Voici le chemin du site web	/mywebsite/index.asp

d'accès		
POST	Méthode de demande POST	Vérifier les données téléchargées sur un site web
Requête	Il s'agit du nom et de la valeur d'une requête. Il peut donc accepter soit le nom de la requête, soit une valeur.	"Best=jetNEXUS" où la correspondance est Best et la valeur est edgeNEXUS
Chaîne de requête	La chaîne de requête complète après le caractère ?	
Demande de cookie	C'est le nom d'un cookie demandé par un client.	MS-WSMAN=afYfn1CDqCDqUD: :
En-tête de la demande	Cela peut être 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 pour la réponse	200 OK, 304 Non modifié
Cookie de réponse	C'est le nom d'un cookie envoyé par le serveur.	MS-WSMAN=afYfn1CDqCDqUD: :
En-tête de réponse	Cela peut être n'importe quel en-tête HTTP	Referrer, User-Agent, From, Date
Version de réponse	La version HTTP envoyée par le serveur	HTTP/1.0 OU HTTP/1.1
Source IP	Il s'agit de l'IP d'origine, de l'IP du serveur proxy ou d'une autre adresse IP agrégée.	ClientIP , Proxy IP, Firewall IP. Vous pouvez également utiliser plusieurs IP et sous-réseaux. Vous devez échapper les points car il s'agit de RegEX. Exemple 10\.1\.2\.3 est 10.1.2.3

Match	**Description**	**Exemple**
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodements acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>
Accept-Language	Langues acceptables pour la réponse	Accept-Language : en-US
Accept-Ranges	Quels types de plages de contenu partiel ce serveur supporte-t-il ?	Accept-Ranges : bytes
Autorisation	Références d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contient des informations comptables sur les coûts de l'application de la méthode	

	demandée.	
Content-Encoding	Le type d'encodage utilisé sur les données.	Content-Encoding : gzip
Content-Length	La longueur du corps de la réponse en octets (octets de 8 bits).	Content-Length : 348
Content-Type	Le type mime du corps de la demande (utilisé avec les demandes 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'origine du message	Date = "Date" " :" HTTP-date
ETag	Un identifiant pour une version spécifique d'une ressource, souvent un résumé 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 304 Not Modified si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	La date de 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 l'implémentation peuvent avoir des effets divers 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.	Referrer : 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	La chaîne de l'agent utilisateur de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Varier	Indique aux mandataires en aval comment faire correspondre les futurs en-têtes de demande pour décider si la réponse mise en cache peut être utilisée plutôt que de demander une nouvelle réponse au serveur d'origine.	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple, ASP.NET, PHP, JBoss) qui prend en charge l'application Web.	X-Powered-By : PHP/5.4.0

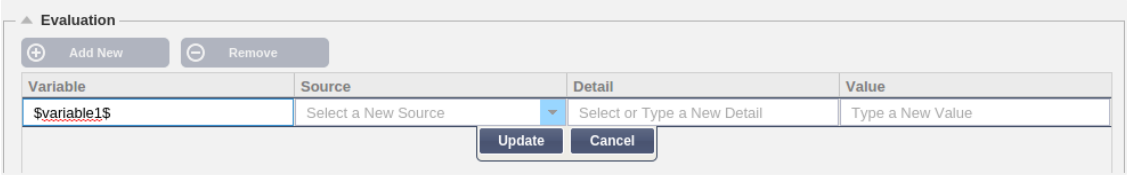
Vérifiez	**Description**	**Exemple**
Existe	Le détail de la condition n'a pas d'importance, il	L'hôte - existe - existe

	suffit de savoir qu'elle existe ou n'existe pas.	
Début	La chaîne de caractères commence par la valeur	Chemin - Does - Start - /secure
Fin	La chaîne se termine par la valeur	Chemin - Fait - Fin - .jpg
Contenir	La chaîne contient bien la valeur	En-tête de la demande - Accepter - Ne - Contenir - image
Equal	La chaîne est égale à la valeur	Hôte - Fait - Égale - www.jetnexus.com
Avoir la longueur	La chaîne a la longueur de la valeur	L'hôte - a - une longueur - 16www.jetnexus.com = VRAIwww.jetnexus.co.uk = FAUX
Match RegEx	Cela vous permet de saisir une expression régulière complète compatible avec Perl.	IP d'origine - Correspond - Regex - 10\..* | 11\..*

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 est la vérification d'un nom d'hôte spécifique

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'utilisateur d'un utilisateur ou envoyer un courriel 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 : Sélectionnez dans la liste si nécessaire. Si la Source=Request Header, le Détail pourrait être User-Agent
- Valeur : Entrez le texte ou l'expression régulière pour affiner la variable.

Variables intégrées :

- Les variables Built-In 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 votre action
- L'explication de chaque variable se trouve dans le tableau "Condition" ci-dessus.
    - Méthode = $method

- Chemin = $path$
- Querystring = $querystring$
- Sourceip = $sourceip$
- Code de réponse (le texte inclut également "200 OK") = $resp$.
- Hôte = $host$
- Version = $version$
- Port du client = $clientport
- Clientip = $clientip$.
- Géolocalisation = $geolocation$"

Exemple d'action :

- Action = Redirection 302
  - Cible = HTTPs://$host$/404.html
- Action = Journal
  - Cible = Un client de $sourceip$:$sourceport$ vient de faire une demande de page $path$.

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 demande 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	C'est le 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 de la 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
Chemin d'accès	Voici le chemin du site web	/mon site web/index.html
POST	Méthode de demande POST	Vérifier les données téléchargées sur un site web
Élément de 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" où la correspondance est Best et la valeur est edgeNEXUS
Chaîne de requête	C'est la chaîne entière après le caractère ?	HTTP://server/path/programme?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...

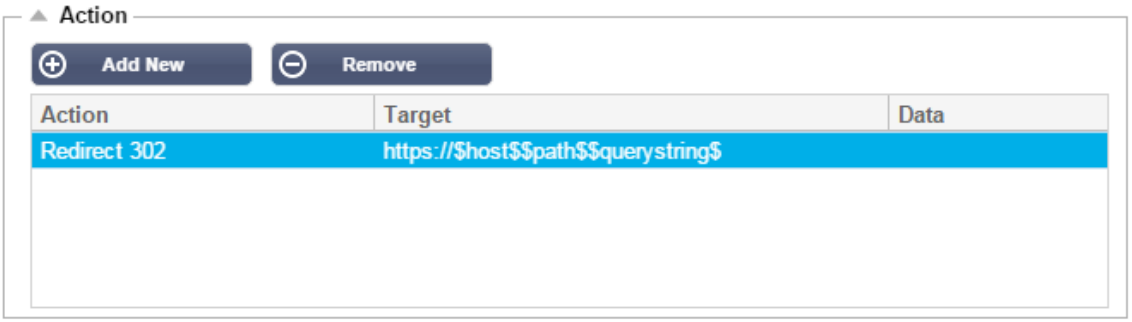
Version	Voici la version HTTP	HTTP/1.0 ou HTTP/1.1

Détail	**Description**	**Exemple**
Accepter	Types de contenu acceptables	Accepter : text/plain
Accept-Encoding	Encodements acceptables	Accept-Encoding : <compress | gzip | deflate | sdch | identity>
Accept-Language	Langues acceptables pour la réponse	Accept-Language : en-US
Accept-Ranges	Quels types de plages de contenu partiel ce serveur supporte-t-il ?	Accept-Ranges : bytes
Autorisation	Références d'authentification pour l'authentification HTTP	Autorisation : Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Charge-To	Contient des informations comptables sur les coûts de l'application de la méthode demandée.	
Content-Encoding	Le type d'encodage utilisé sur les données.	Content-Encoding : gzip
Content-Length	La longueur du corps de la réponse en octets (octets de 8 bits).	Content-Length : 348
Content-Type	Le type mime du corps de la demande (utilisé avec les demandes 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 de l' origine du message	Date = "Date" " :" HTTP-date
ETag	Un identifiant pour une version spécifique d'une ressource, souvent un résumé 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 304 Not Modified si le contenu est inchangé.	If-Modified-Since : Sat, 29 Oct 1994 19:43:31 GMT
Dernière modification	La date de 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 l'implémentation qui peuvent avoir des effets divers 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.	Referrer : 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	La chaîne de l'agent utilisateur de l'agent utilisateur	User-Agent : Mozilla/5.0 (compatible ; MSIE 9.0 ; Windows NT 6.1 ; WOW64 ; Trident/5.0)
Varier	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 au serveur d'origine.	Vary : User-Agent
X-Powered-By	Spécifie la technologie (par exemple, ASP.NET, PHP, JBoss) qui prend en charge l'application Web.	X-Powered-By : PHP/5.4.0

Action

L'action est la ou les tâches qui sont activées une fois que la ou les conditions ont été 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.

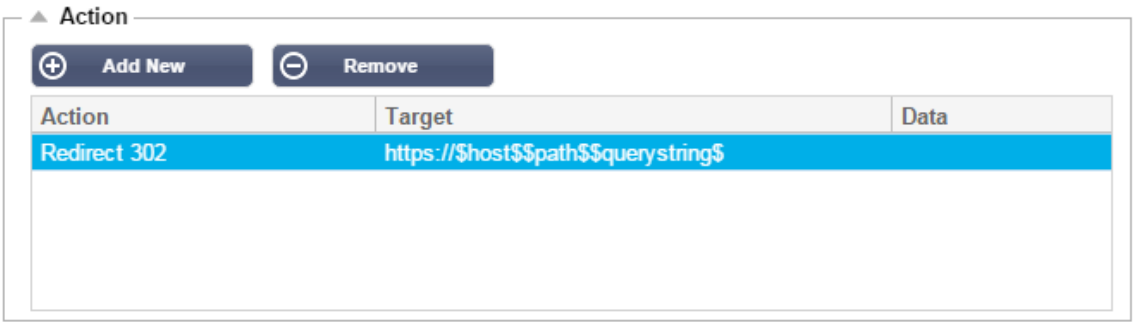
La liste de toutes les actions est détaillée ci-dessous :

Action	**Description**	**Exemple**
Cookie de demande d'ajout	Ajoutez le cookie de demande détaillé dans la section Target avec une valeur dans la section Data.	Target= Cookie Données= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter l'en-tête de la demande	Ajouter un en-tête de demande de type Target avec une valeur dans la section Data.	Target= Accepter Données= image/png
Ajouter un	Ajoutez le cookie de réponse détaillé	Target= Cookie

cookie de réponse	dans la section Cible avec une valeur dans la section Données.	Données= MS-WSMAN=afYfn1CDqqCDqCVii
Ajouter l'en-tête de la réponse	Ajouter un en-tête de demande détaillé dans la section Target avec une valeur dans la section Data.	Target= Cache-Control Données= max-age=8888888
Corps Remplacer tous	Recherchez le corps de la réponse et remplacez toutes les instances	Target= HTTP:// (Chaîne de recherche) Data= HTTPs:// (Chaîne de remplacement)
Remplacement du corps en premier	Rechercher le corps de la réponse et remplacer la première instance seulement	Target= HTTP:// (Chaîne de recherche) Data= HTTPs:// (Chaîne de remplacement)
Corps Remplacement Dernier	Rechercher dans le corps de la réponse et remplacer la dernière instance seulement	Target= HTTP:// (Chaîne de recherche) Data= HTTPs:// (Chaîne de remplacement)
Drop	Cela interrompra la connexion	Objectif = N/A Données = N/A
Courrier électronique	Envoie un e-mail à l'adresse configurée dans Événements e-mail. Vous pouvez utiliser une variable comme adresse ou comme message.	Target= "flightPATH a envoyé un e-mail à cet événement". Données = N/A
Événement de journal	Ceci enregistrera un événement dans le journal du système	Target= "flightPATH a enregistré ceci dans syslog". Données = N/A
Redirection 301	Cela donnera une redirection permanente	Cible= HTTP://www.edgenexus.ioData= N/A
Redirection 302	Cela va créer une redirection temporaire	Cible= HTTP://www.edgenexus.ioData= N/A
Supprimer le cookie de demande	Supprimer le cookie de demande détaillé dans la section Cible	Target= Cookie Données= MS-WSMAN=afYfn1CDqqCDqCVii
Supprimer l'en-tête de la demande	Suppression de l'en-tête de la demande détaillée dans la section Cible	Target=ServerData=N/A
Supprimer le cookie de réponse	Supprimez le cookie de réponse détaillé dans la section Cible	Target=jnAccel
Supprimer l'en-tête de réponse	Supprimez l'en-tête de réponse détaillé dans la section Cible	Target= Etag Données = N/A
Remplacer le cookie de demande	Remplacer le cookie de demande détaillé dans la section Target par la valeur de la section Data.	Target= Cookie Données= MS-WSMAN=afYfn1CDqqCDqCVii
Remplacer l'en-tête de la demande	Remplacer l'en-tête de la demande dans la cible par la valeur des données.	Cible= Connexion Données= keep-alive
Remplacer le cookie de réponse	Remplacez le cookie de réponse détaillé dans la section Target par la valeur de la section Data.	Target=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqCDqCVii

Remplacer l'en-tête de réponse	Remplacer l'en-tête de réponse détaillé dans la section Target par la valeur de la section Data.	Target= 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.	Cible = /test/path/index.html$querystring$. Données = N/A
Utiliser un serveur sécurisé	Sélectionnez le serveur sécurisé ou le service virtuel à utiliser	Target=192.168.101: 443Data=N/A
Utiliser le serveur	Sélectionnez le serveur ou le service virtuel à utiliser	Cible= 192.168.101:80Data= N/A
Chiffrer le cookie	Ceci va crypter les cookies en 3DES et ensuite les encoder en base64.	Target= Entrez le nom du cookie à crypter, vous pouvez utiliser le caractère * comme joker à la finData= Entrez une phrase de passe pour le cryptage.

Exemple :



L'action ci-dessous produira une redirection temporaire du navigateur vers un service virtuel HTTPS sécurisé. Elle utilisera le même nom d'hôte, le même chemin 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 le protocole HTTPS pour certains contenus (ou tous)
- Bloquer ou rediriger les araignées
- Prévenir et alerter les scripts intersites
- Prévention et alerte en cas d'injection SQL
- Cacher la structure du répertoire interne
- Réécrire les cookies
- Répertoire sécurisé pour des utilisateurs particuliers

Caractéristiques

- Rediriger les utilisateurs en fonction du chemin d'accès
- Fournir une authentification unique sur plusieurs systèmes
- Segmenter les utilisateurs en fonction de l'ID utilisateur ou du cookie.
- Ajouter des en-têtes pour le déchargement de SSL
- Détection de la langue

- Réécrire la demande de l'utilisateur
- Corriger les URL cassés
- Enregistrement et alerte par courriel des codes de réponse 404
- Empêcher l'accès aux répertoires/la navigation
- Envoyez aux araignées un contenu différent

Règles préétablies

Extension HTML

Change toutes les requêtes .htm en .html

Condition :

- Condition = Chemin
- Sense = fait
- Check = Match RegEx
- Valeur = \.htm$

Évaluation :

- vierge

Action :

- Action = Réécrire le chemin
- Cible = $path$I

Index.html

Force l'utilisation de index.html dans les requêtes vers les dossiers.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = Hôte
- Sense = fait
- Contrôle = Existe

Évaluation :

- vierge

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 = il faut y réfléchir sérieusement
- Sens =
- Check =

Évaluation :

- vierge

Action :

- Action =
- Cible =

Cachez CGI-BBIN :

Cache le catalogue cgi-bin dans les requêtes aux scripts CGI.

Condition : cette condition est une condition générale qui correspond à la plupart des objets.

- Condition = Hôte
- Sense = fait
- Contrôle = Correspondance avec le RegEX
- Valeur = \.cgi$

Évaluation :

- vierge

Action :

- Action = Réécrire le chemin
- Cible = /cgi-bin$chemin$.

Araignée à bûches

Enregistrez les requêtes des araignées 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
- Match = User-Agent
- Sense = fait
- Contrôle = Correspondance avec le RegEX
- Valeur = Googlebot|Slurp|bingbot|ia_archiver

Évaluation :

- Variable = $crawler
- Source = En-tête de la demande
- Détail = Utilisateur-Agent

Action :

- Action = Enregistrer l'événement
- Cible = [$crawler$] $host$$path$$$querystring

Forcer HTTPS

Force l'utilisation de HTTPS pour certains répertoires. Dans ce cas, si un client accède à un élément contenant le répertoire /secure/, il sera redirigé vers la version HTTP de l'URL demandée.

Condition :

- Condition = Chemin
- Sense = fait
- Vérifier = Contenir
- Valeur = /secure/

Évaluation :

- vierge

Action :

- Action = Redirection 302
- Cible = HTTPs://$host$$path$$$querystring$.

Media Stream :

Redirige Flash Media Stream vers le service approprié.

Condition :

- Condition = Chemin
- Sense = fait
- Contrôle = Fin
- Valeur = .flv

Évaluation :

- vierge

Action :

- Action = Redirection 302
- Cible = HTTP://$host$:8080/$path$.

Passer de HTTP à HTTPS

Changez tout code dur HTTP:// en HTTPS://.

Condition :

- Condition = Code de réponse
- Sense = fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- vierge

Action :

- Action = Remplacer tout le corps
- Cible = HTTP://
- Données = HTTPs://

Videz les cartes de crédit

Vérifiez qu'il n'y a pas de carte de crédit dans la réponse et si vous en trouvez une, effacez-la.

Condition :

- Condition = Code de réponse
- Sense = fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- vierge

Action :

- Action = Remplacer tout le corps
- 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 du contenu raisonnable à la page pour réduire le nombre de demandes 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
- Sense = fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- vierge

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
- Sense = fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation :

- vierge

Action :

- Action = Remplacer l'en-tête de la réponse
- Cible = Serveur
- Données = Secret

Ne jamais envoyer d'erreurs

Le client ne reçoit jamais d'erreurs de votre site.

Condition

- Condition = Code de réponse
- Sense = fait
- Vérifier = Contenir
- Valeur = 404

Évaluation

- vierge

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
- Sense = fait
- Vérifier = Contenir
- Valeur = allemand (standard)

Évaluation

- Variable = $host_template$
- Source = Hôte
- Valeur = .*\.

Action

- Action = Redirection 302
- Cible = HTTP//$host_template$de$path$$$querystring

Google Analytics

Insérez le code requis par Google pour l'analyse - Veuillez changer la valeur MYGOOGLECODE par votre Google UA ID.

Condition

- Condition = Code de réponse
- Sense = fait
- Contrôle = égal
- Valeur = 200 OK

Évaluation

- vierge

Action

- Action = Corps Remplacer le dernier
- Cible = </body>
- Data = <scripttype= '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 d'hôte pour les serveurs IIS IPv4 sur les services IPv6. Les serveurs IIS IPv4 n'aiment pas voir une adresse IPV6 dans la requête du client hôte, cette règle la remplace donc par un nom générique.

Condition

- vierge

Évaluation

- vierge

Action

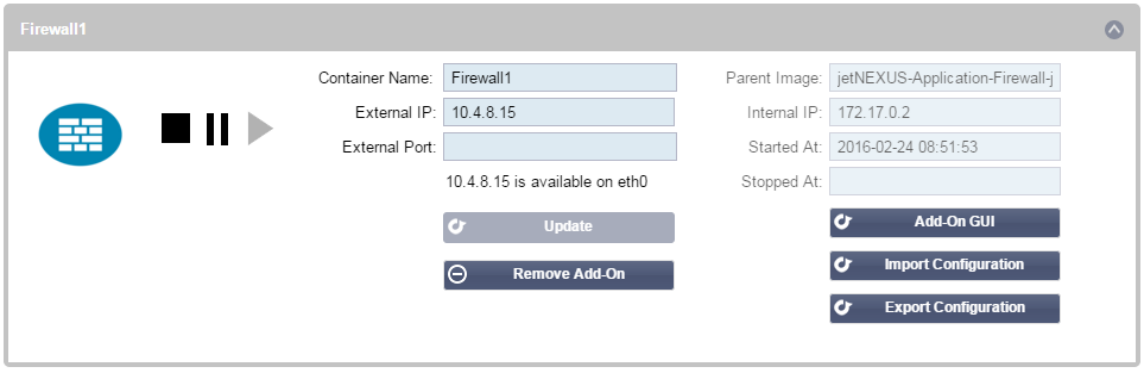
- Action = Remplacer l'en-tête de la demande
- Cible = Hôte
- Données =ipv4.host.header

Pare-feu d'application Web (edgeWAF)

Le pare-feu pour applications Web (WAF) est disponible sur demande et fait l'objet d'une licence annuelle payante. L'installation du WAF se fait à l'aide de la section Apps intégrée dans le CDA.

Exécution du WAF

Exécuté dans un conteneur Docker, le WAF a besoin que certains paramètres réseau soient définis avant son démarrage.

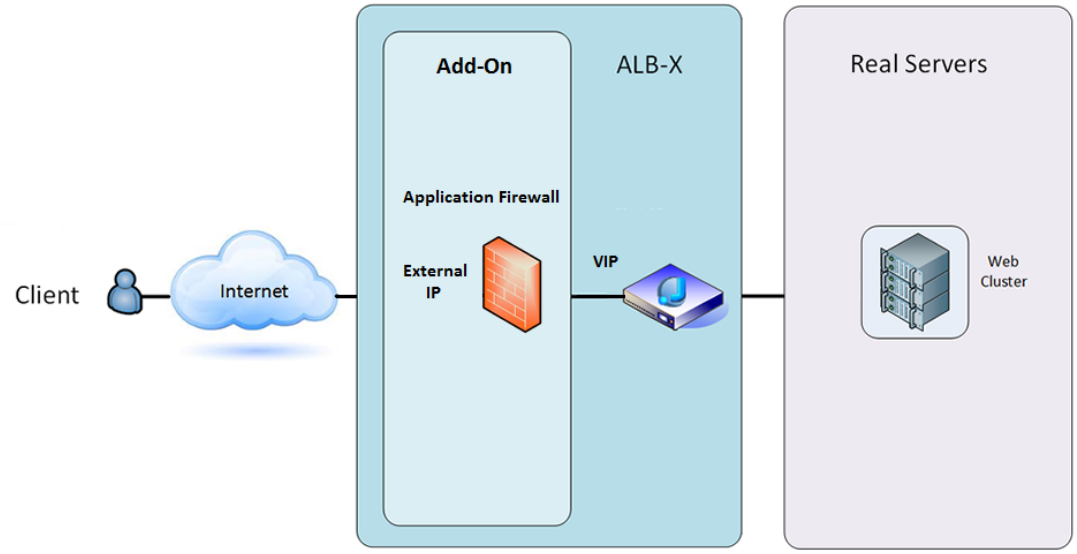


Option	Description
Stop	Il sera grisé jusqu'à ce qu'une instance Add-On soit démarrée. Appuyez sur ce bouton pour arrêter l'instance Docker.
Pause	Ce bouton met en pause le module d'extension.
Jouer	Cela lancera le module complémentaire avec les paramètres actuels.
Nom du conteneur	Donnez à votre conteneur un nom pour l'identifier des autres conteneurs. Ce nom doit être unique. Vous pouvez l'utiliser comme nom pour un serveur réel si vous le souhaitez et il sera automatiquement résolu à l'adresse IP interne de l'instance.
IP externe	Ici, vous pouvez définir une IP externe pour accéder à votre module complémentaire. Il peut s'agir d'accéder à l'interface graphique du module complémentaire ainsi qu'au service qui fonctionne via le module complémentaire. Dans le cas du module complémentaire Firewall, il s'agit de l'adresse IP de votre service HTTP. Le pare-feu peut ensuite être configuré pour accéder à un serveur ou à un VIP ALB-X qui contient plusieurs serveurs pour l'équilibrage de charge.
Port externe	Si vous laissez ce champ vide, tous les ports seront transmis à votre pare-feu. Pour le restreindre, il suffit d'ajouter une liste de ports séparés par des virgules. Exemple 80, 443, 88. Notez que l'adresse GUI du Pare-feu sera **HTTP//[External IP]88/waf.** Donc, laissez le paramètre Port externe vide ou ajoutez le port 88 pour accéder à l'interface graphique si vous limitez la liste des ports.
Mise à jour	Vous ne pouvez mettre à jour les paramètres d'un module complémentaire que lorsqu'il a été arrêté. Une fois votre instance arrêtée, vous pouvez modifier le nom du conteneur, l'IP externe et les paramètres du port externe.
Supprimer l'extension	supprimera complètement le module complémentaire de la page des modules complémentaires. Vous devrez vous rendre sur la page Library-Apps pour déployer à nouveau le module complémentaire.
Image des parents	Indique l'image Docker à partir de laquelle le module complémentaire est construit. Il peut exister plusieurs versions d'un pare-feu ou d'un autre type de module

	complémentaire, ce qui permet de les distinguer. Cette section est uniquement informative et est donc grisée.
IP interne	Docker crée automatiquement l'adresse IP interne et, par conséquent, elle ne peut pas être modifiée. Si vous arrêtez l'instance de Docker et la redémarrez, une nouvelle adresse IP interne sera émise. C'est pour cette raison que vous devez soit utiliser une adresse IP externe pour votre service, soit utiliser le nom du conteneur pour l'adresse réelle du serveur de votre service.
Commencé à	Il s'agit de la date et de l'heure auxquelles le module complémentaire a été lancé. Exemple 2016-02-16 155721
Arrêté à	Il s'agit de la date et de l'heure auxquelles le module complémentaire a été arrêté. Exemple 2016-02-24 095839

Exemple d'architecture

WAF utilisant une adresse IP externe

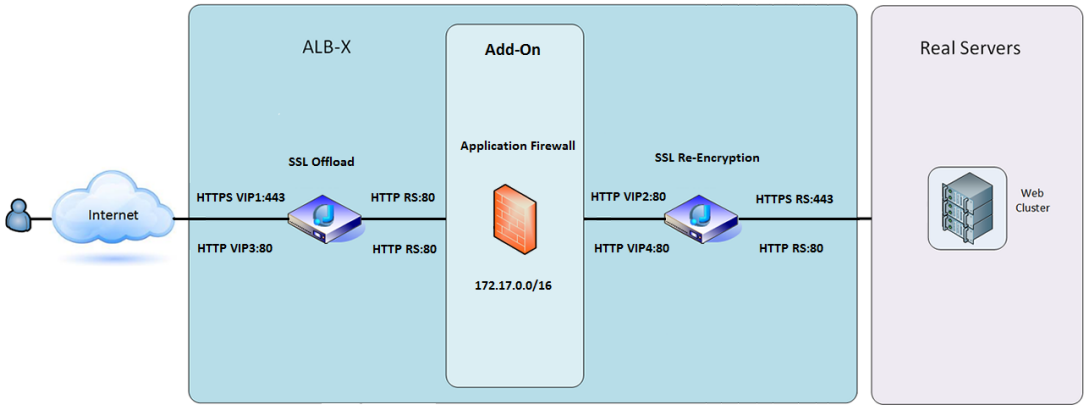


Dans cette architecture, seul le protocole HTTP peut être utilisé pour votre service car le pare-feu ne peut pas inspecter le trafic HTTPS.

Le pare-feu devra être configuré pour envoyer le trafic sur le VIP ALB-X.

Le VIP ALB-X, à son tour, sera configuré pour équilibrer la charge du trafic vers votre cluster web.

WAF utilisant une adresse IP interne



Dans cette architecture, vous pouvez spécifier HTTP et HTTPS.

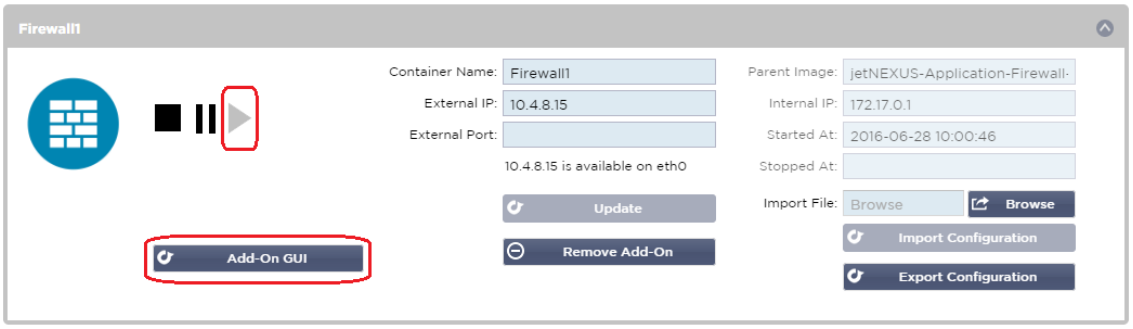
HTTPS peut être de bout en bout où les connexions du client à l'ALB-X sont cryptées et de l'ALB-X aux serveurs réels.

Le trafic de l'ALB-X vers l'adresse IP interne du pare-feu doit être décrypté pour pouvoir être inspecté.

Une fois que le trafic a traversé le pare-feu, il est ensuite transmis à un autre VIP qui peut soit re-crypter le trafic et équilibrer la charge vers des serveurs sécurisés, soit simplement équilibrer la charge vers des serveurs non sécurisés via HTTP.

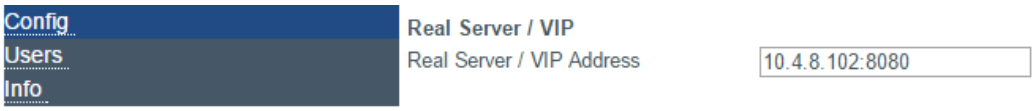
Accéder à votre module complémentaire WAF

- Remplissez les détails de votre pare-feu
- Vous pouvez soit restreindre vos ports à ce dont vous avez besoin, soit laisser le champ vide pour autoriser tous les ports.
- Cliquez sur le bouton "Play".
- Un bouton de l'interface graphique de l'extension apparaît

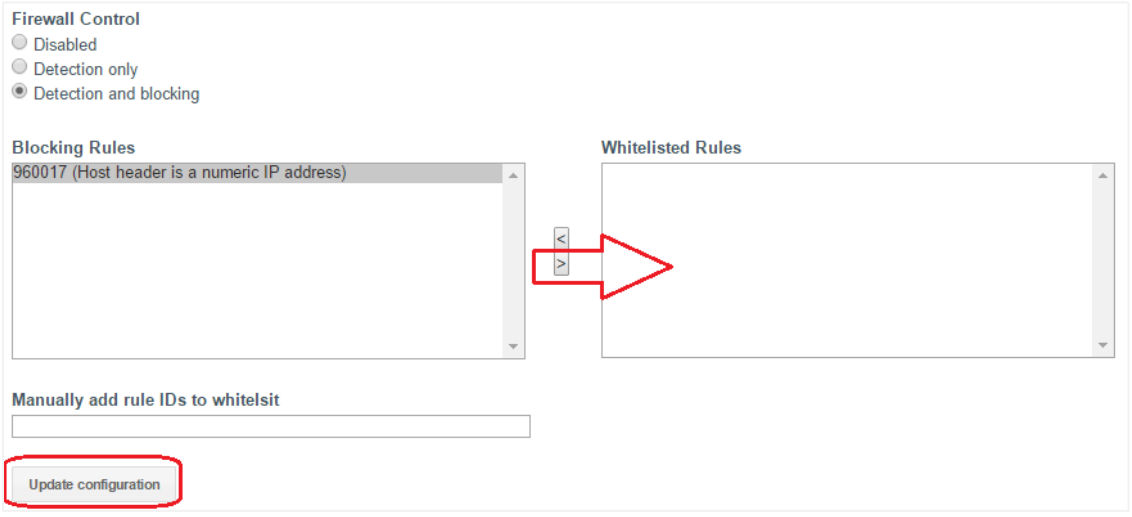


- Cliquez sur ce bouton, et il ouvrira un navigateur sur HTTP://[IP externe]:88/waf
- Dans cet exemple, ce sera HTTP://10.4.8.15:88/waf.
- Une boîte de dialogue de connexion s'affiche.
- Entrez les informations d'identification de votre CDA.
- Une fois la connexion réussie, la page d'accueil du WAF s'affiche.

- La page d'accueil présente un aperçu graphique des événements, c'est-à-dire des actions de filtrage effectuées par le pare-feu d'application.
- Les graphiques seront très probablement vides lorsque vous ouvrirez la page pour la première fois, car il n'y aura aucune tentative d'accès à travers le pare-feu.
- Vous pouvez configurer l'adresse IP ou le nom de domaine du site Web vers lequel vous souhaitez envoyer le trafic après que le pare-feu l'a filtré.
- Ceci peut être modifié dans la section Management > Config.



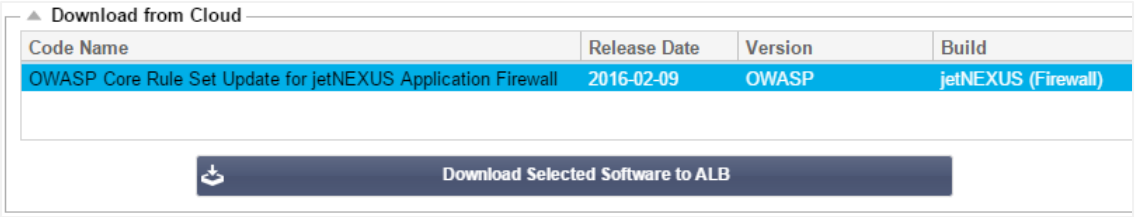
- Le pare-feu inspectera le trafic et l'enverra ensuite à l'adresse IP du serveur réel ou à l'adresse VIP indiquée ici. Vous pouvez également saisir un port en même temps que votre adresse IP. Si vous saisissez une adresse IP seule, le port sera supposé être le port 80. Cliquez sur le bouton "Update Configuration" pour enregistrer ce nouveau paramètre.
- Lorsque le pare-feu bloque une ressource applicative, la règle qui bloque le trafic apparaît dans la liste des règles de blocage de la page Liste blanche.
- Pour empêcher le pare-feu de bloquer la ressource d'application valide, veuillez déplacer la règle de blocage vers la section Règles de liste blanche.



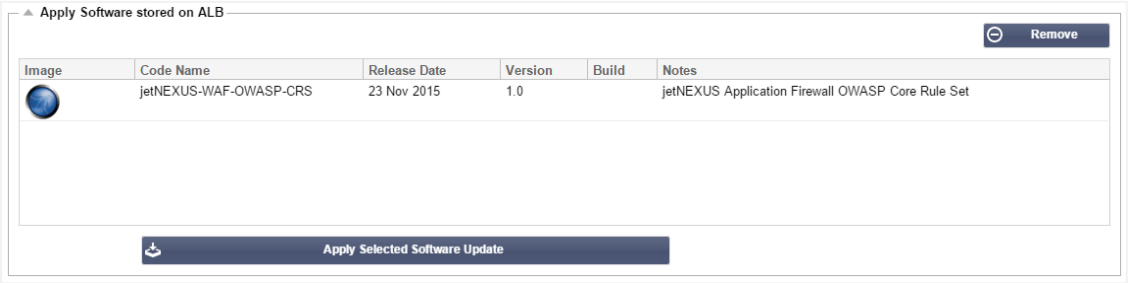
- Appuyez sur Mettre à jour la configuration lorsque vous avez transféré toutes les règles de la section Blocage vers la section Liste blanche.

Mise à jour des règles

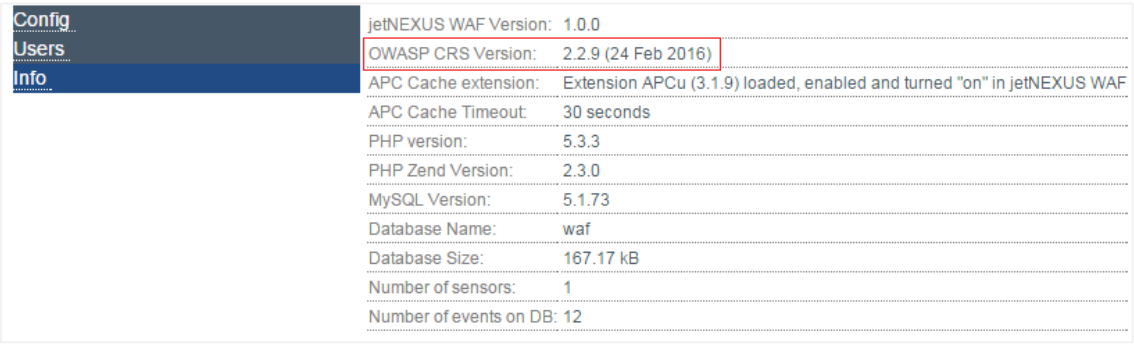
- Les règles du pare-feu d'application peuvent être mises à jour en accédant à la section Avancé - Logiciel
- Cliquez sur le bouton Rafraîchir pour afficher le logiciel disponible dans la section Détails de la mise à niveau du logiciel.
- Une boîte supplémentaire appelée Download from Cloud est maintenant affichée.
- Vérifiez si un ensemble de règles de base de l'OWASP est disponible.



- Si c'est le cas, vous pouvez mettre en surbrillance et cliquer sur Download Selected Software to ALB-X.
- Cette action téléchargera ensuite le fichier intelligent vers le logiciel d'application stocké sur l'ALB.



- Mettez en évidence le jetNEXUS-WAF-OWASP-CRS et cliquez sur Appliquer la mise à jour du logiciel sélectionné et cliquez sur Appliquer.
- Le pare-feu détectera automatiquement le jeu de règles mis à jour, le chargera et l'appliquera.
- Les ID des règles de la liste blanche seront conservés. Cependant, de nouvelles règles peuvent commencer à bloquer des ressources d'applications valides.
- Dans ce cas, veuillez vérifier la liste des règles de blocage sur la page Liste blanche.
- Vous pouvez également vérifier la section Management Info de l'interface graphique du pare-feu pour la version OWASP CRS.



Équilibrage global de la charge des serveurs (edgeGSLB)

Introduction

Global Server Load Balancing (GSLB) est un terme utilisé pour décrire les méthodes de distribution du trafic réseau sur Internet. Le GSLB est différent du Server Load Balancing (SLB) ou de l'Application Load Balancing (ALB), car il est généralement utilisé pour distribuer le trafic entre plusieurs centres de données, alors qu'un ADC/SLB traditionnel est utilisé pour distribuer le trafic au sein d'un seul centre de données.

La GSLB est généralement utilisée dans les situations suivantes :

Résilience et reprise après sinistre

Vous disposez de plusieurs centres de données et vous souhaitez les faire fonctionner dans une situation Active-Passive de sorte que si un centre de données tombe en panne, le trafic sera envoyé vers l'autre.

Équilibrage des charges et géolocalisation

Vous souhaitez répartir le trafic entre les centres de données dans une situation Active-Active en fonction de critères spécifiques tels que les performances du centre de données, sa capacité, le bilan de santé du centre de données, l'emplacement physique du client (afin de l'envoyer vers le centre de données le plus proche), etc.

Considérations commerciales

Veillez à ce que les utilisateurs de certaines zones géographiques soient dirigés vers des centres de données particuliers. S'assurer que des contenus différents sont servis (ou bloqués) aux autres utilisateurs, en fonction de plusieurs critères tels que le pays dans lequel se trouve le client, la ressource qu'il demande, la langue, etc.

Aperçu du système de noms de domaine

Le GSLB peut être complexe ; il vaut donc la peine de prendre le temps de comprendre le fonctionnement du mystérieux système de serveur de noms de domaine (DNS).

Le DNS se compose de trois éléments clés :

- Le résolveur DNS, c'est-à-dire le client : le résolveur est chargé d'initier les requêtes qui conduisent finalement à une résolution complète de la ressource requise.
- Nameserver : il s'agit du nameserver auquel le client se connecte initialement pour effectuer la résolution DNS.
- Serveurs de noms faisant autorité : Inclure les serveurs de noms du domaine de premier niveau (TLD) et les serveurs de noms racine.

Une transaction DNS typique est expliquée ci-dessous :

- Un utilisateur tape "exemple.com" dans un navigateur web, la requête voyage sur Internet et est reçue par un résolveur récursif DNS.
- Le résolveur interroge ensuite un serveur de noms racine DNS (.).
- Le serveur racine répond alors au résolveur avec l'adresse d'un serveur DNS de domaine de premier niveau (TLD) (tel que .com ou .net), qui stocke les informations pour ses domaines. Lorsque nous recherchons exemple.com, notre requête est dirigée vers le TLD .com.
- Le résolveur demande alors le TLD .com.
- Le serveur TLD répond alors avec l'adresse IP du serveur de noms du domaine, exemple.com.

- Enfin, le résolveur récursif envoie une requête au serveur de noms du domaine.
- L'adresse IP, par exemple exemple.com, est ensuite renvoyée au résolveur par le serveur de noms.
- Le résolveur DNS répond alors au navigateur web avec l'adresse IP du domaine demandé initialement.
- Une fois que les huit étapes de la recherche DNS ont renvoyé l'adresse IP, par exemple .com, le navigateur peut demander la page Web :
- Le navigateur effectue une requête **HTTP** vers l'adresse IP.
- Le serveur à cette adresse IP renvoie la page web à rendre dans le navigateur.

Ce processus peut être encore plus compliqué :

Mise en cache

Les serveurs de noms de résolution mettent en cache les réponses et peuvent envoyer la même réponse à de nombreux clients. Les résolveurs et les applications côté client peuvent avoir des politiques de mise en cache différentes.

Remarque : Pour les tests, nous arrêtons et désactivons le client DNS de Windows dans la section des services de votre système d'exploitation. Les noms DNS continueront d'être résolus, mais le client ne mettra pas les résultats en cache et n'enregistrera pas le nom de l'ordinateur. Votre administrateur système devra décider si cette option est la meilleure pour votre environnement, car elle peut affecter d'autres services.

Le temps de vivre

Le serveur de noms qui résout le problème peut ignorer le Time To Live (TTL), c'est-à-dire le temps de mise en cache de la réponse.

Aperçu de la GSLB

GSLB est basé sur le DNS et utilise un mécanisme très similaire à celui décrit ci-dessus.

Le CDA peut modifier la réponse en fonction de plusieurs facteurs décrits plus loin dans le guide. L'ADC utilise les moniteurs pour vérifier la disponibilité des ressources distantes en accédant à la ressource elle-même. Cependant, pour appliquer une quelconque logique, le système doit d'abord recevoir la requête DNS.

Plusieurs conceptions le permettent. La première est celle où le GSLB fait office de serveur de noms faisant autorité.

La deuxième conception est la mise en œuvre la plus courante et est similaire à la configuration du serveur de noms faisant autorité mais utilise un sous-domaine. Le serveur DNS primaire faisant autorité n'est pas remplacé par GSLB mais délègue un sous-domaine pour la résolution. Le fait de déléguer directement des noms ou d'utiliser des CNAME vous permet de contrôler ce qui est et n'est pas géré par la GSLB. Dans ce cas, il n'est pas nécessaire d'acheminer tout le trafic DNS vers le GSLB pour les systèmes qui ne nécessitent pas de GSLB.

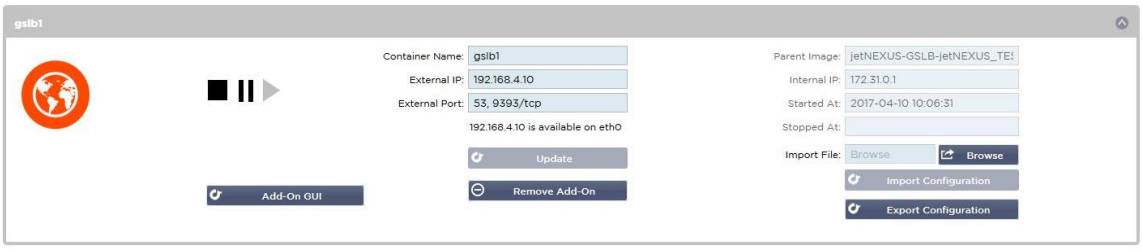
La redondance est assurée de sorte que si un serveur de noms (GSLB) tombe en panne, le serveur de noms distant envoie automatiquement une autre demande à un autre GSLB, ce qui évite que le site web ne tombe en panne.

Configuration du GSLB

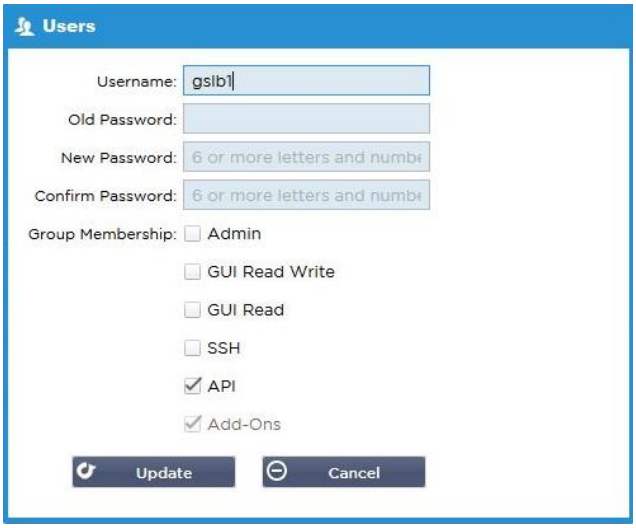
Après avoir téléchargé le module complémentaire GSLB, veuillez le déployer en vous rendant sur la page Library > Apps de l'interface graphique du CDA et en cliquant sur le bouton "Deploy" comme indiqué ci-dessous.

Après l'installation, veuillez configurer les détails de l'extension GSLB, y compris le nom du conteneur, l'IP externe et les ports externes dans la page Library > Add-Ons de l'interface graphique de l'ADC, comme indiqué dans la figure ci-dessous.

- Le nom du conteneur est le nom unique d'une instance d'extension en cours d'exécution, hébergée par ADC. Il est utilisé pour distinguer plusieurs extensions d'un même type.
- L'IP externe est l'IP de votre réseau qui sera attribuée à GSLB.
- Vous devez configurer le GSLB pour avoir une adresse IP externe si vous voulez prendre des décisions basées sur le GEO, car cela permettra au GSLB de voir l'adresse IP réelle des clients.
- Ports externes est la liste des ports TCP et UDP de GSLB, auxquels on peut accéder depuis d'autres hôtes du réseau.
- Veuillez mettre "53/UDP, 53/TCP, 9393/TCP" dans la boîte de saisie Ports externes pour permettre les communications DNS (53/UDP, 53/TCP) et edgeNEXUS GSLB GUI (9393/TCP).
- Après avoir configuré les détails du module complémentaire, veuillez cliquer sur le bouton Mettre à jour.
- Lancez le module d'extension GSLB en cliquant sur le bouton Exécuter.

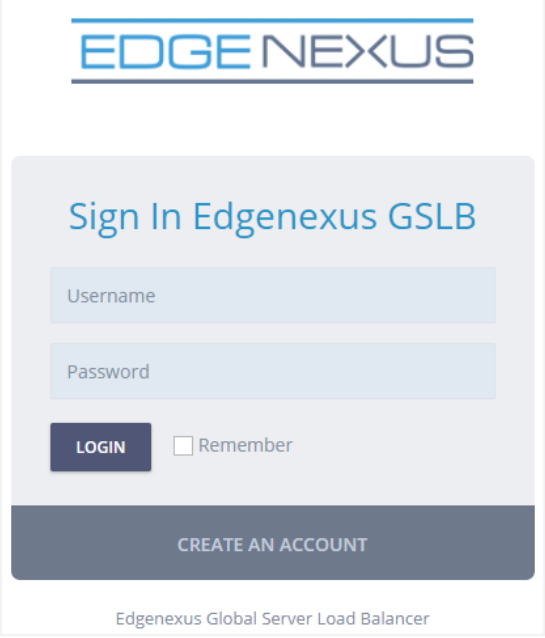


- L'étape suivante consiste à permettre au module d'extension GSLB d'edgeNEXUS de lire et de modifier la configuration de l'ADC.
- Veuillez visiter la page Système > Utilisateurs de l'interface graphique de l'ADC et modifier un utilisateur avec le même nom que l'extension GSLB que vous avez déployée, comme indiqué dans la figure ci-dessous.
- Modifiez l'utilisateur "gslb1" et cochez API, puis cliquez sur Mettre à jour - dans les versions ultérieures du logiciel, cette case peut déjà être cochée par défaut.



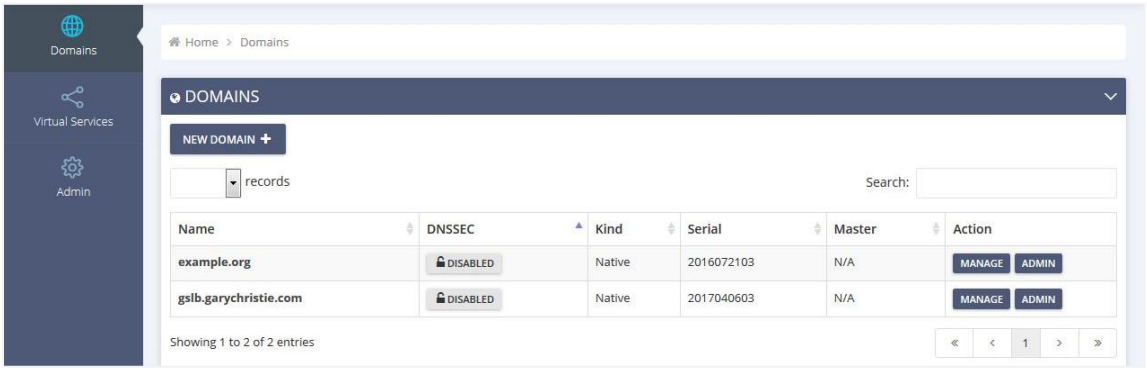
- L'étape suivante n'est nécessaire que si vous configurez GSLB à des fins de test ou d'évaluation et que vous ne souhaitez pas modifier les données de la zone DNS sur Internet.
- Dans ce cas, veuillez demander à l'ADC d'utiliser GSLB Add-On comme serveur de résolution DNS primaire en modifiant "DNS Server 1" dans la page Système > Réseau de l'ADC GUI, comme indiqué dans la figure ci-dessous.
- Le serveur DNS 2 peut être configuré généralement avec votre serveur DNS local ou un autre sur Internet, tel que Google 8.8.8.8.

- Le moment est venu de vous connecter à l'interface graphique GSLB.
- Veuillez naviguer vers la page Bibliothèque > Add-Ons de l'interface graphique du CDA et cliquez sur le bouton Add-On GUI.
- En cliquant, vous ouvrirez un nouvel onglet de navigateur qui présente la page de connexion de l'interface graphique GSLB, comme indiqué ci-dessous.

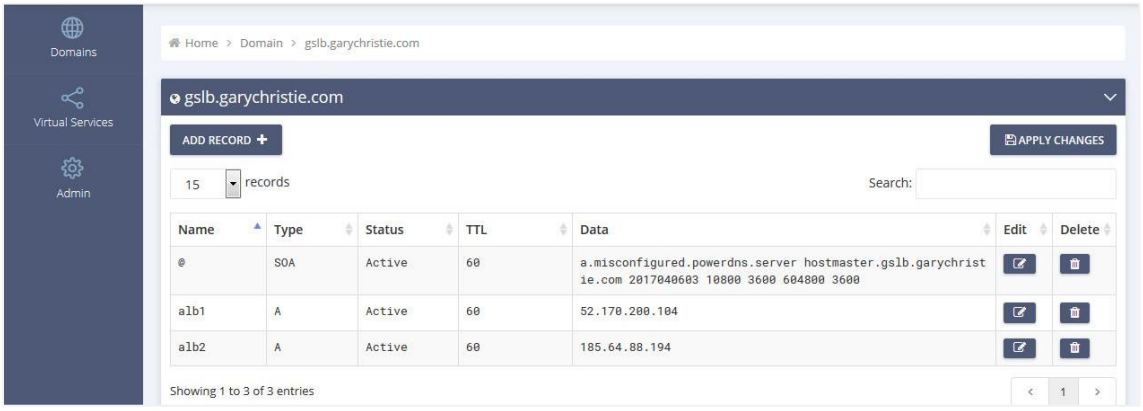


- Le nom d'utilisateur par défaut est admin, et le mot de passe par défaut est jetnexus. N'oubliez pas de changer votre mot de passe sur la page Administrateur > Mon profil de GSLB GUI.
- L'étape suivante de la séquence de configuration consiste à créer une zone DNS dans le serveur de noms PowerDNS, qui fait partie de GSLB, en en faisant soit un serveur de noms faisant autorité pour la zone "example.org", soit une zone de sous-domaine, comme le sous-domaine "geo.example.org" mentionné dans la section "Aperçu de GSLB basé sur les DNS" ci-dessus.
- Pour plus de détails sur la configuration des zones DNS, veuillez consulter la **DOCUMENTATION DU SERVEUR DE NOMS POWERDNS**. Un exemple de zone est présenté dans la Figure 6.

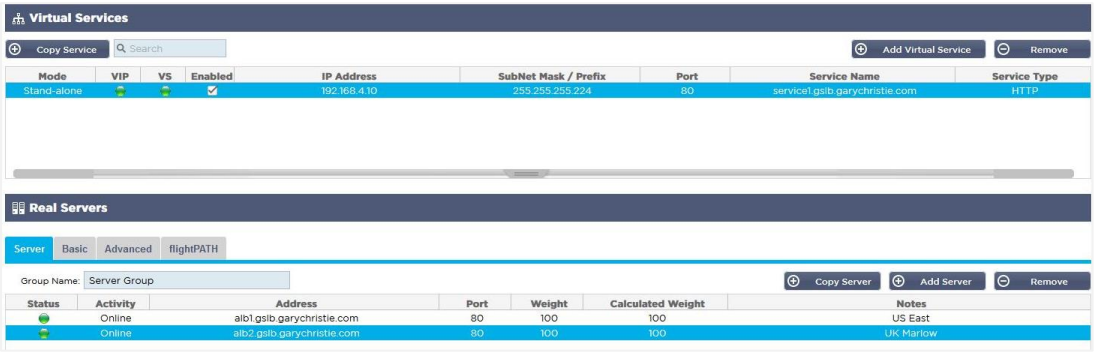
* L'interface graphique GSLB d'edgeNEXUS est basée sur un projet Open Source PowerDNS-Admin.



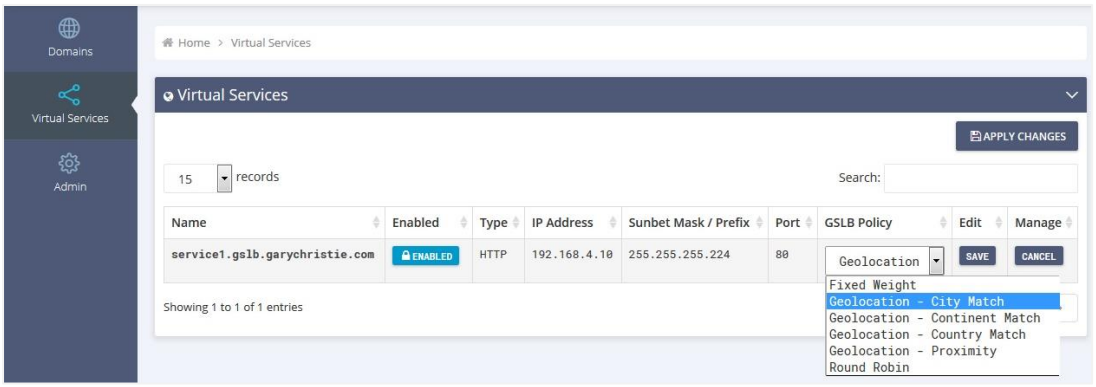
- Après avoir créé une zone DNS, veuillez cliquer sur le bouton Manage et ajouter des noms d'hôtes au domaine, comme indiqué dans la figure ci-dessous.
- Après avoir modifié tout enregistrement existant dans l'interface graphique de la BGDS, veuillez appuyer sur le bouton Enregistrer.
- Après avoir terminé la création des enregistrements de nom d'hôte, veuillez cliquer sur le bouton Appliquer les modifications. Si vous ne cliquez pas sur Appliquer et ne modifiez pas ensuite la page, vous perdrez vos modifications.
- Nous avons créé ci-dessous des enregistrements qui sont des enregistrements d'adresses IPv4.
- Veillez à créer un enregistrement pour tous les enregistrements que vous souhaitez faire résoudre, y compris les enregistrements AAAA pour les adresses IPv6.



- Maintenant, retournons à l'interface graphique de l'ADC et définissons un service virtuel qui correspond à la zone DNS que nous venons de créer.



- Le service virtuel sera utilisé pour le contrôle de l'état des serveurs dans le domaine GSLB.
- La GSLB exploite le mécanisme de vérification de la santé de l'ADC, y compris les moniteurs personnalisés. Il peut être utilisé avec tous les types de services pris en charge par l'ADC.
- Veuillez naviguer vers la page Services > IP-Services de l'ADC GUI et créer un Service Virtuel, comme indiqué dans la figure ci-dessous.
- Veillez à configurer le nom de service avec le nom de domaine correct que vous souhaitez utiliser dans le GSLB. Le GSLB le lira via l'API et remplira automatiquement la section des services virtuels dans l'interface graphique du GSLB.
- Veuillez ajouter tous les serveurs du domaine GSLB dans la section Real Servers de l'image ci-dessus.
- Vous pouvez spécifier les serveurs, soit par leur nom de domaine, soit par leur adresse IP.
- Si vous spécifiez les noms de domaine, alors il utilisera les enregistrements créés sur votre GSLB.
- Vous pouvez choisir différentes méthodes et paramètres de surveillance de la santé du serveur dans les onglets Basique et Avancé.
- Vous pouvez définir l'activité de certains serveurs sur Standby pour un scénario Active-Passive.
- Dans ce cas, si un serveur "en ligne" échoue à un contrôle de santé et qu'il existe un serveur de secours sain, Edgenexus EdgeGSLB résoudra le nom de domaine à une adresse du serveur de secours.
- Veuillez vous reporter à la section **SERVICES VIRTUELS** pour plus de détails sur la configuration des services virtuels.
- Maintenant, passons à l'interface graphique de GSLB.
- Naviguez vers la page des services virtuels et sélectionnez une politique GSLB pour le domaine de l'API récupéré dans la section des services virtuels ADC.
- Ceci est illustré dans la figure ci-dessous.



- Le GSLB soutient les politiques suivantes :

Politique	Description
Poids fixe	Le GSLB sélectionne le serveur ayant le poids le plus élevé (la pondération des

	serveurs peut être attribuée par l'utilisateur). Dans le cas où plusieurs serveurs ont le poids le plus élevé, le GSLB sélectionne l'un de ces serveurs au hasard.
Round Robin pondéré	Choisissez les serveurs un par un, dans une rangée. Les serveurs dont la pondération est la plus élevée sont sélectionnés plus souvent que les serveurs dont la pondération est la plus faible.
Géolocalisation	Proximité - choisir un serveur qui est situé le plus près de l'emplacement du client en utilisant les données de latitude et de longitude géographiques. Les serveurs situés dans le même pays que le client sont préférés, même s'ils sont plus éloignés que les serveurs des pays voisins.
Géolocalisation	Correspondance de ville - choisir un serveur dans la même ville que le client. S'il n'y a pas de serveur dans la ville du client, sélectionnez un serveur dans le pays du client. S'il n'y a pas de serveur dans le pays du client, sélectionnez un serveur sur le même continent. Si cela n'est pas possible, sélectionnez le serveur le plus proche de l'emplacement du client en utilisant les données de latitude et de longitude géographiques.
Géolocalisation	Correspondance de pays - choisir un serveur dans le même pays que le client. S'il n'y a pas de serveur dans le même pays, essayez le même continent, puis la localisation la plus proche.
Géolocalisation	Correspondance continentale : choisissez un serveur sur le même continent que le client. S'il n'y a pas de serveur sur le même continent, essayez l'emplacement le plus proche.

- Après avoir sélectionné une politique de GSLB, n'oubliez pas de cliquer sur le bouton Appliquer les modifications.
- Vous pouvez maintenant revoir et ajuster les détails du service virtuel en cliquant sur le bouton Gérer.
- La page ci-dessous s'affiche.
- Si vous avez sélectionné l'une des politiques basées sur la pondération, vous devrez peut-être ajuster les pondérations GSLB du serveur.
- Si vous avez choisi l'une des politiques GSLB basées sur la géolocalisation, vous devrez peut-être spécifier des données géographiques pour les serveurs.
- Si vous ne spécifiez pas de données géographiques pour les serveurs, le GSLB utilisera les données fournies par la **BASE DE DONNÉES GEOLITE2 DE MAXMIND**.
- Vous pouvez également modifier le nom, le port et l'activité du serveur sur cette page.
- Ces modifications seront synchronisées avec le CDA lorsque vous cliquerez sur le bouton "Appliquer les modifications".

- Un excellent moyen de vérifier les réponses que le GSLB renverra aux clients est d'utiliser le NSLOOKUP.

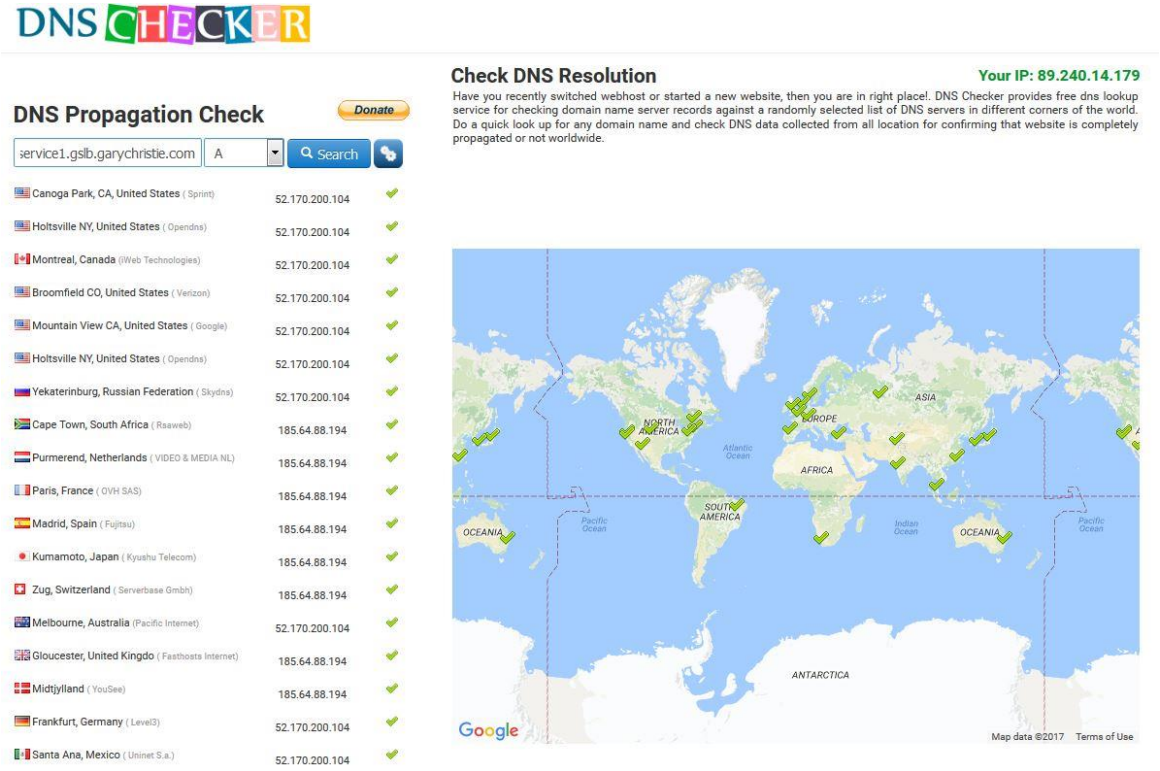
- Si vous utilisez Windows, la commande est la suivante.

  NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Où service1.gslb.garychristie.com est le nom de domaine que vous souhaitez résoudre.
- Où 192.168.4.10 est l'adresse IP externe de votre GSLB.
- Pour vérifier quelle adresse IP sera renvoyée sur l'internet, vous pouvez utiliser le serveur DNS google de 8.8.8.8.

  Nslookup service1.gslb.garychristie.com 8.8.8.8.

- Sinon, vous pouvez utiliser quelque chose comme HTTPs://dnschecker.org. Exemple HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Voir ci-dessous un exemple des résultats.



Emplacements personnalisés

Réseaux privés

Le GSLB peut également être configuré pour utiliser des emplacements personnalisés afin que vous puissiez l'utiliser sur des réseaux internes "privés". Dans le scénario ci-dessus, le GSLB détermine l'emplacement du client en croisant l'adresse IP publique du client avec une base de données pour déterminer son emplacement. Il détermine également l'emplacement de l'adresse IP du service à partir de la même base de données, et si la politique d'équilibrage de la charge est définie sur une politique GEO, il renverra l'adresse IP la plus proche. Cette méthode fonctionne parfaitement bien avec les adresses IP publiques, mais il n'existe pas de base de données de ce type pour les adresses privées internes conformes à la RFC 1918 pour les adresses IPv4 et à la RFC 4193 pour les adresses IPv6.

Veuillez consulter la page Wikipedia expliquant l'adressage privé
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Comment cela fonctionne

En général, l'idée derrière l'utilisation de notre GSLB pour les réseaux internes est que les utilisateurs d'adresses spécifiques reçoivent une réponse différente pour un service en fonction du réseau dans lequel ils se trouvent. Ainsi, considérons deux centres de données, Nord et Sud, fournissant un service appelé respectivement north.service1.gslb.com et south.service1.gslb.com. Lorsqu'un utilisateur du centre de données du Nord interroge le GSLB, nous voulons que le GSLB réponde avec l'adresse IP associée à north.service1.gslb.com, à condition que le service fonctionne correctement. Par contre, si un utilisateur du centre de données du sud interroge le GSLB, nous voulons que le GSLB réponde avec l'adresse IP associée à south.service1.gslb.com, à condition que le service fonctionne correctement.

Alors, que devons-nous faire pour que le scénario ci-dessus se réalise ?

- Nous devons avoir au moins deux emplacements personnalisés, un pour chaque centre de données.
- Attribuez les différents réseaux privés à ces emplacements
- Affecter chaque service à son emplacement respectif

Comment configurer ce look sur le GSLB ?

Ajouter un emplacement pour le centre de données du Nord

- Cliquez sur Emplacements personnalisés dans la partie gauche
- Cliquez sur Ajouter un emplacement
- Nom
  - Nord
- Ajoutez une adresse IP privée et un masque de sous-réseau pour votre réseau du Nord. Pour cet exercice, nous supposerons que les adresses IP du service et du client se trouvent dans le même réseau privé.
  - 10.1.1.0/24
- Ajouter le code Continent
  - UE
- Ajouter le code du pays
  - ROYAUME-UNI
- Ajouter une ville
  - Enfield
- Ajouter la latitude - obtenue à partir de google
  - 51.6523
- Ajouter la longitude - obtenue à partir de google
  - 0.0807

Remarque : veuillez utiliser les codes corrects qui peuvent être obtenus ici.

Ajouter un emplacement pour le centre de données du Sud

- Cliquez sur Emplacements personnalisés dans la partie gauche
- Cliquez sur Ajouter un emplacement
- Nom
  - Sud
- Ajoutez une adresse IP privée et un masque de sous-réseau pour votre réseau Sud. Nous supposerons que les adresses IP du service et du client se trouvent dans le même réseau privé pour cet exercice.
  - 192.168.1.0/24
- Ajouter le code Continent

    - UE
- Ajouter le code du pays
    - ROYAUME-UNI
- Ajouter une ville
    - Croydon
- Ajouter la latitude - obtenue à partir de google
    - 51.3762
- Ajouter la longitude - obtenue à partir de google
    - 0.0982

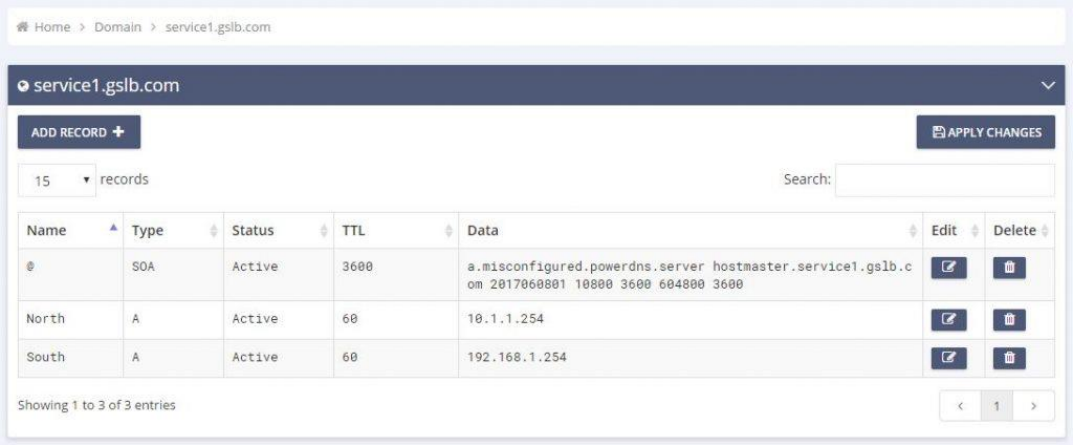
Remarque : veuillez utiliser les codes corrects qui peuvent être obtenus **ICI.**

Ajouter un enregistrement A pour north.service1.gslb.com

- Cliquez sur le domaine service1.gslb.com
- Cliquez sur Ajouter un enregistrement
- Ajouter un nom
    - Nord
- Type
    - A
- Statut
    - Actif
- TTL
    - 1 minute
- Adresse IP
    - 10.1.1.254 (Notez que c'est dans le même réseau que le site d'Enfield)

Ajouter un enregistrement A pour south.service1.gslb.com

- Cliquez sur le domaine service1.gslb.com
- Cliquez sur Ajouter un enregistrement
- Ajouter un nom
    - Sud
- Type
    - A
- Statut
    - Actif
- TTL
    - 1 minute
- Adresse IP
    - 192.168.1.254 (Notez que ceci est dans le même réseau que le site de Croydon)



Flux de trafic

Exemple 1 - Client dans un centre de données du Nord

- Le client IP 10.1.1.23 interroge GSLB pour service1.gslb.com
- GSLB recherche l'adresse IP 10.1.1.23 et la fait correspondre à la localisation personnalisée Enfield 10.1.1.0/24.
- GSLB regarde ses enregistrements A pour le service1.gslb.com et correspond à north.service1.gslb.com car il est aussi dans le réseau 10.1.1.0/24.
- GSLB répond à 10.1.1.23 avec l'adresse IP 10.1.1.254 pour service1.gslb.com

Exemple 2 - Client dans un centre de données du sud

- Le client IP 192.168.1.23 interroge GSLB pour service1.gslb.com
- GSLB recherche l'adresse IP 192.168.1.23 et la fait correspondre à Custom Location Croydon 192.168.1.0/24
- GSLB regarde ses enregistrements A pour le service1.gslb.com et correspond à south.service1.gslb.com car il est également dans le réseau 192.168.1.0/24.
- GSLB répond à 192.168.1.23 avec l'adresse IP 192.168.1.254 pour service1.gslb.com

Support technique

Nous fournissons une assistance technique à tous nos utilisateurs conformément aux conditions générales de service de l'entreprise.

Nous fournirons toute l'assistance via le support technique si vous avez un contrat de support et de maintenance actif pour l'edgeADC, l'edgeWAF ou l'edgeGSLB.

Pour obtenir un ticket d'assistance, veuillez vous rendre sur le site :

https://www.edgenexus.io/support/