EdgeADC

Guia de Administração do EdgeADC

VERSÃO DO SOFTWARE

5.0.0

Conteúdo

Propriedades do documento

Número do documento:2 .0.3.19.25.12.03

Data de criação do documento:19 March 2025

Último documento editado: 19 March 2025

Autor do documento: Jay Savoor

Documento Editado pela última vez por:

Documento: EdgeADC - Versão 5.0.0

Declaração de exoneração de responsabilidade do documento

As imagens de ecrã e os gráficos deste manual podem diferir ligeiramente do seu produto devido a diferenças na versão do produto. A Edgenexus garante que envida todos os esforços razoáveis para assegurar que as informações contidas neste documento são completas e exactas. A Edgenexus não assume qualquer responsabilidade por quaisquer erros. A Edgenexus efectua alterações e correcções às informações contidas neste documento em futuras versões, sempre que necessário.

Direitos de autor

Marcas registadas

O logótipo da Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS são marcas comerciais ou marcas comerciais registadas da Edgenexus Limited. Todas as outras marcas comerciais são propriedade dos respectivos proprietários e são reconhecidas.

Suporte Edgenexus

Se tiver alguma questão técnica relacionada com este produto, abra um pedido de assistência em: support@edgenexus.io

Introdução

Está a ler este guia porque pretende implementar o Edgenexus EdgeADC e equilibrar a carga das suas aplicações baseadas em servidores de forma eficiente e económica.

O EdgeADC é construído em torno de um motor altamente seguro que oferece elevada escalabilidade, segurança, elevado desempenho e uma interface de gestão muito fácil de utilizar. Estes factores asseguram que a sua implementação proporcionará o melhor custo de propriedade possível.

O objetivo do presente documento

Este documento foi redigido para que o usuário possa administrar o EdgeADC por meio de sua interface simples baseada na web. As funções e suas configurações são descritas em detalhes, e esperamos que isso seja suficiente para que você possa configurar o EdgeADC de acordo com suas necessidades.

A quem se destina o presente documento?

Este documento destina-se a pessoas com conhecimentos de redes, nomeadamente protocolos, aplicações e servidores.

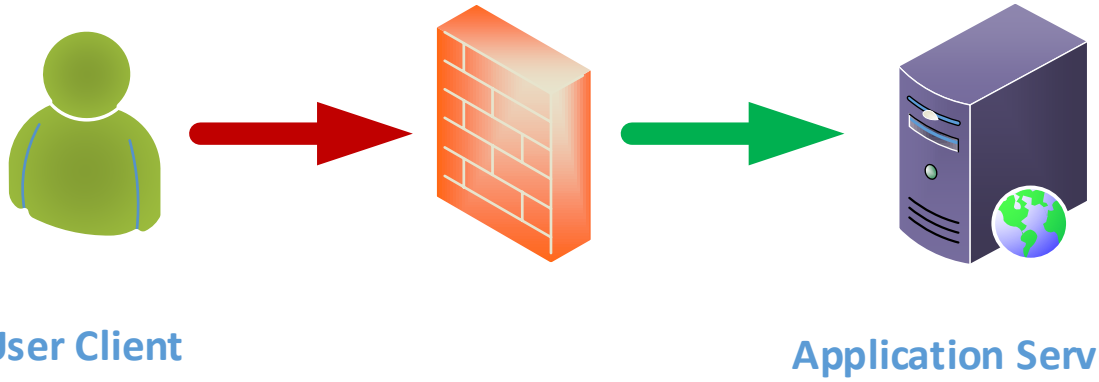
Balanceamento de carga 101

O que é um Load Balancer ou ADC?

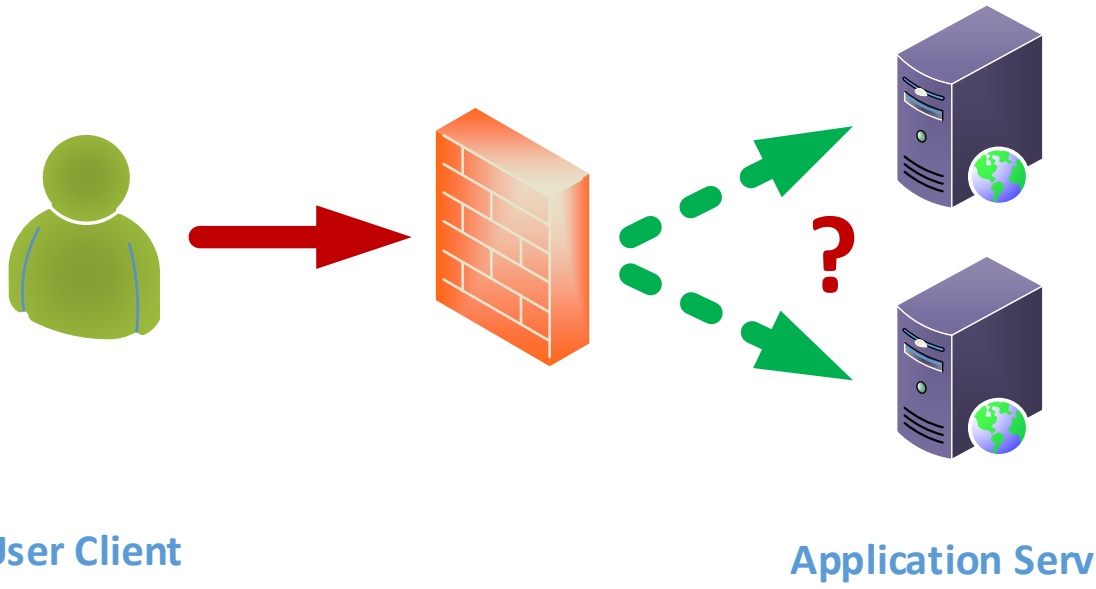
Os balanceadores de carga evoluíram imenso e têm muito mais inteligência incorporada nos seus motores do que anteriormente. Atualmente, são frequentemente designados por controladores de entrega de aplicações ou ADCs.

Antes de podermos compreender o que é um equilibrador de carga ou um ADC, temos de reconhecer os problemas do informático e do utilizador. Vejamos um exemplo.

- Uma empresa tem uma aplicação Web que está a publicar na Internet. A aplicação está alojada num único servidor Web, com os dados a residir num servidor de base de dados separado.



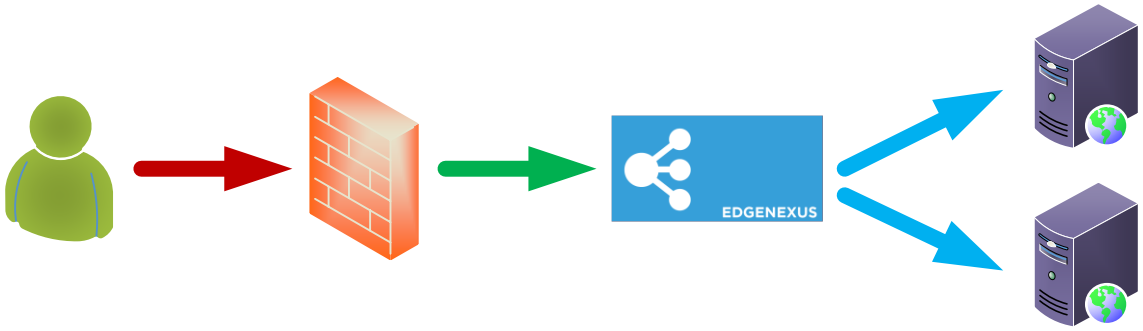
- Este servidor utiliza o endereço IP de 1.2.3.4 como exemplo.
- O número de clientes que acedem à aplicação está a aumentar regularmente, e alguns assinalaram que o desempenho da aplicação está a diminuir.
- A análise do servidor mostra que o tráfego que atinge o servidor aumentou enormemente e continua a progredir.
- Assim, é tomada a decisão de adicionar outro servidor para alojar a aplicação.
- O novo segundo servidor utiliza o endereço IP 1.2.3.5.
- O problema é como direcionar o cliente para o servidor novo e atual para partilhar a carga e garantir que a sessão do utilizador é mantida no primeiro servidor com sessão iniciada.



- A resposta é um balanceador de carga ou ADC.

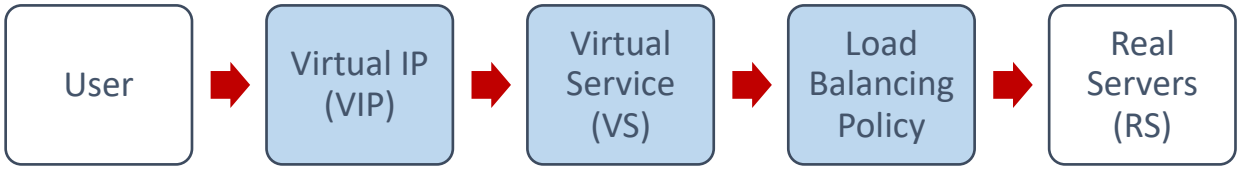
Agora a solução.

- Colocamos um ADC em frente aos dois servidores de aplicações.

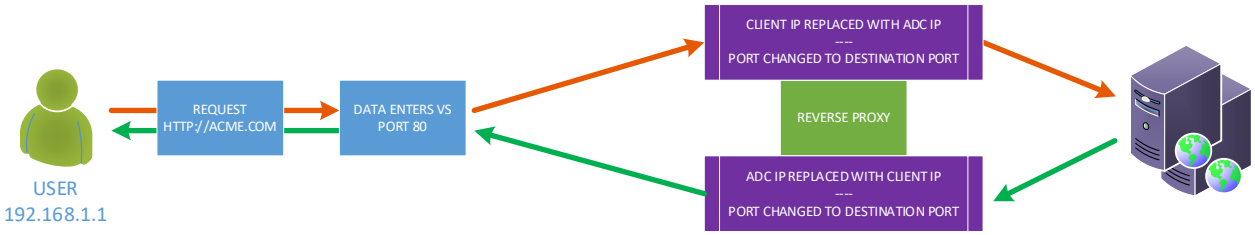


User Client **ADC** **Application Servers**

- O ADC terá um IP externo de 1.2.3.6 e a firewall redireccionará os pedidos para este endereço em vez do anterior 1.2.3.4
- O IP do ADC para receber os pedidos chama-se VIP e a configuração chama-se Virtual Service.
- O ADC recebe os pedidos dos utilizadores clientes e faz o proxy inverso para os servidores reais utilizando políticas de equilíbrio de carga, ao mesmo tempo que monitoriza a saúde dos servidores de aplicações para garantir a eficiência.



- O ADC equilibra o tráfego para os servidores com base na política de equilíbrio de carga em utilização, na natureza da carga e no estado dos servidores de aplicações.
- O tráfego dos servidores será enviado de volta para o cliente através do ADC na direção oposta.
- Devido à natureza do proxy invertido, o servidor e o cliente são anónimos um para o outro.



- A tecnologia de proxy invertido garante um nível ótimo de segurança.

Explicação dos VIPs e dos Serviços Virtuais (VS)

Um VIP é, em essência, um endereço IP definido para uso no EdgeADC e permite que os usuários acessem os serviços vinculados a ele. Isso é basicamente o que é um VIP. Devido à forma como o EdgeADC funciona, o VIP não precisa de estar na mesma sub-rede que os Real Servers, e esta metodologia de tradução de endereços de rede torna a tecnologia muito segura contra hackers que tentem aceder aos servidores internos.

Nota: O endereço IP do VIP não pode ser o mesmo que o endereço IP utilizado para o IP de gestão.

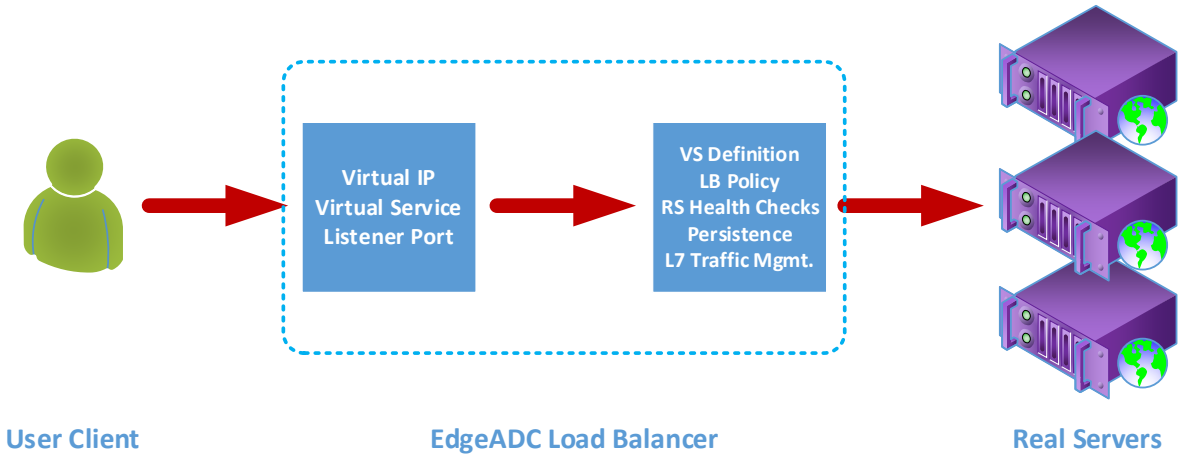
Os serviços virtuais constituem o núcleo das tecnologias de proxy e balanceamento de carga do EdgeADC. O Virtual IP é o endereço através do qual o VS é anunciado para a rede e para o mundo, escutando o tráfego e os pedidos dos clientes que desejam utilizar as aplicações que ele serve.

Quando os clientes chegam ao VS, este será configurado para executar várias acções no tráfego, incluindo, entre outras, as seguintes:

- Proxy da ligação do cliente
- São executadas funções específicas, como compressão, aceleração, equilíbrio de carga, inspeção de tráfego, etc.
- Encaminhar os pedidos do cliente para servidores de destino definidos no âmbito das políticas de equilíbrio de carga do serviço virtual.

Pode-se pensar no VS como casado com um endereço IP (VIP) que o EdgeADC está escutando para preparar as requisições de dados. Ao realizar configurações padrão de TCP ou HTTP, o cliente se conectará ao VIP e o EdgeADC processará a requisição de acordo com a definição que compõe o VS. Feito isso, o EdgeADC enviará o tráfego para os Real Servers especificados.

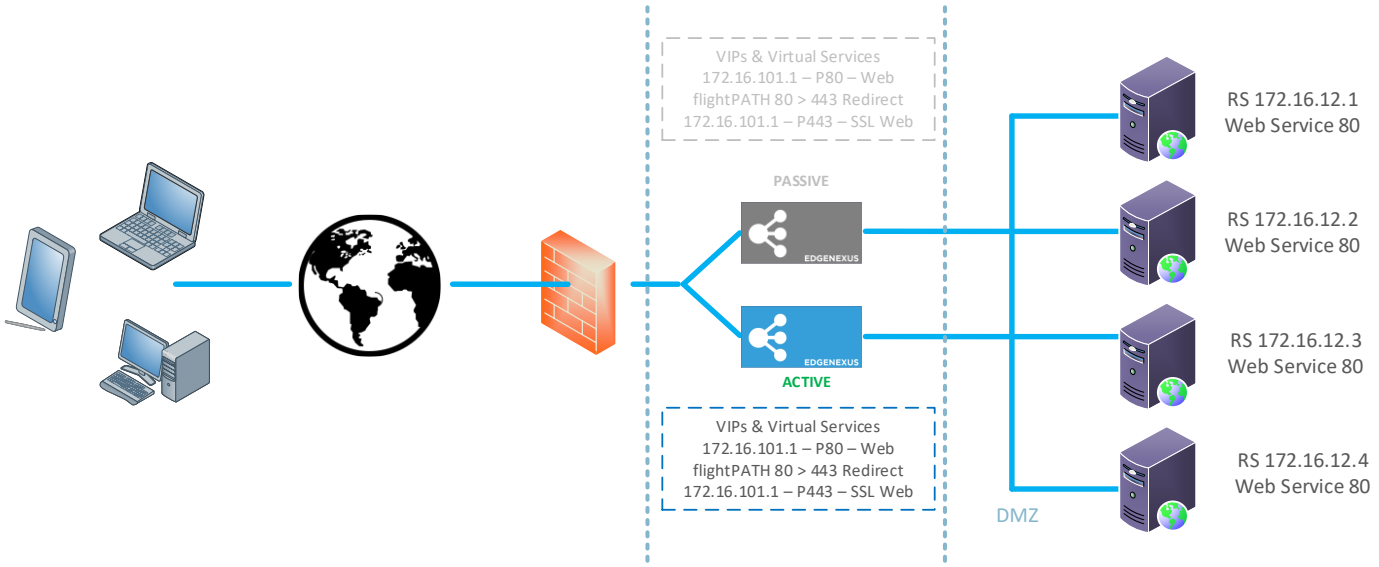
O VS recebe a conexão e os dados em uma configuração típica e, em seguida, termina ou faz proxy usando o mecanismo de proxy reverso dentro do EdgeADC. O EdgeADC então abre uma nova conexão com os Real Servers e envia os dados. Quando os Real Servers responderem à solicitação, o EdgeADC enviará a resposta ao cliente usando um caminho reverso semelhante, dependendo das configurações feitas na opção Connectivity da aba Real Servers Load Balancing.



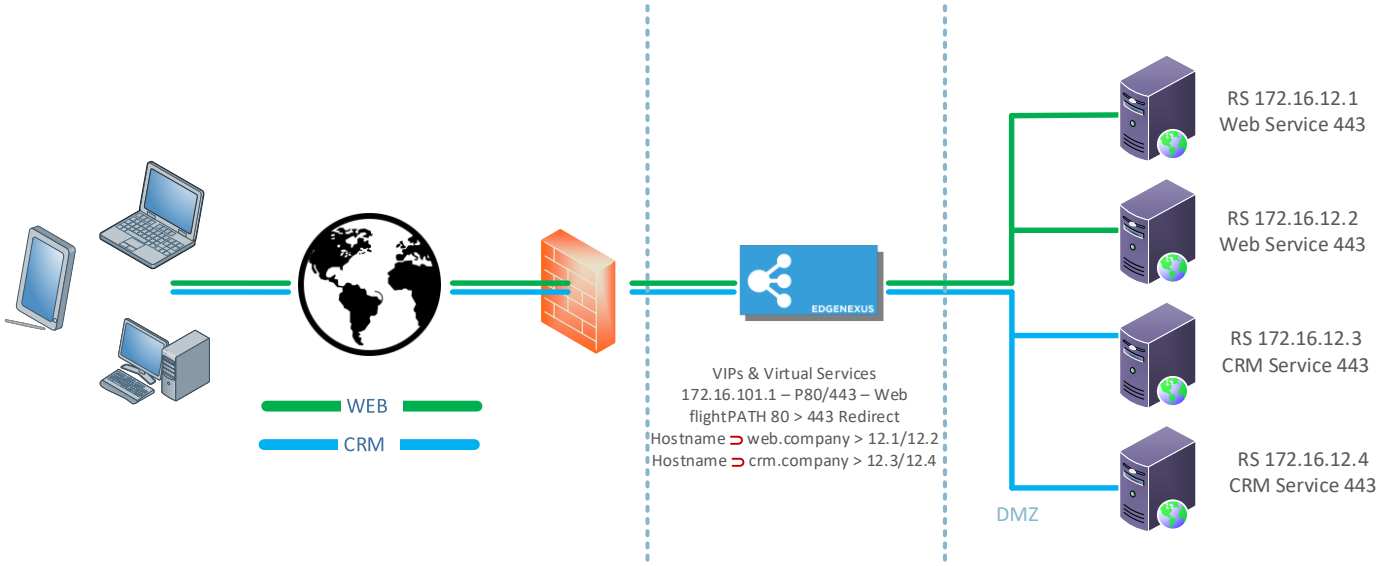
Uma definição de Serviço Virtual inclui um único endereço IP (VIP) e uma coleção de portas que servem como pontos de entrada para diferentes serviços, utilizando uma variedade de protocolos.

Por exemplo, é necessário equilibrar a carga de uma série de servidores Web para proporcionar resiliência. Agora vamos assumir que estes sistemas serão acedidos através de comunicações protegidas por HTTPS utilizando https://myweb.company.com.

Se olharmos para a definição de tal configuração, ela será composta por um único VIP com duas entradas, uma para a porta 80 e outra para a porta 443. O VIP da porta 80 terá uma regra flightPATH anexada que forçará a conversão do tráfego para HTTPS. A segunda entrada para a porta 443 enviará então o tráfego para os Servidores Reais definidos sob ela. Da mesma forma, pode ter outros serviços sob o mesmo VIP para equilibrar a carga do tráfego para servidores de correio eletrónico ou outros servidores de aplicações.



Com ADCs menos funcionais, os serviços que usam as mesmas portas precisariam de VIPs diferentes, mas o ADC e seu sistema flightPATH permitem que você use um único VIP com vários serviços que usam as mesmas portas. Assim, é possível ter duas aplicações, ambas acedidas através da porta 443 com nomes de anfitrião diferentes, utilizando um único VIP. Um exemplo é ilustrado abaixo.



Os sistemas EdgeADC são extremamente flexíveis e permitem a definição de configurações muito complexas e funcionais.

O que é um tipo de serviço de balanceamento de carga?

Os tipos de serviços de balanceamento de carga consistem em algoritmos e metodologias utilizados para distribuir de forma inteligente ou equilibrar a carga do tráfego entre grupos de servidores. O método e o algoritmo que o ADC disponibiliza dependerão do tipo de serviço ou da aplicação utilizada nos servidores que estão a ser objeto de balanceamento de carga, bem como do estado da rede e dos servidores em utilização. É de notar que o tipo de serviço de balanceamento de carga que seleciona utilizar também depende do nível de tráfego que está a ser enviado através do ADC. Assim, quando a taxa de transferência ou a carga de tráfego é baixa, os tipos de serviço de balanceamento de carga podem ser simples. Mas quando as cargas são maiores, pode ser necessário selecionar tipos mais complexos para obter uma distribuição de carga mais eficiente para os servidores back-end.

Os seguintes tipos de serviços de balanceamento de carga estão disponíveis no EdgeADC.

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

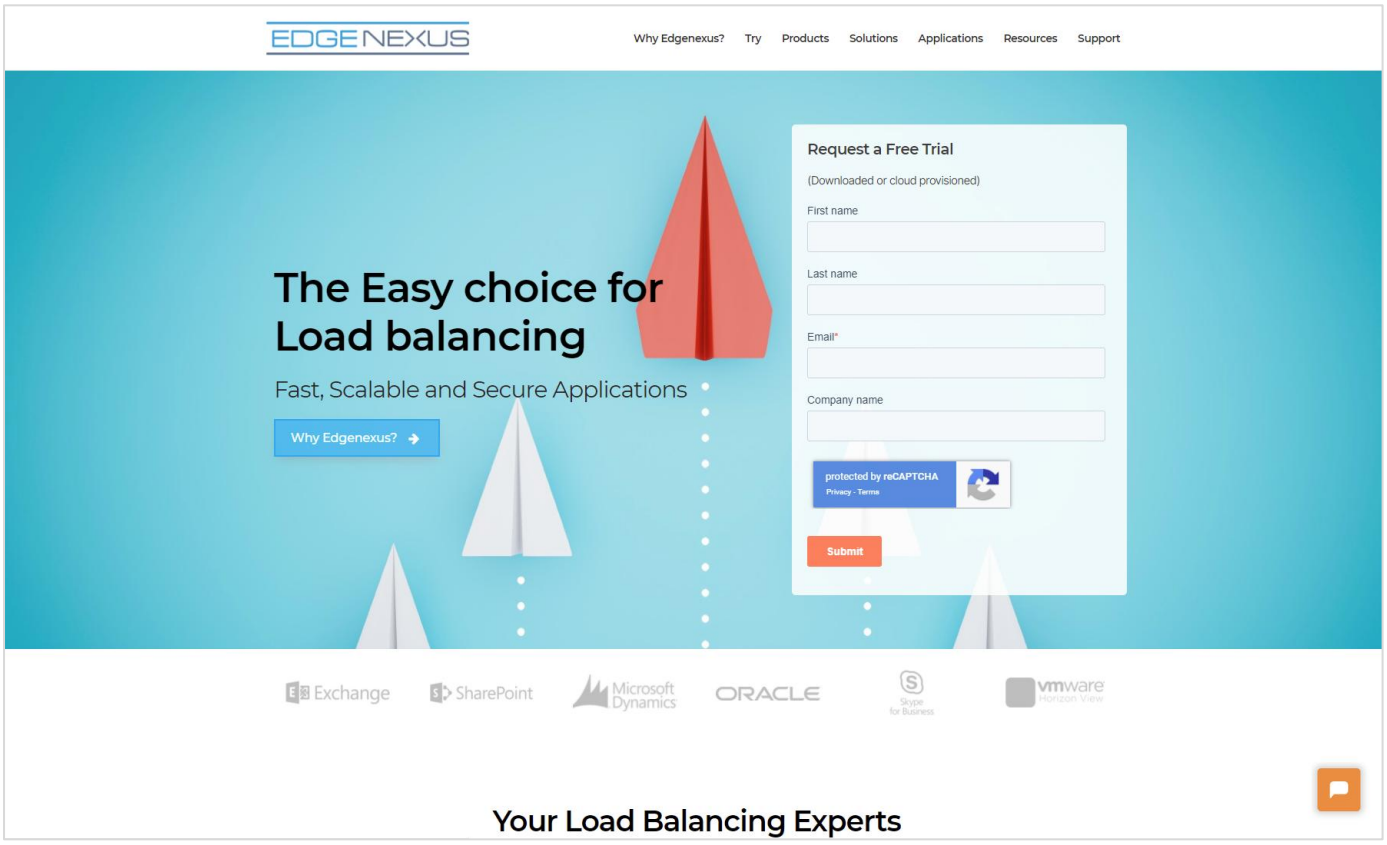
O início da viagem

Descarregamento do EdgeADC

Antes da instalação, o primeiro passo é fazer o download do EdgeADC adequado ao seu ambiente.

Fornecemos edições para a maioria dos ambientes virtualizados e uma edição ISO para instalação direta em hardware bare-metal.

A primeira etapa consiste em preencher o formulário de avaliação que se encontra no sítio Web Edgenexus, em https://www.edgenexus.io/products/load-balancer/free-trial/.



O processo é simples e, após preencher o formulário e submetê-lo, será encaminhado para a página de transferência, onde poderá selecionar a imagem correta para o seu ambiente.

As edições do EdgeADC estão disponíveis para os seguintes sistemas de virtualização:

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

Também pode optar por fazer um teste na Nuvem utilizando as edições do Microsoft Azure ou do Amazon AWS marketplace.

Se optar por descarregar o software para uma instalação no local, receberá o EdgeADC com uma licença de avaliação de 14 dias incorporada. Recomendamos que contactesales@edgenexus.io e solicite uma chave de licença de 30 dias com todas as funcionalidades activadas.

Instalação

Instalação do EdgeADC

O EdgeADC (ADC) está disponível para instalação em vários alvos de plataforma, cada um dos quais requer o seu instalador, que lhe é disponibilizado depois de se registar para descarregar.

Estes são os diferentes modelos de instalação disponíveis.

- VMware ESXi
- KVM
- Citrix Xen
- Nutanix AHV
- Microsoft Hyper-V
- Oracle VM
- Proxmox (Utilizar OVA)
- ISO para hardware BareMetal

O dimensionamento da máquina virtual que irá utilizar para alojar o ADC depende do cenário do caso de utilização e da taxa de transferência de dados.

Instalação no VMware ESXi

O ADC é suportado para instalação no VMware ESXi são 5.x e superior.

- Descarregue o pacote OVA de instalação mais recente do ADC utilizando a ligação adequada fornecida com o e-mail de descarregamento.
- Uma vez descarregado, descompacte-o num diretório adequado no seu anfitrião ESXi ou SAN.
- No cliente vSphere, selecione File: Deploy OVA/OVF Template.
- Procure e selecione o local onde guardou os seus ficheiros; escolha o ficheiro OVF e clique em **NEXT**
- O servidor ESX solicita o nome do dispositivo. Digite um nome adequado e clique em **NEXT**
- Selecione o datastore a partir do qual o dispositivo ADC será executado.
- Selecione um datastore com espaço suficiente e clique em **NEXT**
- Em seguida, ser-lhe-ão fornecidas informações sobre o produto; clique em **SEGUINTE**
- Clique em **SEGUINTE.**
- Depois de ter copiado os ficheiros para o armazenamento de dados, pode instalar a aplicação virtual.

Inicie o seu cliente vSphere para ver o novo dispositivo virtual ADC.

- Clique com o botão direito do rato no VA e vá para Power > Power-On
- O seu VA arrancará e o ecrã de arranque do ADC será apresentado na consola.

Instalar a interface VMXNET3

O controlador VMXnet3 é suportado, mas primeiro terá de efetuar alterações às definições da placa de rede.

***Nota** - NÃO actualize o VMware-tools*

Ativação da interface VMXNET3 num VA recentemente importado (nunca iniciado)

1. Eliminar ambas as NICs da VM
2. Atualizar o hardware da VM - -Clique com o botão direito do rato no VA na lista e selecione Upgrade Virtual Hardware (não inicie uma instalação ou atualização das ferramentas VMware, **apenas** execute a atualização do hardware)
3. Adicione duas placas de rede e selecione-as para serem VMXNET3
4. Inicie o VA utilizando o método padrão. Funcionará com o VMXNET3

Ativação da interface VMXNET3 num VA já em execução

1. Parar a VM (comando CLI shutdown ou GUI power-off)
2. Obtenha os endereços MAC de ambos os NICs (lembre-se da ordem dos NICs na lista!)
3. Eliminar ambas as NICs da VM
4. Atualizar o hardware da VM (não iniciar uma instalação ou atualização das ferramentas VMware, **apenas** efetuar a atualização do hardware)
5. Adicione duas NICs e selecione-as para serem VMXNET3
6. Defina os endereços MAC para os novos NICs de acordo com o passo 2
7. Reiniciar o VA

Suportamos o VMware ESXi como plataforma de produção. Para efeitos de avaliação, pode utilizar o VMware Workstation e o Player.

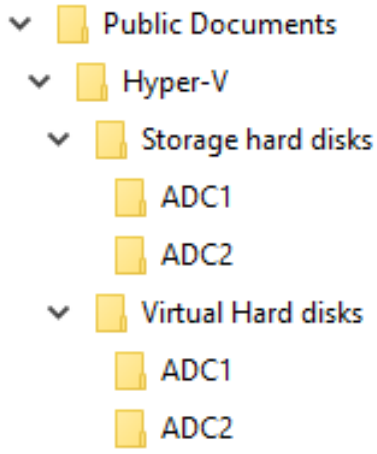
Para continuar, consulte a secção **CONFIGURAÇÃO DO PRIMEIRO ARRANQUE**.

Instalação no Microsoft Hyper-V

A aplicação Edgenexus ADC Virtual pode ser facilmente instalada numa estrutura de virtualização Microsoft Hyper-V. Este guia pressupõe que especificou e configurou corretamente o seu sistema Hyper-V e os recursos do sistema para acomodar o ADC e a sua arquitetura de equilíbrio de carga.

Nota: cada aparelho requer um endereço MAC único.

- Extraia o ficheiro ADC-VA compatível com Hyper-V transferido para o seu computador ou servidor local.
- Abrir o Gestor de Hyper-V.
- Crie uma nova pasta para conter o "Disco rígido virtual" do ADC VA e outra nova pasta para conter o "Disco rígido de armazenamento", por exemplo, C:\Users\Public\Documents\Hyper-V\Discos rígidos virtuais\ADC1 e C:\Users\Public\Documents\Hyper-V\Discos rígidos de armazenamento\ADC1
- **Observação**: Novas subpastas específicas do ADC para os discos rígidos virtuais\ e discos rígidos de armazenamento\ precisam ser criadas para cada instalação de instância do ADC virtual, conforme mostrado abaixo:



- Copie o arquivo .vhd extraído do EdgeADC para a pasta 'Storage hard disk' criada acima.
- No seu cliente Hyper-V Manager, clique com o botão direito do rato no servidor e selecione "Importar máquina virtual"
- Navegue até à pasta que contém o ficheiro de imagem ADC VA descarregado e extraído anteriormente
- Selecionar Máquina Virtual - selecione a máquina virtual a importar e clique em Seguinte
- Selecionar Máquina Virtual - selecione a máquina virtual a importar e clique em Seguinte
- Escolha Import Type - selecione "**Copy the virtual machine (create a new unique ID)**" clique em next
- Escolher Pastas para Ficheiros de Máquina Virtual - o Destino pode ser deixado como a predefinição do Hyper-V ou pode optar por selecionar uma localização diferente
- Localize Virtual Hard Disks (Discos rígidos virtuais) - procure e selecione a pasta de discos rígidos virtuais criada acima e clique em Next (Seguinte)
- Escolha Folders to Store Virtual Hard Disks (Pastas para armazenar discos rígidos virtuais) - procure e selecione a pasta Storage hard disks (Discos rígidos de armazenamento) criada anteriormente e clique em next (Seguinte)
- Verifique se os detalhes na janela Resumo do assistente de importação estão corretos e clique em Concluir
- Clique com o botão direito do rato na máquina virtual **ADC** recentemente importada e selecione Iniciar

NOTA: DE ACORDO COM HTTP://SUPPORT.MICROSOFT.COM/KB/2956569, DEVE IGNORAR A MENSAGEM DE ESTADO "DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)", QUE PODE SER APRESENTADA DA SEGUINTE FORMA DEPOIS DE O VA SER INICIADO. NÃO É NECESSÁRIA QUALQUER AÇÃO E O SERVIÇO NÃO ESTÁ DEGRADADO

- Enquanto a VM está a inicializar, pode clicar com o botão direito do rato na entrada da VM e selecionar Connect... Ser-lhe-á então apresentada a consola do EdgeADC.

- Depois de configurar as propriedades da rede, o VA será reiniciado e apresentará o início de sessão na consola do VA.

Para continuar, consulte a secção **CONFIGURAÇÃO DO PRIMEIRO ARRANQUE**.

Instalação no Citrix XenServer

O dispositivo ADC Virtual pode ser instalado no Citrix XenServer.

- Extraia o ficheiro ALB-VA do ADC OVA para o seu computador ou servidor local.
- Abra o cliente Citrix XenCenter.
- No seu cliente XenCenter, selecione **"Ficheiro: Importar".**
- Navegue até ao ficheiro **OVA**, selecione-o e clique em **"Abrir seguinte".**
- Selecione o local de criação da VM quando solicitado.
- Escolha o XenServer que pretende instalar e clique em **"NEXT" (Seguinte).**
- Selecione o repositório de armazenamento (SR) para a colocação do disco virtual quando solicitado.
- Selecione um SR com espaço suficiente e clique em **"NEXT" (Seguinte).**
- Mapeie suas interfaces de rede virtual. Ambas as interfaces dirão Eth0; no entanto, observe que a interface inferior é Eth1.
- Selecione a rede de destino para cada interface e clique em **SEGUINTE**
- **NÃO** assinale a opção "Utilizar a correção do sistema operativo".
- Clique em **"SEGUINTE"**
- Selecione a interface de rede a utilizar para a VM de transferência temporária.
- Escolha a interface de gestão, normalmente a rede 0, e deixe as definições de rede em DHCP. Tenha em atenção que tem de atribuir detalhes de endereços IP estáticos se não tiver um servidor DHCP a funcionar para a transferência. Se não o fizer, a importação dirá "A ligar continuamente" e depois "Falhou". Clique em **"NEXT" (Seguinte)**
- Reveja todas as informações e verifique as definições corretas. Clique em **"FINALIZAR".**
- A sua VM começará a transferir o disco virtual "ADC" e, uma vez concluída, será apresentada no seu XenServer.
- No seu cliente XenCenter, poderá agora ver a nova máquina virtual.
  Clique com o botão direito do rato na VA e clique em "**START**".
- A sua VM arrancará e o ecrã de arranque do ADC será apresentado.

- Uma vez configurado, apresenta-se o logon no VA.

Para continuar, consulte a secção **CONFIGURAÇÃO DO PRIMEIRO ARRANQUE**.

Instalando no KVM

A seção a seguir mostra como instalar o EdgeADC em uma plataforma KVM. A plataforma KVM utilizada para este exercício foi executada em um sistema operacional CentOS v8 com o Cockpit e a virtualização instalados.

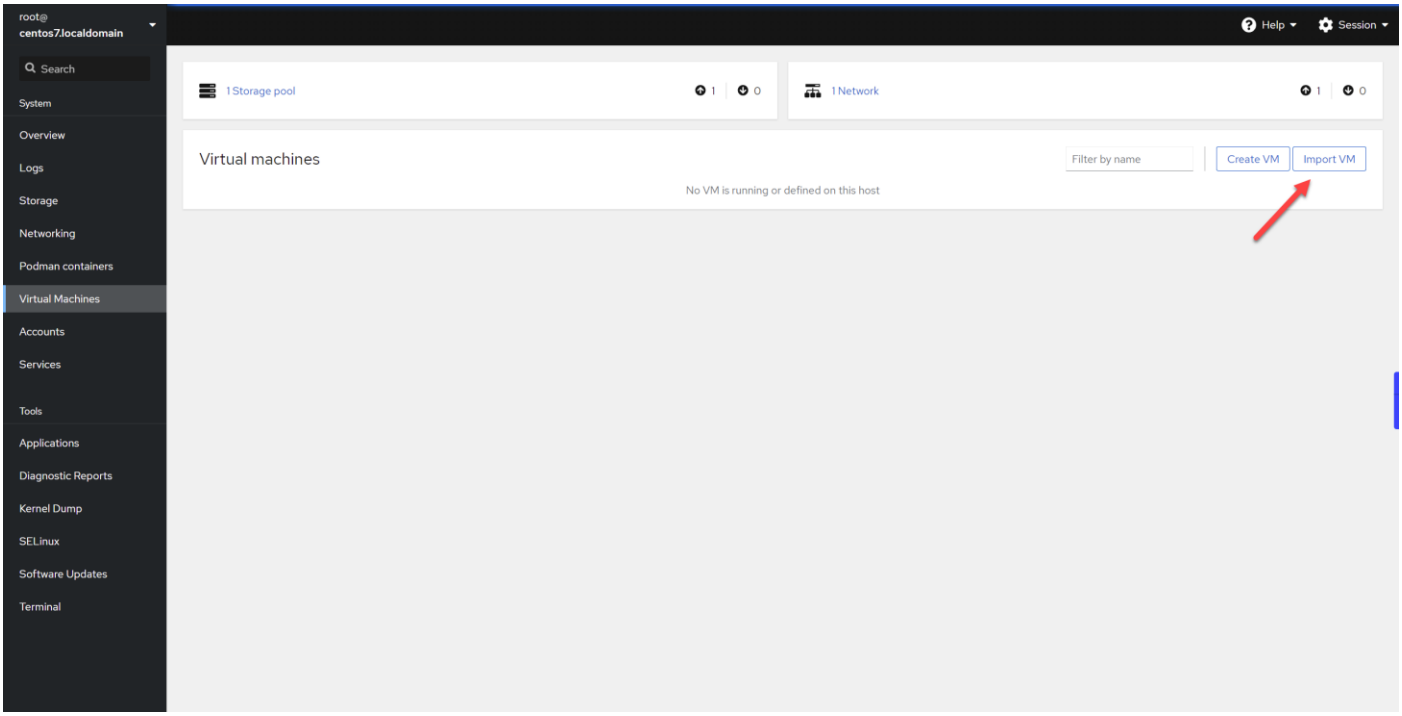
Requisitos e versões

Este guia é relevante para o EdgeADC 4.2.6 e superior.

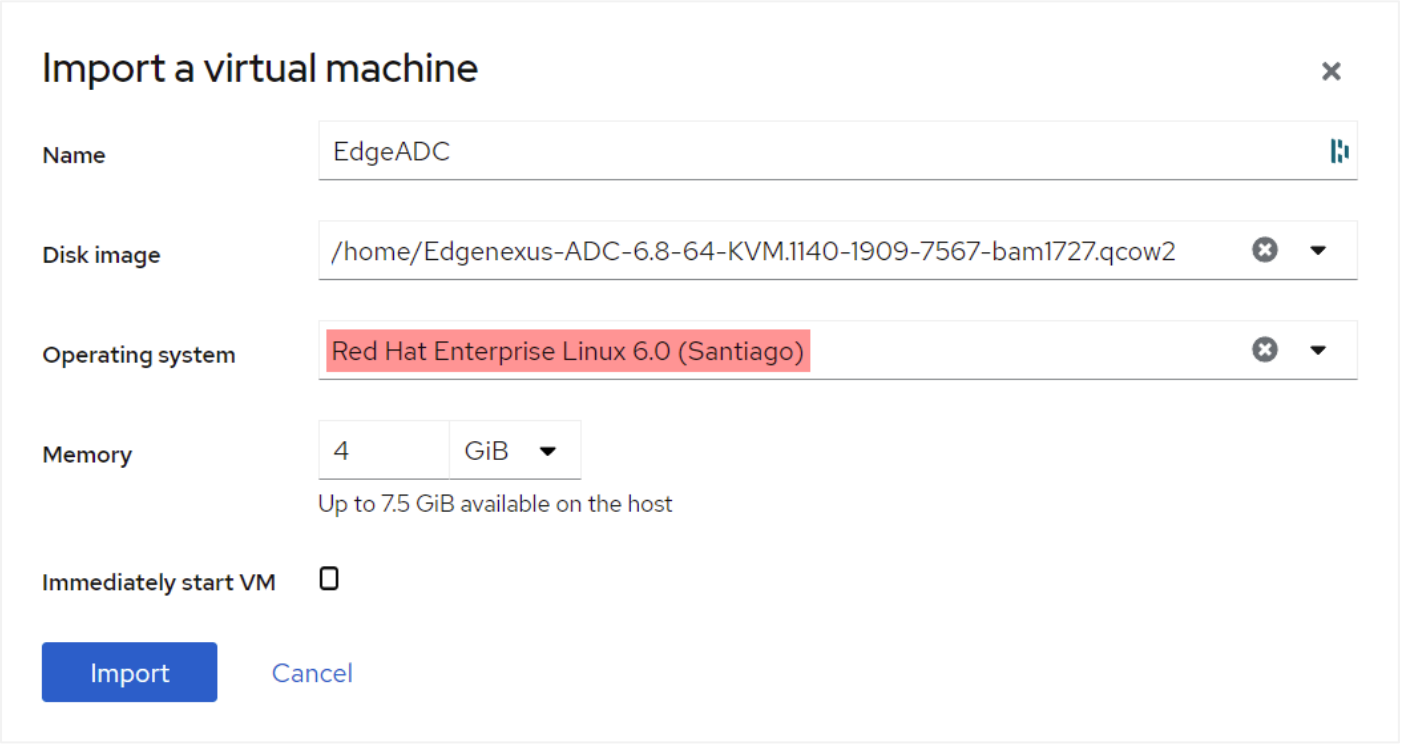
As orientações abaixo não abrangem a instalação do KVM ou a sua ligação em rede.

Assumimos que descarregou a aplicação virtual KVM e a armazenou no anfitrião numa localização acessível.

- O primeiro passo é entrar na consola do Cockpit.

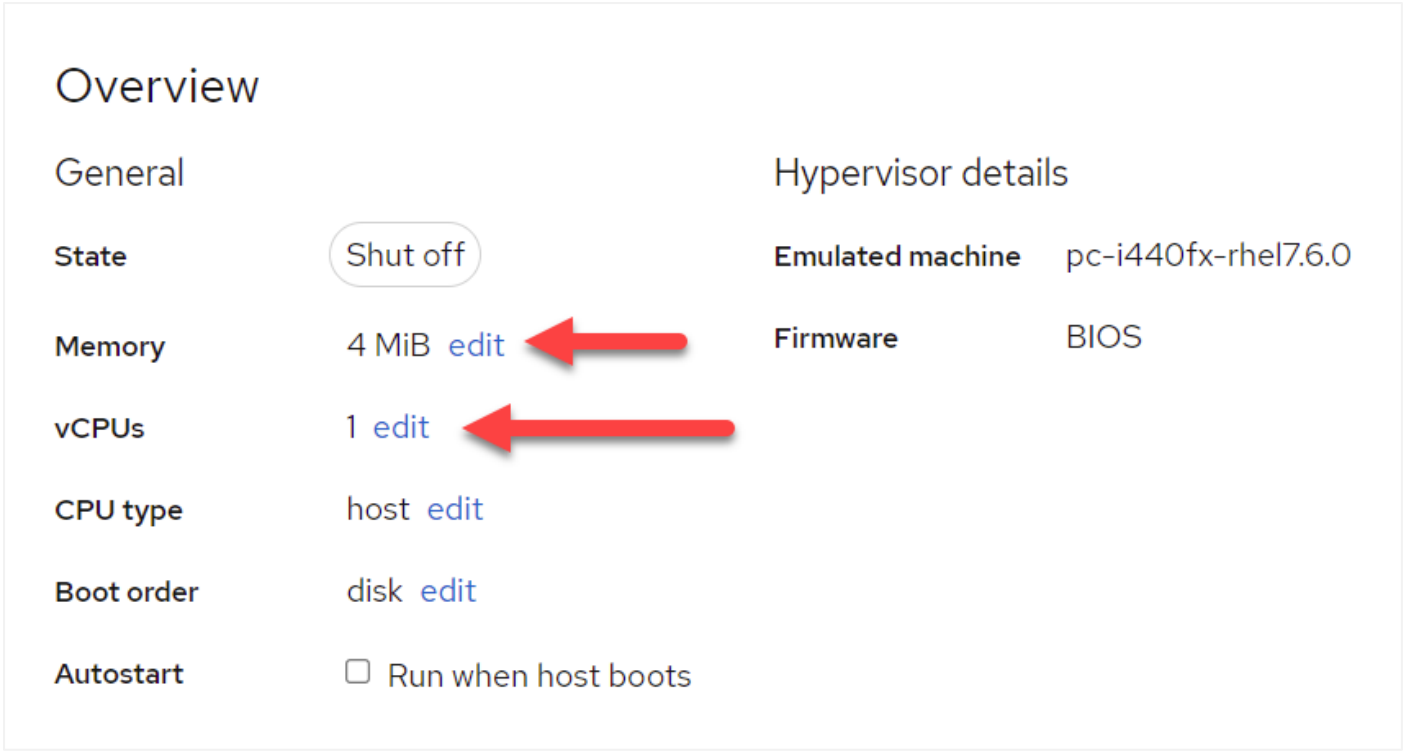


- Clique em Importar VM
- A primeira caixa de diálogo é onde terá de especificar os detalhes para a importação do aparelho virtual. Veja a imagem abaixo para ver o conteúdo dos campos. Você deve especificar o Red Hat Enterprise 6.0 como o sistema operacional.

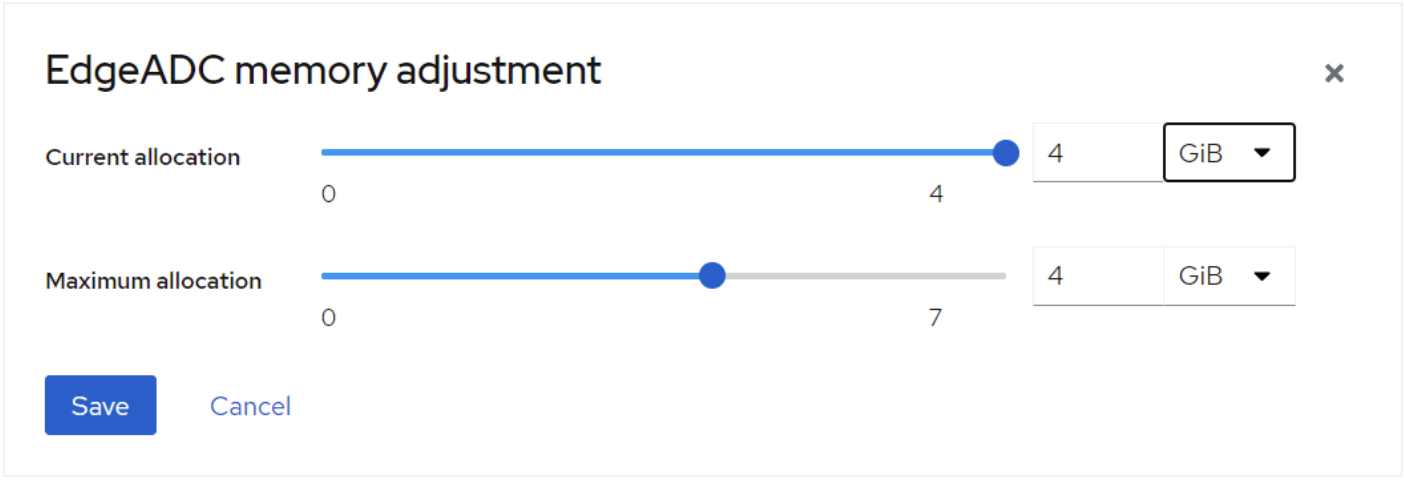


- Certifique-se de que tem a opção "Immediately Start VM" desmarcada.

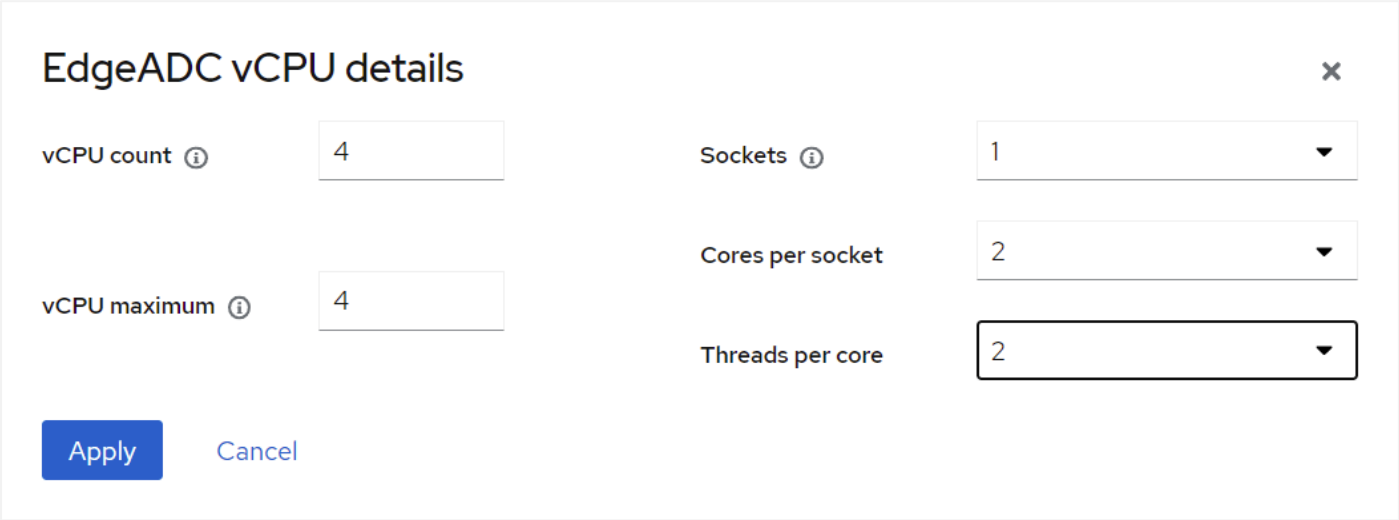
- Depois de preencher os dados, clique no botão Importar.
- A próxima etapa é especificar a vCPU e a alocação de memória que deseja usar.



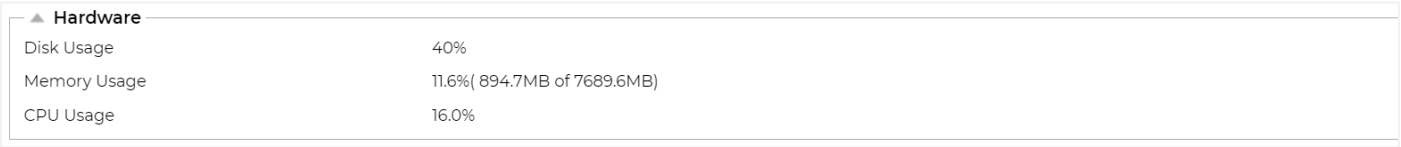
- Para atribuir a memória, verá uma caixa de diálogo semelhante à que se segue.



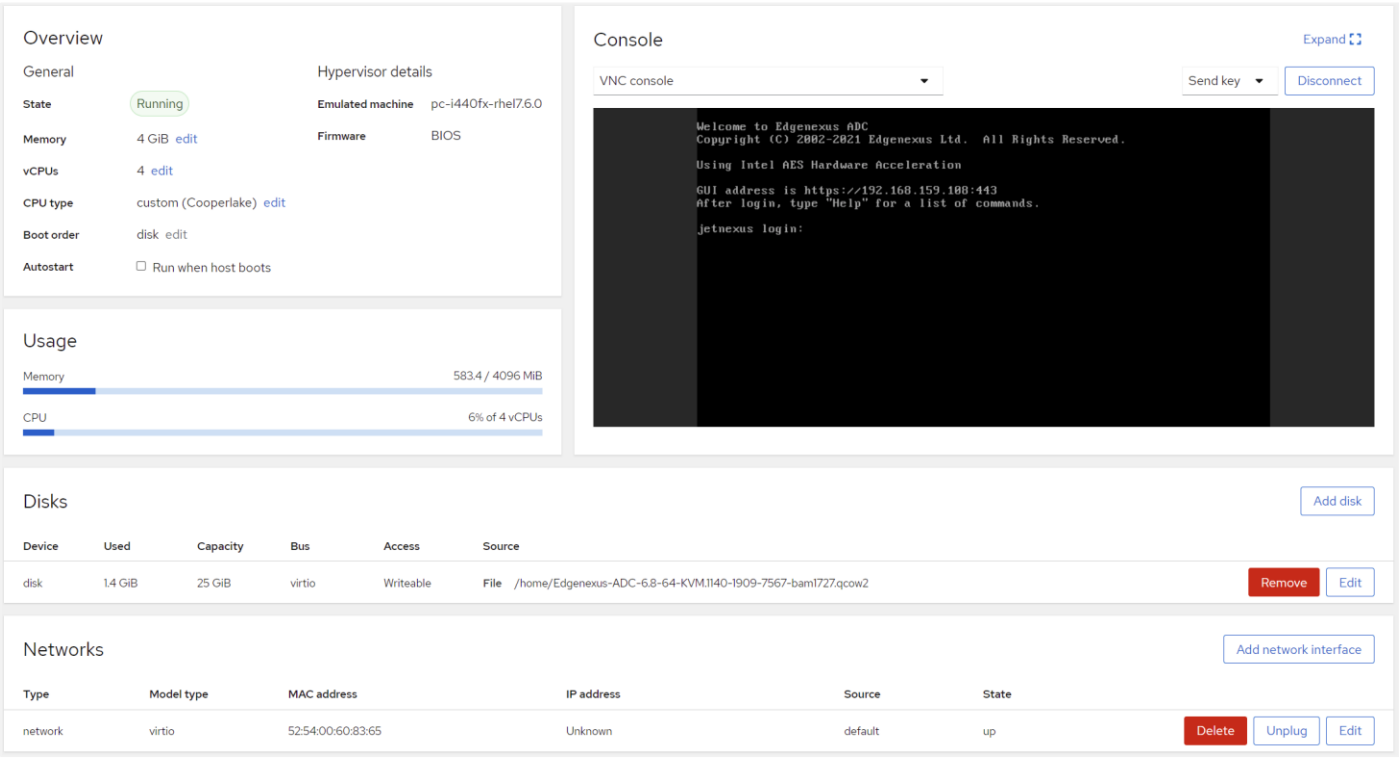
- Para atribuir a vCPU, verá uma caixa de diálogo semelhante à que se segue.



- As escolhas que fizemos são apenas exemplos, mas são viáveis, a não ser que esteja a utilizar uma taxa de transferência elevada com reencriptação SSL, caso em que terá de ajustar em conformidade utilizando a secção Hardware em View > Statistics (Ver > Estatísticas).



- Agora tem um ADC funcional instalado no KVM. Veja a imagem abaixo.



Instalando no Nutanix AHV

A seção a seguir mostra como instalar o EdgeADC em uma plataforma Nutanix AHV.

Requisitos e versões

Este guia é relevante para o EdgeADC 4.2.6 e superior.

Todas as versões do hipervisor Nutanix são compatíveis, mas a certificação foi efectuada na versão 5.10.9 da Nutanix.

- O primeiro passo é fazer login no Nutanix Prism Central.

Carregando a imagem do EdgeADC

- Navegue até Infraestrutura virtual > Imagens
- Clique no botão Adicionar imagem
- Selecione o ficheiro de imagem do EdgeADC que descarregou e clique no botão Abrir para carregar a imagem.
- Introduza um nome para a imagem no campo Descrição da imagem.
- Selecionar uma categoria adequada
- Selecione a imagem e clique na tecla de seta para a direita
- Selecione Todas as imagens e clique em Guardar.

Criar a VM

- Navegue até Infraestrutura virtual > VMs
- Clique no botão Criar VM
- Introduza um nome para a VM, o número de CPUs que pretende ter e o número de núcleos que pretende atribuir à VM.
- Em seguida, desloque-se para baixo na caixa de diálogo e introduza a quantidade de memória que pretende atribuir à VM. Pode começar com 4 GB e aumentá-la consoante a utilização.

Adicionar o disco

- Em seguida, clique na ligação Adicionar novo disco
- Selecione a opção Clone from Image Service (Clonar do serviço de imagens) no menu pendente Operation (Operação).
- Selecione a imagem EdgeADC que adicionou e clique no botão Add (Adicionar).
- Selecione o disco que será o disco de arranque.

Adicionar a placa de rede, a rede e a afinidade

- Em seguida, clique no botão Adicionar nova placa de rede. É necessário ter dois NICS.
- Selecione a Rede e clique no botão Adicionar
- Clique no botão Definir afinidade
- Selecione os hosts da Nutanix nos quais a VM tem permissão para ser executada e clique no botão Salvar.
- Verifique as definições que efectuou e clique no botão Guardar

Ligar a VM

- Na lista de VMs, clique no nome da VM que acabou de criar
- Clique no botão Ligar para a VM
- Quando a VM estiver ligada, clique no botão Iniciar consola

Configuração da rede do EdgeADC

- Siga as instruções na secção Primeiro ambiente de arranque.
- O EdgeADC está pronto para ser usado e você poderá acessar sua GUI usando seu navegador e o endereço IP de gerenciamento.

Instalar no ProxMox

A instalação no ProxMox é simples, mas requer alguns passos adicionais.

Utilizaremos a versão VMWare OVA da instalação. Este é um processo de várias etapas e requer conhecimento de comandos shell no ProxMox. No entanto, tornámos as instruções tão fáceis quanto possível de seguir. Vamos partir do princípio de que está familiarizado com o ProxMox e, por isso, não iremos aprofundar as funcionalidades do ProxMox.

Carregando o OVA para o ProxMox

Uma vez que estamos a utilizar uma versão OVA, teremos primeiro de carregar o OVA para o ProxMox.

- Iniciar sessão na consola do ProxMox
- Criar uma pasta chamada OVA_Import.
- Agora é necessário utilizar um cliente SFTP, como o WinSCP (Windows) ou o CyberDuck (Mac), para transferir o ficheiro OVA.
- Quando o ficheiro for transferido, será apresentado na pasta que criou.
- Digite o seguinte comando para extrair o conteúdo do ficheiro OVA.
- Tar xvf {filename}. Veja o exemplo abaixo.

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

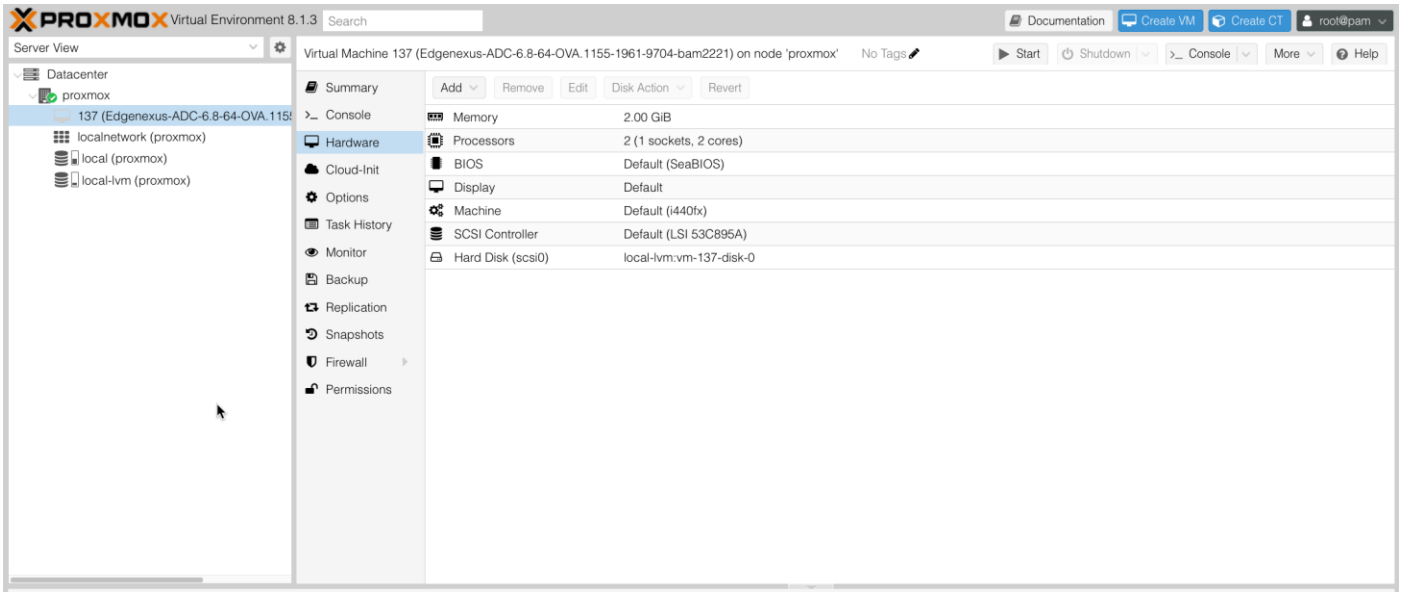
- Uma vez extraído, deverá ver algo como o exemplo abaixo.

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

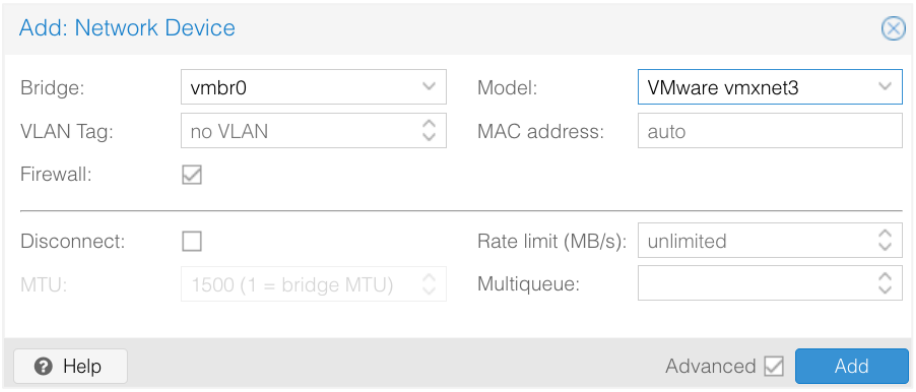
- Existem três ficheiros. Os ficheiros .ovf e .mf são a configuração. O .vmdk é o disco virtual que contém o ADC.
- O próximo passo é importar o VMDK para o ProxMox e criar a máquina virtual.
- Digite o seguinte comando para criar a máquina virtual utilizando os ficheiros de configuração.

```
qm importovf 137 ./{nome do ficheiro.ovf} local-lvm --format qcow2
```

- Neste exemplo, demos um ID de 100, mas isso pode ser diferente para a sua instalação se você já tiver máquinas virtuais criadas no ProxMox. Você pode determinar o próximo ID iniciando o processo de criação de VM no ProxMox ou escolhendo um número maior que 100 que esteja fora do alcance.
- A VM foi criada.



- O próximo passo é adicionar uma interface de rede à VM.
- Clique em Hardware no painel direito.
- Clique em Adicionar e escolha uma interface de rede.



- Configure-o como mostra a imagem acima. É importante escolher o modelo como VMware vmxnet3.
- Clique em Adicionar depois de configurado.
- Pode acrescentar adaptadores de rede adicionais consoante as suas necessidades.
- Agora pode iniciar a VM e continuar a utilizar as instruções no capítulo Configuração do Primeiro Arranque.

Configuração do primeiro arranque

No primeiro arranque, o ADC (também referido como VA abaixo) apresenta o seguinte ecrã a solicitar a configuração para operações de produção.

Primeiro arranque - Detalhes manuais da rede

No primeiro arranque, dispõe de 10 segundos para interromper a atribuição automática de detalhes de IP através de DHCP.

Para interromper este processo, clique na janela da consola e prima qualquer tecla. Pode então introduzir os seguintes detalhes manualmente.

- Endereço IP
- Máscara de sub-rede
- Porta de entrada
- Servidor DNS

Estas alterações são persistentes e sobreviverão a uma reinicialização e não precisam de ser configuradas novamente no VA.

Primeiro arranque - DHCP bem sucedido

Se não interromper o processo de atribuição da rede, o seu terminal entrará em contacto com um servidor DHCP após um tempo limite para obter os dados da sua rede. Se o contacto for bem sucedido, serão atribuídas ao seu terminal as informações seguintes.

- Endereço IP
- Máscara de sub-rede
- Gateway predefinido
- Servidor DNS

Aconselhamos a utilizar o ADC com um endereço DHCP apenas se esse endereço IP estiver permanentemente ligado ao endereço MAC do ADC no servidor DHCP. Aconselhamos sempre a utilização de um **ENDEREÇO IP FIXO** quando utilizar os aparelhos virtuais. Siga os passos em **ALTERAR O ENDEREÇO IP DE GESTÃO** e as secções subsequentes até concluir a configuração da rede.

Primeira inicialização - Falha no DHCP

Se não tiver um servidor DHCP ou se a ligação falhar, será atribuído o endereço IP 192.168.100.100.
O endereço IP será incrementado em '1' até que o VA encontre um endereço IP livre. Da mesma forma, o VA verificará se o endereço IP está a ser utilizado e, em caso afirmativo, aumentará novamente e voltará a verificar.

Alterar o endereço IP de gestão

Pode alterar o endereço IP do VA em qualquer altura, utilizando o comando **set greenside=n.n.n.n,** como se mostra abaixo.

```
set greenside={endereço IP}
```

Alterar a máscara de sub-rede para eth0

As interfaces de rede utilizam o prefixo "eth"; o endereço de rede de base é designado por eth0. A máscara de sub-rede ou máscara de rede pode ser alterada usando o comando **set mask [NIC] [MASK]**. Pode ver um exemplo abaixo.

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

Atribuição de um gateway predefinido

O VA necessita de um gateway predefinido para as suas operações. Para definir o gateway predefinido, utilize o comando **route add default gw [GATEWAY IP]**, como mostra o exemplo abaixo.

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

Verificar o valor do Default Gateway

Para verificar se o gateway predefinido foi adicionado e está correto, utilize o comando **route**. Esse comando exibirá as rotas de rede e o valor do gateway padrão. Veja o exemplo abaixo.

```
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
```

Pode agora aceder à Interface Gráfica do Utilizador (GUI) para configurar o ADC para utilização em produção ou avaliação.

Aceder à interface Web

É possível usar qualquer navegador da Internet com JavaScript para configurar, monitorar e implantar o ADC em uso operacional.

No campo URL do navegador, digite **HTTPS://{ENDEREÇO IP} ou HTTPS://{FQDN}**

O ADC, por defeito, utiliza um certificado SSL auto-assinado. Pode alterar o ADC para utilizar o certificado SSL da sua escolha.

Quando o browser chegar ao ADC, ser-lhe-á apresentado o ecrã de início de sessão. As credenciais predefinidas de fábrica para o ADC são:

Username: admin / Pwd: jetnexus

Tabela de referência de comandos

Comando	Parâmetro1	Parâmetro2	Descrição	Exemplo
data			Mostra a data e a hora configuradas atualmente	Terça-feira 3 de setembro 13:00 UTC 2013
predefinições			Atribuir as predefinições de fábrica ao seu aparelho	
saída			Sair da interface da linha de comandos	
ajuda			Apresenta todos os comandos válidos	
ifconfig	[em branco]		Ver a configuração da interface para todas as interfaces	ifconfig
	eth0		Ver a configuração da interface apenas de eth0	ifconfig eth0
ID da máquina			Este comando fornecerá o machineid utilizado para licenciar o ADC ADC	EF4-3A35-F79
desistir			Sair da interface da linha de comandos	
reiniciar			Terminar todas as ligações e reiniciar o ADC ADC	reiniciar
reiniciar			Reiniciar os serviços virtuais do ADC ADC	
percurso	[em branco]		Ver a tabela de encaminhamento	percurso
	adicionar	gw por defeito	Adicionar o endereço IP do gateway predefinido	route add default gw 192.168.100.254
definir	margem verde		Definir o endereço IP de gestão para o ADC	set greenside=192.168.101.1
	máscara		Define a máscara de sub-rede para uma interface. Os nomes das interfaces são eth0, eth1....	set mask eth0 255.255.255.0
espetáculo			Apresenta as definições de configuração global	
encerramento			Terminar todas as ligações e desligar o ADC ADC	
estatuto			Apresenta as estatísticas de dados actuais	
topo			Ver as informações do processo, como CPU e memória	
registo de visualização	mensagens		Apresenta as mensagens syslog em bruto	Ver mensagens de registo

Nota: Os comandos não são sensíveis a maiúsculas e minúsculas. Não existe um histórico de comandos.

A Consola Web

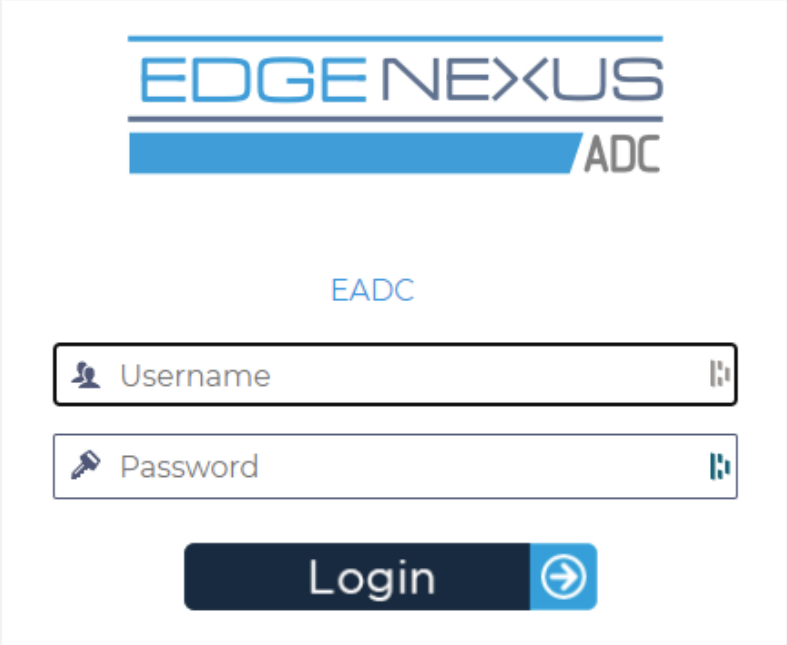
Iniciar a consola Web do ADC

Todas as operações no ADC são configuradas e executadas utilizando a consola Web. A consola Web é acedida através de qualquer navegador com JavaScript.

Para iniciar a consola Web do ADC, introduza o URL ou o endereço IP do ADC no campo URL. Usaremos o exemplo de adc.company.com como exemplo:

https://adc.company.com

Quando iniciada, a consola Web do ADC apresenta-se como indicado abaixo, permitindo-lhe iniciar sessão como utilizador administrador.



Credenciais de início de sessão predefinidas

As credenciais de início de sessão predefinidas são:

Username: admin / Pwd: jetnexus

Pode alterá-lo em qualquer altura utilizando a configuração do utilizador localizada em *Sistema* > *Utilizadores*.

Uma vez iniciada a sessão, é apresentado no ecrã o painel de controlo principal do ADC.

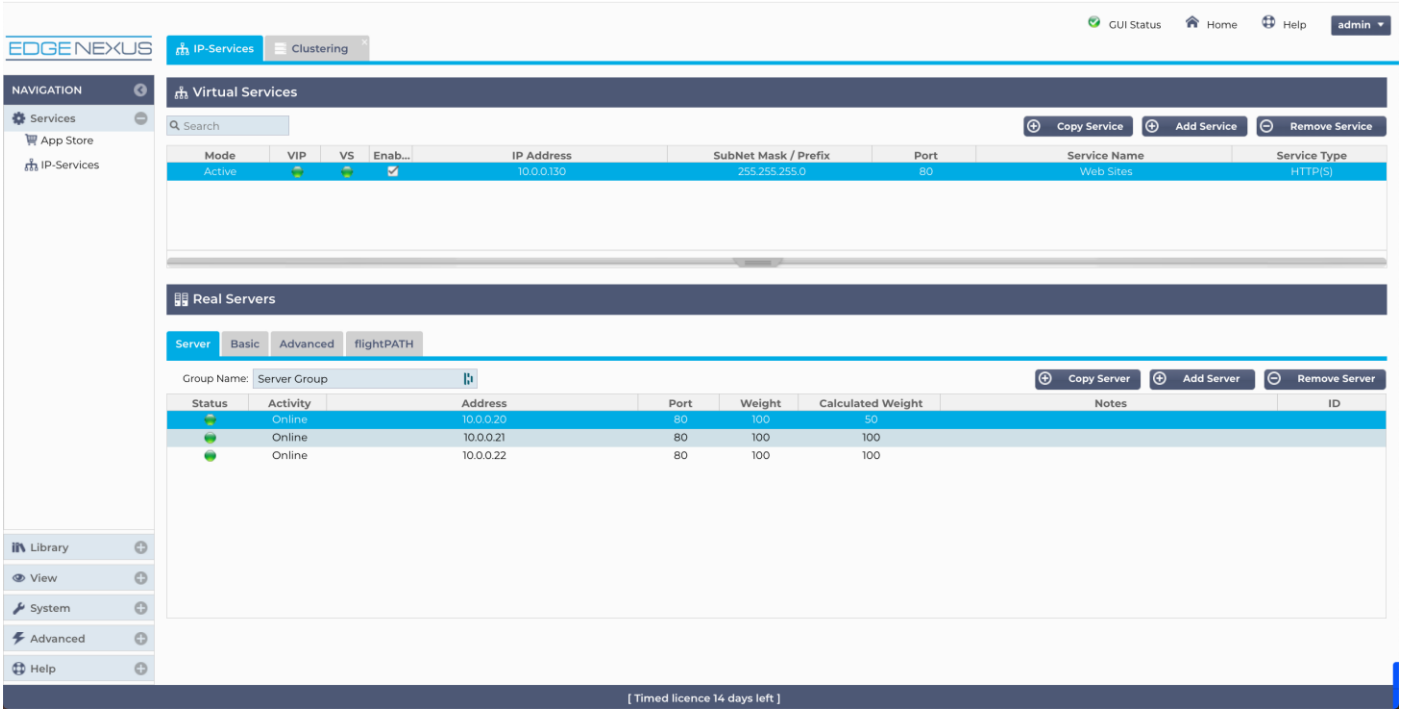
Utilizar um serviço de autenticação externo

Se pretender utilizar um serviço de autenticação externo, pode fazê-lo configurando um servidor de autenticação e um serviço de autenticação.

Para mais informações sobre este assunto, consultarAutenticação eServiço de autenticação

O painel de controlo principal

A imagem abaixo ilustra o aspeto do painel de controlo principal ou "página inicial" da ADC. Podemos ocasionalmente efetuar algumas alterações para melhorar, mas todas as funções serão mantidas.



A secção Navegação, do lado esquerdo, permite navegar pelas várias áreas das funcionalidades dos ADCs. Por defeito, seleciona-se a secção Serviços e abre-se a subsecção Serviços IP, indicada pelo separador situado por cima da secção Serviços Virtuais. Este separador é fixo e está sempre visível.

Quando clica numa secção da Navegação, essa secção é expandida e o seu conteúdo é revelado. Clicar numa opção dentro de uma secção abre o conteúdo da secção no lado direito e é colocado um separador no topo, permitindo uma mudança rápida.

As diferentes secções de navegação são explicadas em pormenor nos capítulos seguintes.

Serviços

Serviços IP

A secção Serviços IP do ADC permite-lhe adicionar, eliminar e configurar os vários serviços IP virtuais de que necessita para o seu caso de utilização específico. As definições e opções são apresentadas nas secções abaixo. Estas secções encontram-se no lado direito do ecrã da aplicação.

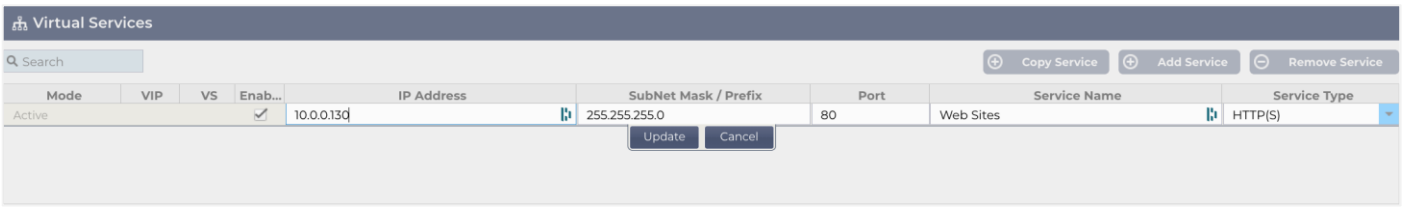
Serviços virtuais

Um Serviço Virtual combina um IP Virtual, ou VIP, e uma porta TCP/UDP na qual o ADC escuta. O tráfego que chega ao IP Virtual é redireccionado para um dos Servidores Reais associados a esse serviço. O endereço IP virtual não pode ser o mesmo que o endereço de gestão do ADC, ou seja, eth0, eth1, etc...

O ADC determina como o tráfego é redistribuído pelos Servidores com base numa política de balanceamento de carga definida no separador Basic (Básico) na secção Real Servers (Servidores reais).

Criar um novo Serviço Virtual utilizando um novo VIP

- Clique no botão Adicionar serviço virtual, como indicado acima.



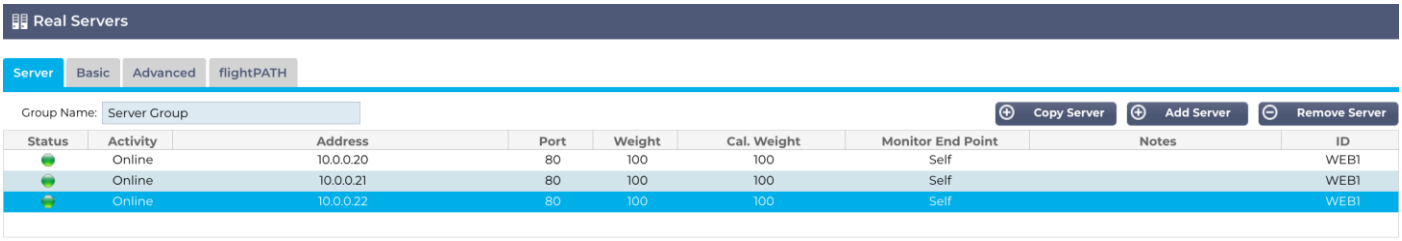
Em seguida, entrará no modo **de edição de linha.**

- Preencha os quatro campos destacados para prosseguir e, em seguida, clique no botão de atualização.

Utilize a tecla TAB para navegar pelos campos.

Campo	Descrição
Endereço IP	Introduza um novo endereço IP virtual para ser o ponto de entrada de destino para aceder ao Servidor Real. Este IP é o ponto para onde os utilizadores ou aplicações irão apontar para aceder à aplicação com equilíbrio de carga.
Máscara de sub-rede/Prefixo	Este campo destina-se à máscara de sub-rede relevante para a rede em que o ADC se encontra
Porto	A porta de entrada utilizada para aceder ao VIP. Este valor não tem necessariamente de ser o mesmo que o Servidor Real se estiver a utilizar o Proxy Reverso.
Nome do serviço	O nome do serviço é uma representação textual do objetivo do VIP. É opcional, mas recomendamos que o forneça para maior clareza. Note que este campo é utilizado para outros fins específicos quando se utiliza GSLB.
Tipo de serviço	Existem muitos tipos de serviços diferentes disponíveis para selecionar. Os tipos de serviço da camada 4 não podem utilizar a tecnologia flightPATH.

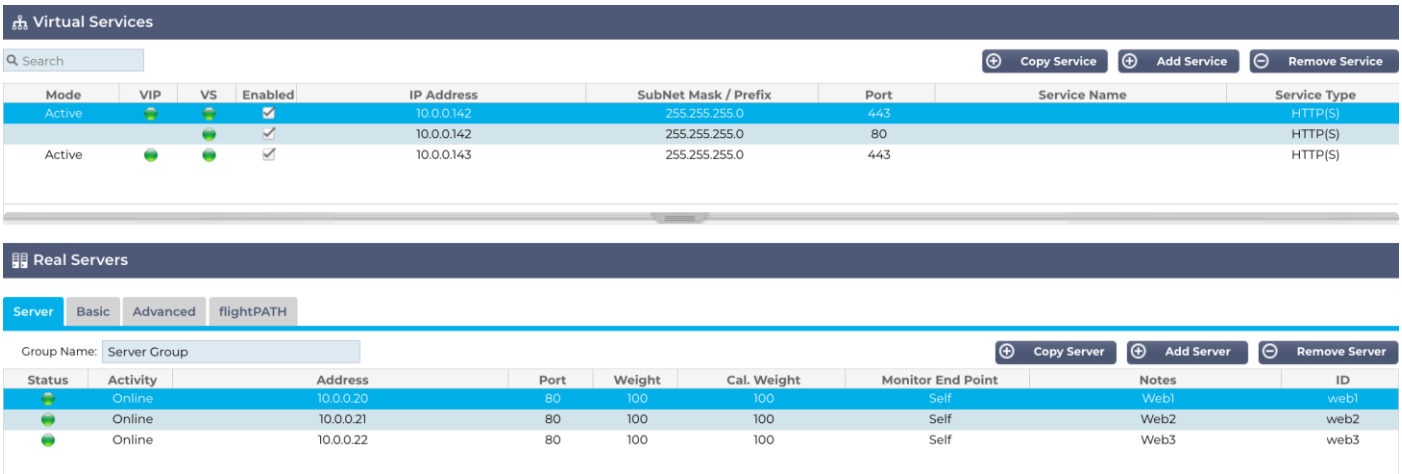
Pode agora premir o botão Update (Atualizar) para guardar esta secção e saltar automaticamente para a secção Real Server (Servidor real), detalhada abaixo:



Campo	Descrição
Atividade	O campo Activity (Atividade) pode ser utilizado para mostrar e alterar o estado do servidor real com balanceamento de carga. Online - Indica que o servidor está ativo e a receber pedidos com balanceamento de carga. Offline - O servidor está offline e não está a receber pedidos. Drenagem - O servidor foi colocado em modo de drenagem para que a persistência possa ser descarregada e o servidor movido para um estado offline sem afetar os utilizadores. Em espera - O servidor foi colocado em estado de espera
Endereço IP	Este valor é o endereço IP do Servidor Real. Tem de ser exato e não deve ser um endereço DHCP.
Porto	A Porta de destino do acesso no Servidor Real. Ao usar um proxy reverso, isso pode ser diferente da porta de entrada especificada no VIP.
Ponderação	Normalmente, esta definição é configurada automaticamente pelo ADC. Pode alterá-la se pretender alterar a ponderação da prioridade.
Cal. Peso	Se deixar a Ponderação no seu valor predefinido, o ADC calculará automaticamente a ponderação com base nos tempos de resposta.
Monitorizar o ponto final	O valor predefinido para esta opção é "Self". No entanto, pode alterá-lo para um valor de Porta ou um Endereço IP:Porta. O campo é utilizado para monitorizar um ponto final diferente e determinar se o tráfego deve ser passado para o Serviço Virtual. ConsulteComo utilizar o Monitor End Point abaixo.

- Clique no botão Atualizar ou prima Enter para guardar as suas alterações
- A luz de estado começa por ficar cinzenta, seguida de verde se a verificação do estado do servidor for bem sucedida. Ficará vermelha se o Monitor de Servidor Real falhar.
- Um servidor que tenha uma luz de estado vermelha não será balanceado em termos de carga.

Exemplo de um serviço virtual concluído

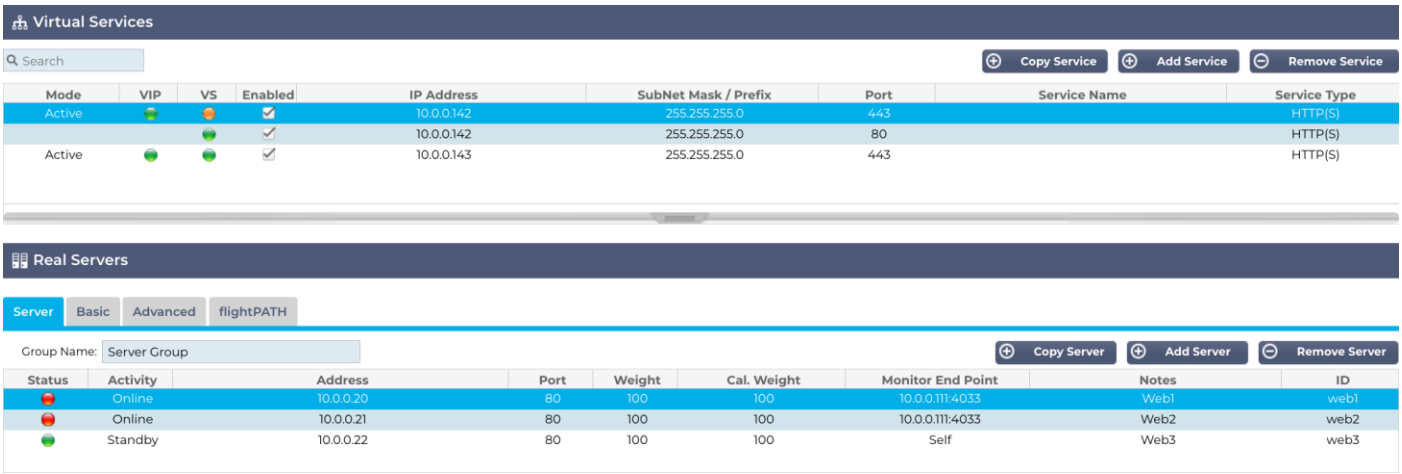


Como utilizar o Monitor End Point

Exemplo 1

Vejamos o exemplo de uma infraestrutura que inclui dois servidores Web de carga equilibrada que fornecem uma aplicação Web ao utilizador final. A aplicação Web está ligada a um servidor de base de dados no back end. O acesso ao servidor de base de dados é interrompido, mas os servidores da aplicação Web permanecem em funcionamento. Os utilizadores tentarão utilizar a aplicação Web e receberão erros.

A solução é utilizar o Monitor End Point.



- O exemplo mostra dois servidores Web, 10.0.0.20 e 10.0.0.21, juntamente com um terceiro servidor Web 10.0.0.22. O servidor 10.0.0.22 foi colocado em modo de espera.
- Os dois servidores Web activos foram configurados com um valor de ponto final de monitorização de 10.0.0.111:4033, que é o endereço IP e a porta de ligação do servidor da base de dados.
- No caso de a ligação do servidor da base de dados cair, os dois servidores activos serão colocados em modo offline e o servidor em espera ficará online, apresentando uma página Web que pode informar o cliente de que os sistemas estão em manutenção.

Exemplo 2

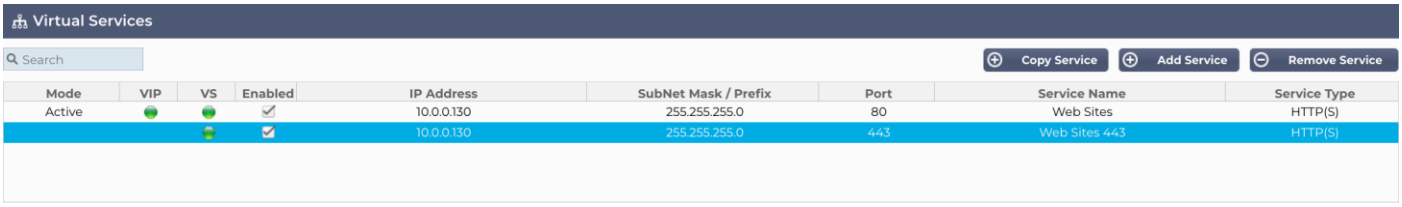
Outro exemplo para o uso do Monitor End Point é quando você está balanceando a carga de servidores de protocolo UDP, como o Always-On-VPN. Como deve saber, as portas UDP não são monitorizadas de forma fiável, pelo que surge a necessidade de monitorizar uma porta TCP.

A utilização do Monitor End Point permite-nos fazer exatamente isso. A porta principal que está a ser utilizada pelos servidores Always-on-VPN será 53/udp, mas irá monitorizar, digamos, 8433/tcp. Nesse caso, só precisa de introduzir o valor da porta no campo Monitor End Point (Ponto final do monitor).

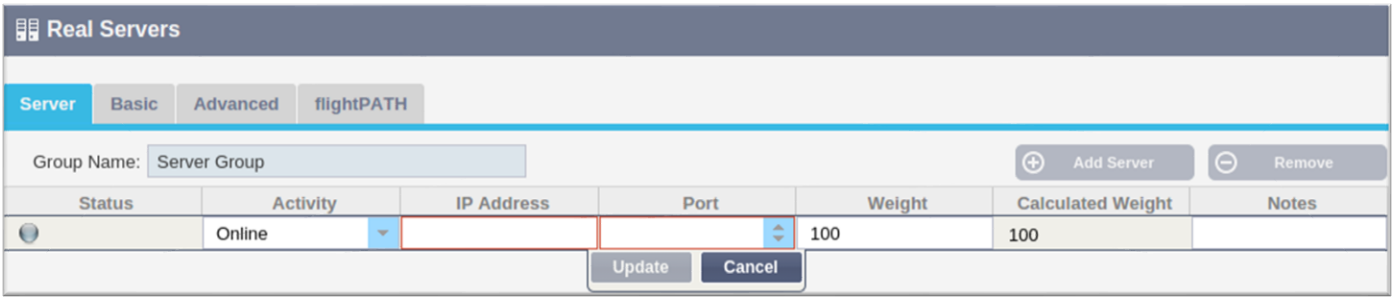
Criar serviços sub virtuais

Também é possível ter serviços subvirtuais nos casos em que é necessário fazer o balanceamento de carga usando portas diferentes no mesmo VIP. Por exemplo, pode ter servidores a serem acedidos utilizando o mesmo IP virtual nas portas 80, 8088 e 443, pelo que terá de criar serviços sub-virtuais para acomodar esta situação.

- Selecione um serviço virtual que pretenda copiar.
- Clique em Adicionar serviço virtual para entrar no modo de edição de linha.



- O endereço IP e a máscara de sub-rede são copiados automaticamente.
- Introduza o número de porta do seu serviço.
- Introduzir um nome de serviço opcional
- Selecionar um tipo de serviço.
- Pode agora premir o botão Atualizar para guardar esta secção e saltar automaticamente para a secção Servidor real abaixo

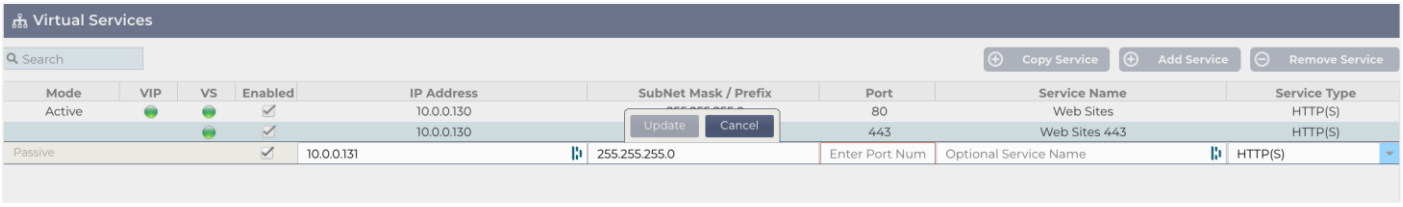


- Deixe a opção Activity (Atividade) do servidor como Online - isto significa que será equilibrada a carga se passar o monitor de saúde predefinido do TCP Connect. Esta definição pode ser alterada mais tarde, se necessário.
- Introduzir um endereço IP para o Servidor Real
- Introduzir um número de porta para o servidor real
- Introduza um nome opcional para o Real Server no campo Notes. Lembre-se que este campo de notas é usado para outros fins específicos, como em variáveis flightPATH, etc.
- Clique em Atualizar para guardar as alterações.
- A luz de estado fica primeiro cinzenta e depois verde se o Monitor de Servidor Real for bem sucedido. Passa a vermelho se o Monitor de Servidor Real falhar.
- Um servidor que tenha uma luz de estado vermelha não será objeto de equilíbrio de carga.

Alterar o endereço IP de um serviço virtual

Pode alterar o endereço IP de um Serviço Virtual ou VIP existente em qualquer altura.

- Realce o serviço virtual cujo endereço IP pretende alterar.
- Clique no campo do endereço IP para esse serviço, para o mudar para um estado editável.



- Altere o endereço IP para o que pretende utilizar
- Clique no botão Atualizar para guardar as alterações.

Nota: A alteração do endereço IP de um Serviço Virtual irá alterar o endereço IP de todos os serviços associados ao VIP

Criar um novo serviço virtual utilizando o serviço de cópia

- O botão Copy Service copia um serviço completo, incluindo todos os Real Servers, definições básicas, definições avançadas e regras flightPATH associadas ao mesmo
- Selecione o serviço que pretende duplicar e clique em Copiar serviço
- O editor de linhas aparecerá com o cursor a piscar na coluna Endereço IP
- Deve alterar o endereço IP para que seja único ou, se pretender manter o endereço IP, deve editar a porta para que seja única para esse endereço IP

Lembre-se de editar cada separador se alterar uma definição, como uma política de balanceamento de carga, o monitor do Servidor Real ou remover uma regra flightPATH.

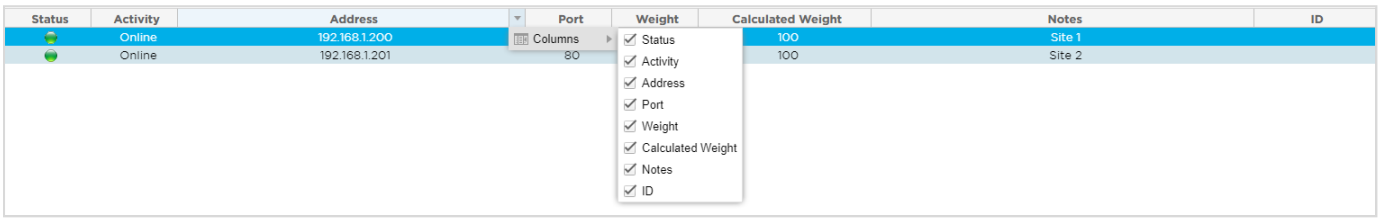
Filtragem dos dados apresentados

Pesquisa de um termo específico

A caixa Pesquisar permite-lhe pesquisar a tabela utilizando qualquer valor, como os octetos do endereço IP ou o nome do serviço.

Seleção da visibilidade da coluna

Também pode selecionar as colunas que pretende apresentar no painel de controlo.



- Mova o rato sobre qualquer uma das colunas
- Aparecerá uma pequena seta no lado direito da coluna
- Ao clicar nas caixas de verificação, seleciona as colunas que pretende ver no painel de controlo.

Compreender as colunas de serviços virtuais

Primário/Modo

A coluna Modo indica a função de alta disponibilidade selecionada para o VIP atual. Para conhecer os modos, consulte Sistema > Clustering > Funções.

Opção	Descrição
Ativo	No modo Cluster, o valor deste campo é Ativo. Quando tiver um par de aparelhos ADC HA no seu centro de dados, um deles mostrará Ativo e o outro Passivo. Se o aparelho atual
Passivo	Quando o ADC está a atuar como um membro secundário de um cluster, então Passivo é mostrado na coluna Modo.
Manual	A função Manual permite que o par ADC seja executado no modo Ativo-Ativo para diferentes endereços IP virtuais. Nesses casos, a coluna Primary (Primário) conterá uma caixa junto a cada IP virtual único que pode ser selecionada para Active (Ativo) ou deixada desmarcada para Passive (Passivo).
Autónomo	O ADC está a atuar como um dispositivo autónomo e não está em modo de Alta Disponibilidade. Como tal, a coluna Primário indicará Autónomo.

VIP

Esta coluna fornece feedback visual sobre o estado de cada serviço virtual. Os indicadores são codificados por cores e são os seguintes:

LED	Significado
●	Em linha
●	Failover-Standby. Este serviço virtual está em espera ativa
●	Indica que um "secundário" está a aguardar por um "primário".
●	O serviço precisa de atenção. Esta indicação pode resultar do facto de um Servidor Real falhar uma verificação do monitor de saúde ou ter sido alterado manualmente para Offline. O tráfego continuará a fluir, mas com uma capacidade reduzida do Real Server
●	Offline. Os servidores de conteúdos não estão acessíveis ou não há servidores de conteúdos activados
●	Estado da constatação
●	IPs virtuais não licenciados ou licenciados excedidos

Ativado

A predefinição para esta opção é Ativado e a caixa de verificação é apresentada como marcada. Pode desativar o Serviço Virtual fazendo duplo clique na linha, desmarcando a caixa de verificação e, em seguida, clicando no botão Atualizar.

Endereço IP

Adicione o seu endereço IPv4 em notação decimal com pontos ou um endereço IPv6. Este valor é o endereço IP virtual (VIP) do seu serviço. Exemplo de IPv4 "192.168.1.100". Exemplo Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334"

Máscara de sub-rede/Prefixo

Adicione a sua máscara de sub-rede em notação decimal com pontos. Exemplo "255.255.255.0". Também pode utilizar o valor da sub-rede, como /24, ou, para IPv6, adicionar o seu Prefixo. Para mais informações sobre o IPv6, consulte **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS**

Porto

Adicione o número da porta associada ao seu serviço. A porta pode ser um número de porta TCP ou UDP. Exemplo: TCP "80" para tráfego Web e TCP "443" para tráfego Web seguro. Também pode especificar um intervalo de valores, como 80-87.

Atualmente, não é possível utilizar valores separados por vírgulas para especificar valores de porta não contíguos.

Nome do serviço

Adicione um nome amigável para identificar o seu serviço. Exemplo "Servidores Web de produção". Este campo também é utilizado quando se utiliza GSLB.

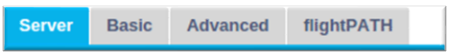
Tipo de serviço

Tenha em atenção que, com todos os tipos de serviço de "Camada 4", o ADC não interage nem modifica o fluxo de dados, pelo que o flightPATH não está disponível com os tipos de serviço de Camada 4. Os serviços da camada 4 simplesmente equilibram o tráfego de acordo com a política de equilíbrio de carga:

Tipo de serviço	Porta/Protocolo	Camada de serviço	Comentário
TCP de camada 4	Qualquer porta TCP	Camada 4	O ADC não altera qualquer informação no fluxo de dados e efectua o equilíbrio de carga normal do tráfego de acordo com a política de equilíbrio de carga
Camada 4 UDP	Qualquer porta UDP	Camada 4	Tal como acontece com o TCP de camada 4, o ADC não altera qualquer informação no fluxo de dados e efectua o equilíbrio de carga normal do tráfego de acordo com a política de equilíbrio de carga
Camada 4 TCP/UDP	Qualquer porta TCP ou UDP	Camada 4	É ideal se o seu serviço tiver um protocolo primário, como o UDP, mas voltará a utilizar o TCP. O ADC não altera qualquer informação no fluxo de dados e efectua o balanceamento de carga padrão do tráfego de acordo com a política de balanceamento de carga
DNS	TCP/UDP	Camada 4	Utilizado para equilibrar a carga dos servidores DNS.
HTTP(S)	Protocolo HTTP ou HTTPS	Camada 7	O ADC pode interagir, manipular e modificar o fluxo de dados utilizando o flightPATH.
FTP	Protocolo de transferência de ficheiros	Camada 7	Utilização de ligações de controlo e de dados separadas entre o cliente e o servidor
SMTP	Protocolo simples de transferência de correio	Camada 4	Utilizar para equilibrar a carga dos servidores de correio
POP3	Protocolo dos Correios	Camada 4	Utilizar para equilibrar a carga dos servidores de correio
IMAP	Protocolo de acesso a mensagens da Internet	Camada 4	Utilizar para equilibrar a carga dos servidores de correio
RDP	Protocolo de Ambiente de Trabalho Remoto	Camada 4	Utilizar para equilibrar a carga dos servidores Terminal Services
RPC	Chamada de procedimento remoto	Camada 4	Utilizar quando os sistemas de balanceamento de carga utilizam chamadas RPC
RPC/ADS	RPC estático do Exchange 2010 para o serviço de catálogo de endereços	Camada 4	Utilizar no balanceamento de carga de servidores Exchange
RPC/CA/PF	RPC estático do Exchange 2010 para acesso de cliente e pastas públicas	Camada 4	Utilizar no balanceamento de carga de servidores Exchange
DICOM	Imagem Digital e Comunicações em Medicina	Camada 4	Utilizar para o equilíbrio de carga de servidores que utilizam protocolos DICOM

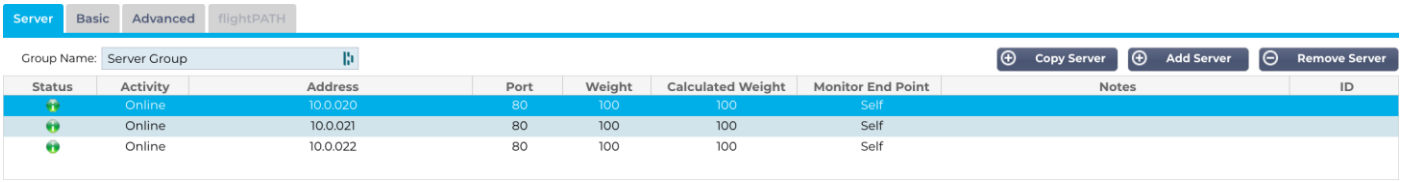
Servidores reais

Existem vários separadores na secção Real Servers (Servidores reais) do painel de controlo: Servidor, Básico, Avançado e flightPATH.



Servidor

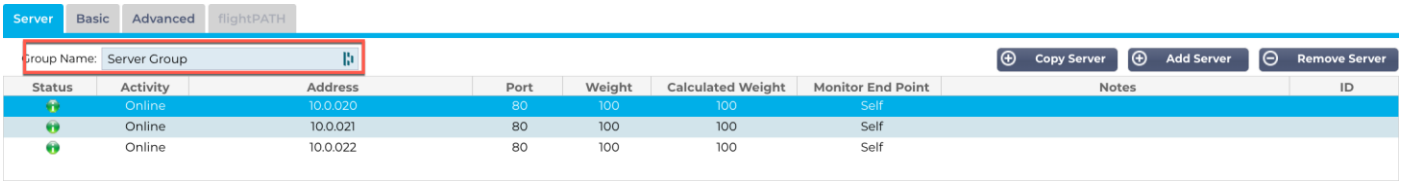
O separador Servidor contém as definições dos servidores back-end reais emparelhados com o Serviço virtual atualmente selecionado. É necessário adicionar pelo menos um servidor à secção Servidores reais.



Adicionar servidor

- Selecione o VIP adequado que definiu anteriormente.
- Clique em Adicionar servidor
- Aparecerá uma nova linha com o cursor a piscar na coluna Endereço IP
- Introduza o endereço IPv4 do seu servidor em notação decimal com pontos. O Servidor Real pode estar na mesma rede que o Serviço Virtual, em qualquer rede local diretamente ligada ou em qualquer rede que o ADC possa encaminhar. Exemplo "10.1.1.1".
- Selecione a coluna Porta e introduza o número da porta TCP/UDP do seu servidor. O número da porta pode ser o mesmo que o número da porta do Serviço Virtual ou outro número de porta para Conectividade de Proxy Reverso. O ADC traduzirá automaticamente para este número.
- Vá para a secção Notas para adicionar qualquer detalhe relevante para o servidor. Exemplo: "Servidor Web IIS 1"

Nome do grupo



Depois de adicionar os servidores que compõem o conjunto com balanceamento de carga, também é possível anexar um Nome do grupo. Depois de editar este campo, o conteúdo é guardado sem ser necessário premir o botão Update (Atualizar).

Luzes de estado do servidor real

Pode ver o estado de um Servidor Real através da cor da luz na coluna Estado. Veja abaixo:

LED	Significado
●	Ligado
◎	Não monitorizado
●	Drenagem
●	Fora de linha

●	Em espera
●	Não ligado
●	Estado da constatação
●	Servidores reais não licenciados ou licenciados excedidos

Atividade

Pode alterar a Atividade de um Servidor real em qualquer altura, utilizando o menu pendente. Para o fazer, faça duplo clique numa linha do Real Server para a colocar no modo de edição.

Opção	Descrição
Em linha	Todos os Servidores reais atribuídos Online receberão tráfego de acordo com a política de balanceamento de carga definida no separador Básico.
Drenagem	Todos os Servidores Reais atribuídos como Drenagem continuarão a servir as ligações existentes, mas não aceitarão novas ligações. A luz de status piscará em verde/azul enquanto o dreno estiver em processo. Depois que as conexões existentes forem encerradas naturalmente, os Servidores reais ficarão offline e a luz de Status ficará azul constante. Também pode ver estas ligações navegando para a secção Navegação > Monitorizar > Estado. O Comportamento de drenagem pode ser alterado no separador Definições avançadas.
Fora de linha	Todos os Servidores Reais definidos como Offline serão imediatamente colocados offline e não receberão qualquer tráfego.
Em espera	Todos os servidores reais definidos como Standby permanecerão offline até que **TODOS** os servidores do grupo Online falhem as verificações do Server Health Monitor. O tráfego é recebido pelo grupo Standby de acordo com a política de balanceamento de carga quando isto acontece. Se um servidor do grupo Online passar na verificação do Monitor de Estado do Servidor, este servidor Online receberá todo o tráfego e o grupo Standby deixará de receber tráfego.

Endereço IP

Este campo é o endereço IP do seu Servidor Real. Exemplo "192.168.1.200".

Porto

Número da porta TCP ou UDP que o Servidor Real está a escutar para o serviço. Exemplo "80" para tráfego Web.

Peso

Esta coluna tornar-se-á editável quando for especificada uma política de balanceamento de carga adequada.

O peso predefinido para um Servidor Real é 100, e pode introduzir valores de 1-100. Um valor de 100 significa carga máxima e 1 significa carga mínima.

Um exemplo para três servidores pode ser mais ou menos assim:

- Servidor 1 Peso = 100
- Servidor 2 Peso = 50
- Servidor 3 Peso = 50

Se considerarmos que a política de balanceamento de carga está definida como Mínimo de ligações e que há um total de 200 ligações de clientes;

- O servidor 1 receberá 100 ligações em simultâneo
- O servidor 2 terá 50 ligações em simultâneo
- O servidor 3 terá 50 ligações em simultâneo

Se utilizarmos o Round Robin como método de balanceamento de carga, que roda os pedidos através do conjunto de servidores com balanceamento de carga, a alteração dos pesos afecta a frequência com que os servidores são escolhidos como alvo.

Se acreditarmos que a política de balanceamento de carga Mais rápida utiliza o menor tempo necessário para OBTER uma resposta, o ajuste dos pesos altera a tendência de forma semelhante à das Ligações mínimas.

Peso calculado

O Peso calculado de cada servidor pode ser visualizado dinamicamente e é calculado automaticamente, não sendo editável. O campo mostra a ponderação real que o ADC está a utilizar quando considera a ponderação manual e a política de equilíbrio de carga.

Monitorizar o ponto final

Esta funcionalidade permite-lhe especificar pontos terminais específicos para monitorizar e, assim, determinar o estado de funcionamento da entrada do Servidor Real. Pode deixá-lo com o valor predefinido de "Self" (Próprio), onde se baseará nos Monitores do Servidor Real especificados para o Serviço Virtual. Em alternativa, também pode especificar um endereço IP, uma porta ou um endereço IP:porta, permitindo-lhe monitorizar outro ponto final na sua rede. Exemplos disto podem incluir, por exemplo, um servidor de base de dados do qual os serviços dependem.

Notas

Introduza quaisquer notas específicas úteis para descrever a entrada definida no campo Notas. Exemplo "IIS Server1 - London DC". Este campo pode ser utilizado para necessidades específicas no âmbito das regras flightPATH e GSLB.

ID

Esta definição tem várias utilizações.

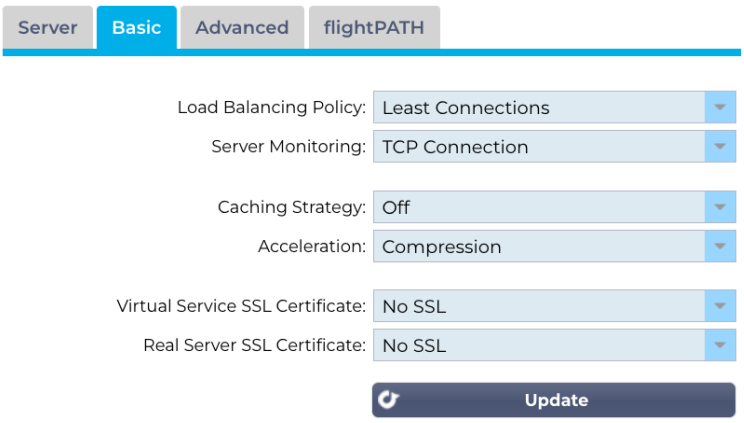
Persistência

O valor pode ser usado em conjunto com o método de persistência baseado em ID de cookie. Isso é muito parecido com a persistência baseada em sessão do PHP, mas usa uma nova técnica chamada Cookie ID Based e cookie RegEx h=[^;]+. O método de persistência baseado em ID de cookie usará o valor no campo ID para gerar um cookie.

Utilização do flightPATH

Também pode utilizar o valor deste campo para direcionar o tráfego, etc.

Básico



Política de balanceamento de carga

A lista pendente mostra-lhe as políticas de balanceamento de carga atualmente suportadas e disponíveis para utilização. Segue-se uma lista das políticas de balanceamento de carga, juntamente com uma explicação.

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

Opção	Descrição
Menos ligações	O equilibrador de carga mantém um registo do número de ligações actuais a cada servidor real. O servidor real com o menor número de ligações recebe o novo pedido subsequente.
Mais rápido	A política de balanceamento de carga Fastest calcula automaticamente o tempo de resposta para todos os pedidos por servidor suavizados ao longo do tempo. A coluna Peso calculado contém o valor calculado automaticamente. A introdução manual só é possível quando se utiliza esta política de balanceamento de carga.
Cookie persistente	Camada 7 Afinidade/Persistência de sessão O modo de balanceamento de carga baseado em lista IP é usado para cada primeira solicitação. O ADC insere um cookie nos cabeçalhos da primeira resposta HTTP. Depois disso, o ADC utiliza o cookie do cliente para encaminhar o tráfego para o mesmo servidor back-end. Este cookie é utilizado para persistência quando o cliente tem de se dirigir sempre ao mesmo servidor back-end. O cookie expirará ao fim de 2 horas e a ligação será equilibrada em termos de carga de acordo com um algoritmo baseado em listas de IP. Este tempo de expiração é configurável utilizando um jetPACK.
Round Robin	O Round Robin é normalmente utilizado em firewalls e balanceadores de carga básicos e é o método mais simples. Cada servidor real recebe um novo pedido em sequência. Este método só é adequado quando é necessário equilibrar a

	carga dos pedidos nos servidores de forma homogénea; um exemplo seriam os servidores Web de pesquisa. No entanto, quando é necessário efetuar o balanceamento de carga com base na carga da aplicação ou do servidor, ou mesmo garantir que é utilizado o mesmo servidor para a sessão, o método Round Robin não é adequado.
Ligação IP	Cookie de afinidade/persistência de sessão da camada 3. Neste modo, o endereço IP do cliente constitui a base para selecionar qual o Servidor Real que irá receber o pedido. Esta ação proporciona persistência. Os protocolos HTTP e de camada 4 podem usar esse modo. Este método é útil para redes internas em que a topologia da rede é conhecida, e pode ter a certeza de que não existem "super proxies" a montante. Com a Camada 4 e os proxies, todos os pedidos podem parecer provenientes de um único cliente e, como tal, a carga não seria uniforme. Com o HTTP, a informação do cabeçalho (X-Forwarder-For) é utilizada quando presente para lidar com proxies.
Baseado na lista IP	A ligação ao Servidor Real é iniciada utilizando "Least connections" e, em seguida, a afinidade da sessão é obtida com base no endereço IP do cliente. Uma lista é mantida por 2 horas por defeito, mas isto pode ser alterado usando um jetPACK.
Baseado em lista de IPs partilhados	Este tipo de serviço só está disponível quando o Modo de conetividade está definido como Retorno direto do servidor. Foi adicionado principalmente para suporte com o balanceamento de carga VMware.
Cookie persistente	Camada 7 Afinidade/Persistência de sessão O modo de balanceamento de carga baseado em lista IP é usado para cada primeira solicitação. O ADC insere um cookie nos cabeçalhos da primeira resposta HTTP. Depois disso, o ADC utiliza o cookie do cliente para encaminhar o tráfego para o mesmo servidor back-end. Este cookie é utilizado para persistência quando o cliente tem de se dirigir sempre ao mesmo servidor back-end. O cookie expirará ao fim de 2 horas e a ligação será equilibrada em termos de carga de acordo com um algoritmo baseado em listas de IP. Este tempo de expiração é configurável utilizando um jetPACK.
Cookie de sessão ASP clássico	Active Server Pages (ASP) é uma tecnologia do lado do servidor da Microsoft. Com esta opção selecionada, o ADC manterá a persistência da sessão no mesmo servidor se um cookie ASP for detectado e encontrado na sua lista de cookies conhecidos. Ao detetar um novo cookie ASP, a carga será equilibrada utilizando o algoritmo Least Connections.
Cookie de sessão ASP.NET	Este modo aplica-se a **ASP.net.** Com este modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie ASP.NET for detectado e encontrado na sua lista de cookies conhecidos. Ao ser detectado um novo cookie ASP, a carga será equilibrada utilizando o algoritmo Least Connections.
Cookie de sessão JSP	Java Server Pages (JSP) é uma tecnologia do lado do servidor da Oracle. Com este modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie JSP for detectado e encontrado na sua lista de cookies conhecidos. Ao detetar um novo cookie JSP, a carga será equilibrada utilizando o algoritmo Least Connections.
Cookie de sessão JAX-WS	Os serviços Web Java (JAX-WS) são uma tecnologia do lado do servidor da Oracle. Com este modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie JAX-WS for detectado e encontrado na sua lista de cookies conhecidos. Quando é detectado um novo cookie JAX-WS, a carga é equilibrada utilizando o algoritmo Least Connections.
Cookie de sessão PHP	Personal Home Page (PHP) é uma tecnologia do lado do servidor de código aberto. Com este modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor quando for detectado um cookie PHP.
Persistência de cookies RDP	Este método de equilíbrio de carga utiliza o cookie RDP criado pela Microsoft com base no nome de utilizador/domínio para fornecer persistência a um servidor. A vantagem deste método significa que é possível manter uma ligação a um servidor mesmo que o endereço IP do cliente mude.

Baseado em Cookie-ID	Um novo método muito semelhante ao "PhpCookieBased" e a outros métodos de balanceamento de carga, mas utilizando CookieIDBased e cookie RegEx h=[^;]+ Este método utilizará o valor definido no campo de notas do servidor real "ID=X;" como o valor do cookie para identificar o servidor. Isto significa, portanto, que é uma metodologia semelhante à CookieListBased, mas utiliza um nome de cookie diferente e armazena um valor de cookie único, não o IP codificado, mas o ID do Servidor Real (lido no momento do carregamento). O valor padrão é CookieIDName="h"; no entanto, se houver um valor de substituição na configuração de definições avançadas do servidor virtual, use-o em vez disso. **NOTA**: Sobrescrevemos a expressão do cookie acima para substituir h= pelo novo valor se este valor for definido. A última parte é que se um valor de cookie desconhecido chegar e corresponder a um dos IDs de servidor real, ele deve selecionar esse servidor; caso contrário, use o próximo método (delegar).

Monitorização do servidor

O ADC contém vários métodos predefinidos de Monitorização do Servidor Real.

Escolha o método de monitorização que pretende aplicar ao Serviço Virtual (VIP)

É essencial escolher o monitor correto para o serviço. Por exemplo, se o Servidor Real for um servidor RDP, um monitor 200OK não é relevante. Da mesma forma, escolher Conexão TCP e 200OK também não faz sentido, pois é necessária uma conexão TCP em funcionamento para que o 200OK funcione. Se não tiver a certeza de qual o monitor a escolher, a Ligação TCP predefinida é um excelente ponto de partida

É possível selecionar vários monitores, clicando em cada um dos monitores que pretende aplicar ao serviço. Os monitores selecionados são executados pela ordem em que selecionados; por isso, comece primeiro pelos monitores das camadas inferiores. Por exemplo, a definição dos monitores Ping/ICMP Echo, Ligação TCP e 200OK será apresentada nos Eventos do Painel como na imagem abaixo:

Podemos ver que o Ping da Camada 3 e a Conexão TCP da Camada 4 foram bem-sucedidos se olharmos para a linha superior, mas o 200OK da Camada 7 falhou. Esses resultados de monitoramento fornecem informações suficientes para indicar que o roteamento está OK e há um serviço em execução na porta relevante, mas o site não está respondendo corretamente à página solicitada. Agora é hora de olhar para o servidor Web e para a secção Biblioteca > Monitor do servidor real para ver os detalhes do monitor com falha.

Opção	**Descrição**
Nenhum	Neste modo, o Servidor Real não é monitorizado e está sempre ativo e a funcionar corretamente. A definição Nenhum é útil para situações em que a monitorização perturba um servidor e para serviços que não devem participar na ação de ativação pós-falha do ADC. É uma via para alojar sistemas não fiáveis ou antigos que não são primários para as operações de H/A. Utilize este método de monitorização com qualquer tipo de serviço.
Eco Ping/ICMP	Neste modo, o ADC envia um pedido de eco ICMP para o IP do servidor de conteúdos. Se for recebida uma resposta de eco válida, o ADC considera que o Servidor Real está ativo e em funcionamento e o débito de tráfego para o servidor continua. Também

	manterá o serviço disponível num par H/A. Este método de monitorização pode ser utilizado com qualquer tipo de serviço.
Ligação TCP	Neste modo, é estabelecida uma ligação TCP com o Servidor Real, que é imediatamente interrompida sem o envio de quaisquer dados. Se a ligação for bem sucedida, o ADC considera que o Servidor Real está a funcionar. Este método de monitorização é utilizável com qualquer tipo de serviço, sendo que os serviços UDP não são atualmente apropriados para a monitorização da ligação TCP.
ICMP Inacessível	O ADC enviará uma verificação de integridade UDP para o servidor e marcará o Servidor Real como indisponível se receber uma mensagem de porta ICMP inacessível. Este método pode ser útil quando é necessário verificar se uma porta de serviço UDP está disponível num servidor, como a porta 53 do DNS.
RDP	Neste modo, uma ligação TCP é inicializada conforme explicado no método ICMP Unreachable. Após a inicialização da ligação, é pedida uma ligação RDP de Camada 7. Se a ligação for confirmada, o ADC considera que o Servidor Real está a funcionar. Este método de monitorização pode ser utilizado com qualquer servidor de terminal da Microsoft.
200 OK	Neste método, uma ligação TCP é inicializada para o Servidor Real. Após o estabelecimento da ligação, o ADC envia ao Servidor Real um pedido HTTP. Aguarda-se uma resposta HTTP e verifica-se o código de resposta "200 OK". O ADC considera que o Servidor Real está a funcionar se for recebido o código de resposta "200 OK". Se o ADC não receber um código de resposta "200 OK" por qualquer razão, incluindo timeouts, falha de ligação e outras razões, o ADC marca o Servidor Real como indisponível. Este método de monitorização só é válido para utilização com tipos de serviço HTTP e HTTP acelerado. Se for utilizado um tipo de serviço da Camada 4 para um servidor HTTP, este poderá ser utilizado se o SSL não estiver a ser utilizado no Servidor Real ou tratado de forma adequada pela funcionalidade "Content SSL".
DICOM	Uma ligação TCP é inicializada para o Real Server no modo DICOM e é efectuado um "Associate Request" (Pedido de associação) do Echoscu para o Real Server na ligação. Uma conversa que inclui um "Associate Accept" (Aceitação de associação) do servidor de conteúdos, uma transferência de uma pequena quantidade de dados seguida de um "Release Request" (Pedido de libertação) e, em seguida, uma "Release Response" (Resposta de libertação) conclui com êxito o monitor. Se o monitor não for concluído com êxito, o Servidor Real é considerado inativo por qualquer motivo.
Definido pelo utilizador	Qualquer monitor configurado na secção Monitorização do servidor real será apresentado na lista.

Estratégia de armazenamento em cache

Por predefinição, a estratégia de armazenamento em cache está desactivada e definida como Desligado. Se o seu tipo de serviço for HTTP, pode aplicar dois tipos de estratégia de armazenamento em cache.

Consulte a página Configurar cache para configurar definições de cache detalhadas. Tenha em atenção que, quando a colocação em cache é aplicada a um VIP com o tipo de serviço "HTTP" acelerado, os objectos comprimidos não são colocados em cache.

Opção	**Descrição**
Por Anfitrião	O armazenamento em cache por anfitrião é baseado na aplicação por nome de anfitrião. Haverá um cache separado para cada domínio/nome de host. Este modo é ideal para servidores web que podem servir vários sites, dependendo do domínio.
Por Virtual Service	A colocação em cache por serviço virtual está disponível quando escolhe esta opção. Apenas uma cache existirá para todos os domínios/nomes de host que passam pelo serviço virtual. Esta opção é uma configuração especializada para uso com vários clones de um único site.

Aceleração

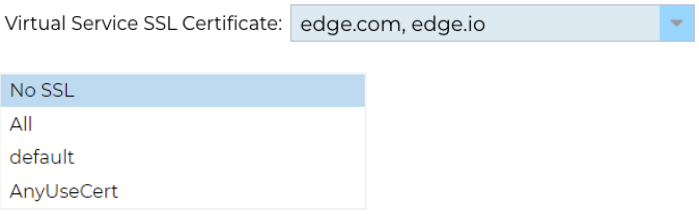
Opção	**Descrição**
Desligado	Desativar a compressão para o Serviço Virtual
Compressão	Quando selecionada, esta opção ativa a compressão para o Serviço Virtual selecionado. O ADC comprime dinamicamente o fluxo de dados para o cliente mediante pedido. Este processo só se aplica a objectos que contenham o cabeçalho content-encoding: gzip. Um exemplo de conteúdo inclui HTML, CSS ou JavaScript. Também pode excluir determinados tipos de conteúdo utilizando a secção Exclusões Globais.

Nota: Se o objeto for armazenável em cache, o ADC armazena uma versão comprimida e serve-a estaticamente (a partir da memória) até que o conteúdo expire e seja revalidado.

Certificado SSL do serviço virtual (encriptação entre o cliente e o ADC)

Por predefinição, a definição é Sem SSL. Se o seu tipo de serviço for "HTTP", pode selecionar um certificado no menu pendente para aplicar ao Serviço virtual. Os certificados que foram criados ou importados aparecerão nesta lista.

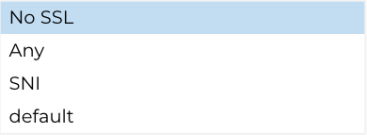
Também é possível destacar vários certificados para aplicar a um serviço. Esta operação activará automaticamente a extensão SNI para permitir um certificado baseado no "Nome de domínio" solicitado pelo cliente.



Opção	**Descrição**
Sem SSL	O tráfego da fonte para o ADC não é encriptado.
Todos	Carrega todos os certificados disponíveis para utilização
Predefinição	Essa opção resulta na aplicação de um certificado criado localmente chamado "Padrão" ao lado do navegador do canal. Use esta opção para testar o SSL quando um não tiver sido criado ou importado.

Certificado SSL do Servidor Real (Encriptação entre o ADC e o Servidor Real)

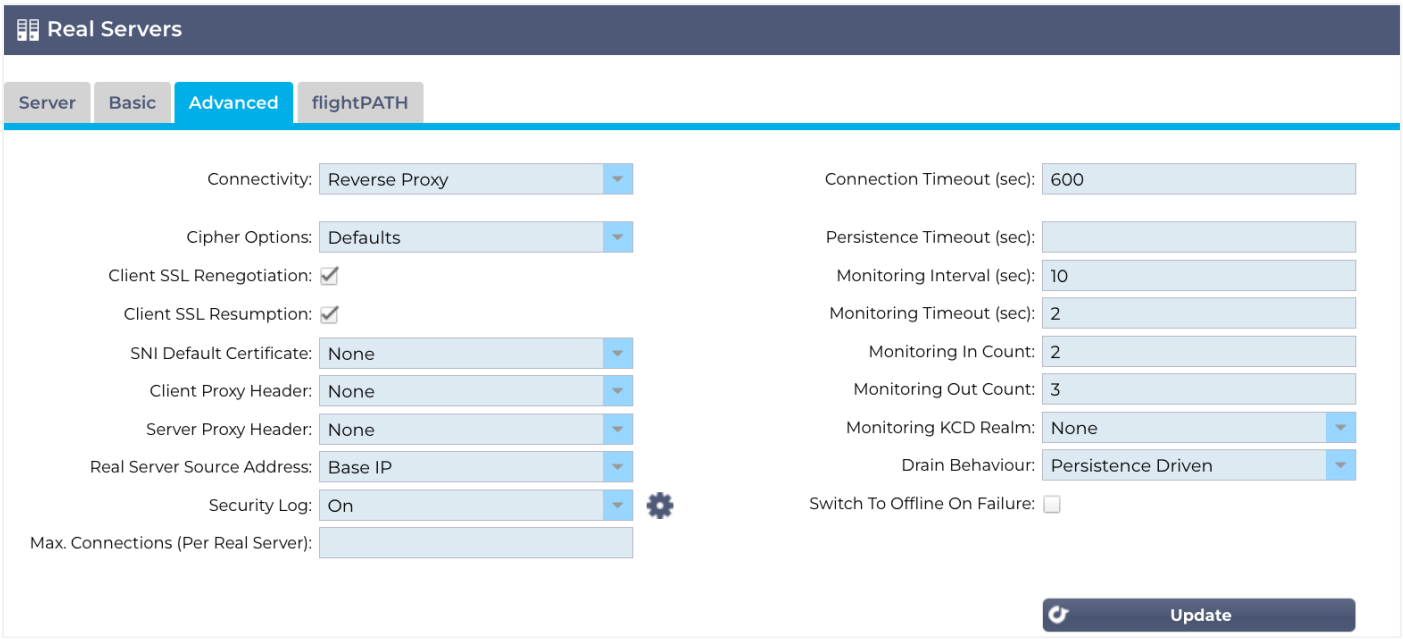
A definição predefinida para esta opção é Sem SSL. Se o seu servidor exigir uma ligação encriptada, este valor tem de ser diferente de Sem SSL. Os certificados que foram criados ou importados aparecerão nesta lista.



Opção	**Descrição**
Sem SSL	O tráfego do ADC para o Servidor Real não é encriptado. A seleção de um certificado no lado do browser significa que "No SSL" pode ser escolhido no lado do cliente para fornecer o que é conhecido como "SSL Offload".
Qualquer	O ADC actua como um cliente e aceitará qualquer certificado que o Servidor Real apresente. O tráfego do ADC para o Servidor Real é encriptado quando esta opção é selecionada. Utilize a opção "Any" (Qualquer) quando for especificado um certificado no

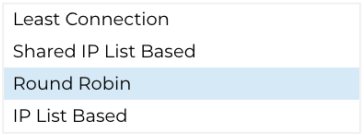
	lado do Serviço Virtual, fornecendo o que é conhecido como "SSL Bridging" (Ligação em ponte SSL) ou "SSL Re-Encryption" (Reencriptação SSL).
SNI	SNI, ou Server Name Indication (Indicação do nome do servidor), é uma extensão do protocolo de rede TLS através da qual o cliente indica a que nome de anfitrião está a tentar ligar-se no início do processo de handshaking . Esta definição permite que o ADC apresente vários certificados no mesmo endereço IP virtual e porta TCP.
Predefinição	Quaisquer certificados auto-assinados que tenha gerado aparecem aqui.

Avançado



Conectividade

O seu Serviço Virtual é configurável com diferentes tipos de conetividade. Selecione o modo de conetividade a aplicar ao serviço.

Opção	Descrição
Proxy inverso	O proxy inverso é o valor predefinido e utiliza a compressão e o armazenamento em cache quando utilizado com a Camada 7. Na Camada 4, o proxy reverso funciona sem cache ou compressão. Neste modo, o ADC actua como um proxy inverso e torna-se o endereço de origem visto pelos Servidores Reais.
Retorno direto do servidor	O Diret Server Return ou DSR, também conhecido como DR - Diret Routing, permite que o servidor por trás do balanceador de carga responda diretamente ao cliente, ignorando o ADC na resposta. O DSR só é adequado para uso com o balanceamento de carga da Camada 4. Portanto, Caching e Compressão não estão disponíveis com esta opção escolhida. **Este modo só pode ser utilizado com os tipos de serviço TCP, UDP e TCP/UDP.** As políticas de persistência de balanceamento de carga também estão limitadas a Ligações Mínimas, Baseado em Lista de IP Partilhada, Round Robin e Baseado em Lista de IP.  A utilização do DSR também requer a realização de alterações no Servidor Real. Consulte a secção Alterações do servidor real.

NAT	Por padrão, o ADC usa o endereço IP do ADC como o endereço IP de origem, e os Servidores Reais enviam a resposta de volta ao ADC para retornar ao Cliente. Isso é bom em quase todas as circunstâncias, mas há cenários em que o Servidor Real precisa ver o endereço IP de origem do Cliente e não do ADC. Quando o modo NAT é aplicado, o ADC recebe o pedido de entrada e envia-o para o Servidor Real depois de alterar o endereço IP de origem para o do Serviço Virtual (endereço VIP). **Este modo só pode ser utilizado com as seguintes políticas de balanceamento de carga:** Least Connection Round Robin IP List Based
Porta de entrada	O modo Gateway permite-lhe encaminhar todo o tráfego através do ADC, permitindo que os Servidores Reais sejam encaminhados através do ADC para outras redes através dos serviços virtuais ou interfaces de hardware do ADC. O uso do dispositivo como um dispositivo de gateway para Servidores Reais é ideal quando executado no modo multi-interface. As políticas de persistência de balanceamento de carga também estão limitadas a Ligações Mínimas, Baseado em Lista de IP Partilhada, Round Robin e Baseado em Lista de IP. Least Connection Shared IP List Based Round Robin IP List Based Este método requer que o Servidor Real defina seu gateway padrão para o endereço da interface local do ADC (eth0, eth1, etc.). Consulte a secção Alterações do servidor real. ***Tenha em atenção que o modo Gateway não suporta a ativação pós-falha num ambiente de cluster.***

Opções de cifra

As cifras constituem a base da criptografia SSL e são extremamente importantes para uma entrega segura e bem sucedida de conteúdos e aplicações Web.

O ADC contém um conjunto integrado de cifras predefinidas, que inclui as mais actualizadas e seguras disponíveis para utilização.

Há ocasiões em que o utilizador deseja anunciar a disponibilidade de um determinado conjunto de Cifras, e o ADC permite a criação de tais Cifras através de jetPACKS de autoria do utilizador. Os jetPACKS escritos pelos utilizadores podem ser importados para o ADC através de Configuração > Software, e depois disponibilizados para escolha através do menu Opções de Cifra.

As opções de cifra são específicas para cada VIP, proporcionando uma elevada flexibilidade e segurança.

Para mais informações sobre as opções de cifra, consulte: *Cipher*

Renegociação SSL do cliente

Assinale esta caixa se pretender permitir a renegociação SSL iniciada pelo cliente. Desactive a renegociação SSL do cliente para evitar possíveis ataques DDOS contra a camada SSL, desmarcando esta opção.

Reinício do SSL do cliente

Assinale esta caixa se pretender ativar as sessões do servidor de Retoma de SSL adicionadas à cache de sessões. Quando um cliente propõe a reutilização de uma sessão, o servidor tentará reutilizar a sessão se

a encontrar. Se a opção Retomar estiver desmarcada, não é efectuada a colocação em cache da sessão para o cliente ou para o servidor.

Certificado por defeito do SNI

Durante uma ligação SSL com a SNI do lado do cliente activada, se o domínio solicitado não corresponder a nenhum dos certificados atribuídos ao serviço, o ADC apresentará o Certificado Predefinido da SNI. A definição predefinida para este é Nenhum, o que efetivamente interromperia a ligação se não houvesse uma correspondência exata. Escolha qualquer um dos certificados instalados a partir do menu pendente para apresentar caso falhe uma correspondência exacta do certificado SSL.

O protocolo proxy

O Protocolo Proxy foi concebido para permitir que os proxies de rede reencaminhem as informações de ligação do cliente (como o endereço IP de origem e o número da porta) para o servidor recetor. Este protocolo é particularmente útil em cenários em que o endereço IP real do utilizador final tem de ser preservado enquanto o tráfego é encaminhado através de um equilibrador de carga ou de um proxy invertido. Ajuda a manter o IP de origem do cliente original para fins de registo, estatísticas ou segurança, melhorando a capacidade de tomar decisões informadas com base na verdadeira origem do tráfego.

Cabeçalho de proxy de cliente

O cabeçalho de proxy de cliente refere-se a um cabeçalho adicionado ao pedido do cliente pelo ADC, encapsulando informações de ligação originais (como o endereço IP e a porta do cliente). Isto é crucial em ambientes em que o ADC actua como proxy e o servidor precisa de saber os detalhes originais do cliente para fins como registo, avaliações de segurança e manutenção do comportamento específico do cliente. O Cabeçalho Proxy de Cliente garante que, apesar do papel de intermediário do ADC, o servidor pode identificar e interagir com precisão com os detalhes originais da ligação do cliente.

As opções incluem:

Opção	**Descrição**
Nenhum	Quando não existe um cabeçalho Proxy ou este não é suportado no tipo de serviço atual
Remover	Remove o cabeçalho Proxy do pacote TCP
Avançar	Reencaminha o cabeçalho Proxy para o servidor

Cabeçalho do servidor proxy

Existem duas versões de cabeçalhos de servidor proxy: Versão 1 e Versão 2.

Opção	Descrição
Versão 1	• Formato baseado em texto, fácil de implementar e depurar. • Fornece informações básicas sobre a ligação do cliente, incluindo o IP de origem, o IP de destino, a porta de origem e a porta de destino. • A linha de protocolo é adicionada ao início da ligação TCP, tornando-a legível, mas ligeiramente menos eficiente em termos de desempenho, em comparação com os formatos binários.
Versão 2	• Formato binário, concebido para um melhor desempenho e eficiência. • Amplia as informações que podem ser transmitidas sobre a ligação, suportando dados adicionais como a família de endereços e informações específicas do protocolo. • Garante uma melhor compatibilidade com protocolos e funcionalidades de rede modernos, incluindo suporte para IPv6 e protocolos de transporte para além do TCP.

As opções de cabeçalho Proxy de Cliente e Proxy de Servidor só estão disponíveis para os tipos de serviço HTTP de Camada 4 e Camada 7.

Endereço de origem do servidor real

Esta definição funciona em conjunto com o proxy inverso e o serviço TCP de camada 4, UDP de camada 4 ou HTTP(S). A definição fornece três opções que pode escolher.

Opção	Descrição
IP de base (predefinição)	Usa a eth0 ou o endereço IP básico do ADC como o IP de origem da solicitação.
IP virtual	Utiliza o IP virtual do serviço.
<endereço IP>	Permite-lhe especificar um endereço IP que faz parte do ADC. Pode ser uma interface de rede diferente ou um VIP diferente.

Registo de segurança

"Ligado" é o valor predefinido e é efectuado por serviço, permitindo o serviço de registo de informações de autenticação nos registos W3C. Clicar no ícone Cog leva-o para a página Sistema > Registo, onde pode verificar as definições do registo W3C.

Máximo. Ligações

Limita o número de conexões simultâneas do Servidor Real e é definido por serviço. Por exemplo, se o configurar para 1000 e tiver dois Servidores reais, o ADC limita **cada** Servidor real a 1000 ligações simultâneas. Também pode optar por apresentar uma página "Servidor demasiado ocupado" assim que este limite for atingido em todos os servidores, ajudando os utilizadores a compreender por que razão ocorreu uma falta de resposta ou um atraso. Deixe esta opção em branco para ligações ilimitadas. O que definir aqui depende dos recursos do seu sistema.

Tempo limite de ligação

O tempo limite de ligação predefinido é de 600 segundos ou 10 minutos. Esta definição ajusta o tempo de expiração da ligação quando não há atividade. Reduza esse valor para o tráfego da Web sem estado de curta duração, que normalmente é de 90s ou menos. Aumente este valor para ligações com estado, como o RDP, para algo como 7200 segundos (2 horas) ou mais, dependendo da sua infraestrutura. O exemplo

do tempo limite do RDP significa que, se um utilizador tiver um período de inatividade de 2 horas ou menos, as ligações permanecerão abertas.

Tempo limite de persistência

A definição Persistence Timeout nos equilibradores de carga especifica a duração durante a qual um equilibrador de carga mantém as informações da sessão para um cliente. Isso garante que as solicitações subsequentes do mesmo cliente sejam direcionadas para o mesmo servidor de back-end, promovendo a consistência da sessão e a comunicação com estado. Uma vez decorrido o período de tempo limite especificado sem mais atividade do cliente, as informações da sessão são eliminadas e os novos pedidos podem ser encaminhados para um servidor diferente.

Intervalo de monitorização

O intervalo é o tempo em segundos entre monitores. O intervalo predefinido é de 1 segundo. Embora 1s seja aceitável para a maioria das aplicações, pode ser benéfico aumentá-lo para outras aplicações ou durante os testes.

Tempo limite de monitorização

O valor do tempo limite é o tempo que o ADC espera que um servidor responda a um pedido de ligação. O valor predefinido é 2s. Aumente esse valor para servidores ocupados.

Monitorização na contagem

O valor predefinido para esta definição é 2. O valor de 2 indica que o Servidor Real tem de passar por duas verificações bem sucedidas do monitor de estado de funcionamento antes de ficar online. Aumentar este valor aumentará a probabilidade de o servidor poder servir o tráfego, mas demorará mais tempo a entrar em serviço, dependendo do intervalo. Diminuir este valor fará com que o servidor entre em funcionamento mais cedo.

Monitorização da contagem de saídas

O valor predefinido para esta definição é 3, o que significa que o monitor do Real Server tem de falhar três vezes antes de o ADC deixar de enviar tráfego para o servidor e este ser marcado como RED e Unreachable (vermelho e inacessível). Aumentar este valor resultará num serviço melhor e mais fiável, à custa do tempo que o ADC demora a deixar de enviar tráfego para este servidor.

Controlo do domínio KCD

Esta definição permite-lhe ativar a monitorização do Kerberos Constrained Delegation Realm que configurou nas definições do Kerberos. Consulte Autenticação > Kerberos.

Comportamento de drenagem

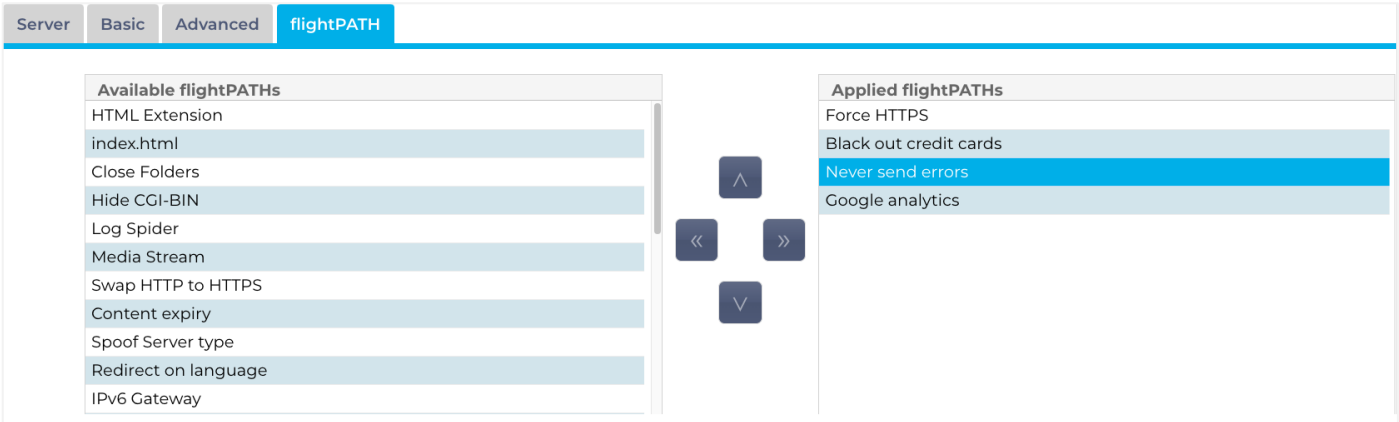
Sempre que um servidor real é colocado em modo de drenagem, é sempre melhor poder controlar o comportamento do tráfego que lhe é enviado. O menu Drain Behaviour (Comportamento de drenagem) permite selecionar o comportamento do tráfego por Serviço Virtual. As opções são:

Opção	Descrição
Orientado para a persistência	Esta é a seleção por defeito. Sempre que o utilizador visita a sessão de persistência, esta é alargada. Com uma utilização de 24 horas, é possível que a drenagem nunca aconteça. No entanto, se o número de ligações ao servidor real chegar a 0, a drenagem termina, as sessões de persistência são eliminadas e todos os visitantes são reequilibrados na próxima ligação que efectuarem.
Migrar visitantes	Sessão persistente ignorada na reconexão - (comportamento herdado antes de 2022) As novas ligações TCP (quer façam parte de uma sessão existente ou não) são sempre efectuadas a um servidor real online. Se a sessão de persistência era para um servidor real que estava a esgotar-se, é substituída. O Serviço Virtual ignorará efetivamente a persistência de quaisquer novas ligações e estas serão equilibradas em termos de carga para um novo servidor.
Sessões de reforma	Sessões persistentes não prolongadas. As ligações de entrada dos utilizadores serão atribuídas ao servidor pretendido, mas a sua sessão de persistência não é prolongada. Assim, após o tempo da sessão de persistência ser excedido, serão tratadas como novas ligações e movidas para um servidor diferente.

Mudar para offline em caso de falha

Quando esta opção está selecionada, os Servidores reais que falharem o seu controlo de saúde são colocados offline e só podem ser colocados online manualmente.

flightPATH



O flightPATH é uma tecnologia de gestão de tráfego concebida pela Edgenexus e disponível exclusivamente no ADC. Ao contrário dos motores baseados em regras de outros fornecedores, o flightPATH não funciona através de uma linha de comandos ou de uma consola de entrada de scripts. Em vez disso, utiliza uma GUI para selecionar os diferentes parâmetros, condições e acções a executar para alcançar o que é necessário. Estas caraterísticas tornam o flightPATH extremamente poderoso e permitem aos administradores de rede manipular o tráfego HTTPS de forma altamente eficaz.

flightPATH só está disponível para utilização com ligações HTTPS e esta secção não é visível quando o Tipo de Serviço Virtual não é HTTP.

Como pode ver na imagem acima, existe uma lista de regras disponíveis à esquerda e as regras aplicadas ao serviço virtual à direita.

Aplique uma regra disponível arrastando e largando a regra do lado esquerdo para o direito, ou realçando uma regra e clicando na seta para a direita para a mover para o lado direito.

A ordem de execução é essencial e começa com a regra de topo executada primeiro. Para alterar a ordem de execução, selecione a regra e desloque-se para cima e para baixo utilizando as setas.

É importante compreender que as regras do flightPATH nesta secção do ADC funcionam numa base booleana **OR**, enquanto que as condições e acções dentro da área de definição do flightPATH funcionam numa base **AND.**

Para remover uma regra, arraste e largue-a de volta para o inventário de regras à esquerda ou selecione a regra e clique na seta para a esquerda.

Pode adicionar, remover e editar regras flightPATH na secção Configurar flightPATH deste guia.

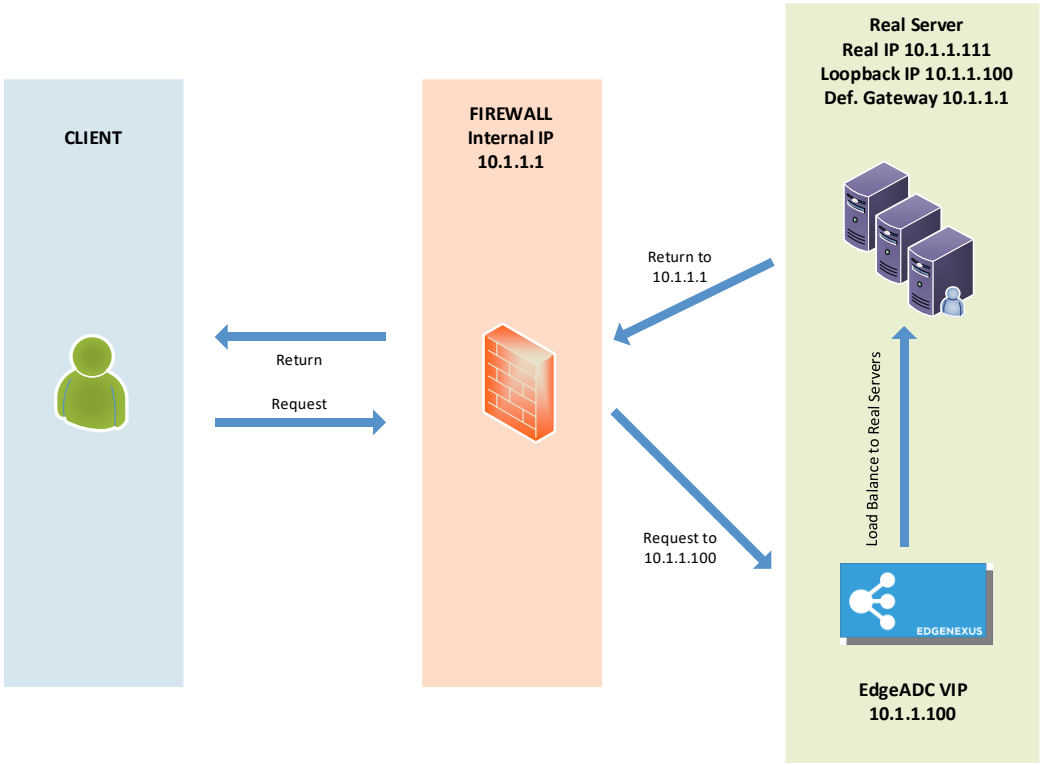
Alterações reais do servidor para o regresso direto ao servidor

O Diret Server Return ou DSR, como é amplamente conhecido (DR - Diret Routing em alguns círculos), permite que o servidor por trás do ADC responda diretamente ao cliente, ignorando o ADC na resposta. O DSR só é adequado para uso com balanceamento de carga da Camada 4. O armazenamento em cache e a compactação não estão disponíveis quando ativados.

O balanceamento de carga da camada 7 com esse método não funcionará, pois não há suporte de persistência além do IP de origem. O balanceamento de carga SSL/TLS com este método não é ideal, pois só há suporte para persistência de IP de origem.

Como funciona

- O cliente envia um pedido ao EdgeADC VIP
- Pedido recebido pelo EdgeADC
- Pedido encaminhado para servidores de conteúdos
- Resposta enviada diretamente ao cliente sem passar pelo EdgeADC



Configuração necessária do servidor de conteúdo

Geral

- O gateway predefinido do servidor de conteúdos deve ser configurado normalmente. (Não através do ADC)
- O servidor de conteúdo e o balanceador de carga devem estar na mesma sub-rede

Janelas

- O servidor de conteúdos tem de ter um loopback ou um Alias configurado com o endereço IP do Canal ou VIP
    - A métrica da rede deve ser 254 para impedir a resposta a pedidos ARP
    - Adicionar um adaptador de loopback no Windows Server 2012 - Clique aqui

    - Adicionar um adaptador de loopback no Windows Server 2003/2008 - Clique aqui
- Execute o seguinte em um prompt de comando para cada interface de rede que você configurou nos Servidores Windows Real

netsh interface ipv4 set interface "Nome da interface de rede do Windows" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostreceive=enable

netsh interface ipv4 set interface "Windows loopback interface name" weakhostsend=enable

Linux

- Adicionar uma interface de loopback permanente
- Editar "/etc/sysconfig/network-scripts"

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

- Editar "/etc/sysctl.conf"

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

- Executar "sysctl - p"

Alterações reais do servidor - Modo Gateway

O modo Gateway permite-lhe encaminhar todo o tráfego através do ADC, o que permite que o tráfego proveniente dos servidores de conteúdos seja encaminhado através do ADC para outras redes através das interfaces na unidade ADC. A utilização do dispositivo como dispositivo de gateway para servidores de conteúdos deve ser utilizada quando estiver a funcionar no modo multi-interface.

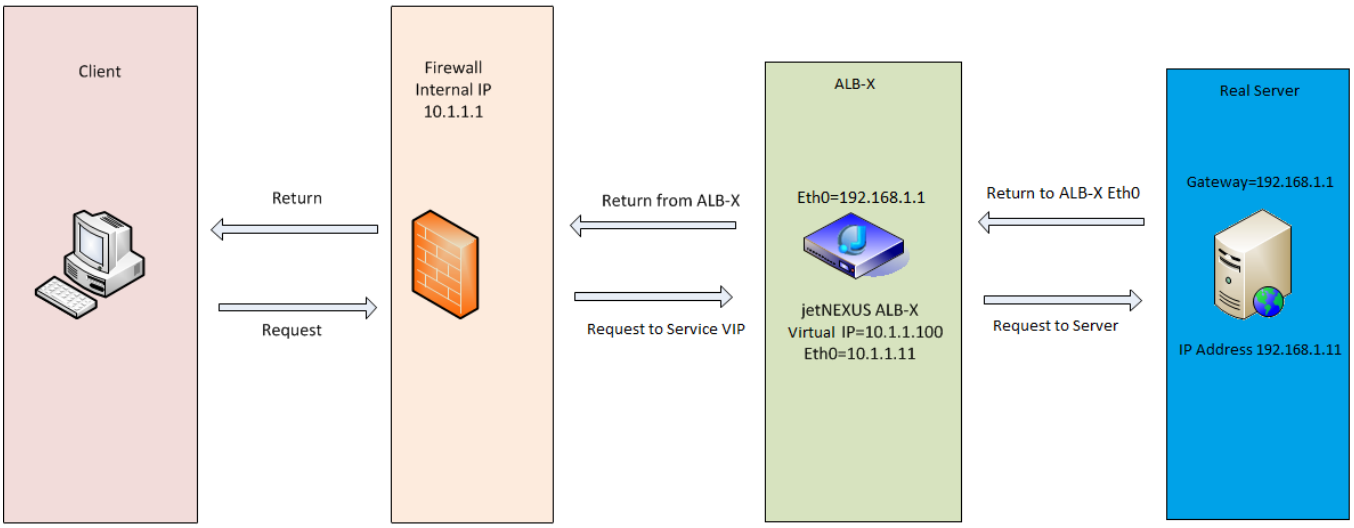
Como funciona

- O cliente envia um pedido ao EdgeADC
- Um pedido é recebido pelo EdgeADC
- Pedido enviado aos servidores de conteúdos
- Resposta enviada à EdgeADC
- O ADC encaminha a resposta para o cliente

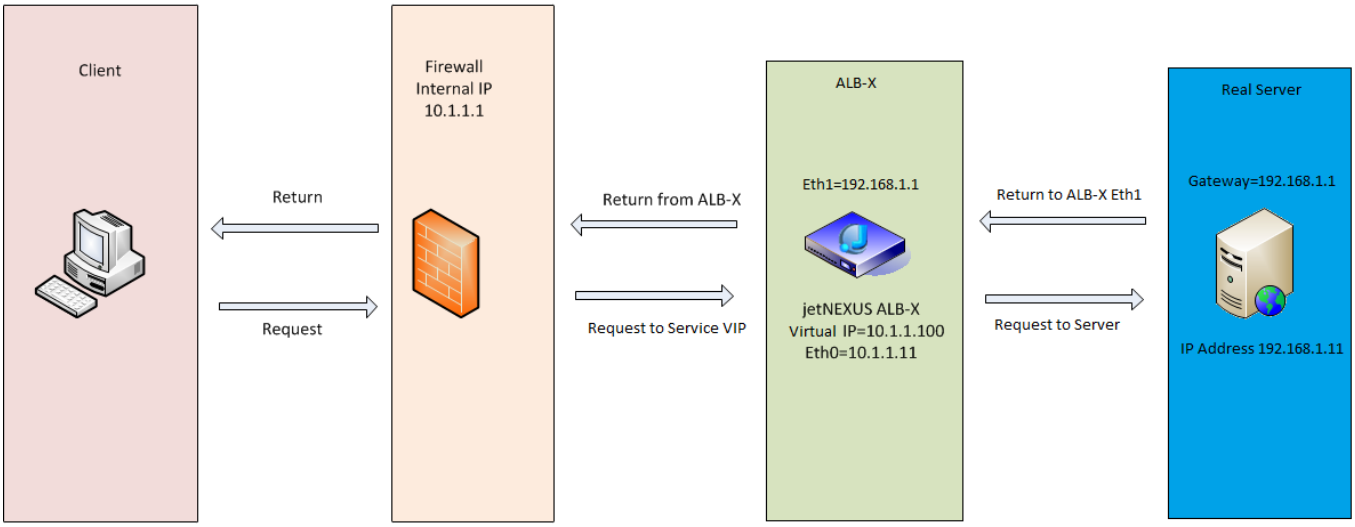
Configuração necessária do servidor de conteúdo

- Modo de braço único - é utilizada uma interface, mas o VIP de serviço e os servidores reais têm de estar em sub-redes diferentes.
- Modo de braço duplo - são utilizadas duas interfaces, mas o VIP de serviço e os servidores reais têm de estar em sub-redes diferentes.
- Em cada caso, Single Arm e Dual Arm, os Real Servers precisam de configurar o seu gateway predefinido para o endereço da interface ADC na sub-rede relevante.

Exemplo de braço único



Exemplo de braço duplo

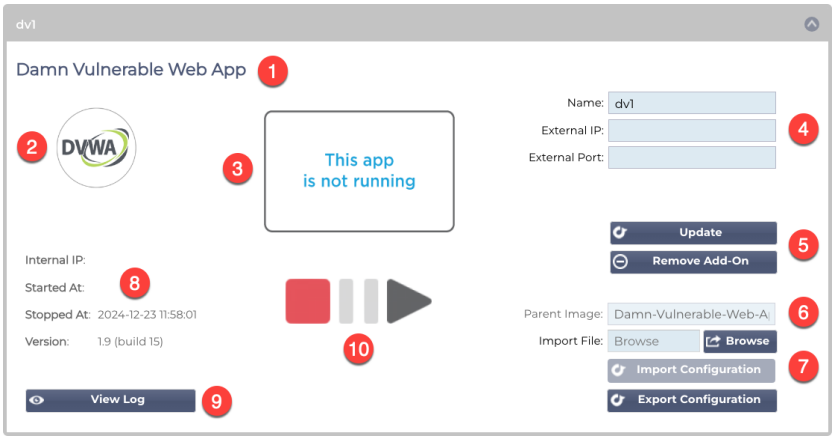


Biblioteca

Suplementos

Os complementos são aplicações que são carregadas como contentores e executadas num modo isolado dentro do ADC. Exemplos de Add-ons podem ser um firewall de aplicativo ou até mesmo uma micro instância do próprio ADC.

Uma aplicação é implementada na secção Add-Ons utilizando a página Aplicações, tal como descrito neste guia. Uma vez implementada, uma aplicação aparece da seguinte forma.



Como se pode ver na imagem acima, há vários elementos que são destacados.

Item	Descrição
❶	Título da aplicação
❷	Ícone da aplicação
❸	Ecrã de execução da aplicação. Se a aplicação estiver a ser executada, será apresentada uma miniatura do ecrã.
❹	Dados de acesso: **Nome**: Este é um nome interno que utiliza para fazer referência à aplicação a partir da secção Serviços virtuais. Não é possível fazer referência a uma aplicação utilizando o seu endereço IP. Apenas alfanumérico, sem espaços. **IP externo**: Este é o endereço IP que tem de fornecer para a aplicação. Este endereço fará parte da sua sub-rede de rede. **Porta externa**: Este é um campo importante. Terá de especificar as portas que serão utilizadas para aceder à aplicação. Quando o tráfego externo à aplicação estiver a aceder à mesma, terá de a especificar utilizando a seguinte notação: 53/tcp ou 53/udp. Para além disso, terá de especificar a porta da IU para a aplicação. Estas são apresentadas na dica de ferramenta do campo para cada aplicação.
❺	Botão Atualizar: Depois de preencher os dados especificados em❸ , clique neste botão para confirmar as entradas e configurar a aplicação. O botão Remover suplemento é utilizado para o remover da secção Aplicações. Para remover uma aplicação, certifique-se de que todas as referências à aplicação também são removidas antes de tentar a remoção.
❻	A imagem dos pais é um campo informativo e não é utilizado do ponto de vista do utilizador.
❼	A importação e exportação de uma configuração é importante para manter uma cópia de segurança das definições. Utilize esta opção para efetuar a função Importar e Exportar.
❽	Os detalhes da execução fornecem informações sobre o endereço IP da API interna, a hora de início e de fim e o número da versão da aplicação.
❾	Este botão permite-lhe descarregar e visualizar o registo. É utilizado principalmente quando é necessário abrir um pedido de assistência.
❿	O funcionamento da aplicação é efectuado através destes botões. Vermelho=Parado, Dourado=Pausado e Verde=Em funcionamento.

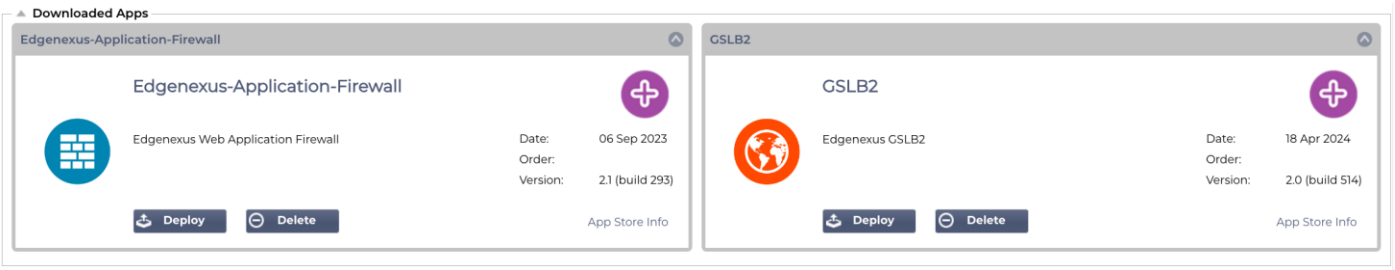
Aplicações

A secção Apps (Aplicações) tem várias subsecções que tratam das Apps disponíveis para utilização no ADC. Estas são o Filtro, as Aplicações descarregadas e as Aplicações compradas.

O filtro

O filtro permite-lhe filtrar as aplicações/ferramentas pelo seu tipo.

Aplicações descarregadas

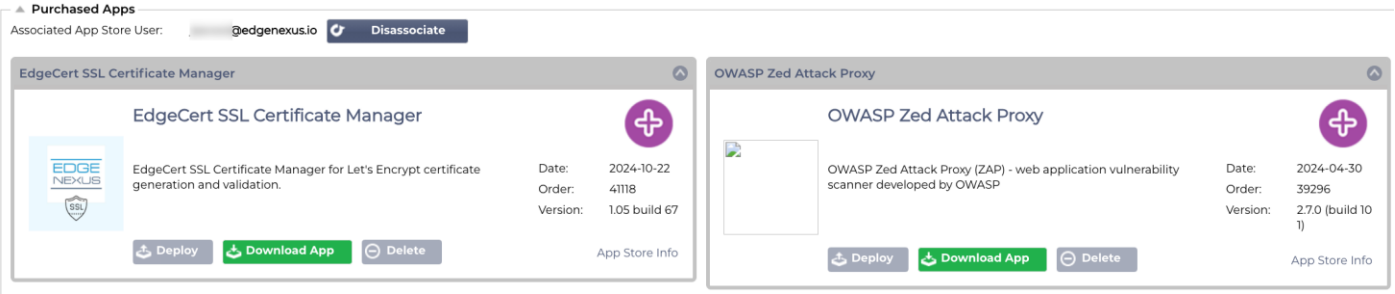


Esta secção contém as aplicações que foram descarregadas para o ADC. Pode tê-las descarregado para o seu ambiente de trabalho local e, posteriormente, carregado para o ADC, ou pode tê-las descarregado através do portal da App Store incorporado.

Cada aplicação está equipada com dois botões, bem como dados que indicam o número da versão e a data em que foi lançada.

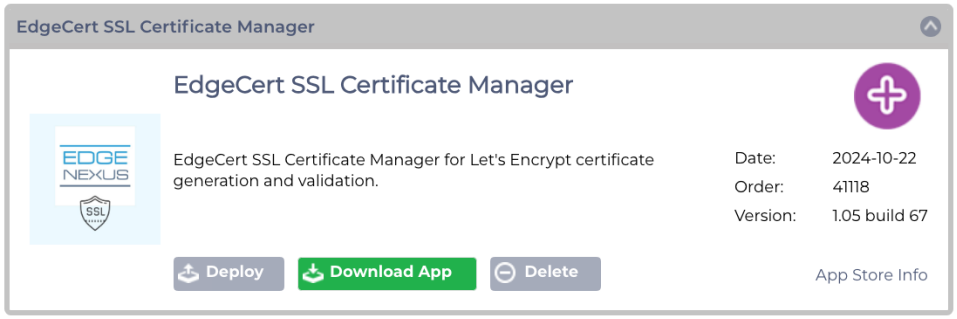
O botão Deploy (Implementar) implementará a aplicação como um contentor seguro, enquanto o botão Delete (Eliminar) eliminará a aplicação de dentro do ADC.

Aplicação comprada



A primeira coisa que irá notar é o Utilizador associado da App Store e o respetivo botão associado. Terá de iniciar sessão utilizando as suas credenciais da App Store para que o ADC seja associado à App Store. Por baixo, encontrará as aplicações associadas à sua conta.

Ao iniciar sessão na App Store, diretamente ou através do portal incorporado, pode adquirir aplicações. Estas são indicadas nesta secção e podem ser carregadas para o ADC, prontas para serem implementadas.



Cada aplicação tem uma série de botões: Implementar, Descarregar aplicação e Eliminar. Para além disso, existe também uma hiperligação Info da App Store no lado direito que o levará para a página relevante da App Store e mostrará informações sobre o Addon.

Implantar

A secção Aplicações dentro de Suplementos detalha as aplicações que comprou, descarregou e implementou. Uma vez implementada, a aplicação aparecerá na secção Transferida.

Descarregar a aplicação

A aplicação pode ser descarregada da App Store, clicando neste botão.

Eliminar

Se pretender eliminar uma aplicação que tenha sido descarregada.

Autenticação

A página Autenticação da Biblioteca> permite-lhe configurar servidores de autenticação e criar regras de autenticação.

Configurar a autenticação - um fluxo de trabalho

Para aplicar a autenticação ao seu serviço, siga, no mínimo, os passos seguintes.

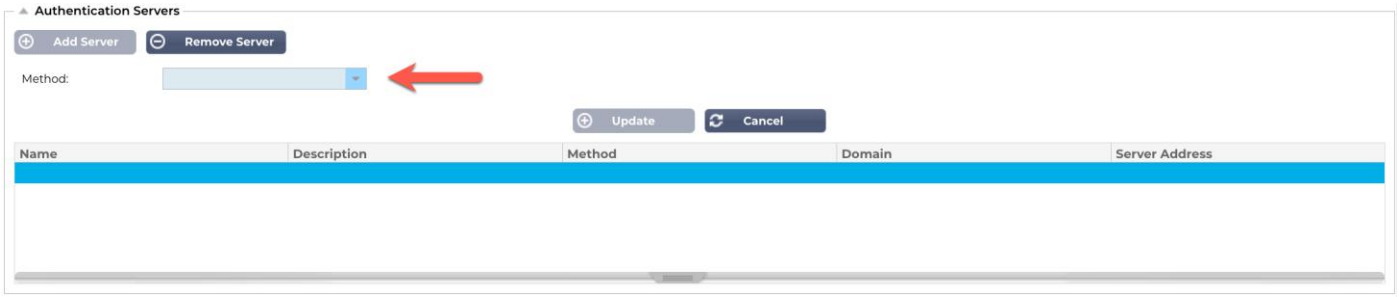
1. Criar um servidor de autenticação.
2. Criar uma regra de autenticação que utilize um servidor de autenticação.
3. Criar uma regra flightPATH que utilize uma regra de autenticação.
4. Aplicar a regra flightPATH a um serviço

Servidores de autenticação

Para configurar um método de autenticação funcional, temos primeiro de configurar um servidor de autenticação.

A primeira etapa consiste em selecionar o método de autenticação necessário.

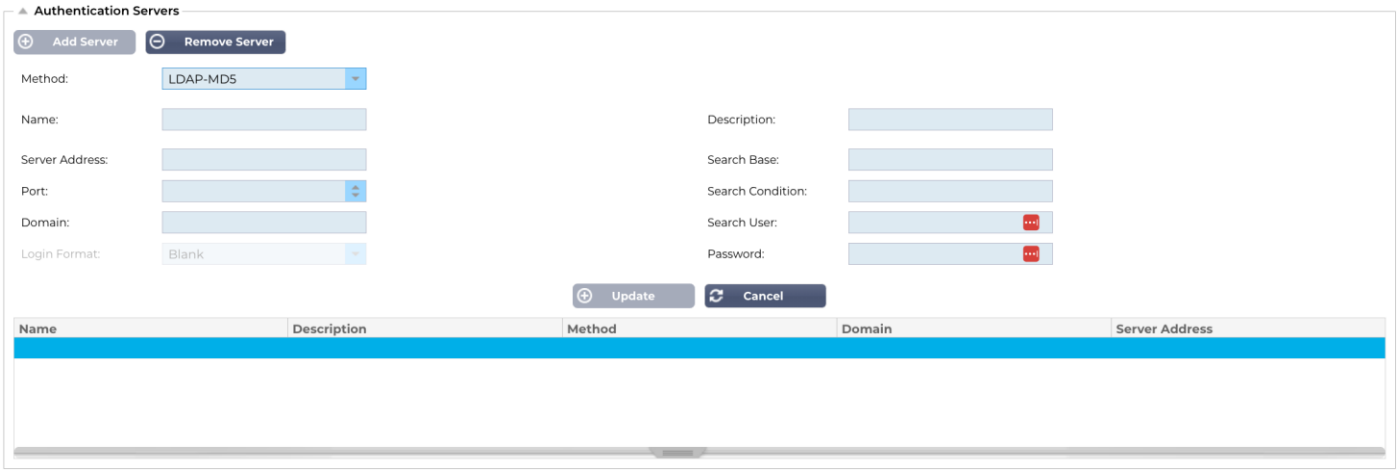
- Clique em Adicionar servidor.
- Selecione o Método no menu pendente.



A função Servidor de autenticação é dinâmica e apresenta apenas os campos que são necessários para o método de autenticação selecionado.

- Preencha os campos com exatidão para garantir uma ligação correta aos servidores.

Opções para LDAP, LDAP-MD5, LSAPS, LDAPS-MD5, Radius e SAML

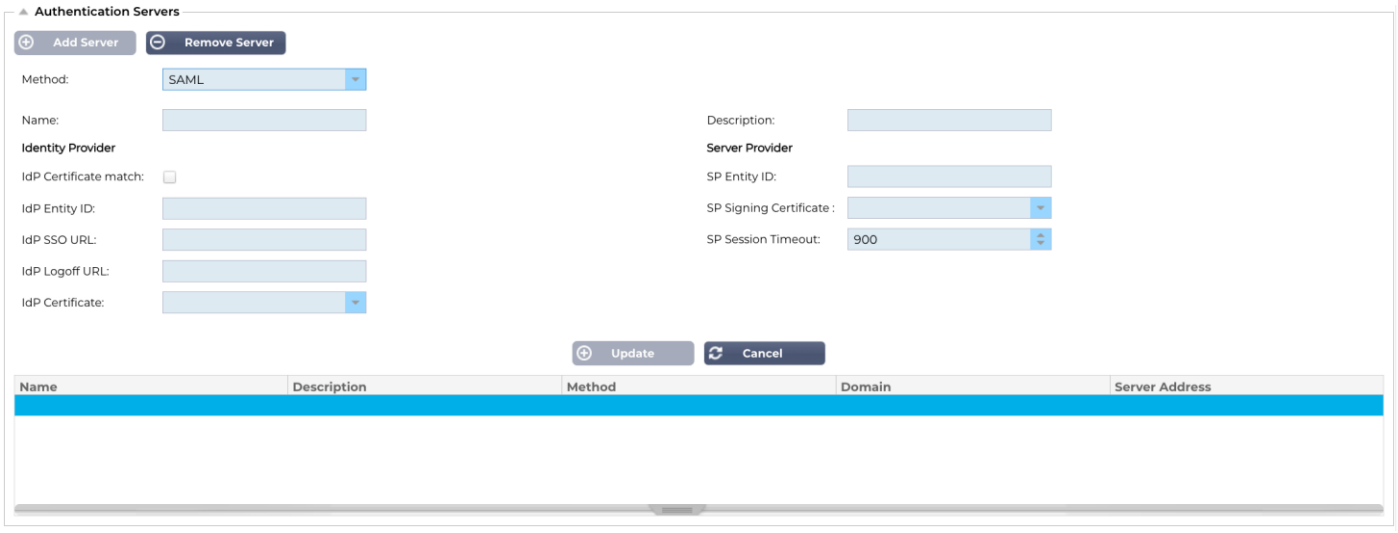


Opção	Descrição

Método	Escolher um método de autenticação LDAP - LDAP básico com nomes de utilizador e palavras-passe enviados em texto claro para o servidor LDAP. LDAP-MD5 - LDAP básico com nome de utilizador em texto simples e palavra-passe com hash MD5 para maior segurança. LDAPS - LDAP sobre SSL. Envia a senha em texto claro dentro de um túnel criptografado entre o ADC e o servidor LDAP. LDAPS-MD5 - LDAP sobre SSL. A palavra-passe é hash MD5 para maior segurança dentro de um túnel encriptado entre o ADC e o servidor LDAP
Nome	Dê um nome ao seu servidor para fins de identificação - este nome é utilizado em todas as regras.
Endereço do servidor	Adicionar o endereço IP ou o nome do anfitrião do servidor de autenticação
Porto	Para LDAP e LDAPS, as portas são definidas como 389 e 636 por defeito. Para o Radius, a porta é geralmente 1812. Para SAML, as portas são definidas no ADC.
Domínio	Adicione o nome de domínio do servidor LDAP.
Formato de início de sessão	Utilize o formato de início de sessão de que necessita. Nome de utilizador - com este formato escolhido, apenas é necessário introduzir o nome de utilizador. Todas as informações de utilizador e domínio introduzidas pelo utilizador são eliminadas e são utilizadas as informações de domínio do servidor. Nome de utilizador e domínio - O utilizador deve introduzir a sintaxe completa do domínio e do nome de utilizador. Exemplo: *minhaempresa\jdoe OU jdoe@minhaempresa*. As informações de domínio introduzidas ao nível do servidor são ignoradas. Em branco - o ADC aceitará tudo o que o utilizador introduzir e enviá-lo-á para o servidor de autenticação. Esta opção é utilizada quando se utiliza MD5.
Descrição	Adicionar uma descrição
Base de pesquisa	Este valor é o ponto de partida para a pesquisa na base de dados LDAP. Exemplo *dc=minhaempresa,dc=local*
Condição de pesquisa	As condições de pesquisa devem estar em conformidade com o RFC 4515. Exemplo: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Procurar utilizador	Efetuar uma pesquisa de um utilizador administrador de domínio no servidor de diretórios.
Palavra-passe	Palavra-passe para o utilizador administrador do domínio.
Tempo morto	O período de tempo após o qual um servidor inativo é marcado como ativo novamente

Opções para autenticação SAML

IMPORTANTE: Ao configurar a autenticação via SAML, é necessário criar um aplicativo corporativo para a autenticação Entra ID. As instruções para fazer isso estão disponíveis no capítuloConfigurando o aplicativo de autenticação Entra ID no Microsoft Entra

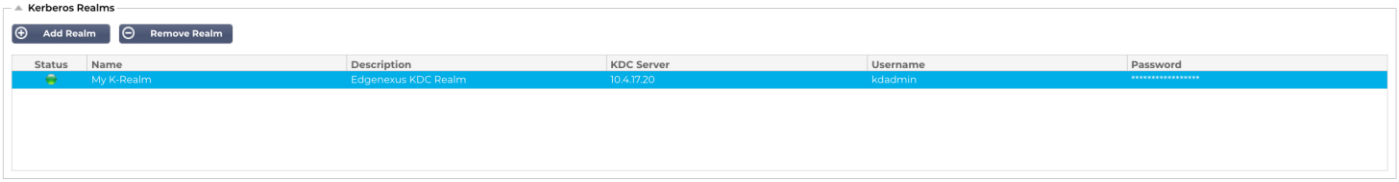


Opção	Descrição
Método	Escolher um método de autenticação LDAP - LDAP básico com nomes de utilizador e palavras-passe enviados em texto claro para o servidor LDAP. LDAP-MD5 - LDAP básico com nome de utilizador em texto simples e palavra-passe com hash MD5 para maior segurança. LDAPS - LDAP sobre SSL. Envia a senha em texto claro dentro de um túnel criptografado entre o ADC e o servidor LDAP. LDAPS-MD5 - LDAP sobre SSL. A palavra-passe é hash MD5 para maior segurança dentro de um túnel encriptado entre o ADC e o servidor LDAP
Nome	Dê um nome ao seu servidor para fins de identificação - este nome é utilizado em todas as regras.
Fornecedor de identidade	
Correspondência de certificados IdP	A correspondência de certificados IdP refere-se ao processo de verificação de que o certificado digital utilizado por um IdP (Identity Provider) para assinar asserções SAML corresponde ao certificado em que o SP (Service Provider) confia. Esta validação garante que o IdP é legítimo e que as asserções que envia são autênticas e inalteradas. Normalmente, o SP armazena o certificado do IdP nos seus metadados e compara o certificado incorporado nas asserções SAML com o certificado armazenado para determinar uma correspondência.
ID da entidade IdP	Uma ID de entidade SAML IdP é um identificador globalmente único que serve de endereço definitivo para um fornecedor de identidade (IdP) no ecossistema SAML (Security Assertion Markup Language). Este identificador é normalmente um URL ou URI que distingue exclusivamente o IdP de outras entidades envolvidas em processos de autenticação e autorização baseados em SAML. Desempenha um papel crucial no estabelecimento da confiança e na facilitação da comunicação segura entre IdPs, Fornecedores de Serviços (SPs) e utilizadores.
URL SSO do IdP	Um URL SSO de IdP, abreviatura de URL de início de sessão único, é um URL de ponto final específico fornecido por um fornecedor de identidade (IdP) que serve como gateway de autenticação para iniciar sessões de início de sessão único (SSO). Ao redirecionar um utilizador para este URL, o IdP pede-lhe que se autentique utilizando as suas credenciais e, após uma autenticação bem sucedida, redirecciona-o para o fornecedor de serviços (SP) com uma asserção que contém as suas informações de identidade. Esta afirmação é então validada pelo SP, permitindo que o utilizador aceda aos recursos do SP sem ter de se autenticar novamente.
URL de desconexão do IdP	O URL de Terminação de Sessão SAML IdP é um ponto final específico no Fornecedor de Identidade (IdP) que inicia e gere o processo de Terminação de Sessão para sessões Single Sign-On (SSO). Quando um utilizador clica no botão de terminar sessão numa aplicação, a aplicação redirecciona o utilizador para o URL de terminar sessão do IdP. Em seguida, o IdP invalida a sessão do utilizador em todas as partes confiáveis associadas à autenticação SSO e envia uma resposta de fim de sessão para a aplicação, terminando efetivamente a sessão do utilizador em todas as aplicações ligadas.
Certificado IdP	Um certificado SAML IdP é um certificado digital X.509 emitido por uma autoridade de confiança para um fornecedor de identidade (IdP) que participa em protocolos de autenticação SAML (Security Assertion Markup Language). Este certificado serve como um meio seguro de verificar a identidade do IdP e autenticar a integridade e a confidencialidade das mensagens SAML trocadas entre o IdP e os fornecedores de serviços (SPs). Pode selecionar o certificado IdP que terá instalado no ADC utilizando o menu pendente.
Descrição	Uma descrição para a definição.
Procurar utilizador	Efetuar uma pesquisa de um utilizador administrador do domínio.
Palavra-passe	Para especificar a palavra-passe do utilizador admin.

Fornecedor de servidores	
ID da entidade SP	Um ID de Entidade SP é um identificador único que serve como um endereço global para um Fornecedor de Serviços (SP) específico no contexto do protocolo SAML. É uma forma normalizada de identificar um SP e é normalmente um URL ou outro URI que identifica os metadados SAML do SP, que contém informações críticas como certificados de encriptação e pontos finais de autenticação.
Certificado de assinatura SP	Um Certificado de Assinatura SAML SP é um certificado X.509 usado por um Provedor de Serviços (SP) para assinar respostas SAML, garantindo a autenticidade e a integridade das mensagens trocadas entre o SP e o Provedor de Identidade (IdP) durante a autenticação Single Sign-On (SSO). O SP assina a resposta usando sua chave privada, e o IdP verifica a assinatura usando a chave pública associada ao certificado, confirmando a identidade do remetente e que o conteúdo da mensagem não foi adulterado.
SP Tempo limite da sessão	O tempo limite da sessão SP refere-se à duração máxima durante a qual a sessão de autenticação de um utilizador é considerada válida no lado do Fornecedor de Serviços (SP) após um Single Sign-On (SSO) bem sucedido através de um Fornecedor de Identidade (IdP). Após este tempo especificado, o SP termina a sessão e exige que o utilizador volte a autenticar-se para recuperar o acesso a recursos protegidos. Este mecanismo ajuda a proteger contra o acesso não autorizado e garante que as sessões de utilizador não ficam inactivas durante longos períodos.

Reinos KDC

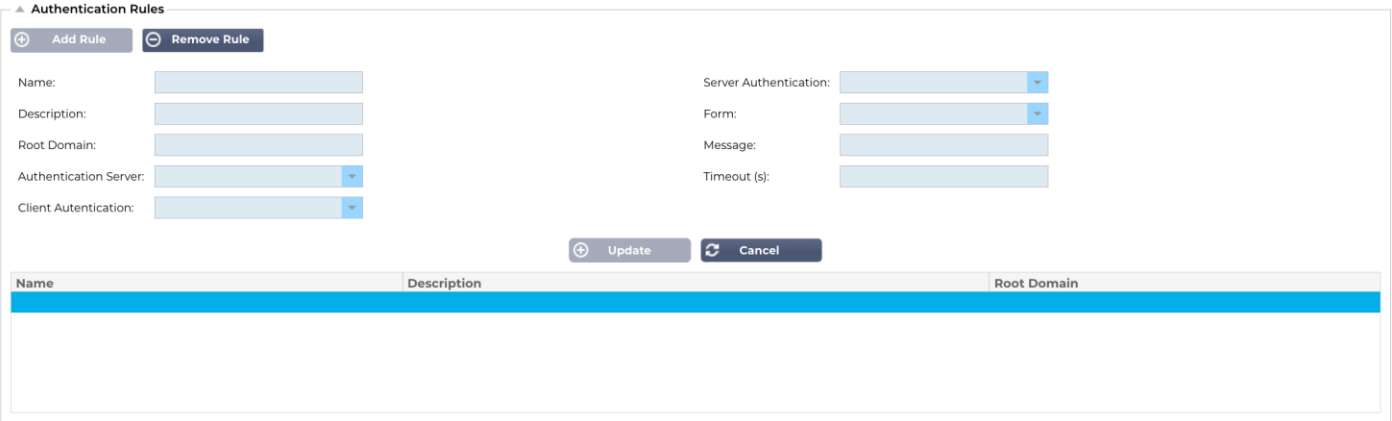
Os reinos KDC referem-se a configurações no âmbito do protocolo de autenticação Kerberos, em que cada reino é essencialmente um domínio ou rede que funciona sob um único Centro de Distribuição de Chaves (KDC). Esta configuração delineia um grupo de sistemas que são geridos sob o mesmo KDC principal, facilitando a autenticação segura e os mecanismos de atribuição de bilhetes em toda a rede. Os domínios podem ser hierárquicos ou não hierárquicos, com a possibilidade de estabelecer relações de confiança entre eles para uma autenticação segura entre domínios.



A interface de utilizador fornecida no ADC, como mostra a imagem acima, permite-lhe definir os seus reinos Kerberos. Esta informação pode depois ser utilizada nas regras de autenticação.

Regras de autenticação

A fase seguinte consiste em criar as regras de autenticação a utilizar com a definição do servidor.



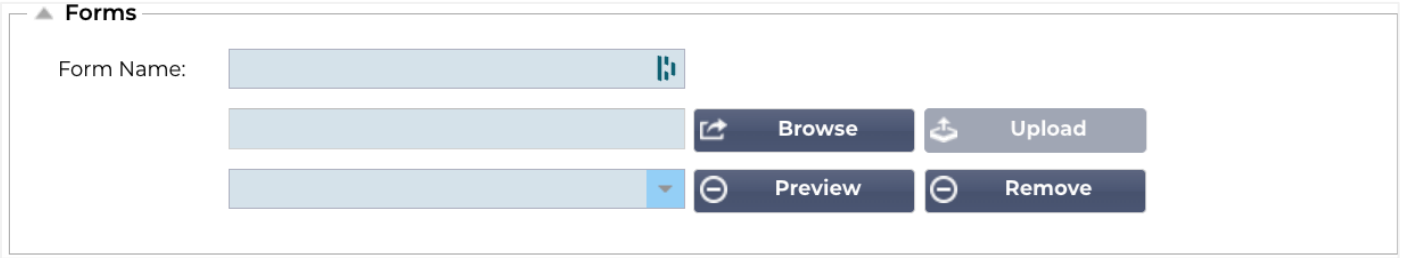
Campo	Descrição
Nome	Adicione um nome adequado para a sua regra de autenticação.
Descrição	Acrescentar uma descrição adequada.
Domínio de raiz	Deve ser deixado em branco, a menos que necessite de um início de sessão único em subdomínios.
Servidor de autenticação	Esta é uma caixa pendente que contém os servidores que configurou.
Autenticação de cliente:	Escolha o valor adequado às suas necessidades: Básico (401) - Este método utiliza o método de autenticação 401 padrão Forms (Formulários) - esta opção apresenta o formulário predefinido do ADC ao utilizador. No formulário, pode adicionar uma mensagem. Pode selecionar um formulário que tenha carregado utilizando a secção abaixo.
Autenticação do servidor	Selecionar o valor adequado. Nenhum - se o servidor não tiver qualquer autenticação existente, selecione esta definição. Esta definição significa que pode adicionar capacidades de autenticação a um servidor que anteriormente não tinha nenhuma. Básico - se o seu servidor tiver a autenticação básica (401) activada, selecione BÁSICO. NTLM - se o servidor tiver a autenticação NTLM activada, selecione NTLM.
Formulário	Selecionar o valor adequado Predefinição - Ao selecionar esta opção, o ADC utiliza a sua forma incorporada. Personalizado - pode adicionar um formulário concebido por si e seleccioná-lo aqui.
Mensagem	Adicionar uma mensagem pessoal ao formulário.
Tempo limite	Adicione um tempo limite à regra, após o qual o utilizador terá de se autenticar novamente. Nota: a definição de Tempo limite só é válida para a autenticação baseada em formulários.

Se pretender fornecer um início de sessão único aos utilizadores, preencha o campo Domínio raiz com o seu domínio. Neste exemplo, mycompany.com. Podemos agora ter vários serviços que utilizarão edgenexus.io como domínio de raiz, e o utilizador só terá de iniciar sessão uma vez. Se considerarmos os seguintes serviços:

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

Estes serviços podem residir num VIP ou podem ser distribuídos por 3 VIPs. A um utilizador que aceda a usercentral.mycompany.com pela primeira vez será apresentado um formulário que lhe pede para iniciar sessão, dependendo da regra de autenticação utilizada. O mesmo utilizador pode depois ligar-se a App Store.mycompany.com e será autenticado automaticamente pelo ADC. Pode definir o tempo limite, que forçará a autenticação quando este período de inatividade for atingido.

Formulários



Esta secção permite-lhe carregar um formulário personalizado.

Como criar o seu formulário personalizado

Embora o formulário básico fornecido pela ADC seja suficiente para a maioria das finalidades, haverá ocasiões em que as empresas pretendem apresentar a sua própria identidade ao utilizador. Nestes casos, pode criar um formulário personalizado que será apresentado aos utilizadores para preenchimento. Este formulário deve estar no formato HTM ou HTML.

Opção	Descrição
Nome	nome do formulário = loginform ação = %JNURL% Método = POST
Nome de utilizador	Sintaxe: name = "JNUSER"
Palavra-passe:	name="JNPASS"
Mensagem facultativa1:	%JNMESSAGE%
Mensagem facultativa2:	%JNAUTHMESSAGE%
Imagens	Se pretender adicionar uma imagem, adicione-a em linha utilizando a codificação Base64.

Exemplo de código html de um formulário muito básico e simples

```
<HTML>
<HEAD>
<TITLE>AMOSTRA DE FORMULÁRIO DE AUTENTICAÇÃO</TITLE>
</HEAD>
<BODY>
%JNMESSAGE%<br>
<form name="loginform" action="%JNURL%" method="post"> USUÁRIO: <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>
```

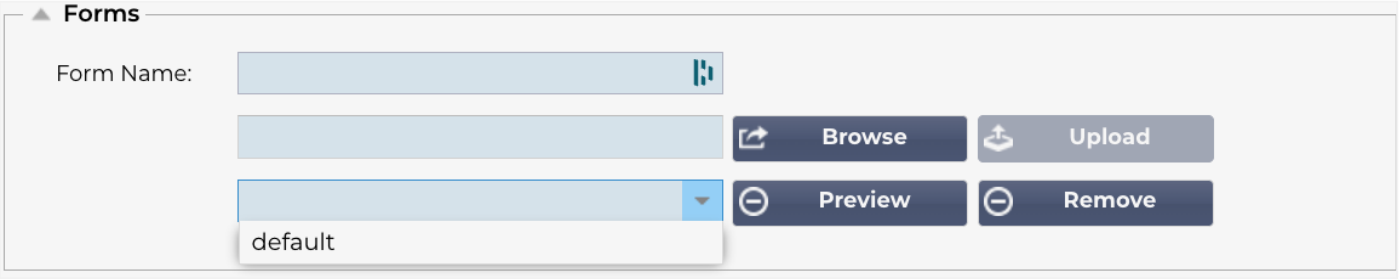
Adicionar um formulário personalizado

Depois de ter criado um formulário personalizado, pode adicioná-lo utilizando a secção Formulários.

1. Escolha um nome para o seu formulário
2. Procurar localmente o seu formulário

3. Clique em Carregar

Pré-visualização do formulário personalizado



Para ver o formulário personalizado que acabou de carregar, selecione-o e clique em Pré-visualizar. Também pode utilizar esta secção para eliminar formulários que já não são necessários

Nota: Quando utiliza produtos de filtragem de cookies, como o AdGuard, pode receber uma mensagem de erro 404. Coloque o endereço IP do ADC na lista de permissões para evitar isso.

Cache

O ADC é capaz de armazenar dados em cache na sua memória interna e melhora a prestação de serviços Web. As definições que gerem esta funcionalidade são apresentadas nesta secção.

Definições globais de cache

Tamanho máximo da cache (MB)

Este valor determina a RAM máxima que a Cache pode consumir. A Cache ADC é uma cache na memória que também é periodicamente descarregada para o meio de armazenamento para manter a persistência da cache após reinícios, reinicializações e operações de encerramento. Esta funcionalidade significa que o tamanho máximo da cache deve caber no espaço de memória do dispositivo (em vez de no espaço do disco) e não deve ser superior a metade da memória disponível.

Tamanho pretendido da cache (MB)

Este valor indica a RAM óptima para a qual a Cache será cortada. Enquanto o tamanho máximo da cache representa o limite superior absoluto da Cache, o tamanho desejado da cache pretende ser o tamanho ótimo que a Cache deve tentar atingir sempre que é feita uma verificação automática ou manual do tamanho da cache. O intervalo entre o tamanho máximo e o tamanho desejado da cache existe para acomodar a chegada e a sobreposição de novos conteúdos entre as verificações periódicas do tamanho da cache para eliminar o conteúdo expirado. Mais uma vez, pode ser mais eficaz aceitar o valor predefinido (30 MB) e rever periodicamente o tamanho da cache em "Monitorizar -> Estatísticas" para um dimensionamento adequado.

Tempo de cache predefinido (D/HH:MM)

O valor introduzido aqui representa a vida útil do conteúdo sem um valor de expiração explícito. O tempo de cache predefinido é o período durante o qual o conteúdo sem uma diretiva "no-store" ou um tempo de expiração explícito no cabeçalho de tráfego é armazenado.

A entrada de campo assume a forma "D/HH:MM" - por isso, uma entrada de "1/01:01" (a predefinição é 1/00:00) significa que o ADC guardará o conteúdo durante um dia, "01:00" durante uma hora e "00:01" durante um minuto.

Códigos de resposta HTTP armazenáveis em cache

Um dos conjuntos de dados armazenados em cache são as respostas HTTP. Os códigos de resposta HTTP que são armazenados em cache são:

- 200 - Resposta padrão para pedidos HTTP bem sucedidos
- 203 - Os cabeçalhos não são definitivos, mas são recolhidos a partir de uma cópia local ou de terceiros
- 301 - O recurso solicitado foi atribuído a um novo URL permanente

- 304 - Não foi modificado desde o último pedido e deve ser utilizada uma cópia armazenada localmente em cache
- 410 - O recurso já não está disponível no servidor e não é conhecido nenhum endereço de reencaminhamento

Este campo deve ser editado com cuidado, uma vez que os códigos de resposta mais comuns que podem ser armazenados em cache já estão listados.

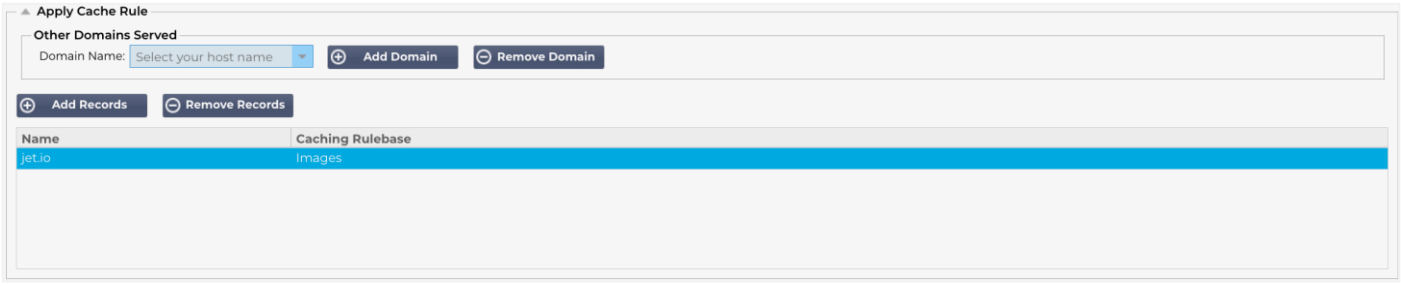
Temporizador de verificação da cache (D/HH:MM)

Esta definição determina o intervalo de tempo entre as operações de corte da cache.

Contagem de preenchimento de cache

Esta definição é um recurso auxiliar que ajuda a preencher a cache quando é detectado um determinado número de 304.

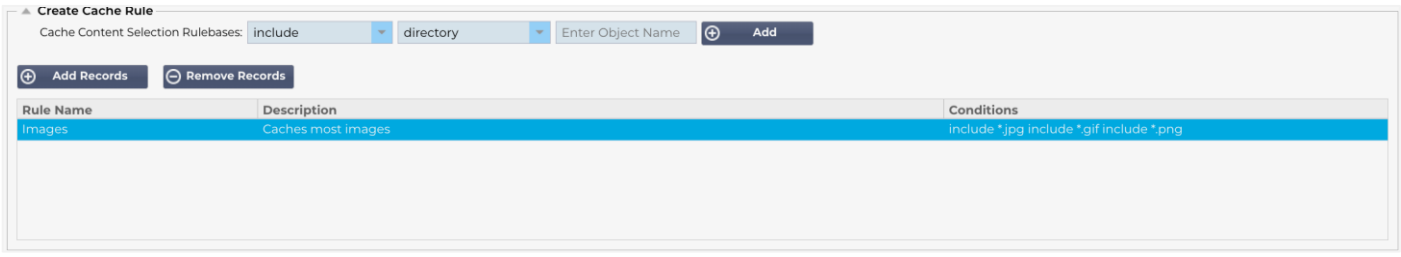
Aplicar regra de cache



Esta secção permite-lhe aplicar uma regra de cache a um domínio:

- Adicione o domínio manualmente com o botão Adicionar registos. Tem de utilizar um nome de domínio totalmente qualificado ou um endereço IP em notação decimal com pontos. Exemplo: www.mycompany.com ou 192.168.3.1:80
- Clique na seta do menu suspenso e escolha o seu domínio na lista
- A lista será preenchida desde que o tráfego tenha passado por um serviço virtual e uma estratégia de cache tenha sido aplicada ao serviço virtual
- Escolha a sua regra de cache fazendo duplo clique na coluna Caching Rulebase e selecionando-a na lista

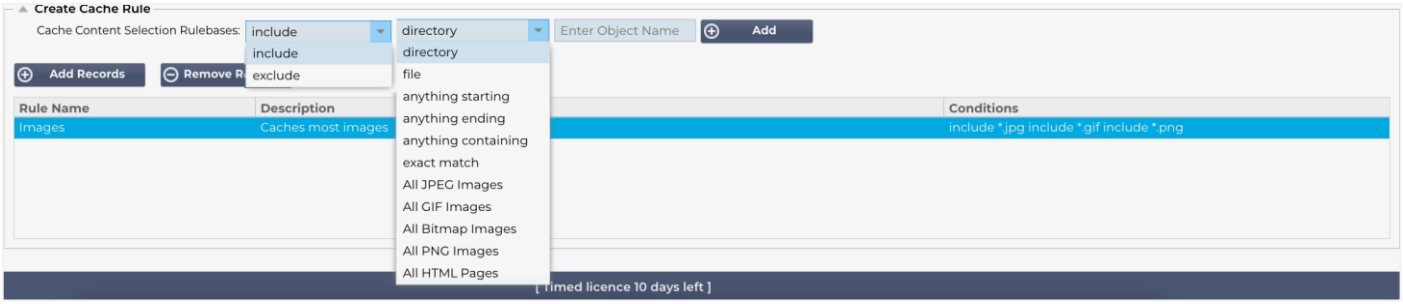
Criar regra de cache



Esta secção permite-lhe criar várias regras de cache diferentes que podem ser aplicadas a um domínio:

- Clique em Adicionar registos e atribua um nome e uma descrição à sua regra
- Pode introduzir as condições manualmente ou utilizar a opção Adicionar condição

Para adicionar uma condição utilizando a Base de regras de seleção:



- Selecione Incluir ou Excluir.
- Escolha um critério de seleção, por exemplo, Todas as imagens JPEG
- Clique no símbolo + Adicionar.
- Verá que 'include *.jpg' foi agora adicionado às condições.
- Pode adicionar mais condições. Se optar por fazer isto manualmente, tem de adicionar cada condição numa NOVA linha. Tenha em atenção que as suas regras serão apresentadas na mesma linha até clicar na caixa Condições e, em seguida, serão apresentadas numa linha separada.

flightPATH

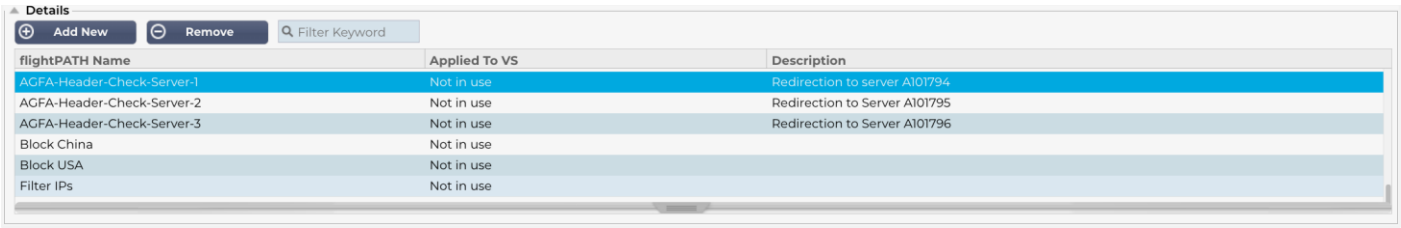
O flightPATH é a tecnologia de gestão de tráfego integrada no ADC e permite a inspeção do tráfego HTTP e HTTPS em tempo real e a realização de acções com base nas condições.

Para utilizar as regras flightPATH, estas devem ser aplicadas a um Serviço Virtual utilizando o separador flightPATH na secção Servidores reais.

Uma regra de trajetória de voo é composta por quatro elementos:

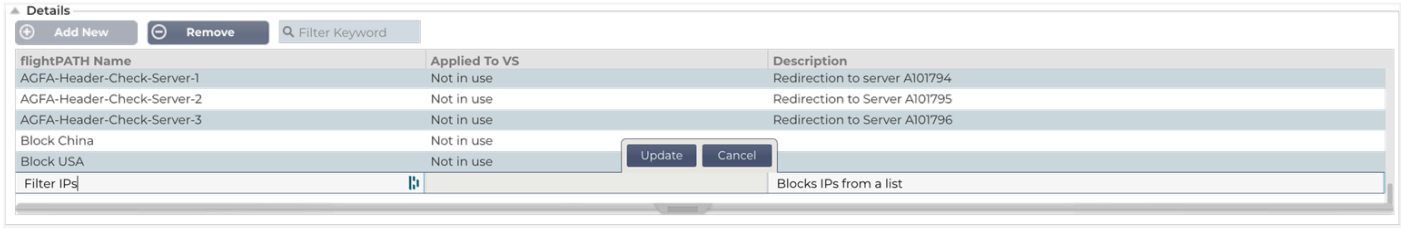
1. Details, onde se define o nome do flightPATH e o serviço ao qual está ligado.
2. Condição(ões) que pode(m) ser definida(s) para que a regra seja acionada.
3. Avaliação que permite a definição de variáveis que podem ser utilizadas nas Acções.
4. Acções que são utilizadas para gerir o que deve acontecer quando as condições são cumpridas.

Detalhes



A secção de detalhes mostra as regras flightPATH disponíveis. Pode adicionar novas regras flightPATH e remover as definidas a partir desta secção.

Adição de uma nova regra flightPATH



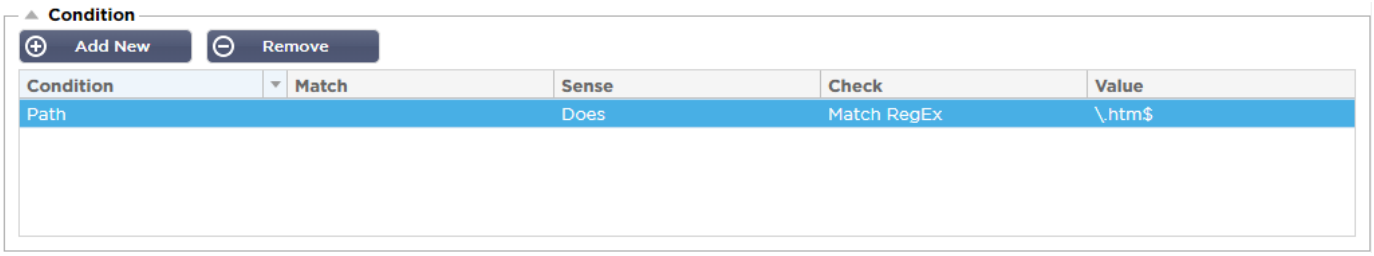
Campo	Descrição
Nome do FlightPATH	Este campo é para o nome da regra flightPATH. O nome fornecido aqui aparece e é referenciado noutras partes do ADC.
Aplicado a VS	Esta coluna é só de leitura e mostra o VIP ao qual a regra flightPATH é aplicada.
Descrição	Valor que representa uma descrição fornecida para efeitos de legibilidade.

Passos para adicionar uma regra flightPATH

1. Primeiro, clique no botão Adicionar novo localizado na secção Detalhes.
2. Introduza um nome para a sua regra. Exemplo Auth2
3. Introduza uma descrição da sua regra
4. Quando a regra tiver sido aplicada a um serviço, verá a coluna Aplicado a ser preenchida automaticamente com um endereço IP e um valor de porta
5. Não se esqueça de premir o botão Atualizar para guardar as suas alterações ou, se cometer um erro, basta premir Cancelar para voltar ao estado anterior.

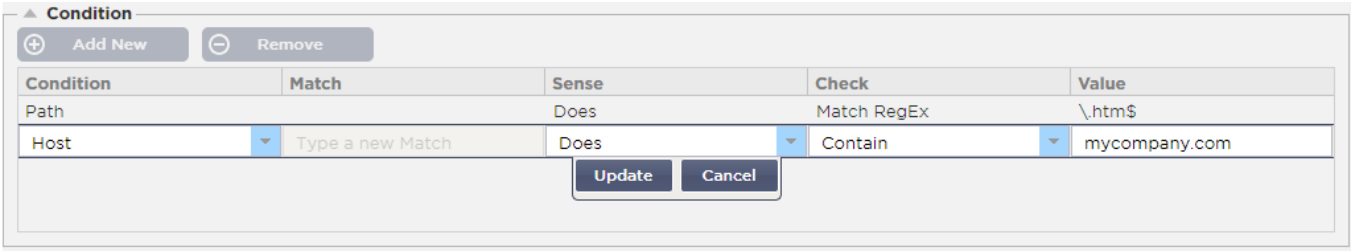
Estado

Uma regra flightPATH pode ter qualquer número de condições. As condições funcionam numa base **AND**, o que lhe permite definir a condição em que a ação é desencadeada. Se pretender utilizar uma condição **OR**, crie regras flightPATH adicionais e aplique-as ao VIP pela ordem correta.



Também pode utilizar RegEx selecionando Match RegEx no campo Check e o valor RegEx no campo Value. A inclusão da avaliação RegEx alarga tremendamente a capacidade do flightPATH.

Criar uma nova condição flightPATH



Em primeiro lugar, é necessário selecionar um valor na coluna Condição.

Fornecemos várias condições no menu suspenso e cobrimos todos os cenários previstos. Quando forem adicionadas novas condições, estas estarão disponíveis através das actualizações do Jetpack.

As opções disponíveis são:

CONDIÇÃO	DESCRIÇÃO	EXEMPLO
<form>	Os formulários HTML são utilizados para transmitir dados a um servidor	Exemplo "o formulário não tem comprimento 0"
Localização GEO	Compara o endereço IP de origem com os códigos de país ISO 3166	A localização GEO é igual a GB, OU a localização GEO é igual a Alemanha
Anfitrião	Anfitrião extraído do URL	www.mywebsite.com ou 192.168.1.1
Língua	Idioma extraído do cabeçalho HTTP do idioma	Esta condição produzirá um menu suspenso com uma lista de idiomas
Método	Lista pendente de métodos HTTP	Menu suspenso que inclui GET, POST, etc
Origem IP	Se o proxy a montante suportar X-Forwarded-for (XFF), utilizará o verdadeiro endereço de origem	IP do cliente. Ele também pode usar vários IPs ou sub-redes. 10\.1\.2\.* é a sub-rede 10.1.2.0 /24 10\.1\.2\.3|10\.1\.2\.4 Use | para vários IPs
Caminho	Caminho do sítio Web	/mywebsite/index.asp
POST	Método de pedido POST	Verificar os dados que estão a ser carregados num sítio Web
Consulta	Nome e valor de uma consulta e pode aceitar o nome da consulta ou também um valor	"Best=jetNEXUS" Em que a correspondência é Best e o valor é edgeNEXUS

Cadeia de caracteres de consulta	Toda a cadeia de consulta após o carácter ?	
Pedir cookie	Nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho do pedido	Qualquer cabeçalho HTTP	Referenciador, User-Agent, De, Data
Versão de pedido	A versão HTTP	HTTP/1.0 OU HTTP/1.1
Corpo da resposta	Uma cadeia definida pelo utilizador no corpo da resposta	Servidor UP
Código de resposta	O código HTTP da resposta	200 OK, 304 Não Modificado
Biscoito de resposta	O nome de um cookie enviado pelo servidor	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho de resposta	Qualquer cabeçalho HTTP	Referenciador, User-Agent, De, Data
Versão de resposta	A versão HTTP enviada pelo servidor	HTTP/1.0 OU HTTP/1.1
Fonte IP	O IP de origem, o IP do servidor proxy ou algum outro endereço IP agregado	IP do cliente, IP do proxy, IP da firewall. Também pode usar vários IPs e sub-redes. Os pontos devem ser escapados, pois são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Jogo

O campo Correspondência pode ser um menu pendente ou um valor de texto e é definível consoante o valor no campo Condição. Por exemplo, se a Condição for definida como Host, o campo Correspondência não estará disponível. Se a Condição estiver definida como <form>, o campo Corresponder é apresentado como um campo de texto e, se a Condição for POST, o campo Corresponder é apresentado como um drop-down que contém valores pertinentes.

As opções disponíveis são:

COMBINAÇÃO	DESCRIÇÃO	EXEMPLO
Aceitar	Tipos de conteúdo aceitáveis	Aceitar: text/plain
Aceitar codificação	Codificações aceitáveis	Aceitar codificação: <compress | gzip | deflate | sdch | identity>
Aceitar-Língua	Línguas aceitáveis para a resposta	Accept-Language: en-US
Aceitar intervalos	Que tipos de intervalo de conteúdo parcial este servidor suporta	Accept-Ranges: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básica QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carregar-até	Contém informações contabilísticas relativas aos custos de aplicação do método solicitado	
Content-Encoding	O tipo de codificação utilizado	Content-Encoding: gzip
Comprimento do conteúdo	O comprimento do corpo da resposta em octetos (bytes de 8 bits)	Content-Length: 348

Tipo de conteúdo	O tipo mime do corpo do pedido (utilizado com pedidos POST e PUT)	Content-Type: application/x-www-form-urlencoded
Biscoito	Um cookie HTTP previamente enviado pelo servidor com Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Date = "Date" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, frequentemente um resumo de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de correio eletrónico do utilizador que faz o pedido	De: user@example.com
Se-Modificado-Desde	Permite que seja devolvido um 304 Not Modified se o conteúdo não for alterado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificação	A data da última modificação do objeto pedido, no formato RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Implementação: Cabeçalhos específicos que podem ter vários efeitos em qualquer ponto da cadeia pedido-resposta.	Pragma: no-cache
Referenciador	Endereço da página Web anterior a partir da qual se seguiu uma ligação para a página atualmente solicitada	Referenciador: HTTP://www.edgenexus.io
Servidor	Um nome para o servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	Um cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente do utilizador	A cadeia do agente do utilizador do agente do utilizador	User-Agent: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variar	Diz aos proxies a jusante como fazer corresponder os cabeçalhos de pedidos futuros para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova do servidor de origem	Vary: User-Agent
X-Powered-By	Especifica a tecnologia (por exemplo, ASP.NET, PHP, JBoss) que suporta a aplicação Web	X-Powered-By: PHP/5.4.0

Sentido

O campo Sentido é um campo booleano pendente e contém as opções Faz ou Não faz.

Verificar

O campo Verificar permite a definição de valores de controlo em relação à Condição.

As opções disponíveis são: Contain, End, Equal, Exist, Have Length, Match RegEx, Match List, Start, Exceed Length

VERIFICAR	DESCRIÇÃO	EXEMPLO
Existir	Não se preocupa com o pormenor da condição, apenas com o facto de existir ou não existir	Host> Does> Exist
Início	A cadeia começa com o valor	Caminho> Does> Start> /secure
Fim	A cadeia termina com o valor	Caminho> Does> End - .jpg

Conter	A cadeia de caracteres contém efetivamente o valor	Request Header> Accept> Does> Contain> image
Igual	A cadeia de caracteres é igual ao valor	Anfitrião> Does> Equal> www.edgenexus.io
Ter comprimento	A cadeia tem um comprimento do valor	Anfitrião> O> tem comprimento> 16 www.edgenexus.io = VERDADEIRO www.edgenexus.com = FALSO
Corresponder RegEx	Permite-lhe introduzir uma expressão regular completa compatível com Perl	IP de origem> Does> Match Regex
Lista de jogos	Permite-lhe fazer corresponder o valor a uma lista de valores. Isso é útil quando há, digamos, endereços IP específicos que precisam ser comparados. Os valores são separados por vírgulas (,) ou pip (|).	Source IP> Does > Match List > 10.10.10.1, 10.10.10.2, 10.10.10.3 etc
Exceder o comprimento	Permite-lhe verificar se o valor excede o comprimento especificado.	Caminho > Faz > Excede o comprimento > 200

Passos para adicionar uma condição

Adicionar uma nova condição flightPATH é muito fácil. Um exemplo é mostrado acima.

1. Clique no botão Adicionar novo na área Condição.
2. Selecione uma condição na caixa pendente. Tomemos como exemplo o Anfitrião. Também pode escrever no campo, e o ADC mostrará o valor numa lista pendente.
3. Escolha um Sentido. Por exemplo, Será que
4. Selecionar uma verificação. Por exemplo, Conter
5. Escolha um valor. Por exemplo, mycompany.com

O exemplo acima mostra que existem duas condições que têm de ser VERDADEIRAS para que a regra seja concluída

- A primeira é verificar se o objeto pedido é uma imagem
- O segundo verifica se o anfitrião no URL é www.imagepool.com

Avaliação

A capacidade de adicionar variáveis definíveis é uma capacidade atraente. Outros ADCs oferecem essa capacidade usando opções de script ou de linha de comando que não são ideais para qualquer pessoa. O EdgeADC permite-lhe definir qualquer número de variáveis através de uma GUI fácil de utilizar, como se mostra e descreve abaixo.

A definição da variável flightPATH inclui quatro entradas que precisam de ser efectuadas.

- Variável - este é o nome da variável
- Fonte - uma lista pendente de possíveis pontos de origem
- Detalhe - selecione valores a partir de uma lista pendente ou digite-os manualmente.
- Valor - o valor que a variável contém e pode ser um valor alfanumérico ou um RegEx para ajuste fino.

Variáveis incorporadas:

As variáveis incorporadas já foram codificadas, pelo que não é necessário criar uma entrada de análise para elas.

Pode utilizar qualquer uma das variáveis listadas abaixo na secção Ação.

- $sourceip$ - O endereço IP de origem do pedido
- $sourceport$ - A porta de origem que foi utilizada
- $clientip$ - O endereço IP do cliente
- $clientport$ - A porta utilizada pelo cliente
- $host$ - O anfitrião indicado no pedido
- $method$ - O método utilizado: GET, POST, etc.
- $path$ - O caminho especificado no pedido
- $querystring$ - A querystring utilizada no pedido
- $version$ - A versão do pedido HTTP no REQUEST (atualmente só são permitidas as versões 1 e 1.1).
- $resp$ - A RESPOSTA do servidor, por exemplo, 200OK, 404, etc.
- $geolocation$ - A localização GEO de onde o pedido foi originado.

ACÇÃO	ALVO
Ação = Redirecionar 302	Destino = HTTPs://$host$/404.html
Ação = Registo	Target = Um cliente de $sourceip$:$sourceport$ acabou de efetuar um pedido de página $path$

Explicação:

- Um cliente que aceda a uma página que não existe seria normalmente confrontado com a página de erro 404 do browser
- Em vez disso, o utilizador é redireccionado para o nome de anfitrião original que utilizou, mas o caminho incorreto é substituído por 404.html
- É adicionada uma entrada ao Syslog que diz: "Um cliente de 154.3.22.14:3454 acabou de pedir a página wrong.html".

Ação

A fase seguinte do processo consiste em adicionar uma ação associada à regra e condição flightPATH.

Neste exemplo, queremos reescrever a parte do caminho do URL para refletir o URL digitado pelo utilizador.

- Clique em Adicionar novo
- Escolha Reescrever caminho no menu suspenso Ação
- No campo Destino, digite $path$/myimages
- Clique em Atualizar

Esta ação irá adicionar /myimages ao caminho, pelo que o URL final passa a ser www.imagepool.com/myimages

Ação	Descrição	Exemplo
Adicionar cookie de pedido	Adicionar cookie de pedido detalhado na secção Destino com valor na secção Dados	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar cabeçalho do pedido	Adicionar um cabeçalho de pedido do tipo Target com valor na secção Data	Target= Aceitar Dados= imagem/png
Adicionar cookie de resposta	Adicionar o cookie de resposta detalhado na secção Destino com o valor na secção Dados	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar cabeçalho de resposta	Adicionar cabeçalho de pedido detalhado na secção Destino com valor na secção Dados	Target= Cache-Control Data= max-age=8888888
Corpo Substituir tudo	Pesquisar o corpo da resposta e substituir todas as instâncias	Target= http:// (Cadeia de pesquisa) Data= https:// (Cadeia de substituição)
Corpo Substituir primeiro	Pesquisar o corpo da resposta e substituir apenas a primeira instância	Target= http:// (Cadeia de pesquisa) Data= https:// (Cadeia de substituição)
Corpo Substituir Último	Pesquisar o corpo da resposta e substituir apenas a última instância	Target= http:// (Cadeia de pesquisa) Data= https:// (Cadeia de substituição)
Gota	Isto fará com que a ligação seja interrompida	Objetivo= N/A Dados= N/A
Correio eletrónico	Enviará uma mensagem de correio eletrónico para o endereço configurado em Eventos de correio eletrónico. Pode utilizar uma variável como endereço ou mensagem	Target= "flightPATH enviou este evento por correio eletrónico" Data= N/A
Evento de registo	Isto irá registar um evento no registo do sistema	Target= "flightPATH has logged this in syslog" Data= N/A
Redirecionar 301	Isto irá emitir um redireccionamento permanente	Objetivo= http://www.edgenexus.io Dados= N/A
Redirecionar 302	Isto irá emitir um redireccionamento temporário	Objetivo= http://www.edgenexus.io Dados= N/A

Remover cookie de pedido	Remover o cookie de pedido detalhado na secção Destino	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remover o cabeçalho do pedido	Remover o cabeçalho do pedido detalhado na secção Destino	Destino=Dados do servidor=N/A
Remover resposta	Remover o cookie de resposta detalhado na secção Alvo Cookie	Objetivo=jnAccel
Remover resposta	Remover o cabeçalho de resposta detalhado na secção Destino Cabeçalho	Alvo= Etag Dados= N/A
Substituir o cookie de pedido	Substituir o cookie de pedido detalhado na secção Destino pelo valor na secção Dados	Target= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho do pedido	Substituir o cabeçalho do pedido no Target pelo valor Data	Target= Connection Data= keep-alive
Substituir	Substituir o cookie de resposta detalhado na secção Destino pelo valor na secção Dados Cookie	Target=jnAccel=afYfn1CDqqCDqCVii Date=MSWSMAN=afYfn1CDqqCDqCVii
Substituir Resposta	Substituir o cabeçalho de resposta detalhado na secção Destino pelo valor na secção Dados Cabeçalho	Alvo= Dados do servidor= Retidos por razões de segurança
Reescrever caminho	Isto permitir-lhe-á redirecionar o pedido para um novo URL com base na condição	Target= /test/path/index.html$querystring$ Data= N/A
Utilizar um servidor seguro	Selecionar o servidor seguro ou serviço virtual a utilizar	Target=192.168.101:443 Data=N/A
Utilizar	Selecionar o servidor ou serviço virtual a utilizar	Alvo= 192.168.101:80 Dados= N/A
Encriptar cookie	Isto irá encriptar os cookies em 3DES e depois codificá-los em base64	Target= Introduzir o nome do cookie a ser encriptado, pode utilizar o * como um wild card no final Data= Introduzir uma frase-passe para a encriptação

Um cenário de regra flightPATH

Um cliente tem um sítio de comércio eletrónico e está a ter problemas com o bloqueio de cookies pelas versões mais recentes de um browser.

O cliente rastreia os problemas e descobre que a causa principal é a falta de etiquetagem "segura" e "no mesmo sítio" para os cookies em questão.

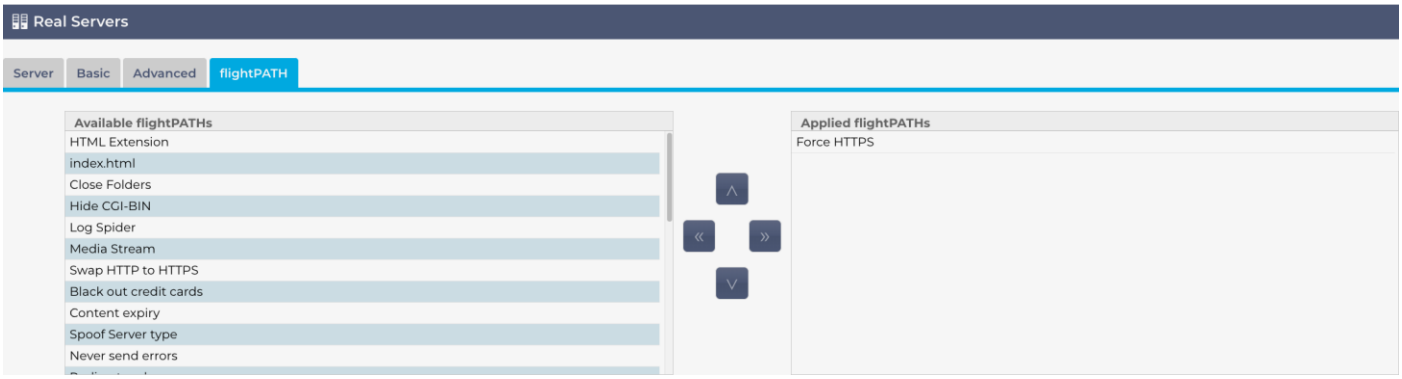
Vejamos como o flightPATH pode ajudar.

- Temos um cookie com o nome 'wp_woocommerce_session_97929973749972642'
- O nome do cookie é "wp_woocommerce_session_" com um valor de ID único aleatório de "97929973749972642" gerado pelo sistema de comércio eletrónico.
- As etiquetas para as etiquetas "same-site" e "secure" parecem estar em branco, pelo que o cookie é bloqueado pelas novas restrições de segurança do browser.
- Para evitar que isso aconteça, podemos criar as seguintes regras flightPATH.
- **flightPATH Regra para o ID da sessão**
    - **Condição**:
      Deixar em branco
    - **Avaliação**:
      Variável = $variable_1$
      Fonte = cookie de resposta
      Detalhe = wp_woocommerce_session_*
    - Ação
      Ação = Substituir o cookie de resposta
      Target = wp_woocommerce_session_*
      Dados = $variable_1$
- **Regra flightPATH para etiquetas**
    - **Condição:**
      Condição = Cookie de resposta
      Correspondência = woocommerce_cart_hash
      Sense = Faz
      Verificar = Existe
      Valor = Deixar em branco
    - **Avaliação:**
      Variável = $variavel_2$
      Fonte = Cookie de resposta
      Detalhe = woocommerce_cart_hash
      Valor = Deixar em branco
    - **Ação:**
      Ação = Substituir o cookie de resposta
      Target = woocommerce_cart_hash
      Dados = $variable_2$,SameSite=None,Secure

Agora aplica as regras ao(s) serviço(s) virtual(ais) que as requerem.

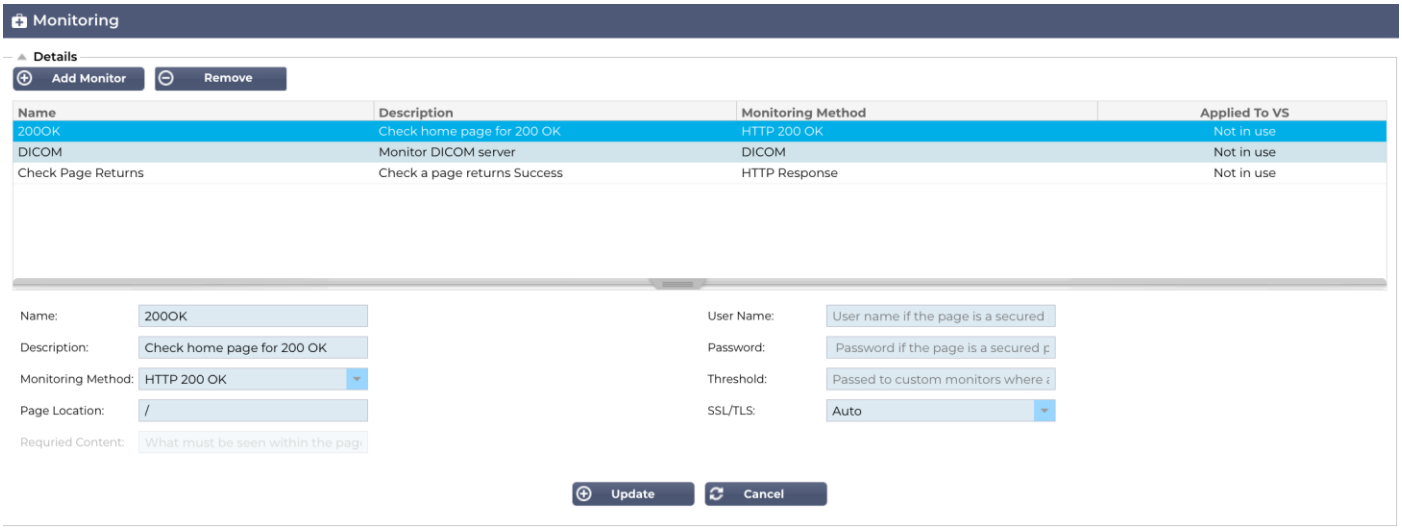
Aplicar a regra flightPATH

A aplicação de qualquer regra flightPATH é feita no separador flightPATH de cada VIP/VS.



- Navegue para Serviços > Serviços IP e escolha o VIP ao qual pretende atribuir a regra flightPATH.
- É apresentada a lista de servidores reais abaixo
- Clique no separador flightPATH
- Selecione a regra flightPATH que configurou ou uma das regras pré-construídas suportadas. Pode selecionar várias regras flightPATH, se necessário.
- Arraste e largue o conjunto selecionado para a secção Applied flightPATHs ou clique no botão de seta >>.
- A regra será movida para o lado direito e aplicada automaticamente.

Monitores de servidor reais



A monitorização de servidores reais é importante num cenário de equilíbrio de carga para detetar e responder a problemas do servidor, garantir uma distribuição de carga equilibrada, otimizar a utilização de recursos, dar prioridade a serviços críticos e identificar e resolver vulnerabilidades de software.

A página Library> Real Server Monitors permite-lhe adicionar, visualizar e editar a monitorização personalizada. Estes são os "controlos de saúde" do servidor da camada 7 e selecione-os no campo Monitorização do servidor no separador Básico do serviço virtual que definir.

Tipos de monitores de servidores reais

Existem vários Monitores de Servidor Real disponíveis, e a tabela abaixo explica-os. É claro que é possível escrever monitores adicionais usando PERL.

Método de controlo	Descrição	Exemplo
HTTP 200 OK	É estabelecida uma ligação TCP com o Servidor Real. Depois de estabelecida a ligação, é enviado um breve pedido HTTP para o Servidor Real. Quando a resposta é recebida, é verificada a existência da cadeia "200 OK". Se esta estiver presente, o servidor é considerado operacional. Tenha em atenção que a utilização deste monitor vai buscar a página inteira com os conteúdos. Este método de monitorização só pode realmente ser utilizado com tipos de serviço HTTP e HTTP Acelerado. No entanto, se um tipo de serviço da camada 4 estiver a ser utilizado para um servidor HTTP, pode ainda ser utilizado se o SSL não estiver a ser utilizado no servidor real ou tratado adequadamente pela funcionalidade "Content SSL".	**Pedido** GET / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:55:47 GMT Content-Length: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head>

		<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- corpo { cor:#FFFFFF; ... </body> </html>
Cabeçalho HTTP 200	É efectuada uma ligação TCP ao Servidor Real com o campo PATH a especificar a localização a ser verificada. A parte do cabeçalho da resposta é obtida do servidor, com o conteúdo descartado. A resposta é verificada quanto a 200 OK. Se estiver presente, o servidor é considerado operacional. Tenha em atenção que a utilização deste monitor apenas obtém a parte da cabeça. Este método de monitorização só pode realmente ser utilizado com tipos de serviço HTTP e HTTP Acelerado. No entanto, se um tipo de serviço da camada 4 estiver a ser utilizado para um servidor HTTP, pode ainda ser utilizado se o SSL não estiver a ser utilizado no servidor real ou tratado adequadamente pela funcionalidade "Content SSL".	**Pedido** HEAD / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Tue, 13 Jul 2021 15:49:19 GMT
Opções HTTP 200	É estabelecida uma ligação TCP com o Servidor Real e é efectuado um pedido de Opções. As opções são devolvidas e verificadas quanto ao conteúdo 200 OK. Se o conteúdo 200 OK for encontrado, considera-se que o servidor está disponível.	**Pedido** OPÇÕES / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Permitir: OPTIONS, TRACE, GET, HEAD, POST Servidor: Microsoft-IIS/10.0 Público: OPÇÕES, RASTREAR, OBTER, CABEÇA, POSTAR Data: Tue, 13 Jul 2021 16:23:39 GMT Content-Length: 0
Cabeça HTTP	O monitor HTTP Head permite-nos verificar se existe um valor específico na parte Head do fluxo HTTP. Podemos inserir um Caminho e uma Resposta obrigatória nos campos apropriados e, em seguida, verificar se há esse valor na resposta. Se o valor da resposta requerida for encontrado no cabeçalho, considera-se que o servidor está ativo e disponível. Também podemos utilizá-lo em páginas especialmente protegidas que necessitem de um nome de utilizador e de uma palavra-passe. Desta forma, o resultado do monitor pode ser considerado exato.	**Pedido** HEAD /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Content-Length: 1364 Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes

	Por exemplo, fornecer **/ispagethere.html** e valores **200 OK** nos campos Caminho e Resposta obrigatória devolverá um resultado bem sucedido se o servidor estiver ativo, a página estiver disponível e responder ao pedido. Este método de monitorização só pode realmente ser utilizado com tipos de serviço HTTP e HTTP Acelerado. No entanto, se um tipo de serviço da camada 4 estiver a ser utilizado para um servidor HTTP, pode ainda ser utilizado se o SSL não estiver a ser utilizado no servidor real ou tratado adequadamente pela funcionalidade "Content SSL".	ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Wed, 14 Jul 2021 08:28:18 GMT
Opções HTTP	O monitor de Opções HTTP permite-lhe verificar se existe um valor específico nos dados de Opções devolvidos. Introduzimos um caminho e uma resposta obrigatória nos campos adequados e, em seguida, verificamos a resposta. Se a resposta requerida for encontrada nos dados das opções, o servidor está disponível e a funcionar. Os valores da resposta obrigatória podem ser qualquer um dos seguintes: OPTIONS, TRACE, GET, HEAD e POST. Por exemplo, fornecer **/ispagethere.html** e valores **GET** nos campos Caminho e Resposta obrigatória devolverá um resultado bem sucedido se o servidor estiver ativo, a página estiver disponível e responder ao pedido. Este método de monitorização só pode realmente ser utilizado com tipos de serviço HTTP e HTTP Acelerado. No entanto, se um tipo de serviço da camada 4 estiver a ser utilizado para um servidor HTTP, pode ainda ser utilizado se o SSL não estiver a ser utilizado no servidor real ou tratado adequadamente pela funcionalidade "Content SSL".	**Pedido** OPÇÕES /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Permitir: OPTIONS, TRACE, GET, HEAD, POST Servidor: Microsoft-IIS/10.0 Público: OPÇÕES, RASTREAR, OBTER, CABEÇA, POSTAR Data: Wed, 14 Jul 2021 09:47:27 GMT Content-Length: 0
Resposta HTTP	É efectuada uma ligação e um pedido/resposta HTTP ao Servidor Real e verificada tal como explicado nos exemplos anteriores. Mas em vez de verificar um código de resposta "200 OK", o cabeçalho da resposta HTTP é verificado quanto ao conteúdo de texto personalizado. O texto pode ser um cabeçalho completo, parte de um cabeçalho, uma linha de parte de uma página ou apenas uma palavra. Por exemplo, no exemplo mostrado à direita, especificámos **/ispagethere.htm** como o Caminho e **Microsoft-IIS** como a Resposta Necessária. Se o texto for encontrado, considera-se que o Servidor Real está a funcionar.	**Pedido** GET /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Accept-Language: en-gb User-Agent: Edgenexus-ADC/4.0 Ligação: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Content-Type: text/html Last-Modified: Wed, 31 Jan 2018 15:08:18 GMT Accept-Ranges: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Wed, 14 Jul 2021 10:07:13 GMT Content-Length: 1364

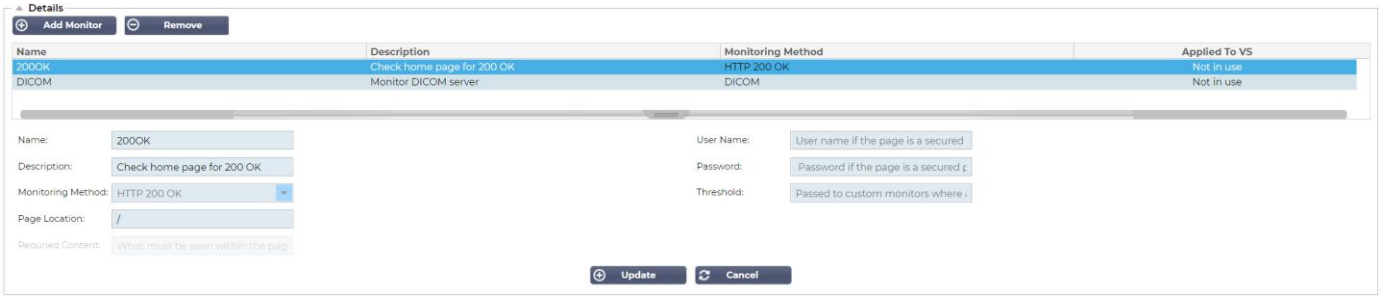
	Este método de monitorização só pode ser realmente utilizado com os tipos de serviço HTTP e HTTP acelerado. No entanto, se um Tipo de Serviço de Camada 4 estiver a ser utilizado para um servidor HTTP, poderá ainda ser utilizado se o SSL não estiver a ser utilizado no Servidor Real ou tratado adequadamente pela funcionalidade "Content SSL".	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <style type="text/css"> <!-- corpo { cor:#FFFFFF; ...
Monitor TCP multiporta	Este método é como o anterior, exceto que pode ter várias portas diferentes. O monitor só é considerado bem sucedido se todas as portas especificadas na secção de conteúdo necessário responderem corretamente.	Nome: Monitor multiporta Descrição: Monitorizar várias portas para o sucesso Localização da página: N/A Conteúdo necessário: 135,59534,59535
TCP fora de banda	O método TCP Out of Band é semelhante a um TCP Connect, exceto que pode especificar a porta que pretende monitorizar na coluna de conteúdo necessário. Normalmente, esta porta não é a mesma que a porta de tráfego e é utilizada quando se pretende associar serviços	Nome: TCP fora de banda Descrição: Monitorizar porta de tráfego/fora de banda Localização da página: N/A Conteúdo obrigatório: 555
DICOM	Enviamos um eco DICOM utilizando o valor "Source Calling" AE Title na coluna de conteúdo necessária. Também pode definir o valor do título AE "Destination Called" (Destino chamado) na secção Notes (Notas) de cada servidor. Pode encontrar a coluna Notes (Notas) na secção IP Services--Serviços virtuais--Página do servidor.	Nome: DICOM Descrição: Controlo de saúde L7 para o serviço DICOM Método de monitorização: DICOM Localização da página: N/A Conteúdo obrigatório: Valor AET
LDAPS	Este novo controlo de saúde é utilizado para verificar a saúde e a resposta de um servidor LDAP/AD.	Nome: LDAPS Descrição: Verificação do estado do servidor LDAP/AD Os parâmetros de utilização são os seguintes: **Nome de utilizador**: cn=username,cn=users,dc=domainname, dc=local **Palavra-passe**: DomainUserPassword **Conteúdo**: 200OK
SNMP v2	Este método de monitorização permite-lhe verificar o estado de disponibilidade de um servidor utilizando a resposta SNMP MIB do servidor. O valor da resposta obrigatória deve conter o nome da comunidade.	
Verificação do servidor DNS	Ao fazer o balanceamento de carga de servidores DNS, é útil verificar se o servidor responde a consultas DNS. O monitor pode ser utilizado da seguinte forma: • O campo Path (Caminho) é utilizado para o FQDN que está a consultar. Por exemplo, se pretender consultar www.edgenexus.io, introduza-o no campo Path (Caminho). • Se deixar esta opção em branco, o monitor utilizará a sua pesquisa predefinida para efetuar a consulta. • O campo Resposta obrigatória pode ser deixado em branco, e o monitor assumirá que qualquer resposta é considerada válida. Caso contrário, deve introduzir o IP esperado no campo Resposta obrigatória. Por exemplo, este pode ser 101.10.10.100. Se a consulta devolver este valor, o monitor assinala um sucesso; caso contrário, assinala uma falha.	

	Um resultado de sucesso indica que o servidor DNS que está a equilibrar a carga está operacional.

A página Monitores de servidor real está dividida em três secções.

Detalhes

A secção Detalhes é utilizada para adicionar novos monitores e remover os que não são necessários. Também é possível editar um monitor existente fazendo duplo clique sobre o mesmo.



Nome

Nome da sua escolha para o seu monitor.

Descrição

Descrição textual para este Monitor, e recomendamos que seja o mais descritiva possível.

Método de controlo

Escolha o método de monitorização na lista pendente. As opções disponíveis são:

- HTTP 200 OK
- Cabeçalho HTTP 200
- Opções HTTP 200
- Cabeça HTTP
- Opções HTTP
- Resposta HTTP
- Monitor TCP multiporta
- TCP fora de banda
- DICOM
- SNMP v2
- Verificação do servidor DNS
- LDAPS

Localização da página

URL Localização da página para um monitor HTTP. Este valor pode ser uma ligação relativa, como /pasta1/pasta2/página1.html. Também pode utilizar uma ligação absoluta em que o sítio Web está ligado ao nome do anfitrião.

Conteúdo obrigatório

Este valor contém qualquer conteúdo que o monitor precisa de detetar e utilizar. O valor aqui representado mudará consoante o método de monitorização escolhido.

Aplicado a VS

Este campo é automaticamente preenchido com o IP/Porta do Serviço Virtual ao qual o monitor é aplicado. Não será possível eliminar qualquer Monitor que tenha sido utilizado com um Serviço Virtual.

Utilizador

Alguns monitores personalizados podem utilizar este valor juntamente com o campo de palavra-passe para iniciar sessão num Servidor Real.

Palavra-passe

Alguns monitores personalizados podem utilizar este valor juntamente com o campo Utilizador para iniciar sessão num Servidor Real.

Limiar

O campo Limiar é um número inteiro geral utilizado em monitores personalizados em que é necessário um limiar, como o nível de CPU.

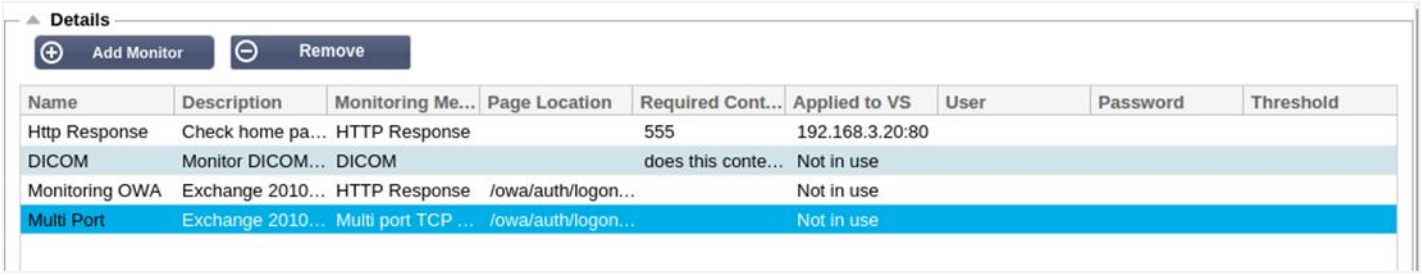
NOTA: Certifique-se de que a resposta do servidor de aplicações não é uma resposta "Chunked".

SSL/TLS

Este campo permite-lhe forçar a utilização ou não de SSL. As definições são as seguintes:

- Ligado - Isto irá forçar o SSL
- Desligado - Esta opção desactivará o SSL
- Auto - Esta opção mantém o estado atual

Exemplos do Real Server Monitor



Monitor de carregamento

Haverá muitas ocasiões em que os utilizadores desejarão criar os seus próprios monitores personalizados e esta secção permite-lhes carregá-los para o ADC.

Os monitores personalizados são escritos utilizando scripts PERL e têm uma extensão de ficheiro .pl.

- Dê um nome ao seu monitor para o poder identificar na lista Método de monitorização
- Procurar o ficheiro .pl
- Clique em Carregar novo monitor
- O seu ficheiro será carregado para a localização correta e ficará visível como um novo método de monitorização.

Monitores personalizados

Nesta secção, é possível ver os monitores personalizados carregados e removê-los se já não forem necessários.

- Clique na caixa pendente
- Selecionar o nome do monitor personalizado
- Clique em Remover
- O monitor personalizado deixará de ser visível na lista Método de monitorização

Criando um script Perl de monitor personalizado

CUIDADO: Esta secção destina-se a pessoas com experiência na utilização e escrita em Perl

Esta secção mostra-lhe os comandos que pode utilizar no seu script Perl.

O comando #Monitor-Name: é o nome usado para o Perl Script armazenado no ADC. Se não incluir esta linha, o seu script não será encontrado!

Os seguintes elementos são obrigatórios:

- #Nome-do-Monitor
- usar rigorosamente;
- aviso de utilização;

Os scripts Perl são executados num ambiente CHROOTED. Chamam frequentemente outra aplicação, como o WGET ou o CURL. Por vezes, estes precisam de ser actualizados para uma funcionalidade específica, como o SNI.

Valores dinâmicos

- my $host = $_[0]; ### IP ou nome do host (vem dos detalhes do RS ou OOB se usado)
- my $port = $_[1]; ### Porta do anfitrião (vem dos detalhes do RS ou OOB se usado)
- my $content = $_[2]; ### Conteúdo necessário das definições do monitor (o que deve ser visto na resposta)
- my $notes = $_[3]; ### notas dos detalhes do RS nos Serviços IP (utilize isto para personalizar cada monitor RS de forma única)
- my $page = $_[4]; ### localização da página nas definições do monitor
- my $user = $_[5]; ### nome de utilizador das definições do monitor
- my $password = $_[6]; ### palavra-passe das definições do monitor
- my $threshold = $_[7]; ### parâmetro de limiar das definições do monitor
- my $rsaddr = $_[8]; ### RS IP (diferente de _[0] se a monitorização for fora da banda)
- my $rsport = $_[9]; ### Porta RS (diferente de _[1] se a monitorização for fora de banda)
- my $timeout = $_[10]; ### monitorizar o tempo limite de contacto em segundos a partir de Serviços IP > Servidor Real > Avançado > Monitorização do tempo limite

Os controlos de saúde personalizados têm dois resultados

- Bem-sucedido
  Valor de retorno 1

Imprimir uma mensagem de sucesso no Syslog
Marcar o Real Server Online (desde que IN COUNT corresponda)

- Sem êxito
  Valor de retorno 2
  Imprime uma mensagem dizendo Unsuccessful para o Syslog
  Marcar o servidor real como offline (desde que a contagem de OUT coincida)

Exemplo de um monitor de saúde personalizado

```
#Nome do monitor HTTPS_SNI
usar rigorosamente:
avisos de utilização;
# O nome do monitor, tal como acima, é apresentado no menu pendente de Controlos de saúde disponíveis
# Existem 6 valores passados para este script (ver abaixo)
# O guião devolverá os seguintes valores
# 1 se o teste for bem sucedido
# 2 se o teste não for bem sucedido sub monitor
{
my Shost        = $_[0]; ### IP ou nome do anfitrião
meu Esporte     = $_[1]; ### Porta do anfitrião
my Scontent     = $_[2]; ### Conteúdo a procurar (na página Web e nos cabeçalhos HTTP)
my Snotes       = $_[3]; ### Nome do anfitrião virtual
my Spage        = $_[4]; ### A parte do URL depois do endereço do anfitrião
meu Suser       = $_[5]: ### domínio/usemame (opcional)
my Spassword    = $_[6]; ### password (opcional)
my $resolve;
meu $auth       =;
se ($port)
{
        $resolve = "$notes:$port:$host":
}
senão {
        $resolve = "$notes:$host";
}
se ($user && $password) {
        $auth = "-u $user:$password :
}
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@linhas)=~/$conteúdo/)
        {
        print "HTTPs://$notes}${page} à procura de - $content - Health check successful.\n";
        retorno(1);
        }
senão
        {
```

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

NOTA:

Monitorização personalizada - A utilização de variáveis globais não é possível. Utilizar apenas variáveis locais - variáveis definidas dentro de funções

Utilização de RegEx - Todas as expressões regulares devem utilizar uma sintaxe de declaração compatível com Perl.

Certificados SSL

Para utilizar com êxito o balanceamento de carga da camada 7 com servidores que utilizam ligações encriptadas utilizando SSL, o ADC tem de estar equipado com os certificados SSL utilizados nos servidores de destino. Este requisito é necessário para que o fluxo de dados possa ser desencriptado, examinado, gerido e depois novamente encriptado antes de ser enviado para o servidor de destino.

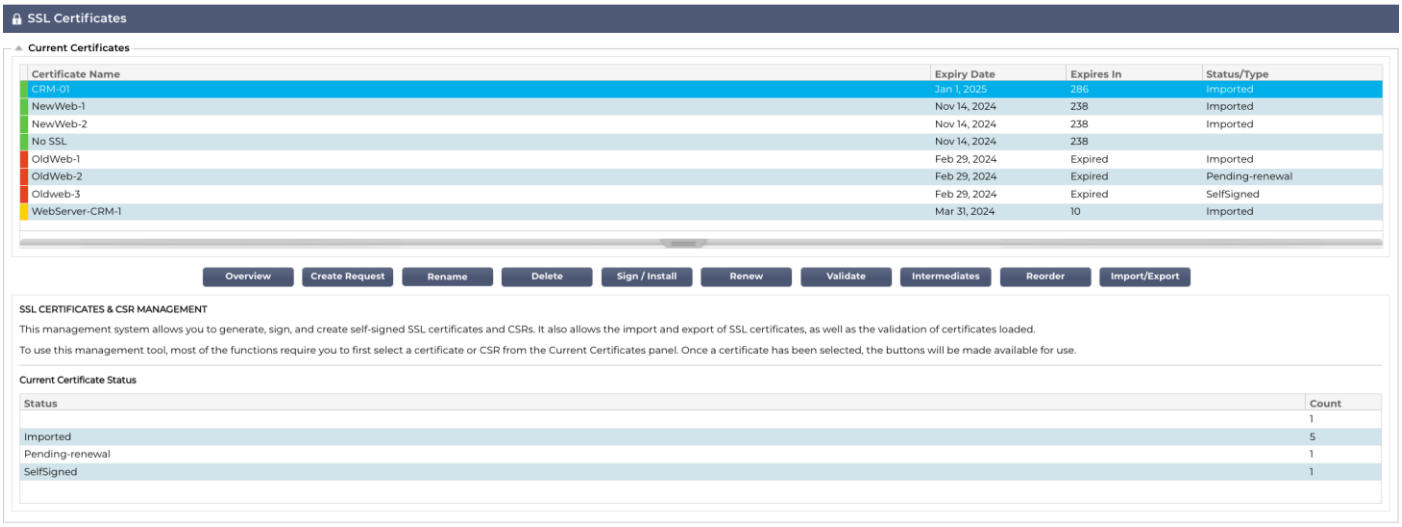
Os certificados SSL podem variar entre certificados auto-assinados que o ADC pode gerar e os certificados tradicionais (com curinga incluído) disponíveis em provedores confiáveis. Também é possível utilizar certificados assinados pelo domínio que são gerados a partir do Active Diretory.

O que é que o ADC faz com o certificado SSL?

O ADC pode efetuar regras de gestão do tráfego (flightPATH) em função do conteúdo dos dados. Esta gestão não pode ser efectuada em dados encriptados SSL. Quando o ADC tem de inspecionar os dados, precisa primeiro de os desencriptar e, para isso, precisa de ter o certificado SSL utilizado pelo servidor. Uma vez desencriptados, o ADC poderá então examinar e executar as regras flightPATH. De seguida, os dados serão novamente encriptados utilizando o certificado SSL e enviados para o servidor Real final.

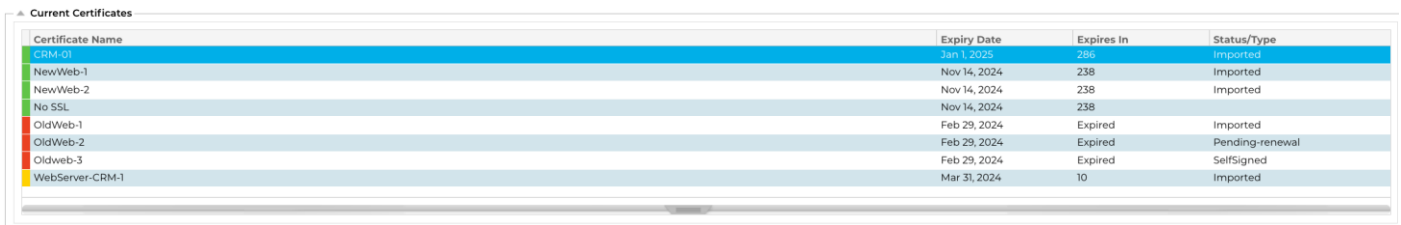
O Gestor de Configuração SSL

A versão 196X em diante apresenta um método novo e mais simples de configurar e gerir certificados SSL e Pedidos de Certificado.



Existem três secções principais no Gestor de Configuração SSL.

A área de listagem de certificados



A parte superior do Gestor mostra os certificados SSL que estão disponíveis para utilização ou que estão pendentes de ativação por parte de uma Autoridade de Confiança.

Os certificados são apresentados num ecrã de quatro colunas, mostrando o Nome do certificado, a Data de expiração, Expira em (número de dias até à expiração) e o Estado/Tipo do certificado.

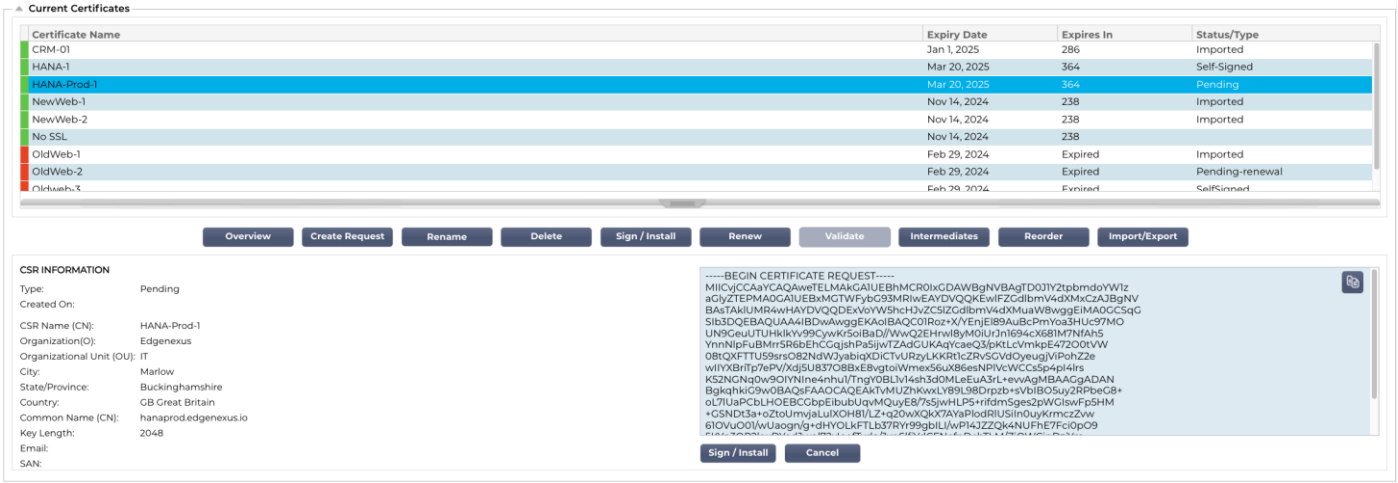
Códigos de cores

Como pode ver, cada linha apresenta um certificado juntamente com um bloco codificado por cores. Abaixo encontra-se uma tabela que mostra os diferentes blocos codificados por cores e o seu significado.

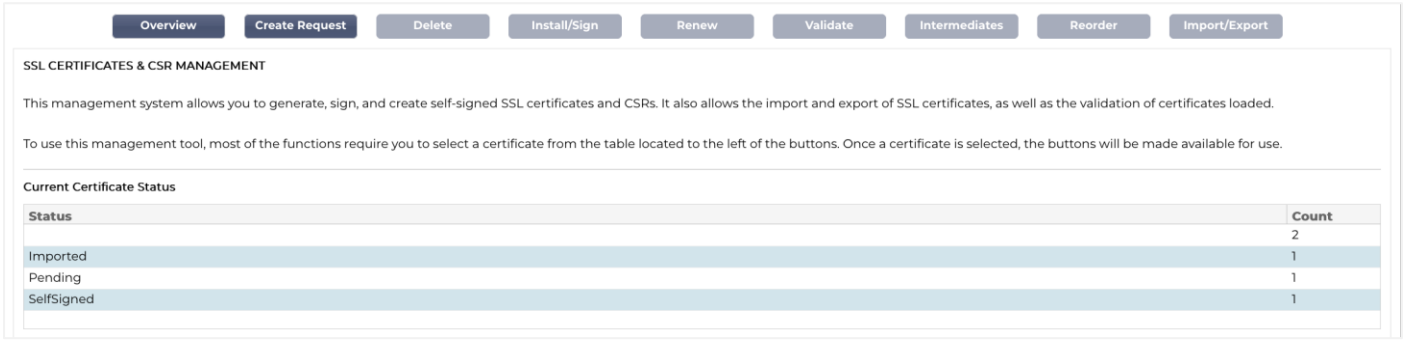
Código de cores	Significado
	O certificado está atualizado e tem mais de 60 dias antes da expiração
	O certificado expirará em menos de 30 dias
	O certificado tem entre 30 e 60 dias de validade
	O certificado está prestes a expirar com menos de 1 dia
	O certificado expirou

Visualização das informações do certificado/CSR

Clicar num certificado ou num CSR apresenta as respectivas informações no painel inferior. Veja a imagem abaixo.

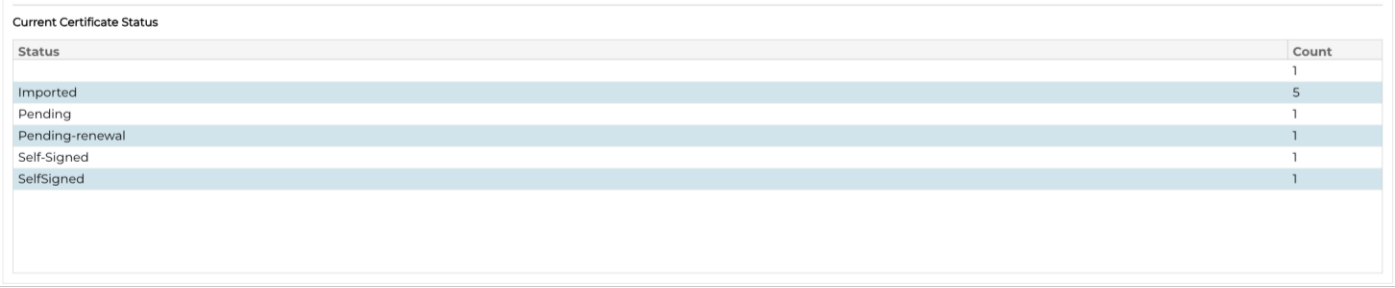


Os botões de ação e as áreas de configuração



Há uma série de botões de ação que estão disponíveis e que entram em ação quando um certificado é selecionado na área Listagem.

Visão geral

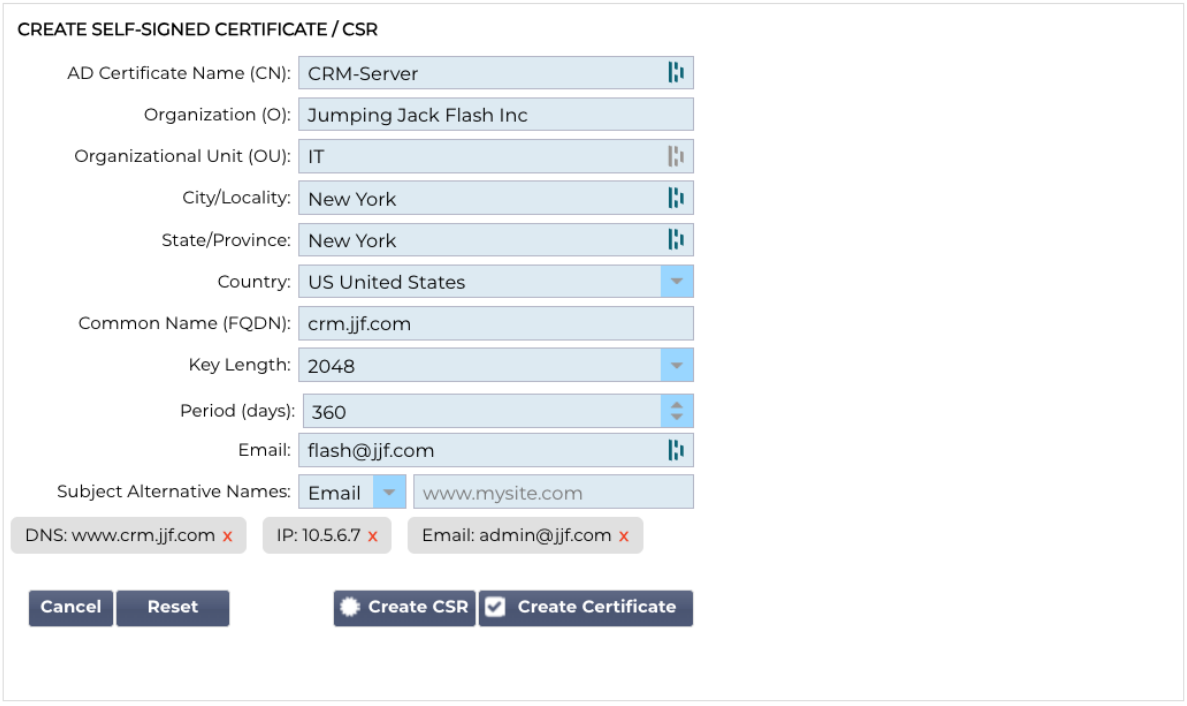

Current Certificate Status

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

O botão Visão geral apresenta uma situação geral dos certificados na secção inferior. Ao contrário de outras acções, o botão Síntese é independente e não requer que um certificado seja selecionado.

Criar pedido

Se pretender criar um certificado auto-assinado ou um CSR, tem de clicar no botão Criar pedido. Isto irá abrir um painel de entrada comum que lhe permite fornecer todos os detalhes necessários.



Nome do certificado AD (CN)

Este é um campo descritivo que é utilizado para apresentar o nome do certificado no ADC. A entrada de campo deve ser especificada como alfanumérica sem espaços.

Organização (O)

Este campo é utilizado para especificar o nome da organização que vai utilizar o certificado.

Unidade Organizacional (UO)

Normalmente utilizado para especificar o departamento ou a unidade organizacional, este é um campo facultativo.

Cidade/Localidade

Como o nome sugere, os utilizadores tendem geralmente a especificar onde a organização está localizada.

Estado/Província

Especifique o estado, concelho ou província neste campo.

País

Este é um campo obrigatório e deve ser preenchido selecionando o país em que o certificado será utilizado. Certifique-se de que as informações aqui fornecidas são exactas.

Nome comum (FQDN)

Este é um campo crítico e é utilizado para especificar o nome de domínio totalmente qualificado (FQDN) do(s) servidor(es) que deve(m) ser protegido(s) utilizando o certificado. Pode ser algo como www.edgenexus.io, ou **edgenexus.io**, ou mesmo um wildcard ***.edgenexus.io**. Também pode utilizar um endereço IP, caso pretenda associar o certificado ao mesmo.

Comprimento da chave

Utilizado para especificar o comprimento da chave de encriptação para o certificado SSL.

Período (dias)

A duração da validade do certificado em dias. Uma vez expirado o período, o certificado tornar-se-á não operacional.

Correio eletrónico

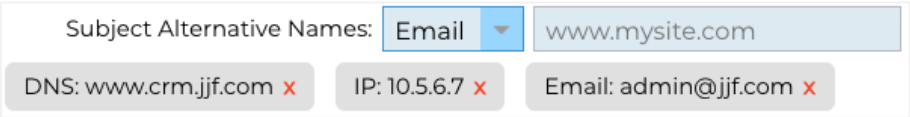
Este é o ID do correio eletrónico administrativo utilizado para o certificado.

Nomes alternativos de assuntos (SAN)

O Subject Alternative Name (SAN) é uma extensão dos certificados SSL que permite que vários nomes de domínio sejam protegidos num único certificado. Esta funcionalidade é especialmente útil para proteger sítios Web com vários subdomínios ou nomes de domínio diferentes, permitindo uma abordagem mais simplificada e económica à gestão de SSL. Ao incluir SANs, um único certificado SSL pode abranger uma variedade de nomes de domínio e subdomínios, eliminando a necessidade de certificados individuais para cada endereço Web, simplificando assim o processo de proteção das comunicações Web e garantindo a encriptação de dados em diversos domínios.

Este campo é composto por dois elementos: uma lista pendente que permite selecionar o tipo de RAS e um campo de texto para especificar o valor.

O EdgeADC possui as seguintes SANs disponíveis para uso: DNS, IP Address, Email Address e URI. É possível selecionar e especificar vários SANs para um certificado ou CSR.



As SANs que foram especificadas podem ser removidas clicando no **x** vermelho localizado em cada valor SAN.

- **DNS** - O Nome Alternativo de Assunto DNS (SAN) permite-lhe especificar nomes de domínio adicionais para os quais o certificado é válido. Ao contrário do campo Nome Comum (CN), que permite apenas um domínio, o campo SAN pode incluir vários nomes de domínio, oferecendo flexibilidade e escalabilidade na gestão de certificados. Isto é particularmente útil para organizações que alojam vários serviços em diferentes domínios e subdomínios, uma vez que lhes permite proteger as comunicações de todas estas entidades com um único certificado SSL/TLS, simplificando a administração e melhorando a segurança.
- **Endereço IP** - O Nome Alternativo de Assunto IP (SAN) permite a inclusão de endereços IP juntamente com nomes de domínio como entidades protegidas pelo certificado. Esta caraterística é crucial para garantir o

acesso direto a serviços através de endereços IP, assegurando que as ligações encriptadas também podem ser estabelecidas quando se acede a um servidor não através do seu nome de domínio, mas diretamente através do seu endereço IP. Ao incorporar SANs IP, as organizações podem melhorar a sua segurança de rede, permitindo a encriptação SSL/TLS para comunicações baseadas em domínio e baseadas em IP, tornando-a versátil para ambientes em que os nomes de domínio podem não ser utilizados ou preferidos para aceder a recursos internos ou serviços específicos.

- **Endereço de correio eletrónico** - O Nome alternativo de assunto de endereço de correio eletrónico (SAN) permite-lhe especificar endereços de correio eletrónico adicionais a serem associados ao certificado, para além do domínio ou entidade principal para o qual foi emitido. Isto permite que o certificado valide a identidade do emissor para múltiplos endereços de correio eletrónico, e não apenas para um único domínio ou Nome Comum (CN). É particularmente útil em cenários em que é necessária uma comunicação segura por correio eletrónico para vários endereços de correio eletrónico da mesma organização ou entidade, garantindo que as trocas de correio eletrónico encriptado são autenticadas e associadas à identidade do emissor verificada pelo certificado. Isto faz com que o Email Address SAN seja uma caraterística essencial para melhorar a segurança e a fiabilidade das comunicações por correio eletrónico numa estrutura encriptada.
- **URI** - O URI (Uniform Resource Identifier) SAN é utilizado para especificar identidades adicionais representadas por URIs para uma única entidade protegida pelo certificado. Ao contrário das entradas SAN tradicionais que normalmente incluem nomes de domínio (nomes DNS) ou endereços IP, um URI SAN permite que o certificado associe a entidade a URIs específicos, como um URL para um recurso específico ou um ponto final de serviço. Isto permite uma identificação mais flexível e precisa, possibilitando o estabelecimento de ligações seguras com recursos ou serviços específicos num domínio, em vez de proteger apenas o próprio domínio, melhorando assim a granularidade e o âmbito dos certificados SSL/TLS.

Uma vez preenchido corretamente, pode optar por criar um Pedido de Assinatura de Certificado (CSR) e enviá-lo para ser assinado por uma Autoridade de Certificação ou criar um Certificado Autoassinado para utilização imediata.

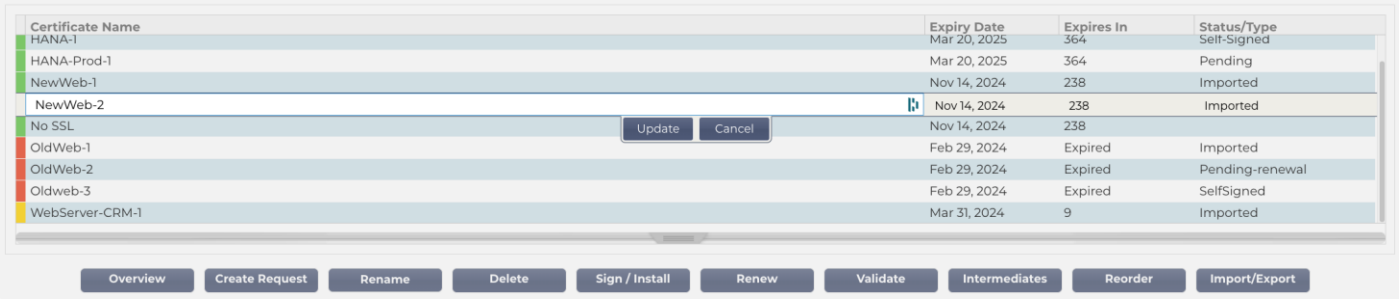
O botão Cancelar cancelará todo o pedido, enquanto o botão Repor reporá todos os campos.

Mudar o nome

O botão Mudar nome permite-lhe mudar o nome de certificados que não estão a ser utilizados nos Serviços virtuais.

Para utilizar esta função:

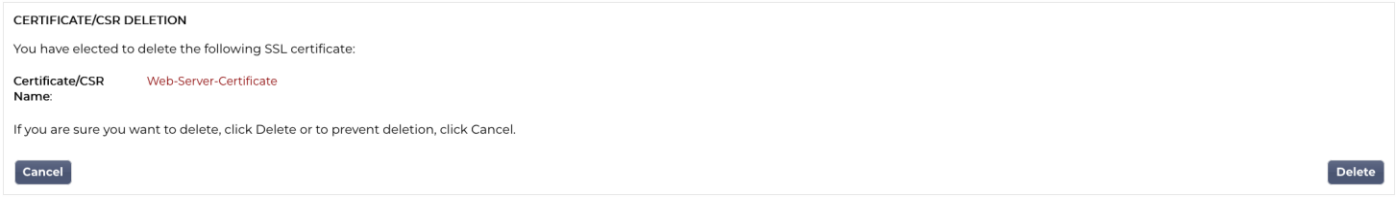
- Clique no certificado que pretende mudar o nome e clique no botão Mudar o nome.
- A linha do certificado será alterada e poderá mudar o seu nome.



- Quando tiver terminado, clique no botão Atualizar.
- Também pode fazer duplo clique no certificado para mudar o nome do certificado.

Eliminar

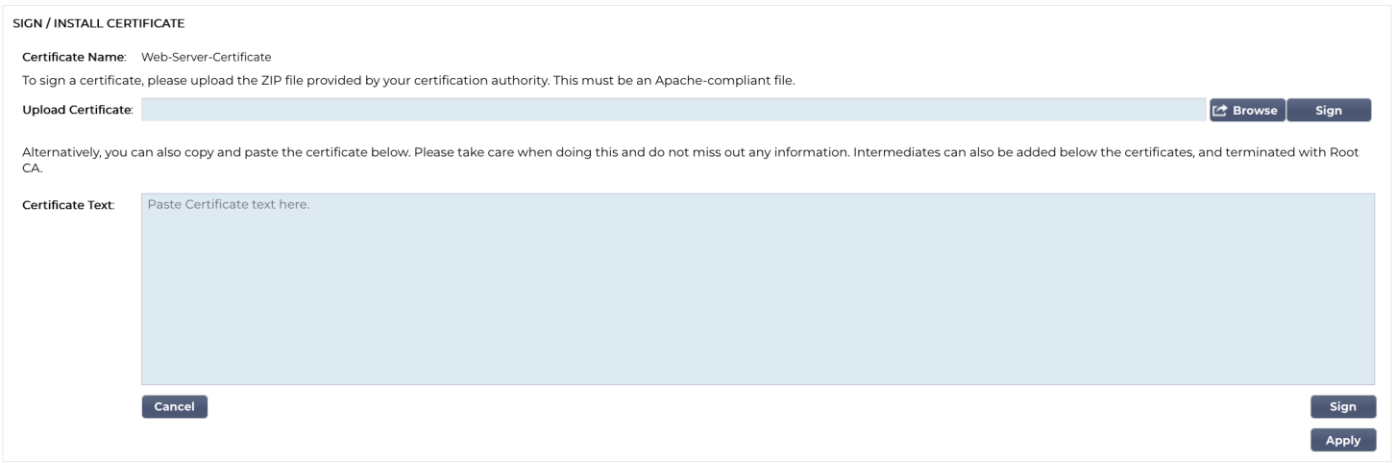
O botão Eliminar só estará disponível quando um certificado estiver selecionado. Quando clicado, apresenta o seguinte conteúdo



O painel inferior apresentará o pedido de eliminação juntamente com o nome do certificado para o qual foi pedida a eliminação.

Clique no botão Eliminar no canto inferior direito do painel para prosseguir com a eliminação.

Instalar/assinar



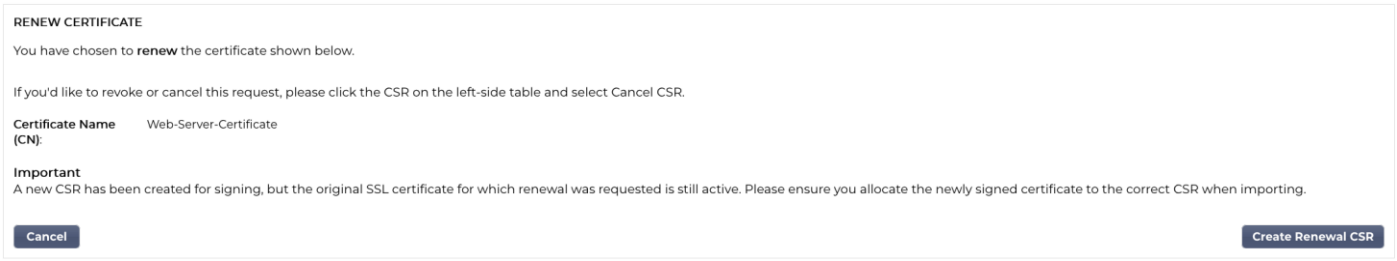
Quando cria um CSR e pretende que o pedido seja assinado por uma Autoridade de Certificação (AC), envia o CSR para a AC. Em troca, a CA enviará o certificado assinado juntamente com o ficheiro da chave privada e quaisquer intermediários necessários para que o certificado funcione corretamente.

É possível que lhe enviem um ficheiro ZIP com todos os elementos necessários, que pode ser carregado utilizando a parte superior do painel direito.

Em alternativa, também é possível construir o conjunto de certificados num editor de texto e colar o conteúdo no campo Texto do certificado na secção inferior do painel.

Depois de ter utilizado qualquer um dos métodos, clique no botão Assinar e, em seguida, no botão Aplicar. O certificado assinado será agora apresentado no painel esquerdo.

Renovar



Quando um certificado está prestes a expirar para além dos seus dados de validade, o botão Renovar permite-lhe prolongar e renovar o certificado. Existem dois tipos de renovação.

Certificados auto-assinados

Os certificados auto-assinados, ao contrário dos certificados de confiança, não podem ser renovados utilizando um CSR. Em vez disso, o certificado auto-assinado é renovado através da apresentação de uma

nova configuração utilizando os dados existentes. O utilizador pode então especificar um novo nome para o certificado, juntamente com um novo valor de expiração para o certificado.

Assim que isto for feito, o novo certificado auto-assinado será criado e guardado no repositório de certificados. É então da responsabilidade do administrador garantir que os serviços virtuais que utilizam o certificado são reconfigurados a tempo.

Certificados assinados fiáveis

Quando se trata de certificados de confiança e assinados por uma Autoridade de Certificação, é adoptada a utilização de CSRs.

Quando clicar num certificado expirado no painel superior e clicar em Renovar, ser-lhe-á apresentado um novo CSR utilizando os detalhes do certificado atual. O CSR pode então ser descarregado e apresentado à autoridade de certificação para assinatura, após o que o certificado assinado pode ser instalado.

O certificado que tinha pedido para renovar terá um novo estado, Renovando. Quando o certificado assinado estiver instalado, ser-lhe-á pedido que atribua um novo nome ao certificado. Este será então apresentado como Confiável. O certificado original será retido e todos os serviços que o utilizam devem ser configurados para utilizar o novo certificado o mais rapidamente possível.

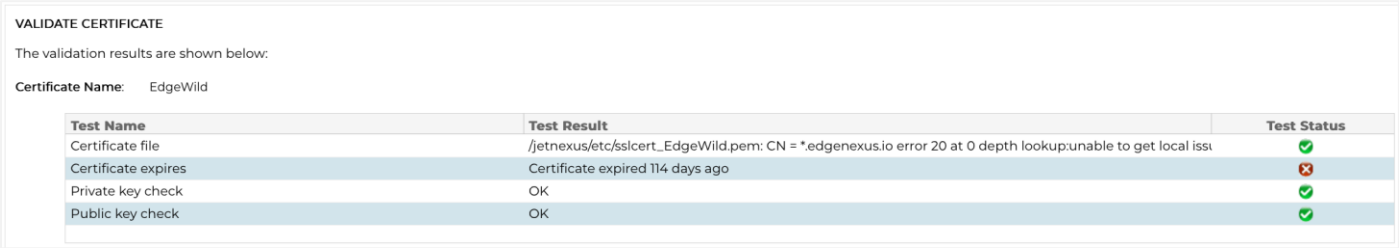
Validar certificado

Existem várias partes que compõem um certificado SSL e é essencial que essas partes não só estejam presentes, como também estejam na ordem correta. As razões para validar os certificados SSL obtidos de organizações terceiras são indicadas abaixo.

- **Autenticação**: A validação garante que o certificado provém de uma autoridade fiável e verifica a identidade do sítio Web ou do servidor. Isto ajuda a evitar ataques man-in-the-middle, em que um atacante pode intercetar a comunicação entre um cliente e um servidor.
- **Integridade**: Ao validar um certificado SSL, pode garantir que o certificado não foi adulterado ou alterado. Isto é crucial para manter a integridade da ligação segura.
- **Verificação da cadeia de confiança**: Os certificados SSL são emitidos por Autoridades de Certificação (CAs). A validação de um certificado inclui a verificação de que ele está ligado a uma CA raiz de confiança. Este processo garante que o certificado é legítimo e fiável.
- **Estado de revogação**: Durante a validação, também é importante verificar se o certificado SSL foi revogado pela CA emissora. Um certificado pode ser revogado se tiver sido emitido erradamente, se a chave privada do sítio Web tiver sido comprometida ou se o sítio já não precisar do certificado. A importação de um certificado revogado pode levar a vulnerabilidades de segurança.
- **Verificação da expiração**: Os certificados SSL são válidos por um período específico. A validação de um certificado na importação inclui a verificação da data de expiração para garantir que ainda é válido. A utilização de um certificado expirado pode conduzir a vulnerabilidades e fazer com que os navegadores ou clientes rejeitem a ligação segura.
- **Configuração e compatibilidade**: A validação garante que a configuração do certificado é compatível com as políticas de segurança do cliente e com os requisitos técnicos do servidor ou da aplicação. Isto inclui a verificação dos algoritmos utilizados, o objetivo do certificado e outros detalhes técnicos.
- **Conformidade**: Em determinados sectores, os regulamentos podem exigir a validação de certificados SSL para garantir o tratamento seguro de informações sensíveis. Isto é especialmente importante em sectores como o financeiro, a saúde e o comércio eletrónico.

O sistema de gestão SSL da ADC permite validar um certificado SSL importado.

- Selecione um certificado SSL que tenha importado.
- Clique no botão Validar.
- Os resultados são apresentados no painel inferior, conforme representado na imagem abaixo.

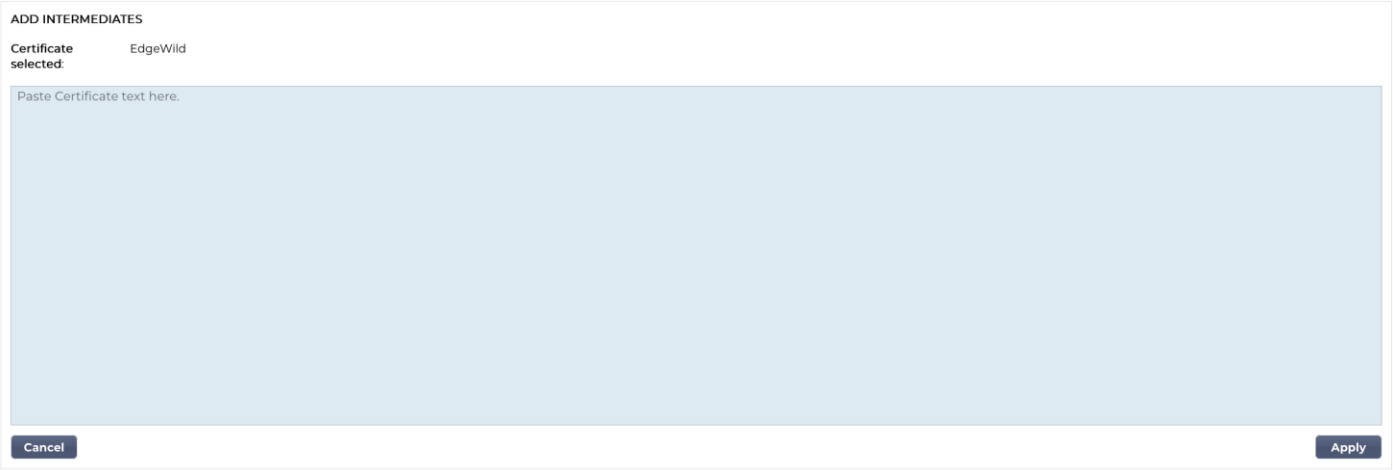


Adição de intermediários

Como já foi referido, os certificados SSL são compostos por várias partes, uma das quais são os certificados intermédios que constituem a cadeia completa.

O Gestor SSL no ADC permite-lhe adicionar quaisquer certificados intermédios em falta.

- Clique no SSL ao qual pretende adicionar o certificado intermédio.
- Clique no botão Intermediários.
- É apresentado um painel semelhante ao da imagem abaixo.



- Colar o conteúdo do certificado intermédio.
- Clique em Aplicar.

Pode ser necessário alterar a ordem dos certificados intermédios, para que o certificado SSL seja validado corretamente. Isto é feito utilizando o botão Reordenar.

Reordenar

Para que um certificado SSL funcione corretamente, tem de estar na ordem correta.

A regra de ouro é que o certificado do remetente deve vir em primeiro lugar, com o certificado raiz final em último lugar na cadeia. Geralmente, isto parece-se um pouco com a representação abaixo:

```
Emissor original > Intermediário 1 > Raiz final.
```

A raiz final é um certificado de raiz fiável fornecido por uma autoridade de certificação.

Em alguns casos, existem vários certificados intermédios e estes também devem ser colocados na posição correta. Essencialmente, cada certificado seguinte deve certificar o anterior. Portanto, o resultado pode ser o seguinte.

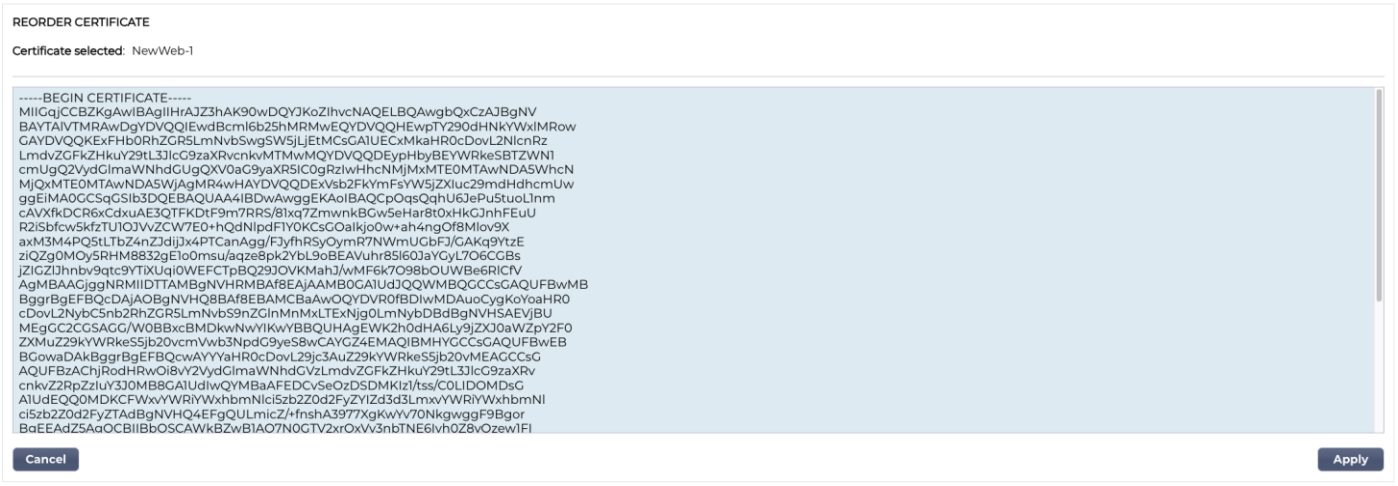
```
Emissor original > Intermediário 1 > Raiz final
```

Quando se importa, por exemplo, a Intermédia 2, esta pode ser colocada no fim da cadeia, o que significaria que a certificação deixaria de ser válida. Daí a necessidade de reordenar a cadeia e colocar o Intermediário 2 na sua posição correta (indicada a vermelho).

Assim, o resultado final seria o seguinte:

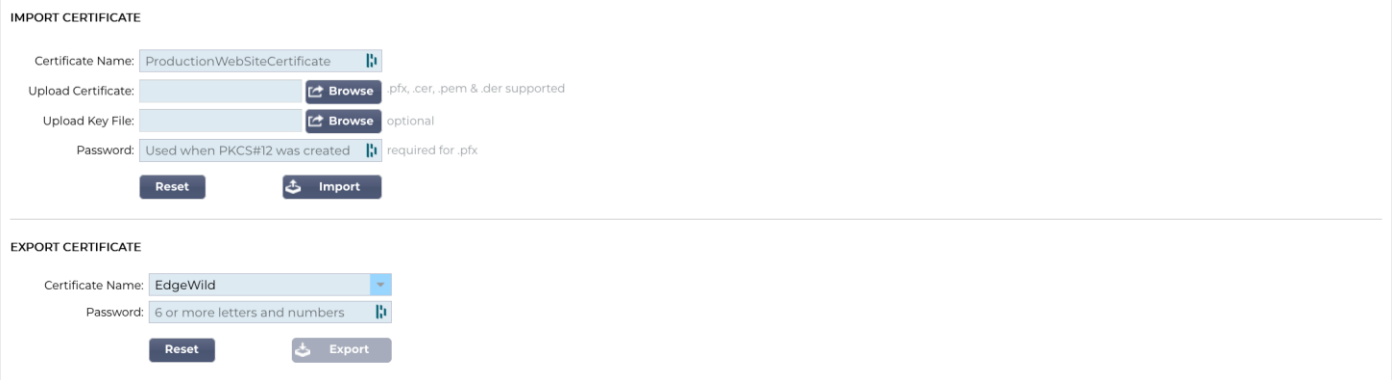
```
Emissor original > Intermediário 1 > Intermediário 2 >  Raiz final


-----BEGIN CERTIFICATE-----
MIIFKTCCBBGgAwIBAgISA/UUyBjJ71fucZuvpiLsdfsfsdfsdfd
...
hoFWWJt3/SeBKn+ci03RRvZsdfdsfsdfw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFFjCCAv6gAwIBAgIRAJErCErPDBinsdfsdfsdfsdfdsfsdfsd
....
nLRbwHqsdqD7hHwg==
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIFYDCCBsdfSDFSDFVSDVzfsdffvqdsfgsT664ScbvsfGDGSDV
...
Dfvp7OOGAN6dEOM4+SDFSDZET+DFGDFQSD45Bddfghqsqf6Bsff
-----END CERTIFICATE-----
```

A secção Reordenar tem o aspeto da imagem abaixo, depois de selecionar um certificado e premir o botão Reordenar.



Para reordenar as secções do certificado, pode copiar o texto dentro da caixa, editar e reordenar o conteúdo num editor de texto e, em seguida, colá-lo novamente para substituir o conteúdo existente. Uma vez concluído, clique no botão Aplicar.

Importação/Exportação



Sempre que receber um certificado do seu fornecedor de certificados SSL, este virá como um ficheiro ZIP ou um conjunto de ficheiros. Estes contêm o certificado SSL, o ficheiro chave e o root ca, bem como quaisquer ficheiros intermédios

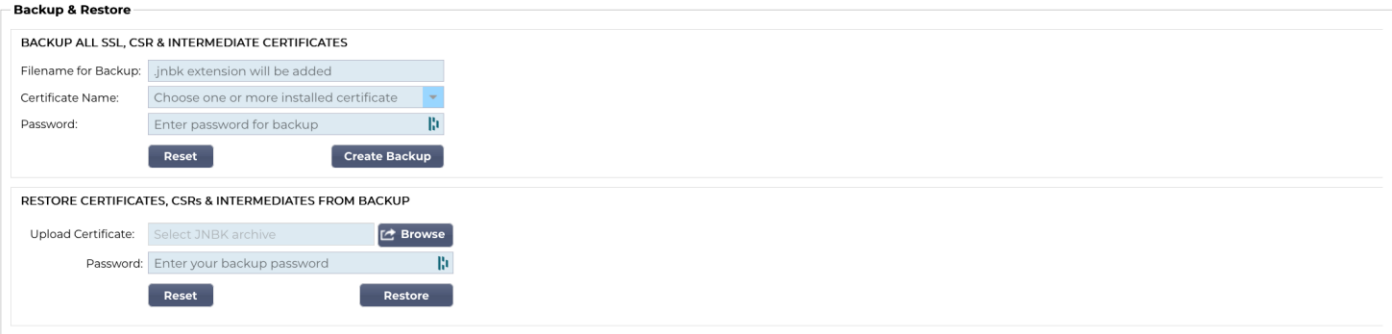
Terá de os importar para o ADC e, por isso, fornecemos um método para os importar.

Existem vários formatos para certificados SSL, tais como CER, DER, PEM e PFX. Alguns formatos requerem que um ficheiro KEY seja adicionado ao procedimento de importação. Os ficheiros PFX requerem a palavra-passe para importar o certificado PFX.

Também disponibilizámos os meios para exportar um certificado do ADC, se necessário. Quando exportado, o ficheiro estará no formato PFX, pelo que é necessária uma palavra-passe para criar a exportação.

Cópia de segurança e restauro

Cópia de segurança



Para efetuar uma cópia de segurança dos certificados no armazenamento de certificados do ADC:

- Adicione um nome de ficheiro a ser utilizado para a cópia de segurança.
- Utilize o menu pendente para selecionar um único certificado ou TODOS para efetuar a cópia de segurança de todos os certificados.
- Adicionar uma palavra-passe
- Clique no botão Criar cópia de segurança.
- O ficheiro criado é um ficheiro JNBK que está encriptado.

IMPORTANTE

A cópia de segurança só funcionará com certificados fidedignos que tenham sido importados.

Restaurar

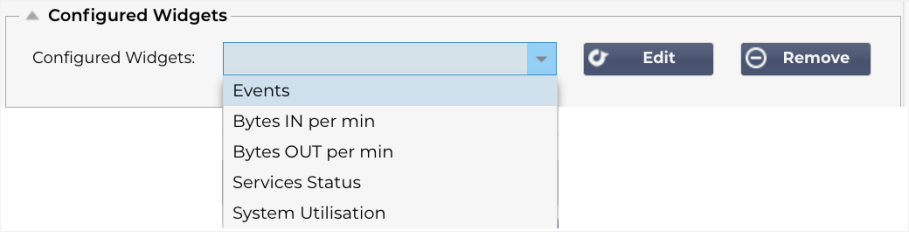
Quando pretender restaurar a cópia de segurança, utilize a secção inferior da secção Cópia de segurança e restauro.

- Navegue até ao ficheiro de cópia de segurança e localize-o.
- Introduzir a palavra-passe.
- Clique no botão Restaurar.
- Os certificados contidos no ficheiro de cópia de segurança serão restaurados.

Widgets

A página Biblioteca > Widgets permite-lhe configurar vários componentes visuais ligeiros apresentados no seu painel de controlo personalizado.

Widgets configurados

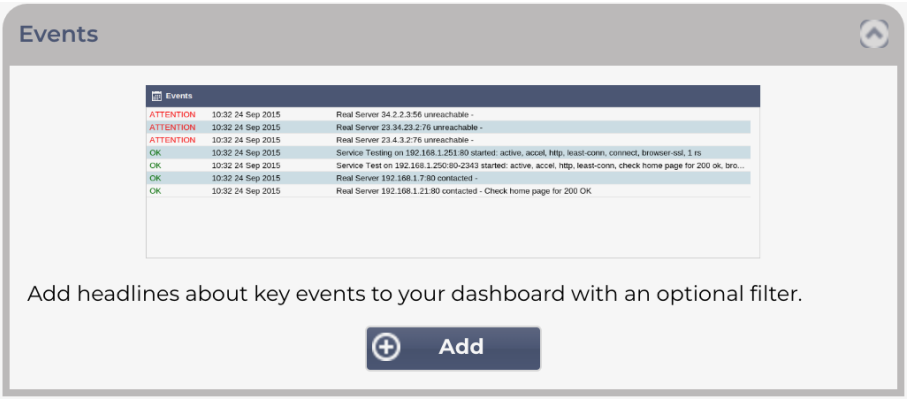


A secção Widgets configurados permite-lhe ver, editar ou remover quaisquer widgets criados a partir da secção de widgets disponíveis.

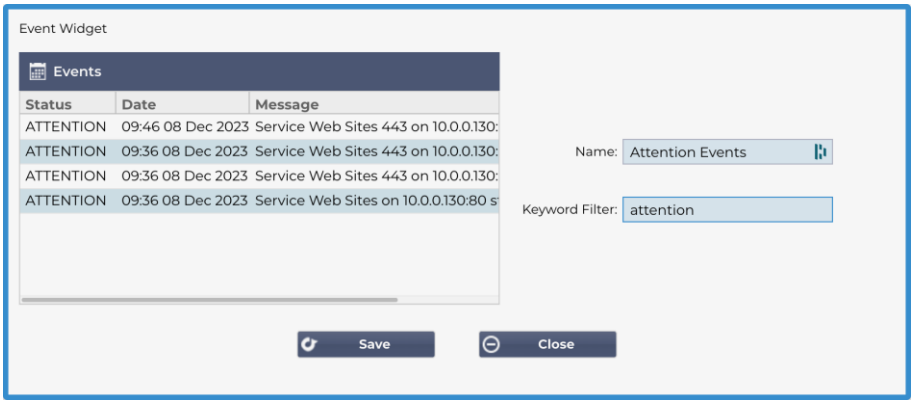
Widgets disponíveis

Existem cinco widgets diferentes no ADC, que podem ser configurados de acordo com as necessidades do utilizador.

O widget de eventos

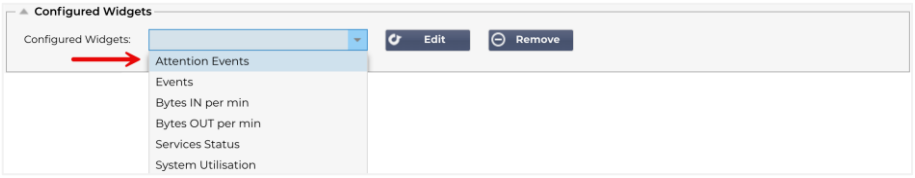


- Para adicionar um evento ao widget Eventos, clique no botão Adicionar.
- Forneça um nome para o seu evento. No nosso exemplo, acrescentámos "Eventos de atenção" como nome do evento.
- Adicionar um filtro de palavras-chave. Também adicionámos o valor de filtro de Atenção



- Clique em Guardar e depois em Fechar

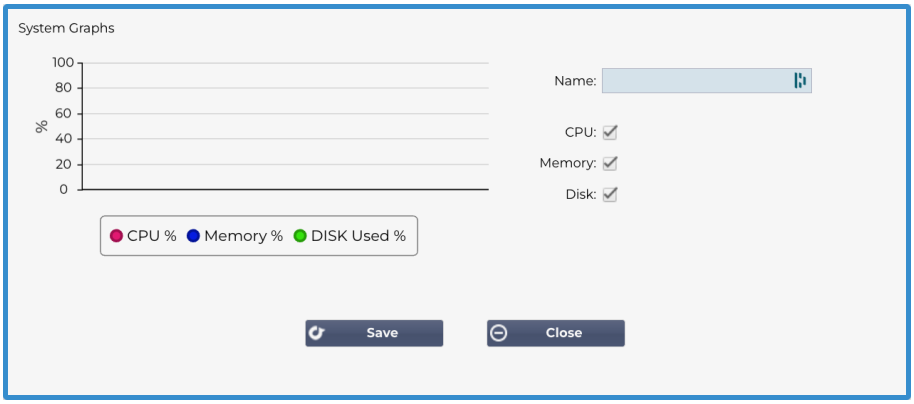
- Verá agora um Widget adicional chamado Eventos de atenção no menu pendente Widgets configurados.



- Pode ver que adicionámos este widget na secção View > Dashboard (Ver > Painel).
- Selecione o widget Eventos de atenção para o visualizar no painel de controlo. Ver abaixo.

Também pode fazer uma pausa e reiniciar o feed de dados em direto, clicando no botão Pausar dados em direto. Além disso, pode reverter para o painel de controlo predefinido em qualquer altura, clicando no botão Painel de controlo predefinido.

O widget de gráficos do sistema

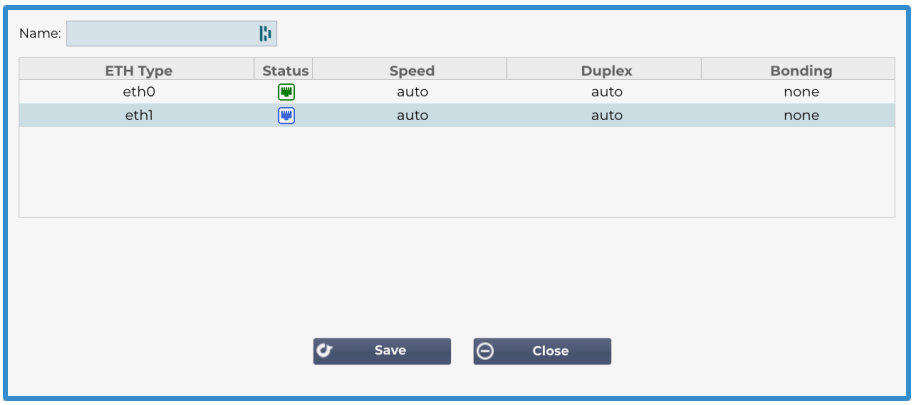


O ADC tem um widget configurável de Gráfico do sistema. Ao clicar no botão Adicionar no widget, pode adicionar os seguintes gráficos de monitorização para serem apresentados.

- CPU
- MEMÓRIA
- DISCO

Depois de os ter adicionado, estarão disponíveis individualmente no menu de widgets do Painel de Controlo.

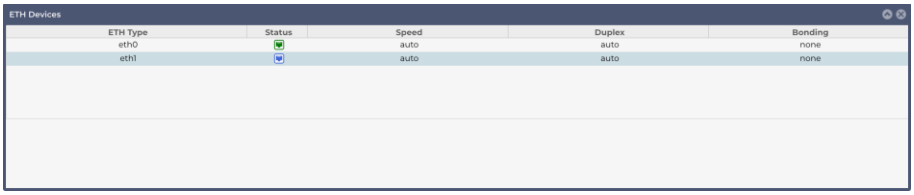
Widget de interface



O widget Interface permite-lhe apresentar os dados da interface de rede escolhida, como ETH0, ETH1, etc. O número de interfaces disponíveis para adição depende de quantas interfaces de rede foram definidas para o dispositivo virtual ou provisionadas no dispositivo de hardware.

Quando tiver terminado, clique no botão Guardar e, em seguida, no botão Fechar.

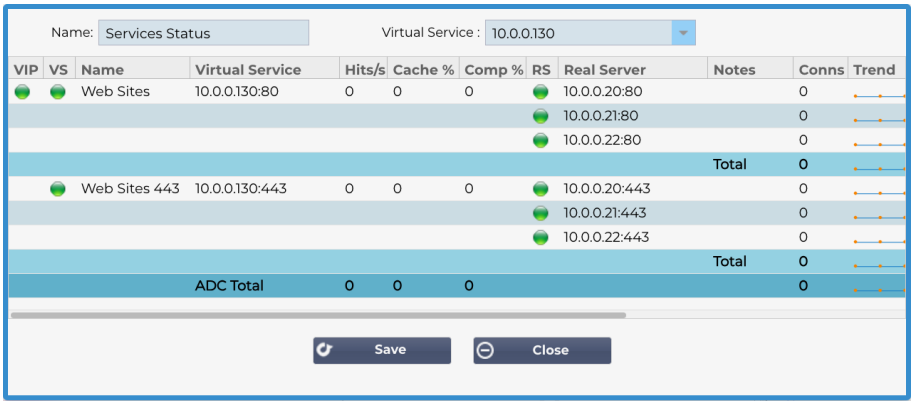
Selecione o Widget que acabou de personalizar no menu pendente do widget no Painel de controlo. Verá um ecrã como o que se segue.



Widget de estado

O widget de Estado permite-lhe ver o balanceamento de carga em ação. Também pode filtrar a vista para mostrar informações específicas.

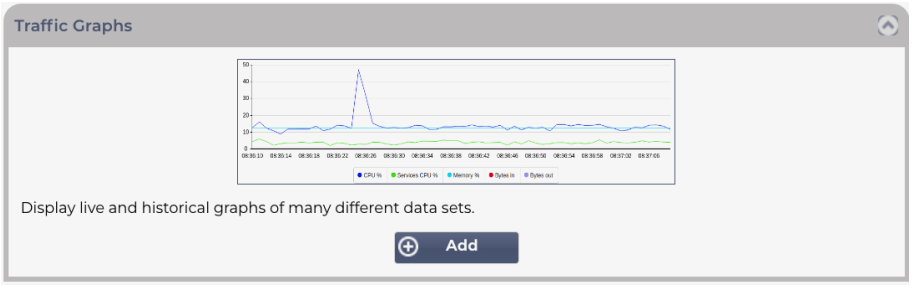
- Clique em Adicionar.



- Introduza um nome para o serviço que pretende monitorizar
- Também pode escolher as colunas que pretende apresentar no widget, clicando no cabeçalho da coluna.
- Quando estiver satisfeito, clique em Guardar e, em seguida, em Fechar.
- O widget de Estado escolhido estará disponível na secção Painel.

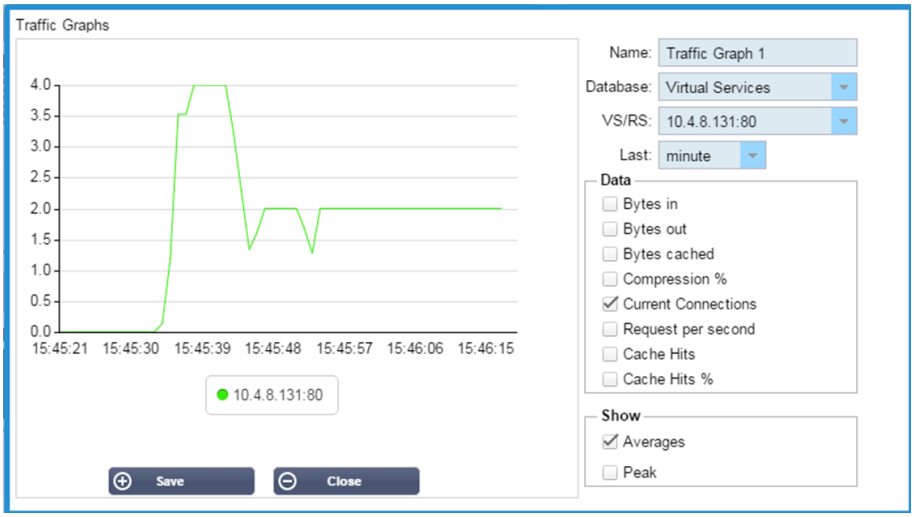
Widget de gráficos de tráfego

Este widget pode ser configurado para mostrar dados de tráfego actuais e históricos por Virtual Services e Real Servers. Além disso, pode ver os dados gerais actuais e históricos do tráfego global



- Clique no botão Adicionar
- Dê um nome ao seu widget.
- Escolha uma base de dados entre Serviços virtuais, Servidores reais ou Sistema.
- Se selecionar Serviços virtuais, pode selecionar um serviço virtual a partir do menu pendente VS/RS.
- Selecione um período de tempo no menu pendente Último.
    - Minuto - últimos 60s
    - Hora - dados agregados de cada minuto para os últimos 60 minutos
    - Dia - dados agregados de cada hora das 24 horas anteriores
    - Semana - dados agregados de cada dia durante os sete dias anteriores
    - Mês - dados agregados de cada semana nos últimos sete dias
    - Ano - dados agregados de cada mês durante os 12 meses anteriores
- Selecionar os Dados disponíveis em função da base de dados escolhida
    - Base de dados de serviços virtuais
    - Bytes em
    - Bytes enviados
    - Bytes armazenados em cache
    - Compressão %
    - Ligações actuais
    - Pedidos por segundo
    - Acertos de cache
    - Hits de cache %
- Servidores reais
    - Bytes em
    - Bytes enviados
    - Ligações actuais
    - Pedidos por segundo
    - Tempo de resposta
- Sistema
    - CPU %
    - Serviços CPU
    - Memória %
    - Disco livre %
    - Bytes em
    - Bytes enviados
- Opção para mostrar os valores médios ou de pico
- Depois de ter escolhido todas as opções, clique em Guardar e fechar

Exemplo de gráfico de tráfego



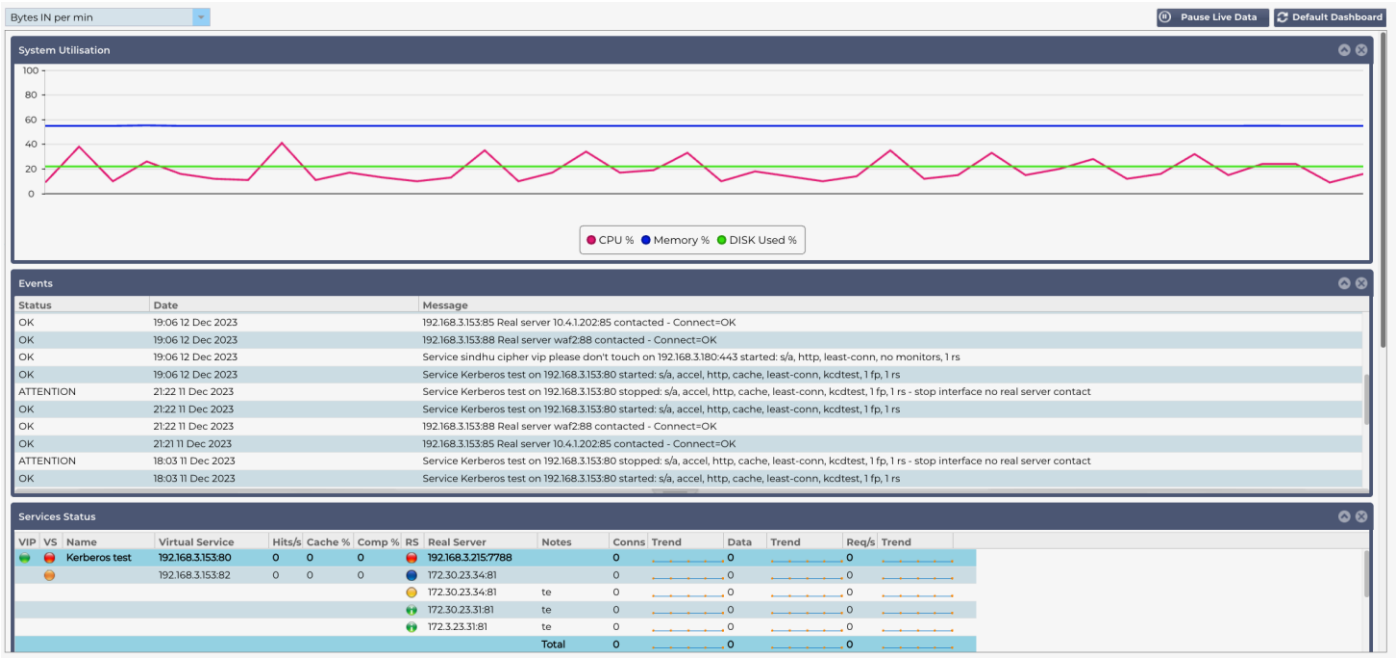
Agora pode adicionar o seu widget de gráfico de tráfego ao Painel de controlo View> .

Ver

Painel de controlo

Tal como acontece com todas as interfaces de gestão de sistemas de TI, há muitas ocasiões em que é necessário analisar as métricas de desempenho e os dados que o ADC está a tratar. Fornecemos um painel de controlo personalizável para que o possa fazer de uma forma fácil e significativa.

O Dashboard pode ser acedido utilizando o segmento Ver do painel do navegador. Quando selecionado, mostra vários widgets predefinidos e permite-lhe escolher quaisquer widgets personalizados que tenha definido.



Utilização do painel de controlo

Existem quatro elementos no Dashboard U: O menu Widgets, o botão Pausa/Reprodução e o botão Dashboard predefinido.

O menu Widgets

O menu Widgets localizado no canto superior esquerdo do painel permite-lhe selecionar e adicionar quaisquer widgets padrão ou personalizados que tenha definido. Para utilizar este menu, selecione o widget a partir do menu pendente.

Botão Pausar dados em direto

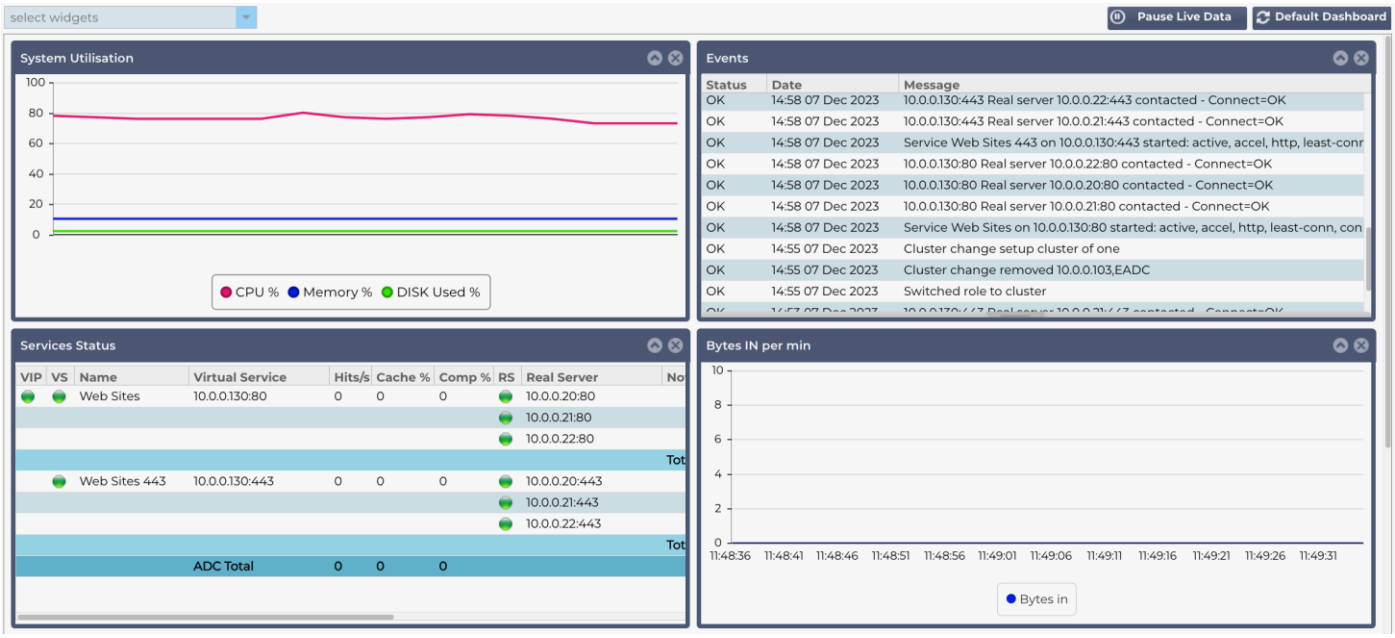
Este botão permite-lhe selecionar se o ADC deve atualizar o painel de instrumentos em tempo real. Uma vez em pausa, nenhum widget do painel será atualizado, permitindo-lhe examinar o conteúdo à sua vontade. O botão muda de estado para apresentar Reproduzir dados em direto quando é iniciada uma pausa.

Quando tiver terminado, basta clicar no botão Reproduzir dados em direto para reiniciar a recolha de dados e atualizar o Painel de controlo.

Botão predefinido do painel de controlo

Pode acontecer que queira repor a disposição do Painel de Controlo para a disposição predefinida. Nesse caso, prima o botão Painel de controlo predefinido. Uma vez premido, todas as alterações efectuadas no Painel de Controlo serão perdidas.

Redimensionar, minimizar, reordenar e remover widgets



Redimensionar um widget

Pode redimensionar um widget muito facilmente. Clique sem soltar na barra de título do widget e arraste-o para o lado esquerdo ou direito da área do Painel. Verá um retângulo pontilhado que representa o novo tamanho do widget. Solte o widget no retângulo e solte o botão do rato. Se pretender largar um widget redimensionado ao lado de um widget previamente redimensionado, verá o retângulo aparecer adjacente ao widget que pretende largar ao lado.

Minimizar um widget

Pode minimizar os widgets em qualquer altura, clicando na barra de título do widget. Esta ação minimiza o widget e apresenta apenas a barra de título.

Mover a ordem dos widgets

Para mover um widget, pode arrastar e largar clicando e mantendo premido na barra de título e movendo o rato.

Remover um Widget

Pode remover um clicando no ícone⊗ na barra de título do widget.

História

A opção Histórico, selecionável a partir do navegador, permite ao administrador examinar o desempenho histórico do ADC. As visualizações históricas podem ser geradas para Serviços virtuais, Servidores reais e Sistema.

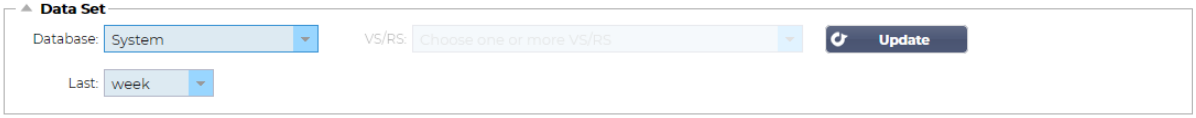
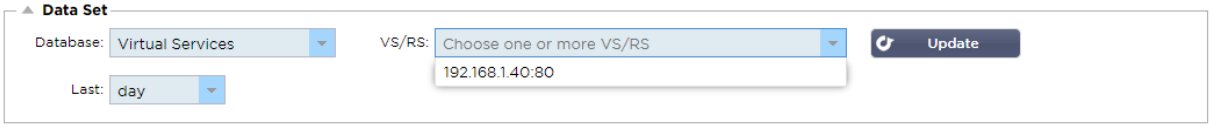
Também lhe permite ver o balanceamento de carga em ação e ajuda a detetar quaisquer erros ou padrões que necessitem de ser investigados. Note que é necessário ativar o registo histórico em Sistema > Histórico para utilizar esta funcionalidade.

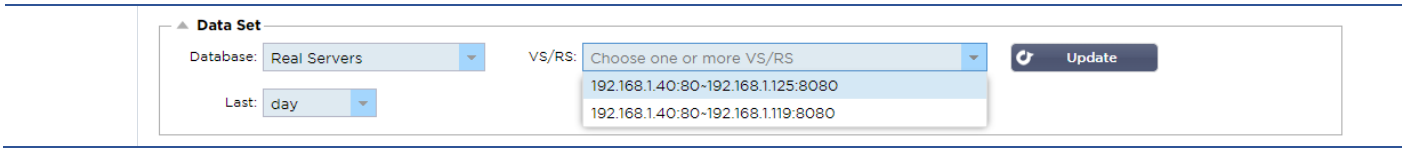
Visualização de dados gráficos

Conjunto de dados

Para visualizar os dados históricos em formato gráfico, proceda da seguinte forma:

O primeiro passo é escolher a base de dados e o período relevante para as informações que pretende visualizar. O período que pode selecionar no menu pendente Último é Minuto, Hora, Dia, Semana, Mês e Ano.

Base de dados	Descrição
Sistema	A seleção desta base de dados permite-lhe ver o espaço da CPU, da memória e da unidade de disco ao longo do tempo 
Serviços virtuais	A seleção desta base de dados permite-lhe escolher todos os serviços virtuais da base de dados desde o início do registo de dados. Aparecerá uma lista de Serviços Virtuais a partir da qual pode selecionar um. 
Serviços reais	A seleção desta base de dados permite-lhe escolher todos os Servidores reais na base de dados desde o início do registo de dados. É apresentada uma lista de Servidores reais a partir da qual pode selecionar um.



Métricas

Depois de selecionar o Conjunto de Dados que vai utilizar, é altura de escolher as Métricas que pretende apresentar. A imagem abaixo ilustra as métricas disponíveis para seleção pelo administrador: estas selecções correspondem a System, Virtual services e Real Servers (da esquerda para a direita).

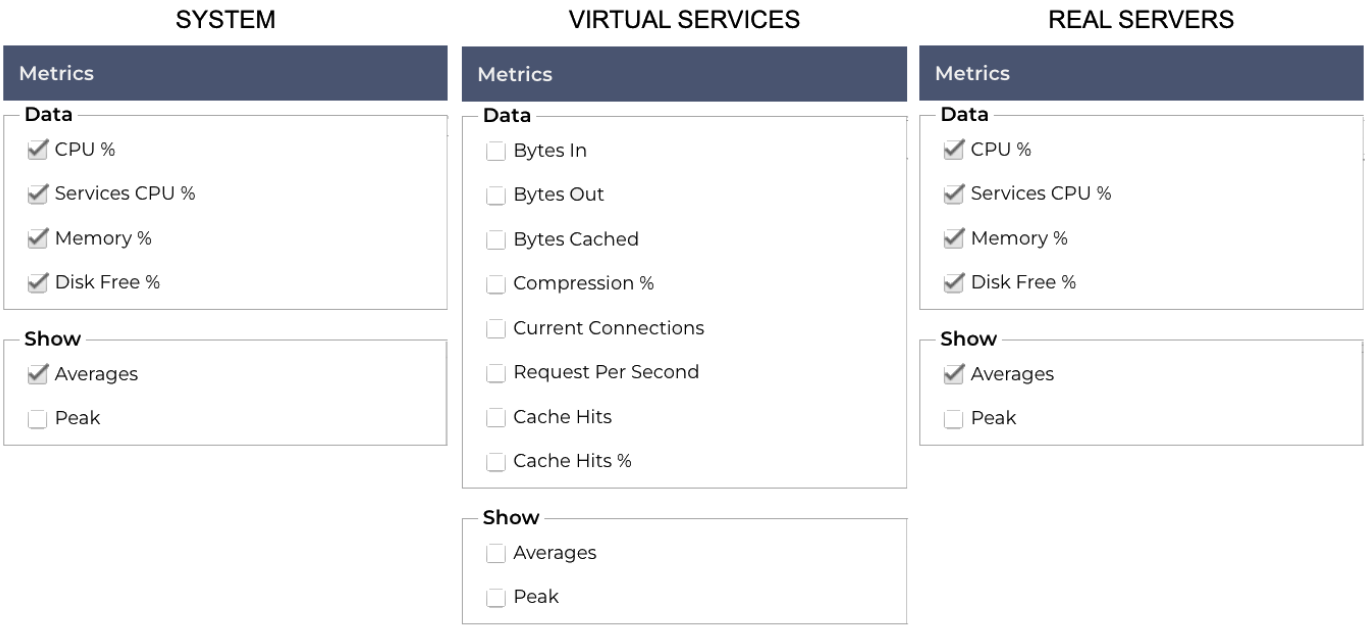
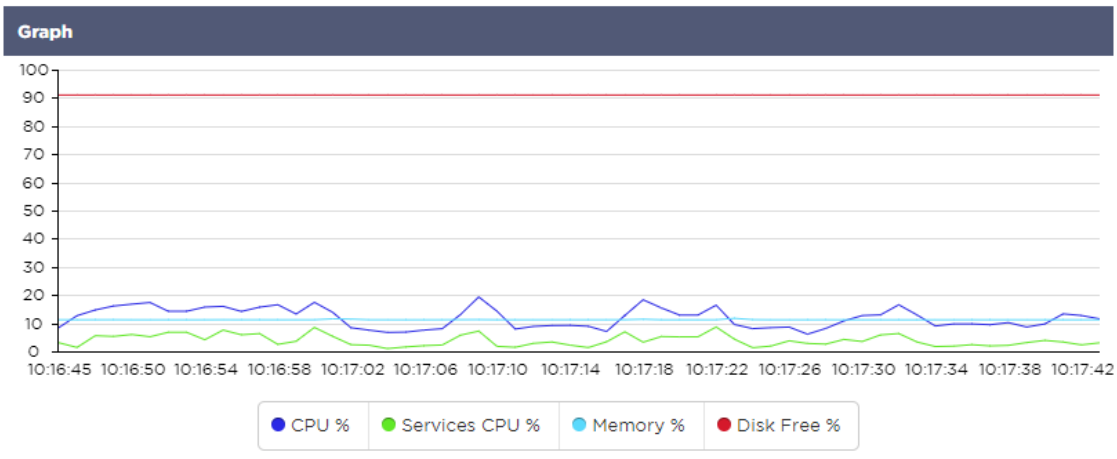


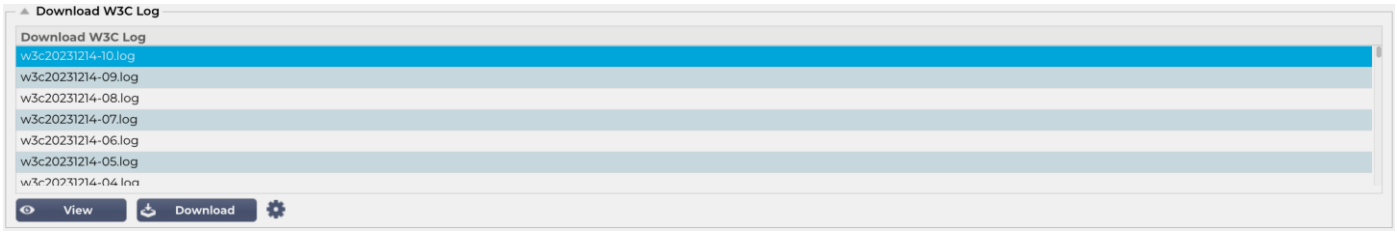
Gráfico de amostra



Registos

A página Registos na secção Ver permite-lhe pré-visualizar e transferir os registos do W3C e do sistema. A página está organizada em duas secções, conforme detalhado abaixo.

Registos do W3C



O registo W3C é ativado na secção Sistema > Registo. Um registo W3C é um registo de acesso para servidores Web em que são gerados ficheiros de texto com dados sobre cada pedido de acesso, incluindo o endereço IP de origem, a versão HTTP, o tipo de browser, a página de referência e o carimbo de data/hora. Os registos W3C podem tornar-se muito grandes, dependendo da quantidade de dados e da categoria de registo que está a ser gravada.

Na secção W3C, pode selecionar o registo de que necessita e, em seguida, visualizá-lo ou descarregá-lo.

Ver botão

O botão Ver permite-lhe ver o registo escolhido na janela do editor de texto, como o Bloco de notas.

Botão de descarregamento

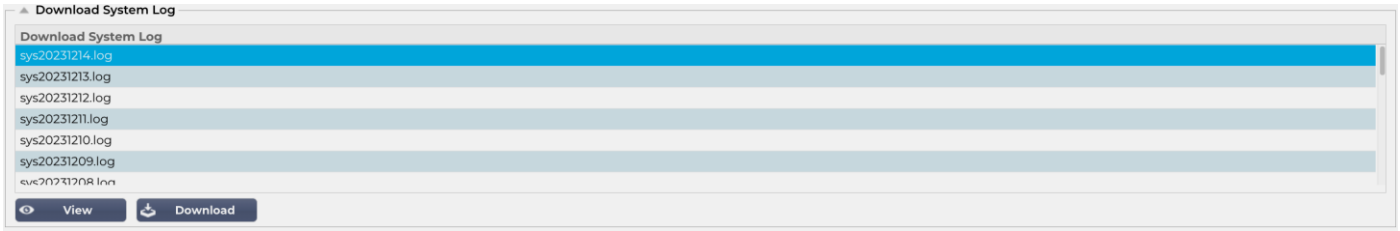
Este botão permite-lhe descarregar o registo para a sua memória local para o visualizar mais tarde.

O ícone da roda dentada

Clicar neste ícone leva-o para a secção Definições de registo W3C, localizada em Sistema > Registo. Falaremos sobre isto em pormenor na secção Registo do guia.

Registo do sistema

O registo do sistema é fundamental para a depuração ou análise do que está a acontecer com o ADC. Destina-se a pessoas com pouca experiência no departamento de TI.



Ver botão

O botão Ver permite-lhe ver o registo escolhido na janela do editor de texto, como o Bloco de notas.

Botão de descarregamento

Este botão permite-lhe descarregar o registo para a sua memória local para o visualizar mais tarde.

Estatísticas

A secção Estatísticas do ADC é uma área muito utilizada pelos administradores de sistemas que pretendem garantir que o desempenho do ADC está de acordo com as suas expectativas.

Compressão

O objetivo do ADC é monitorizar os dados e direccioná-los para os servidores reais configurados para os receber. O recurso de compactação é fornecido no ADC para aumentar o desempenho do ADC. Haverá momentos em que os administradores desejarão testar e verificar as informações de compressão de dados do ADC; esses dados são fornecidos pelo painel Compressão dentro de Estatísticas.

Compressão de conteúdos até à data

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

Os dados apresentados nesta secção detalham o nível de compressão alcançado pelo ADC em conteúdos compressíveis. Um valor de 60-80% é o que chamaríamos de típico

Compressão global até à data

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

Os valores fornecidos nesta secção indicam a quantidade de compressão que o ADC alcançou em todo o conteúdo. Uma percentagem típica para isto depende do número de imagens pré-comprimidas contidas nos seus serviços. Quanto maior for o número de imagens, menor será provavelmente a percentagem global de compressão.

Entrada/Saída total

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

Os valores de Entrada/Saída total representam a quantidade de dados em bruto que entram e saem do ADC. A unidade de medida muda à medida que o tamanho aumenta de kbps para Mbps e para Gbps.

Sucessos e ligações

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

A secção Hits and Connections (Acessos e ligações) contém as estatísticas gerais dos acessos e das transacções que passam pelo ADC. O que significam os acessos e as ligações?

- Um Hit é definido como uma transação do nível 7. Normalmente utilizada em servidores Web, trata-se de um pedido GET para um objeto, como uma imagem.

- Uma ligação é definida como uma ligação TCP de camada 4. Podem ocorrer muitas transacções numa única ligação TCP.

Total de visitas contadas

As figuras desta secção mostram o número cumulativo de acessos não armazenados em cache desde a última reposição. No lado direito, a figura mostrará o número atual de acessos por segundo.

Total de ligações

O valor Total de ligações representa o número acumulado de ligações TCP desde a última reposição. O número na segunda coluna indica as ligações TCP efectuadas por segundo ao ADC. O número na coluna do lado direito é o número de ligações TCP por segundo efectuadas aos Servidores Reais. Exemplo 6/8 conexões/segundo. Temos 6 ligações TCP por segundo ao Serviço Virtual e 6 ligações TCP por segundo aos Servidores Reais no exemplo apresentado.

Ligações de pico

O valor de pico Ligações representa o número máximo de ligações TCP efectuadas ao ADC. O número na coluna mais à direita indica o número atual de ligações TCP activas.

Armazenamento em cache

Como se recorda, o ADC está equipado com compressão e armazenamento em cache. Esta secção mostra as estatísticas gerais relacionadas com o armazenamento em cache quando aplicado a um canal. Se o armazenamento em cache não tiver sido aplicado a um canal e configurado corretamente, verá 0 conteúdos de cache.

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

Da Cache

Hits: A primeira coluna apresenta o número total de transacções servidas a partir da cache ADC desde a última reposição. Também é fornecida uma percentagem do total de transacções.

Bytes: A segunda coluna apresenta a quantidade total de dados em Kilobytes servidos a partir da cache do ADC. Também é fornecida uma percentagem do total de dados.

Do servidor

Acertos: A coluna 1 indica o número total de transacções efectuadas a partir dos servidores reais desde a última reposição. Também é fornecida uma percentagem do total de transacções.

Bytes: A segunda coluna fornece a quantidade total de dados em Kilobytes servidos a partir dos Servidores Reais. Também é fornecida uma percentagem do total de dados.

Conteúdo da cache

Hits: Este número indica o número total de objectos contidos na cache do ADC.

Bytes: O primeiro número fornece o tamanho total em Megabytes dos objectos em cache do ADC. Também é fornecida uma percentagem do tamanho máximo da cache.

Buffer de aplicação

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

A utilização de buffers de aplicação no ADC ajuda a otimizar o desempenho, a melhorar o débito e a garantir o fluxo fiável e eficiente de dados entre clientes e servidores. Os tamanhos dos buffers, as políticas de tratamento e outros parâmetros são optimizados pelo ADC para ajustar a carga com base nos requisitos específicos das aplicações e da infraestrutura.

No EdgeADC, fazemos o trabalho árduo por si e ajustamos automaticamente os parâmetros do buffer conforme as necessidades.

Persistência da sessão

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

A secção Session Persistence fornece informações sobre vários parâmetros.

Total de sessões actuais

Mostra quantas sessões de persistência estão em curso - actualizadas a cada minuto

% Utilizada (do máximo)

Isto mostra a quantidade de utilização do espaço total permitido para as informações da sessão

Nova sessão neste minuto

Isto mostra, no último minuto, quantas novas sessões de persistência foram adicionadas

Revalidar este min

Isto mostra, no último minuto, quantas sessões de persistência existentes foram revalidadas por mais tráfego

Sessões expiradas este mês

Isto mostra, no último minuto, quantas sessões de persistência existentes expiraram devido ao facto de não haver mais tráfego dentro do tempo limite

Hardware

Quer esteja a utilizar o ADC num ambiente virtual ou em hardware, esta secção irá fornecer-lhe informações valiosas sobre o desempenho do aparelho.

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

Utilização do disco

O valor fornecido na coluna 2 fornece a percentagem de espaço em disco atualmente utilizado e inclui informações sobre ficheiros de registo e dados de cache, que são periodicamente armazenados no armazenamento.

Utilização da memória

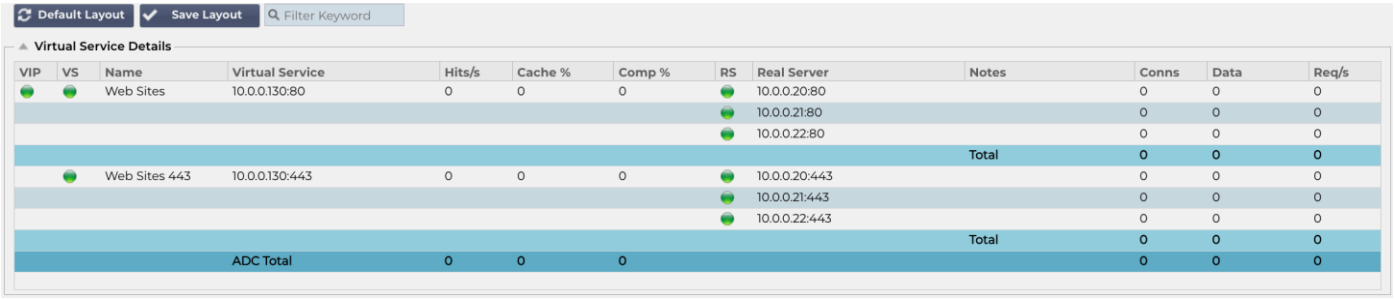
A segunda coluna indica a percentagem de memória atualmente utilizada. O número mais significativo entre parêntesis é a quantidade total de memória atribuída ao ADC. Recomenda-se que seja atribuído ao ADC um mínimo de 2 GB de RAM.

Utilização da CPU

Um dos valores críticos fornecidos é a percentagem da CPU atualmente utilizada pelo ADC. É natural que este valor flutue.

Estado

A página Ver > Estado apresenta o tráfego em tempo real que atravessa o ADC para os Serviços virtuais que definiu. Também mostra o número de ligações e dados para cada Real Server para que possa experimentar o balanceamento de carga em tempo real.



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

Detalhes do serviço virtual

Coluna VIP

A cor da luz indica o estado do endereço IP virtual associado a um ou vários serviços virtuais.

Estado	Descrição
●	Em linha
●	Failover-Standby. Este serviço virtual está em espera ativa
●	Indica que um "passivo" está a aguardar por um "ativo"
●	Offline. Os servidores reais estão inacessíveis ou não há servidores reais activados
●	Estado da constatação
●	IPs virtuais não licenciados ou licenciados excedidos

Coluna de estado VS

A cor da luz indica o estado do Serviço Virtual.

Estado	Descrição
●	Em linha
●	Failover-Standby. Este serviço virtual está em espera ativa
●	Indica que um "passivo" está a aguardar por um "ativo"
●	O serviço precisa de atenção. Esta indicação de estado pode resultar do facto de um Servidor Real ter falhado um monitor de saúde ou ter sido alterado manualmente para Offline. O tráfego continuará a fluir, mas com uma capacidade reduzida do servidor real.
●	Offline. Os servidores reais estão inacessíveis ou não há servidores reais activados
●	Estado da constatação
●	IPs virtuais não licenciados ou licenciados excedidos

Nome

O nome do Serviço Virtual

Serviço virtual (VIP)

O endereço IP virtual e a porta para o serviço e o endereço que os utilizadores ou as aplicações irão utilizar.

Acerto/Segundo

Camada 7 transacções por segundo no lado do cliente.

Cache%

O valor aqui apresentado representa a percentagem de objectos que foram servidos a partir da Cache RAM do ADC.

Compressão%

Este valor representa a percentagem de objectos que foram comprimidos entre o cliente e o ADC.

Estado RS (Servidor remoto)

A tabela abaixo descreve o significado do estado dos Servidores Reais ligados ao VIP.

Estado	Descrição
●	Ligado
●	Não monitorizado
●	Drenagem ou offline
●	Em espera
●	Não ligado
●	Estado da constatação
●	IPs virtuais não licenciados ou licenciados excedidos

Servidor real

O endereço IP e a porta do servidor real.

Notas

Este valor pode ser constituído por quaisquer notas úteis para que os outros compreendam o objetivo da entrada.

Conns (Ligações)

A representação do número de ligações a cada Servidor Real permite-lhe ver o balanceamento de carga em ação. Muito útil para verificar se a sua política de balanceamento de carga está a funcionar corretamente.

Dados

O valor desta coluna mostra a quantidade de dados que estão a ser enviados para cada Servidor Real.

Req/Sec (Pedidos por segundo)

O número de pedidos por segundo enviados para cada Servidor Real.

Sistema

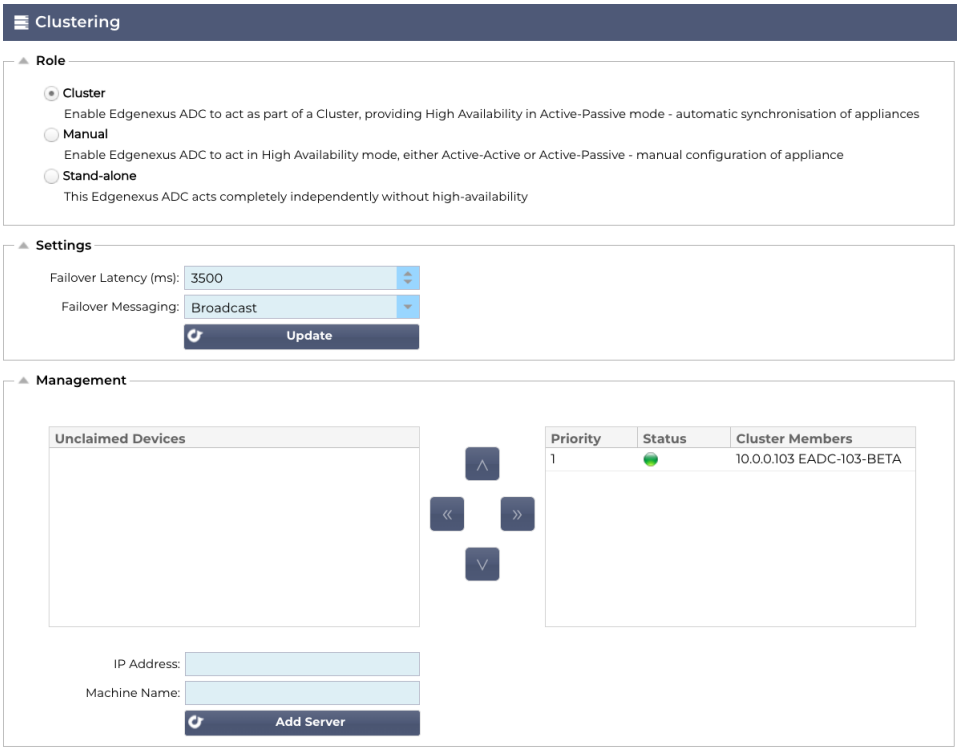
Agrupamento

O ADC pode ser utilizado como um único dispositivo autónomo, e funcionará perfeitamente bem nesse caso. No entanto, quando se considera que o objetivo do ADC é equilibrar a carga de conjuntos de servidores, a necessidade de agrupar o próprio ADC torna-se evidente. O design da interface de utilizador facilmente navegável do ADC torna a configuração do sistema de agrupamento simples.

A página Sistema > Clustering é onde se configura a alta disponibilidade dos dispositivos ADC. Esta secção está organizada em várias secções.

Nota importante

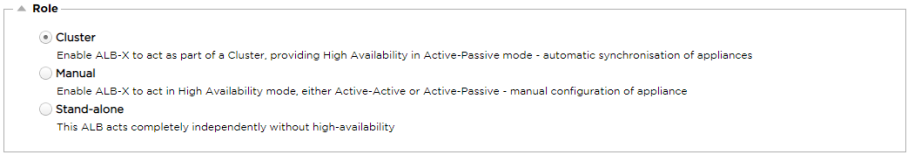
- Não é necessário um cabo dedicado entre o par de ADCs para manter um heartbeat de alta disponibilidade.
- O heartbeat tem lugar na mesma rede que o Serviço Virtual que requer a implementação de alta disponibilidade.
- Não há failover de estado entre os dispositivos ADC.
- Quando a alta disponibilidade estiver activada em dois ou mais ADC, cada caixa transmitirá via UDP os Serviços virtuais que está configurada para fornecer.
- O fail-over de alta disponibilidade utiliza mensagens unicast e ARP gratuito para informar os novos comutadores do balanceador de carga ativo.



Papel

Existem três funções de cluster disponíveis quando se configura o ADC para alta disponibilidade.

Aglomerado



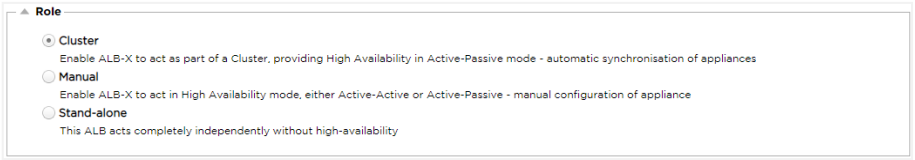
- Por padrão, um novo ADC será ligado usando a função Cluster. Nesta função, cada membro do cluster terá a mesma "configuração de trabalho" e, como tal, apenas um ADC no cluster estará ativo de cada vez.
- Uma "configuração de trabalho" significa todos os parâmetros de configuração, exceto os itens que têm de ser únicos, como o endereço IP de gestão, o nome ALB, as definições de rede, os detalhes da interface, etc.
- O ADC na prioridade 1, a posição mais alta, da caixa Membros do cluster é o proprietário do cluster e o balanceador de carga ativo, enquanto todos os outros ADCs são membros passivos.
- É possível editar qualquer ADC no Cluster, e as alterações serão sincronizadas com todos os membros do Cluster.
- Quando você remove um ADC do cluster, todos os serviços virtuais serão excluídos desse ADC.
- Não é possível remover o último membro do Cluster para Dispositivos não reclamados. Para remover o último membro, altere a função para Manual ou Autónomo.
- Os seguintes objectos não estão sincronizados:
    - Secção Data e hora manual - (A secção NTP está sincronizada)
    - Latência de ativação pós-falha (ms)
    - Secção de hardware
    - Secção de aparelhos
    - Secção de rede

Falha do proprietário do cluster

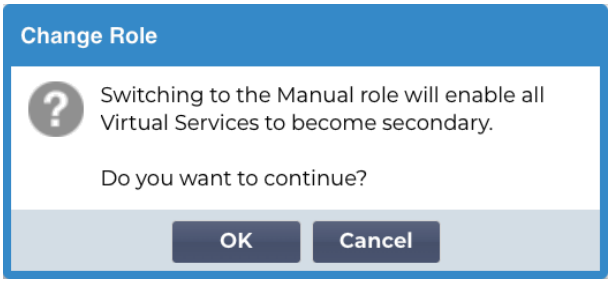
- Quando um proprietário de cluster falha, um dos membros restantes assume automaticamente o controlo e continua a equilibrar a carga do tráfego.
- Quando o proprietário do cluster regressar, retomará o tráfego de equilíbrio de carga e assumirá a função de proprietário.
- Vamos supor que o Proprietário falhou e um Membro assumiu o balanceamento de carga. Se pretender que o membro que assumiu o balanceamento de carga se torne o novo proprietário, selecione o membro e clique na seta para cima para o mover para a posição de Prioridade 1.
- Se editar um dos restantes membros do cluster e o proprietário estiver inativo, o membro editado será automaticamente promovido a proprietário sem perda de tráfego

Modificação de função de Cluster para função Manual

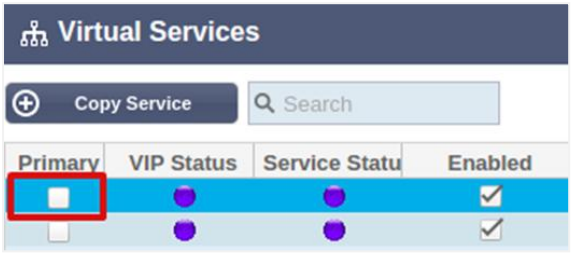
- Se pretender alterar a função de Cluster para Manual, clique no botão de rádio junto à opção de função Manual



- Depois de clicar no botão de rádio, verá a seguinte mensagem:



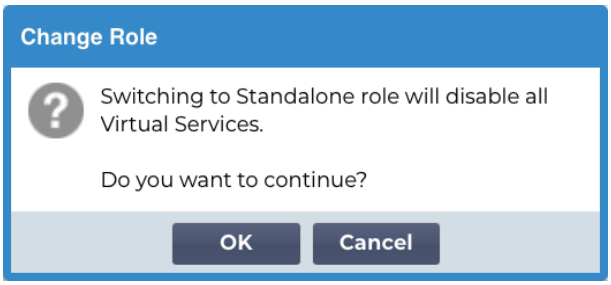
- Clique no botão OK
- Verifique a secção Serviços virtuais. Verificará que a coluna Primário apresenta agora uma caixa desmarcada.



- É uma caraterística de segurança e significa que, se tiver outro ADC com os mesmos Serviços Virtuais, não haverá interrupção do fluxo de tráfego.

Mudança de função de Cluster para Autónomo

- Se pretender alterar a função de Cluster para Autónomo, clique no botão de rádio junto à opção Autónomo.
- Ser-lhe-á apresentada a seguinte mensagem:



- Clique em OK para alterar as funções.
- Verifique os seus Serviços virtuais. Verá que a coluna Primário mudou de nome para Autónomo
- Verá também que todos os serviços virtuais estão desactivados (desmarcados) por razões de segurança.
- Quando tiver a certeza de que nenhum outro ADC na mesma rede tem Serviços Virtuais duplicados, pode ativar cada um deles.

Função manual

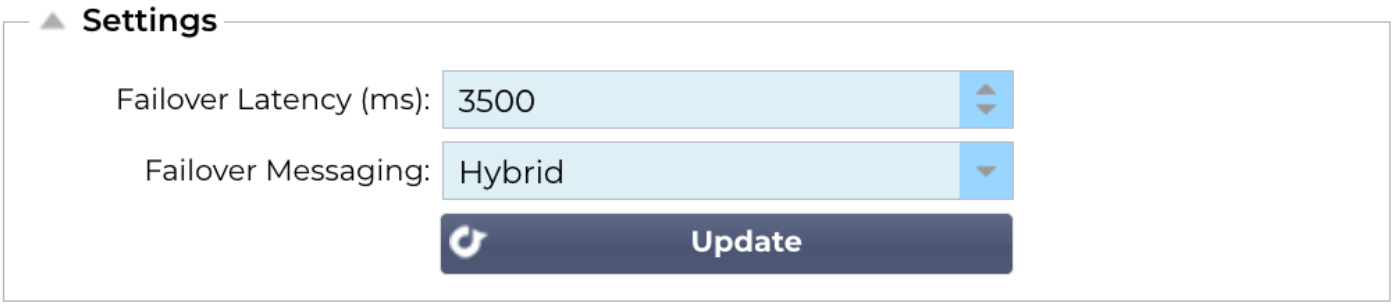
Um ADC na função Manual trabalhará com outros ADCs na função Manual para fornecer alta disponibilidade. A principal vantagem em relação à função Cluster é a capacidade de definir qual ADC está ativo para um IP virtual. A desvantagem é que não há sincronização de configuração entre os ADCs. Quaisquer alterações devem ser replicadas manualmente em cada caixa através da GUI, ou para muitas alterações, pode criar um jetPACK a partir de um ADC e enviá-lo para o outro.

- Para tornar um endereço IP virtual "ativo", assinale a caixa de verificação na coluna principal (página Serviços IP)
- Para tornar um endereço IP virtual "Passivo", deixe a caixa de verificação em branco na coluna principal (página Serviços IP)
- No caso de um serviço Ativo falhar para o Passivo:
    - Se ambas as colunas primárias estiverem assinaladas, é realizado um processo de eleição e o endereço MAC mais baixo fica ativo
    - Se ambos estiverem desmarcados, ocorre o mesmo processo de eleição. Além disso, se ambos estiverem desmarcados, não há retrocesso automático para o ADC ativo original

Papel autónomo

Um ADC na função Autónomo não comunicará com qualquer outro ADC relativamente aos seus serviços e, por conseguinte, todos os Serviços Virtuais permanecerão no estado Verde e ligados. Deve certificar-se de que todos os Virtual Services têm endereços IP únicos, caso contrário haverá um conflito na sua rede.

Definições

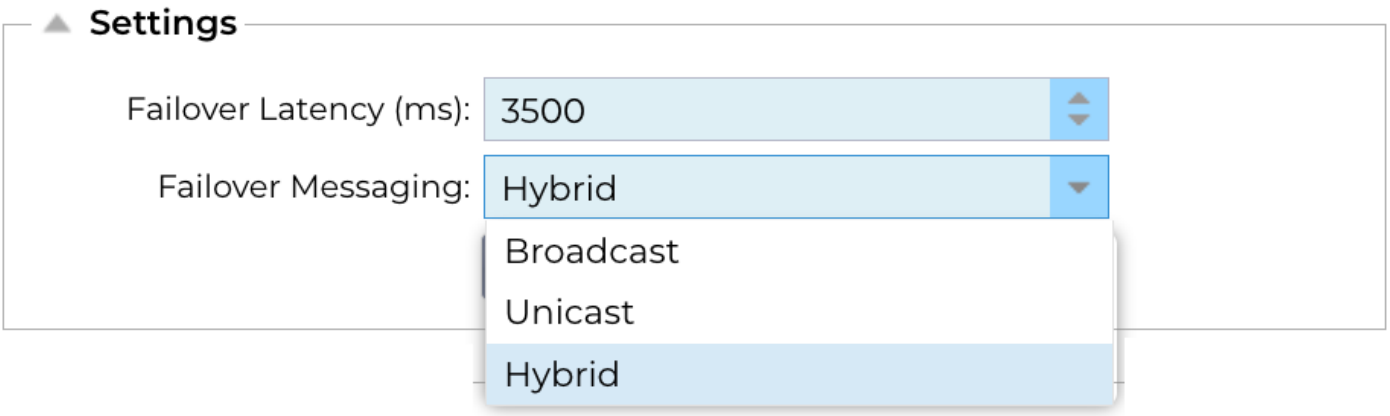


Latência de ativação pós-falha (ms)

É possível definir a Latência de Failover em milissegundos. Este é o tempo que um ADC passivo aguardará antes de assumir os serviços virtuais após a falha do ADC ativo.

Recomendamos que defina este valor para 10000ms ou 10 segundos, mas pode diminuir ou aumentar este valor para se adequar à sua rede e aos seus requisitos. Os valores aceitáveis situam-se entre 1500ms e 20000ms. Se sentir instabilidade no cluster com uma latência mais baixa, deve aumentar este valor.

Mensagens em Failover

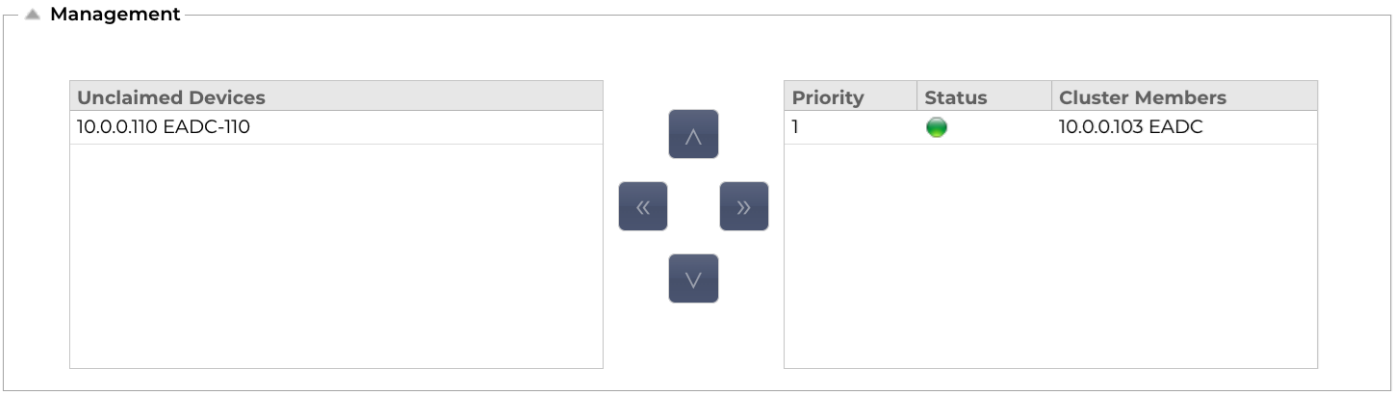


Por predefinição, o ADC utiliza Broadcast para o envio de mensagens de ativação pós-falha. No entanto, algumas redes bloqueiam a difusão, pelo que disponibilizámos Unicast e Hybrid, uma mistura de Unicast e Broadcast.

Quando estiver a funcionar no modo de difusão predefinido, os dispositivos não reclamados serão automaticamente listados e as mensagens de difusão serão utilizadas para ativação pós-falha. Quando estiver a ser executado no modo Híbrido, os dispositivos não reclamados continuarão a anunciar através de Broadcast, mas a comunicação de ativação pós-falha será feita através de Unicast. O modo Unicast não transmitirá como tal, e poderá ser necessário introduzir manualmente os membros do cluster.

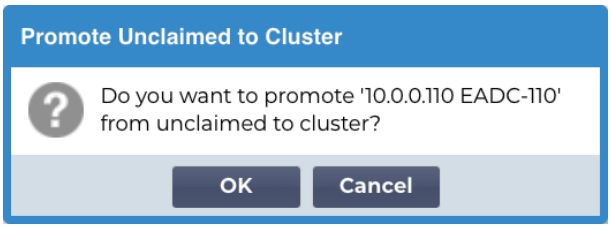
Gestão

Nesta secção, é possível adicionar e remover membros do cluster, bem como alterar a prioridade de um ADC no cluster. A secção é composta por dois painéis e um conjunto de teclas de seta no meio. A área à esquerda é a dos Dispositivos não reclamados, enquanto a área mais à direita é o próprio Cluster.

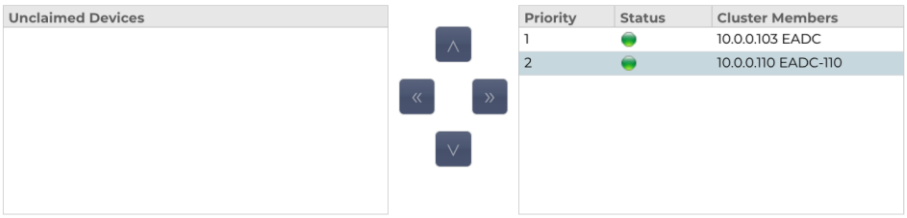


Adicionar um ADC ao cluster

- Antes de adicionar o ADC ao cluster, deve certificar-se de que todos os dispositivos ADC foram fornecidos com um nome único definido na secção Sistema > Rede.
- Deverá ver o ADC como Prioridade 1 com Estado verde e o seu nome na coluna Membros do Cluster na secção de gestão. Este ADC é o dispositivo primário predefinido.
- Todos os outros ADCs disponíveis aparecerão na janela Dispositivos não reclamados na secção de gestão. Um dispositivo não reclamado é o ADC que foi atribuído na função de cluster, mas não tem serviços virtuais configurados.
- Realce o ADC na janela Dispositivos não reclamados e clique no botão de seta para a direita.
- Aparecerá a seguinte mensagem:

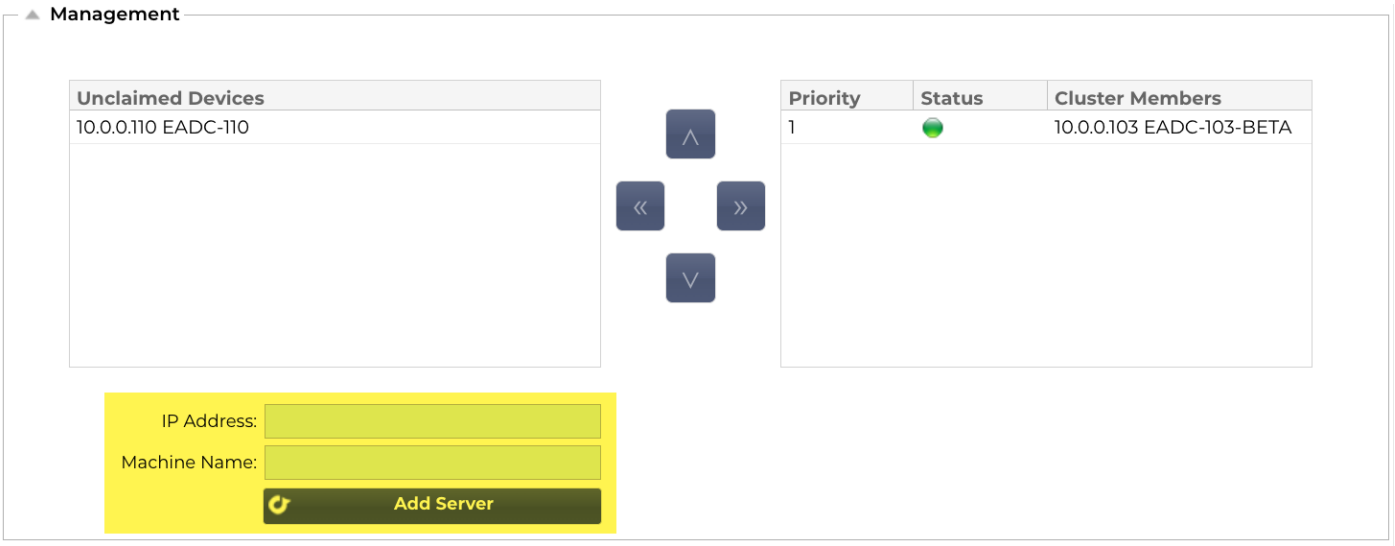


- Clique em OK para promover o ADC para o cluster.
- O seu ADC deve agora ser apresentado como Prioridade 2 na lista de membros do cluster.



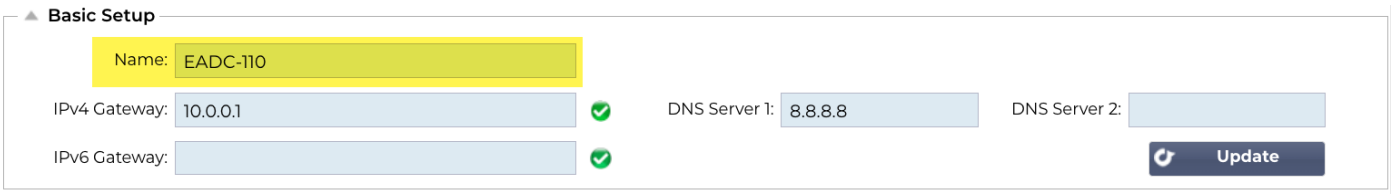
Adicionar manualmente um ADC ao cluster

Nos sistemas em que a Difusão está bloqueada, terá de escolher o modo Unicast ou Híbrido para adicionar um ADC ao cluster.



Para adicionar um ADC manualmente ao cluster:

1. Fornecer o seu endereço IP
2. Forneça o Nome da máquina - este está disponível na secção Sistema > Rede.



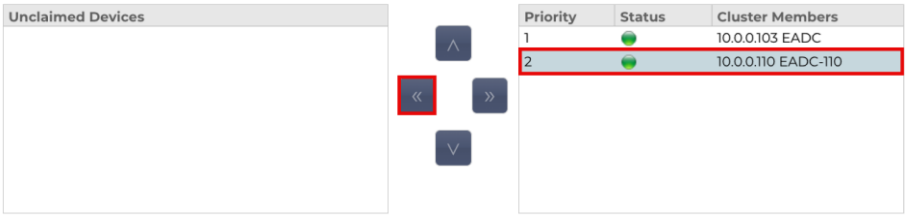
3. Clique em Adicionar servidor

O ADC será então adicionado ao cluster.

Se o ADC que está a tentar adicionar já estiver num cluster, será notificado através de uma mensagem de erro.

Remoção de um membro do cluster

- Realce o membro do cluster que pretende remover do cluster.
- Clique no botão de seta para a esquerda.



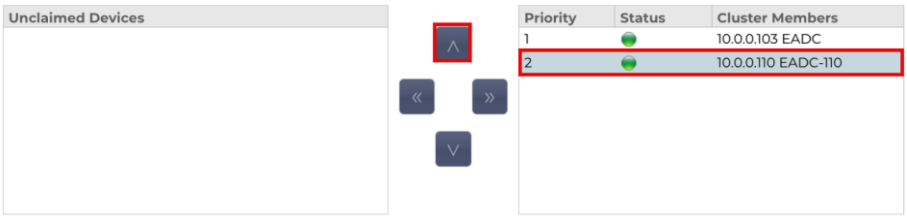
- Ser-lhe-á apresentado um pedido de confirmação.
- Clique em OK para confirmar.
- O seu ADC será removido e será apresentado no lado dos Dispositivos não reclamados.

Alterar a prioridade de um ADC

Pode haver alturas em que se pretenda alterar a prioridade de uma ADC na lista de membros.

- O ADC no topo da lista de membros do cluster recebe a prioridade 1 e é o ADC ativo para todos os serviços virtuais
- O ADC que está em segundo lugar na lista recebe a Prioridade 2 e é o ADC Passivo para todos os Serviços Virtuais

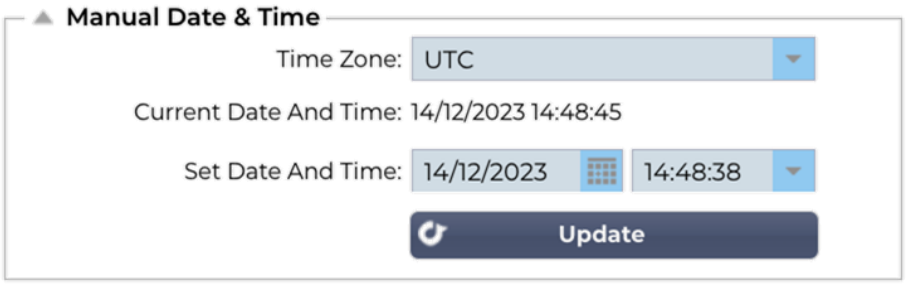
- Para alterar qual o ADC que está ativo, basta realçar o ADC e clicar na seta para cima até estar no topo da lista



Data e hora

A secção de data e hora permite a definição das caraterísticas de data/hora do ADC, incluindo o fuso horário em que o ADC se encontra. Juntamente com o fuso horário, a data e a hora desempenham um papel vital nos processos criptográficos associados à encriptação SSL.

Data e hora manuais



Fuso horário

O valor definido neste campo representa o fuso horário em que o ADC está localizado.

- Clique na caixa pendente para o fuso horário e comece a escrever a sua localização.
- Por exemplo, Londres
- Quando se começa a escrever, o ADC mostra automaticamente as localizações que contêm a letra L.
- Continue a escrever "Lon", e assim por diante - os locais listados serão reduzidos aos que contêm "Lon".
- Se estiver, por exemplo, em Londres, selecione Europa/Londres para definir a sua localização

Se a data e a hora continuarem incorrectas após a alteração acima referida, altere a data manualmente

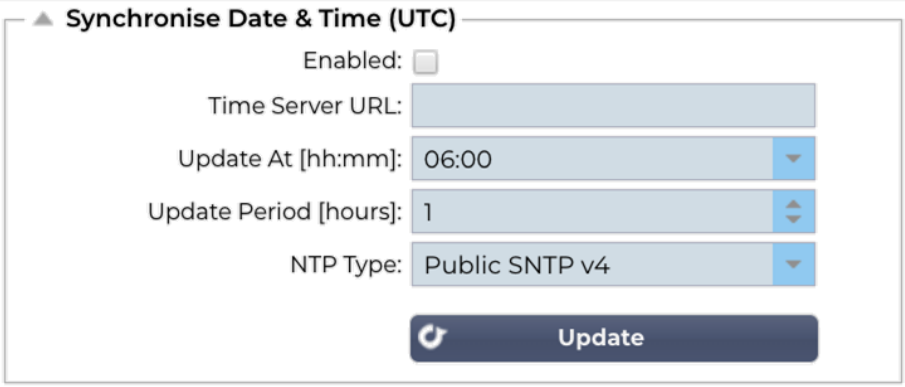
Definir data e hora

Esta definição representa a data e a hora actuais.

- Escolha a data correta na primeira lista pendente ou,
  em alternativa, pode escrever a data no seguinte formato DD/MM/AAAA
- Adicione a hora no seguinte formato hh: mm: ss, por exemplo, 06:00:10 para 6 horas e 10 segundos.
- Depois de o ter introduzido corretamente, clique em Atualizar para se candidatar.
- Deverá então ver a nova data e hora em caracteres a negrito.

Sincronizar data e hora (UTC)

Pode utilizar servidores NTP para sincronizar a data e a hora com precisão. Os servidores NTP estão localizados globalmente, e também pode ter o seu próprio servidor NTP interno quando a sua infraestrutura tem limitações de acesso externo.



URL do servidor de hora

Introduza um endereço IP válido ou um nome de domínio totalmente qualificado (FQDN) para o servidor NTP. Se o servidor for um servidor localizado globalmente na Internet, recomendamos a utilização de um FQDN.

Atualização em [hh:mm]

Selecione a hora programada em que pretende que o ADC se sincronize com o servidor NTP.

Período de atualização [horas]:

Selecione a frequência com que pretende que a sincronização ocorra.

Tipo de NTP:

- SNTP V4 público - Este é o método atual e preferido para sincronizar com um servidor NTP. **RFC 5905**
- NTP v1 sobre TCP - Versão antiga do NTP sobre TCP. **RFC 1059**
- NTP v1 sobre UDP - Versão antiga do NTP sobre UDP. **RFC 1059**

Nota: Tenha em atenção que a sincronização é efectuada apenas em UTC. Se pretender definir uma hora local, isso só pode ser feito manualmente. Esta limitação será alterada em versões posteriores para permitir a capacidade de selecionar um fuso horário.

Eventos por correio eletrónico

O ADC é um dispositivo crítico e, como qualquer sistema essencial, está equipado com a capacidade de informar o administrador de sistemas sobre quaisquer problemas que possam exigir atenção.

A página Sistema > Eventos de correio eletrónico permite-lhe configurar uma ligação ao servidor de correio eletrónico e enviar notificações aos administradores do sistema. A página está organizada nas secções abaixo.

Endereço

Enviar para eventos de correio eletrónico para endereços de correio eletrónico

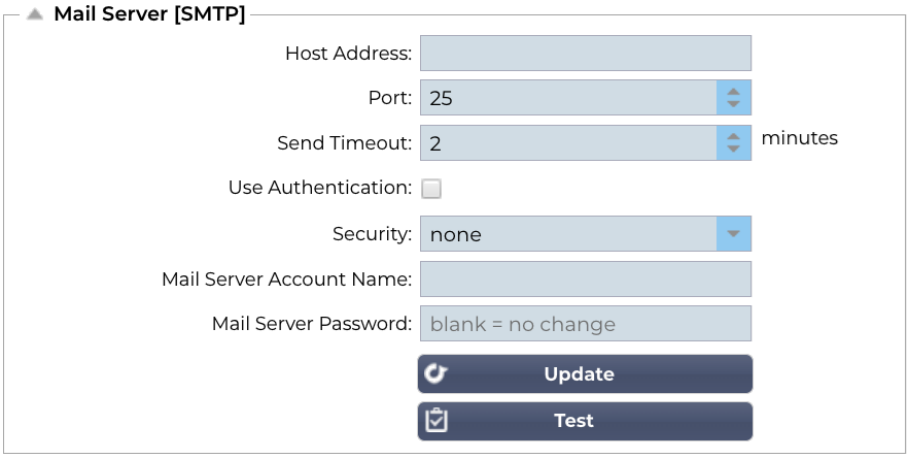
Adicione um endereço de correio eletrónico válido para o qual enviar os alertas, notificações e eventos. Exemplosupport@domain.com . Também pode adicionar vários endereços de correio eletrónico utilizando um separador de vírgulas.

Endereço de correio eletrónico de retorno:

Adicione um endereço de correio eletrónico que aparecerá na caixa de entrada. Exemplo . adc@domain.com

Servidor de correio eletrónico (SMTP)

Nesta secção, tem de adicionar os detalhes do servidor SMTP a utilizar para enviar as mensagens de correio eletrónico. Certifique-se de que o endereço de correio eletrónico que utiliza para o envio está autorizado a fazê-lo.



Endereço do anfitrião

Adicione o FQDN ou o endereço IP do seu servidor SMTP.

Porto

Adicione a porta do seu servidor SMTP. A porta predefinida para SMTP é 25 ou 587 se utilizar SSL.

Tempo limite de envio

Adicione um tempo limite de SMTP. A predefinição é de 2 minutos.

Utilizar autenticação

Assinale a caixa se o seu servidor SMTP exigir autenticação.

Segurança

- Nenhum
- A definição predefinida é nenhum.
- SSL - Utilize esta definição se o seu servidor SMTP exigir autenticação Secure Sockets Layer.
- TLS - Utilize esta definição se o seu servidor SMTP exigir autenticação Transport Layer Security.

Nome da conta do servidor principal

Adicione o nome de utilizador necessário para a autenticação.

Palavra-passe do servidor de correio eletrónico

Adicione a palavra-passe necessária para a autenticação.

Notificações e alertas

Existem vários tipos de notificações de eventos que o ADC envia às pessoas configuradas para as receber. É possível marcar e ativar as notificações e alertas que devem ser enviados. As notificações ocorrem quando os Servidores reais são contactados ou os canais iniciados. Os alertas ocorrem quando os Servidores reais não podem ser contactados ou os canais deixam de funcionar.

Serviço IP Aviso

O aviso do Serviço IP informá-lo-á quando qualquer endereço IP virtual estiver online ou tiver deixado de funcionar. Esta ação é executada para todos os serviços virtuais que pertencem ao VIP.

Serviço virtual Aviso

Informa o destinatário de que um Serviço Virtual está online ou deixou de funcionar.

Servidor real Aviso

Quando um Servidor Real e uma Porta estão ligados ou não estão contactáveis, o ADC envia um aviso ao Servidor Real.

flightPATH

Este aviso é um e-mail enviado quando uma condição é cumprida e existe uma ação configurada que instrui o ADC a enviar o evento por e-mail.

Agrupar notificações

Assinale para agrupar notificações. Com esta opção assinalada, todas as notificações e alertas serão agregados num único e-mail.

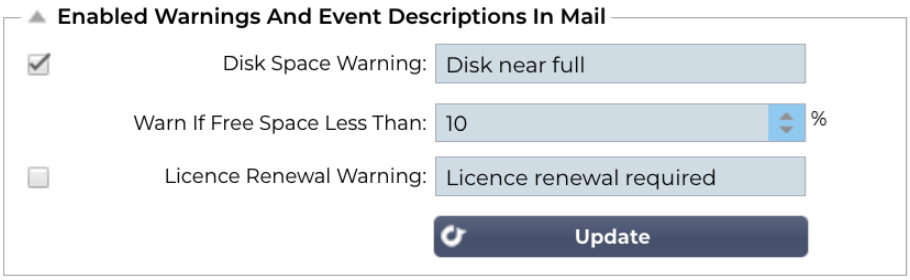
Correio de grupo Descrição

Especifique o assunto relevante para a mensagem de correio eletrónico de aviso de grupo.

Intervalo de envio do grupo

Estipule o período de tempo que pretende aguardar antes de enviar uma mensagem de correio eletrónico de notificação de grupo. O tempo mínimo é de 2 minutos. A predefinição é de 30 minutos.

Avisos activados e descrições de eventos no Mail



Existem dois tipos de mensagens electrónicas de aviso, e nenhuma delas deve ser ignorada.

Espaço em disco

Defina a percentagem de espaço livre em disco antes da qual o aviso é enviado. Quando este valor for atingido, ser-lhe-á enviado um e-mail.

Avisar se o espaço livre for inferior a

Pode definir aqui um valor percentual para que o ADC possa enviar um e-mail de aviso caso o espaço em disco desça abaixo deste limite.

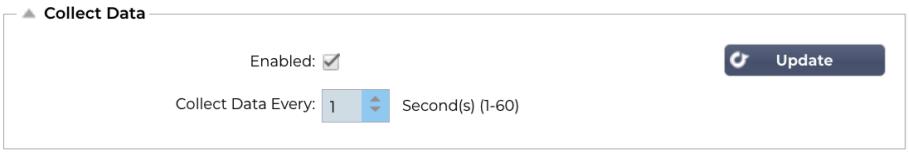
Caducidade da licença

Esta definição permite-lhe ativar ou desativar o e-mail de aviso de expiração da licença enviado para o administrador do sistema. Quando este valor for atingido, ser-lhe-á enviado um e-mail.

História

Na secção Sistema, existe a opção Histórico do sistema, que permite o fornecimento de dados históricos para elementos como CPU, memória, pedidos por segundo e outras caraterísticas. Uma vez activada, pode visualizar os resultados em forma de gráfico através da página Ver > Histórico. Esta página também permite fazer uma cópia de segurança ou restaurar os ficheiros de histórico para o ADC local.

Recolher dados



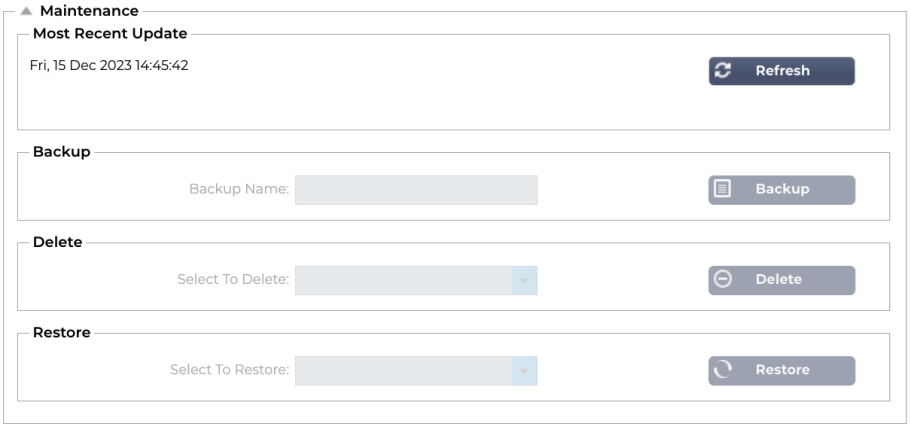
Ativar

Para permitir a recolha de dados, assinale a caixa de verificação.

Recolher dados todos os dias

De seguida, defina o intervalo de tempo em que pretende que o ADC recolha os dados. Este valor de tempo pode variar entre 1 e 60 segundos.

Manutenção



Atualização mais recente

Mostra quando foram recolhidos os últimos dados do histórico do ADC.

Esta secção ficará a cinzento se tiver ativado o registo histórico. Desmarque a caixa de verificação Ativado na secção Recolher dados e clique em Atualizar para permitir a manutenção dos registos históricos.

ADCs baseados em empresas HP

Esta secção de funcionalidades só é válida para ADCs que estejam instalados em servidores HPE ProLiant bare metal e utilizem ILO.

Cópia de segurança

Dê um nome descritivo ao seu backup. Clique em Backup para fazer backup de todos os arquivos para o ADC

Eliminar

Selecione um ficheiro de cópia de segurança a partir da lista pendente. Clique em Excluir para remover o arquivo de backup do ADC

Restaurar

Selecione um ficheiro de cópia de segurança armazenado anteriormente. Clique em Restaurar para preencher os dados deste ficheiro de cópia de segurança.

Licença

O ADC é licenciado para utilização através de um dos seguintes modelos, que depende dos parâmetros de compra e do tipo de cliente.

Tipo de licença	Descrição
Perpétuo	O cliente tem o direito de utilizar o ADC e outro software de forma perpétua. Tal não impede que tenha de adquirir suporte para receber assistência e actualizações.
SaaS	SaaS ou Software-as-a-Service significa que, essencialmente, aluga o software numa base contínua ou de pagamento conforme o uso. Neste modelo, o utilizador paga um aluguer anual pelo software. O utilizador não tem direitos perpétuos de utilização do software.
MSP	Os Managed Service Providers podem oferecer o ADC como um serviço e adquirir a licença numa base por VIP, cobrada e paga anualmente.

Detalhes da licença

Cada licença inclui pormenores específicos pertinentes para a pessoa ou organização que a adquire.

ID da licença

O ID da licença está diretamente ligado ao ID da máquina e a outros detalhes específicos da sua compra e do dispositivo ADC. Esta informação é essencial e é necessária quando se pretende obter actualizações e outros itens da App Store.

ID da máquina

A ID da máquina é gerada usando o endereço IP eth0 do dispositivo ADC. Se alterar o endereço IP do dispositivo ADC, a licença deixará de ser válida. Terá de contactar o suporte para obter assistência. Recomendamos que o(s) seu(s) dispositivo(s) ADC tenha(m) endereços IP fixos com instruções para que o seu pessoal de TI não os altere. O suporte técnico está disponível através da criação de um bilhete em https://www.edgenexus.io/support.

Nota: Não deve alterar o endereço IP dos seus dispositivos ADC. Se estiver numa estrutura virtualizada, corrija a ID MAC e utilize um endereço IP estático.

Emitido para

Este valor contém o nome do comprador associado à ID da máquina do ADC.

Pessoa de contacto

Este valor contém a pessoa de contacto a ser contactada na empresa do cliente associada à ID da máquina

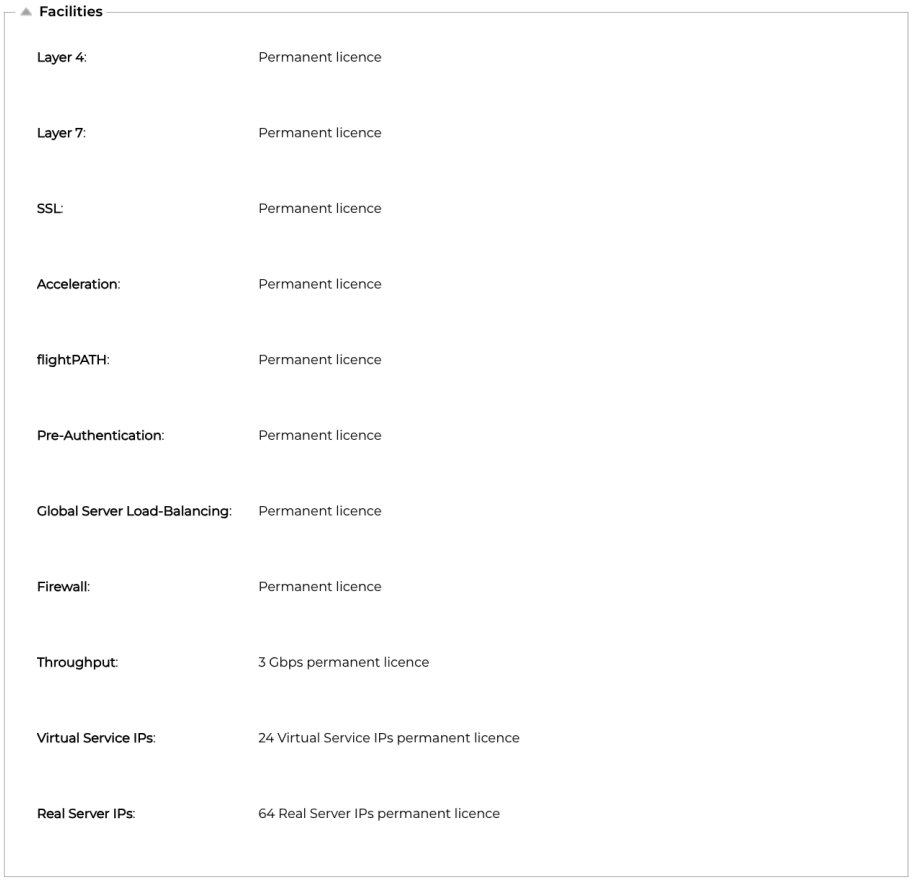
Data de emissão d

A data em que a licença foi emitida.

Nome

Este valor mostra o nome descritivo do aparelho ADC que forneceu em Sistema > Rede.

Instalações



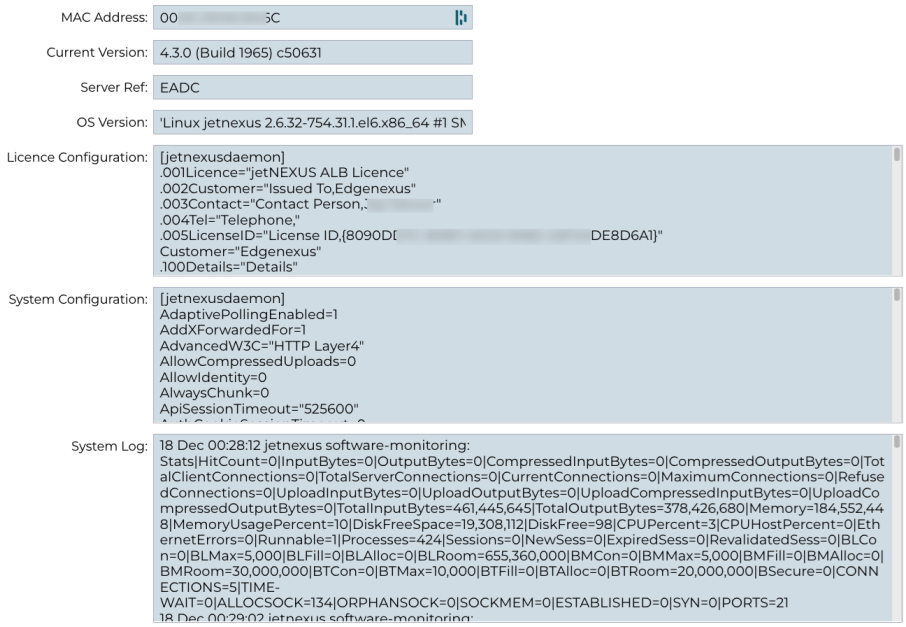
A secção de recursos fornece informações sobre as funções do ADC que foram licenciadas para utilização e a validade da licença. Também é exibida a taxa de transferência que foi licenciada para o ADC e o número de Servidores Reais. Estas informações dependem da licença adquirida.

Instalar licenças e

- A instalação de uma nova licença é muito simples. Quando receber a sua licença nova ou de substituição da Edgenexus, esta será enviada sob a forma de um ficheiro de texto. Pode abrir o ficheiro e depois copiar e colar o conteúdo no campo Colar Licença.
- Também pode carregá-lo para a ADC se copiar/colar não for uma opção para si.
- Depois de o ter feito, clique no botão de atualização.
- A licença está agora instalada.

Informações sobre o serviço de licenças

Ao clicar no botão Informações sobre o serviço de licença, são apresentadas todas as informações sobre a licença. Esta função pode ser utilizada para enviar os detalhes ao pessoal de apoio.

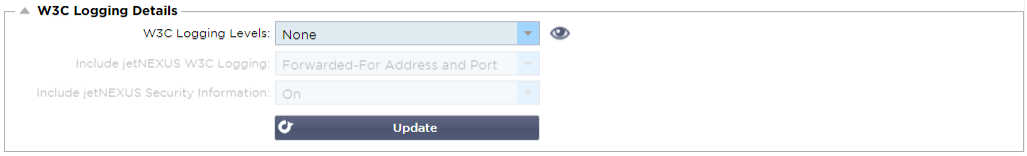


Registo

A página Sistema > Registo permite-lhe definir os níveis de registo W3C e especificar o servidor remoto para o qual os registos serão exportados automaticamente. A página está organizada nas quatro secções abaixo.

Detalhes do registo W3C

A ativação do registo W3C fará com que o ADC comece a gravar um ficheiro de registo compatível com W3C. Um registo W3C é um registo de acesso para servidores Web em que são gerados ficheiros de texto contendo dados sobre cada pedido de acesso, incluindo o endereço IP (Internet Protocol) de origem, a versão HTTP, o tipo de browser, a página de referência e o carimbo de data/hora. O formato foi desenvolvido pelo World Wide Web Consortium (W3C), uma organização que promove normas para a evolução da Web. O ficheiro está em texto ASCII, com colunas delimitadas por espaços. O ficheiro contém linhas de comentário que começam com o carácter #. Uma dessas linhas de comentário é uma linha que indica os campos (fornecendo nomes de colunas) para que os dados possam ser extraídos. Existem ficheiros separados para os protocolos HTTP e FTP.



Níveis de registo W3C

Existem diferentes níveis de registo disponíveis e, dependendo do tipo de serviço, os dados fornecidos variam.

A tabela acima descreve os níveis de registo para W3C HTTP.

Valor	Descrição
Nenhum	O registo W3C está desativado.
Breve	Os campos presentes são: #Campos: 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).
Completo	Este é um formato mais compatível com o processador, com campos de data e hora separados. Para obter informações sobre o significado dos campos, consulte o resumo dos campos abaixo. Os campos presentes são: #Campos: 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).
Sítio	Este formato é muito semelhante ao "Completo", mas tem um campo adicional. Consulte o resumo dos campos abaixo para obter informações sobre o significado dos campos. Os campos presentes são: #Campos: 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).
Diagnóstico	Este formato é preenchido com todo o tipo de informações relevantes para o pessoal de desenvolvimento e de apoio. Para obter informações sobre o significado dos campos, consulte o resumo dos campos abaixo. Os campos presentes são: #Campos: date time 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

A tabela abaixo descreve os níveis de registo para o W3C FTP.

Valor	Descrição
Breve	#Campos: 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
Completo	#Campos: 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
Diagnóstico	#Campos: 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

Incluir o registo W3C

Esta opção permite-lhe definir que informações do ADC devem ser incluídas nos registos do W3C.

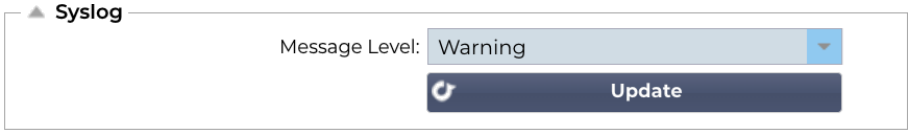
Valor	Descrição
Endereço e porta de rede do cliente	O valor aqui apresentado mostra o endereço IP real do cliente juntamente com a porta.
Endereço de rede do cliente	Esta opção inclui e mostra apenas o endereço IP real do cliente.
Endereço e porta de encaminhamento	Esta opção mostrará os detalhes contidos no cabeçalho XFF, incluindo o endereço e a porta.
Endereço para envio	Esta opção mostra os pormenores contidos no cabeçalho XFF, incluindo apenas o endereço.

Incluir informações de segurança

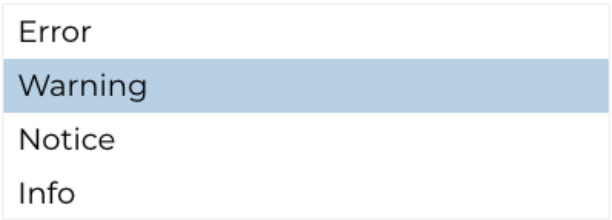
Este menu é composto por duas opções:

Valor	Descrição
Em	Esta definição é global. Quando definido como ligado, o nome de utilizador será anexado ao registo W3C quando qualquer Serviço Virtual estiver a utilizar a Autenticação e tiver o registo W3C ativado.
Desligado	Isto irá desativar a capacidade de registar o nome de utilizador no registo do W3C a nível global.

Servidor Syslog



Esta secção permite-lhe definir o nível de registo de mensagens efectuado no servidor SYSLOG. As opções disponíveis são as seguintes.

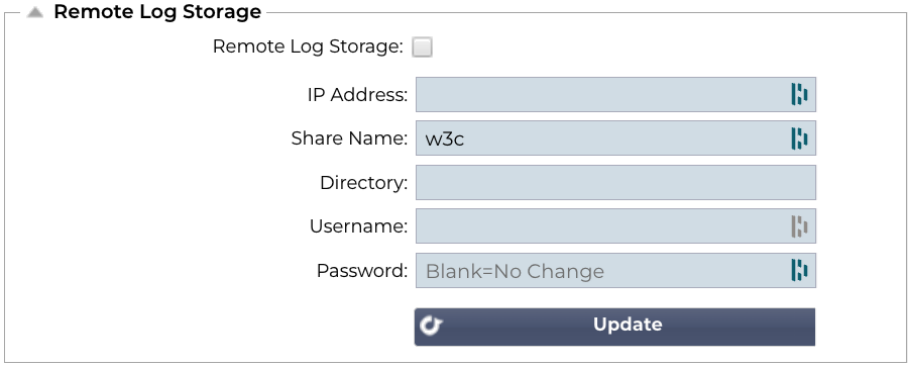


Servidor Syslog remoto

Nesta secção, pode configurar dois servidores Syslog externos para enviar todos os registos do sistema.

- Adicione o endereço IP do seu servidor Syslog
- Adicionar o porto
- Escolha se pretende utilizar TCP ou UDP
- Assinale a caixa de verificação Ativado para iniciar o registo
- Clique em Atualizar

Armazenamento remoto de registos



Todos os registos do W3C são armazenados em formato comprimido no ADC de hora a hora. Os ficheiros mais antigos serão eliminados quando restarem 30% do espaço em disco. Se pretender exportar estes ficheiros para um servidor remoto para os guardar, pode configurá-lo utilizando uma partilha SMB. Tenha em atenção que o registo W3C não será transferido para a localização remota até que o ficheiro tenha sido concluído e comprimido. Como os registos são escritos a cada hora, isto pode demorar até duas horas numa máquina virtual e cinco horas numa máquina de hardware.

Col1	**Col2**
Armazenamento remoto de registos	Assinale a caixa para ativar o armazenamento remoto de registos
Endereço IP	Especifique o endereço IP do seu servidor SMB. Este deve estar em notação decimal com pontos. Exemplo: 10.1.1.23
Nome da ação	Especifique o nome da partilha no servidor SMB. Exemplo: w3c.
Diretório	Especifique o diretório no servidor SMB. Exemplo: /log.
Nome de utilizador	Especifique o nome de utilizador para a partilha SMB.
Palavra-passe	Especificar a palavra-passe para a partilha SMB

Resumo do campo

Estado	**Descrição**
Data	Não localizado = sempre AAAA-MM-DD (GMT/UTC)
Tempo	Não localizado = HH:MM:SS ou HH:MM:SS.ZZZ (GMT/UTC) * Nota - infelizmente, isto tem dois formatos (Site

	não tem .ZZZ milissegundos)
x-mil	Apenas formato do sítio = milissegundos do carimbo de data/hora
c-ip	IP do cliente, o melhor que se pode deduzir da rede ou do cabeçalho X-Forwarded-For
porta c	Porta do cliente, conforme melhor se pode deduzir da rede ou do cabeçalho X-Forwarded-For
cs-username	Campo de pedido de nome de utilizador do cliente
s-ip	Porta de escuta do ALB
porta s	VIP de escuta da ALB
x-xff	Valor do cabeçalho X-Forwarded-For
x-xffcustom	Valor do cabeçalho do pedido do tipo X-Forwarded-For com nome configurado
cs-hospedeiro	Nome do anfitrião no pedido
x-r-ip	Endereço IP do servidor real utilizado
porta x-r	Porta do servidor real utilizada
método cs	Método de pedido HTTP * exceto formato Brief
método	* Apenas o formato breve utiliza este nome para cs-method
cs-uri-stem	Caminho do recurso solicitado * exceto formato Brief
cs-uri-query	Consulta do recurso solicitado * exceto formato Brief
uri	* O formato breve regista um caminho combinado e uma cadeia de consulta
sc-status	Código de resposta HTTP
cs(User-Agent)	Cadeia de caracteres User-Agent do navegador (tal como enviada pelo cliente)
referenciador	Página de referência (tal como enviada pelo cliente)
x-c-versão	Versão HTTP do pedido do cliente
x-r-versão	Conteúdo-Resposta do servidor Versão HTTP
cs-bytes	Bytes do cliente, no pedido
sr-bytes	Bytes encaminhados para o Real Server, no pedido
rs-bytes	Bytes do Real Server, na resposta
sc-bytes	Bytes enviados ao cliente, na resposta
x-percentagem	Percentagem de compressão * = 100 * (1 - saída / entrada) incluindo cabeçalhos
tempo gasto	Quanto tempo o Real Server demorou, em segundos
x-trip-times novo pcon	milissegundos desde a ligação até à publicação na "lista de novatos" milissegundos desde a ligação até ao estabelecimento da ligação ao Servidor Real
acon	milissegundos desde a ligação até à conclusão da ligação ao Servidor Real
rcon	milissegundos desde a ligação até ao estabelecimento da ligação ao servidor real
rqf	milissegundos desde a ligação até à receção do primeiro byte de pedido do cliente
rql	milissegundos desde a ligação até à receção do último byte do pedido do cliente
tqf	milissegundos desde a ligação até ao envio do primeiro byte do pedido ao Servidor Real
tql	milissegundos desde a ligação até ao envio do último byte do pedido ao Servidor Real
rsf	milissegundos desde a ligação até à receção do primeiro byte de resposta do Servidor Real
rsl	milissegundos desde a ligação até à receção do último byte de resposta do Servidor Real
tsf	milissegundos desde a ligação até ao envio do primeiro byte de resposta ao cliente
tsl	milissegundos desde a ligação até ao envio do último byte de resposta ao cliente

des	milissegundos entre a ligação e a desativação (ambos os lados - o último a desativar)
registo	milissegundos desde a ligação até este registo de registo, normalmente seguido de (Política de equilíbrio de carga e raciocínio)
x-tempo de ida e volta	Quanto tempo demorou o ALB em segundos
x-fechado-por	Que ação fez com que a ligação fosse encerrada (ou mantida aberta)
x-compress-action	Como é que a compressão foi efectuada ou evitada
x-sc(Content-Type)	Content-Type da resposta
x-cache-action	Como é que o armazenamento em cache respondeu ou foi impedido
x-acabamento	Acionador que causou esta linha de registo

Limpar ficheiros de registo

Esta função permite-lhe limpar os ficheiros de registo do dispositivo. Pode selecionar o tipo de registo que pretende eliminar a partir do menu pendente e, em seguida, clicar no botão Limpar.

Rede

A secção Rede da Biblioteca permite a configuração das interfaces de rede do ADC e do seu comportamento.

IMPORTANTE

Gerir interfaces de rede virtuais num ambiente virtual

Ao implantar VMs em um ambiente virtualizado como o ESXi, as interfaces de rede (por exemplo, eth0, eth1) são criadas automaticamente e mapeadas para adaptadores de rede de configuração do host (por exemplo, Adaptador de rede 1, Adaptador de rede 2). No entanto, estes mapeamentos podem nem sempre estar alinhados de forma consistente devido às regras do sistema operativo que associam as interfaces a endereços MAC específicos. Esta seção descreve as etapas para gerenciar as interfaces de rede no host para evitar interrupções nos serviços quando o usuário não puder acessar a VM.

Considerações fundamentais

1. **Persistência do endereço MAC**:
    a. O sistema operativo atribui nomes de interface (por exemplo, eth0, eth1) com base em regras que associam um nome a um endereço MAC específico.
    b. Excluir e recriar uma interface de rede de VM sem reutilizar o endereço MAC original pode resultar em uma configuração de rede inconsistente ou não funcional.
2. **Mapeamentos internos no ADC (EdgeOS)**:
    a. As interfaces de rede virtual são automaticamente reconhecidas pelo ADC (Application Delivery Controller) e mapeadas internamente.
    b. A remoção de uma interface de rede do host da VM pode deixar mapeamentos obsoletos no ADC, potencialmente interrompendo o acesso de gerenciamento ou os serviços de rede.

Passos recomendados para a configuração do anfitrião

1. **Antes de remover uma placa de rede**:
    a. Registe o endereço MAC da interface que pretende remover. Isso pode ser visto nas configurações da VM no host ESXi.
2. **Ao adicionar uma placa de rede de substituição**:
    a. Atribua o endereço MAC gravado anteriormente ao novo adaptador de rede para garantir que os mapeamentos de interface da VM permaneçam consistentes.
3. **Evitar a eliminação acidental de NICs críticos**:
    a. Identifique quais NICs estão mapeadas para interfaces ADC críticas (por exemplo, ETH0 (Greenside) para acesso de gerenciamento). Evite remover essas NICs, a menos que seja absolutamente necessário.
4. **Verificar a consistência do endereço MAC**:
    a. Certifique-se de que os endereços MAC atribuídos às interfaces de rede da VM correspondem à configuração esperada no ADC. Use as ferramentas do host ESXi para confirmar esse mapeamento.
5. **Coordenar com os administradores de VM**:
    a. Se forem necessárias alterações que possam afetar a configuração interna da VM, informe os administradores da VM para se prepararem para potenciais interrupções e garantir que os mapeamentos adequados são mantidos.

Cenário de exemplo

1. **Configuração inicial**:
    a. A VM do ADC tem duas NICs: NIC1 (MAC: 00:11:22:33:44:55) e NIC2 (MAC: 00:11:22:33:44:66).
2. **Ação**: Remover o NIC1 e adicionar um novo NIC (NIC3).
    a. Atribua o endereço MAC original (00:11:22:33:44:55) ao NIC3 durante a criação no host ESXi.
3. **Evitar o impacto**:

   a. Ao reutilizar o endereço MAC original, os mapeamentos internos do ADC (por exemplo, ETH0) permanecem consistentes, evitando qualquer interrupção no acesso de gestão ou nos serviços de rede.

Ao gerenciar interfaces de rede em um ambiente virtualizado, é crucial manter a consistência nas atribuições de endereços MAC. Se o acesso à VM não estiver disponível, todas as etapas necessárias devem ser concluídas no lado do host para garantir uma operação contínua e evitar interrupções de serviço. Coordene sempre com os administradores relevantes para abordar os potenciais impactos de forma eficaz.

Evitando o vMotion frequente para dispositivos críticos

O vMotion é um poderoso recurso do VMware que permite a migração em tempo real de máquinas virtuais (VMs) entre hosts ESXi sem tempo de inatividade. No entanto, embora o vMotion seja muito útil para manter a flexibilidade e a disponibilidade da infraestrutura, não se recomenda a migração frequente de dispositivos críticos, como os balanceadores de carga, especialmente quando estes estão a gerir ativamente um elevado volume de ligações.

Podem existir outras tecnologias semelhantes e fornecidas por outros fornecedores, mas para esta secção, trabalharemos com base na VMware.

Por que o vMotion frequente não é recomendado

1. **Interrupções de sessão**:
   a. Os balanceadores de carga gerenciam sessões ativas entre clientes e servidores de back-end. Durante uma operação de vMotion, há um breve período em que o estado da rede é reinicializado, potencialmente interrompendo essas sessões.
   b. A interrupção pode causar quedas de ligação, obrigando os clientes a restabelecer as suas sessões, o que pode degradar a experiência do utilizador.
2. **Latência e perda de pacotes**:
   a. O processo de migração de uma VM envolve a pausa temporária e a sincronização da sua memória e estado. Para dispositivos que lidam com tráfego em tempo real, essa pausa pode introduzir latência ou até mesmo perda de pacotes.
   b. As aplicações que dependem de respostas de baixa latência podem registar um desempenho degradado ou tempos limite.
3. **Aumento da utilização de recursos**:
   a. O vMotion requer recursos de CPU, memória e largura de banda de rede para sincronização de dados entre os hosts de origem e destino.
   b. As migrações frequentes podem sobrecarregar os recursos da infraestrutura, afectando potencialmente outras VMs e serviços alojados no mesmo ambiente.
4. **Impacto nas configurações de alta disponibilidade**:
   a. Em ambientes com configurações de alta disponibilidade (HA), o vMotion frequente pode entrar em conflito com os mecanismos de failover, levando a um comportamento inesperado ou a atrasos nas acções de failover.
5. **Complexidade operacional**:
   a. A movimentação constante de VMs críticas aumenta a complexidade das configurações de rede, incluindo mapeamentos de VLAN e regras de firewall, o que pode introduzir erros de configuração.

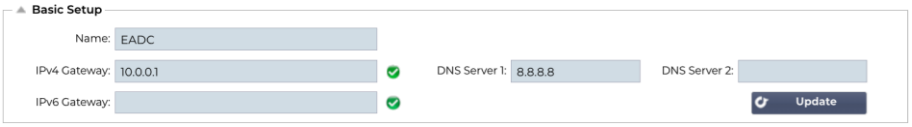
Recomendações para a gestão de aparelhos críticos

1. **Planejar operações de vMotion durante janelas de manutenção**:
   a. Programe as migrações durante períodos de pouco tráfego para minimizar o impacto nas sessões activas.
2. **Implementar o agrupamento de balanceadores de carga**:
   a. Utilize configurações de clustering ou de alta disponibilidade para os balanceadores de carga para garantir a redundância. Isto permite que o tráfego seja redireccionado sem problemas para outro nó durante as operações vMotion.
3. **Monitorizar os recursos de infra-estruturas**:

   a. Certifique-se de que CPU, memória e largura de banda de rede suficientes estejam disponíveis antes de iniciar o vMotion para evitar a contenção de recursos.
4. **Minimizar a frequência de migração**:
   a. Limite o vMotion de appliances críticos a cenários em que seja absolutamente necessário, como manutenção do host ou recuperação de falhas.
5. **Teste antes da produção**:
   a. Teste as operações do vMotion em um ambiente de preparação para entender seu impacto nas sessões ativas e garantir que as configurações sejam otimizadas.

Embora o vMotion seja uma ferramenta inestimável para o gerenciamento de VMs, ele deve ser usado criteriosamente para dispositivos críticos, como balanceadores de carga. As migrações frequentes podem interromper os serviços, aumentar a latência e sobrecarregar os recursos. Ao planear cuidadosamente as operações de vMotion e ao empregar estratégias como clustering e agendamento de manutenção, pode garantir uma prestação de serviços fiável e minimizar o risco de interrupções.

Configuração básica



Nome ALB

Especifique um nome para o seu dispositivo ADC. Observe que isso não pode ser alterado se houver mais de um membro no cluster. Consulte a secção sobre Clustering.

Gateway IPv4

Especifique o endereço de gateway IPv4. Este endereço terá de estar na mesma sub-rede que um adaptador existente. Se adicionar a Gateway incorretamente, verá uma Cruz branca num círculo vermelho. Quando adicionar uma gateway correta, verá uma faixa verde de sucesso na parte inferior da página e um visto branco num círculo verde junto ao endereço IP.

Gateway IPv6

Especifique o endereço de gateway IPv6. Este endereço terá de estar na mesma sub-rede que um adaptador existente. Se adicionar a Gateway incorretamente, verá uma Cruz branca num círculo vermelho. Quando adicionar uma gateway correta, verá uma faixa verde de sucesso na parte inferior da página e um visto branco num círculo verde junto ao endereço IP.

Servidor DNS 1 e Servidor DNS 2

Adicione o endereço IPv4 do seu primeiro e segundo (opcional) servidor DNS.

Detalhes do adaptador

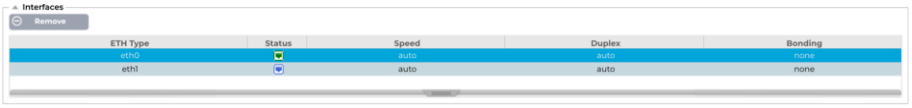
Esta secção do painel Rede mostra as interfaces de rede que estão instaladas no seu dispositivo ADC. É possível adicionar e remover adaptadores conforme necessário.

Coluna	**Descrição**

Adaptador	Esta coluna apresenta os adaptadores físicos instalados no seu aparelho. Escolha um adaptador da lista de adaptadores disponíveis clicando nele - um clique duplo colocará a linha de listagem no modo de edição.
VLAN	Faça duplo clique para adicionar o ID da VLAN para o adaptador. Uma VLAN é uma rede local virtual que cria um domínio de difusão distinto. Uma VLAN tem os mesmos atributos que uma LAN física, mas permite que as estações finais sejam agrupadas mais facilmente se não estiverem no mesmo comutador de rede
Endereço IP	Faça duplo clique para adicionar o endereço IP associado à interface do adaptador. É possível adicionar vários endereços IP à mesma interface. Este deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 192.168.101.2
Máscara de sub-rede	Faça duplo clique para adicionar a máscara de sub-rede atribuída à interface do adaptador. Este deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 255.255.255.0
Porta de entrada	Adicionar um gateway para a interface. Quando isto é adicionado, o ADC configura uma política simples que permite que as ligações iniciadas a partir desta interface sejam devolvidas através desta interface ao router de gateway especificado. Isso permite que o ADC seja instalado em ambientes de rede mais complexos sem o problema de configurar manualmente um roteamento complexo baseado em políticas.
Descrição	Faça duplo clique para adicionar uma descrição para o seu adaptador. Exemplo de interface pública. Nota: O ADC designará automaticamente a primeira interface como Lado Verde, a segunda interface como Lado Vermelho e a terceira interface como Lado 3, etc. Não hesite em alterar estas convenções de nomenclatura à sua escolha.
Consola Web	Faça duplo clique na coluna e assinale a caixa para atribuir a interface como endereço de gestão da Consola Web da Interface Gráfica de Utilizador. Tenha muito cuidado ao alterar a interface em que a Consola Web irá escutar. Será necessário ter o roteamento correto configurado ou estar na mesma sub-rede que a nova interface para acessar o Console da Web após a alteração. A única maneira de alterar isso de volta é acessar a linha de comando e emitir o comando set greenside. Isso excluirá todas as interfaces, exceto a eth0.

Interfaces

A secção Interfaces do painel Rede permite a configuração de determinados elementos relativos à interface de rede. Também é possível remover uma interface de rede da listagem, clicando no botão Remover. Quando utiliza uma aplicação virtual, as interfaces que vê aqui são limitadas pela estrutura de virtualização subjacente.



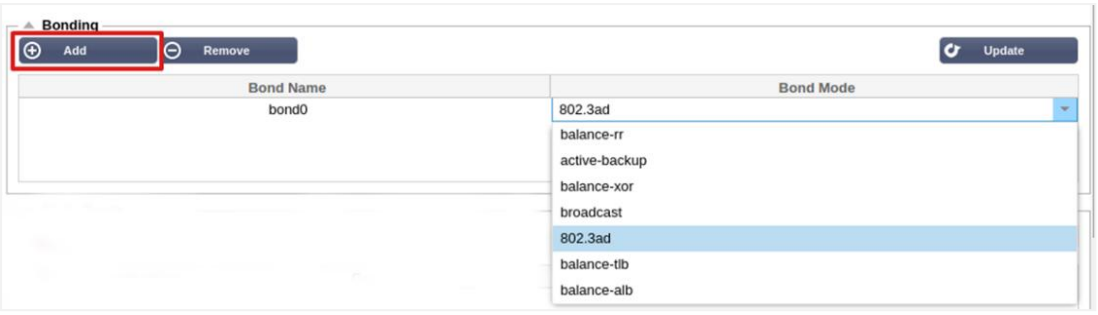
Coluna	Descrição
Tipo de ETH	Este valor indica a referência interna do SO à interface de rede. Este campo não pode ser personalizado. Os valores começam com ETH0 e continuam em sequência, dependendo do número de interfaces de rede.
Estado	Esta indicação gráfica mostra o estado atual da interface de rede. Um estado verde indica que a interface está ligada e ativa. Os outros indicadores de estado são apresentados abaixo.  **Adaptador UP**  Adaptador para baixo  Adaptador desligado  Adaptador em falta
Velocidade	Por predefinição, este valor está definido para negociar automaticamente a velocidade. Mas pode alterar a velocidade de rede da interface para qualquer valor disponível no menu pendente (10/100/1000/AUTO).
Duplex	O valor deste campo é personalizável e pode escolher entre Auto (predefinição), Full-Duplex e Half-Duplex.
Ligação	É possível selecionar um dos tipos de ligação definidos pelo utilizador. Para mais informações, consulte a secção sobre Ligações.

Ligação

Muitos nomes são usados para designar a união de interfaces de rede: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming e outros. A ligação combina ou agrega várias conexões de rede em uma única interface ligada por canal. A ligação permite que duas ou mais interfaces de rede atuem como uma só, aumentem a taxa de transferência e forneçam redundância ou failover.

O kernel do ADC tem um controlador Bonding incorporado para agregar várias interfaces de rede físicas numa única interface lógica (por exemplo, agregar eth0 e eth1 em bond0). Para cada interface bonded, é possível definir o modo e as opções de monitoramento de link. Existem sete opções de modo diferentes, cada uma fornecendo caraterísticas específicas de balanceamento de carga e tolerância a falhas. Elas são mostradas na imagem abaixo.

Nota: A ligação só pode ser configurada para dispositivos ADC baseados em hardware.

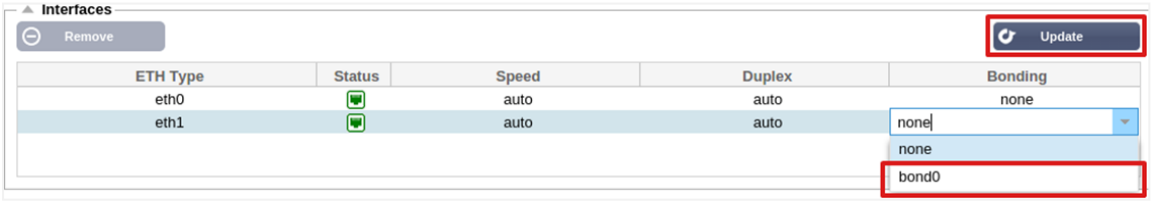


Criar um perfil de ligação

- Clique no botão Adicionar para adicionar uma nova obrigação
- Fornecer um nome para a configuração de ligação
- Escolha o modo de ligação que pretende utilizar

Em seguida, na secção Interfaces, selecione o modo de ligação que pretende utilizar no campo pendente Ligação para a interface de rede.

No exemplo abaixo, eth0, eth1 e eth2 agora fazem parte de bond0. Enquanto a Eth0 permanece sozinha como a interface de gerenciamento.

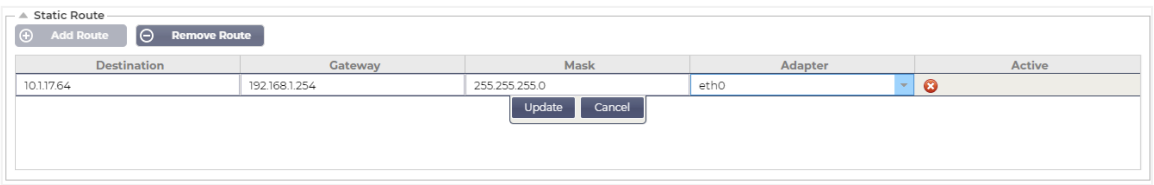


Modos de ligação

Modo de ligação	Descrição
equilíbrio-rr:	Os pacotes são transmitidos/recebidos sequencialmente através de cada interface, um a um.
cópia de segurança ativa:	Neste modo, uma interface estará ativa e a segunda interface estará em standby. Esta interface secundária só fica ativa se a ligação ativa na primeira interface falhar.
equilíbrio-xor:	Transmite com base no endereço MAC de origem XOR'd com o endereço MAC de destino. Esta opção seleciona o mesmo slave para cada endereço MAC de destino.
transmissão:	Este modo transmite todos os dados em todas as interfaces slave.
802.3ad:	Cria grupos de agregação que partilham as mesmas definições de velocidade e duplex e utiliza todos os escravos no agregador ativo, seguindo a especificação 802.3ad.
equilíbrio-tlb:	O modo de ligação de balanceamento de carga de transmissão adaptável: Fornece ligação de canal que não requer nenhum suporte especial de switch. O tráfego de saída é distribuído de acordo com a carga atual (calculada em relação à velocidade) em cada slave. O escravo atual recebe o tráfego de entrada. Se o slave recetor falhar, outro slave assume o endereço MAC do slave recetor que falhou.
equilíbrio-alb:	O modo de ligação de balanceamento de carga adaptativo: também inclui balance-tlb mais balanceamento de carga de receção (rlb) para tráfego IPV4 e não requer nenhum suporte especial do comutador. O balanceamento de carga de receção é obtido por negociação ARP. O controlador de ligação intercepta as respostas ARP enviadas pelo sistema local no seu caminho de saída e substitui o endereço de hardware de origem pelo endereço de hardware único de um dos escravos na ligação, de modo a que diferentes pares utilizem diferentes endereços de hardware para o servidor.

Rota estática

Haverá alturas em que será necessário criar rotas estáticas para sub-redes específicas dentro da sua rede. O ADC oferece-lhe a possibilidade de o fazer utilizando o módulo Static Routes (Rotas estáticas).



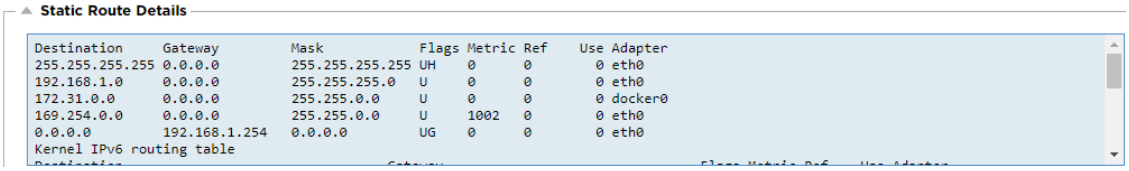
Adicionar uma rota estática

- Clique no botão Adicionar rota
- Preencher o campo utilizando os dados do quadro abaixo como orientação.
- Clique no botão Atualizar quando terminar.

Campo	Descrição
Destino	Introduza o endereço da rede de destino em notação decimal pontilhada. Exemplo 123.123.123.5
Porta de entrada	Introduza o endereço IPv4 do gateway em notação decimal com pontos. Exemplo 10.4.8.1
Máscara	Introduza a máscara de sub-rede de destino em notação decimal com pontos. Exemplo 255.255.255.0
Adaptador	Introduza o adaptador através do qual se pode aceder ao gateway. Exemplo: eth1.
Ativo	Uma caixa de verificação verde indica que a porta de ligação pode ser acedida. Uma cruz vermelha indica que a gateway não pode ser acedida nessa interface. Certifique-se de que configurou uma interface e um endereço IP na mesma rede que a gateway

Detalhes da rota estática

Esta secção fornece informações sobre todas as rotas configuradas no ADC.



Definições de rede avançadas

O que é Nagle?

O algoritmo de Nagle, também conhecido como algoritmo TCP No Delay, é uma técnica utilizada na comunicação em rede para reduzir o número de pacotes retransmitidos devido a dados fora de ordem. Funciona atrasando o envio de pequenos pacotes se não tiver sido recebida qualquer confirmação de receção de pacotes anteriores. Isto ajuda a garantir que os dados chegam na ordem correta e reduz a carga na rede.

Ver **ARTIGO DA WIKIPÉDIA SOBRE NAGLE**

Servidor Nagle

Assinale esta caixa para ativar a definição Nagle do servidor. O Nagle do servidor é um meio de melhorar a eficiência das redes TCP/IP, reduzindo o número de pacotes que precisam de ser enviados através da rede. Esta definição é aplicada ao lado do servidor da transação. É necessário ter cuidado com as definições do servidor, uma vez que o Nagle e o ACK atrasado podem afetar gravemente o desempenho.

Cliente Nagle

Assinale a caixa para ativar a definição Nagle do Cliente. Como acima, mas aplicada ao lado do Cliente da transação.

SNAT

SNAT significa Source Network Address Translation (tradução de endereço de rede de origem), e diferentes fornecedores têm pequenas variações na implementação do SNAT. Uma explicação simples do SNAT do EdgeADC seria a seguinte.

Em circunstâncias normais, os pedidos de entrada seriam direcionados para o VIP que veria o IP de origem do pedido. Assim, por exemplo, se um ponto de extremidade do navegador tivesse um endereço IP de 81.71.61.51, este seria visível para o VIP.

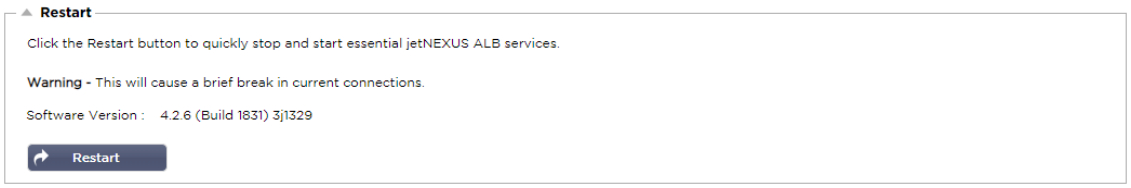
Quando o SNAT estiver em vigor, o IP de origem original da solicitação será ocultado do VIP e, em vez disso, ele verá o endereço IP fornecido na regra SNAT. Assim, o SNAT pode ser usado nos modos de balanceamento de carga da Camada 4 e da Camada 7.

Campo	Descrição
Fonte IP	O endereço IP de origem é opcional e pode ser um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser uma máscara de rede ou um número simples, especificando o número de 1's no lado esquerdo da máscara de rede. Assim, uma máscara de /24 é equivalente a 255.255.255.0.
IP de destino	O endereço IP de destino é opcional e pode ser um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser uma máscara de rede ou um número simples, especificando o número de 1's no lado esquerdo da máscara de rede. Assim, uma máscara de /24 é equivalente a 255.255.255.0.
Porto de origem	A porta de origem é opcional, pode ser um único número, caso em que especifica apenas essa porta, ou pode incluir dois pontos, o que especifica um intervalo de portas. Exemplos: 80 ou 5900:5905.
Porto de destino	A porta de destino é opcional, pode ser um único número, caso em que especifica apenas essa porta, ou pode incluir dois pontos, o que especifica um intervalo de portas. Exemplos: 80 ou 5900:5905.
Protocolo	Pode escolher se pretende utilizar o SNAT num único protocolo ou em todos os protocolos. Sugerimos que seja específico para ser mais preciso.
SNAT para IP	SNAT para IP é um endereço IP obrigatório ou um intervalo de endereços IP. Exemplos: 10.0.0.1 ou 10.0.0.1-10.0.0.3.
SNAT para o porto	O SNAT to Port é opcional, pode ser um único número, caso em que especifica apenas essa porta, ou pode incluir um traço, que especifica um intervalo de portas. Exemplos: 80 ou 5900-5905.
Notas	Utilize esta opção para colocar um nome amigável para se lembrar da razão da existência das regras. Isso também é útil para depuração no Syslog.

Potência

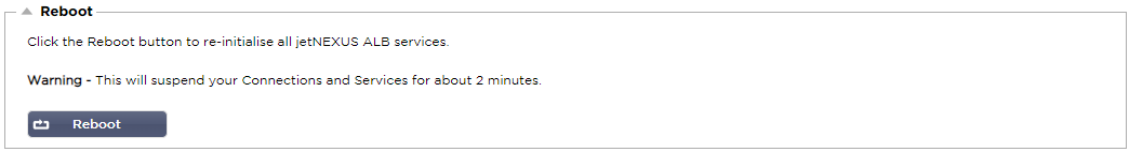
Esta funcionalidade do sistema ADC permite-lhe também realizar várias tarefas relacionadas com a energia no seu ADC.

Reiniciar



Esta definição inicia um reinício global de todos os Serviços e, consequentemente, interrompe todas as ligações atualmente activas. Todos os serviços serão retomados automaticamente após um curto período de tempo, mas o tempo dependerá do número de serviços configurados. Será apresentada uma janela pop-up a pedir confirmação para a ação de reinício.

Reiniciar



Clicar no botão Reboot (Reiniciar) fará com que o ADC entre em ciclo de energia e volte automaticamente ao estado ativo. Será apresentada uma janela pop-up a solicitar a confirmação da ação de reinicialização.

Desligar

Ao clicar no botão Desligar, o ADC será desligado. Se se tratar de um dispositivo de hardware, será necessário ter acesso físico ao dispositivo para o voltar a ligar. Será apresentada uma janela pop-up a solicitar a confirmação da ação de encerramento.

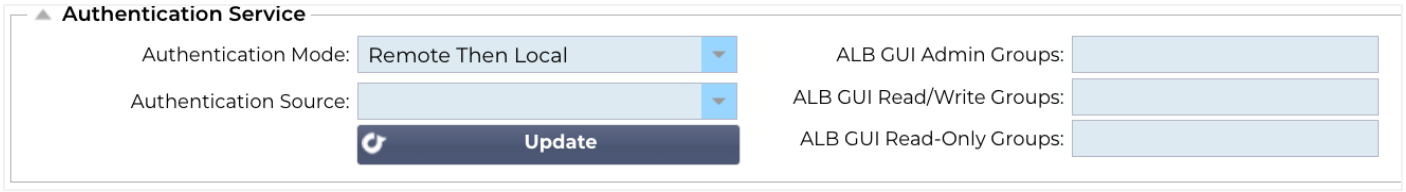
Segurança

Esta secção permite-lhe alterar a palavra-passe da consola Web e ativar ou desativar o acesso Secure Shell. Também permite a ativação da capacidade da API REST.

SSH

Opção	Descrição
Ligação remota Secure Shell	Assinale a caixa se pretender aceder ao ADC através de SSH. O "Putty" é uma excelente aplicação para o fazer.

Serviço de autenticação



Na maioria das organizações, será necessário que o acesso à interface de gestão do ADC seja feito através dos serviços de autenticação da própria empresa.

Para esses cenários, fornecemos a funcionalidade Authentication Service aqui descrita. Esta funcionalidade funciona com serviços de diretório locais, bem como com serviços externos, como o SAML.

Opção	Descrição
Modo de autenticação	Local Only (Apenas local): Este é o modo predefinido e utiliza a base de dados local dentro do ADC, por exemplo, para o utilizador admin. Remoto e depois Local: O ADC tentará validar o utilizador em relação ao servidor de autenticação remoto especificado no campo Fonte de autenticação. Se não for bem sucedido, utilizará a base de dados local como fonte de validação.
Fonte de autenticação	Este menu pendente permite-lhe selecionar um dos servidores de autenticação que definiu em Biblioteca > Autenticação.
Grupos de administradores da GUI do ALB	Especificar os grupos de administradores permitidos.
Grupos de leitura/escrita do GUI ALB	Especificar os grupos de leitura/escrita permitidos
Grupos só de leitura do GUI do ALB	Especifique os grupos só de leitura permitidos.

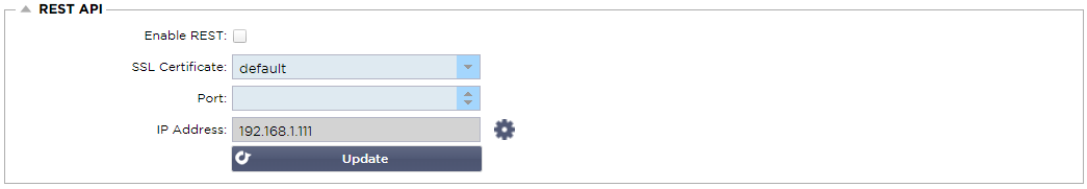
Consola Web

Certificado SSL Escolha um certificado na lista suspensa. O certificado escolhido será utilizado para proteger a sua ligação à interface de utilizador Web do ADC. É possível criar um certificado auto-assinado dentro do ADC ou importar um da secção **CERTIFICADOS SSL**.

Opção	**Descrição**
Porto seguro	A porta predefinida para a consola Web é TCP 443. Se pretender utilizar uma porta diferente por motivos de segurança, pode alterá-la aqui.

API REST

A API REST, também conhecida como RESTful API, é uma interface de programação de aplicações que está em conformidade com o estilo arquitetónico REST e permite a configuração do ADC ou a extração de dados do ADC. O termo REST significa transferência de estado representacional e foi criado pelo cientista informático Roy Fielding.



Opção	**Descrição**
Ativar REST	Assinale esta caixa para ativar o acesso utilizando a API REST. Note que também terá de configurar o adaptador no qual o REST está ativado. Consulte a nota sobre a ligação Cog abaixo.
Certificado SSL	Escolha um certificado para o serviço REST. O menu suspenso mostrará todos os certificados instalados no ADC.
Porto	Defina a porta para o serviço REST. É uma boa ideia utilizar uma porta diferente de 443.
Endereço IP	Isso exibirá o endereço IP ao qual o serviço REST está vinculado. Pode clicar na ligação Cog para aceder à página Rede e alterar o adaptador em que o serviço REST está ativado.
Ligação Cog	Se clicar nesta ligação, será encaminhado para a página Rede, onde pode configurar um adaptador para o REST.

Documentação para a API REST

A documentação sobre como usar a API REST está disponível: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Nota: Se obtiver erros na página Swagger, isso deve-se a um problema de suporte das cadeias de consulta
Percorra os erros até à API REST do jetNEXUS

Exemplos

GUID utilizando CURL:

- Comando

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

- devolverá

```
{"Loginstatus": "OK", "Username":"<nome de utilizador restante>", "GUID":"<guid>"}
```

- Validade
    - O GUID é válido durante 24 horas

Detalhes da licença

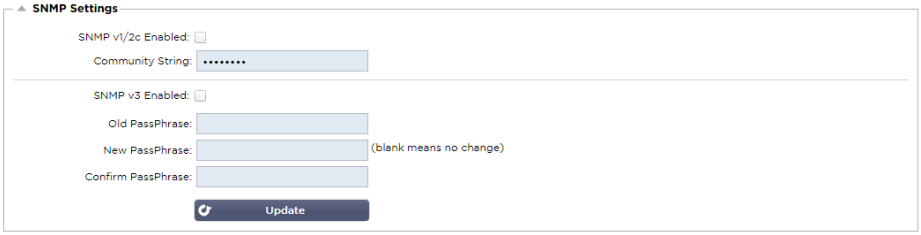
- Comando

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

SNMP

A secção SNMP permite a configuração da MIB SNMP que reside no ADC. O MIB pode então ser consultado por software de terceiros capaz de comunicar com dispositivos equipados com SNMP.

Definições SNMP



Opção	Descrição
SNMP v1 / V2C	Assinale a caixa de verificação para ativar a MIB V1/V2C. O SNMP v1 está em conformidade com o RFC-1157. SNMP V2c está em conformidade com o RFC-1901-1908
SNMP v3	Assinale a caixa de verificação para ativar a MIB V3. RFC-3411-3418. O nome de utilizador para a v3 é admin. Exemplo:- snmpwalk -v3 -u admin -A jetnexus -l authNoPriv 192.168.1.11 1.3.6.1.4.1.38370
Cadeia comunitária	Esta é a cadeia de caracteres só de leitura definida no agente e utilizada pelo gestor para obter as informações SNMP. A cadeia de comunidade predefinida é jetnexus
Frase de passagem	Esta é a palavra-passe necessária quando o SNMP v3 está ativado e deve ter pelo menos 8 caracteres ou mais e conter apenas letras Aa-Zz e números 0-9. A frase-passe predefinida é **jetnexus**

MIB SNMP

As informações visualizáveis através do SNMP são definidas pela Base de Informações de Gestão (MIB). As MIB descrevem a estrutura dos dados de gestão e utilizam identificadores de objectos hierárquicos (OID). Cada OID pode ser lido através de uma aplicação de gestão SNMP.

Descarregar MIB

O MIB pode ser descarregado aqui:

OID DO ADC

OID DA RAIZ

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

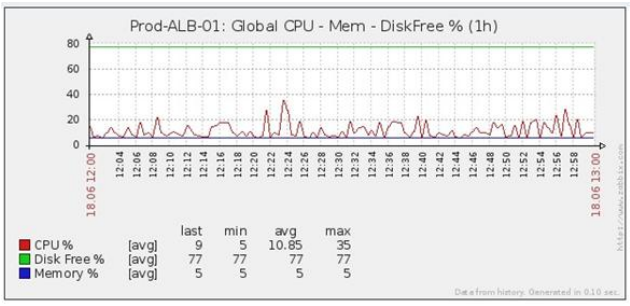
Os nossos OIDs

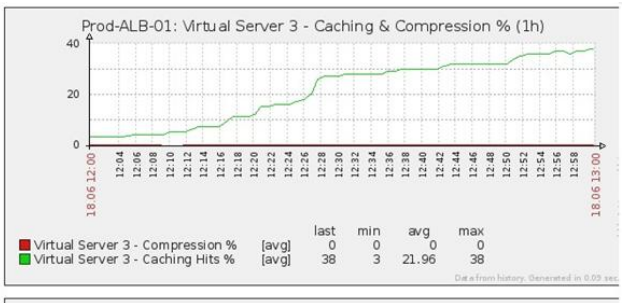
```
.38370 jetnexusMIB
    .1 jetnexusData   (1.3.6.1.4.1.38370.1)
        .1 jetnexusGlobal (1.3.6.1.4.1.38370.1.1)
        .2 jetnexusVirtualServices   (1.3.6.1.4.1.38370.1.2)
        .3 jetnexusServers   (1.3.6.1.4.1.38370.1.3)
            .1 jetnexusGlobal   (1.3.6.1.4.1.38370.1.1)
             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

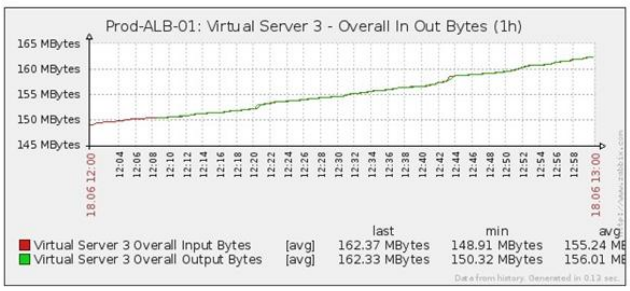
```
            .6 jetnexusTotalClientConnections  (1.3.6.1.4.1.38370.1.1.6.0)
            .7 jetnexusCpuPercent  (1.3.6.1.4.1.38370.1.1.7.0)
            .8 jetnexusDiskFreePercent  (1.3.6.1.4.1.38370.1.1.8.0)
            .9 jetnexusMemoryPercent  (1.3.6.1.4.1.38370.1.1.9.0)
            .10 jetnexusCurrentConnections  (1.3.6.1.4.1.38370.1.1.10.0)

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

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

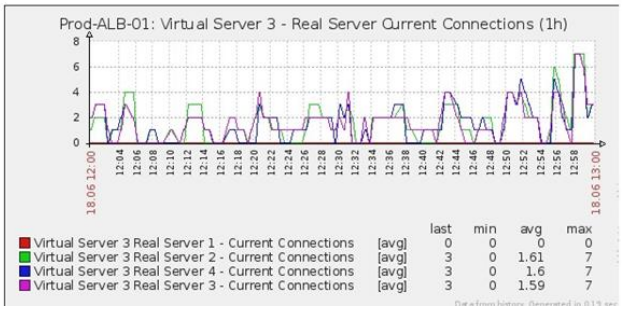
Gráficos históricos

A melhor utilização para a MIB SNMP personalizada do ADC é a capacidade de descarregar o gráfico histórico para uma consola de gestão à sua escolha. Abaixo estão alguns exemplos do Zabbix que sondam um ADC para vários valores OID listados acima.









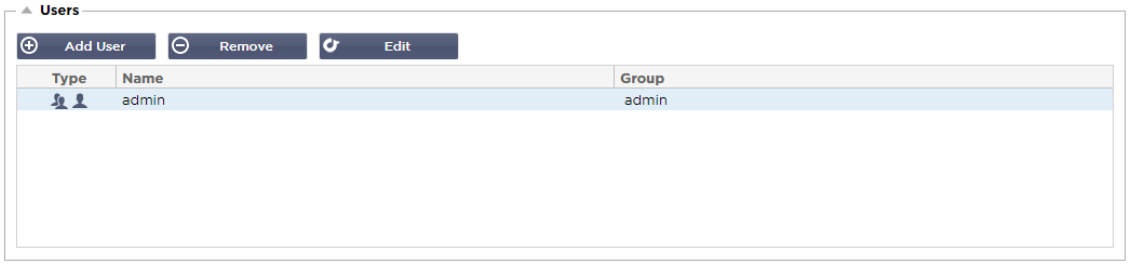
Utilizadores e registos de auditoria

O ADC permite ter um conjunto interno de utilizadores para configurar e definir o que o ADC faz. Os utilizadores definidos no ADC podem efetuar uma série de operações em função da função que lhes é atribuída.

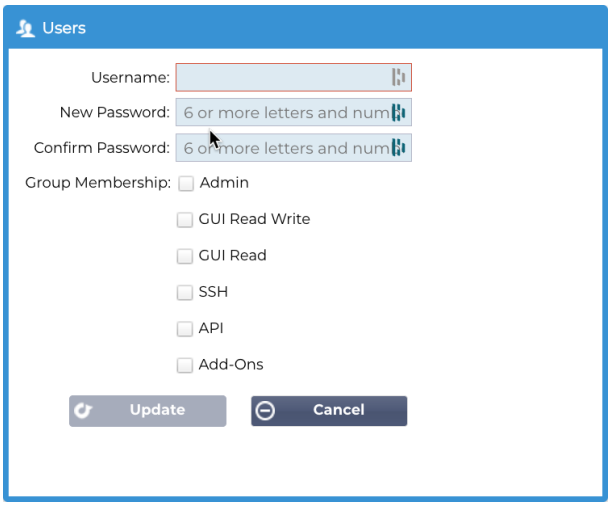
Existe um utilizador predefinido chamado **admin** que é utilizado quando se configura o ADC pela primeira vez. A palavra-passe predefinida para admin é **jetnexus**.

Utilizadores

A secção Utilizadores permite-lhe criar, editar e eliminar utilizadores da ADC.



Adicionar utilizador



Clique no botão Adicionar utilizador mostrado na imagem acima para abrir a caixa de diálogo Adicionar utilizador.

Parâmetro	Descrição/Utilização
Nome de utilizador	Introduza um nome de utilizador à sua escolha. O nome de utilizador deve cumprir o seguinte: • Número mínimo de caracteres 1 • Número máximo de caracteres 32 • As letras podem ser maiúsculas e minúsculas. • Podem ser utilizados números. • Os símbolos não são permitidos
Palavra-passe	Introduza uma palavra-passe **forte** que esteja em conformidade com os requisitos abaixo indicados. • Número mínimo de caracteres 6 • Número máximo de caracteres 32 • Deve utilizar, pelo menos, uma combinação de letras e números. • As letras podem ser maiúsculas ou minúsculas. • Os símbolos são permitidos, exceto os do exemplo seguinte **£**, **%**, &, **<** , **>**
Confirmar a palavra-passe	Confirmar novamente a palavra-passe para garantir que está correta
Membros do grupo	Assinale o grupo a que pretende que o utilizador pertença. • Administrador - Este grupo pode fazer tudo. • GUI Read Write (Leitura e escrita da GUI) - Os utilizadores deste grupo podem aceder à GUI e efetuar alterações através da mesma. • GUI Read (Leitura da GUI) - Os utilizadores deste grupo podem aceder à GUI apenas para visualizar informações. Não podem ser efectuadas alterações. • SSH - Os utilizadores deste grupo podem aceder ao ADC através do Secure Shell. Esta opção dá acesso à linha de comandos, que tem um conjunto mínimo de comandos disponíveis. • API - Os utilizadores deste grupo terão acesso à interface programável SOAP e REST. A REST estará disponível a partir da versão de software 4.2.1 • Add-Ons - É concedida permissão para aceder às configurações de Add-On.

Tipo de utilizador

	Utilizador local O ADC na função Autónomo ou Manual H/A criará apenas Utilizadores locais. Por defeito, um utilizador local chamado "admin" é membro do grupo admin. Para efeitos de compatibilidade com versões anteriores, este utilizador nunca pode ser eliminado. Pode alterar a palavra-passe deste utilizador ou eliminá-la, mas não pode eliminar o último administrador local.
	Utilizador do cluster A função ADC em Cluster apenas criará utilizadores de cluster. Os usuários do cluster são sincronizados em todos os ADCs do cluster Qualquer alteração a um utilizador do cluster será alterada em todos os membros do cluster. Se tiver sessão iniciada como utilizador de um cluster, não poderá mudar de função de Cluster para Manual ou Autónomo
	Cluster e utilizador local Todos os utilizadores criados na função Autónoma ou Manual serão copiados para o Cluster. Se o ADC sair posteriormente do Cluster, apenas os Utilizadores Locais permanecerão. A última palavra-passe configurada para o utilizador será válida.

Remover um utilizador

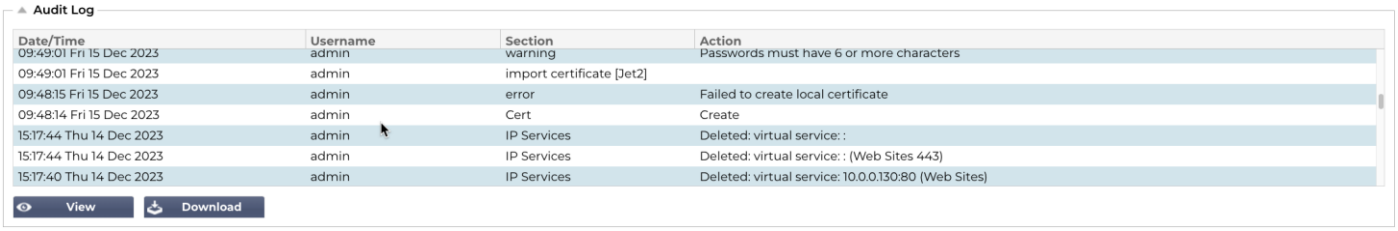
- Destacar um utilizador existente.
- Clique em Remover.
- Não é possível eliminar o utilizador que tem sessão iniciada.
- Não será possível remover o último utilizador local do grupo de administradores.
- Não será possível remover o último utilizador de cluster restante no grupo de administradores.
- Não será possível eliminar o utilizador administrador por motivos de compatibilidade com versões anteriores.
- Se remover o ADC do cluster, todos os utilizadores, exceto os utilizadores locais, serão eliminados.

Editar um utilizador

- Destacar um utilizador existente.
- Clique em Editar
- Pode alterar a pertença do utilizador ao grupo assinalando as caixas adequadas e actualizando.
- Também pode alterar a palavra-passe de um utilizador, desde que tenha direitos de administrador.

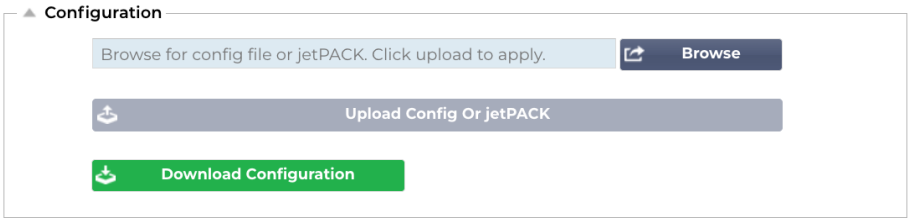
Registo de auditoria

O ADC regista as alterações feitas à configuração do ADC por utilizadores individuais. O registo de auditoria apresenta as últimas 50 acções realizadas por todos os utilizadores. Também pode ver TODAS as entradas na secção **REGISTOS**. Por exemplo:



Avançado

Configuração



É sempre uma boa prática descarregar e guardar a configuração do ADC quando este estiver totalmente configurado e a funcionar conforme necessário. Pode utilizar o módulo de Configuração para descarregar e carregar uma configuração.

Os Jetpacks são ficheiros de configuração para aplicações standard e são fornecidos pela Edgenexus para simplificar o seu trabalho. Também estes podem ser carregados no ADC através do módulo de configuração.

Um ficheiro de configuração é essencialmente um ficheiro de texto e, como tal, pode ser editado pelo utilizador utilizando um editor de texto como o Notepad++, Nano ou VI. Depois de editado conforme necessário, o ficheiro de configuração pode ser carregado no ADC.

CUIDADO:

A edição do ficheiro de configuração do EdgeADC destina-se apenas a especialistas com formação específica. Se o utilizador decidir editar o ficheiro de configuração por si próprio e surgir um problema técnico, a Assistência Técnica da Edgenexus deixará de poder prestar apoio ao produto.

Descarregar uma configuração

- Para descarregar a configuração atual do ADC, prima o botão Download Configuration (Descarregar configuração).
- Aparecerá uma janela pop-up pedindo para abrir ou salvar o arquivo .conf.
- Guardar numa localização conveniente.
- Pode abrir este ficheiro com qualquer editor de texto, como o Notepad++.

Carregamento de uma configuração

- Pode carregar um ficheiro de configuração guardado, procurando o ficheiro .conf guardado.
- Clique no botão "Upload Config or Jetpack" (Carregar configuração ou Jetpack).
- O ADC carregará e aplicará a configuração e, em seguida, actualizará o browser. Se o navegador não for atualizado automaticamente, clique em atualizar no navegador.
- Após a conclusão, será redireccionado para a página Painel de controlo.

Crítico: É fundamental que não tente copiar a configuração de um ADC para outro sem consultar previamente o Suporte da Edgenexus. Se o fizer, pode tornar o seu ADC irrecuperável.

Carregar um JetPACK

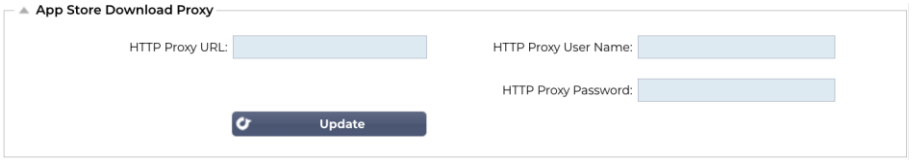
- Um JetPACK é um conjunto de actualizações de configuração para a configuração existente.
- Um JetPACK pode ser tão pequeno como alterar o valor do TCP Timeout até uma configuração completa de uma aplicação específica, como o Microsoft Exchange ou o Microsoft Lync.
    - Pode obter um JetPACK no portal de apoio indicado no final deste guia.
- Procure o ficheiro jetPACK.txt.
- Clique em carregar.
- O browser será atualizado automaticamente após o carregamento.

- Após a conclusão, será redireccionado para a página Painel de controlo.
- A importação pode demorar mais tempo para implantações mais complexas, como o Microsoft Lync, etc.

Definições globais

A secção Definições globais permite-lhe alterar vários elementos, incluindo a biblioteca criptográfica SSL.

Proxy de transferência da App Store



As redes seguras geralmente não permitem o acesso à Internet, a menos que os dados sejam enviados através dos servidores proxy da organização. O EdgeADC é um dispositivo de perímetro e precisa de poder aceder aos servidores Edgenexus para verificar a validade do suporte e também para aceder à App Store para descarregar actualizações e aplicações.

URL de proxy HTTP

Este campo é utilizado para especificar o nome do anfitrião ou o endereço IP do seu servidor proxy.

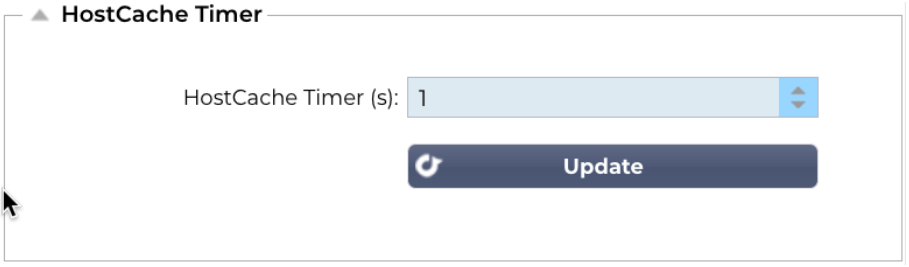
Nome de utilizador do proxy HTTP

Introduza o nome de utilizador especificamente utilizado para autorizar dispositivos e utilizadores que utilizam o servidor proxy.

Palavra-passe do proxy HTTP

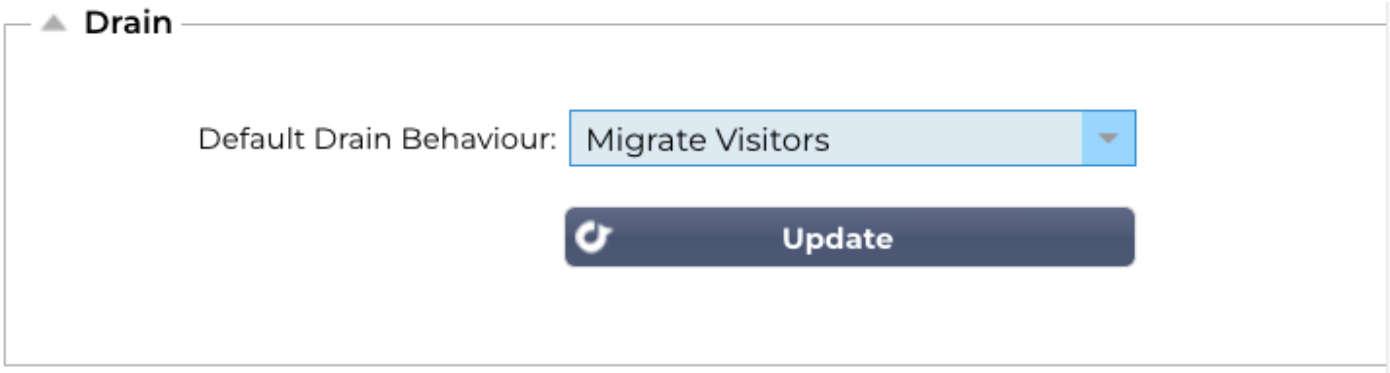
O nome de utilizador especificado em Nome de utilizador do proxy HTTP será um nome seguro. Terá de introduzir a palavra-passe associada neste campo.

Temporizador da cache do anfitrião



O Temporizador da Cache de Anfitrião é uma definição que armazena o Endereço IP de um Servidor Real durante um determinado período quando o nome de domínio foi utilizado em vez de um Endereço IP. A cache é descarregada em caso de falha de um servidor real. Definir este valor como zero impedirá que a cache seja limpa. Não existe um valor máximo para esta definição.

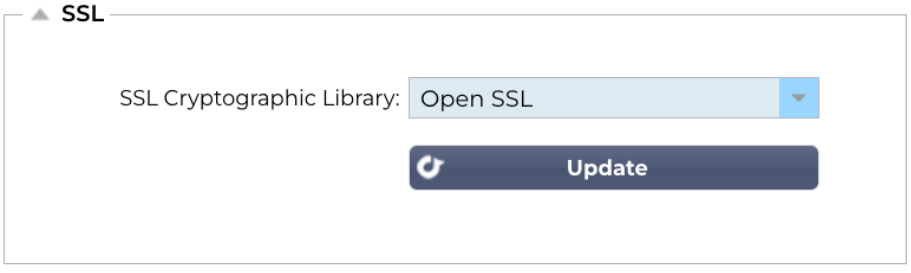
Drenagem



Sempre que um servidor real é colocado em modo de drenagem, é sempre melhor poder controlar o comportamento do tráfego que lhe é enviado. O menu Drain Behaviour (Comportamento de drenagem) permite selecionar o comportamento do tráfego por Serviço Virtual. As opções são:

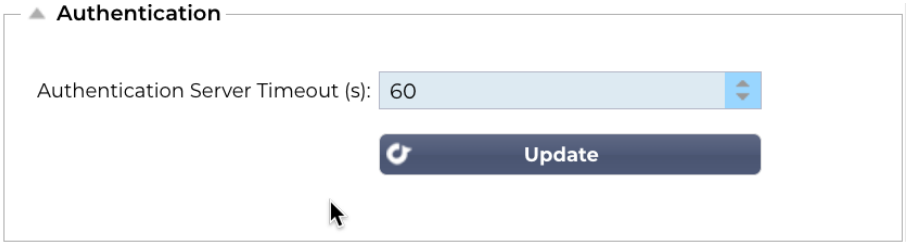
Opção	Descrição
Orientado para a persistência	Esta é a seleção por defeito. Sempre que o utilizador visita a sessão de persistência, esta é alargada. Com uma utilização de 24 horas, é possível que a drenagem nunca aconteça. No entanto, se o número de ligações ao servidor real chegar a 0, a drenagem termina, as sessões de persistência são eliminadas e todos os visitantes são reequilibrados na próxima ligação que efectuarem.
Migrar visitantes	Sessão persistente ignorada na reconexão - (comportamento herdado antes de 2022) As novas ligações TCP (quer façam parte de uma sessão existente ou não) são sempre efectuadas a um servidor real online. Se a sessão de persistência era para um servidor real que estava a esgotar-se, é substituída. O Serviço Virtual ignorará efetivamente a persistência de quaisquer novas ligações e estas serão equilibradas em termos de carga para um novo servidor.
Sessões de reforma	As sessões persistentes não são prolongadas. As ligações de entrada dos utilizadores serão atribuídas ao servidor pretendido, mas a sua sessão de persistência não é prolongada. Assim, após o tempo da sessão de persistência ser excedido, serão tratadas como uma nova ligação e movidas para um servidor diferente.

SSL



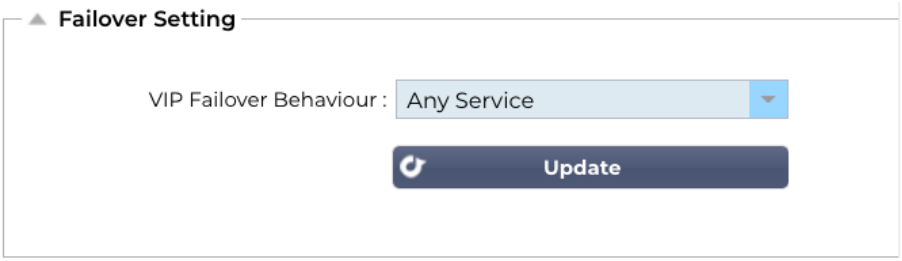
Esta configuração global permite que a biblioteca SSL seja alterada conforme necessário. A biblioteca criptográfica SSL padrão usada pelo ADC é a OpenSSL. Se você quiser usar uma biblioteca criptográfica diferente, isso pode ser alterado aqui.

Autenticação



Este valor define o valor do tempo limite para a autenticação, após o qual a tentativa de autenticação será considerada falhada.

Definição de ativação pós-falha



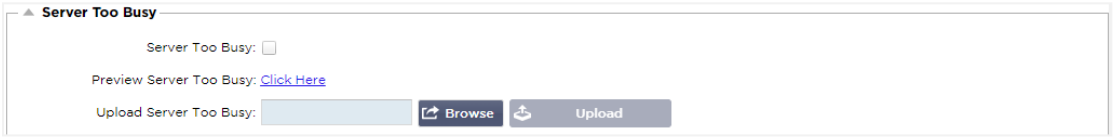
Quando um conjunto de ADCs em cluster é criado, agora há dois métodos para especificar como um Serviço Virtual fará o failover.

Opção	Descrição
Qualquer serviço	Quando esta opção é escolhida, a falha de qualquer Serviço no VIP fará com que todo o VIP com os seus Serviços Virtuais falhe no parceiro de cluster. Por exemplo, pode ter um VIP 10.0.100.101, com Serviços Virtuais, cada um utilizando as portas 443, 8080, 4399,2020, etc. Se algum desses sub-serviços falhar, o VIP inteiro falhará.
Todos os serviços	Quando esta opção é escolhida, se um ou mais sub-serviços falharem, o VIP permanecerá no membro atual do cluster. O VIP só será transferido para o parceiro de cluster se **todos os** serviços falharem. Esta opção é útil quando se pretende desativar um determinado serviço, mas não se pretende que o VIP faça o fail over.

Protocolo

A secção Protocolo é utilizada para definir as várias definições avançadas do protocolo HTTP.

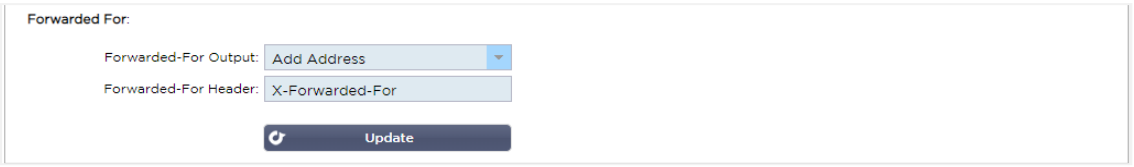
Servidor demasiado ocupado



Suponha que limitou o número máximo de ligações aos seus servidores reais; pode optar por apresentar uma página Web amigável quando este limite for atingido.

- Crie uma página Web simples com a sua mensagem. Pode incluir ligações externas a objectos noutros servidores e sítios Web. Em alternativa, se quiser ter imagens na sua página Web, utilize imagens codificadas em linha com base64.
- Procure o ficheiro HTM(L) da sua página Web recentemente criada.
- Clique em Carregar
- Se desejar pré-visualizar a página, pode fazê-lo através da ligação Clique aqui.

Encaminhado para



O Forwarded For é a norma de facto para identificar o endereço IP de origem de um cliente que se liga a um servidor Web através de equilibradores de carga da camada 7 e servidores proxy.

Saída encaminhada para

Opção	**Descrição**
Desligado	O ADC não altera o cabeçalho Forwarded-For.
Adicionar endereço e porta	Esta opção irá anexar o endereço IP e a porta do dispositivo ou cliente ligado ao ADC ao cabeçalho Forwarded-For.
Adicionar endereço	Esta opção irá anexar o endereço IP do dispositivo ou cliente ligado ao ADC ao cabeçalho Forwarded-For.
Substituir endereço e porta	Esta opção substituirá o valor do cabeçalho Forwarded-For pelo endereço IP e pela porta do dispositivo ou cliente ligado ao ADC.
Substituir o endereço	Esta opção substituirá o valor do cabeçalho Forwarded-For pelo endereço IP do dispositivo ou cliente ligado ao ADC.

Cabeçalho "Forwarded-For

Este campo permite-lhe especificar o nome dado ao cabeçalho Forwarded-For. Normalmente, este é "X-Forwarded-For", mas pode ser alterado para alguns ambientes.

Registo avançado para o IIS - Registo personalizado

Pode obter as informações X-Forwarded-For instalando a aplicação IIS Advanced logging 64-bit. Uma vez descarregada, crie um campo de registo personalizado chamado X-Forwarded-For com as definições abaixo.

Selecione Predefinição na lista Tipo de origem na lista Categoria, selecione Cabeçalho do pedido na caixa Nome da origem e escreva X-Forwarded-For.

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

Alterações no Apache HTTPd.conf

É necessário efetuar várias alterações ao formato predefinido para registar o endereço IP do cliente X-Forwarded-For ou o endereço IP real do cliente se o cabeçalho X-Forwarded-For não existir.

Essas alterações são apresentadas abaixo:

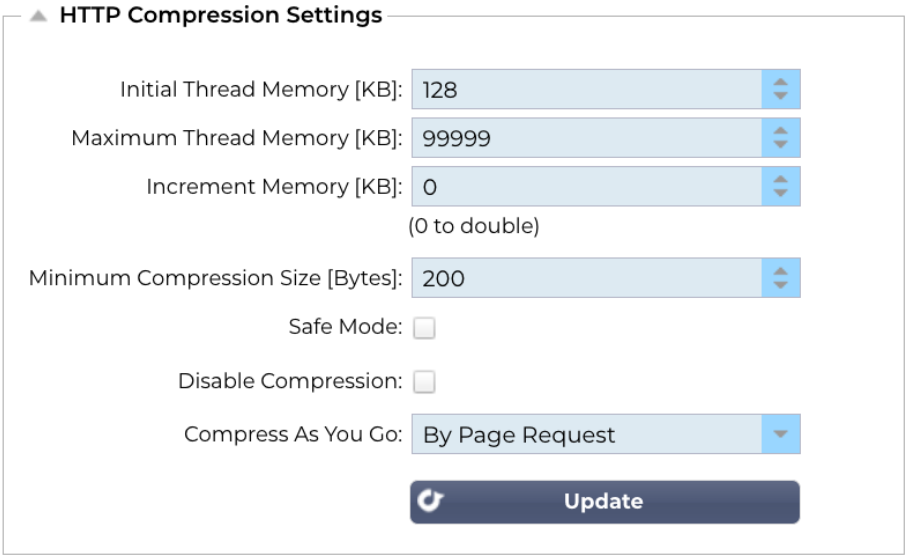
Tipo	Valor
LogFormat:	"%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combinado
LogFormat:	"%{X-Forwarded-For}i %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" proxy SetEnvIf X- Forwarded-For "^.*\..*\..*\..*\..*" encaminhado
CustomLog:	"logs/access_log" combined env=!forwarded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

Este formato tira partido do suporte integrado do Apache para registo condicional baseado em variáveis ambientais.

- A linha 1 é a cadeia de caracteres formatada do registo combinado padrão a partir da predefinição.
- A linha 2 substitui o campo %h (anfitrião remoto) pelo(s) valor(es) retirado(s) do cabeçalho X-Forwarded-For e define o nome deste padrão de ficheiro de registo como "proxy".
- A linha 3 é uma definição para a variável de ambiente "forwarded" que contém uma expressão regular solta que corresponde a um endereço IP, o que está bem neste caso, uma vez que nos interessa mais se existe um endereço IP no cabeçalho X-Forwarded-For.
- Além disso, a linha 3 poderia ser lida como: "Se existir um valor X-Forwarded-For, utilize-o."
- As linhas 4 e 5 dizem ao Apache qual o padrão de registo a utilizar. Se existir um valor X-Forwarded-For, use o padrão "proxy", caso contrário use o padrão "combined" para o pedido. Para facilitar a leitura, as linhas 4 e 5 não tiram partido da funcionalidade de registo rotate logs (piped) do Apache, mas assumimos que quase toda a gente a utiliza.

Estas alterações resultarão no registo de um endereço IP para cada pedido.

Definições de compressão HTTP



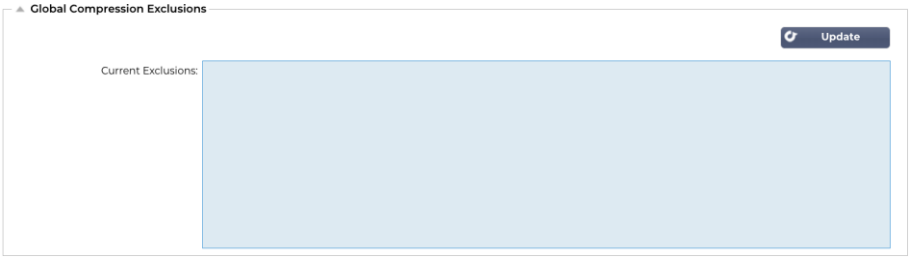
A compressão é uma funcionalidade de aceleração e é activada para cada serviço na página Serviços IP.

AVISO - Tenha muito cuidado ao ajustar estas definições, uma vez que definições inadequadas podem afetar negativamente o desempenho do ADC

Opção	**Descrição**
Memória inicial da thread [KB]	Este valor é a quantidade de memória que cada pedido recebido pelo ADC pode alocar inicialmente. Para um desempenho mais eficiente, este valor deve ser definido para um valor ligeiramente superior ao maior ficheiro HTML não comprimido que os servidores Web possam enviar.
Memória máxima da thread [KB]	Este valor é a quantidade máxima de memória que o ADC atribuirá num pedido. Para obter o máximo desempenho, o ADC armazena e comprime normalmente todos os conteúdos na memória. Se for processado um ficheiro de conteúdo excecionalmente grande que exceda esta quantidade, o ADC gravará no disco e comprimirá os dados aí.
Memória de incremento [KB]	Este valor define a quantidade de memória adicionada à Atribuição inicial de memória da thread quando é necessário mais. A configuração padrão é zero. Isso significa que o ADC dobrará a alocação quando os dados excederem a alocação atual (por exemplo, 128Kb, depois 256Kb, depois 512Kb, etc) até o limite definido pelo Uso máximo de memória por thread. Isto é eficiente quando a maioria das páginas tem um tamanho consistente, mas existem ocasionalmente ficheiros maiores. (por exemplo, a maioria das páginas tem 128Kb ou menos, mas as respostas ocasionais têm 1Mb de tamanho). No cenário em que há arquivos grandes de tamanho variável, é mais eficiente definir um incremento linear de um tamanho significativo (por exemplo, as respostas têm de 2Mb a 10Mb de tamanho, uma configuração inicial de 1Mb com incrementos de 1Mb seria mais eficiente).
Tamanho mínimo de compressão [Bytes]	Este valor é o tamanho, em bytes, abaixo do qual o ADC não tentará comprimir. Isto é útil porque tudo o que for inferior a 200 bytes não comprime bem e pode até aumentar de tamanho devido às despesas gerais dos cabeçalhos de compressão.
Modo de segurança	Assinale esta opção para impedir que o ADC aplique compressão a folhas de estilo de JavaScript. A razão para isto é que, embora o ADC saiba quais os navegadores individuais que podem lidar com conteúdo comprimido, alguns outros servidores proxy, apesar de afirmarem ser compatíveis com HTTP/1.1, não conseguem transportar corretamente folhas de estilo e JavaScript comprimidos. Se estiverem a ocorrer problemas com folhas de estilo ou JavaScript através de um servidor proxy, utilize esta opção para desativar a compressão destes tipos. No entanto, isso reduzirá a quantidade total de compactação de conteúdo.

Desativar a compressão	Assinale esta opção para impedir o ADC de comprimir qualquer resposta.
Comprimir à medida que avança	Ligado - Utilizar Comprimir à medida que se avança nesta página. Isto comprime cada bloco de dados recebido do servidor num bloco discreto que é totalmente descomprimível. DESLIGADO - Não usar a Compressão conforme o uso nesta página. Por solicitação de página - Usar a Compressão conforme o uso por solicitação de página.

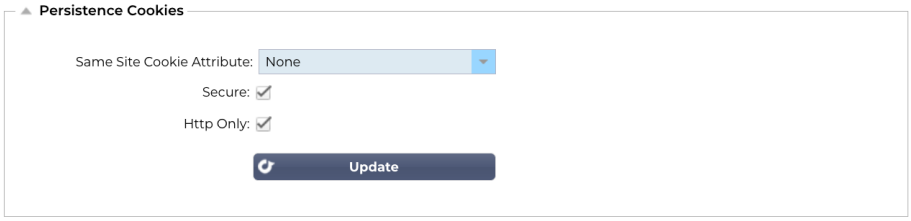
Exclusões de compressão global



As páginas com a extensão adicionada na lista de exclusão não serão comprimidas.

- Introduza o nome do ficheiro individual.
- Clique em atualizar.
- Se pretender adicionar um tipo de ficheiro, basta escrever "*.css" para que todas as folhas de estilo em cascata sejam excluídas.
- Cada ficheiro ou tipo de ficheiro deve ser adicionado a uma nova linha.

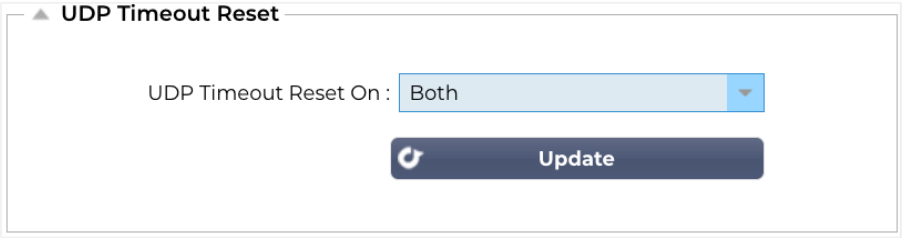
Cookies de persistência



Esta definição permite-lhe especificar a forma como os cookies de persistência são tratados.

Campo	Descrição
Atributo Cooke do mesmo local	**Nenhum**: Todos os cookies são acessíveis a scripts **Laxista**: Impede que os cookies sejam acedidos através dos sítios, mas são armazenados para se tornarem acessíveis e enviados para o sítio proprietário se este for visitado **Estrito**: impede que qualquer cookie de um sítio diferente seja acedido ou armazenado **Desligado**: regressa ao comportamento predefinido do browser
Seguro	Esta caixa de verificação, quando selecionada, aplica a persistência ao tráfego seguro
Apenas HTTP	Quando selecionada, esta opção permite Cookes persistentes apenas no tráfego HTTP

Reposição do tempo limite UDP



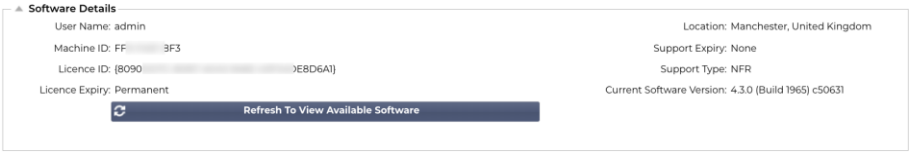
O UDP Timeout Reset é um mecanismo utilizado nas comunicações de rede em que o tempo limite relativo a uma sessão UDP (User Datagram Protocol) é reiniciado. A reposição ajuda a manter a sessão ativa, assegurando um fluxo de dados contínuo e sem interrupções.

Opção	Descrição
Ambos	Repõe o tempo limite do UDP no servidor e no cliente.
Servidor	Repõe o tempo limite do UDP no servidor.
Cliente	Repõe o tempo limite do UDP no cliente.

Software

A secção Software permite-lhe atualizar a configuração e o firmware do seu ADC.

Detalhes da atualização de software



As informações nesta secção serão preenchidas se tiver uma ligação à Internet a funcionar. Se o seu browser não tiver uma ligação à Internet, esta secção ficará em branco. Uma vez ligado, receberá a mensagem de banner abaixo.

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

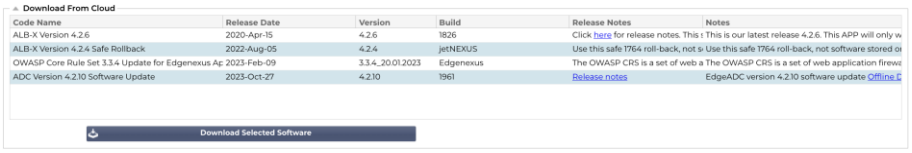
A secção Descarregar da nuvem apresentada abaixo será preenchida com informações que mostram as actualizações disponíveis para si ao abrigo do seu plano de suporte. Deve ter em atenção o tipo de suporte e a data de expiração do suporte.

Nota: Utilizamos a ligação à Internet do seu browser para ver o que está disponível na Edgenexus Cloud. Só será possível descarregar actualizações de software se o ADC tiver uma ligação à Internet.

Para verificar isso:

- Avançado--Solução de problemas--Ping
- Endereço IP - App Store.edgenexus.io
- Clique em Ping
- Se o resultado mostrar "ping: host desconhecido App Store.edgenexus.io".
- O ADC NÃO poderá descarregar nada da nuvem

Descarregar da nuvem



Se o seu browser estiver ligado à Internet, verá detalhes do software disponível na nuvem.

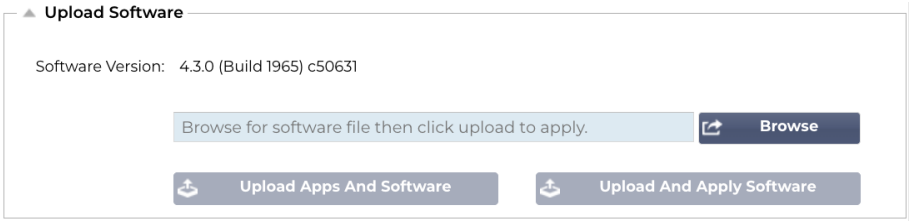
- Selecione a linha em que está interessado e clique no botão "Transferir o software selecionado para o ALB".
- O software selecionado será descarregado para o seu ALB quando clicado, podendo ser aplicado na secção "Aplicar software armazenado no ALB" abaixo.

Nota: Se a ADC não tiver acesso direto à Internet, receberá um erro como o que se segue:

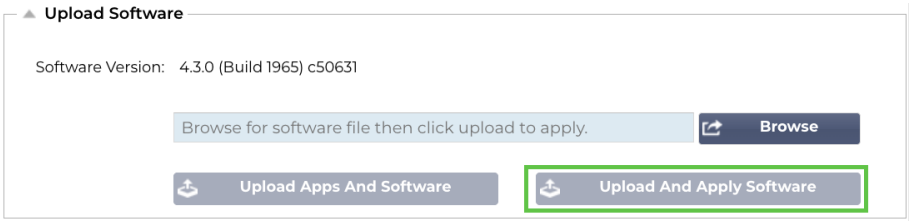
Erro de transferência, o ALB não consegue aceder aos ADC Cloud Services para o ficheiro build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Se a sua rede estiver protegida por um servidor proxy, consulteProxy de transferência da App Store

Carregar software



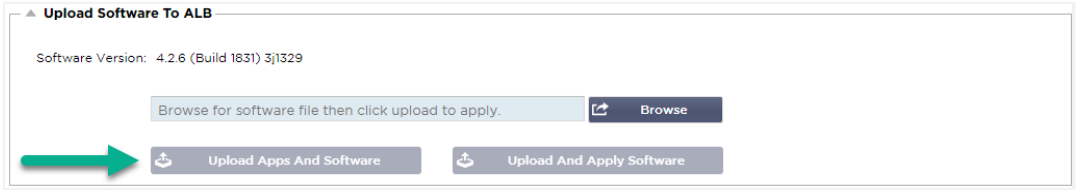
Upload de aplicações



Se tiver um ficheiro de aplicação que termine com <appname> .<apptype>.alb, pode utilizar este método para o carregar.

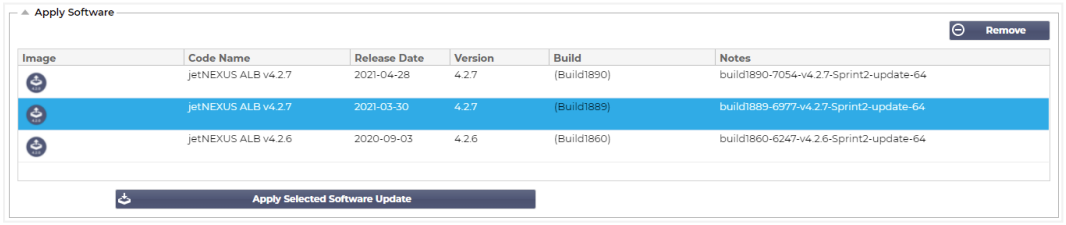
- Existem cinco tipos de aplicações
  - <nome da aplicação>flightpath.alb
  - <nome da aplicação>.monitor.alb
  - <nome da aplicação>.jetpack.alb
  - <nome da aplicação>.addons.alb
  - <nome da aplicação>.featurepack.alb
- Uma vez carregada, cada aplicação será encontrada na secção Biblioteca>Apps.
- Em seguida, é necessário implementar cada aplicação dessa secção individualmente.

Software /Actualizações de firmware



- Se pretender carregar software sem o aplicar, utilize o botão destacado.
- O ficheiro de software é <softwarename>.software.alb.
- Será então apresentado na secção "Software armazenado no ALB", a partir da qual poderá aplicá-lo quando lhe for conveniente.

Aplicar o software armazenado em ADC



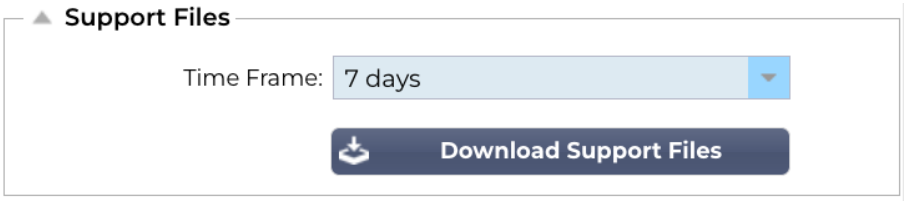
Esta secção mostrará todos os ficheiros de Software armazenados no ALB e disponíveis para implementação. A listagem incluirá assinaturas actualizadas da Firewall de Aplicação Web (WAF).

- Realce a linha de Software que está interessado em utilizar.
- Clique em "Apply Software from Selected" (Aplicar software da seleção)
- Se se tratar de uma atualização de software do ALB, tenha em atenção que esta será carregada e, em seguida, o ALB será reiniciado para ser aplicada.
- Se a atualização que está a aplicar for uma atualização de assinatura OWASP, será aplicada automaticamente sem reiniciar.

Resolução de problemas

Há sempre problemas que requerem a resolução de problemas para se chegar a uma causa e solução de raiz. Esta secção permite-lhe fazer isso.

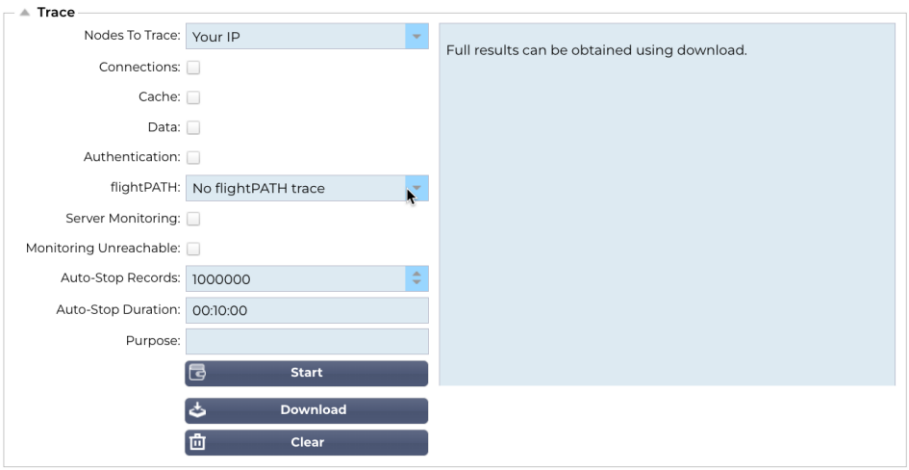
Ficheiros de apoio



Se tiver um problema com o ADC e precisar de abrir um pedido de assistência, o suporte técnico solicitará frequentemente vários ficheiros diferentes da aplicação ADC. Estes ficheiros foram agora agregados num único ficheiro .dat que pode ser descarregado através desta secção.

- Selecione um período de tempo a partir do menu pendente: Tem à sua disposição uma escolha de 3, 7, 14 e Todos os dias.
- Clique em "Transferir ficheiros de suporte"
- Será descarregado um ficheiro com o formato Support-jetNEXUS-yyymmddhh-NAME.dat
- Abrir um pedido de assistência no portal de assistência, cujos pormenores estão disponíveis no final do presente documento.
- Certifique-se de que descreve o problema minuciosamente e anexa o ficheiro .dat ao pedido.

Traço



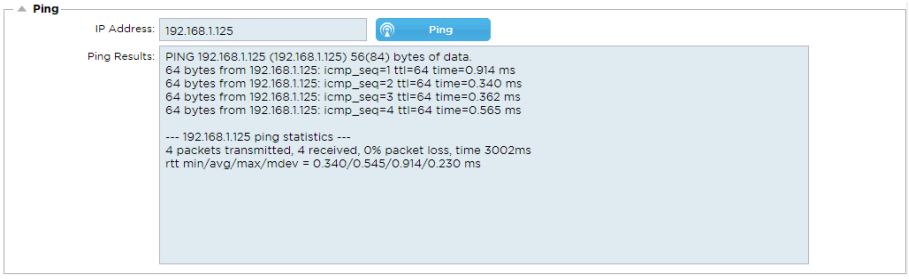
A secção Trace permite-lhe examinar as informações que possibilitam a depuração do problema. As informações fornecidas dependem das opções que escolher nos menus pendentes e nas caixas de seleção.

Opção	**Descrição**
Nós para rastrear	**Your IP (O seu IP**): Esta opção filtrará a saída para utilizar o endereço IP a partir do qual está a aceder à GUI (Nota: não escolha esta opção para Monitorização, uma vez que a Monitorização utilizará o endereço da interface do ADC) **Todos os IP**: Não será aplicado qualquer filtro. É de notar que, numa caixa ocupada, isto afectará negativamente o desempenho.

Ligações	Esta caixa de verificação, quando selecionada, mostra informações sobre as ligações do lado do cliente e do lado do servidor.
Cache	Esta caixa de verificação assinalada mostra informações sobre os objectos colocados em cache.
Dados	Quando esta caixa de verificação estiver selecionada, incluirá os bytes de dados brutos tratados à entrada e à saída pelo ADC.
flightPATH	O menu flightPATH permite-lhe selecionar uma regra flightPATH específica para monitorizar ou todas as regras flightPATH.
Monitorização do servidor	Esta caixa de verificação, quando marcada, mostrará os monitores de estado do servidor activos no ADC e os respectivos resultados.
Monitorização Inacessível	Quando esta opção está selecionada, o seu comportamento é muito semelhante ao da Monitorização do servidor, exceto que apenas mostrará os monitores que falharam, funcionando assim como um filtro apenas para estas mensagens.
Registos de paragem automática	O valor predefinido é de 1.000.000 de registos, após o que a função Trace pára automaticamente. Esta definição é uma precaução de segurança para evitar que o Rastreio seja acidentalmente deixado ligado e afecte o desempenho do ADC.
Duração da paragem automática	O tempo predefinido é de 10 minutos, após os quais a função Trace pára automaticamente. Esta função é uma precaução de segurança para evitar que o rastreio seja acidentalmente deixado ligado e afecte o desempenho do ADC.
Início	Clique nesta opção para iniciar manualmente o recurso Trace.
Parar	Clique para parar manualmente a funcionalidade Traçado antes de o registo automático ou o tempo ser atingido.
Descarregar	Embora possa ver o visualizador em direto no lado direito, a informação pode ser apresentada demasiado rapidamente. Em vez disso, pode descarregar o Trace.log para ver todas as informações recolhidas durante os vários traços desse dia. Esta funcionalidade é uma lista filtrada de informações de rastreio. Se pretender visualizar as informações de rastreio de dias anteriores, pode descarregar o Syslog para esse dia, mas terá de filtrar manualmente.
Limpo	Limpa o registo de rastreio

Ping

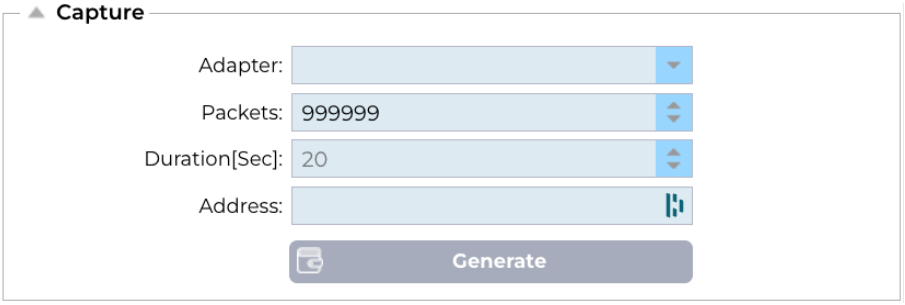
Pode verificar a conetividade de rede com servidores e outros objectos de rede na sua infraestrutura utilizando a ferramenta Ping.



Introduza o endereço IP do anfitrião que pretende testar, por exemplo, o gateway predefinido utilizando a notação decimal com pontos ou um endereço IPv6. Pode ser necessário aguardar alguns segundos para que o resultado seja apresentado depois de premir o botão "Ping".

Se tiver configurado um servidor DNS, pode introduzir o nome de domínio totalmente qualificado. Pode configurar um servidor DNS na secção **Servidor DNS 1 e Servidor DNS 2**. Poderá ter de aguardar alguns segundos para que o resultado seja apresentado depois de premir o botão "Ping".

Captura



Para capturar o tráfego de rede, siga as instruções simples abaixo.

- Preencher as opções do formulário
- Clique em Gerar
- Quando a captura tiver sido executada, o seu browser irá aparecer e perguntar-lhe onde deseja guardar o ficheiro. O ficheiro terá o formato "jetNEXUS.cap.gz"
- Abrir um pedido de assistência no portal de assistência, cujos pormenores estão disponíveis no final do presente documento.
- Certifique-se de que descreve o problema minuciosamente e anexa o ficheiro ao pedido.
- Também pode ver o conteúdo utilizando o Wireshark

Opção	**Descrição**
Adaptador	Escolha o seu adaptador no menu suspenso, normalmente eth0 ou eth1. Também é possível capturar todas as interfaces com "any"
Pacotes	Este valor é o número máximo de pacotes a capturar. Normalmente, 99999
Duração	Escolha o tempo máximo de execução da captura. Um tempo típico é de 15 segundos para sites com muito tráfego. A GUI estará inacessível durante o período de captura
Endereço	Este valor filtrará qualquer endereço IP introduzido na caixa. Deixe este valor em branco para não filtrar.

Para manter o desempenho, limitámos o ficheiro de transferência a 10 MB. Se achar que não é suficiente para captar todos os dados necessários, podemos aumentar este valor.

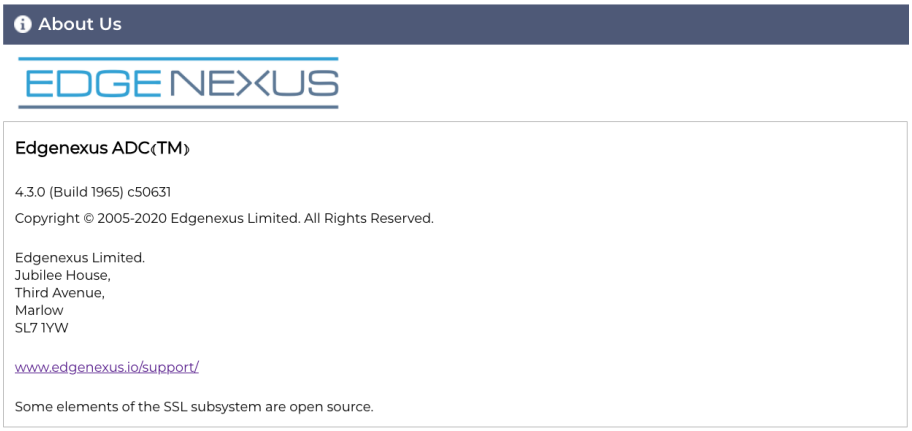
Nota: Isto terá um impacto no desempenho dos sítios em direto. Para aumentar o tamanho da captura disponível, aplique uma definição global jetPACK para aumentar o tamanho da captura.

Ajuda

A secção Ajuda permite aceder às informações sobre o Edgenexus e aceder aos guias do utilizador e a outras informações úteis.

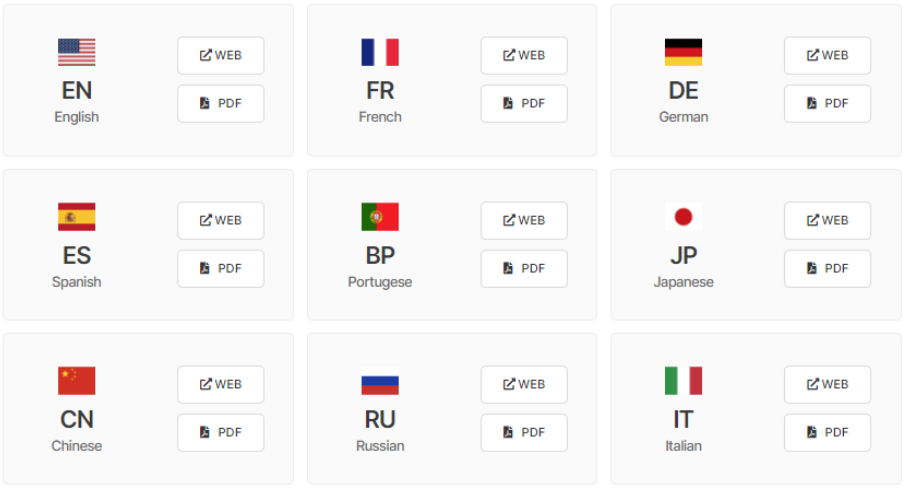
Sobre nós

Ao clicar na opção Sobre nós, são apresentadas informações sobre a Edgenexus e a sua sede social.



Referência

A opção de referência abrirá a página Web que contém os manuais do utilizador e outros documentos úteis. A página Web também pode ser encontrada utilizando https://www.edgenexus.io/documentation.



Se não encontrar o que procura, contacte .support@edgenexus.io

JetPACKs

Edgenexus jetPACK s

Os jetPACKs são um método exclusivo de configurar instantaneamente seu ADC para aplicações específicas. Estes modelos fáceis de utilizar vêm pré-configurados e totalmente ajustados com todas as definições específicas da aplicação de que necessita para usufruir de uma prestação de serviços optimizada do seu ADC. Alguns dos jetPACKs usam o flightPATH para manipular o tráfego, e é necessário ter uma licença do flightPATH para que esse elemento funcione. Para saber se tem uma licença para o flightPATH, consulte a página **LICENÇA**.

Descarregar um jetPACK

- Cada jetPACK abaixo foi criado com um endereço IP virtual único contido no título do jetPACK. Por exemplo, o primeiro jetPACK abaixo tem um endereço IP virtual de 1.1.1.1
- Pode carregar este jetPACK como está e alterar o endereço IP na GUI ou editar o jetPACK com um editor de texto como o Notepad++ e procurar e substituir 1.1.1.1 pelo seu endereço IP virtual.
- Para além disso, cada jetPACK foi criado com 2 Servidores Reais com endereços IP 127.1.1.1 e 127.2.2.2. Mais uma vez pode alterar estes endereços no GUI após o upload ou antes usando o Notepad++.
- Clique numa das ligações jetPACK abaixo e guarde a ligação como um ficheiro jetPACK-VIP-Application.txt na localização escolhida

Microsoft Exchange

Aplicação	Ligação para descarregar	O que é que ele faz?	O que é que está incluído?
Exchange 2010	jetPACK-1.1.1.1-Exchange-2010	Este jetPACK adicionará as configurações básicas para balancear a carga do Microsoft Exchange 2010. Existe uma regra flightPATH incluída para redirecionar o tráfego no serviço HTTP para HTTPS, mas é uma opção. Se não tiver uma licença para o flightPATH, este jetPACK continuará a funcionar.	Definições globais: Tempo limite do serviço 2 horas Monitores: Monitor da camada 7 para a aplicação Web do Outlook e monitor da camada 4 fora da banda para o serviço de acesso do cliente IP do serviço virtual: 1.1.1.1 Portas de serviço virtuais: 80, 443, 135, 59534, 59535 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	O mesmo que acima, mas adicionará um serviço SMTP na porta 25 em conetividade de proxy reverso. O servidor SMTP verá o endereço da interface ALB-X como o IP de origem.	Definições globais: Tempo limite do serviço 2 horas Monitores: Monitor de camada 7 para a aplicação Web do Outlook. Monitor de camada 4 fora da banda para o serviço de acesso do cliente IP do serviço virtual: 1.1.1.1 Portas de serviço virtual: 80, 443, 135, 59534, 59535, 25 (proxy reverso) Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	O mesmo que acima, exceto que este jetPACK irá configurar o serviço SMTP para usar a conetividade Diret Server Return. Este jetPACK é necessário se o	Definições globais: Tempo limite do serviço 2 horas Monitores: Monitor de camada 7 para a aplicação Web do Outlook.

		seu servidor SMTP precisar de ver o endereço IP real do cliente.	Monitor de camada 4 fora da banda para o serviço de acesso do cliente IP do serviço virtual: 1.1.1.1 Portas de serviço virtual: 80, 443, 135, 59534, 59535, 25 (retorno direto do servidor) Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPs
Exchange 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Esta configuração adiciona 1 VIP e dois serviços para tráfego HTTP e HTTPS e requer menos CPU. É possível adicionar vários controlos de saúde ao VIP para verificar se cada um dos serviços individuais está ativo	Definições globais: Monitores: Monitor da camada 7 para OWA, EWS, OA, EAS, ECP, OAB e ADS IP do serviço virtual: 2.2.2.1 Portas de serviço virtual: 80, 443 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Esta configuração usa um endereço IP exclusivo para cada serviço e, portanto, usa mais recursos do que acima. Tem de configurar cada serviço como uma entrada DNS individual Exemplo owa.edgenexus.com, ews.edgenexus.com, etc. Será adicionado um monitor para cada serviço e aplicado ao serviço relevante	Definições globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell IP de serviço virtual: 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 Portas de serviço virtual: 80, 443 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Este jetPACK irá adicionar um endereço IP único e vários serviços virtuais em diferentes portas. flightPATH irá então mudar de contexto baseado no caminho de destino para o Serviço Virtual correto. Este jetPACK requer a maior quantidade de CPU para efetuar a mudança de contexto	Definições globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell IP do serviço virtual: 2.2.2.3 Portas de serviço virtuais: 80, 443, 1, 2, 3, 4, 5, 6, 7 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redireccionamento de HTTP para HTTPS

Microsoft Lync 2010/2013

Proxy inverso	Front-end	Borda interna	Borda Externa
jetPACK-3.3.3.1-Lync-Reverse-Proxy	jetPACK-3.3.3.2-Lync-Front -End	jetPACK-3.3.3.3-Lync-Edge-Internal	jetPACK-3.3.3.4-Lync-Edge-External

Serviços Web

HTTP normal	Descarregamento de SSL	Reencriptação SSL	Passagem SSL
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.2-Descarregamento Web-SSL	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Ambiente de trabalho remoto da Microsoft

Normal
jetPACK-5.5.5.1-Remote-Desktop

DICOM - Imagem Digital e Comunicação em Medicina

HTTP normal
jetPACK-6.6.6.1-DICOM

Oracle e-Business Suite

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

VMware Horizon View

Servidores de ligação - Descarregamento de SSL	Servidores de segurança - Reencriptação SSL
jetPACK-8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

Definições globais

- GUI Secure Port 443 - este jetPACK irá alterar a sua porta GUI segura de 27376 para 443. HTTPs://x.x.x.x
- GUI Timeout 1 day (Tempo limite da GUI 1 dia) - a GUI pede-lhe que introduza a sua palavra-passe de 20 em 20 minutos. Esta definição aumentará esse pedido para 1 dia
- ARP Refresh 10 - durante um failover entre aparelhos HA, esta configuração aumentará o número de **ARP's gratuitos** para ajudar os switches durante a transição
- Tamanho da captura 16MB - o tamanho de captura predefinido é de 2MB. Este valor aumentará o tamanho para um máximo de 16MB

Cipher s e Cipher jetPACKs

O EdgeADC possui as melhores práticas de cifras incluídas como padrão. Estas cifras estão associadas aos respectivos protocolos TLS, o que facilita a tarefa dos utilizadores.

Fornecemos um conjunto de cifras adicionais para utilização, caso seja necessário.

Cifras fortes

Adiciona a capacidade de escolher "Cifras fortes" na lista de opções de cifra:

```
ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
```

Anti-besta

Adiciona a possibilidade de escolher "Anti-Besta" na lista de Opções de Cifra:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
```

Sem SSLv3

Adiciona a capacidade de escolher "Sem SSLv3" na lista Opções de Cifra:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

Não SSLv3 Não TLSv1 Não RC4

Adiciona a capacidade de escolher "No-TLSv1 No-SSLv3 No-RC4" na lista Opções de Cifra:

```
ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
```

NO_TLSv1.1

Adiciona a capacidade de escolher "NO_TLSv1.1" na lista Opções de Cifra:

```
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
```

Ativar as cifras TLS-1.0-1.1

A partir da versão 4.2.10, o suporte de cifra para os protocolos TLS1.0 e TLS 1.1 foi descontinuado. No entanto, alguns clientes continuam a usar esses protocolos antigos e legados para seus servidores internos. O Cipher abaixo adiciona a capacidade de ativar o TLS v1.0 e o TLS v1.1.

```
AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM
```

Exemplo de cifra jetPACK

As cifras são importadas para o ADC usando jetPACKs. Um jetPACK é um ficheiro de texto simples que contém parâmetros que o ADC reconhecerá. O exemplo abaixo mostra um jetPACK usando a cifra Enable TLS-1.0-1.1.

```
#!atualização

[jetnexusdaemon-cipher-TLS1-0-TLS-1-1]

Cifra="AES128-SHA:AES256-SHA:DES-CBC-SHA:DES-CBC3-SHA:EXP-DES-CBC-SHA:RC4-SHA:RC4-MD5:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA:EDH-RSA-DES-CBC-SHA:EDH-RSA-DES-CBC3-SHA:EXP-EDH-RSA-DES-CBC-SHA:EXP-RC2-CBC-MD5:AES128-SHA256:AES256-SHA256:DHE-RSA-AES128-SHA256:DHE-RSA-AES256-SHA256:AES128-GCM-SHA256:AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:DHE-DSS-AES128-SHA256:DHE-DSS-AES256-SHA256:DHE-DSS-AES128-GCM-SHA256:DHE-DSS-AES256-GCM-SHA384:AES:ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM"

Cifra1=""

Cifra2=""

CipherOptions="-NO_TLSv1.0 -NO_TLSv1.1 -NO_TLSv1.2 -NO_TLSv1"

Description=" TLS v1.0 - v1.1 Ativado"
```

- X-Content-Type-Options - adicione este cabeçalho se não existir e defina-o como "nosniff" - impede que o browser efectue automaticamente "MIME-Sniffing".
- X-Frame-Options - adicione este cabeçalho se não existir e defina-o como "SAMEORIGIN" - as páginas do seu sítio Web podem ser incluídas em Frames, mas apenas noutras páginas do mesmo sítio Web.
- X-XSS-Protection - adicione este cabeçalho se não existir e defina-o como "1; mode=block" - ativa as protecções de scripts entre sítios do browser
- Strict-Transport-Security - adicionar cabeçalho se não existir e defini-lo como "max-age=31536000 ; includeSubdomains" - garante que o cliente deve respeitar o facto de todas as hiperligações deverem ser HTTPs:// para a max-age

Aplicação de um jetPACK

Pode aplicar qualquer jetPACK em qualquer ordem, mas tenha cuidado para não utilizar um jetPACK com o mesmo endereço IP virtual. Esta ação irá causar um endereço IP duplicado na configuração. Se o fizer por engano, pode alterá-lo na GUI.

- Navegue para Avançado > Atualizar software
- Secção de configuração
- Carregar nova configuração ou jetPACK
- Procurar por jetPACK
- Clique em Carregar
- Quando o ecrã do navegador ficar branco, clique em atualizar e aguarde que a página do painel de controlo apareça

Criar um jetPACK

Uma das grandes vantagens do jetPACK é o facto de poder criar o seu próprio. Pode acontecer que tenha criado a configuração perfeita para uma aplicação e queira utilizá-la para várias outras caixas de forma independente.

- Comece por copiar a configuração atual do seu ALB-X existente
  - Avançado
  - Atualizar software
  - Descarregar a configuração atual
- Editar este ficheiro com o Notepad++
- Abra um novo documento txt e chame-lhe "yourname-jetPACK1.txt"
- Copie todas as secções relevantes do ficheiro de configuração para "yourname-jetPACK1.txt"
- Guardar uma vez concluído

IMPORTANTE: Cada jetPACK está dividido em diferentes secções, mas todos os jetPACKs têm de ter #!jetpack no topo da página.

As secções que são recomendadas para edição/cópia são as seguintes

Secção 0:

```
#!jetpack
```

Esta linha tem de estar no topo do jetPACK, ou a sua configuração atual será substituída.

Secção 1:

```
[jetnexusdaemon]
```

Esta secção contém definições globais que, uma vez alteradas, se aplicam a todos os serviços. Algumas destas definições podem ser alteradas a partir da consola Web, mas outras só estão disponíveis aqui.

Exemplos:

```
ConnectionTimeout=600000
```

Este exemplo é o valor do tempo limite do TCP em milissegundos. Esta definição significa que uma ligação TCP será fechada após 10 minutos de inatividade

```
ContentServerCustomTimer=20000
```

Este exemplo é o atraso em milissegundos entre as verificações de estado do servidor de conteúdos para monitores personalizados, como o DICOM

```
jnCookieHeader="MS-WSMAN"
```

Este exemplo irá alterar o nome do cabeçalho do cookie utilizado no balanceamento de carga persistente da predefinição "jnAccel" para "MS-WSMAN". Esta alteração específica é necessária para o proxy reverso do Lync 2010/2013.

Secção 2:

```
[jetnexusdaemon-Csm-Rules]
```

Esta secção contém as regras personalizadas de monitorização do servidor que são normalmente configuradas a partir da consola Web.

Exemplo:

```
[jetnexusdaemon-Csm-Rules-0]
Content="Servidor Ativo"
Desc="Monitor 1″
Método="CheckResponse"
Name="Controlo de saúde - O servidor está operacional"
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html"
```

Secção 3:

```
[jetnexusdaemon-LocalInterface]
```

Esta secção contém todos os detalhes da secção Serviços IP. Cada interface é numerada e inclui sub-interfaces para cada canal. Se o seu canal tiver uma regra flightPATH aplicada, também conterá uma secção Path.

Exemplo:

```
[jetnexusdaemon-LocalInterface1]
1.1="443″
1.2="104″
1.3="80″
1.4="81″
Ativado=1
Netmask=”255.255.255.0″
PrimaryV2=”{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}”
[jetnexusdaemon-LocalInterface1.1]
1=">,""Grupo seguro"",2000,"
2="192.168.101.11:80,Y,""IIS WWW Server 1″""
3="192.168.101.12:80,Y,""IIS WWW Server 2″""
AddressResolution=0
CachePort=0
CertificateName="default"
ClientCertificateName="Sem SSL"
Comprimir=1
ConnectionLimiting=0
DSR=0
DSRProto="tcp"
Ativado=1
LoadBalancePolicy="CookieBased"
MaxConnections=10000
MonitoringPolicy="1″
Passagem=0
```

```
Protocolo="Acelerar HTTP"
ServiceDesc="Servidores seguros VIP"
SNAT=0
SSL=1
SSLClient=0
SSLInternalPort=27400
[jetnexusdaemon-LocalInterface1.1-Path]
1="6″
```

Secção 4:

```
[jetnexusdaemon-Path]
```

Esta secção contém todas as regras flightPATH. Os números devem corresponder ao que foi aplicado à interface. No exemplo acima, vemos que a regra flightPATH "6" foi aplicada ao canal, incluindo isso como um exemplo abaixo.

Exemplo:

```
[jetnexusdaemon-Path-6]
Desc="Forçar a utilização de HTTPS para um determinado diretório"
Name="Gary - Forçar HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Verificar="conter"
Condição="caminho"
Corresponder=
Sentido="faz"
Valor="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Detalhe=
Fonte="anfitrião"
Valor=
Variável="$host$"[jetnexusdaemon-Path-6-Function-1]
Ação="redirecionar"
Target="HTTPs://$host$$path$$$querystring$"
Valor=
```

flightPATH

Introdução ao flightPATH

O que é flightPATH?

O flightPATH é um motor de regras inteligente desenvolvido pela Edgenexus para manipular e encaminhar o tráfego HTTP e HTTPS. É altamente configurável, muito poderoso e, no entanto, muito fácil de utilizar.

Embora alguns componentes do flightPATH sejam objectos IP, como o IP de origem, o flightPATH só pode ser aplicado a um tipo de serviço da camada 7 igual a HTTP(s). Se escolher qualquer outro tipo de serviço, o separador flightPATH em IP Services ficará em branco.

O que é que o flightPATH pode fazer?

O flightPATH pode ser utilizado para modificar o conteúdo e os pedidos HTTP(s) de entrada e de saída.

Para além de utilizar correspondências de cadeias simples, como "Começa com" e "Termina com", por exemplo, pode ser implementado um controlo completo utilizando poderosas Expressões Regulares (RegEx) compatíveis com Perl.

Para obter mais informações sobre o RegEx, consulte este site útil

Além disso, podem ser criadas variáveis personalizadas na secção Avaliação e utilizadas na área Ação, permitindo muitas possibilidades diferentes.

Uma regra flightPATH tem três componentes:

Opção	Descrição
Detalhes	Utilizado para adicionar ou remover um flightPATH e listar os disponíveis
Estado	Definir vários critérios para acionar a regra flightPATH.
Avaliação	Permite a utilização de variáveis que podem ser utilizadas na área de Ação.
Ação	O comportamento quando a regra é acionada.

Estado

Nesta secção, é possível especificar cinco parâmetros individuais que se aplicam a uma condição. Estes parâmetros são descritos abaixo com uma descrição de cada opção e um exemplo.

Estado	Descrição	Exemplo
<form>	Os formulários HTML são utilizados para transmitir dados a um servidor	Exemplo "o formulário não tem comprimento 0"
Localização GEO	Isto compara o endereço IP de origem com o código de país ISO 3166	A localização GEO é igual a GB OU a localização GEO é igual a Alemanha
Anfitrião	Este é o anfitrião extraído do URL	www.mywebsite.com ou 192.168.1.1
Língua	Esta é a língua extraída do cabeçalho HTTP da língua	Esta condição produzirá um menu suspenso com uma lista de idiomas
Método	Este é um menu suspenso de métodos HTTP	Trata-se de um menu pendente que inclui GET, POST, etc.
Origem IP	Se o proxy a montante suportar X-Forwarded-for (XFF), utilizará o verdadeiro endereço de origem	IP do cliente. Também pode usar vários IPs ou sub-redes. 10\.1\.2\.* é a sub-rede 10.1.2.0 /24 10\.1\.2\.3|10\.1\.2\.4 Use | para vários IPs

Caminho	Este é o caminho do sítio web	/mywebsite/index.asp
POST	Método de pedido POST	Verificar os dados que estão a ser carregados num sítio Web
Consulta	Este é o nome e o valor de uma consulta, pelo que pode aceitar o nome da consulta ou também um valor	"Best=edgeNEXUS" Em que a correspondência é Best e o valor é edgeNEXUS
Cadeia de consulta	Toda a cadeia de consulta após o carácter ?	
Pedir cookie	Este é o nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho do pedido	Este pode ser qualquer cabeçalho HTTP	Referenciador, User-Agent, De, Data
Versão de pedido	Esta é a versão HTTP	HTTP/1.0 OU HTTP/1.1
Corpo da resposta	Uma cadeia definida pelo utilizador no corpo da resposta	Servidor UP
Código de resposta	O código HTTP da resposta	200 OK, 304 Não Modificado
Biscoito de resposta	Este é o nome de um cookie enviado pelo servidor	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho de resposta	Este pode ser qualquer cabeçalho HTTP	Referenciador, User-Agent, De, Data
Versão de resposta	A versão HTTP enviada pelo servidor	HTTP/1.0 OU HTTP/1.1
Fonte IP	Este é o IP de origem, o IP do servidor proxy ou outro endereço IP agregado	IP do cliente IP do cliente, IP do proxy, IP da firewall. Também pode usar vários IPs e sub-redes. É deve escapar dos pontos, pois eles são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Jogo

O parâmetro Match (Corresponder) é sensível ao contexto, dependendo do valor do parâmetro Condition (Condição).

Jogo	**Descrição**	**Exemplo**
Aceitar	Tipos de conteúdo aceitáveis	Aceitar: text/plain
Aceitar codificação	Codificações aceitáveis	Aceitar codificação: <compress | gzip | deflate | sdch | identity>
Aceitar-Língua	Línguas aceitáveis para a resposta	Accept-Language: en-US
Aceitar intervalos	Que tipos de intervalo de conteúdo parcial este servidor suporta	Accept-Ranges: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básica QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carregar-até	Contém informações contabilísticas relativas aos custos de aplicação do método solicitado	
Content-Encoding	O tipo de codificação utilizado nos dados.	Content-Encoding: gzip

Comprimento do conteúdo	O comprimento do corpo da resposta em octetos (bytes de 8 bits)	Content-Length: 348
Tipo de conteúdo	O tipo mime do corpo do pedido (utilizado com pedidos POST e PUT)	Content-Type: application/x-www-form-urlencoded
Biscoito	Um cookie HTTP previamente enviado pelo servidor com Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Date = "Date" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, frequentemente um resumo de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de correio eletrónico do utilizador que faz o pedido	De: user@example.com
Se-Modificado-Desde	Permite que seja devolvido um 304 Not Modified se o conteúdo não for alterado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificação	A data da última modificação do objeto pedido, no formato RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Os cabeçalhos específicos da implementação podem ter vários efeitos em qualquer ponto da cadeia pedido-resposta.	Pragma: no-cache
Referenciador	Este é o endereço da página Web anterior a partir da qual foi seguida uma ligação para a página atualmente solicitada	Referenciador: HTTP://www.edgenexus.io
Servidor	Um nome para o servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	Um cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente do utilizador	A cadeia do agente do utilizador do agente do utilizador	User-Agent: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variar	Diz aos proxies a jusante como fazer corresponder os cabeçalhos de pedidos futuros para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova do servidor de origem	Vary: User-Agent
X-Powered-By	Especifica a tecnologia (por exemplo, ASP.NET, PHP, JBoss) que suporta a aplicação Web	X-Powered-By: PHP/5.4.0

Verificar

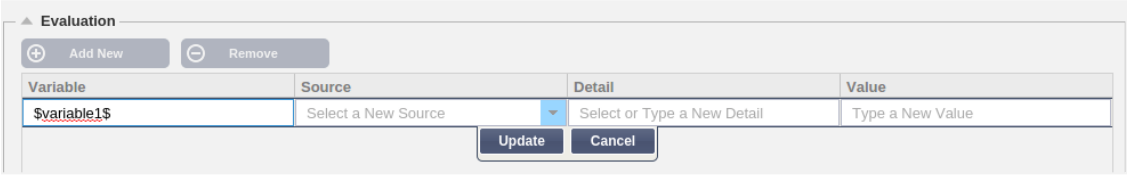
Verificar	**Descrição**	**Exemplo**
Existir	Não se preocupa com o pormenor da condição, apenas com o facto de existir ou não existir	Host> Does> Exist
Início	A cadeia começa com o valor	Caminho> Does> Start> /secure
Fim	A cadeia termina com o valor	Caminho> Does> End> .jpg
Conter	A cadeia de caracteres contém efetivamente o valor	Request Header> Accept> Does> Contain> Image
Igual	A cadeia de caracteres é igual ao valor	Anfitrião> Does> Equal> www.edgenexus.io

Ter comprimento	A cadeia tem de facto o comprimento do valor	Anfitrião> O> tem comprimento> 16 www.edgenexus.io = VERDADEIRO www.edgenexus.com = FALSO
Exceder o comprimento	Verificar se o valor excede/não excede o comprimento especificado.	Caminho > Faz > Exceder o comprimento - 10
Corresponder RegEx	Isto permite-lhe introduzir uma expressão regular completa compatível com Perl	IP de origem> Does> Match Regex> 10\..* | 11\..*
Lista de jogos	Permite fornecer uma lista delimitada PIPE (|) de valores que podem ser verificados.	IP de origem > Faz > Lista de correspondências > 10.0.0.1 | 10.0.0.100 | 192.178.28.32

Exemplo

- O exemplo tem duas condições, e **AMBAS** têm de ser cumpridas para executar a ação
- A primeira é verificar se o objeto pedido é uma imagem
- A segunda é a verificação de um nome de host específico

Avaliação



A adição de uma variável é um recurso atraente que permite extrair dados do pedido e utilizá-los nas ações. Por exemplo, pode registar um nome de utilizador ou enviar um e-mail se houver um problema de segurança.

- Variável: Deve começar e terminar com o símbolo $. Por exemplo, $variable1$
- Fonte: Selecione na caixa pendente a fonte da variável
- Detalhe: Selecionar da lista quando relevante. Se a Fonte=Cabeçalho de pedido, os Detalhes podem ser User-Agent
- Valor: Introduza o texto ou a expressão regular para afinar a variável.

Variáveis incorporadas:

- As variáveis incorporadas já foram codificadas, pelo que não é necessário criar uma entrada de análise para elas.
- Pode utilizar qualquer uma das variáveis abaixo indicadas na sua ação
- A explicação de cada variável encontra-se no quadro "Condição" acima
    - Método = $método$
    - Caminho = $caminho$
    - Querystring = $querystring$
    - Sourceip = $sourceip$
    - Código de resposta (o texto também inclui "200 OK") = $resp$
    - Anfitrião = $host$
    - Versão = $versão$

- Porta do cliente = $clientport$
- Clientip = $clientip$
- Geolocalização = $geolocalização$"

Exemplo de ação:

- Ação = Redirecionar 302
  - Destino = HTTPs://$host$/404.html
- Ação = Registo
  - Target = Um cliente de $sourceip$:$sourceport$ acabou de efetuar um pedido de página $path$

Explicação:

- Um cliente que aceda a uma página que não existe seria normalmente confrontado com uma página 404 do navegador
- Neste caso, o utilizador é redireccionado para o nome de anfitrião original que utilizou, mas o caminho errado é substituído por 404.html
- É adicionada uma entrada ao syslog dizendo "Um cliente de 154.3.22.14:3454 acabou de fazer um pedido à página wrong.html"

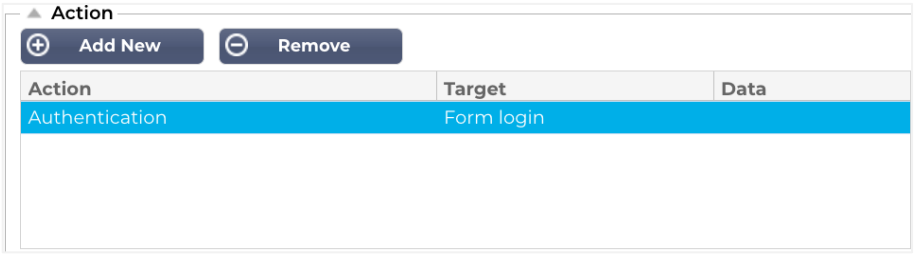
Fonte	Descrição	Exemplo
Biscoito	Este é o nome e o valor do cabeçalho do cookie	MS-WSMAN=afYfn1CDqqCDqUD::Em que o nome é MS-WSMAN e o valor é afYfn1CDqqCDqUD::
Anfitrião	Este é o nome do anfitrião extraído do URL	www.mywebsite.com ou 192.168.1.1
Língua	Esta é a língua extraída do cabeçalho HTTP Language	Esta condição produzirá um menu pendente com uma lista de línguas.
Método	Este é um menu suspenso de métodos HTTP	O menu suspenso incluirá GET, POST
Caminho	Este é o caminho do sítio web	/mywebsite/index.html
POST	Método de pedido POST	Verificar os dados que estão a ser carregados para um sítio Web
Item de consulta	Este é o nome e o valor de uma consulta. Como tal, pode aceitar o nome da consulta ou também um valor	"Best=jetNEXUS" Em que a correspondência é Best e o valor é edgeNEXUS
Cadeia de consulta	Esta é a cadeia inteira depois do carácter ?	HTTP://servidor/caminho/programa?query_string
Cabeçalho do pedido	Pode ser qualquer cabeçalho enviado pelo cliente	Referrer, User-Agent, From, Date...
Cabeçalho de resposta	Pode ser qualquer cabeçalho enviado pelo servidor	Referrer, User-Agent, From, Date...
Versão	Esta é a versão HTTP	HTTP/1.0 ou HTTP/1.1

Detalhes	Descrição	Exemplo
Aceitar	Tipos de conteúdo aceitáveis	Aceitar: text/plain
Aceitar codificação	Codificações aceitáveis	Aceitar codificação: <compress | gzip | deflate | sdch | identity>
Aceitar-Língua	Línguas aceitáveis para a resposta	Accept-Language: en-US
Aceitar intervalos	Que tipos de intervalo de conteúdo parcial este servidor suporta	Accept-Ranges: bytes

Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básica QWxhZGRpbjpvcGVuIHNlc2FtZQ==
Carregar-até	Contém informações contabilísticas relativas aos custos de aplicação do método solicitado	
Content-Encoding	O tipo de codificação utilizado nos dados.	Content-Encoding: gzip
Comprimento do conteúdo	O comprimento do corpo da resposta em octetos (bytes de 8 bits)	Content-Length: 348
Tipo de conteúdo	O tipo mime do corpo do pedido (utilizado com pedidos POST e PUT)	Content-Type: application/x-www-form-urlencoded
Biscoito	um cookie HTTP previamente enviado pelo servidor com Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Date = "Date" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, frequentemente um resumo de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de correio eletrónico do utilizador que faz o pedido	De: user@example.com
Se-Modificado-Desde	Permite que seja devolvido um 304 Not Modified se o conteúdo não for alterado	If-Modified-Since: Sat, 29 Oct 1994 19:43:31 GMT
Última modificação	A data da última modificação do objeto pedido, no formato RFC 2822	Last-Modified: Tue, 15 Nov 1994 12:45:26 GMT
Pragma	Cabeçalhos específicos da implementação que podem ter vários efeitos em qualquer ponto da cadeia pedido-resposta.	Pragma: no-cache
Referenciador	Este é o endereço da página Web anterior a partir da qual foi seguida uma ligação para a página atualmente solicitada	Referenciador: HTTP://www.edgenexus.io
Servidor	Um nome para o servidor	Servidor: Apache/2.4.1 (Unix)
Set-Cookie	um cookie HTTP	Set-Cookie: UserID=JohnDoe; Max-Age=3600; Version=1
Agente do utilizador	A cadeia do agente do utilizador do agente do utilizador	User-Agent: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Variar	Diz aos proxies a jusante como fazer corresponder os cabeçalhos de pedidos futuros para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova do servidor de origem	Vary: User-Agent
X-Powered-By	Especifica a tecnologia (por exemplo, ASP.NET, PHP, JBoss) que suporta a aplicação Web	X-Powered-By: PHP/5.4.0

Ação

A ação é a tarefa ou tarefas que são activadas quando a condição ou condições são satisfeitas.



Ação

Faça duplo clique na coluna Ação para ver a lista pendente.

Objetivo

Faça duplo clique na coluna Destino para ver a lista pendente. A lista muda consoante a Ação.

Também pode escrever manualmente com algumas acções.

Dados

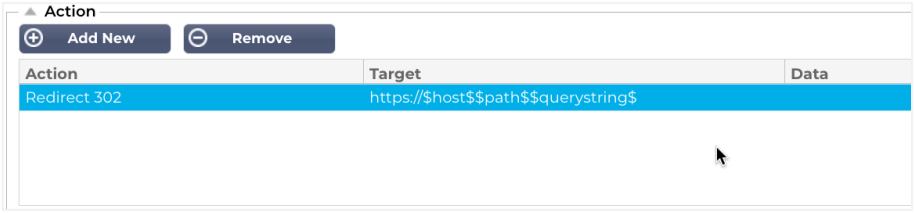
Faça duplo clique na coluna Dados para adicionar manualmente os dados que pretende acrescentar ou substituir.

A lista de todas as acções é apresentada em seguida:

Ação	Descrição	Exemplo
Adicionar cookie de pedido	Adicionar cookie de pedido detalhado na secção Destino com valor na secção Dados	Alvo= Cookie Dados= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar cabeçalho do pedido	Adicionar um cabeçalho de pedido do tipo Target com valor na secção Data	Objetivo= Aceitar Dados= imagem/png
Adicionar cookie de resposta	Adicione o cookie de resposta detalhado na secção Destino com o valor na secção Dados	Alvo= Cookie Dados= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar cabeçalho de resposta	Adicionar cabeçalho de pedido detalhado na secção Destino com valor na secção Dados	Target= Cache-Control Dados= max-age=8888888
Corpo Substituir tudo	Pesquisar o corpo da resposta e substituir todas as instâncias	Target= HTTP:// (Cadeia de pesquisa) Data= HTTPs:// (Cadeia de substituição)
Corpo Substituir primeiro	Pesquisar o corpo da resposta e substituir apenas a primeira instância	Target= HTTP:// (Cadeia de pesquisa) Data= HTTPs:// (Cadeia de substituição)
Corpo Substituir Último	Pesquisar o corpo da resposta e substituir apenas a última instância	Target= HTTP:// (Cadeia de pesquisa) Data= HTTPs:// (Cadeia de substituição)
Gota	Isto irá interromper a ligação	Objetivo= N/A Dados= N/A
Correio eletrónico	Enviará uma mensagem de correio eletrónico para o endereço configurado em Eventos de correio eletrónico. Pode utilizar uma variável como o endereço ou a mensagem	Target= "flightPATH enviou este evento por correio eletrónico" Dados= N/A
Evento de registo	Isto irá registar um evento no registo do sistema	Target= "flightPATH registou isto no syslog" Dados= N/A

Redirecionar 301	Isto irá emitir um redireccionamento permanente	Alvo= HTTP://www.edgenexus.io Dados= N/A
Redirecionar 302	Isto irá emitir um redireccionamento temporário	Alvo= HTTP://www.edgenexus.io Dados= N/A
Remover cookie de pedido	Remover o cookie de pedido detalhado na secção Destino	Alvo= Cookie Dados= MS-WSMAN=afYfn1CDqqCDqCVii
Remover o cabeçalho do pedido	Remover o cabeçalho do pedido detalhado na secção Destino	Destino=Servidor Dados=N/A
Remover cookie de resposta	Remover o cookie de resposta detalhado na secção Destino	Objetivo=jnAccel
Remover o cabeçalho de resposta	Remover o cabeçalho de resposta detalhado na secção Destino	Target= Etag Dados= N/A
Substituir o cookie de pedido	Substituir o cookie de pedido detalhado na secção Destino pelo valor na secção Dados	Alvo= Cookie Dados= MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho do pedido	Substituir o cabeçalho do pedido no Target pelo valor Data	Objetivo= Ligação Data= keep-alive
Substituir cookie de resposta	Substituir o cookie de resposta detalhado na secção Destino pelo valor na secção Dados	Target=jnAccel=afYfn1CDqqCDqCVii Date=MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho de resposta	Substituir o cabeçalho de resposta detalhado na secção Destino pelo valor na secção Dados	Objetivo= Servidor Dados= Retidos por razões de segurança
Reescrever caminho	Isto permitir-lhe-á redirecionar o pedido para um novo URL com base na condição	Target= /test/path/index.html$querystring$ Dados= N/A
Utilizar um servidor seguro	Selecionar o servidor seguro ou serviço virtual a utilizar	Target=192.168.101:443 Dados=N/A
Utilizar o servidor	Selecionar o servidor ou serviço virtual a utilizar	Alvo= 192.168.101:80 Dados= N/A
Encriptar cookie	Isto irá encriptar os cookies em 3DES e depois codificá-los em base64	Target= Introduzir o nome do cookie a ser encriptado, podendo utilizar o * como wild card no final Data= Introduzir uma frase-passe para a encriptação

Exemplo:



A ação abaixo emitirá um redireccionamento temporário para o browser para um Serviço Virtual HTTPS seguro. Ele usará o mesmo nome de host, caminho e string de consulta que a solicitação.

Utilizações comuns

Firewall e segurança de aplicações

- Bloquear IPs indesejados
- Forçar o utilizador a utilizar HTTPS para conteúdos específicos (ou todos)
- Bloquear ou redirecionar os spiders
- Prevenir e alertar o cross-site scripting
- Prevenir e alertar a injeção de SQL
- Ocultar a estrutura interna do diretório
- Reescrever cookies
- Diretório seguro para determinados utilizadores

Caraterísticas

- Redirecionar os utilizadores com base no caminho
- Proporcionar um início de sessão único em vários sistemas
- Segmentar utilizadores com base no ID de utilizador ou Cookie
- Adicionar cabeçalhos para descarregamento de SSL
- Deteção de línguas
- Reescrever o pedido do utilizador
- Corrigir URLs quebrados
- Registo e alerta por correio eletrónico dos códigos de resposta 404
- Impedir o acesso a diretórios/ navegação
- Enviar conteúdos diferentes aos spiders

Regras pré-construídas

Extensão HTML

Altera todos os pedidos .htm para .html

Estado:

- Condição = Caminho
- Sentido = Faz
- Check = Corresponder RegEx
- Valor = \.htm$

Avaliação:

- Em branco

Ação:

- Ação = Reescrever caminho
- Destino = $caminho$l

Índice.html

Força a utilização de index.html em pedidos para pastas.

Condição: esta condição é uma condição geral que corresponde à maioria dos objectos

- Condição = Anfitrião

- Sentido = Faz
- Verificar = Existir

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Destino = HTTP://$host$$path$index.html$querystring$

Fechar pastas

Recusar pedidos de pastas.

Condição: esta condição é uma condição geral que corresponde à maioria dos objectos

- Condição = isto precisa de ser bem pensado
- Sentido =
- Verificar =

Avaliação:

- Em branco

Ação:

- Ação =.
- Alvo =

Ocultar CGI-BBIN:

Oculta o catálogo cgi-bin em pedidos para scripts CGI.

Condição: esta condição é uma condição geral que corresponde à maioria dos objectos

- Condição = Anfitrião
- Sentido = Faz
- Verificar = Corresponder ao RegEX
- Valor = \.cgi$

Avaliação:

- Em branco

Ação:

- Ação = Reescrever caminho
- Destino = /cgi-bin$path$

Aranha de tronco

Registar pedidos de spider de motores de pesquisa populares.

Condição: esta condição é uma condição geral que corresponde à maioria dos objectos

- Condição = Cabeçalho do pedido
- Correspondência = User-Agent
- Sentido = Faz
- Verificar = Corresponder ao RegEX

- Valor = Googlebot|Slurp|bingbot|ia_archiver

Avaliação:

- Variável = $crawler$
- Fonte = Cabeçalho do pedido
- Detalhe = User-Agent

Ação:

- Ação = Registar evento
- Alvo = [$crawler$] $host$$path$$$querystring$

Forçar HTTPS

Força a utilização de HTTPS para um determinado diretório. Neste caso, se um cliente estiver a aceder a algo que contenha o diretório /secure/, será redireccionado para a versão HTTPs do URL solicitado.

Estado:

- Condição = Caminho
- Sentido = Faz
- Verificar = Conter
- Valor = /secure/

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Destino = HTTPs://$host$$path$$$querystring$

Fluxo dos media:

Redirecciona o Flash Media Stream para o serviço adequado.

Estado:

- Condição = Caminho
- Sentido = Faz
- Verificar = Fim
- Valor = .flv

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Destino = HTTP://$host$:8080/$path$

Trocar HTTP por HTTPS

Altere qualquer HTTP:// codificado para HTTPS://

Estado:

- Condição = Código de resposta

- Sentido = Faz
- Verificar = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Corpo Substituir tudo
- Destino = HTTP://
- Dados = HTTPs://

Esgotar os cartões de crédito

Verificar se não existem cartões de crédito na resposta e, se for encontrado um, apagá-lo.

Estado:

- Condição = Código de resposta
- Sentido = Faz
- Verificar = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Corpo Substituir tudo
- 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]+
- Dados = xxxx-xxxx-xxxx-xxxx

Expiração de conteúdo

Acrescente uma data de expiração de conteúdo sensata à página para reduzir o número de pedidos e 304s.

Condição: esta é uma condição genérica que serve para englobar tudo. Recomenda-se que esta condição se centre na sua

- Condição = Código de resposta
- Sentido = Faz
- Verificar = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Adicionar cabeçalho de resposta
- Objetivo = Cache-Control
- Dados = max-age=3600

Tipo de servidor de falsificação

Obtenha o Tipo de servidor e altere-o para outra coisa.

Condição: esta é uma condição genérica que serve para englobar tudo. Recomenda-se que esta condição se centre na sua

- Condição = Código de resposta
- Sentido = Faz
- Verificar = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Substituir o cabeçalho da resposta
- Objetivo = Servidor
- Dados = Secretos

Nunca enviar erros

O cliente nunca recebe nenhum erro do vosso site.

Estado

- Condição = Código de resposta
- Sentido = Faz
- Verificar = Conter
- Valor = 404

Avaliação

- Em branco

Ação

- Ação = Redirecionar 302
- Destino = HTTP//$host$/

Redirecionar para a língua

Encontre o código da língua e redireccione para o domínio do país relacionado.

Estado

- Condição = Língua
- Sentido = Faz
- Verificar = Conter
- Valor = Alemão (Standard)

Avaliação

- Variável = $host_template$
- Fonte = Anfitrião
- Valor = .*\.

Ação

- Ação = Redirecionar 302
- Objetivo = HTTP//$host_template$de$path$$$querystring$

Google Analytics

Insira o código exigido pelo Google para a análise - Altere o valor MYGOOGLECODE para o seu ID UA do Google.

Estado

- Condição = Código de resposta
- Sentido = Faz
- Verificar = Igual
- Valor = 200 OK

Avaliação

- em branco

Ação

- Ação = Corpo Substituir Último
- Objetivo = </body>
- Dados = <script type='text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs//ssl' 'HTTP//www') + '.google-analytics.com/ga.js'; var s = document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); })(); </script> </body>

Gateway IPv6

Ajustar o cabeçalho do host para servidores IPv4 do IIS em serviços IPv6. Os servidores IPv4 do IIS não gostam de ver um endereço IPV6 no pedido do cliente anfitrião, pelo que esta regra substitui-o por um nome genérico.

Estado

- em branco

Avaliação

- em branco

Ação

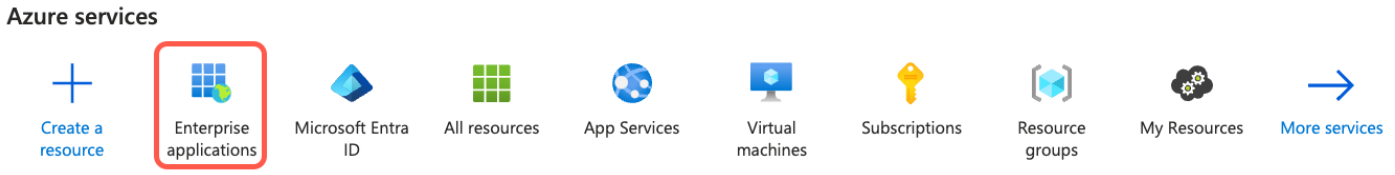
- Ação = Substituir o cabeçalho do pedido
- Alvo = Anfitrião
- Dados =ipv4.host.header

SAML e Entra ID

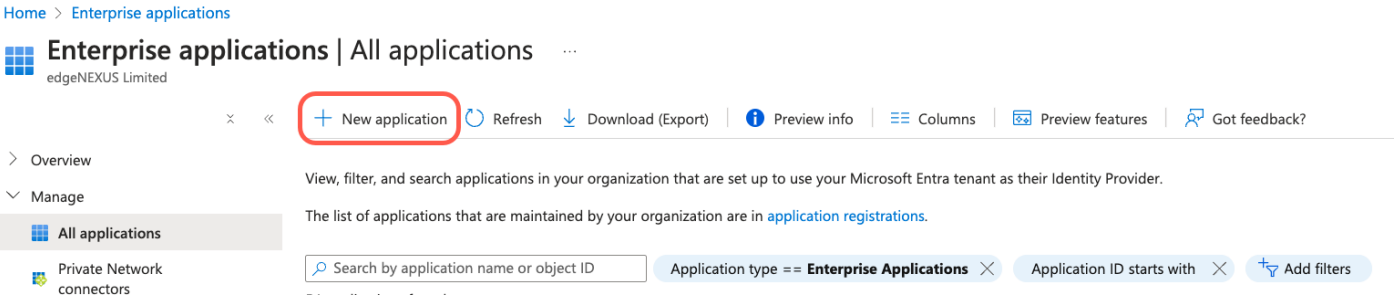
Configurando o aplicativo de autenticação Entra ID no Microsoft Entra

Para que a autenticação SAML funcione com êxito, é necessário configurar uma aplicação empresarial no seu portal Microsoft Entra Admin. Esta é uma tarefa simples e permite o aprovisionamento do certificado de assinatura necessário para pedidos de autenticação SAML e tokens, bem como os dados XML de configuração.

Para tal, deve começar por iniciar sessão no Portal Microsoft Entra (https://portal.azure.com) e certificar-se de que está na página Serviços Azure, onde encontrará uma lista de ícones na parte superior da página (ver abaixo).

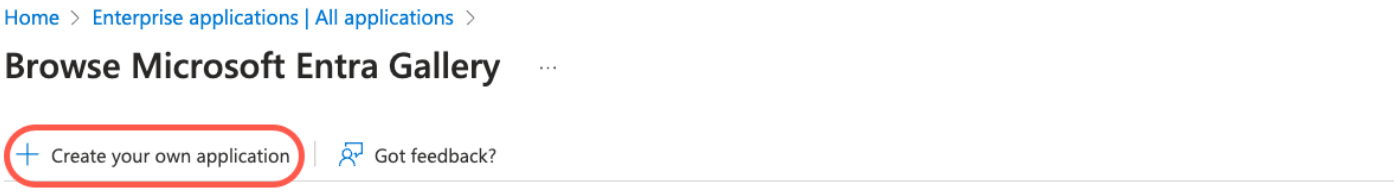


- Clique em Aplicações Empresariais. Se não conseguir ver Aplicações Empresariais na lista de ícones, pode introduzir o nome na barra de pesquisa na parte superior. Aparecerá uma página como a mostrada abaixo.

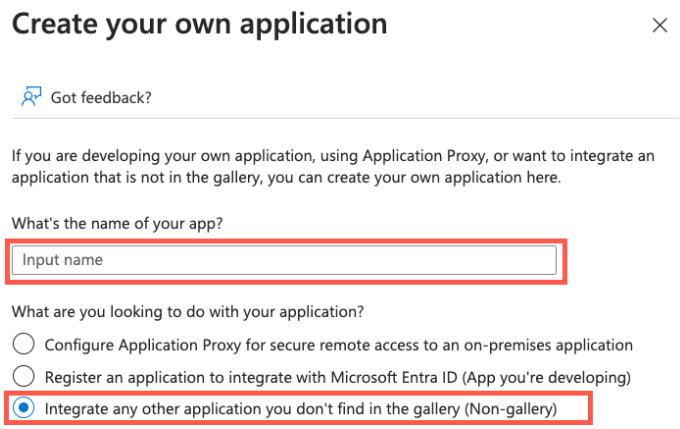


Clique em *Nova aplicação*

Na página seguinte, clique em *Criar a sua própria aplicação*.

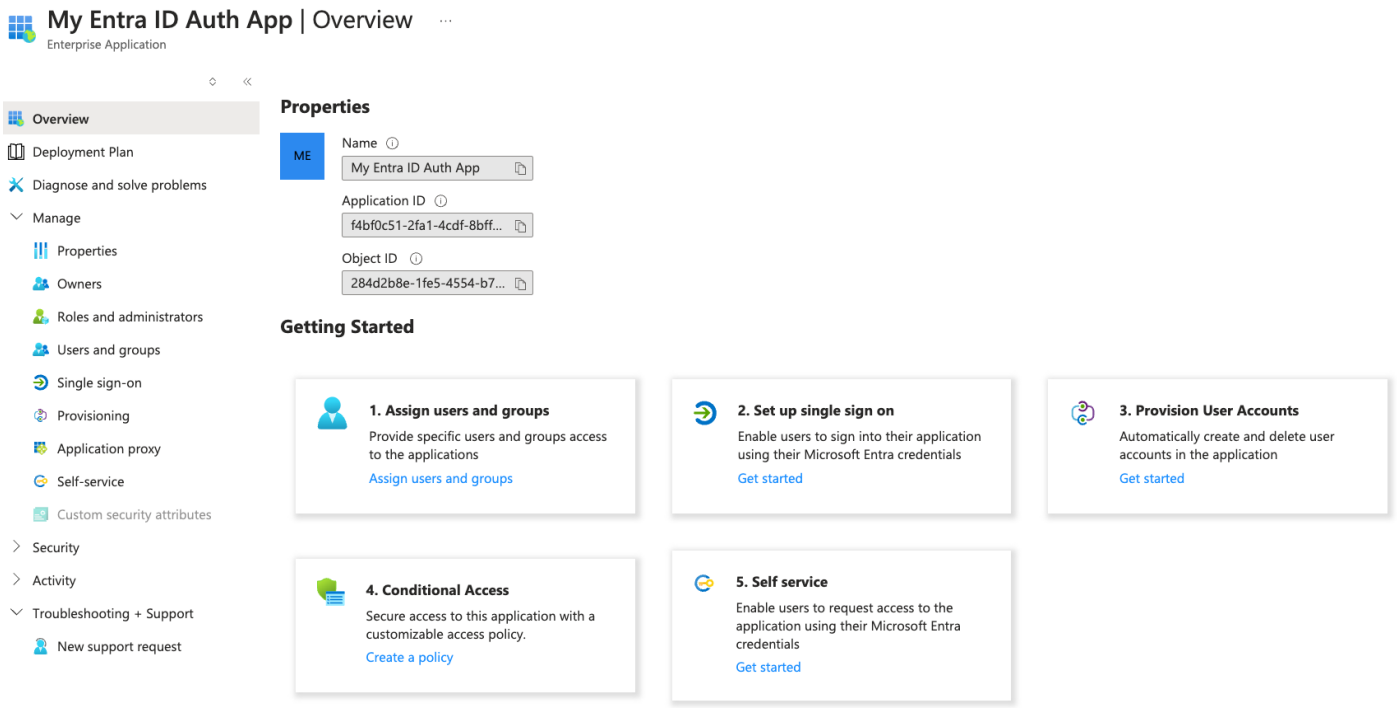


- Será aberta uma secção no lado direito da página com o título "*Criar a sua própria aplicação*".

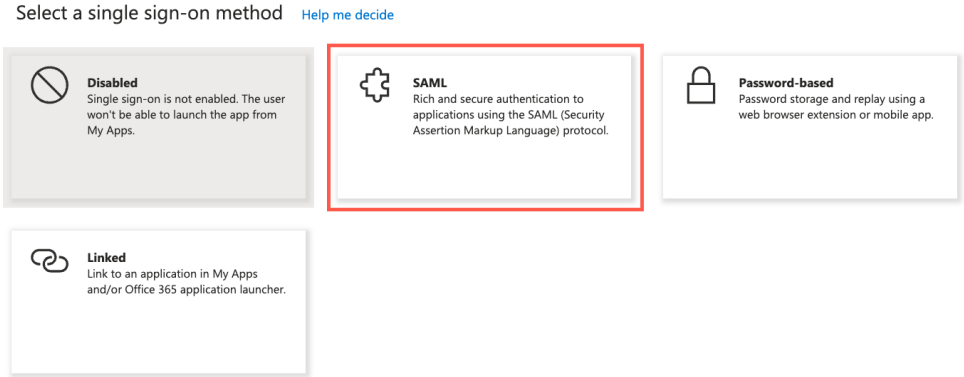


- Forneça um nome para o seu aplicativo, por exemplo, "Meu aplicativo Entra ID Auth". Pode escolher o nome que desejar.
- Clique na opção de botão de rádio *Integrar qualquer outra aplicação que não se encontre na galeria (não pertencente à galeria)*.
- Clique no botão *Criar*.

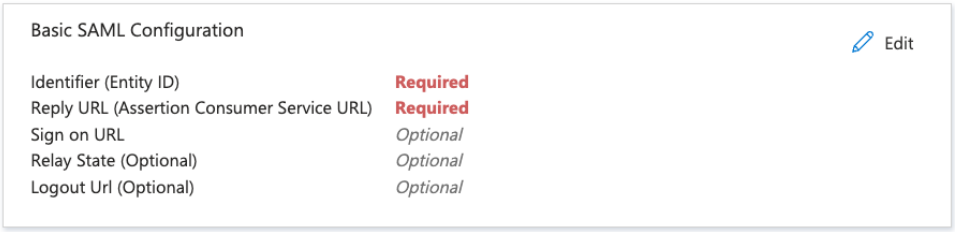
Ser-lhe-á apresentada uma página semelhante à que se segue.



- Clique na opção Início de sessão único localizada na barra de navegação esquerda.
- Selecione a caixa SAML



- É apresentada uma página que contém a secção Configuração básica de SAML.



- Na área Configuração básica de SAML, preencha:
  - Identificador (ID da entidade)
  - URL de resposta (URL do serviço de consumidor de asserções)
  - URL de início de sessão
  - URL de saída (opcional)
- Guarde a sua configuração e teste a aplicação.

Para obter orientações mais detalhadas, pode consultar a documentação Ativar início de sessão único para uma aplicação empresarial no site da Microsoft.

Apoio técnico

Prestamos apoio técnico a todos os nossos utilizadores de acordo com as condições de serviço padrão da empresa.

Forneceremos suporte técnico se você tiver um contrato de suporte e manutenção ativo para o EdgeADC, EdgeWAF ou EdgeGSLB.

Para criar um ticket de suporte, visite:

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