EdgeADC

GUIA DE ADMINISTRAÇÃO

Conteúdo

Propriedades do documento 7
Documento Disclaimer 7
Direitos autorais 7
Marcas 7
Apoio da Edgenexus 7
Instalar o EdgeADC 8
VMware ESXi 8
Instalação da interface VMXNET3 8
Microsoft Hyper-V 9
Citrix XenServer 11
Primeira configuração da bota 12
Primeira Bota - Detalhes da Rede Manual 12
Primeira Bota - DHCP bem-sucedido 12
Primeira Bota - DHCP Falhas 12
Mudança do endereço IP da Administração 13
Mudança da Máscara de sub-rede para eth0 13
Atribuição de um Portal de Inadimplência 13
Verificação do valor do Default Gateway 13
Acesso à interface web 13
Tabela de Referência do Comando 14
Lançamento do ADC Web Console 16
Credenciais de Login Padrão 16
O Painel Principal 17
Serviços 18
Serviços de PI 18
Serviços virtuais 18
Servidores reais 25
Mudanças Reais no Servidor para Retorno Direto do Servidor 37
Configuração do Servidor de Conteúdo Requerido 38
Mudanças reais no servidor - Modo Gateway 39
Configuração do Servidor de Conteúdo Requerido 39
Exemplo de braço único 39
Exemplo de braço duplo 40
Biblioteca 41
Suplementos 41
Apps 41
Compra de um suplemento 41

Implantação de uma App 42
Autenticação 43
Estabelecimento da Autenticação - Um Fluxo de Trabalho 43
Servidores de autenticação 43
Regras de autenticação 44
Assinatura única 45
Formulários 45
Cache 47
vôoPATH 49
Monitores de servidores reais 56
Detalhes 56
Exemplos de monitoramento de servidores reais 59
Certificados SSL 61
O que o ADC faz com o Certificado SSL? 61
Criar certificado 62
Gerenciar Certificado 63
Importação de um certificado 66
Importação de certificados múltiplos 67
Widgets 68
Ver 75
Painel de controle 75
Uso do painel de instrumentos 75
História 77
Visualização dos dados gráficos 77
Logs 78
Download dos logs do W3C 79
Estatísticas 79
Compressão 79
Acertos e conexões 80
Caching 81
Persistência da sessão 81
Hardware 82
Status 82
Detalhes do Serviço Virtual 82
Sistema 85
Clustering 85
Papel 85
Configurações 88

Administração....88
Mudança da prioridade de um ADC....89
Data e hora....90
Manual Data e hora....90
Sincronizar data e hora (UTC)....90
Eventos por e-mail....91
Endereço....91
Servidor de correio (SMTP)....92
Notificações e alertas....92
Avisos....93
Histórico do sistema....93
Coleta de dados....94
Manutenção....94
Licença....94
Detalhes da licença....95
Instalações....96
Instalar Licenças e....96
Logging....96
W3C Detalhes de registro....96
Servidor Syslog....98
Servidor remoto Syslog....98
Armazenamento remoto de logs....99
Limpar arquivos de log....101
Rede....101
Configuração básica....101
Detalhes do Adaptador....102
Interfaces....102
Ligação....103
Rota estática....105
Detalhes da rota estática....105
Configurações avançadas da rede....105
SNAT....106
Poder....107
Segurança....107
SNMP....109
Configurações do SNMP....109
SNMP MIB....109
MIB Download....109

ADC OID 110
Gráfico Histórico 110
Usuários e diários de auditoria 111
Usuários 111
Diário de Auditoria 113
Avançado 114
Configuração 114
Descarregar uma configuração 114
Carregamento de uma configuração 114
Configurações globais 115
Timer Cache anfitrião 115
Dreno 115
SSL 115
Autenticação 115
Protocolo 116
Servidor muito ocupado 116
Encaminhado para 116
Configurações de Compressão HTTP 117
Exclusões de Compressão Global 119
Biscoitos de persistência 119
Software 119
Detalhes da atualização do software 120
Baixar do Cloud 120
Upload de software para a ALB 121
Aplicar o software armazenado na ALB 121
Solução de problemas 122
Arquivos de apoio 122
Trace 122
Ping 123
Captura 124
Ajuda 125
Sobre nós 125
Referência 125
O que é um jetPACK 126
Descarregamento de um jetPACK 126
Microsoft Exchange 126
Microsoft Lync 2010/2013 128
Serviços Web 128

Área de trabalho remota da Microsoft....128
DICOM - Imagem e Comunicação Digital em Medicina....128
Oracle e-Business Suite....128
Vista Horizonte VMware....128
Configurações globais....128
Opções cifradas....129
vôosPATHs....129
Aplicação de um jetPACK....129
Criação de um jetPACK....130
Introdução ao FlightPATH....133
O que é vôoPATH?....133
O que pode fazer o FlightPATH?....133
Condição....133
Exemplo....136
Avaliação....136
Ação....139
Ação....139
Alvo....139
Dados....139
Usos comuns....141
Aplicação Firewall e Segurança....141
Características....141
Regras pré-construídas....141
Extensão HTML....141
Index.html....142
Fechar Pastas....142
Ocultar CGI-BBIN:....142
Aranha de madeira....143
Forçar HTTPS....143
Media Stream:....144
Trocar HTTP para HTTPS....144
Cartões de crédito em branco....144
Expiração do conteúdo....145
Spoof Server Tipo....145
Web Application Firewall (edgeWAF)....148
Execução do WAF....148
Exemplo de arquitetura....149
WAF usando endereço IP externo....149

WAF usando endereço IP interno 149
Acesso ao seu WAF add-on 150
Atualização das Regras 151
Balanceamento de Carga do Servidor Global (edgeGSLB) 153
Introdução 153
Resiliência e recuperação de desastres 153
Balanceamento de carga e geo-localização 153
Considerações comerciais 153
Visão geral do sistema de nomes de domínio 153
O DNS é composto de três componentes-chave: 153
Uma transação típica do DNS é explicada abaixo: 153
Caching 154
Tempo para viver 154
Visão geral da GSLB 154
Configuração da GSLB 154
Locais personalizados 160
Redes Privadas 160
Como funciona 160
Como configuramos esse aspecto na GSLB? 161
Fluxo de tráfego 163
Apoio técnico 164

Propriedades do documento

Número do documento: 2.0.6.16.21.17.06

Data de criação do documento: 30 de abril de 2021

Documento Editado por último: June 16, 2021

Autor do documento: Jay Savoor

Último documento editado por:

Indicação de documentos: EdgeADC - Versão 4.2.7.1895

Documento Disclaimer

As imagens e gráficos deste manual podem diferir ligeiramente de seu produto devido a diferenças na versão de lançamento de seu produto. A Edgenexus se assegura de que eles fazem todo o esforço razoável para assegurar que as informações contidas neste documento sejam completas e precisas. A Edgenexus não assume nenhuma responsabilidade por qualquer erro. A Edgenexus faz mudanças e correções nas informações deste documento em futuros lançamentos, quando a necessidade surgir.

Direitos autorais

© 2021Todos os direitos reservados.

As informações contidas neste documento estão sujeitas a mudanças sem aviso prévio e não representam um compromisso da parte do fabricante. Nenhuma parte deste guia pode ser reproduzida ou transmitida de qualquer forma ou meio, eletrônico ou mecânico, inclusive fotocópia e gravação, para qualquer finalidade, sem a permissão expressa por escrito do fabricante. As marcas registradas são propriedades de seus respectivos proprietários. Todo esforço é feito para tornar este guia tão completo e preciso quanto possível, mas nenhuma garantia de aptidão está implícita. Os autores e o editor não terão qualquer responsabilidade ou obrigação perante qualquer pessoa ou entidade por perdas ou danos decorrentes do uso das informações contidas neste guia.

Marcas

O logotipo da Edgenexus, Edgenexus, EdgeADC, EdgeWAF, EdgeGSLB, EdgeDNS são marcas registradas ou marcas comerciais da Edgenexus Limited. Todas as outras marcas registradas são propriedades de seus respectivos proprietários e são reconhecidas.

Apoio da Edgenexus

Caso tenha alguma dúvida técnica a respeito deste produto, favor levantar um ticket de apoio em: support@edgenexus.io

Instalar o EdgeADC

O produto EdgeADC (referido a partir de agora como ADC) está disponível para instalação por vários métodos. Cada alvo de plataforma requer seu instalador, e todos eles estão à disposição do senhor.

Estes são os vários modelos de instalação disponíveis.

- VMware ESXi
- KVM
- Microsoft Hyper-V
- Oráculo VM
- ISO para ferragens BareMetal

O dimensionamento da máquina virtual que o senhor usará para hospedar o ADC depende do cenário do caso de uso e da produção de dados.

VMware ESXi

O ADC está disponível para instalação no VMware ESXi são 5,x e acima.

- Faça o download do último pacote de instalação OVA do ADC usando o link apropriado fornecido com o e-mail de download.
- Uma vez baixado, favor descompactar em um diretório adequado em seu ESXi host ou SAN.
- Em seu cliente vSphere, selecione File: Deploy OVA/OVF Template.
- Navegue e selecione o local onde você salvou seus arquivos; escolha o arquivo OVF e clique em **SEGUINTE**
- O servidor ESX solicita o nome do aparelho. Digite um nome adequado e clique em **SEGUINTE**
- Selecione o datastore de onde seu aparelho do ADC irá funcionar.
- Selecione um datastore com espaço suficiente e clique em **SEGUINTE**
- Em seguida, você será informado sobre o produto; clique em **SEGUINTE**
- Clique em **NEXT.**
- Uma vez que o senhor tenha copiado os arquivos para o datastore, poderá instalar o aparelho virtual.

Lance seu cliente vSphere para ver o novo aparelho virtual do ADC.

- Clique com o botão direito do mouse no VA e vá para Power-On > Power-On
- Seu VA iniciará então, e a tela de inicialização do ADC aparecerá no console.

Instalação da interface VMXNET3

O motorista da VMXnet3 é apoiado, mas o senhor terá que fazer primeiro mudanças nos ajustes do NIC.

***Nota** - NÃO atualize as ferramentas da VMware-tools*

Habilitação da interface VMXNET3 em um VA recém-importado (nunca iniciado)

1. Eliminar ambos os DNIs do VM
2. Atualize o hardware da VM - - Clique com o botão direito do mouse no VA da lista e selecione Upgrade Virtual Hardware (não inicie uma instalação ou atualização de ferramentas VMware, **apenas** faça o upgrade do hardware)
3. Acrescentar dois DNIs e selecioná-los para serem VMXNET3
4. Iniciar o VA usando o método padrão. Ele trabalhará com a VMXNET3.

Habilitação da interface VMXNET3 em um VA já em execução

1. Parar o VM (CLI shutdown command ou GUI power-off)
2. Obtenha os endereços MAC dos dois DNIs (lembre-se da ordem dos DNIs na lista!)
3. Eliminar ambos os DNIs do VM
4. Atualize o hardware da VM (não inicie a instalação ou atualização de ferramentas VMware, **apenas** faça a atualização do hardware)
5. Acrescentar dois DNIs e selecioná-los para serem VMXNET3
6. Fixar os endereços MAC para os novos DNIs de acordo com o passo 2
7. Reiniciar a VA

Nós apoiamos a VMware ESXi como plataforma de produção. Para fins de avaliação, o senhor pode usar a estação de trabalho e o Player VMware.

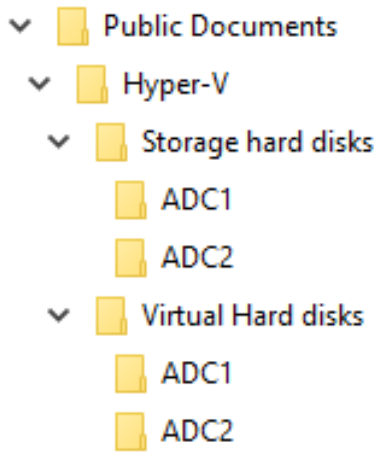
Queira consultar a seção **PRIMEIRA CONFIGURAÇÃO DA PRIMEIRA BOTA** para proceder mais adiante.

Microsoft Hyper-V

O aparelho virtual Edgenexus ADC pode ser facilmente instalado dentro de uma estrutura de virtualização do Microsoft Hyper-V. Este guia supõe que o senhor especificou e configurou corretamente seu sistema Hyper-V e recursos do sistema para acomodar o ADC e sua arquitetura de balanceamento de carga.

Note que cada aparelho requer um endereço MAC único.

- Extraia o arquivo ADC-VA compatível com Hyper-V baixado para sua máquina ou servidor local.
- Abra o gerente do Hyper-V.
- Criar uma nova pasta para conter o ADC VA "Disco rígido virtual" e outra nova pasta para conter o "Disco rígido de armazenamento", por exemplo, C:UUSADORES Público-Documentos Hyper-VVirtual discos rígidosADC1 e C:USADORES Público-Documentos Hyper-V Armazenamento de discos rígidosADC1
- **Nota**: Novas subpastas específicas do ADC para os discos rígidos virtuais e discos rígidos de armazenamento precisam ser criados para cada instalação de instância virtual do ADC, como se vê abaixo:



- Copie o arquivo .vhd extraído do EdgeADC para a pasta "Storage hard disk", criada acima.
- Em seu cliente Hyper-V Manager, clique com o botão direito do mouse sobre o servidor e selecione "Importar Máquina Virtual".
- Navegue até a pasta que contém o arquivo de imagem ADC VA, extraído anteriormente
- Selecione Máquina Virtual - destaque a máquina virtual a importar e clique em Next
- Selecione Máquina Virtual - destaque a máquina virtual a importar e clique em Next
- Escolha Import Type - selecione "**Copy the virtual machine (create a new unique ID)"** clique em next
- Escolha pastas para arquivos de máquinas virtuais - o destino pode ser deixado como o padrão Hyper-V ou você pode escolher um local diferente
- Localizar discos rígidos virtuais - navegue e selecione a pasta de discos rígidos virtuais criada acima e clique em next
- Escolha Folders to Store Virtual Hard Disks - navegue até e selecione a pasta Storage hard disks criada anteriormente e clique em next
- Verifique se os detalhes na janela Resumo do Assistente de Importação Completa estão corretos e clique em Finish
- Clique com o botão direito do mouse na máquina virtual **ADC** recém importada e selecione Start

NOTA: DE ACORDO COM HTTP://SUPPORT.MICROSOFT.COM/KB/2956569 O SENHOR DEVE IGNORAR A MENSAGEM DE STATUS "DEGRADED (DEGRADED (INTEGRATION SERVICES UPGRADE REQUIRED)", QUE PODE SER EXIBIDA COMO ABAIXO APÓS O VA SER INICIADO. NENHUMA AÇÃO É NECESSÁRIA, E O SERVIÇO NÃO ESTÁ DEGRADADO.

- Enquanto a VM está se inicializando, o senhor pode clicar com o botão direito do mouse na entrada da VM e selecionar Connect... Será então apresentado ao senhor o console do EdgeADC.

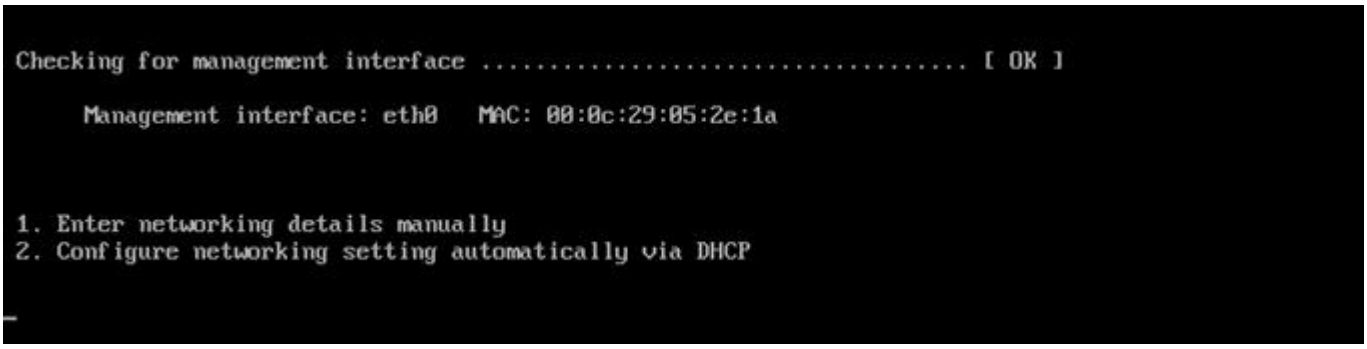
- Uma vez que o senhor configure as propriedades da rede, a VA reiniciará e apresentará o logon ao console da VA.

Queira consultar a seção **PRIMEIRA CONFIGURAÇÃO DA PRIMEIRA BOTA** para proceder mais adiante.

Citrix XenServer

O aparelho virtual do ADC é instalável no Citrix XenServer.

- Extraia o arquivo da ADC OVA ALB-VA para sua máquina ou servidor local.
- Cliente Open Citrix XenCenter.
- Em seu cliente XenCenter, selecione **"Arquivo: Importação".**
- Navegue até, e selecione o arquivo **OVA**, depois clique em **"Open Next" (Abrir próximo).**
- Selecione o local de criação da VM, quando solicitado.
- Escolha qual XenServer deseja instalar e clique em **"NEXT".**
- Selecionar o repositório de armazenamento (SR) para colocação de disco virtual quando solicitado.
- Selecione um RS com espaço suficiente e clique em **"SEGUINTE".**
- Faça o mapa das interfaces de sua rede virtual. Ambas as interfaces dirão Eth0; note, porém, que a interface inferior é Eth1.
- Selecione a rede alvo para cada interface e clique em **SEGUINTE**
- **NÃO** assinale o "Uso do sistema operacional".
- Clique em **"PRÓXIMO".**
- Escolha a interface da rede a ser usada para a transferência temporária do VM.
- Escolha a interface da Administração, geralmente a Rede 0, e deixe as configurações da rede no DHCP. O senhor deve estar ciente de que deve atribuir detalhes de endereço IP estático se não tiver um servidor DHCP funcionando para a transferência. Se isso não for feito, o ditado de importação "Conectar continuamente" falhará. Clique em **"NEXT".**
- Revise todas as informações e verifique os ajustes corretos então. Clique em **"FINISH".**
- Seu VM começará a transferir o disco virtual "ADC ADC" e, uma vez concluído, aparecerá sob seu XenServer.
- Dentro de seu cliente XenCenter, o senhor poderá agora ver a nova máquina virtual.
  Clique com o botão direito do mouse sobre a VA e clique em "**START**".
- Seu MV iniciará então, e a tela de inicialização do ADC aparecerá.



- Uma vez configurado, o diário de bordo da VA se apresenta.

Queira consultar a seção **PRIMEIRA CONFIGURAÇÃO DA PRIMEIRA BOTA** para proceder mais adiante.

Primeira configuração da bota

Na primeira inicialização, o ADC VA exibe a seguinte tela solicitando configuração para as operações de produção.

```
Checking for management interface ..................................... [ OK ]

     Management interface: eth0   MAC: 00:0c:29:05:2e:1a


1. Enter networking details manually
2. Configure networking setting automatically via DHCP

_
```

Primeira Bota - Detalhes da Rede Manual

Na primeira inicialização, o senhor terá 10 segundos para interromper a atribuição automática de detalhes de PI via DHCP

Para interromper esse processo, clique na janela do console e pressione qualquer tecla. O senhor poderá então introduzir manualmente os seguintes dados.

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

Essas mudanças são persistentes e sobreviverão a uma reinicialização e não precisam ser configuradas novamente na VA.

Primeira Bota - DHCP bem-sucedido

Se o senhor não interromper o processo de atribuição da rede, seu ADC entrará em contato com um servidor DHCP após um intervalo de tempo para obter os detalhes de sua rede. Se o contato for bem sucedido, então sua máquina receberá as seguintes informações.

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

Aconselhamos o senhor a não operar o ADC VA usando um endereço DHCP, a menos que esse endereço IP se ligue permanentemente ao endereço MAC do VA dentro do servidor DHCP. Sempre aconselhamos o uso de um **endereço IP FIXADO** ao usar o VA. Seguir as etapas de **MODIFICAÇÃO DO ENDEREÇO IP DA ADMINISTRAÇÃO** e seções subseqüentes até que o senhor tenha completado a configuração da rede.

Primeira Bota - DHCP Falhas

Se o senhor não tiver um servidor DHCP ou a conexão falhar, o endereço IP 192.168.100.100 será atribuído.
O endereço IP será incrementado por "1" até que o VA encontre um endereço IP livre. Da mesma forma, o VA verificará se o endereço IP está em uso no momento e, em caso afirmativo, aumentará novamente e voltará a verificar.

Mudança do endereço IP da Administração

O senhor pode mudar o endereço IP da VA a qualquer momento usando o **conjunto de** comandos **greenside=n.n.n.n,** como mostra a seguir.

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

Mudança da Máscara de sub-rede para eth0

As interfaces de rede usam o prefixo "eth"; o endereço da rede de base é chamado eth0. A máscara de sub-rede ou máscara de rede pode ser mudada usando o **conjunto de** comandos **eth0 n.n.n.n.** O senhor pode ver um exemplo abaixo.

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

Atribuição de um Portal de Inadimplência

A VA precisa de uma porta de entrada padrão para suas operações. Para definir a porta de entrada padrão, use a **rota de** comando **add default gw n.n.n.n,** como mostra o exemplo abaixo.

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

Verificação do valor do Default Gateway

Para verificar se a porta de entrada padrão foi acrescentada e se está correta, use a **rota de** comando. Esse comando mostrará as rotas da rede e o valor padrão da porta de entrada. 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
```

O senhor pode agora acessar a Interface Gráfica do Usuário (GUI) para configurar o ADC para uso na produção ou avaliação.

Acesso à interface web

O senhor pode usar qualquer navegador da Internet com Javascript para configurar, monitorar e implantar o ADC para uso operacional.

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

O ADC, por padrão, usa um certificado SSL autoassinado. O senhor pode mudar o ADC para usar o certificado SSL de sua própria escolha.

Quando seu navegador chegar ao ADC, ele lhe mostrará a tela de login. As credenciais padrão de fábrica para o ADC são:

Nome de usuário por defeito = **admin** / Senha por defeito = **jetnexus**

Tabela de Referência do Comando

Comando	Parâmetro1	Parâmetro2	Descrição	Exemplo
data			Mostra a data e a hora configuradas atualmente	Ter 3 de setembro 13:00 UTC 2013
inadimplementos			Atribuir as configurações padrão de fábrica para seu aparelho	
saída			Sair da interface da linha de comando	
ajuda			Exibe todos os comandos válidos	
ifconfig	[em branco]		Ver a configuração da interface para todas as interfaces	ifconfig
	eth0		Veja apenas a configuração da interface de eth0	ifconfig eth0
machineid			Este comando fornecerá a máquina usada para licenciar o ADC ADC	EF4-3A35-F79
desistir			Sair da interface da linha de comando	
reinicialização			Encerrar todas as conexões e reiniciar o ADC ADC	reinicialização
reinício			Reiniciar os serviços virtuais do ADC ADC	
rota	[em branco]		Ver a tabela de roteamento	rota
	acrescentar	padrão gw	Acrescentar o endereço IP padrão do gateway	rota adicionar gw default 192.168.100.254
conjunto	verde		Estabelecer o endereço IP da administração para a ADC	set greenside=192.168.101.1
	máscara		Coloque a máscara de sub-rede para uma interface. Os nomes das interfaces são eth0, eth1....	definir máscara eth0 255.255.255.255.0
show			Mostra os ajustes de configuração global	
desligamento			Encerrar todas as conexões e desligar o ADC ADC	
status			Mostra os dados estatísticos atuais	
topo			Veja as informações do processo, como CPU e Memória	

viewlog	mensagens	Exibe as mensagens cruas do syslog	Ver mensagens de log

Queira notar: os comandos não são sensíveis a maiúsculas e minúsculas. Não há histórico de comando.

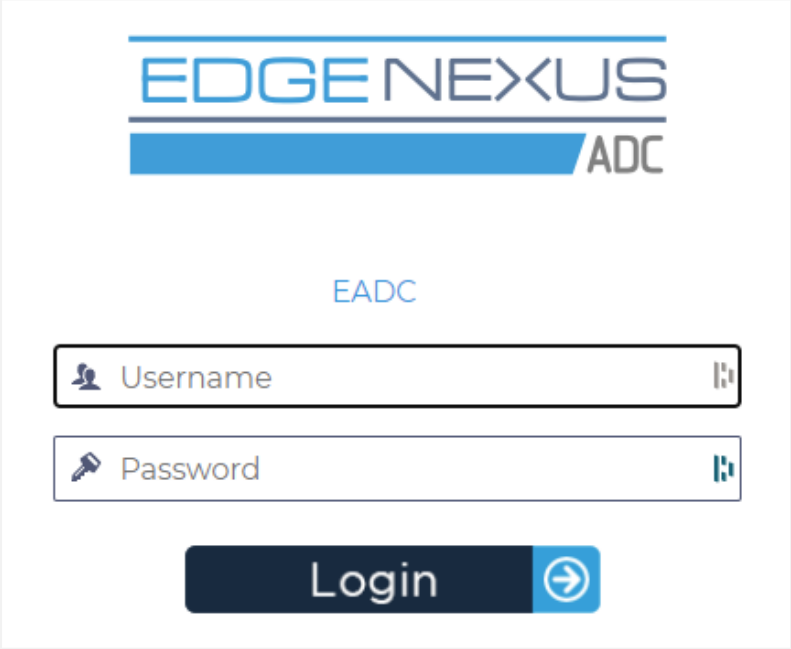
Lançamento do ADC Web Console

Todas as operações no ADC (também referido como ADC) são configuradas e realizadas usando o console da web. O console da web é acessado usando qualquer navegador com Javascript.

Para lançar o console da ADC na Internet, digite o URL ou endereço IP da ADC no campo URL. Vamos usar o exemplo da adc.company.com como exemplo:

https://adc.company.com

Quando lançado, o console da ADC é como mostrado abaixo, permitindo que o senhor faça o login como usuário administrativo.



Credenciais de Login Padrão

As credenciais de login padrão são:

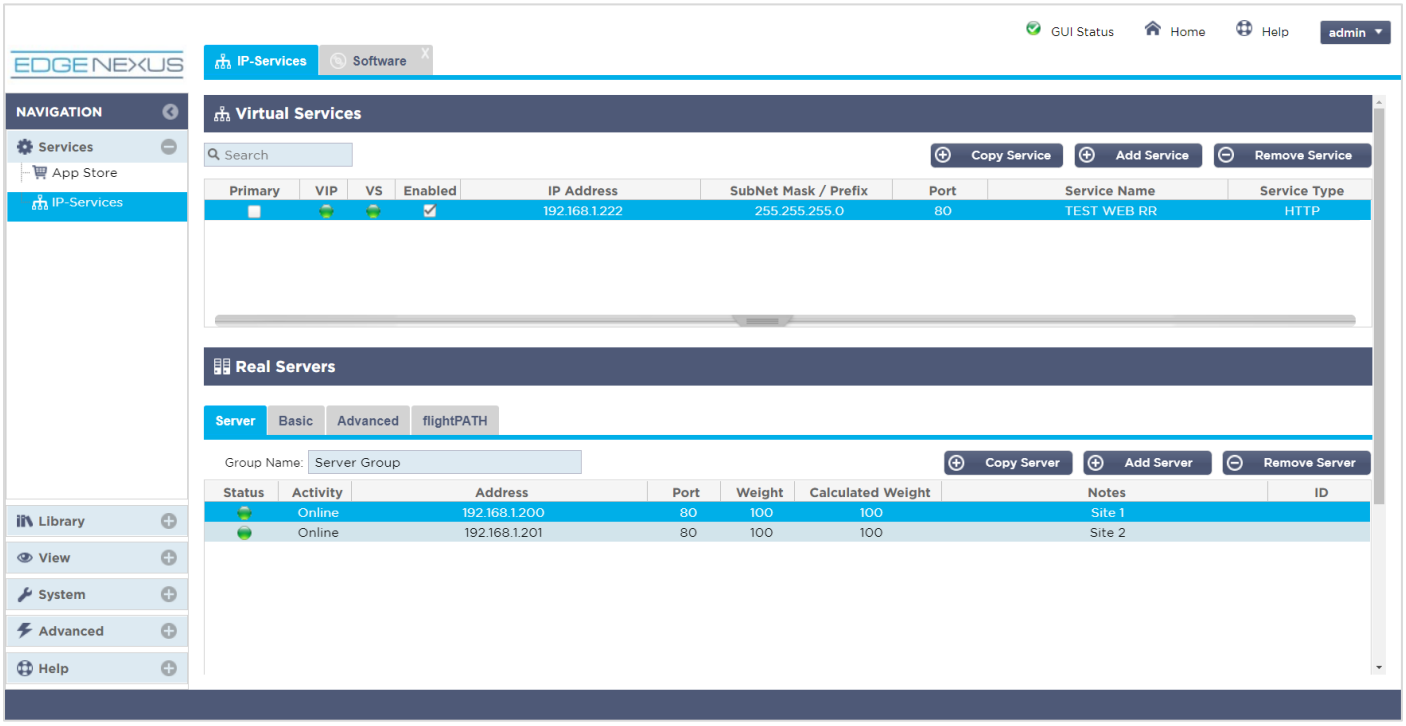
- Nome de usuário: admin
- Senha: jetnexus

O senhor pode mudar isso a qualquer momento usando as capacidades de configuração do usuário localizadas em *Sistema* > *Usuários.*

Uma vez que o senhor tenha feito o log in com sucesso, o painel principal do ADC será exibido.

O Painel Principal

A imagem abaixo ilustra o aspecto do painel principal ou "home page" do ADC. Podemos fazer algumas mudanças de tempos em tempos devido a razões de melhoria, mas todas as funções permanecerão.



Para ser o mais conciso possível, assumiremos que essa primeira introdução às seções da tela se mostrará suficientemente consciente das diferentes seções da área de configuração do ADC, de modo que não as descreveremos em detalhes à medida que avançarmos, mas sim nos concentraremos nos elementos de configuração.

Indo da esquerda para a direita, temos primeiro a Navegação. A seção de Navegação consiste nas diferentes áreas dentro da ADC. Quando o senhor clicar em uma determinada escolha dentro da Navegação, isso mostrará a seção correspondente no lado direito da tela. O senhor também pode ver a seção de configuração escolhida na parte superior da tela, adjacente ao logotipo do produto. As abas permitem uma navegação mais rápida para as áreas pré-utilizadas da configuração do ADC.

Serviços

A seção de serviços da ADC tem várias áreas dentro dela. Quando o senhor clicar no item "Serviços", isso se expandirá para mostrar as opções disponíveis.

Serviços de PI

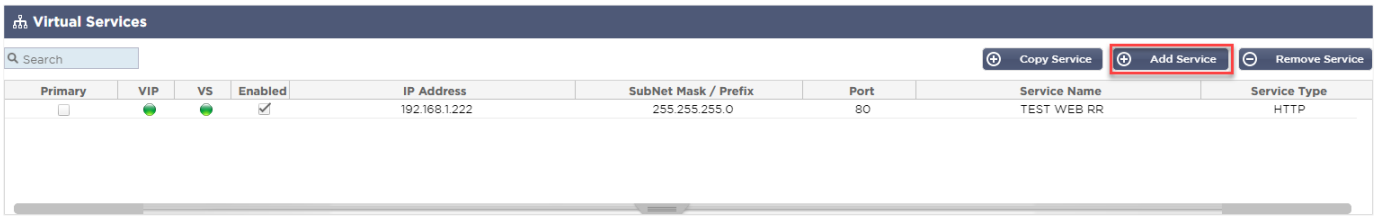
A seção de Serviços de PI do ADC permite ao senhor acrescentar, apagar e configurar os vários serviços de PI virtuais de que necessita para seu caso particular de uso. As configurações e opções se enquadram nas seções abaixo. Essas seções estão no lado direito da tela do pedido.

Serviços virtuais

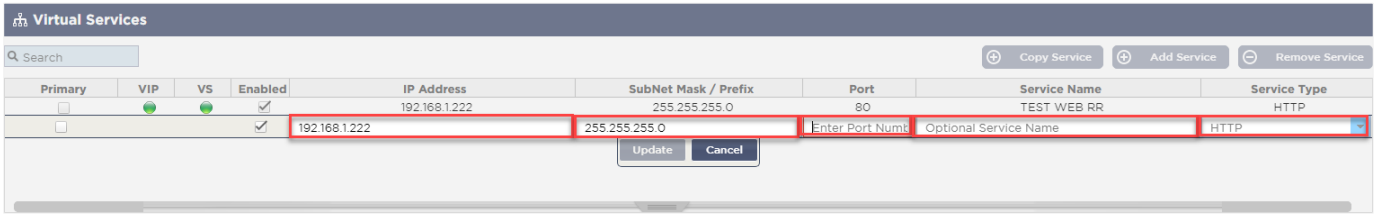
Um Serviço Virtual combina um IP Virtual (VIP) e um porto TCP/UDP no qual o ADC ouve. O tráfego que chega ao IP do Serviço Virtual é redirecionado para um dos Servidores Reais associados a esse serviço. O endereço IP do Serviço Virtual não pode ser o mesmo que o endereço administrativo do ADC, ou seja, eth0, eth1 etc...

O ADC determina como o tráfego é redistribuído aos Servidores com base em uma política de equilíbrio de carga estabelecida dentro da guia Básica na seção Servidores Reais.

Criação de um novo Serviço Virtual usando um novo VIP



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

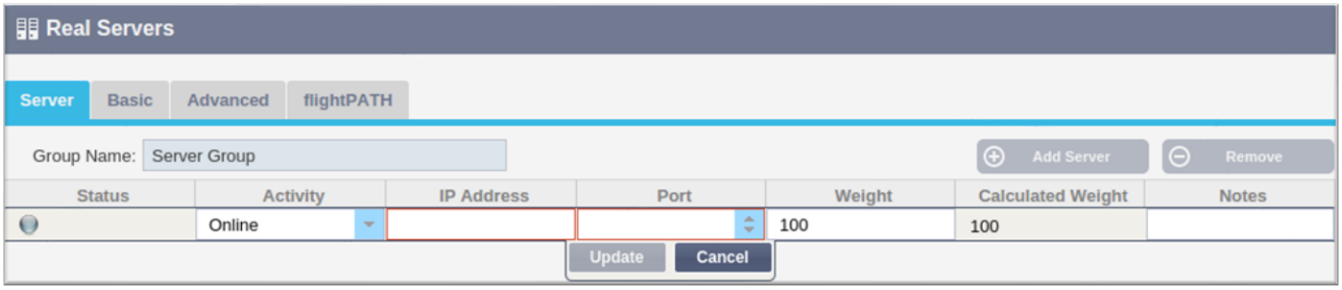


- O senhor entrará então no modo de **edição em linha.**
- Complete os quatro campos destacados para prosseguir, e depois clique no botão de atualização.

Queira usar a chave TAB para navegar através dos campos.

Campo	Descrição
Endereço IP	Digite um novo endereço IP Virtual para ser o ponto de entrada alvo para acessar o Servidor Real. Esse IP é onde os usuários ou aplicações vão apontar para acessar a aplicação balanceada de carga.
Subrede Máscara/Prefixo	Este campo é para a máscara de sub-rede relevante para a rede na qual o ADC está localizado.
Porto	O porto de entrada utilizado para o acesso ao VIP. Esse valor não precisa necessariamente ser o mesmo que o Real Server se o senhor usar o Reverse Proxy.
Nome do serviço	O nome do serviço é uma representação textual do propósito do VIP. É opcional, mas recomendamos que o senhor o esclareça.
Tipo de serviço	Há muitos tipos diferentes de serviços disponíveis para que o senhor possa selecionar. Os tipos de serviço de camada 4 não podem usar a tecnologia flightPATH.

O senhor pode agora pressionar o botão Atualizar para salvar esta seção e saltar automaticamente para a seção Servidor Real detalhada abaixo:

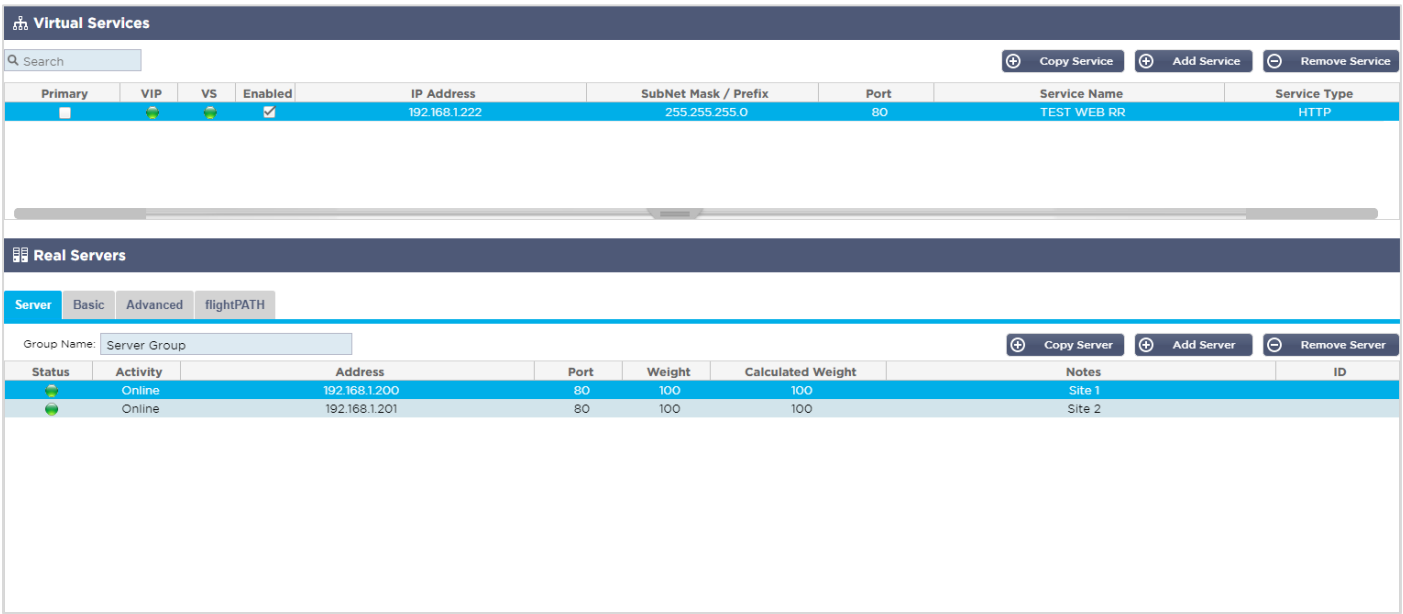


Campo	Descrição
Atividade	O campo de atividade pode ser usado para mostrar e mudar o status do servidor real balanceado de carga. Online - Denota que o servidor está ativo e recebendo pedidos de balanceamento de carga Offline - O servidor está offline e não está recebendo pedidos Drenagem - O servidor foi colocado em modo de drenagem, de modo que a persistência pode ser nivelada e o servidor passou para um estado off-line sem afetar os usuários. Standby - O servidor foi colocado em estado de espera
Endereço IP	Esse valor é o endereço IP do Real Server. Ele deve ser preciso e não deve ser um endereço DHCP.
Porto	O porto alvo de acesso no Real Server. Quando se usa um proxy reverso, isso pode ser diferente do porto de entrada especificado no VIP.
Ponderação	Essa configuração geralmente é configurada automaticamente pela ADC. O senhor pode mudar isso se desejar alterar a ponderação de prioridade.

- Clique no botão Update ou pressione Enter para salvar suas mudanças
- A luz de status primeiro ficará cinza, seguida de verde, caso o exame de saúde do servidor seja bem sucedido. Ele ficará vermelho se o Monitor do Servidor Real falhar.

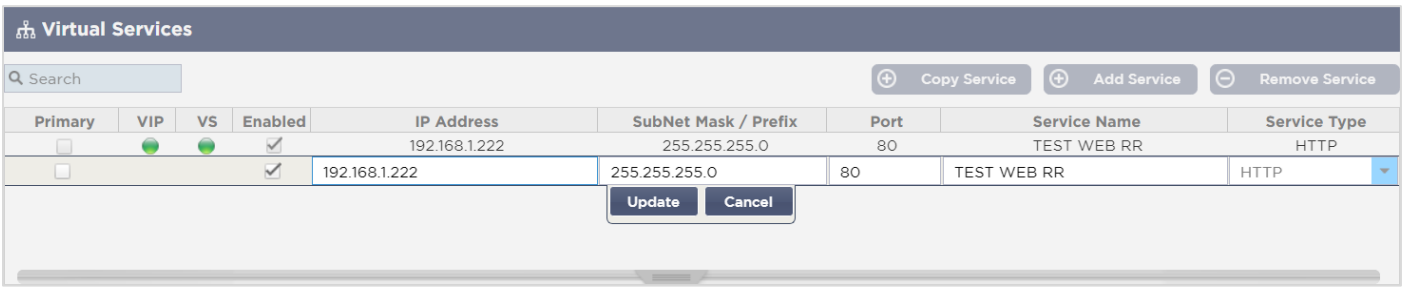
- Um servidor que tenha uma luz vermelha de status não será equilibrado na carga.

Exemplo de um serviço virtual completo

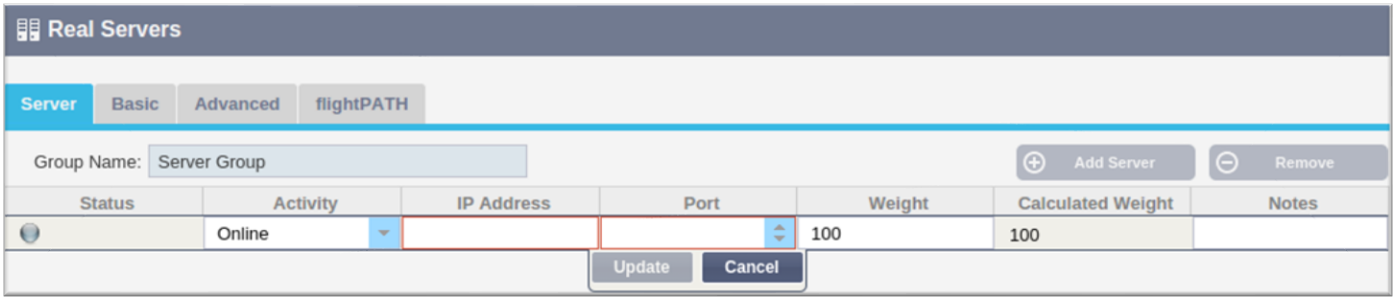


Criar um novo Serviço Virtual usando um VIP existente

- Destacar um serviço virtual que o senhor deseja copiar
- Clique em Add Virtual Service para entrar no modo de edição de linha



- O endereço IP e a Máscara de sub-rede são automaticamente transmitidos
- Digite o número do porto para seu serviço
- Digite um nome de serviço opcional
- Selecione um tipo de serviço
- Você pode agora pressionar o botão Atualizar para salvar esta seção e pular automaticamente para a seção Servidor Real abaixo



- Deixe a opção de atividade do servidor como Online - isso significa que a carga será balanceada se ela passar pelo monitor de saúde padrão do TCP Connect. Essa configuração pode ser alterada mais tarde, se necessário.

- Digite um endereço IP do Real Server
- Digite um número de porta para o Real Server
- Digite um nome opcional para o Servidor Real
- Clique em Update para salvar suas mudanças
- A luz de status primeiro ficará cinza, depois verde se o exame de saúde do servidor for bem sucedido. Se o Monitor do Servidor Real falhar, ele ficará vermelho.
- Um servidor que tenha uma luz vermelha de status não será equilibrado na carga.

Mudança do endereço IP de um serviço virtual

O senhor pode mudar o endereço IP de um Serviço Virtual ou VIP existente a qualquer momento.

- Destacar o Serviço Virtual cujo endereço IP o senhor deseja alterar

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
			✓	192.168.1.248	255.255.255.0	80	VIP1	HTTP
			✓	192.168.1.251	255.255.255.0	80	VS2	HTTP
			✓	192.168.1.253	255.255.255.0	80	VIP2	HTTP

- Clique duas vezes no campo de endereço IP para esse serviço

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
			✓	192.168.1.248	255.255.255.0	80	VIP1	HTTP
			✓	192.168.1.251	255.255.255.0	80	VS2	HTTP
			✓	192.168.1.254	255.255.255.0	80	VIP2	HTTP

Update Cancel

- Mudar o endereço IP para aquele que o senhor deseja usar
- Clique no botão Atualizar para salvar as mudanças.

Primary	VIP Status	Service Status	Enabled	IP Address	SubNet Mask	Port	Service Name	Service Type
			✓	192.168.1.248	255.255.255.0	80	VIP1	HTTP
			✓	192.168.1.251	255.255.255.0	80	VS2	HTTP
			✓	192.168.1.254	255.255.255.0	80	VIP2	HTTP

Nota: A mudança do endereço IP de um Serviço Virtual mudará o endereço IP de todos os serviços associados com o VIP.

Criação de um novo Serviço Virtual usando o Serviço de Cópia

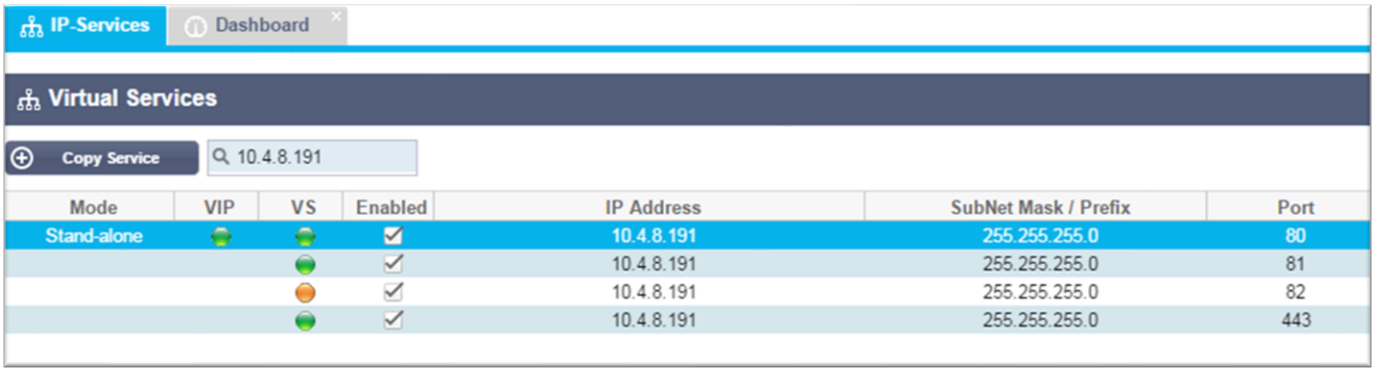
- O botão Copy Service copiará um serviço completo, incluindo todos os Servidores Reais, configurações básicas, configurações avançadas e regras de flightPATH associadas a ele
- Destacar o serviço que deseja duplicar e clicar em Copy Service
- O editor de linha aparecerá com o cursor piscando na coluna Endereço IP
- O usuário deve mudar o endereço IP para ser único, ou se desejar manter o endereço IP, deve editar o Porto para que seja único para esse endereço IP

Não se esqueça de editar cada guia se o senhor mudar uma configuração como uma política de equilíbrio de carga, o monitor do Servidor Real, ou remover uma regra do FlightPATH.

Filtragem dos dados exibidos

Procura de um termo específico

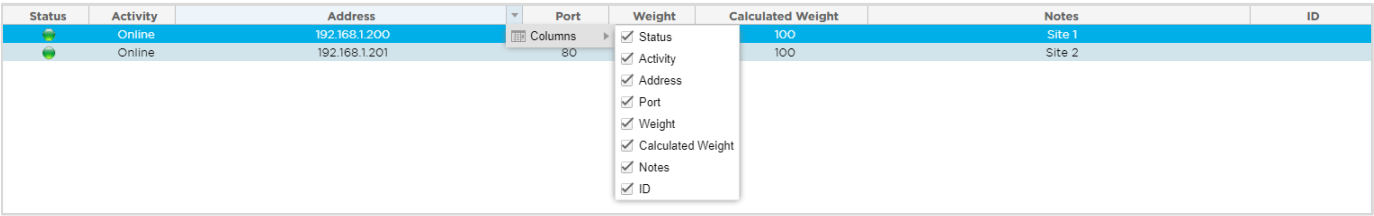
A caixa de busca permite ao senhor pesquisar a tabela usando qualquer valor, como os octetos do endereço IP ou o nome do serviço.



O exemplo acima mostra o resultado da busca de um endereço IP específico de 10.4.8.191.

Seleção da visibilidade da coluna

O senhor também pode selecionar as colunas que deseja exibir no painel de instrumentos.

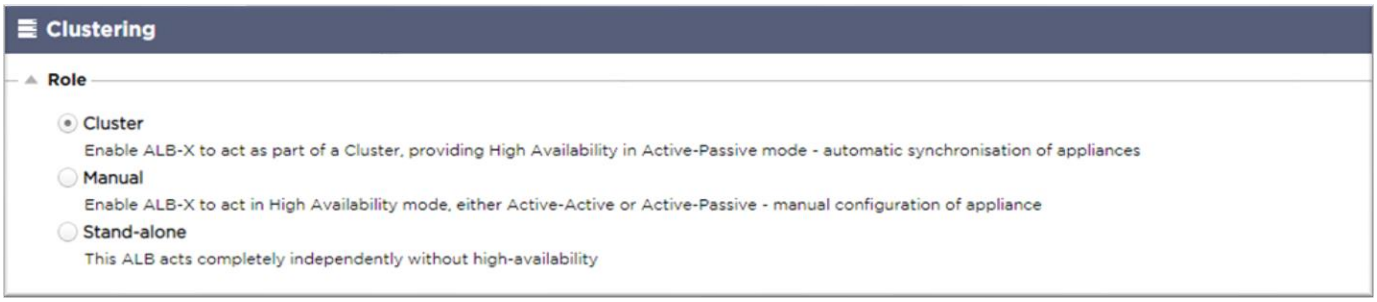


- Mova o mouse sobre qualquer uma das colunas
- O senhor verá uma pequena seta aparecer no lado direito da coluna
- Clicando nas caixas de seleção, o senhor seleciona as colunas que deseja ver no painel de instrumentos.

Compreensão das colunas de Serviços Virtuais

Primário/Modo

A coluna Principal/Modo indica o papel de alta disponibilidade selecionado para o atual VIP. Use as opções disponíveis em Sistema > Clustering para configurar essa opção.



Opção	Descrição
Cluster	Cluster é o papel padrão do ADC na instalação, e a coluna Principal/Modo indicará o modo em que ele está funcionando atualmente. Quando o senhor tiver um par de aparelhos do ADC em seu centro de dados, um deles mostrará Ativo e o outro Passivo.
Manual	O papel do Manual permite que o par ADC funcione em modo Ativo-Ativo para diferentes endereços IP virtuais. Nesses casos, a coluna primária conterá uma caixa ao lado de cada IP Virtual único que pode ser marcado para Ativo ou deixado sem marcar para Passivo.

Stand-Alone	O ADC está agindo como um dispositivo autônomo e não está no modo de Alta Disponibilidade. Como tal, a coluna Primária indicará autônoma.

VIP

Esta coluna fornece feedback visual sobre a situação de cada Serviço Virtual. Os indicadores são codificados por cores e são os seguintes:

LED	Significado
●	Online
●	Failover-Standby. Este serviço virtual é hot-standby
●	Indica que um "secundário" está se atrasando para um "primário".
●	O serviço precisa de atenção. Essa indicação pode resultar de um servidor real falhar em um exame de monitoramento de saúde ou ter sido mudado manualmente para Offline. O tráfego continuará a fluir, mas com capacidade reduzida do Real Server
●	Fora de linha. Os servidores de conteúdo são inacessíveis, ou não há servidores de conteúdo habilitados.
●	Situação de busca
●	Não licenciados ou licenciados IPs Virtuais excedidos

Habilitado

O padrão para essa opção é Habilitado, e a caixa de seleção mostra como assinalado. O senhor pode desativar o Serviço Virtual clicando duas vezes na linha, desmarcando a caixa de seleção, e depois clicando no botão Atualizar.

Endereço IP

Adicione seu endereço IPv4 em notação decimal pontilhada ou um endereço IPv6. Esse valor é o endereço IP Virtual (VIP) para seu serviço. Exemplo IPv4 "192.168.1.100". Exemplo Ipv6 "2001:0db8:85a3:0000:0000:8a2e:0370:7334".

Subrede Máscara/Prefixo

Acrescente sua máscara de sub-rede em notação decimal pontilhada. Exemplo "255.255.255.0". Ou para IPv6, acrescente em seu prefixo. Para mais informações sobre IPv6, veja **HTTPS://EN.WIKIPEDIA.ORG/WIKI/IPV6_ADDRESS.**

Porto

Acrescente o número do porto associado ao seu serviço. O porto pode ser um número de porto TCP ou UDP. Exemplo TCP "80" para Web Traffic e TCP "443" para Secured Web Traffic.

Nome do serviço

Acrescente um nome amigável para identificar seu serviço. Exemplo: "Web Servers de produção".

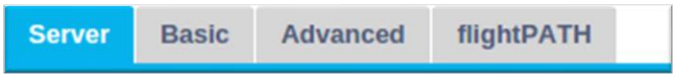
Tipo de serviço

Observe que com todos os tipos de serviço de "Camada 4", o ADC não interagirá ou modificará o fluxo de dados, de modo que o flightPATH não está disponível com os tipos de serviço de Camada 4. Os serviços de Camada 4 simplesmente balanceiam o tráfego de acordo com a política de balanceamento de carga:

Tipo de serviço	Porto/Protocolo	Camada de serviço	Comentário
Camada 4 TCP	Qualquer porto TCP	Camada 4	O ADC não alterará nenhuma informação no fluxo de dados e realizará o balanceamento de carga padrão do tráfego de acordo com a política de balanceamento de carga
Camada 4 UDP	Qualquer porto UDP	Camada 4	Assim como no Layer 4 TCP, o ADC não alterará nenhuma informação no fluxo de dados e realizará o balanceamento de carga padrão do tráfego de acordo com a política de balanceamento de carga
Camada 4 TCP/UDP	Qualquer porto TCP ou UDP	Camada 4	É ideal que seu serviço tenha um protocolo primário como o UDP, mas que volte ao TCP. O ADC não alterará nenhuma informação no fluxo de dados e realizará o balanceamento de carga padrão do tráfego de acordo com a política de balanceamento de carga.
DNS	!!!		
HTTP	Protocolo HTTP ou HTTPS	Camada 7	O ADC pode interagir, manipular e modificar o fluxo de dados usando o flightPATH.
FTP	Protocolo de transferência de arquivos	Camada 7	Usando controle separado e conexões de dados entre cliente e servidor
SMTP	Protocolo de transferência de correio simples	Camada 4	Uso ao equilibrar a carga dos servidores de correio
POP3	Protocolo dos Correios	Camada 4	Uso ao equilibrar a carga dos servidores de correio
IMAP	Protocolo de acesso a mensagens na Internet	Camada 4	Uso ao equilibrar a carga dos servidores de correio
RDP	Protocolo de Desktop Remoto	Camada 4	Uso no balanceamento de carga de servidores de Serviços Terminais
RPC	Chamada de procedimento remoto	Camada 4	Uso quando sistemas de balanceamento de carga usando chamadas RPC
RPC/ADS	Troca 2010 Static RPC para serviço de catálogo de endereços	Camada 4	Uso no balanceamento de carga Servidores de câmbio
RPC/CA/PF	Troca 2010 Static RPC para Acesso do Cliente e Pastas Públicas	Camada 4	Uso no balanceamento de carga Servidores de câmbio
DICOM	Imagens e Comunicações Digitais em Medicina	Camada 4	Uso quando servidores de balanceamento de carga usando protocolos DICOM

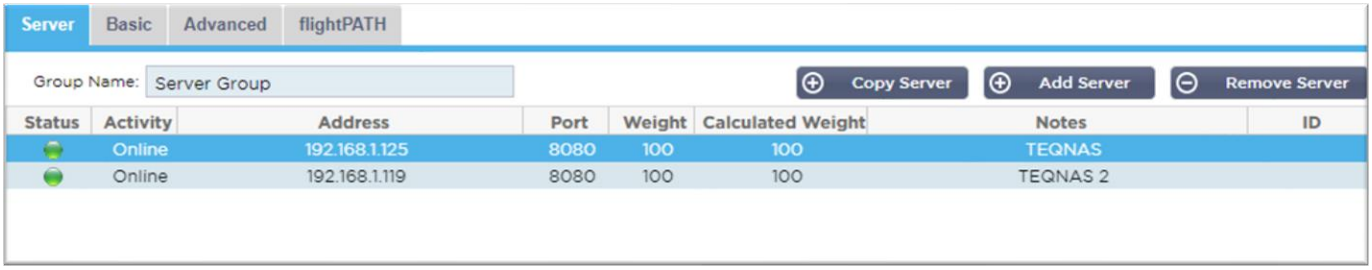
Servidores reais

Há vários separadores na seção dos Servidores Reais do painel de instrumentos: Server, Basic, Advanced, e flightPATH.



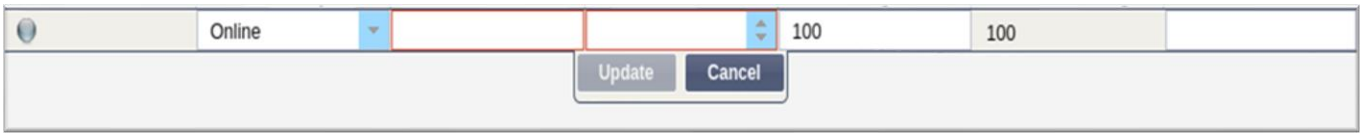
Servidor

A aba Servidor contém as definições dos verdadeiros servidores back-end emparelhados com o Serviço Virtual atualmente selecionado. O senhor é obrigado a acrescentar pelo menos um servidor à seção "Servidores Reais".



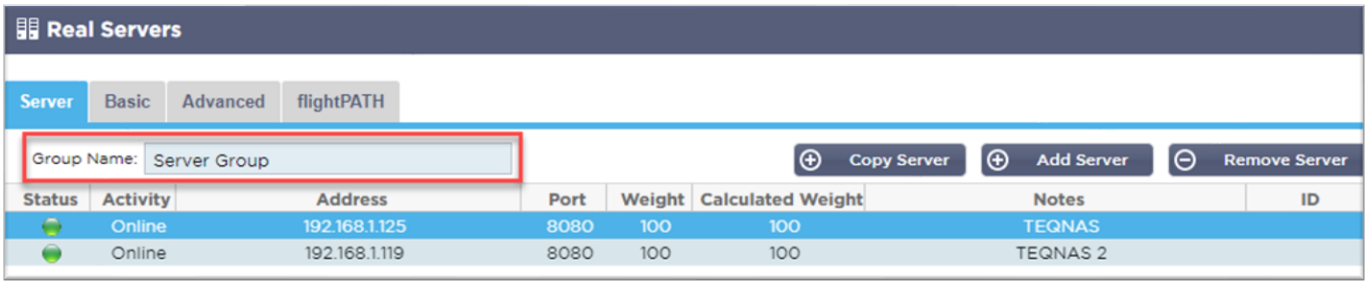
Adicionar servidor

- Selecione o VIP apropriado que o senhor definiu anteriormente.
- Clique em Add Server
- Uma nova linha aparecerá com o cursor piscando na coluna Endereço IP



- Digite o endereço IPv4 de seu servidor em notação decimal pontilhada. O servidor real pode estar na mesma rede do seu serviço virtual, em qualquer rede local anexada diretamente, ou em qualquer rede que seu ADC possa encaminhar. Exemplo "10.1.1.1.1".
- Tab na coluna Porto e digite o número do porto TCP/UDP do seu servidor. O número da porta pode ser o mesmo que o número da porta do Serviço Virtual ou outro número da porta para Conectividade de Proxy Reversa. O ADC traduzirá automaticamente para esse número.
- Tab à seção de Notas para acrescentar qualquer detalhe relevante para o servidor. Exemplo: "IIS Web Server 1".

Nome do grupo



Quando o senhor tiver acrescentado nos servidores que compõem o conjunto equilibrado de carga, poderá também anexar-lhes um Nome de Grupo. Uma vez que o senhor tenha editado esse campo, o conteúdo será salvo sem a necessidade de pressionar o botão Atualizar.

Luzes de status de servidor real

O senhor pode ver o status de um Servidor Real pela cor clara na coluna Status. Veja abaixo:

LED	Significado
●	Conectado
○	Não monitorado
●	Drenagem
●	Offline
●	Espera
●	Não Ligado
●	Situação de busca
●	Não licenciados ou licenciados Servidores Reais excederam

Atividade

O senhor pode mudar a atividade de um servidor real a qualquer momento, usando o menu suspenso. Para fazer isso, clique duas vezes na fileira de um Servidor Real para colocá-lo no modo de edição.

Opção	Descrição
Online	Todos os Servidores Reais designados on-line receberão tráfego de acordo com a política de balanceamento de carga estabelecida dentro da guia Básica.
Dreno	Todos os Servidores Reais designados como Drain continuarão a servir as conexões existentes, mas não aceitarão nenhuma nova conexão. A luz de status piscará verde/azul enquanto o dreno estiver em andamento. Uma vez que as conexões existentes tenham sido fechadas naturalmente, os Verdadeiros Servidores ficarão offline, e a luz de Status será azul sólido. O senhor também pode ver essas conexões navegando até a seção Navegação > Monitor > Status.
Offline	Todos os Servidores Reais definidos como Offline serão imediatamente desligados e não receberão nenhum tráfego.
Espera	Todos os Servidores Reais definidos como Standby permanecerão off-line até que **TODOS** os servidores do grupo Online falhem em suas verificações do Monitor de Saúde do

	Servidor. O tráfego é recebido pelo grupo "Standby" de acordo com a política de equilíbrio de carga quando isso acontece. Se um servidor do grupo Online passar na verificação do Monitor de Saúde do Servidor, esse servidor Online receberá todo o tráfego, e o grupo Standby deixará de receber tráfego.

Endereço IP

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

Porto

Número de porta TCP ou UDP que o Real Server está escutando para o serviço. Exemplo "80" para o tráfego da Web.

Peso

Essa coluna se tornará editável quando houver uma Política de Balanceamento de Carga apropriada especificada.

O peso padrão para um servidor real é 100, e o senhor pode digitar valores de 1-100. Um valor de 100 significa carga máxima, e 1 significa carga mínima.

Um exemplo para três servidores pode ser algo parecido com isto:

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

Se considerarmos que a política de balanceamento de carga está definida para Ligações Mínimas, e há um total de 200 ligações de clientes;

- O Servidor 1 receberá 100 conexões simultâneas
- O Servidor 2 terá 50 conexões simultâneas
- O Servidor 3 terá 50 conexões simultâneas

Se usarmos Round Robin como o método de balanceamento de carga, que gira os pedidos através do conjunto de servidores balanceados de carga, a alteração dos pesos afeta a freqüência com que os servidores são escolhidos como alvo.

Se acreditamos que a política de equilíbrio de carga mais rápida usa o menor tempo possível para obter uma resposta, o ajuste dos pesos altera o viés de maneira semelhante ao das Ligações Mínimas.

Peso calculado

O Peso calculado de cada servidor pode ser visualizado dinamicamente e é calculado automaticamente e não é editável. O campo mostra a ponderação real que o ADC está usando ao considerar a ponderação manual e a política de equilíbrio de carga.

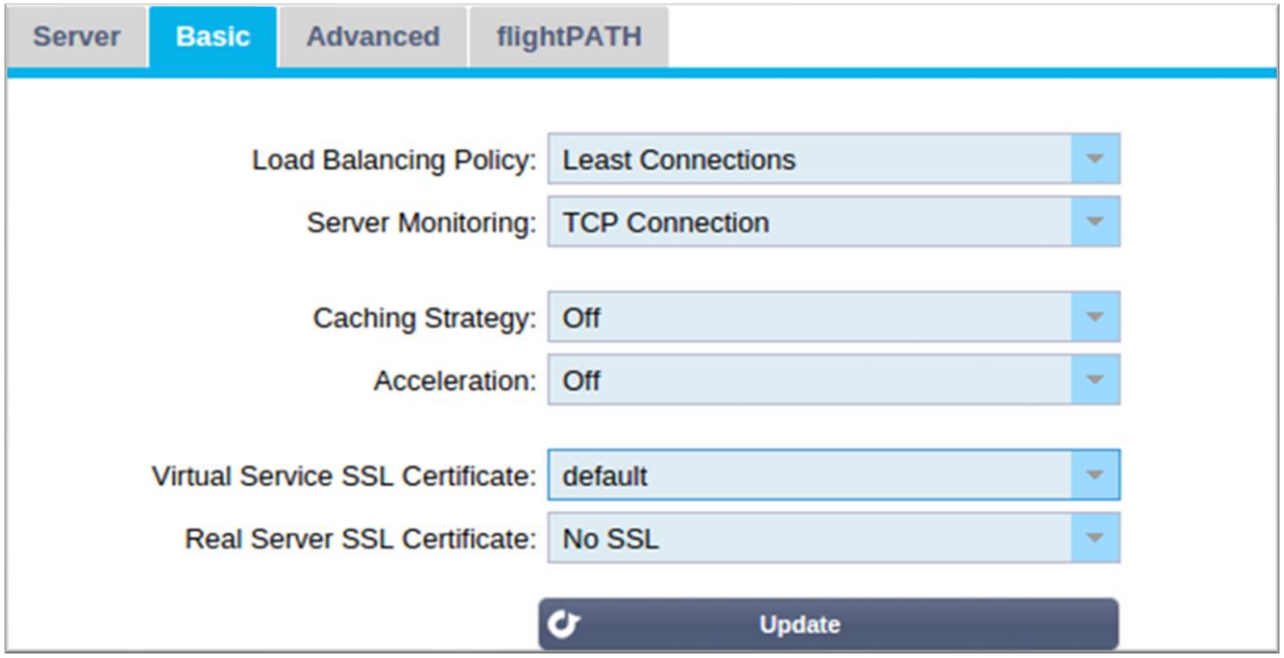
Notas

Digite quaisquer notas particulares úteis para descrever a entrada definida no campo Notas. Exemplo "IIS Server1 - London DC".

ID

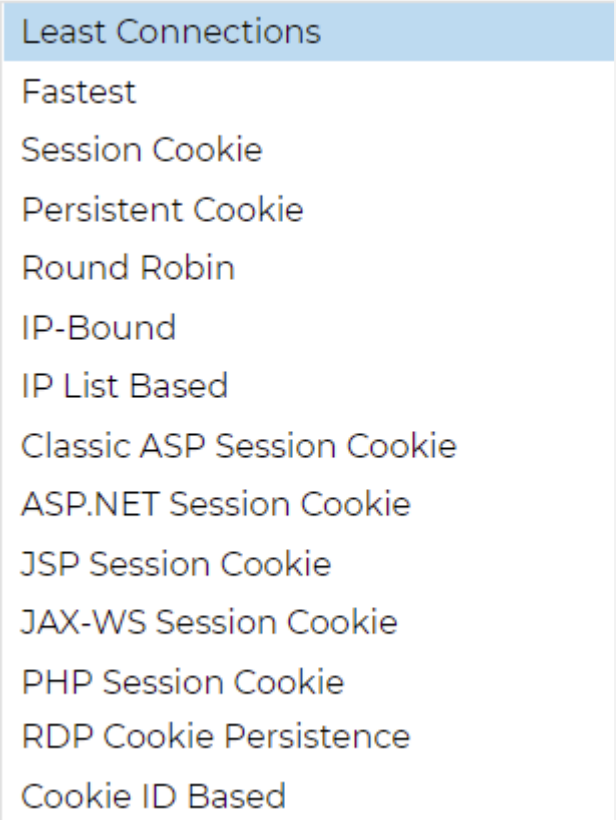
O campo ID é usado dentro da política de equilíbrio de carga do Cookie ID. O número de identificação aqui colocado é usado para identificar

Básico



Política de Balanceamento de Carga

A lista suspensa mostra ao senhor as políticas de equilíbrio de carga atualmente apoiadas e disponíveis para uso. Uma lista de políticas de balanceamento de carga, juntamente com uma explicação, está abaixo.



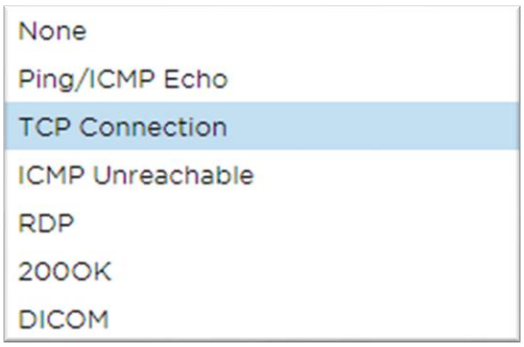
Opção	Descrição
O mais rápido	A política de equilíbrio de carga mais rápida calcula automaticamente o tempo de resposta para todos os pedidos por servidor suavizados ao

	longo do tempo. A coluna Peso Calculado contém o valor calculado automaticamente. A entrada manual só é possível quando se usa essa política de balanceamento de carga.
Round Robin	Round Robin é comumente usado em firewalls e equilibradores de carga básica e é o método mais simples. Cada Real Server recebe um novo pedido em seqüência. Esse método só é apropriado quando o senhor precisa carregar os pedidos de equilíbrio de carga para os servidores de maneira uniforme; um exemplo seria os servidores web look-up. No entanto, quando o senhor precisa carregar o saldo com base na carga de pedidos ou na carga do servidor, ou mesmo garantir que o senhor use o mesmo servidor para a sessão, o método Round Robin é inadequado.
Ligações Mínimas	O equilibrador de carga manterá um registro do número de conexões atuais com cada servidor real. O Servidor Real com o menor número de conexões recebe o novo pedido subseqüente.
Camada 3 Sessão Afinidade/Persistência - IP Limitada	Nesse modo, o endereço IP do cliente forma a base para selecionar qual Servidor Real receberá o pedido. Essa ação proporciona persistência. Os protocolos HTTP e Layer 4 podem usar esse modo. Esse método é útil para redes internas onde a topologia da rede é conhecida, e o senhor pode estar confiante de que não há "super proxies" a montante. Com o Layer 4 e os proxies, todos os pedidos podem parecer que vêm de um cliente, e como tal, a carga não seria uniforme. Com HTTP, a informação do cabeçalho (X-Forwarder-For) é usada quando presente para lidar com os procuradores.
Afinidade/Persistência de Camada 3 Sessões - Lista de PI	A conexão com o Real Server inicia-se então usando "Menos conexões", a afinidade da sessão é alcançada com base no endereço IP do cliente. Uma lista é mantida por 2 horas por padrão, mas isso pode ser mudado usando um jetPACK.
Camada 7 Afinidade/Persistência da Sessão - Cookie da Sessão	Esse modo é o método de persistência mais popular para o balanceamento de carga HTTP. Nesse modo, o ADC usa o balanceamento de carga baseado em lista de IP para cada primeira solicitação. Ele insere um cookie nos cabeçalhos da primeira resposta HTTP. Depois disso, o ADC usa o cookie do cliente para encaminhar o tráfego para o mesmo servidor back-end. Esse cookie é usado para persistência quando o cliente precisa ir ao mesmo servidor de back-end cada vez. O cookie expira uma vez que a sessão é encerrada.
Afinidade/Persistência de Camada 7 Sessão - Cookie Persistente	O modo de equilíbrio de carga baseado na lista de PI é usado para cada primeiro pedido. O ADC insere um cookie nos cabeçalhos da primeira resposta HTTP. Depois disso, o ADC usa o cookie do cliente para encaminhar o tráfego para o mesmo servidor back-end. Esse cookie é usado para persistência quando o cliente deve ir ao mesmo servidor de back-end cada vez. O cookie expirará após 2 horas, e a conexão será balanceada de acordo com um algoritmo baseado em uma lista de IP. Esse tempo de expiração é configurável usando um jetPACK.
Cookie de Sessão - Cookie de Sessão Clássico ASP	O Active Server Pages (ASP) é uma tecnologia do lado do servidor da Microsoft. Com essa opção selecionada, o ADC manterá a persistência da sessão no mesmo servidor se um cookie ASP for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie ASP, a carga será balanceada usando o algoritmo de Conexões Mínimas.
Cookie de Sessão - ASP.NET Cookie de Sessão	Esta modalidade se aplica ao **ASP.net.** Com essa modalidade selecionada, o ADC manterá a persistência da sessão no mesmo servidor se um cookie ASP.NET for detectado e encontrado em sua lista de

	cookies conhecidos. Na detecção de um novo cookie ASP, a carga será balanceada usando o algoritmo de Ligações Mínimas.
Cookie de Sessão - Cookie de Sessão JSP	Java Server Pages (JSP) é uma tecnologia do lado do servidor Oracle. Com esse modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie JSP for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie JSP, a carga será balanceada usando o algoritmo de Ligações Mínimas.
Cookie de Sessão - JAX-WS Cookie de Sessão	Java web services (JAX-WS) é uma tecnologia do lado do servidor Oracle. Com esse modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie JAX-WS for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie JAX-WS, ele será carregado em equilíbrio usando o algoritmo de Conexões Mínimas.
Cookie de Sessão - Cookie de Sessão PHP	A Personal Home Page (PHP) é uma tecnologia de código aberto do lado do servidor. Com esse modo selecionado, o ADC manterá a persistência da sessão para o mesmo servidor quando um cookie PHP for detectado.
Sessão Cookie - RDP Cookie Persistência	Esse método de equilíbrio de carga usa o Cookie RDP, criado pela Microsoft com base no nome de usuário/domínio, para dar persistência a um servidor. A vantagem desse método significa que é possível manter uma conexão com um servidor, mesmo que o endereço IP do cliente mude.
Baseado em Cookie-ID	Um novo método muito semelhante ao "PhpCookieBased" e outros métodos de balanceamento de carga, mas usando CookieIDBased e cookie RegEx h=[^;]+ Esse método usará o valor definido no campo de notas do Real Server "ID=X;" como o valor do cookie para identificar o servidor. Isso, portanto, significa que é uma metodologia semelhante à CookieListBased, mas usa um nome de cookie diferente e armazena um valor de cookie único, não o IP codificado, mas o ID do Real Server (lido no tempo de carga). O valor padrão é CookieIDName="h"; entretanto, se houver um valor de substituição na configuração avançada do servidor virtual, use esse valor em seu lugar. **NOTA**: Se esse valor for definido, nós substituímos a expressão "cookie" acima para substituir h= pelo novo valor. A última parte é que se um valor desconhecido de cookie chegar e corresponder a uma das IDs do servidor real, ele deve selecionar esse servidor; caso contrário, use o próximo método (delegado).

Monitoramento do servidor

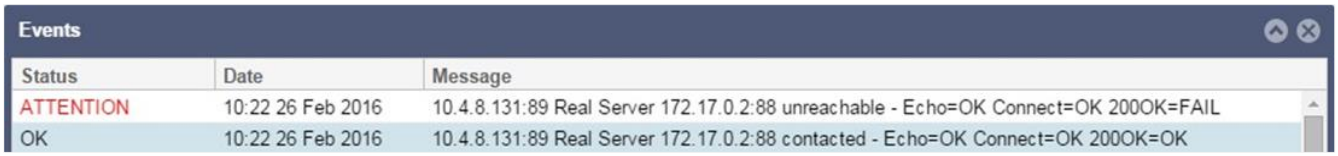
Seu ADC contém seis métodos padrão de monitoramento de servidores reais listados abaixo.



Escolha o método de monitoramento que deseja aplicar ao Serviço Virtual (VIP).

É essencial escolher o monitor certo para o serviço. Por exemplo, se o Real Server é um servidor RDP, um monitor de 200OK não é relevante. Se o senhor não tiver certeza de qual monitor escolher, a conexão TCP padrão é um excelente lugar para começar.

O senhor pode escolher vários monitores clicando em cada um deles, que, por sua vez, deseja aplicar ao serviço. Os monitores selecionados executam na ordem em que o senhor os seleciona; portanto, comece com os monitores das camadas inferiores primeiro. Por exemplo, os monitores de ajuste Ping/ICMP Echo, conexão TCP, e 200OK serão exibidos no Painel de eventos, como a imagem abaixo:



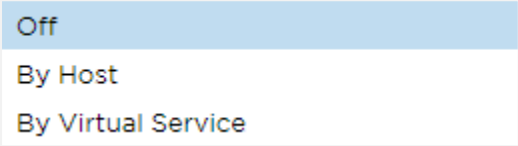
Podemos ver que a Camada 3 Ping e a Camada 4 TCP Connect tiveram êxito se olharmos para a linha superior, mas a Camada 7 200OK falhou. Esses resultados de monitoramento fornecem informações suficientes para indicar que o roteamento está OK e que há um serviço funcionando no porto relevante, mas o website não está respondendo corretamente à página solicitada. Agora é hora de olhar para o webserver e a seção Biblioteca > Monitor do Servidor Real para ver os detalhes do monitor que falhou.

Opção	Descrição
Nenhum	Nesse modo, o Real Server não é monitorado e está sempre funcionando corretamente. O ajuste Nenhum é útil para situações em que o monitoramento perturba um servidor e para serviços que não deveriam participar da ação de fail-over da ADC. É um caminho para hospedar sistemas não confiáveis ou legados que não são primários para as operações do H/A. Use esse método de monitoramento com qualquer tipo de serviço.
Ping/ICMP Echo	Nesse modo, o ADC envia um pedido de eco ICMP para o IP do servidor de conteúdo. Se uma resposta de eco válida for recebida, a ADC considera que o Real Server está em funcionamento, e o tráfego de passagem para o servidor continua. Ele também manterá o serviço disponível em um par H/A. Esse método de monitoramento é utilizável com qualquer tipo de serviço.
Conexão TCP	Nesse modo, uma conexão TCP é feita ao Real Server e imediatamente quebrada sem o envio de quaisquer dados. Se a conexão tiver êxito, o ADC considera que o Servidor Real está em funcionamento. Esse método de monitoramento é utilizável com qualquer tipo de serviço. Os serviços UDP são os únicos atualmente não apropriados para o monitoramento da conexão TCP.
ICMP Inacessível	O ADC enviará um exame de saúde da UDP ao servidor e marcará o Real Server como indisponível se ele receber uma mensagem não alcançável na porta do ICMP. Esse método pode ser útil quando o senhor precisar verificar se uma porta de serviço UDP está disponível em um servidor, tal como a porta 53 do DNS.
RDP	Nesse modo, uma conexão TCP se inicia, como explicado no ICMP, método inalcançável. Após a inicialização da conexão, é solicitada uma conexão RDP de Camada 7. Se a conexão for confirmada, o ADC considera que o Real Server está instalado e funcionando. Esse método de monitoramento é utilizável com qualquer servidor terminal da Microsoft.
200 OK	Nesse método, uma conexão TCP inicializa-se no Real Server. Após o sucesso da conexão, o ADC envia ao Servidor Real um pedido HTTP. Uma resposta HTTP é aguardada e verificada para o código de resposta "200 OK". Se o código

	de resposta "200 OK" for recebido, o ADC considera que o Real Server está em funcionamento. Se o ADC não receber um código de resposta "200 OK" por qualquer razão, incluindo timeouts, falha na conexão, e outras razões, o ADC marca o Servidor Real indisponível. Esse método de monitoramento só é válido para uso com tipos de serviço HTTP e HTTP acelerado. Se um tipo de serviço de Camada 4 estiver em uso para um servidor HTTP, ele é utilizável se o SSL não estiver em uso no Servidor Real ou se for tratado apropriadamente pela instalação "Conteúdo SSL".
DICOM	Uma conexão TCP inicializa-se ao Real Server no modo DICOM, e um "Pedido de Associado" Echoscu é feito ao Real Server na conexão. Uma conversa que inclui um "Associate Accept" do servidor de conteúdo, uma transferência de uma pequena quantidade de dados seguida por um "Release Request", e depois um "Release Response" conclui com sucesso o monitor. Se, por qualquer razão, o monitor não concluir com sucesso, então o Servidor Real é considerado como desligado.
Usuário Definido	Qualquer monitor configurado na seção de Monitoramento do Servidor Real aparecerá na lista.

Estratégia de Caching

Por default, a Estratégia de Caching é desativada e definida como Off. Se seu tipo de serviço é HTTP, então o senhor pode aplicar dois tipos de Estratégia de Caching.



Queira consultar a página Configurar Cache para configurar as configurações detalhadas do cache. Observe que quando o cache é aplicado a um VIP com o tipo de serviço "HTTP" acelerado, os objetos comprimidos não são colocados em cache.

Opção	Descrição
Por anfitrião	O cache por anfitrião é baseado na aplicação por nome de anfitrião. Haverá um Cache separado para cada domínio/nome de anfitrião. Esse modo é ideal para servidores web que podem servir múltiplos websites, dependendo do domínio.
Por Serviço Virtual	O senhor está disponível quando escolhe essa opção. Apenas um Cache existirá para todos os domínios/nomes de domínios que passarem pelo serviço virtual. Essa opção é um ambiente especializado para uso com vários clones de um único site.

Aceleração

Opção	Descrição
Off	Desligar a compressão para o Serviço Virtual
Compressão	Quando selecionada, essa opção ativa a compressão para o Serviço Virtual selecionado. O ADC comprime dinamicamente o fluxo de dados para o cliente, mediante solicitação. Esse processo só se aplica a objetos que contenham a codificação de conteúdo: cabeçalho gzip. O conteúdo de exemplo inclui HTML, CSS, ou Javascript. O cliente também pode excluir certos tipos de conteúdo usando a seção Exclusões Globais.

Nota: Se o objeto for armazenável, o ADC armazenará uma versão comprimida e a servirá estaticamente (de memória) até que o conteúdo expire e seja novamente validado.

Serviço Virtual Certificado SSL (Encriptação entre o Cliente e o ADC)

Por padrão, a configuração é Sem SSL. Se seu tipo de serviço for "HTTP" ou "Layer4 TCP", o senhor pode selecionar um certificado no menu suspenso para candidatar-se ao Serviço Virtual. Os certificados que tiverem sido criados ou importados aparecerão nessa lista. O senhor pode destacar vários certificados para solicitar a um serviço. Essa operação permitirá automaticamente que a extensão do SNI permita um certificado baseado no "Nome de Domínio" solicitado pelo cliente.

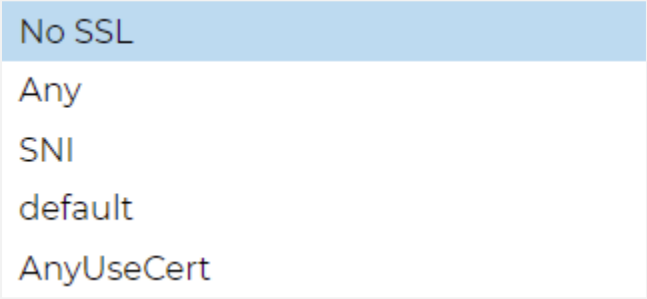
Indicação do nome do servidor

Essa opção é uma extensão do protocolo de rede TLS, usando o qual o cliente indica a que hostname ele está tentando se conectar no início do processo de aperto de mão. Essa configuração permite ao ADC apresentar vários certificados no mesmo endereço IP virtual e porta TCP.

Opção	Descrição
Sem SSL	O tráfego da fonte para o ADC não é criptografado.
Todos	Carrega todos os certificados disponíveis para uso
Inadimplência	Essa opção resulta na aplicação de um certificado criado localmente, chamado "Default", ao lado do navegador do canal. Use essa opção para testar o SSL quando um não tiver sido criado ou importado.
AnyUseCert	Usar qualquer certificado presente no ADC que o usuário tenha carregado ou gerado

Certificado SSL do Real Server (Criptografia entre o ADC e o Real Server)

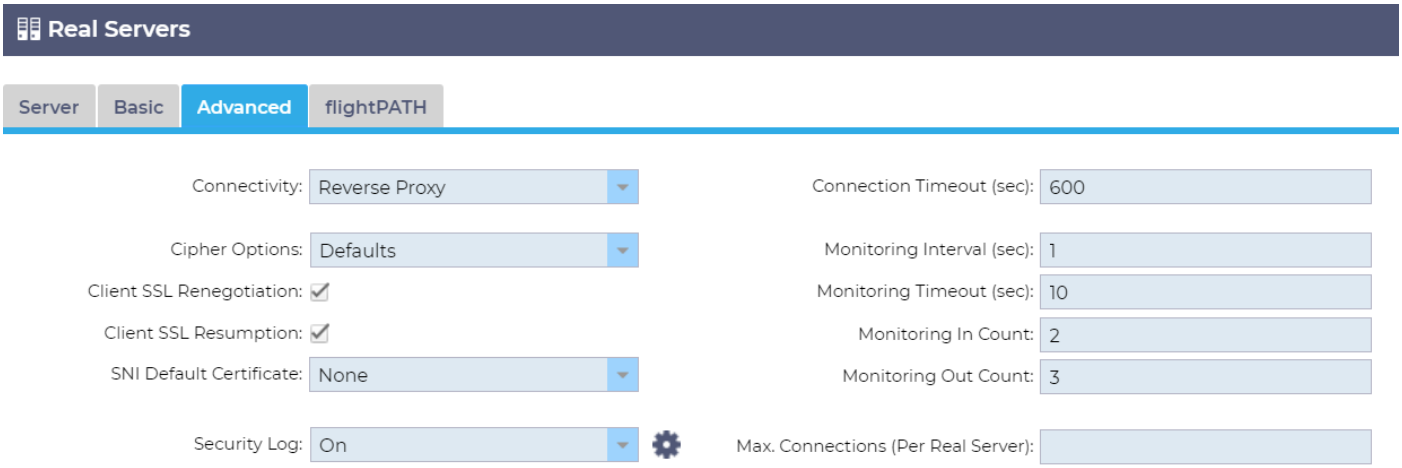
A configuração padrão para essa opção é Sem SSL. Se seu servidor requer uma conexão criptografada, esse valor deve ser qualquer outra coisa além de No SSL. Os certificados que tenham sido criados ou importados aparecerão nessa lista.



Opção	Descrição
Sem SSL	O tráfego do ADC para o Real Server não é criptografado. A seleção de um certificado no lado do navegador significa que "No SSL" pode ser escolhido no lado do cliente para fornecer o que é conhecido como "SSL Offload".
Qualquer	O ADC atua como cliente e aceitará qualquer certificado que o Real Server apresentar. O tráfego do ADC para o Real Server é criptografado quando essa opção é selecionada. Use a opção "Qualquer" quando um certificado é

	especificado no lado do Serviço Virtual, fornecendo o que é conhecido como "SSL Bridging" ou "SSL Re-Encryption".
SNI	O ADC atua como cliente e aceitará qualquer certificado que o Real Server apresentar. O tráfego do ADC para o Servidor Real é criptografado se este for selecionado. Use a opção "Qualquer" quando um certificado for especificado no lado do Serviço Virtual, fornecendo o que é conhecido como "SSL Bridging" ou "SSL Re-Encryption". Escolha essa opção para habilitar o SNI no lado do servidor.
AnyUseCert	Quaisquer certificados que o senhor tenha gerado ou importado para o ADC aparecem aqui.

Avançado



Conectividade

Seu Serviço Virtual é configurável com quatro tipos diferentes de conectividade. Queira selecionar o modo de conectividade a ser aplicado ao serviço.

Opção	Descrição
Procuração reversa	A Reverse Proxy é o valor padrão e trabalha em Layer7 com compressão e caching. E na Camada4 sem caching ou compressão. Nesse modo, seu ADC age como um proxy reverso e se torna o endereço de origem visto pelos Servidores Reais.
Retorno direto do servidor	Direct Server Return ou DSR como é amplamente conhecido (DR - Direct Routing em alguns círculos) permite ao servidor por trás do equilibrador de carga responder diretamente ao cliente contornando o ADC na resposta. O DSR só é adequado para uso com o balanceamento de carga de Camada 4. Portanto, Caching e Compressão não estão disponíveis com essa opção escolhida. O balanceamento de carga da camada 7 não funciona com esse DSR. Além disso, não há nenhum apoio persistente além do baseado na Lista de PI. O balanceamento de carga SSL/TLS com esse método não é o ideal, já que o suporte de persistência de IP de origem é o único tipo disponível. O DSR também requer mudanças no Real Server para ser feito. Consulte a seção Mudanças no Servidor Real.
Porta de entrada	O modo Gateway permite que o senhor encaminhe todo o tráfego através do ADC, permitindo que o tráfego dos Servidores Reais seja encaminhado através do ADC para outras redes através das máquinas virtuais ou interfaces de hardware do ADC. Usar o dispositivo como um dispositivo de gateway para Servidores Reais é ideal quando estiver rodando em modo multi-interface.

	O equilíbrio de carga da camada 7 com esse método não funciona, pois não há nenhum outro apoio de persistência além do baseado na lista de IP. Esse método exige que o Real Server defina seu gateway padrão para o endereço de interface local (eth0, eth1, etc.) do ADC. Por favor, consulte a seção Mudanças no Servidor Real. ***Queira observar que o modo Gateway não suporta falhas em um ambiente de cluster.***

Opções cifradas

O senhor pode colocar cifras por serviço, e isso só é relevante para serviços com SSL/TLS habilitado. O ADC faz a escolha automática da cifra, e o senhor pode acrescentar diferentes cifras usando jetPACKS. Ao adicionar o jetPACK apropriado, o senhor pode definir as opções de cifras por serviço. O benefício disso é que o senhor pode criar vários serviços com diferentes níveis de segurança. Esteja ciente de que clientes mais antigos não são compatíveis com cifras mais novas para reduzir o número de clientes quanto mais seguro for o serviço.

Cliente SSL Renegociação

Marque esta caixa se desejar permitir a renegociação SSL iniciada pelo cliente. Desativar a renegociação SSL do cliente para evitar qualquer possível ataque do DDOS contra a camada SSL, desmarcando essa opção.

Cliente SSL Retomada

Assinale esta caixa se o senhor deseja habilitar sessões do Servidor de Retomada SSL adicionadas ao cache da sessão. Quando um cliente propõe a reutilização de uma sessão, o servidor tentará reutilizar a sessão, se encontrada. Se o Resumption não for verificado, nenhuma sessão será armazenada em cache para cliente ou servidor.

SNI Certificado de inadimplência

Durante uma conexão SSL com o SNI do lado do Cliente habilitado, se o domínio solicitado não corresponder a nenhum dos certificados designados para o serviço, o ADC apresentará o Certificado Default do SNI. A configuração padrão para isso é Nenhuma, o que efetivamente deixaria a conexão de lado se não houvesse uma correspondência exata. Escolha qualquer um dos certificados instalados da lista suspensa para apresentar, caso um certificado SSL coincida exatamente.

Diário de Segurança

On" é o valor padrão e é por serviço, permitindo o serviço de autenticação dos registros do W3C. Clicando no ícone Cog, o senhor será levado à página Sistema > Logging, onde poderá verificar as configurações do W3C logando.

Tempo limite de conexão

O tempo limite padrão de conexão é de 600 segundos ou 10 minutos. Essa configuração ajustará o tempo para a conexão ao tempo esgotado, quando não houver atividade. Reduza isso para o tráfego de curta duração da rede sem Estado, que normalmente é de 90s ou menos. Aumente esse número para conexões estaduais como o RDP para algo como 7200 segundos (2 horas) ou mais, dependendo de sua infra-estrutura. O exemplo do RDP significa que se um usuário tiver um período de inatividade de 2 horas ou menos, as conexões permanecerão abertas.

Configurações de monitoramento

Essas configurações estão relacionadas com os monitores do servidor real na guia Básico. Há entradas globais na configuração para contar o número de monitores bem-sucedidos ou falhados antes que o status de um servidor seja marcado on-line ou falhe.

Intervalo

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

Tempo limite de monitoramento

O valor de timeout é quando o ADC esperará que um servidor responda a um pedido de conexão. O valor padrão é 2s. Aumente esse valor para servidores ocupados.

Monitoramento em Contagem

O valor padrão para essa configuração é 2. O valor de 2 indica que o Servidor Real deve passar por duas verificações bemsucedidas do monitor de saúde antes de entrar on-line. Aumentar esse valor aumentará a probabilidade de que o servidor possa servir ao tráfego, mas levará mais tempo para entrar em serviço, dependendo do intervalo. Diminuir esse valor fará com que seu servidor entre em serviço mais cedo.

Monitoramento da contagem

O valor padrão para essa configuração é 3, o que significa que o monitor do Servidor Real deve falhar três vezes antes que o ADC deixe de enviar tráfego para o servidor, e é marcado como VERMELHO e Inaceitável. Aumentar esse valor resultará em um serviço melhor e mais confiável às custas do tempo que o ADC leva para parar de enviar tráfego para esse servidor.

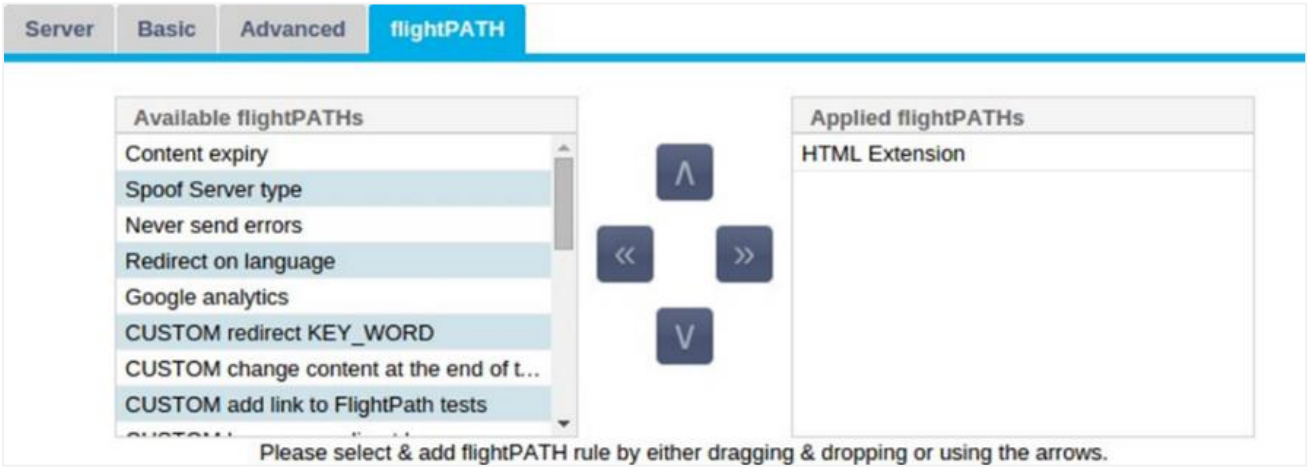
Mudança para falha off-line

Quando isso é verificado, os Servidores Reais que falham no exame de saúde são colocados off-line e só podem ser colocados on-line manualmente.

Max. Conexões

Limita o número de conexões simultâneas do Real Server e é definido por serviço. Por exemplo, se o senhor configurar isso para 1000 e tiver dois Servidores Reais, o ADC limita **cada** Servidor Real a 1000 conexões simultâneas. O senhor também pode escolher apresentar uma página "Servidor muito ocupado" assim que esse limite for atingido em todos os servidores, ajudando os usuários a entender por que ocorreu qualquer não-resposta ou atraso. Deixe isso em branco para conexões ilimitadas. O que o senhor aqui estabelece depende dos recursos de seu sistema.

vôoPATH



flightPATH é um sistema projetado pela Edgenexus e disponível exclusivamente dentro do ADC. Ao contrário dos motores baseados em regras de outros fornecedores, o flightPATH não opera através de uma linha de comando ou de um console de entrada de scripts. Em vez disso, ele usa um GUI para selecionar os diferentes parâmetros, condições e ações a serem executadas para alcançar o que eles

precisam. Essas características tornam o flightPATH extremamente poderoso e permitem que os administradores da rede manipulem o tráfego HTTPS de maneiras altamente eficazes.

flightPATH só está disponível para uso com conexões HTTPS, e essa seção não é visível quando o tipo de serviço virtual não é HTTP.

O senhor pode ver na imagem acima; há uma lista de regras disponíveis à esquerda e as regras aplicadas ao serviço virtual à direita.

Adicione uma regra disponível, arrastando e soltando a regra do lado esquerdo para o direito ou destacando uma regra e clicando na seta para a direita para movê-la para o lado direito.

A ordem de execução é essencial e começa com a regra máxima executada primeiro. Para mudar a ordem de execução, destaque a regra e suba e desça usando as setas.

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

O senhor pode acrescentar, remover e editar as regras do flightPATH na seção Configure flightPATH deste guia.

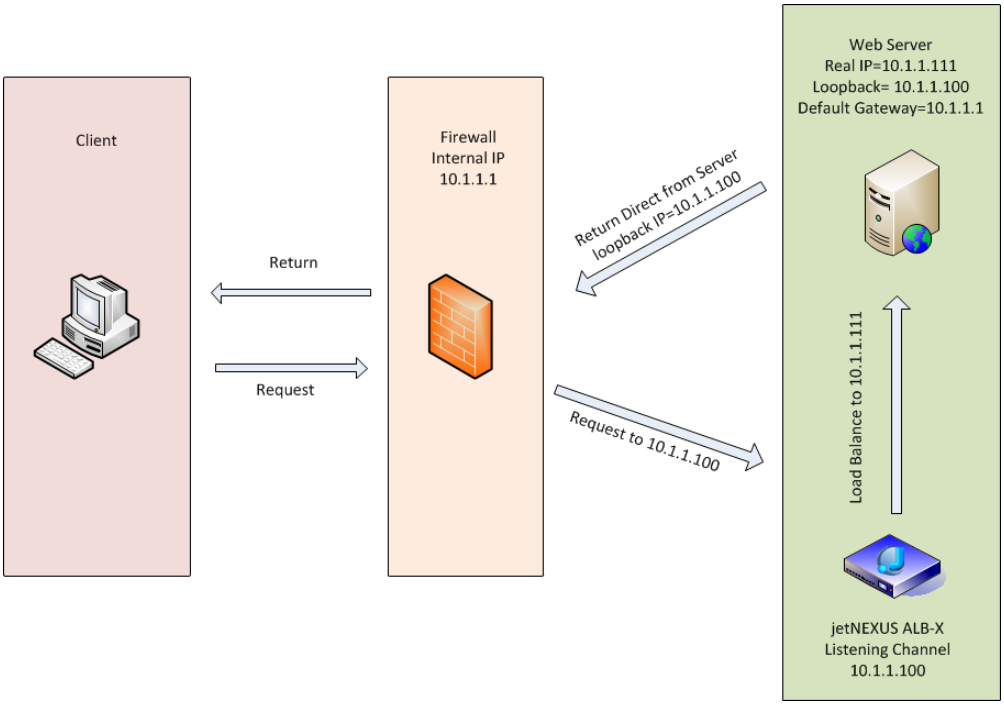
Mudanças Reais no Servidor para Retorno Direto do Servidor

Direct Server Return ou DSR como é amplamente conhecido (DR - Direct Routing em alguns círculos) permite ao servidor por trás do ADC responder diretamente ao cliente, contornando o ADC na resposta. O DSR só é adequado para uso com balanceamento de carga de Camada 4. Caching e Compressão não estão disponíveis quando ativados.

A camada 7 de equilíbrio de carga com esse método não funcionará, pois não há nenhum outro suporte de persistência além do PI de origem. O balanceamento de carga SSL/TLS com esse método não é ideal, já que só há suporte de persistência de IP de origem.

Como funciona

- Cliente envia um pedido para o jetNEXUS ALB-X
- Pedido recebido por edgeNEXUS
- Pedido roteado para servidores de conteúdo
- Resposta enviada diretamente ao cliente sem passar pelo edgeNEXUS



Configuração do Servidor de Conteúdo Requerido

Geral

- O gateway padrão do servidor de conteúdo deve ser configurado como normal. (Não através do ADC)
- O servidor de conteúdo e o equilibrador de carga devem estar na mesma sub-rede

Janelas

- O servidor de conteúdo precisa ter um loopback ou Alias configurado com o endereço IP do Canal ou VIP
    - A métrica da rede deve ser 254 para evitar resposta aos pedidos da 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 reais do Windows

netsh interface ipv4 set interface "Windows network interface name" 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

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

ifcfg-lo:1DEVICE=lo
:1IPADDR=x
.x.x.xNETMASK=255
.255.255.255BROADCAST=x
.x.x.x.xONBOOT=yes

- Edição "/etc/sysctl.conf"

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

- Executar "sysctl - p".

Mudanças reais no servidor - Modo Gateway

O modo Gateway permite que o senhor encaminhe todo o tráfego através do ADC, e isso permite que o tráfego proveniente dos servidores de conteúdo seja encaminhado através do ADC para outras redes através das interfaces na unidade do ADC. O uso do dispositivo como um dispositivo de gateway para servidores de conteúdo deve ser usado quando em funcionamento em modo multi-interface.

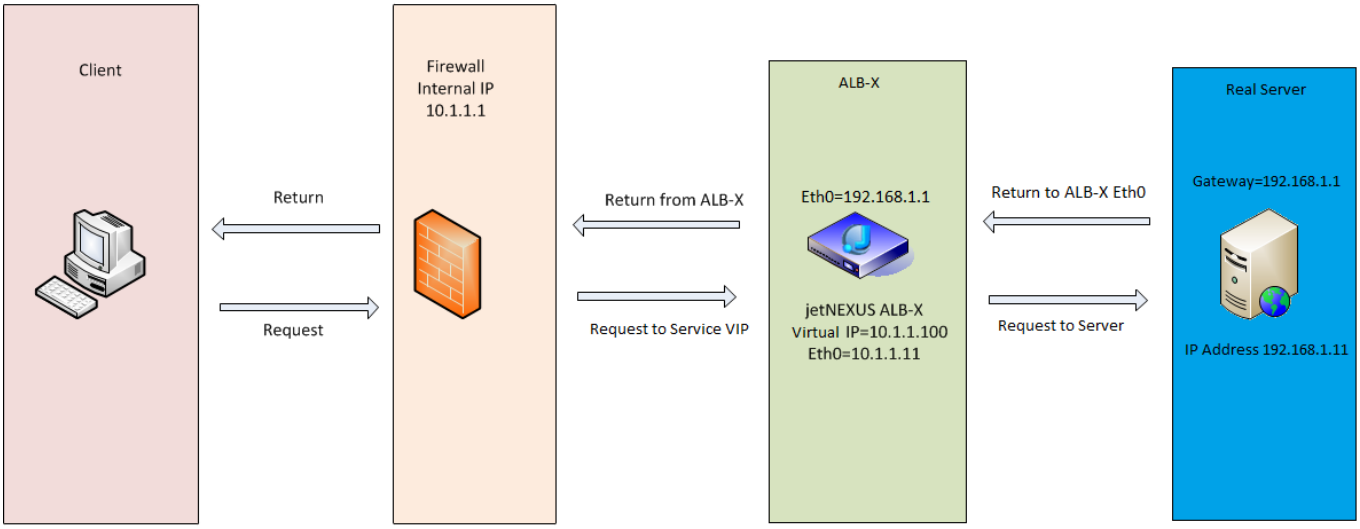
Como funciona

- O cliente envia um pedido para o jetNEXUS ALB-X
- Um pedido é recebido por edgeNEXUS
- Pedido enviado aos servidores de conteúdo
- Resposta enviada à edgeNEXUS
- ADC encaminha a resposta para o cliente

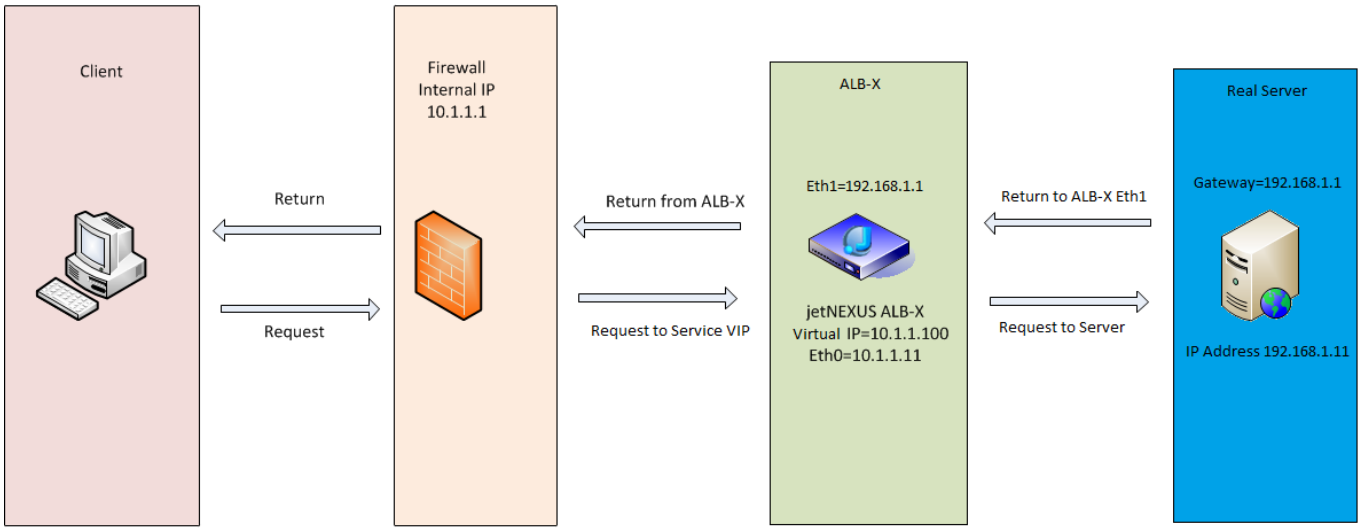
Configuração do Servidor de Conteúdo Requerido

- Modo braço único - uma interface é utilizada, mas o serviço VIP e os Servidores Reais devem estar em sub-redes diferentes.
- Modo braço duplo - são utilizadas duas interfaces, mas o serviço VIP e os servidores reais devem estar em sub-redes diferentes.
- Em cada caso, de braço simples e duplo, os Servidores Reais precisam configurar sua porta de entrada padrão para o endereço de interface do ADC na sub-rede relevante.

Exemplo de braço único



Exemplo de braço duplo



Biblioteca

Suplementos

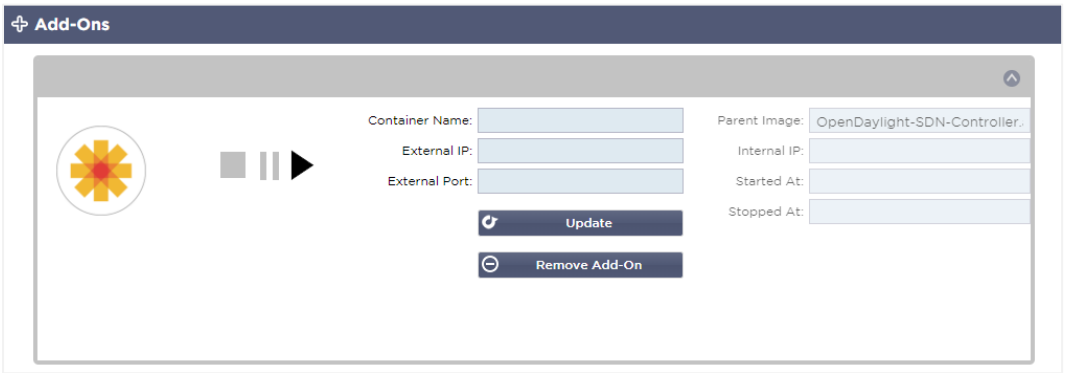
Os complementos são recipientes baseados em Docker que podem funcionar de forma isolada dentro do ADC. Exemplos de complementos podem ser um firewall de aplicação ou mesmo uma micro instância do próprio ADC.

Apps

A seção de APPs dentro de Add-Ons detalha os APPs que o senhor comprou, baixou e implantou.

Se não houver nenhum APP presente, esta seção exibirá uma mensagem solicitando que o senhor vá até a seção de APPs e faça o download e a distribuição de um APP.

Uma vez que o senhor tenha implantado um APP, ele aparecerá na área dos APPs.



Compra de um suplemento

Para comprar uma App, o senhor precisa se registrar na App Store. A compra é feita usando o próprio ADC. O senhor encontrará

Navegue até a biblioteca > página Apps do painel de instrumentos do ADC.

Aqui o senhor pode selecionar o aplicativo que deseja baixar e depois instalar.

Se o senhor está fazendo isso a partir do painel do ADC, queira selecionar apenas um item. O senhor pode ser proprietário de vários conjuntos do ADC, e os pedidos precisam ser associados ao ADC no qual eles são instalados.

Se o senhor acessar a App Store através de seu desktop e de seu navegador, poderá fazer o download de quantos quiser. Por exemplo, quatro exemplos do WAF ou GSLB. Elas aparecerão na área de suas Aplicativos de Compras do ADC, para que o senhor possa baixá-las.

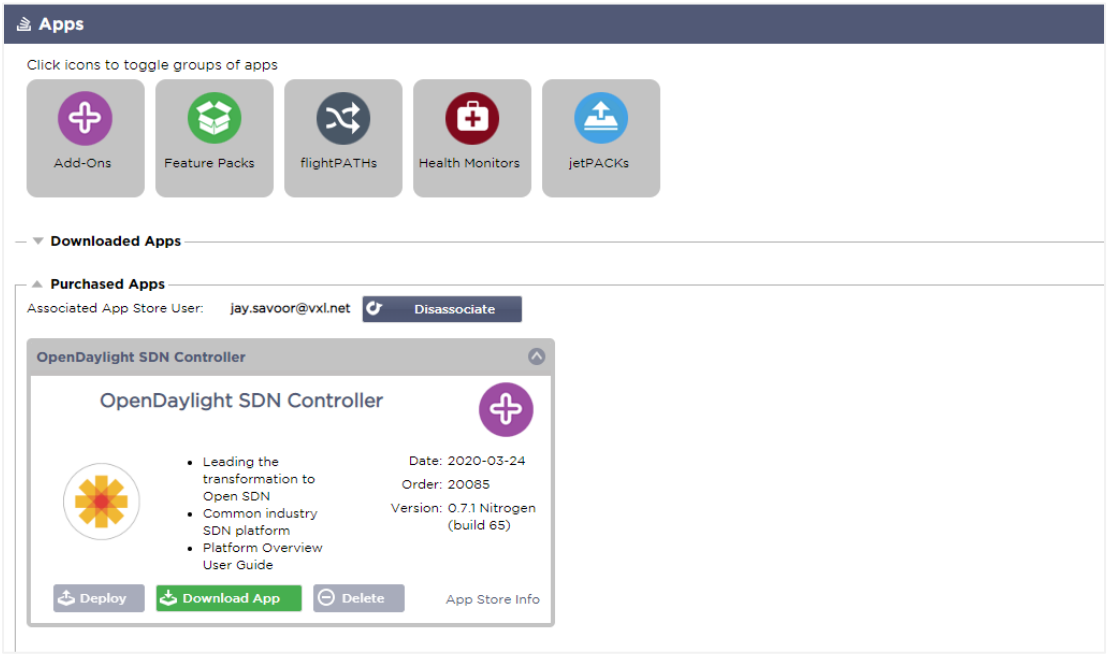
Os APPs associados ao ADC de que o senhor é proprietário e que se registraram.

Quando o senhor decidir fazer o download de um Aplicativo, ser-lhe-á solicitada a identificação da máquina, após a qual o Aplicativo será criptografado e ligado ao ADC.

Os links para a App Store são:

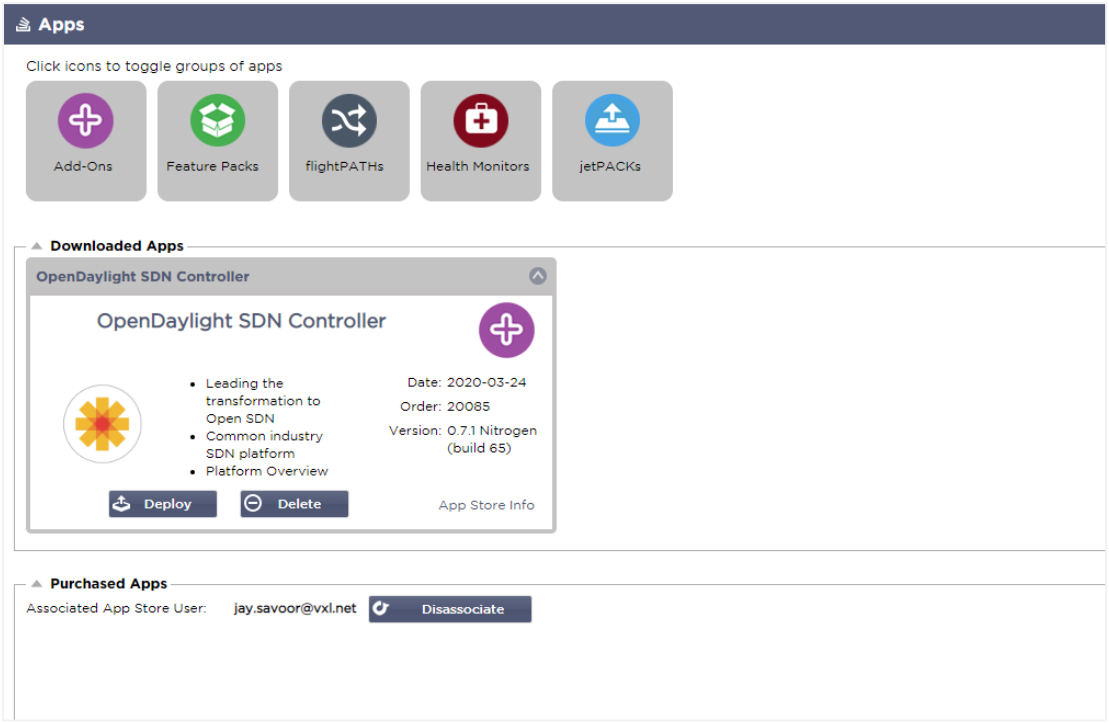
- Adições: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Monitores de saúde: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**

- Pacotes de características: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/
- Regras do FlightPATH: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/
- Atualizações de software: HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/



Implantação de uma App

Uma vez baixado para o ADC, o Aplicativo será movido para a seção de Aplicativos baixados e colocado no ADC usando o botão Deploy. Esse processo leva algum tempo, dependendo dos recursos disponíveis para o ADC. Uma vez que for descarregado, ele aparecerá na seção de Aplicativos descarregados.



Autenticação

A Biblioteca > Página de autenticação permite ao senhor estabelecer servidores de autenticação e criar regras de autenticação com opções para o lado do cliente Basic ou Forms e server-side NTLM ou BASIC.

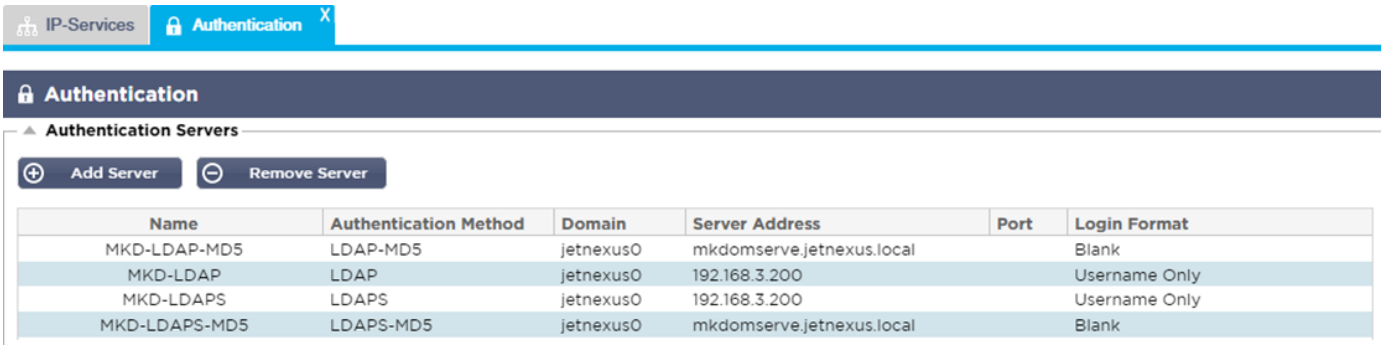
Estabelecimento da Autenticação - Um Fluxo de Trabalho

Queira fazer o favor de, no mínimo, as seguintes diligências para aplicar a autenticação ao seu serviço.

1. Criar um Servidor de Autenticação.
2. Criar uma Regra de Autenticação que use um Servidor de Autenticação.
3. Criar uma regra de flightPATH que use uma Regra de Autenticação.
4. Aplicar a regra flightPATH a um serviço

Servidores de autenticação

Para estabelecer um método de autenticação funcional, é preciso primeiro estabelecer um servidor de autenticação.



Name	Authentication Method	Domain	Server Address	Port	Login Format
MKD-LDAP-MD5	LDAP-MD5	jetnexus0	mkdomserve.jetnexus.local		Blank
MKD-LDAP	LDAP	jetnexus0	192.168.3.200		Username Only
MKD-LDAPS	LDAPS	jetnexus0	192.168.3.200		Username Only
MKD-LDAPS-MD5	LDAPS-MD5	jetnexus0	mkdomserve.jetnexus.local		Blank

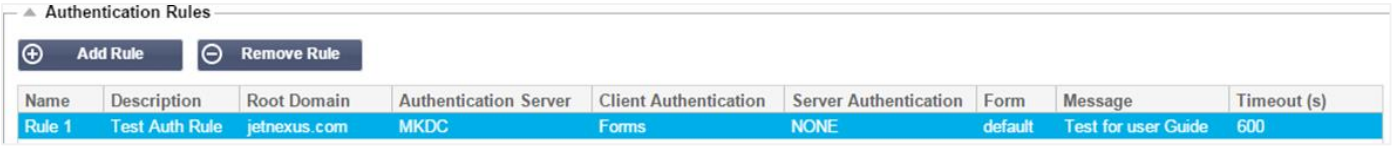
- Clique no botão Add Server.
- Essa ação produzirá uma fila em branco, pronta para ser concluída.

Opção	Descrição
Nome	Dê a seu servidor um nome para fins de identificação - esse nome é usado no regulamento
Descrição	Acrescentar uma descrição
Método de autenticação	Escolher um método de autenticação LDAP - LDAP básico com nomes de usuário e senhas enviadas em texto claro para o servidor do LDAP. LDAP-MD5 - LDAP básico com o nome de usuário em texto claro e senha MD5 tem sido um hashed para aumentar a segurança. LDAPS - LDAP sobre SSL. Envia a senha em texto claro dentro de um túnel criptografado entre o ADC e o servidor do LDAP. LDAPS-MD5 - LDAP sobre SSL. A senha é MD5 para maior segurança dentro de um túnel criptografado entre o ADC e o servidor LDAP.
Domínio	Acrescentar no nome de domínio para o servidor LDAP.
Endereço do servidor	Adicionar o endereço IP ou hostname do servidor de autenticação LDAP - endereço IPv4 ou hostname. LDAP-MD5 - somente hostname (endereço IPv4 não vai funcionar) LDAPS - endereço IPv4 ou hostname. LDAPS-MD5 - somente hostname (endereço IPv4 não vai funcionar).
Porto	Use o porto 389 para LDAP e o porto 636 para LDAPS por padrão. Não há necessidade de acrescentar o número do porto para LDAP e LDAPS. Quando outros métodos estiverem disponíveis, o senhor poderá configurá-los aqui.
Condições de busca	As condições de busca devem estar de acordo com o RFC 4515. Exemplo:

	(MembroOf=CN=Fone- VPN,CN=Usuários,DC=empresa microscópica,DC=local).
Base de busca	Esse valor é o ponto de partida para a busca na base de dados do LDAP. Exemplo *dc=empresa microscópica,dc=local*
Formato de Login	Use o formato de login que o senhor precisa. Nome de usuário - com este formato escolhido, o senhor só precisa digitar o nome de usuário. Qualquer informação de usuário e domínio digitada pelo usuário é apagada, e a informação de domínio do servidor é usada. Nome de usuário e domínio - O usuário deve digitar todo o domínio e a sintaxe do nome de usuário. Exemplo: *mycompany\gchristie OU alguém@mycompany*. As informações de domínio digitadas no nível do servidor são ignoradas. Em branco - o ADC aceitará tudo o que o usuário inserir e o enviará para o servidor de autenticação. Essa opção é usada quando se usa o MD5.
Senha	Essa opção não é usada nesta versão.
Tempo morto	Não usado nesta versão

Regras de autenticação

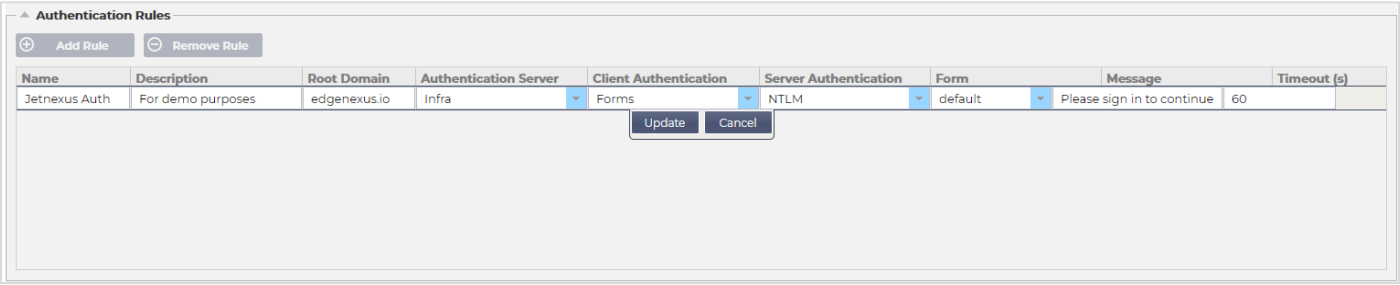
A próxima etapa é criar as regras de autenticação para uso com a definição do servidor.



Campo	Descrição
Nome	Acrescente um nome adequado para sua regra de autenticação.
Descrição	Acrescente uma descrição adequada.
Domínio Raiz	Isso deve ser deixado em branco, a menos que o senhor precise de um único sinal para todos os sub-domínios.
Servidor de autenticação	Esta é uma caixa suspensa contendo servidores que o senhor configurou.
Autenticação do cliente:	Escolha o valor adequado às suas necessidades: Básico (401) - Este método usa o método de autenticação padrão 401 Formulários - isso apresentará ao usuário o formulário padrão do ADC. Dentro do formulário, o senhor pode acrescentar uma mensagem. O senhor pode selecionar um formulário que tenha carregado, usando a seção abaixo.
Autenticação do servidor	Escolha o valor apropriado. Nenhuma - se seu servidor não tiver nenhuma autenticação existente, selecione esta configuração. Essa configuração significa que o senhor pode acrescentar habilidades de autenticação a um servidor que anteriormente não possuía nenhuma. Básico - se o seu servidor tem autenticação básica (401) habilitada, então selecione BASIC. NTLM - se seu servidor tem a autenticação NTLM habilitada, então selecione NTLM.
Formulário	Escolha o valor apropriado Default - A seleção dessa opção resultará no ADC usando sua forma embutida. Personalizado - o senhor pode acrescentar um formulário que o senhor projetou e selecioná-lo aqui.
Mensagem	Acrescente uma mensagem pessoal ao formulário.

Tempo esgotado	Acrescente um timeout à regra, após o qual o usuário será obrigado a autenticar novamente. Observe que a regra de tempo limite só é válida para autenticação baseada em formulários.

Assinatura única



Se o senhor deseja fornecer um único sinal para os usuários, complete a coluna do Domínio Raiz com seu domínio. Neste exemplo, usamos edgenexus.io. Agora podemos ter vários serviços que usarão edgenexus.io como o domínio raiz, e o senhor só terá que fazer o login uma única vez. Se considerarmos os seguintes serviços:

- Sharepoint.mycompany.com
- usercentral. mycompany.com
- appstore. mycompany.com

Esses serviços podem residir em um VIP ou podem ser distribuídos entre três VIPs. Um usuário que acesse o site usercentral. mycompany.com pela primeira vez receberá um formulário solicitando que faça o login de acordo com a regra de autenticação usada. O mesmo usuário pode então conectar-se ao appstore. mycompany.com e será autenticado automaticamente pelo ADC. O senhor pode definir o tempo limite, o que forçará a autenticação assim que esse período de inatividade for alcançado.

Formulários

Esta seção permitirá que o senhor carregue um formulário personalizado.

Como criar seu formulário personalizado

Embora a forma básica que o ADC fornece seja suficiente para a maioria dos fins, haverá ocasiões em que as companhias desejarão apresentar sua própria identidade ao usuário. O senhor pode criar seu formulário personalizado, que será apresentado aos usuários para preencher em tais casos. Esse formulário deve estar no formato HTM ou HTML.

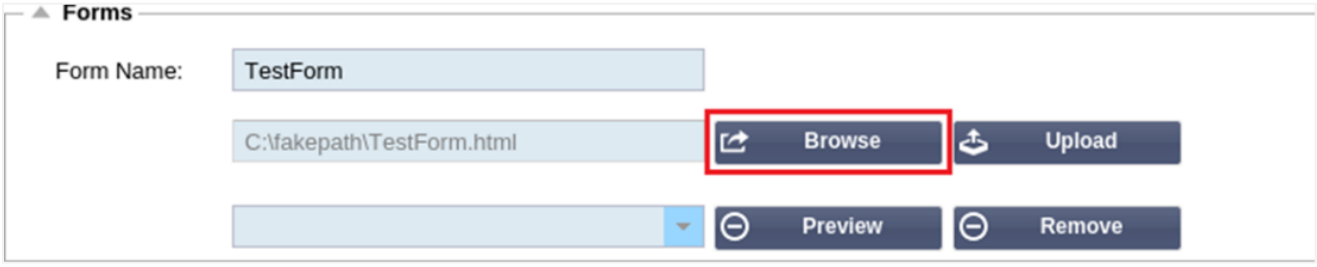
Opção	Descrição
Nome	nome do formulário = formulário de login ação = %JNURL% Método = POST
Nome de usuário	Sintaxe: nome = "JNUSER".
Senha:	name="JNPASS"
Mensagem facultativa1:	%JNMESSAGEM%
Mensagem facultativa2:	%JNAUTHMESSAGE%
Imagens	Se o senhor deseja acrescentar uma imagem, queira acrescentá-la em linha usando a codificação Base64.

Exemplo de código html de uma forma muito simples e básica

```
<HTML>
<CABEÇA>
<TÍTULO>FORMULÁRIO DE EXEMPLO</TÍTULO>
</HEAD>
<CORPO>
%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>
</CORPO>
</HTML>
```

Acréscimo de um formulário personalizado

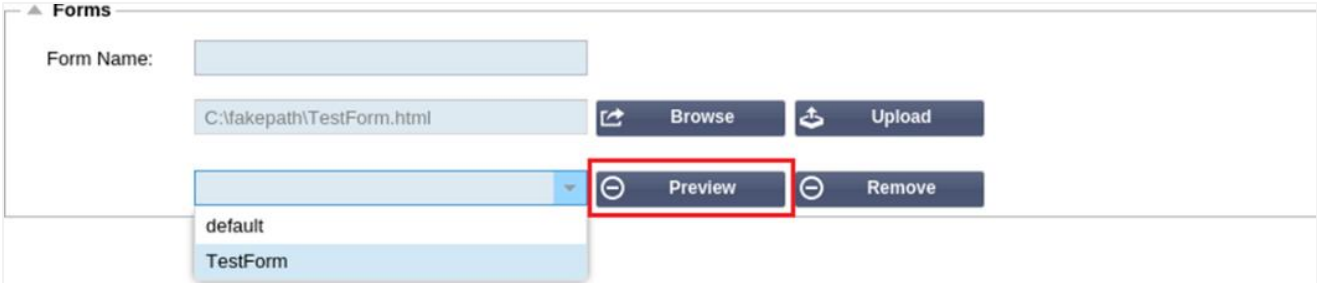
Uma vez que o senhor tenha criado um formulário personalizado, poderá adicioná-lo usando a seção Formulários.



1. Escolha um nome para seu formulário
2. Procure localmente seu formulário
3. Clique em Upload

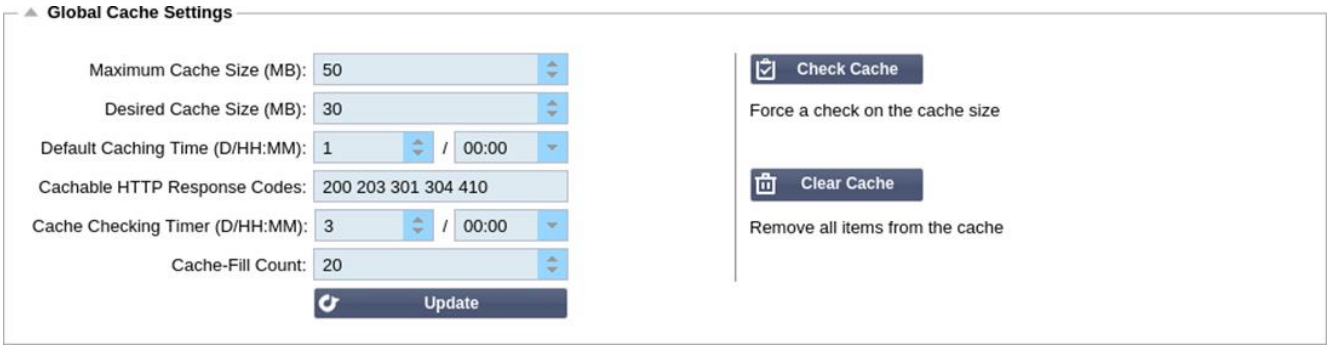
Pré-visualização de seu formulário personalizado

Para ver o formulário personalizado que o senhor acabou de carregar, selecione-o e clique em Preview (Visualização). O senhor também pode usar esta seção para eliminar formulários que não são mais necessários.



Cache

O ADC é capaz de armazenar dados em cache dentro de sua memória interna e periodicamente descarrega esse Cache para o armazenamento interno do ADC. Os ajustes que gerenciam essa funcionalidade são fornecidos dentro desta seção.



Cache Global Settings

Tamanho Máximo do Cache (MB)

Esse valor determina o máximo de RAM que a Cache pode consumir. O ADC Cache é um cache em memória que também é periodicamente lavado no meio de armazenamento para manter a persistência do cache após reinícios, reinicializações e operações de desligamento. Essa funcionalidade significa que o tamanho máximo do cache deve caber dentro da área de memória do aparelho (em vez de espaço em disco) e não deve ser mais que a metade da memória disponível.

Tamanho desejado do Cache (MB)

Esse valor denota o RAM ótimo ao qual a Cache será aparada. Enquanto o tamanho máximo do cache representa o limite superior absoluto do Cache, o tamanho desejado do cache é o tamanho ótimo que o Cache deve tentar alcançar sempre que uma verificação automática ou manual do tamanho do cache for feita. A lacuna entre o tamanho máximo e o tamanho desejado do cache existe para acomodar a chegada e a sobreposição de novo conteúdo entre as verificações periódicas do tamanho do cache e o conteúdo expirado. Mais uma vez, pode ser mais eficaz aceitar o valor padrão (30 MB) e revisar periodicamente o tamanho do cache em "Monitor -> Estatísticas" para o tamanho apropriado.

Tempo de Cache por Defeito (D/HH:MM)

O valor aqui informado representa a vida útil do conteúdo sem um valor de expiração explícito. O tempo de armazenamento padrão é o período durante o qual o conteúdo sem uma diretriz "sem loja" ou tempo de expiração explícita no cabeçalho do tráfego é armazenado.

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

Códigos de resposta HTTP em cache

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

- 200 - Resposta padrão para pedidos HTTP bem sucedidos
- 203 - Os cabeçalhos não são definitivos, mas são reunidos a partir de uma cópia local ou de uma cópia de terceiros
- 301 - O recurso solicitado foi designado um novo URL permanente
- 304 - Não modificado desde o último pedido e uma cópia em cache local deve ser usada em seu lugar

- 410 - O recurso não está mais disponível no servidor, e nenhum endereço de encaminhamento é conhecido

Esse campo deve ser editado com cautela, pois os códigos de resposta mais comuns já estão listados.

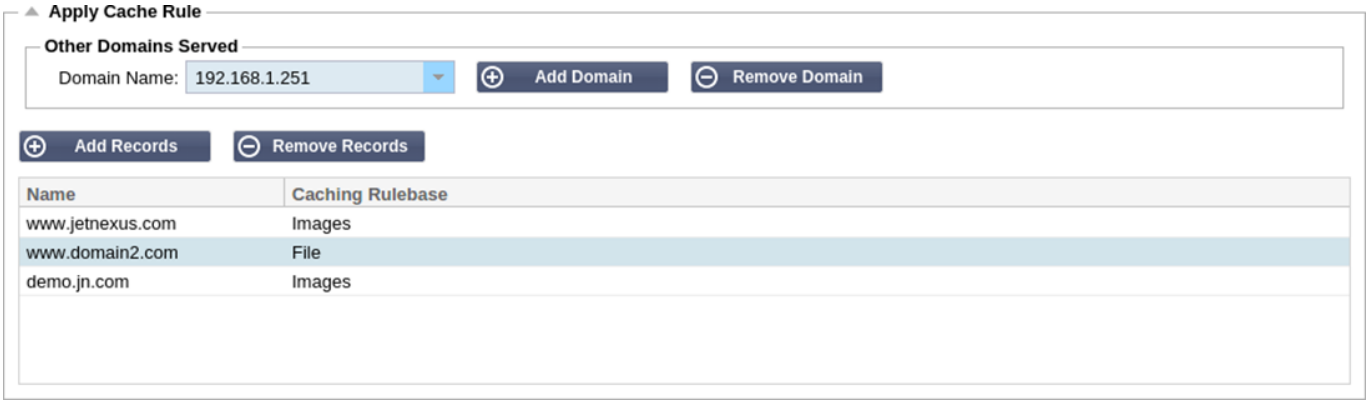
Tempo de Verificação de Cache (D/HH:MM)

Esse ajuste determina o intervalo de tempo entre as operações de corte de cache.

Contagem de Cache-Fill

Esse quadro é uma instalação de ajuda para ajudar a preencher o Cache quando um certo número de 304's tiver sido detectado.

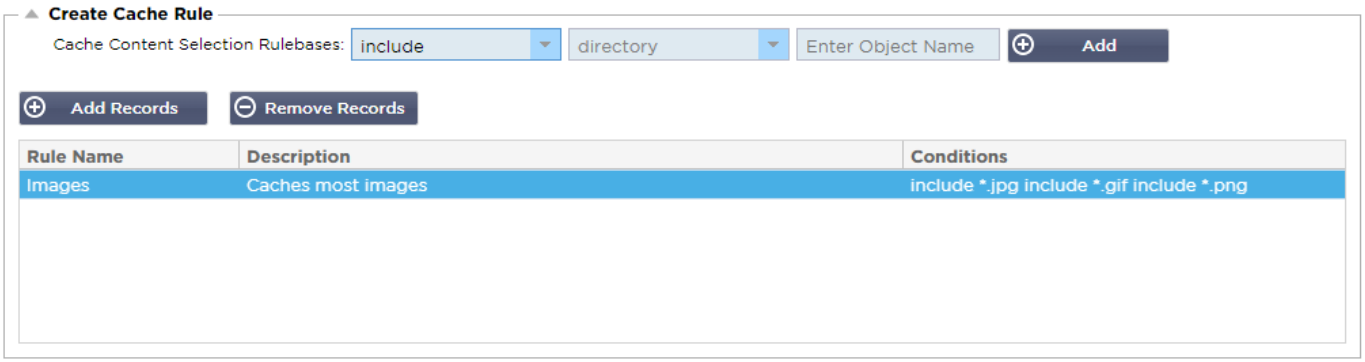
Aplicar a regra de Cache



Esta seção permite que o senhor aplique uma regra de cache a um domínio:

- Adicione o domínio manualmente com o botão Add Records. O senhor deve usar um nome de domínio totalmente qualificado ou um endereço IP em notação ponto-decimal. Exemplo www. mycompany.com ou 192.168.3.1:80
- Clique na seta suspensa e escolha seu domínio da lista
- A lista será preenchida desde que o tráfego tenha passado por um serviço virtual e que uma estratégia de cache tenha sido aplicada ao serviço virtual
- Escolha sua regra de cache clicando duas vezes na coluna Caching Rulebase e selecionando da lista

Criar Regra de Cache



Esta seção permite ao senhor deputado criar várias regras diferentes de cache que podem então ser aplicadas a um domínio:

- Clique em Add Records e dê a sua regra um nome e descrição
- O senhor pode digitar suas condições manualmente ou usar a Condição Adicional

Acrescentar uma condição usando a base da regra de seleção:

- Escolha Incluir ou Excluir
- Escolha todas as imagens JPEG
- Clique sobre o símbolo + Adicionar
- O senhor verá que "incluir *.jpg" foi agora adicionado às condições
- O senhor pode acrescentar mais condições. Se o senhor decidir fazer isso manualmente, precisará acrescentar cada condição em uma NOVA linha. Queira observar que suas regras serão exibidas na mesma linha até que o senhor clique na caixa de Condições e depois serão exibidas em uma linha separada.

vôoPATH

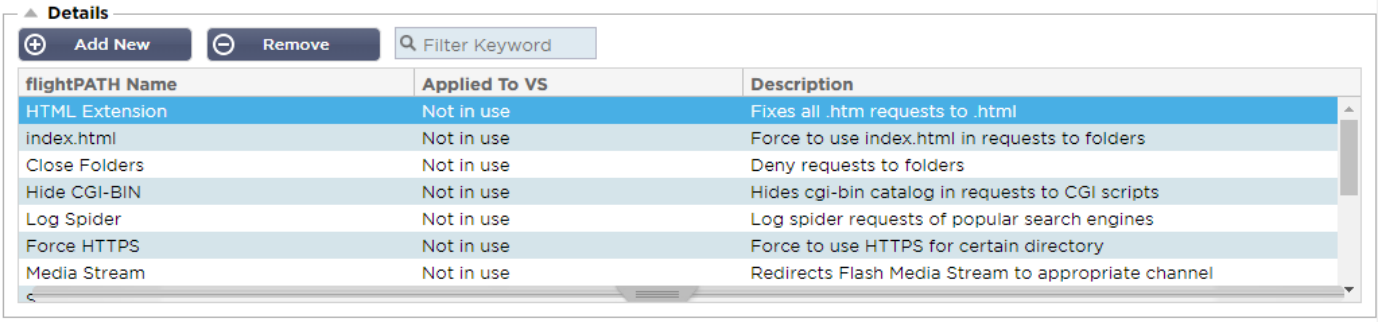
flightPATH é a tecnologia de gestão de tráfego incorporada no ADC. flightPATH permite que o senhor inspecione o tráfego HTTP e HTTPS em tempo real e execute ações com base nas condições.

As regras do flightPATH devem ser aplicadas a um VIP quando objetos de PI são usados dentro das regras.

Uma regra de rota de vôo é composta de quatro elementos:

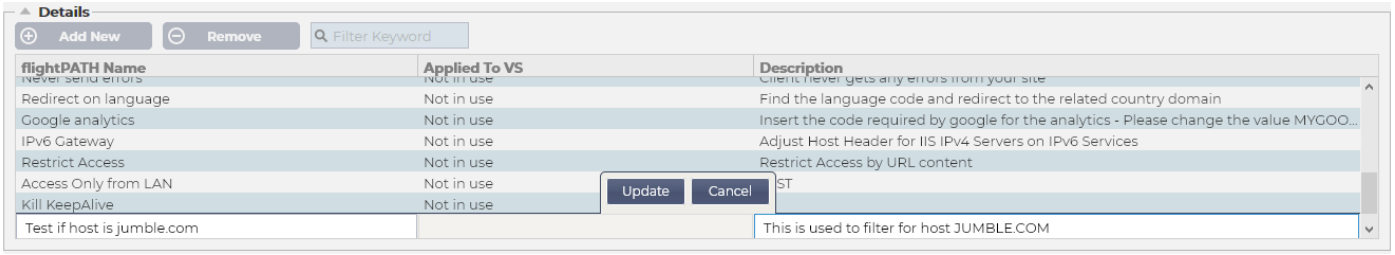
1. Detalhes, onde o senhor define o vôoPATH Nome e serviço ao qual ele está anexado.
2. Condição(ões) que pode(m) ser definida(s) e que faz(m) com que a regra seja acionada.
3. Avaliação que permite a definição de variáveis que podem ser usadas dentro das Ações
4. Ações que são usadas para administrar o que deve acontecer quando as condições são cumpridas

Detalhes



A seção de detalhes mostra as regras de vooPATH disponíveis. O senhor pode acrescentar novas regras do flightPATH e remover as definidas dessa seção.

Acrescentando uma nova regra de vooPATH



Campo	Descrição
FlightPATH Nome	Este campo é para o nome da regra flightPATH. O nome que o senhor fornece aqui aparece e é referenciado em outras partes do ADC.

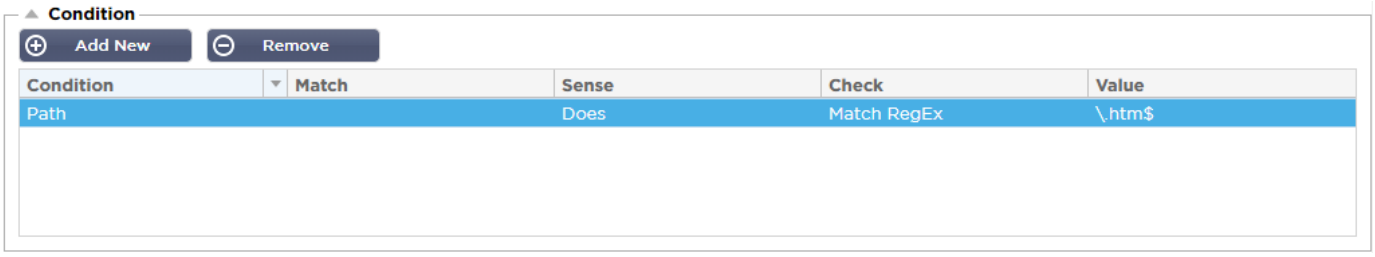
Aplicado ao VS	Esta coluna é somente de leitura e mostra o VIP ao qual é aplicada a regra flightPATH.
Descrição	Valor que representa uma descrição fornecida para fins de legibilidade.

Passos para acrescentar uma regra de vooPATH

1. Primeiro, clique no botão Adicionar novo, localizado na seção de detalhes.
2. Digite um nome para sua regra. Exemplo Auth2
3. Digite uma descrição de sua regra
4. Uma vez que a regra tenha sido aplicada a um serviço, o senhor verá a coluna Aplicada à autopopulação com um endereço IP e valor portuário
5. Não se esqueça de apertar o botão Atualizar para salvar suas mudanças ou, se cometer um erro, basta apertar cancelar e voltar ao estado anterior.

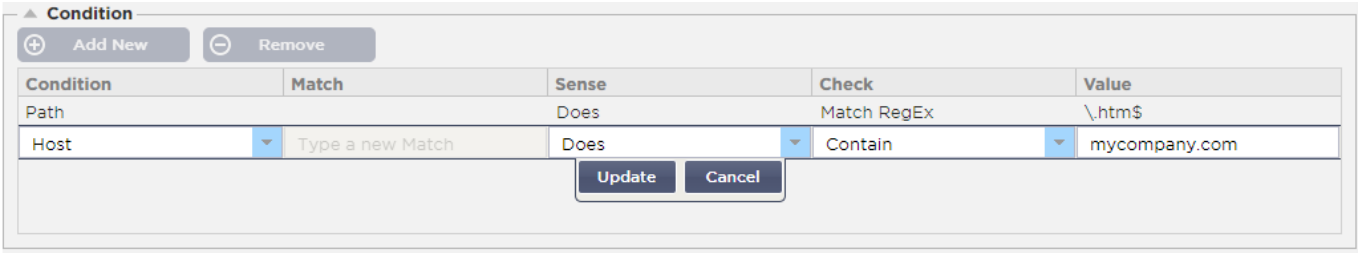
Condição

Uma regra de FlightPATH pode ter qualquer número de condições. As condições funcionam numa base AND, o que permite ao senhor estabelecer a condição sobre a qual a ação é desencadeada. Se o senhor quiser usar uma condição OR, crie uma regra flightPATH adicional e a aplique ao VIP na ordem correta.



O senhor também pode usar o RegEx selecionando a opção Match RegEx no campo Check e o valor do RegEx no campo Value. A inclusão da avaliação do RegEx amplia tremendamente a capacidade do FlightPATH.

Criação de uma nova condiçãoPATH de vôo



Condição

Fornecemos várias Condições como pré-definidas dentro do período de suspensão e cobrimos todos os cenários previstos. Quando novas Condições forem acrescentadas, elas estarão disponíveis através de atualizações do Jetpack.

As opções disponíveis são:

CONDIÇÃO	DESCRIÇÃO	EXEMPLO
<form>	Os formulários HTML são usados para passar dados a um servidor	Exemplo "o formulário não tem comprimento 0".
Localização da GEO	Compara o endereço IP de origem com os códigos de país ISO 3166	GEO Localização é igual a GB, OU GEO Localização é igual a Alemanha
Anfitrião	Anfitrião extraído do URL	www.mywebsite.com ou 192.168.1.1

Idioma	Idioma extraído do cabeçalho HTTP do idioma	Esta condição produzirá uma queda com uma lista de idiomas
Método	Abandono dos métodos HTTP	Desistência que inclui GET, POST, etc.
Origem PI	Se o representante a montante apoiar X-Forwarded-for (XFF), ele usará o verdadeiro endereço de origem	PI do cliente. Pode também usar múltiplos IPs ou sub-redes. 10.1.2.* é 10.1.2.0 /24 subnet10 10. 1.2.3|10.1.2.4 Utilização | para múltiplos IP's
Caminho	Caminho do site	/mywebsite/index.asp
POST	Método de solicitação de pós-venda	Verificar os dados que estão sendo carregados em um website
Consulta	Nome e valor de uma consulta, e pode aceitar o nome da consulta ou um valor também	"Best=jetNEXUS" Onde a partida é melhor e o valor é edgeNEXUS
Query String	Toda a seqüência de perguntas após o ? caráter	
Solicitação Cookie	Nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Pedido Cabeçalho	Qualquer cabeçalho HTTP	Referente, Usuário-Agente, De, Data
Versão do pedido	A versão HTTP	HTTP/1.0 OU HTTP/1.1
Órgão de resposta	Uma cadeia definida pelo usuário no corpo de resposta	Servidor UP
Código de resposta	O código HTTP para a resposta	200 OK, 304 Não modificado
Cookie de resposta	O nome de um cookie enviado pelo servidor	MS-WSMAN=afYfn1CDqqCDqUD::
Resposta Cabeçalho	Qualquer cabeçalho HTTP	Referente, Usuário-Agente, De, Data
Versão de resposta	A versão HTTP enviada pelo servidor	HTTP/1.0 OU HTTP/1.1
Fonte IP	Ou o IP de origem, IP do servidor proxy, ou algum outro endereço IP agregado	ClientIP , Proxy IP, Firewall IP. Pode também usar múltiplos IP e sub-redes. O senhor deve escapar dos pontos, pois estes são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Jogo

O campo Partida pode ser ou um valor de descida ou um valor de texto e pode ser definido de acordo com o valor no campo Condição. Por exemplo, se a Condição for definida como Anfitrião, o campo de partida não está disponível. Se a Condição for definida como <form>, o campo Correspondência é mostrado como um campo de texto, e se a Condição for POST, o campo Correspondência é apresentado como um drop-down contendo valores pertinentes.

As opções disponíveis são:

MATCH	DESCRIÇÃO	EXEMPLO
Aceitar	Tipos de conteúdo que são aceitáveis	Aceitar: texto/plainar
Aceitação-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>
Aceitação-Língua	Idiomas aceitáveis para a resposta	Aceitação-Língua: en-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Gama de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ====
Carga-To	Contém informações sobre os custos da aplicação do método solicitado	
Codificação do conteúdo	O tipo de codificação utilizada	Codificação do conteúdo: gzip
Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (8-bit bytes)	Comprimento do conteúdo: 348
Content-Type	O tipo mímico do corpo do pedido (usado com pedidos POST e PUT)	Tipo de conteúdo: aplicação/x-www-form-urlencoded
Cookie	Um cookie HTTP previamente enviado pelo servidor com o Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Data = "Data" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, muitas vezes uma digestão de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de e-mail do usuário que faz o pedido	De: user@example.com
Se-Modificado - desde	Permite que um 304 Não modificado seja devolvido se o conteúdo não for modificado.	Se-Modified-Since: Sábado, 29 de outubro de 1994 19:43:31 GMT
Última Modificação	A última data modificada para o objeto solicitado, no formato RFC 2822	Modificado por último: Ter, 15 de novembro de 1994 12:45:26 GMT
Pragma	Implementação: Cabeçalhos específicos que podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta aos pedidos.	Pragma: sem cache
Referência	Endereço da página web anterior, a partir da qual foi seguido um link para a página atualmente solicitada	Referência: 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; Versão=1
Agente-usuário	A seqüência do agente do usuário do agente do usuário	Agente-usuário: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)

Vary	Diz aos procuradores abaixo como combinar futuros cabeçalhos de pedidos para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova resposta do servidor de origem.	Vary: Agente-usuário
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 dos Sentidos é um campo booleano de queda e contém opções de "faz" ou "não faz".

Verifique

O campo Verificar permite o estabelecimento de valores de verificação em relação à Condição.

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

CHECK	DESCRIÇÃO	EXEMPLO
Existente	Isto não se preocupa com os detalhes da condição apenas que ela existe/não existe.	Anfitrião - Existente
Início	O cordel começa com o Valor	Caminho - Começa - /secura
Fim	O fio termina com o Valor	Caminho - Faz - Termina - .jpg
Conter	O fio contém o Valor	Solicitar Cabeçalho - Aceitar - Conter - Imagem
Igual	O fio faz igualar o valor	Anfitrião - Does - Equal - www.jetnexus.com
Ter comprimento	O fio tem um comprimento do valor	Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
Partida RegEx	Permite que o senhor entre com uma expressão regular compatível com Perl	Origem IP - Does - Match Regex - 10\...* | 11\...*

Passos para acrescentar uma Condição

É muito fácil acrescentar uma nova condição de vooPATH Condition. Um exemplo é mostrado acima.

1. Clique no botão Add New dentro da área Condition.
2. Escolha uma condição a partir da caixa drop-down. Tomemos como exemplo a Anfitriã. O senhor também pode digitar no campo, e o ADC mostrará o valor em uma caixa suspensa.
3. Escolha um Sentido. Por exemplo, Será que
4. Escolha um cheque. Por exemplo, Conter
5. Escolha um valor. Por exemplo, mycompany.com

Condition

Add New | Remove

Condition	Match	Sense	Check	Value
Request Header		Does	Contain	image
Host		Does	Equal	www.imagepool.com

O exemplo acima mostra que há duas condições que ambas têm de ser VERDADEIRAS para que a regra seja completada

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

Avaliação

A capacidade de acrescentar variáveis definíveis é uma capacidade convincente. O ADC oferece regularmente essa capacidade usando opções de script ou de linha de comando que não são ideais para ninguém. O ADC permite que o senhor defina qualquer número de variáveis usando uma GUI fácil de usar, como mostrado e descrito abaixo.

A definição variável flightPATH compreende quatro entradas que precisam ser feitas.

- Variável - este é o nome da variável
- Fonte - uma lista drop-down de possíveis pontos de origem
- Detalhe - selecionar valores de um drop-down ou datilografados manualmente.
- Valor - o valor que a variável detém e pode ser um valor alfanumérico ou um RegEx para afinação.

Variáveis embutidas:

As variáveis embutidas já foram codificadas, de modo que o senhor não precisa criar uma entrada de avaliação para elas.

O senhor pode usar qualquer uma das variáveis listadas abaixo na seção Ação.

A explicação para cada variável está localizada na tabela "Condição" acima.

- Método = $method$
- Caminho = $caminho$$
- Querystring = $querystring $querystring
- Sourceip = $sourceip$
- Código de resposta (o texto também incluía "200 OK") = $respasse$
- Anfitrião = $host$
- Versão = $version$
- Clientport = $clientport$
- Clientip = $clientip$
- Geolocalização = $geolocalização$".

ACÇÃO	TARGET
Ação = Redirecionar 302	Alvo = HTTPs://$host$/404.html
Ação = Log	Alvo = Um cliente de $sourceip$:$sourceport$ acabou de fazer um pedido $path$ página

Explicação:

- Um cliente que acesse uma página que não existe seria normalmente apresentado com a página de erro 404 do navegador.
- Em vez disso, o usuário é redirecionado para o nome original da hostname que usou, mas o caminho incorreto é substituído por 404.html
- Uma entrada é acrescentada ao Syslog dizendo: "Um cliente de 154.3.22.14:3454 acaba de pedir a página errada.html".

Ação

A próxima etapa do processo é acrescentar uma ação associada com a regra e a condição do FlightPATH.

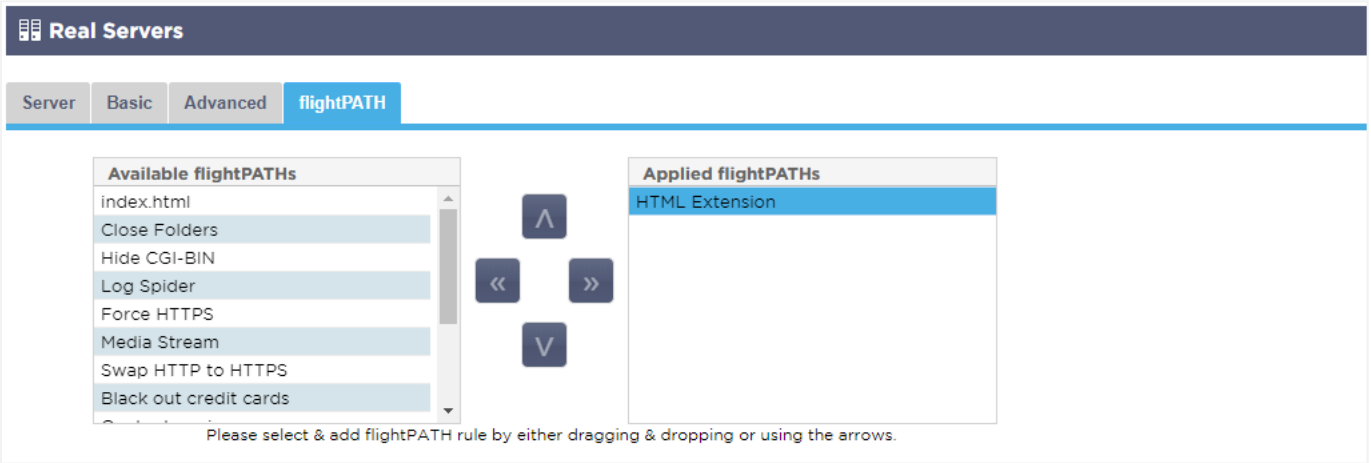
Neste exemplo, queremos reescrever a parte do caminho do URL para refletir o URL digitado pelo usuário.

- Clique em Add New
- Escolha Rewrite Path no menu suspenso Action
- No campo Alvo, digite em $path$/myimages
- Clique em Atualizar

Esta ação acrescentará /myimages ao caminho, de modo que a URL final se torna www.imagepool.com/myimages.

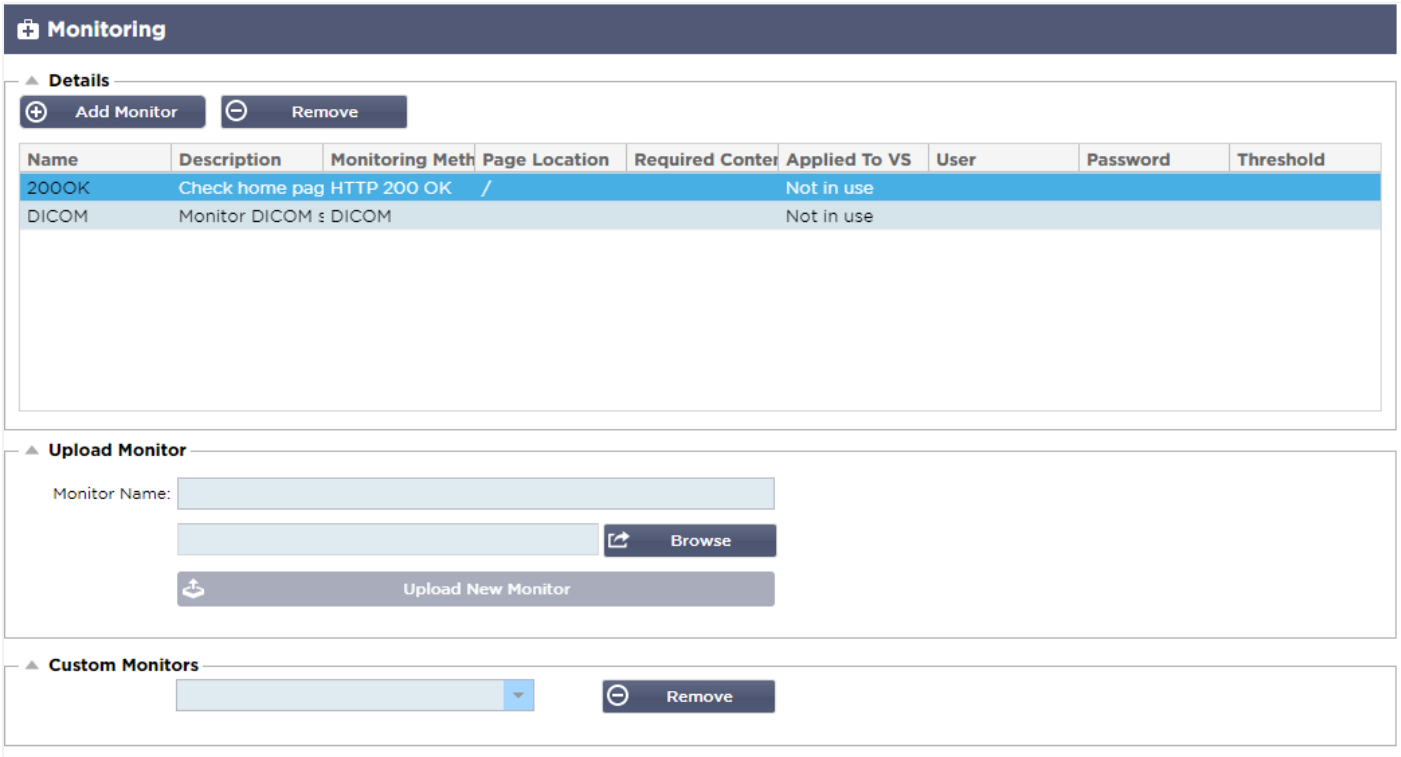
Aplicação da regra flightPATH

A aplicação de qualquer regra flightPATH é feita dentro da aba flightPATH de cada VIP/VS.



- Navegue até Services > IP Services e escolha o VIP ao qual deseja atribuir a regra flightPATH.
- O senhor verá a lista do Real Server, abaixo
- Clique na guia flightPATH
- Selecione a regra flightPATH que o senhor configurou ou uma das regras pré-construídas suportadas. O senhor pode selecionar várias regras de flightPATH, se necessário.
- Arraste e solte o conjunto selecionado para a seção de PAATOS DE VOOO Aplicados ou clique no botão >> seta.
- A regra será transferida para o lado certo e automaticamente aplicada.

Monitores de servidores reais



Quando o equilíbrio de carga é estabelecido, é útil monitorar a saúde dos servidores reais e as aplicações que neles funcionam. Por exemplo, em servidores web, o senhor pode criar uma página específica que pode ser usada para monitorar o estado ou usar um dos outros sistemas de monitoramento que o ADC possui.

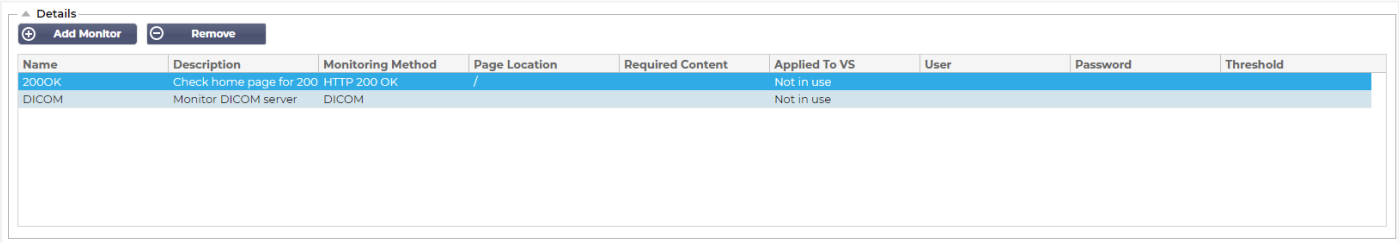
A página Biblioteca > Monitores de Servidores Reais permite ao senhor acrescentar, visualizar e editar monitoração personalizada. Esses são os "Cheques de Saúde" do servidor Layer 7 e selecioná-los no campo Monitoramento do servidor dentro da guia Básico do serviço Virtual que o senhor definir.

A página dos Verdadeiros Monitores do Servidor está dividida em três seções.

- Detalhes
- Upload
- Monitores personalizados

Detalhes

A seção de detalhes é usada para acrescentar novos monitores e para remover os que o senhor não precisa. O senhor também pode editar um monitor existente clicando duas vezes sobre ele.



Nome

Nome de sua escolha para seu monitor.

Descrição

Descrição textual para este Monitor, e recomendamos que o melhor é torná-la o mais descritiva possível.

Método de monitoramento

Escolha o método de monitoramento a partir da lista suspensa. As opções disponíveis são:

Método de monitoramento	Descrição	Exemplo
HTTP 200 OK	É feita uma conexão TCP com o Real Server. Após feita a conexão, um breve pedido HTTP é enviado ao Real Server. Uma resposta HTTP do servidor é aguardada e é então verificada para o código de resposta "200 OK". Se o código de resposta "200 OK" for recebido, o Servidor Real é considerado como estando instalado e funcionando. Se, por qualquer razão, o código de resposta "200 OK" não for recebido, incluindo timeouts ou falha na conexão, então o Servidor Real é considerado como desligado e indisponível. Esse método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e HTTP Acelerado. Entretanto, se um tipo de serviço Layer 4 estiver em uso para um servidor HTTP, ele ainda poderá ser usado se o SSL não estiver em uso no Servidor Real ou se for tratado apropriadamente pela instalação "Content SSL".	Nome: 200OK Descrição: Verifique o website de produção Método de monitoramento: HTTP 200 OK Localização da página: /main/index.html OU HTTP://www.edgenexus.io/main/index.html Conteúdo necessário: N/A
Resposta HTTP	Uma conexão e uma solicitação/resposta HTTP é feita ao Real Server e verificada como explicado no exemplo anterior. Mas ao invés de verificar se há um código de resposta "200 OK", o cabeçalho da resposta HTTP é verificado quanto ao conteúdo do texto personalizado. O texto pode ser um cabeçalho completo, parte de um cabeçalho, uma linha de parte de uma página, ou apenas uma palavra. Se o texto for encontrado, o Real Server é considerado como estando em funcionamento. Esse método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e HTTP Acelerado. Entretanto, se um tipo de serviço Layer 4 estiver em uso para um servidor HTTP, ele ainda poderá ser usado se o SSL não estiver em uso no Servidor Real ou se for tratado apropriadamente pela instalação "Content SSL".	Nome: Servidor Up Descrição: Verifique o conteúdo da página para "Server Up". " Método de monitoramento: Resposta HTTP Localização da página: /main/index.html OU HTTP://www.edgenexus.io/main/index.html Conteúdo necessário: Servidor Up

DICOM	Enviamos um eco DICOM usando o valor do título AE "Source Calling" na coluna de conteúdo exigido. O senhor também pode definir o valor do título da AE "Destination Calling" na seção Notes de cada servidor. O senhor pode encontrar a coluna Notes dentro dos Serviços IP. -Virtual Services--Server page.	Nome: DICOM Descrição: L7 exame de saúde para o serviço DICOM Método de monitoramento: DICOM Localização da página: N/A Conteúdo necessário: Valor AET
TCP Fora de Banda	O método TCP Out of Band é como um TCP Connect, exceto que o senhor pode especificar o porto que deseja monitorar na coluna de conteúdo exigido. Esse porto normalmente não é o mesmo que o porto de tráfego e é usado quando o usuário deseja ligar serviços juntos.	Nome: TCP Fora de Banda Descrição: Monitor fora do porto de Banda/Trafficio Localização da página: N/A Conteúdo necessário: 555
Monitor TCP Multi-Portas	Esse método é como o acima mencionado, exceto pelo fato de que o senhor pode ter vários portos diferentes. O monitor só é considerado bem-sucedido se todos os portos especificados na seção de conteúdo exigido responderem corretamente.	Nome: Monitor Multi-Portas Descrição: Monitorar múltiplos portos para o sucesso Localização da página: N/A Conteúdo necessário: 135,59534,59535

Localização da página

URL Localização da página para um monitor HTTP. Esse valor pode ser um link relativo como /folder1/folder2/page1.html. O senhor também pode usar um link absoluto onde o site está vinculado ao nome da pessoa que o hospeda.

Conteúdo Requerido

Esse valor contém qualquer conteúdo que o monitor precisa detectar e utilizar. O valor aqui representado mudará de acordo com o método de monitoramento que for escolhido.

Aplicado ao VS

Esse campo é automaticamente preenchido com o IP/Porto do Serviço Virtual ao qual o monitor é aplicado. O senhor não poderá apagar nenhum Monitor que tenha sido usado com um Serviço Virtual.

Usuário

Alguns monitores personalizados podem usar esse valor junto com o campo de senha para fazer login em um servidor real.

Senha

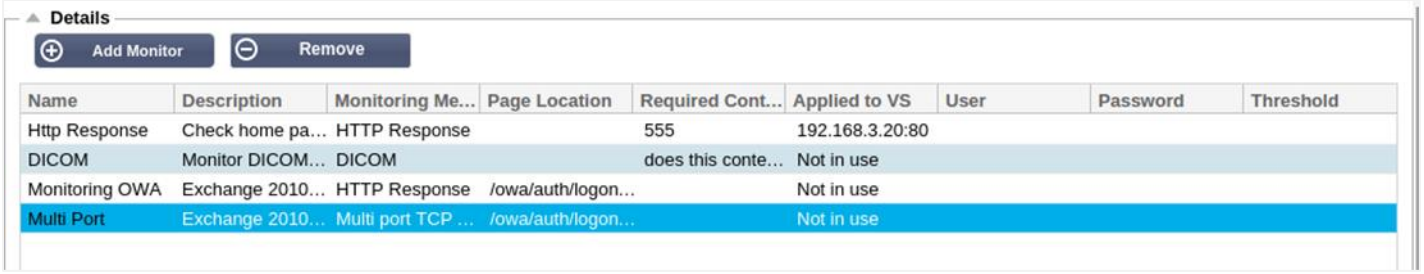
Alguns monitores personalizados podem usar esse valor junto com o campo Usuário para fazer login em um servidor real.

Limiar

O campo Threshold é um número inteiro geral usado em monitores personalizados onde um limite como o nível da CPU é exigido.

NOTA: Por favor, assegure-se de que a resposta do servidor de aplicação não seja uma resposta "em pedaços".

Exemplos de monitoramento de servidores reais



Upload Monitor

Haverá muitas ocasiões em que os usuários desejarão criar seus próprios monitores personalizados e esta seção permite que eles os enviem para o ADC.

Os monitores personalizados são escritos usando scripts PERL e têm uma extensão .pl do arquivo.

- Dar a seu monitor um nome para que o senhor possa identificá-lo na lista do Método de Monitoramento
- Procurar o arquivo .pl
- Clique em Upload Novo Monitor
- Seu arquivo será carregado no local correto e será visível como um novo método de monitoramento.

Monitores personalizados

Nesta seção, o senhor pode ver os monitores personalizados carregados e removê-los se não forem mais necessários.

- Clique na caixa drop-down
- Selecione o nome do monitor personalizado
- Clique Remover
- Seu monitor personalizado não será mais visível na lista do Método de Monitoramento

Criação de um roteiro personalizado do Monitor Perl

CUIDADO: Esta seção é destinada a pessoas com experiência no uso e escrita em Perl

Esta seção mostra ao senhor as ordens que pode usar dentro de seu script Perl.

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

Os seguintes são obrigatórios:

- #Monitor-Nome
- uso rigoroso;
- usar advertência;

Os roteiros do Perl são executados em um ambiente CHROOTED. Eles freqüentemente chamam de outra aplicação, como WGET ou CURL. Às vezes eles precisam ser atualizados para uma característica específica, como o SNI.

Valores dinâmicos

- meus $host = $_[0]; - Este usa o "Endereço" da seção de Serviços de IP--Real Server
- meu porto = $_[1]; - Este usa o "Porto" da seção de Serviços de PI--Real Server
- meu conteúdo = $_[2]; - Isto usa o valor "Conteúdo Requerido" da Biblioteca - Seção de Monitoramento do Servidor Real
- minhas $notes = $_[3]; - Isto usa a coluna "Notes" na seção "Real Server" do IP Services
- meus $page = $_[4]; - Isto usa os valores de "Page Location" da Biblioteca - seção Monitor do Servidor Real
- meu $user = $_[5]; - Isto usa o valor "Usuário" da Biblioteca - seção Monitor do Servidor Real
- minhas $password = $_[6]; - Isto usa o valor "Password" da biblioteca - seção Real Server Monitor

Os cheques de saúde personalizados têm dois resultados

- Bem sucedido
  Return Value 1 Imprima
  uma mensagem de sucesso para SyslogMark
  the Real Server Online (fornecido em partida de COUNT)
- Sem sucesso
  Return Value 2 Imprima
  uma mensagem dizendo Unsuccessful to SyslogMark
  the Real Server Offline (provided OUT Count match)

Exemplo de um Monitor de Saúde Personalizado

```
#Monitor-Nome HTTPS_SNI
uso rigoroso:
usar advertências;
# O nome do monitor como acima é exibido no drop-down dos cheques de saúde disponíveis
# Há 6 valores passados a este roteiro (ver abaixo)
# O roteiro retornará os seguintes valores
# 1 é o teste é bem sucedido
# 2 se o teste não for bem sucedido sub-monitor
{
meu Shost=      $_[0]; #### Host IP ou nome
my Sport=       $_[1]; #### Host Port
meu Scontent= $_[2]; #### Conteúdo a procurar (na página web e cabeçalhos HTTP)
meus Snotes=  $_[3]; #### Nome do anfitrião virtual
meu Spage=      $_[4]; #### A parte do URL após o endereço do anfitrião
meu Suser=      $_[5]: ### domínio/usemame (opcional)
minha senha Spassword=          $_[6]; #### senha (opcional)
meus $resolve;
meus $auth      =;
```

```
se ($port)
{
        $resolve = "$notes:$port:$host":
}
senão {\i1}
        $resolve = "$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}${page} 2>&1';
if(join(""@lines)=~/$content/)
        {
        print "HTTPs://$notes}${page} procurando - $content - Health check successful.\n";
        devolução(1);
        }
senão
        {
        print "HTTPs://${notes}${page} procurando - $content - Health check failed.\n";
        retorno(2)
        }
}
monitor(@ARGV):
```

NOTA: Acompanhamento personalizado - O uso de variáveis globais não é possível. Uso apenas de variáveis locais - variáveis definidas dentro de funções

Certificados SSL

Para usar com sucesso o balanceamento de carga de Camada 7 com servidores que usam conexões criptografadas usando SSL, o ADC deve estar equipado com os certificados SSL usados nos servidores alvo. Essa exigência é para que o fluxo de dados possa ser descriptografado, examinado, gerenciado e depois re-encriptado antes de ser enviado para o servidor alvo.

Os certificados SSL podem variar de certificados autoassinados que o ADC pode gerar até os certificados tradicionais (inclusive wildcard) disponíveis em fornecedores confiáveis. O senhor também pode usar certificados de domínio assinados que são gerados a partir do Active Directory.

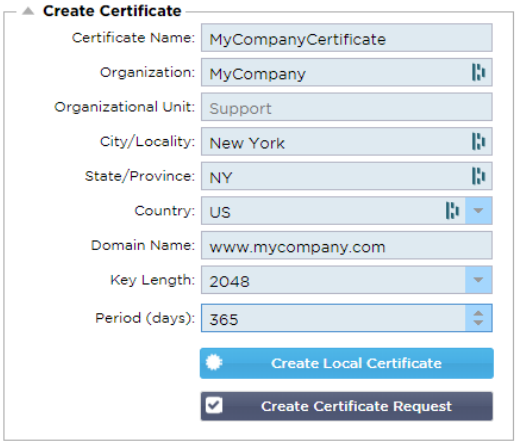
O que o ADC faz com o Certificado SSL?

O ADC pode executar regras de gestão de tráfego (flightPATH) dependendo do que os dados contêm. Essa gestão não pode ser feita com dados criptografados por SSL. Quando o ADC tem que inspecionar os dados, precisa primeiro descriptografá-los, e para isso, precisa ter o certificado SSL usado pelo servidor. Uma vez descriptografados, o ADC poderá então examinar e executar as regras do flightPATH. Depois disso, os dados serão reencriptados usando o certificado SSL e enviados para o servidor real final.

Criar certificado

Embora o ADC possa usar um certificado SSL de confiança mundial, ele pode gerar um certificado SSL autoassinado. O SSL Auto-assinado é perfeito para os requisitos de equilíbrio de carga interna. No entanto, suas políticas de TI podem exigir um certificado CA de confiança ou de domínio.

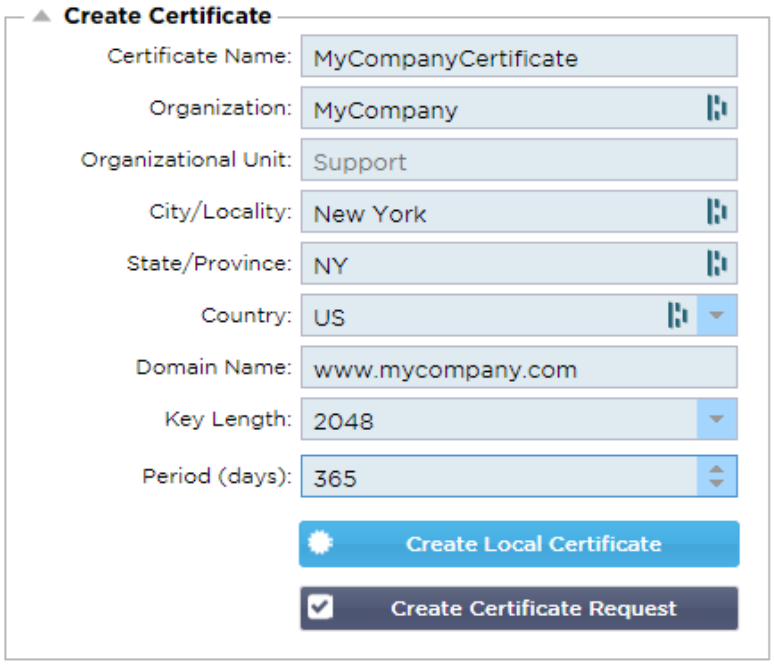
Como criar um certificado local SSL



- Preencher todos os detalhes como o exemplo acima
- Clique em Create Local Certificate (Criar certificado local)
- Uma vez que o senhor tenha clicado nisso, poderá aplicar o certificado a um **SERVIÇO VIRTUAL.**

Criar um Pedido de Certificado (CSR)

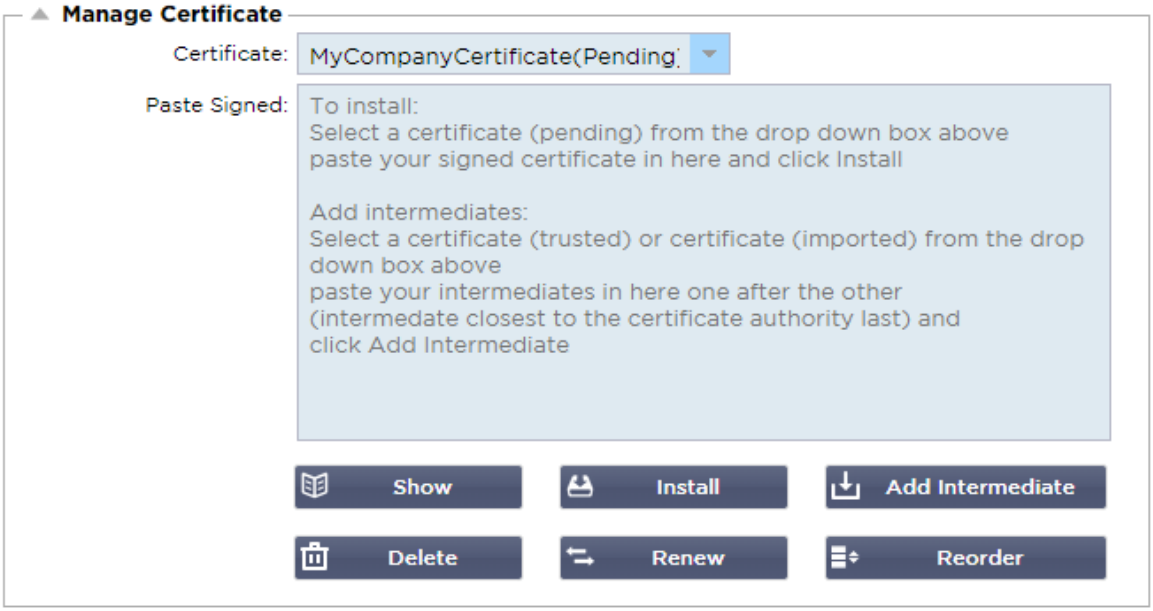
Quando o senhor precisar obter um SSL de confiança global de um fornecedor externo, precisará gerar um CSR para gerar o certificado SSL.



Preencha o formulário como mostrado acima com todos os dados relevantes, e depois clique no botão Solicitação de Certificado. Será apresentado ao senhor o popup correspondente aos dados que forneceu.

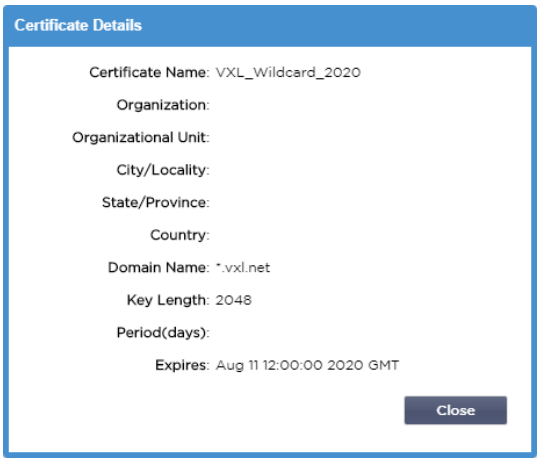
O senhor precisará cortar e colar o conteúdo em um arquivo TEXT e nomeá-lo com uma extensão do arquivo CSR, por exemplo, *mycert.csr*. Esse arquivo CSR precisará então ser fornecido à autoridade certificadora do senhor para criar o certificado SSL.

Gerenciar Certificado



Esta subseção contém várias ferramentas para permitir a administração dos certificados SSL que o senhor possui dentro da ADC.

Mostrar

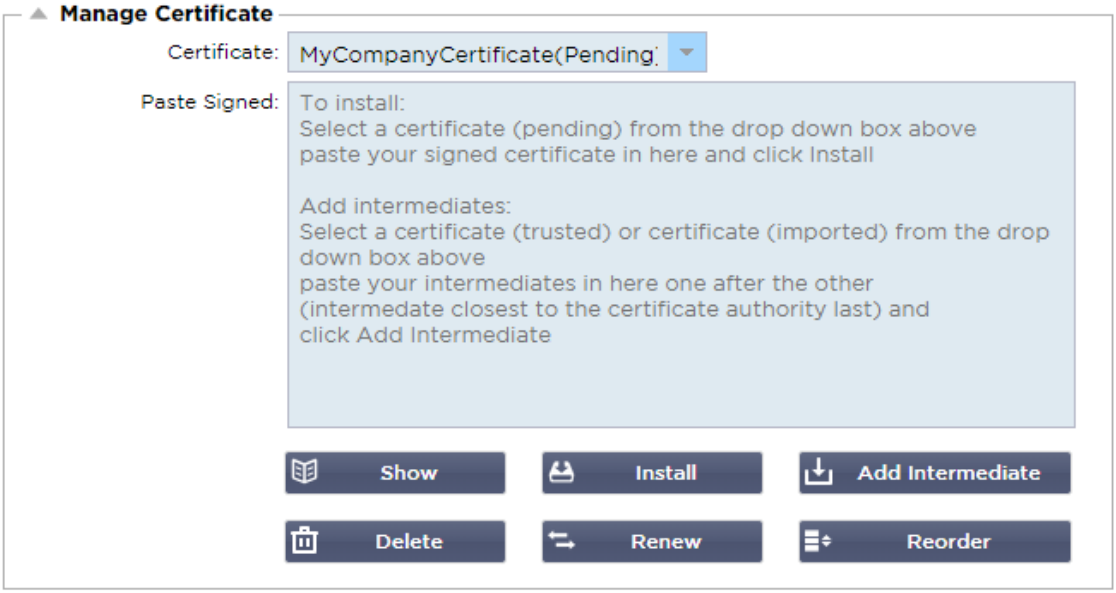


Pode haver ocasiões em que o senhor deseje examinar os detalhes de um certificado SSL instalado.

- Selecione o certificado a partir do menu suspenso
- Clique no botão Mostrar
- O popup mostrado abaixo será apresentado com os detalhes do certificado.

Instalação de um certificado

Uma vez que o senhor obtenha o certificado da Autoridade Certificadora Fiduciária, precisará compará-lo ao CSR gerado e instalá-lo dentro da ADC.



- Selecione um certificado que o senhor tenha gerado nas etapas acima. Haverá um status (pendente) fixado para o item de linha. No exemplo, o MyCompanyCertificate é mostrado na imagem acima.
- Abrir o arquivo do certificado em um editor de texto
- Copiar todo o conteúdo do arquivo para a prancheta
- Cole o conteúdo do certificado SSL assinado que o senhor recebeu da autoridade de confiança no campo marcado "Paste Signed" (Colar Assinado).
- O senhor também pode colar nos Intermediários abaixo disso, tendo o cuidado de seguir a ordem correta:
    1. (TOPO) Seu Certificado assinado
    2. (2º De cima) Intermediário 1

3. (3º de cima) Intermediário 2
4. (Fundo) Intermediário 3
5. Autoridade do Certificado de Raiz Não há necessidade de acrescentar isso, uma vez que eles existem nas máquinas dos clientes.
   (o ADC também contém um pacote de raiz para reencriptação onde atua como cliente para um servidor real).

- Clique Instalar
- Uma vez instalado o certificado, o senhor deve ver o status (Trusted) ao lado de seu certificado

Se o senhor cometeu um erro ou entrou com a ordem intermediária errada, então selecione o Certificado (Trusted) e acrescente os certificados (inclusive o certificado assinado) novamente na ordem correta e clique em Install

Acrescentar Intermediário

Ocasionalmente, é necessário acrescentar certificados intermediários separadamente. Por exemplo, o senhor pode ter importado um certificado que não possui os intermediários.

- Destacar um Certificado (de confiança) ou certificado (importado)
- Colar os intermediários um abaixo do outro, cuidando para que o intermediário mais próximo da autoridade do Certificado seja colado por último.
- Clique em Add Intermediate (Adicionar intermediário).

Se o senhor cometer um erro com a ordem, poderá repetir o processo e acrescentar novamente os intermediários. Essa ação só sobregravará os intermediários anteriores.

Eliminar um certificado

O senhor pode apagar um certificado usando o botão Apagar. Uma vez eliminado, o certificado será removido inteiramente do ADC e precisará ser substituído, e então reaplicado aos Serviços Virtuais, se necessário, novamente.

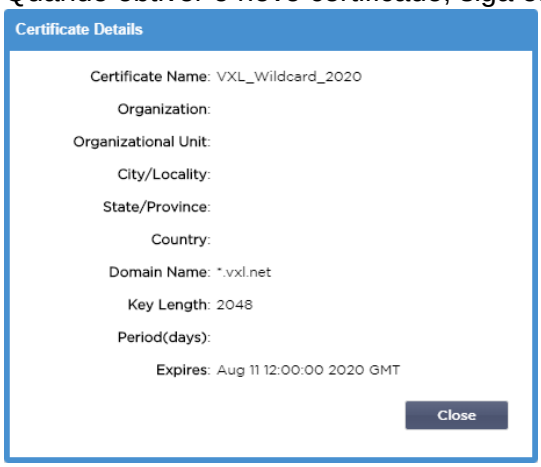
Nota: Queira certificar-se de que o certificado não esteja anexado a um VIP operacional antes de apagá-lo.

Renovar um certificado

O botão de renovação permite ao senhor obter um novo pedido de assinatura de certificado. Essa ação é necessária quando o certificado está para expirar e precisa ser renovado.

- Selecione um certificado da lista suspensa; você pode escolher qualquer certificado com o status (Pendente), (Confiável), ou (Importado)
- Clique Renovar
- Copiar os novos dados do CSR para que o senhor possa obter um novo certificado

- Quando obtiver o novo certificado, siga os passos detalhados em **SHOW**



-
- Pode haver ocasiões em que o senhor deseje examinar os detalhes de um certificado SSL instalado.
- Selecione o certificado a partir do menu suspenso
- Clique no botão Mostrar
- O popup mostrado abaixo será apresentado com os detalhes do certificado.
- Instalação de um certificado.
- O novo e renovado certificado será agora instalado no ADC.

Importação de um certificado

Em muitos casos, as empresas corporativas precisarão usar seus certificados de domínio assinados como parte de seus regimes de segurança interna. Os certificados devem estar no formato PKCS#12, e as senhas invariavelmente protegem esses certificados.

A imagem abaixo mostra a subseção para a importação de um único certificado SSL.

- Dê a seu certificado um nome amigável. O nome o identifica nas listas de suspensões usadas no ADC. Não precisa ser o mesmo que o nome de domínio do certificado, mas deve ser alfanumérico, sem espaços. Não são permitidos outros caracteres especiais além de _ e - são permitidos.
- Digite a senha que você usou para criar o certificado PKCS#12
- Procurar o {certificado}.pfx
- Clique Importar.
- Seu certificado estará agora nos menus suspensos relevantes do SSL dentro do ADC

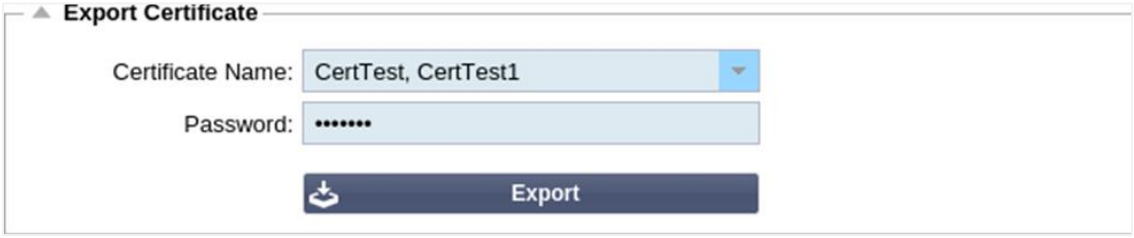
Importação de certificados múltiplos

Esta seção permite ao senhor importar um arquivo JNBK que contém vários certificados. Um arquivo JNBK é criptografado e produzido pela ADC quando da exportação de certificados múltiplos.

- Procure seu arquivo JNBK - o senhor pode criar um desses documentos exportando vários certificados
- Digite a senha que usou para criar o arquivo JNBK
- Clique Importar.
- Seus certificados estarão agora nos menus suspensos relevantes do SSL dentro do ADC

Exportação de um certificado

De tempos em tempos, o senhor poderá desejar exportar um dos certificados detidos na ADC. O ADC foi dotado da capacidade para fazer isso.



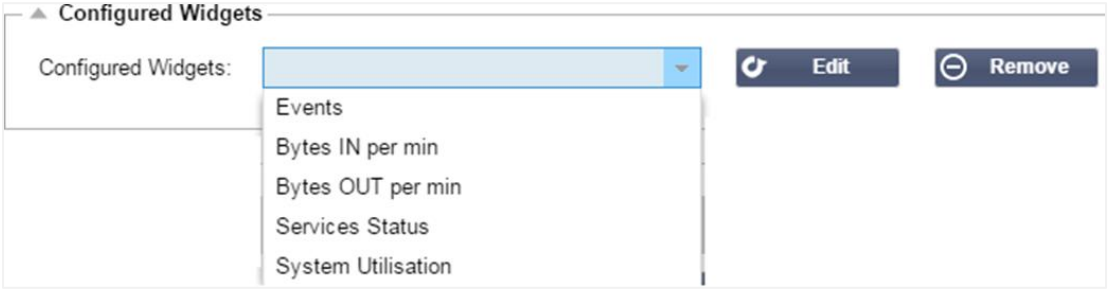
- Clique no certificado ou certificados que o senhor deseja instalar. Todos os senhores podem clicar na opção Todos para selecionar todos os certificados listados.
- Digite uma senha para proteger o arquivo exportado. A senha deve ter pelo menos seis caracteres de comprimento. Cartas, números, e certos símbolos podem ser usados. Os seguintes caracteres **não** são aceitáveis: < > " ( ) ; \ A3 % & ( ) ; \ A3 % &
- Clique Exportar
- Quando o senhor estiver exportando um único certificado, o arquivo resultante será denominado sslcert_{certname}.pfx. Por exemplo, sslcert_Test1Cert.pfx
- No caso de uma exportação com vários certificados, o arquivo resultante será um arquivo JNBK. O nome do arquivo será sslcert__pack.jnbk.

Nota: Um arquivo JNBK é um arquivo de container criptografado produzido pela ADC e válido apenas para importação para a ADC.

Widgets

A página Biblioteca > Widgets permite que o senhor configure vários componentes visuais leves exibidos em seu painel personalizado.

Widgets configurados

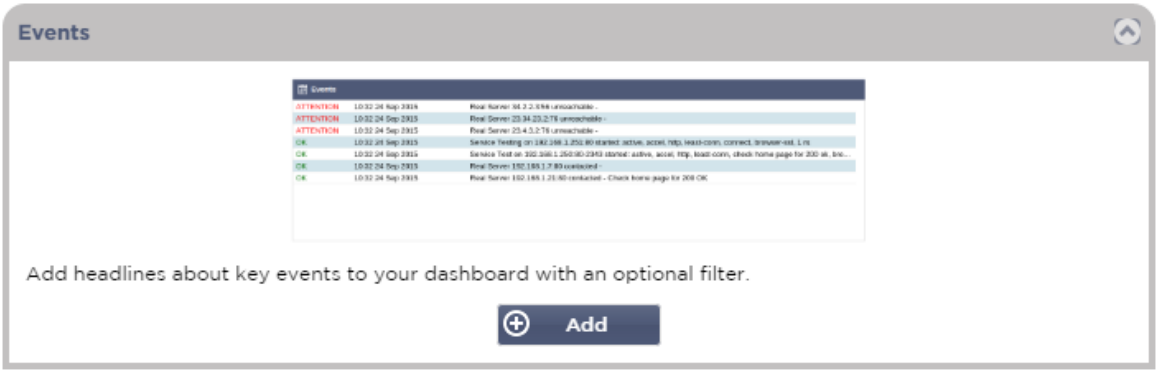


A seção Widgets configurados permite ao senhor ver, editar ou remover quaisquer widgets criados a partir da seção de widgets disponíveis.

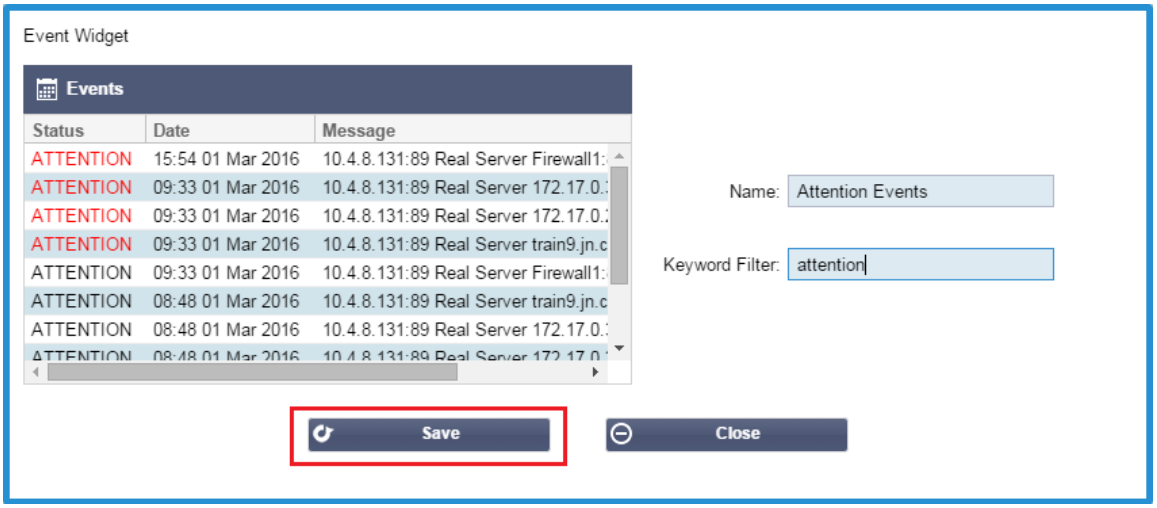
Widgets disponíveis

Há cinco widgets diferentes fornecidos dentro do ADC, e o senhor pode configurá-los de acordo com suas necessidades.

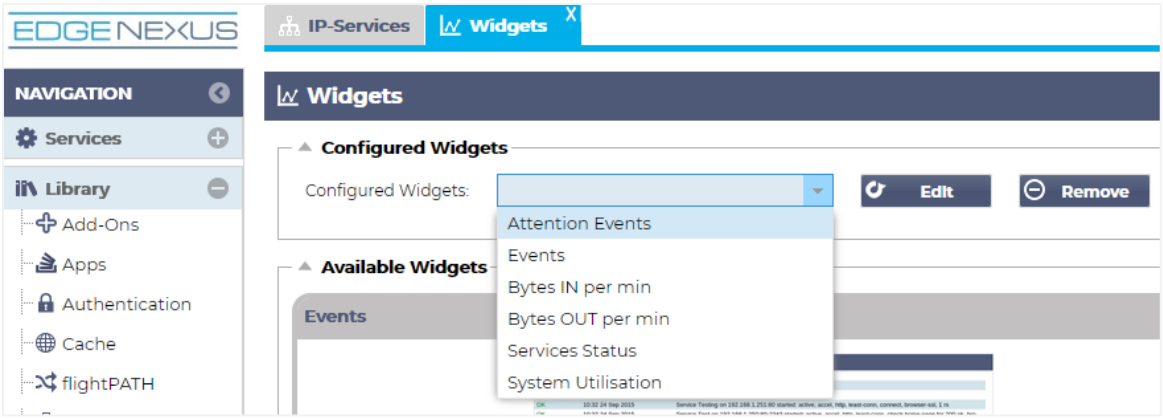
Os Eventos Widget



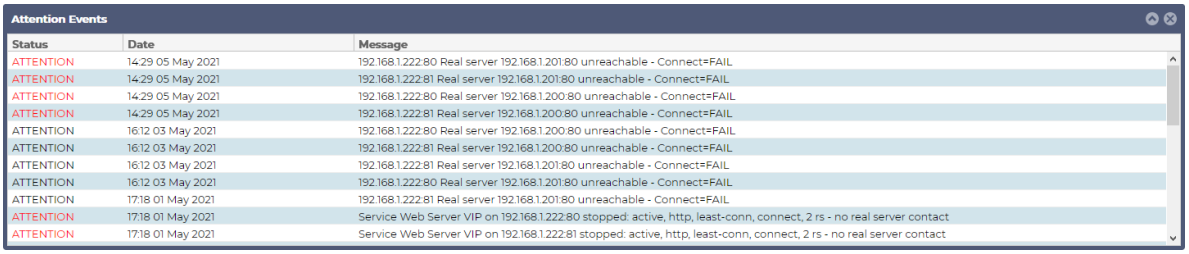
- Para acrescentar um evento ao widget Events, clique no botão Add.
- Forneça um nome para seu evento. Em nosso exemplo, acrescentamos Eventos de Atenção como o nome do evento.
- Acrescente um filtro de palavras-chave. Acrescentamos também o valor de filtro de Atenção



- Clique em Salvar, depois Fechar
- O senhor verá agora um Widget adicional chamado Eventos de Atenção nos Widgets Configurados.

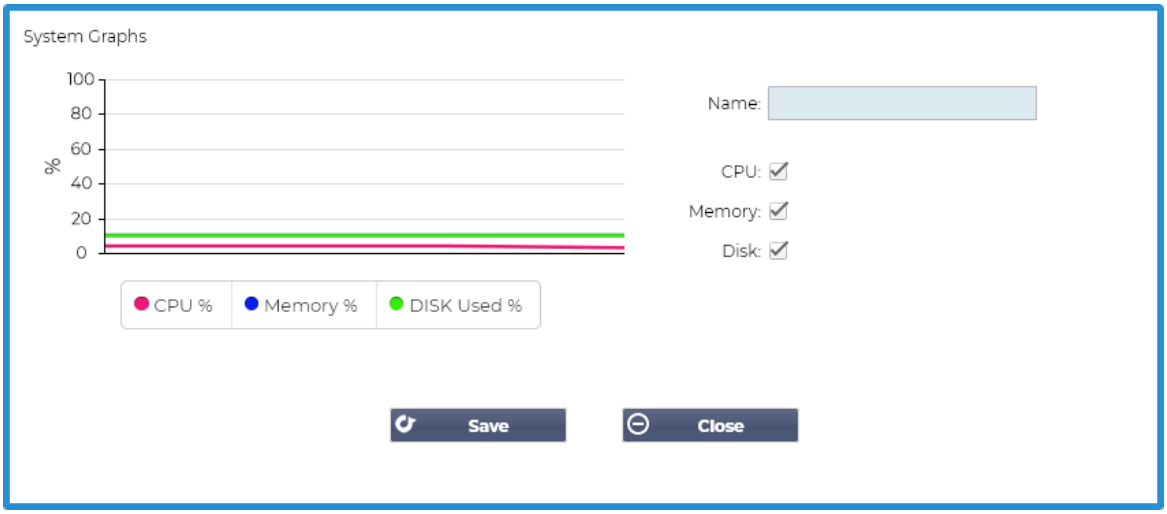


- O senhor pode ver que agora acrescentamos este widget na seção View > Dashboard.
- Selecione o widget Atenção Eventos para exibir isso dentro do Painel de Controle. Veja abaixo.



O senhor também pode pausar e reiniciar a transmissão de dados ao vivo clicando no botão Pausar dados ao vivo. Além disso, o senhor pode voltar ao painel padrão a qualquer momento, clicando no botão Default Dashboard (Painel padrão).

Os gráficos do sistema Widget

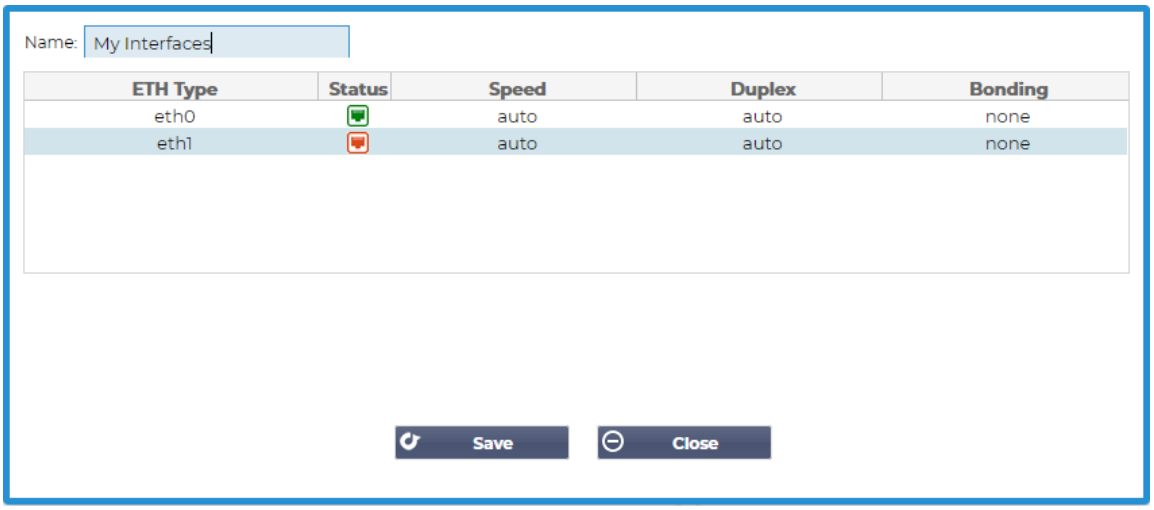


O ADC tem um widget gráfico de sistema configurável. Ao clicar no botão Adicionar no widget, o senhor pode acrescentar os seguintes gráficos de monitoramento a serem exibidos.

- CPU
- MEMÓRIA
- DISCO

Uma vez que o senhor os tenha acrescentado, eles estarão individualmente disponíveis no menu do Painel de Controle.

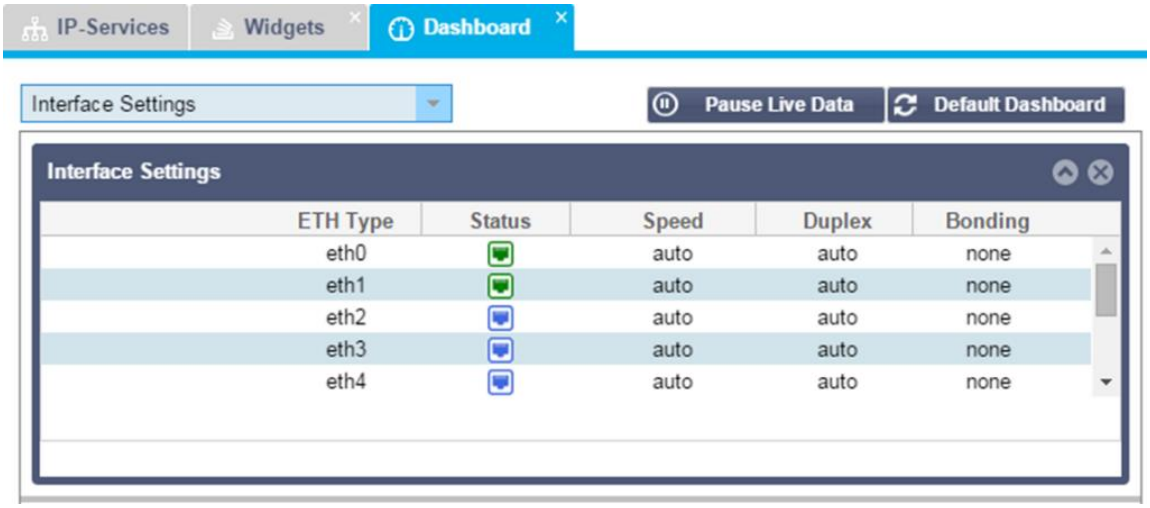
Interface Widget



O widget Interface permite ao senhor exibir os dados para a interface da rede escolhida, como ETH0, ETH1, e assim por diante. O número de interfaces disponíveis para adição depende de quantas interfaces de rede o senhor definiu para o dispositivo virtual ou provisionadas dentro do dispositivo de hardware.

Uma vez terminado, clique no botão Salvar e depois no botão Fechar.

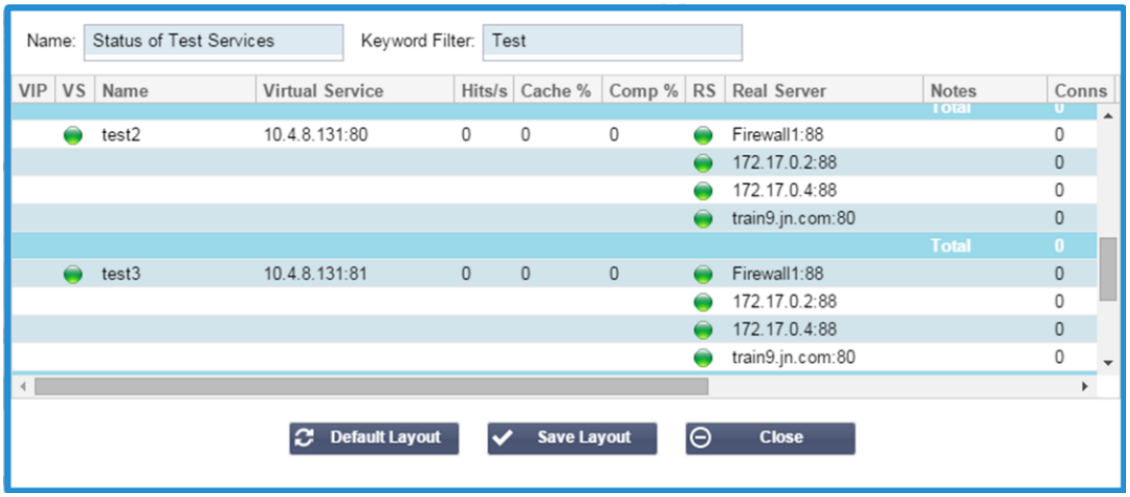
Selecione o Widget que acabou de personalizar a partir do menu suspenso widget dentro do Painel. O senhor verá uma tela como a que está abaixo.



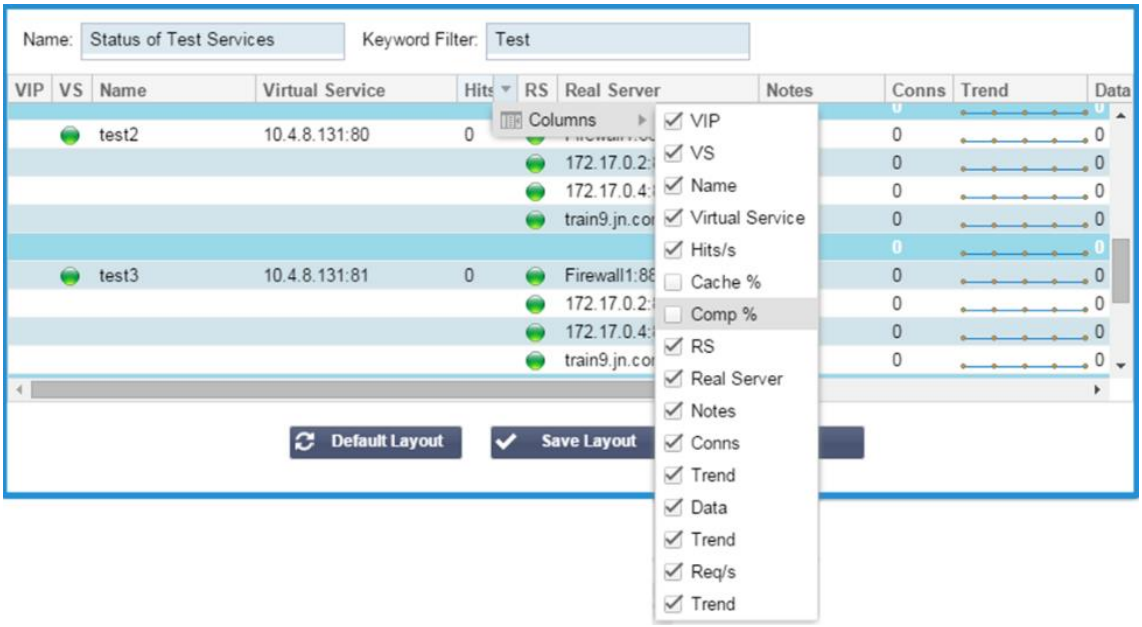
Status Widget

O widget Status permite que o senhor veja o equilíbrio da carga em ação. O senhor também pode filtrar a visão para mostrar informações específicas.

- Clique em Add.



- Digite um nome para o serviço que o senhor deseja monitorar
- O senhor também pode escolher quais colunas deseja exibir no widget.



- Quando estiver satisfeito, clique em Save, seguido de Close.
- O widget Status escolhido estará disponível na seção Dashboard.

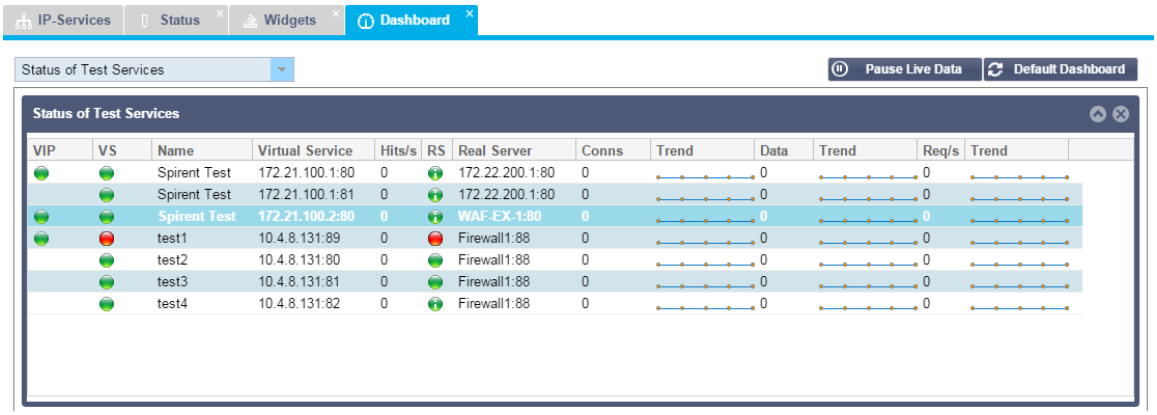
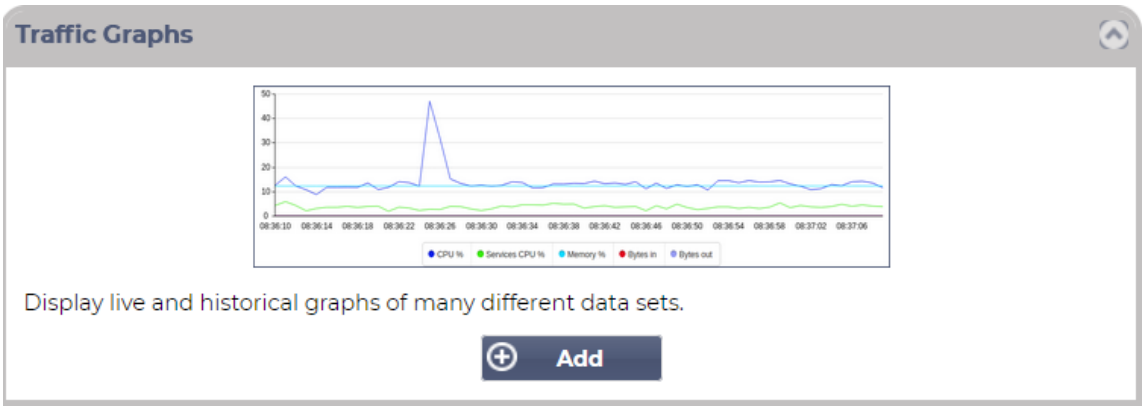


Gráfico de tráfego Widget

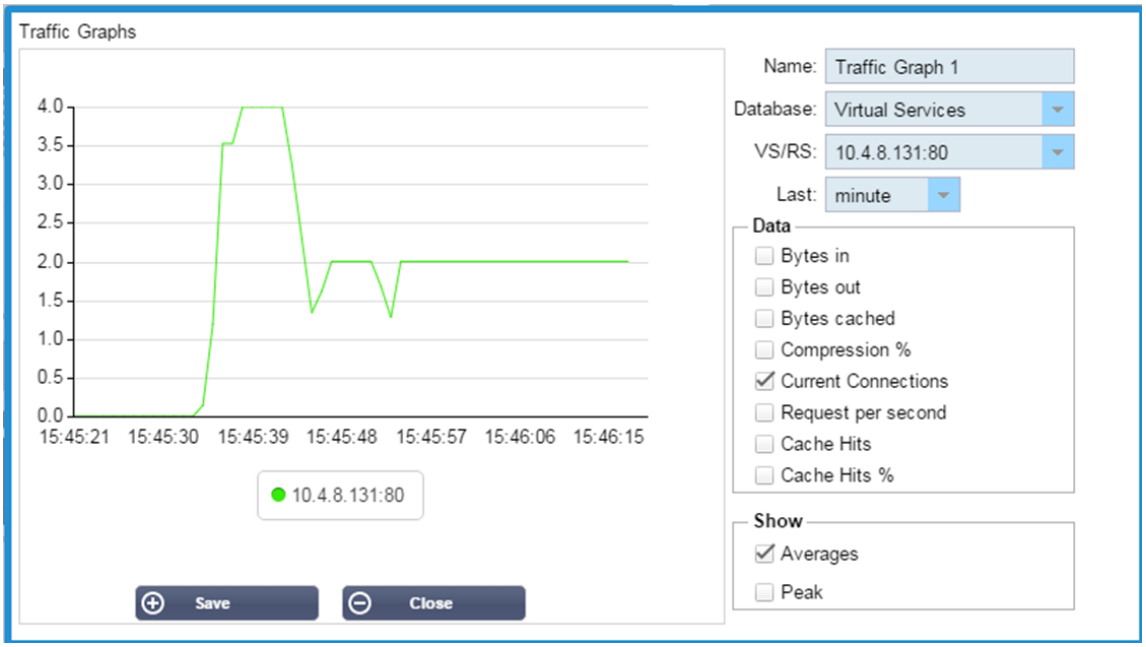
Esse widget pode ser configurado para mostrar dados de tráfego atuais e históricos por Serviços Virtuais e Servidores Reais. Além disso, o senhor pode ver os dados globais atuais e históricos do tráfego global



- Clique no botão Adicionar
- Diga seu widget.
- Escolha um banco de dados de Serviços Virtuais, Servidores Reais, ou Sistema.

- Se o senhor escolher os Serviços Virtuais, poderá selecionar um serviço virtual a partir do menu suspenso VS/RS.
- Escolha um cronograma a partir da última queda.
    - Ata - últimos 60 anos
    - Hora - dados agregados de cada minuto durante os últimos 60 minutos
    - Dia - dados agregados de cada hora para as 24 horas anteriores
    - Semana - dados agregados de cada dia durante os sete dias anteriores
    - Mês - dados agregados de cada semana para os últimos sete dias
    - Ano - dados agregados de cada mês durante os 12 meses anteriores
- Escolha os Dados disponíveis de acordo com o banco de dados que você escolheu
    - Banco de dados de serviços virtuais
    - Bytes em
    - Bytes out
    - Bytes armazenados em cache
    - Compressão %
    - Conexões atuais
    - Pedidos por segundo
    - Cache Hits
    - Cache Hits %
- Servidores reais
    - Bytes em
    - Bytes out
    - Conexões atuais
    - Pedido por segundo
    - Tempo de resposta
- Sistema
    - CPU
    - Serviços CPU
    - Memória
    - Disco livre
    - Bytes em
    - Bytes out
- Escolhido para mostrar valores Médios ou de Pico
- Uma vez que tenha escolhido todas as opções, clique em Salvar e Fechar.

Exemplo Gráfico de tráfego



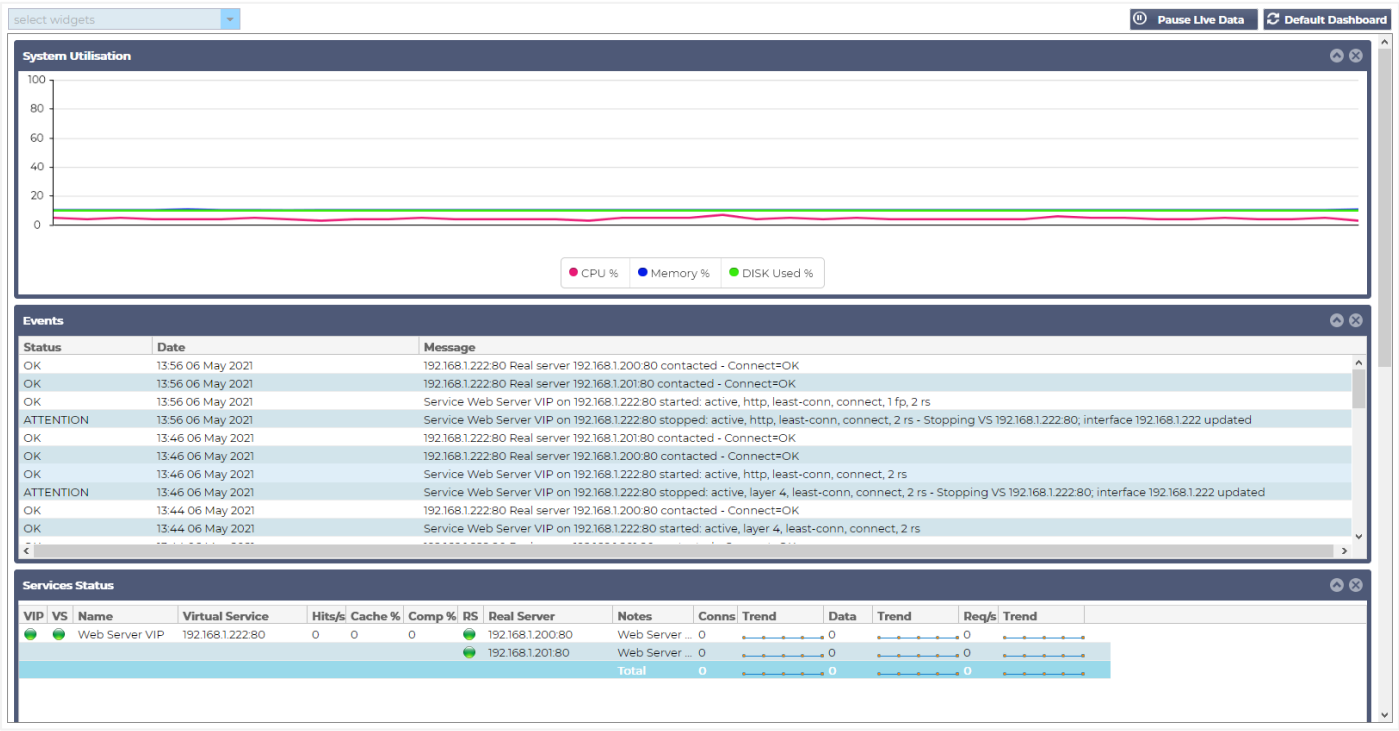
O senhor pode agora acrescentar seu widget do gráfico de tráfego ao View > Dashboard.

Ver

Painel de controle

Como todas as interfaces de gestão de sistemas de TI, há muitas vezes em que o senhor precisa olhar para as métricas e dados de desempenho que o ADC está tratando. Fornecemos um painel de controle personalizável para que o senhor possa fazer isso de uma maneira fácil e significativa.

O Painel é acessível usando o segmento View do painel do navegador. Quando selecionado, ele mostra vários widgets padrão e permite que o senhor escolha quaisquer widgets personalizados que tenha definido.



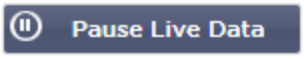
Uso do painel de instrumentos

Há quatro elementos no Dashboard U: o Menu Widgets, o Botão Pause/Play e o botão Default Dashboard.

O menu Widgets

O menu Widgets localizado na parte superior esquerda do painel de instrumentos permite ao senhor selecionar e acrescentar quaisquer widgets padrão ou personalizados que tenha definido. Para usar isso, selecione o widget a partir do menu suspenso.

Pausa Botão "Live Data Button



Esse botão permite que o senhor selecione se o ADC deve atualizar o painel de instrumentos em tempo real. Uma vez pausado, nenhum widget do painel de instrumentos será atualizado, permitindo ao senhor examinar o conteúdo à sua vontade. O botão muda de estado para mostrar Play Live Data uma vez que uma pausa seja iniciada.

Quando o senhor tiver terminado, basta clicar no botão Play Live Data para reiniciar a coleta de dados e atualizar o Painel de Controle.

Botão Default Dashboard Button

Pode ser que o senhor deseje repor o layout do Painel de Controle no padrão. Nesse caso, pressione o botão Default Dashboard. Uma vez clicado, todas as mudanças feitas no Painel serão perdidas.

Redimensionamento, minimização, reordenação e remoção de widgets

Redimensionamento de um Widget

O senhor pode redimensionar um widget muito facilmente. Clique e segure na barra de título do widget e arraste-o para o lado esquerdo ou direito da área do Painel. O senhor verá um retângulo pontilhado que representa o novo tamanho do widget. Largue o widget no retângulo e solte o botão do mouse. Se o senhor quiser deixar cair um widget redimensionado ao lado de um widget redimensionado anteriormente, verá o retângulo aparecer ao lado do widget que deseja deixar cair ao lado.

Minimização de um Widget

O senhor pode minimizar os widgets a qualquer momento, clicando na barra do título do widget. Essa ação minimizará o widget e exibirá apenas a barra de título.

Ordem Widget Moving

Para mover um widget, o senhor pode arrastar e soltar por clique e segurar a barra de título e mover o mouse.

Remoção de um Widget

O senhor pode remover uma clicando no ⊗ícone na barra de título widget.

História

A opção Histórico, selecionável do navegador, permite ao administrador examinar o desempenho histórico do ADC. É possível gerar visões históricas para Serviços Virtuais, Servidores Reais e Sistema.

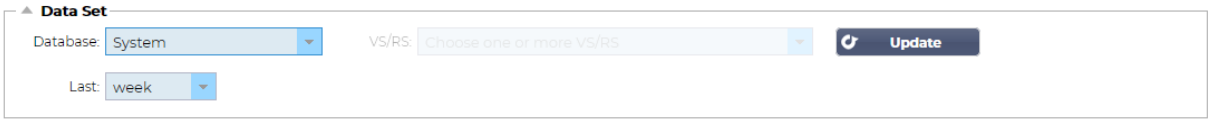
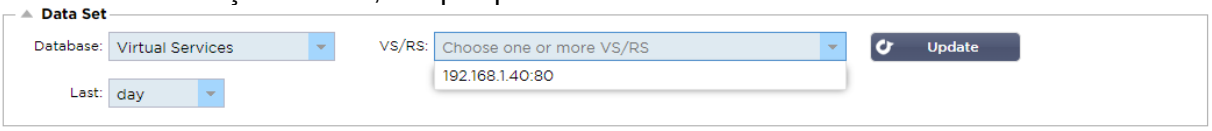
Também permite que o senhor veja o equilíbrio da carga em ação e ajuda a detectar quaisquer erros ou padrões que precisem ser investigados. Observe que o senhor deve permitir o registro histórico no Sistema > Histórico para fazer uso desse recurso.

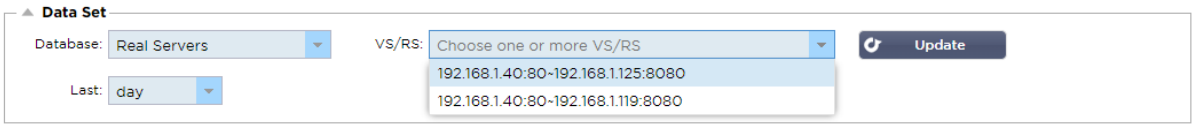
Visualização dos dados gráficos

Conjunto de dados

Para visualizar os dados históricos em formato gráfico, favor proceder da seguinte maneira:

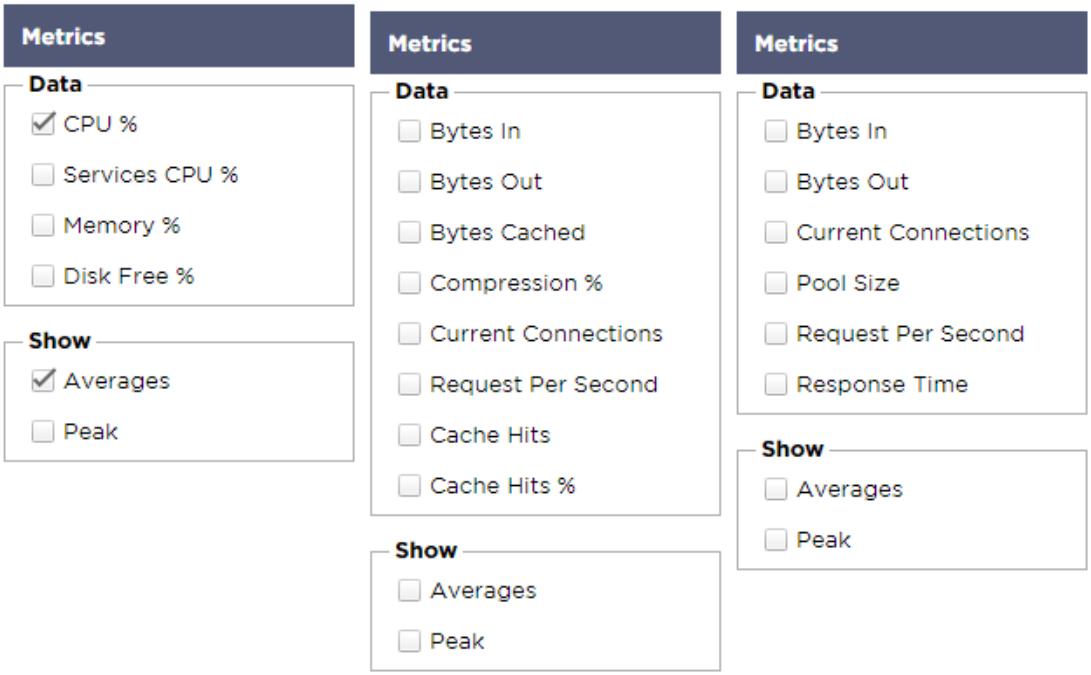
O primeiro passo é escolher o banco de dados e o período relevante para as informações que o senhor deseja ver. O período que o senhor pode selecionar da última gota é Minuto, Hora, Dia, Semana, Mês e Ano.

Base de dados	Descrição
Sistema	A seleção desse banco de dados permitirá que o usuário veja a CPU, a memória e o espaço em disco ao longo do tempo 
Serviços virtuais	A seleção desse banco de dados permitirá ao senhor escolher todos os serviços virtuais do banco de dados a partir de quando o senhor começou a registrar os dados. O senhor verá uma lista de serviços virtuais, da qual poderá selecionar um. 
Serviços reais	A seleção desse banco de dados permitirá ao senhor escolher todos os Servidores Reais do banco de dados a partir de quando o senhor começou a registrar os dados. O senhor verá uma lista de Servidores Reais, da qual poderá selecionar um.

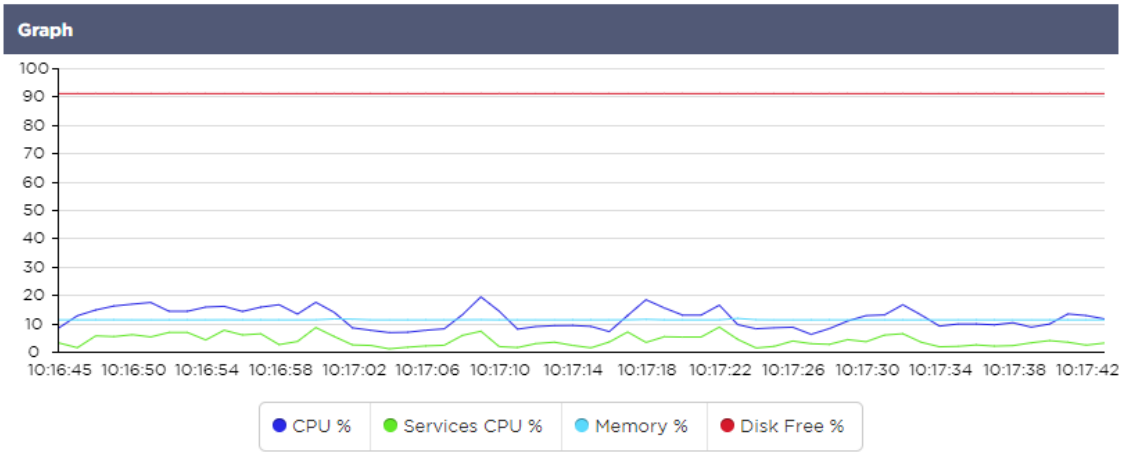


Métricas

Uma vez selecionado o conjunto de dados que o senhor usará, é hora de escolher a métrica que deseja exibir. A imagem abaixo ilustra as métricas disponíveis para seleção pelo administrador: essas seleções correspondem a System, Virtual services e Real Servers (da esquerda para a direita).



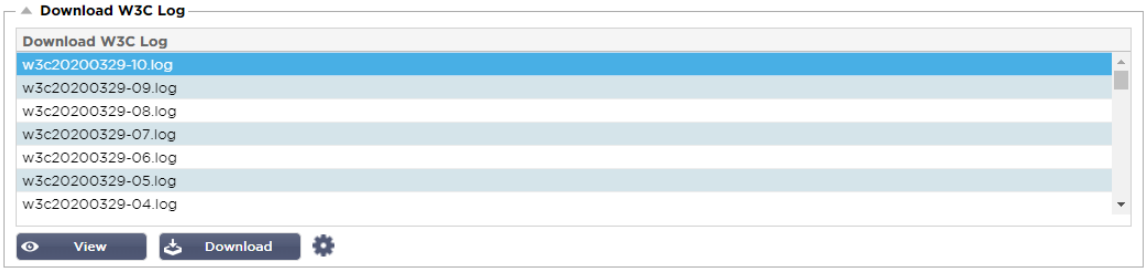
Exemplo de gráfico



Logs

A página de logs dentro da seção View permite ao senhor visualizar e baixar os logs do W3C e do Sistema. A página está organizada em duas seções, como detalhado abaixo.

Download dos logs do W3C



O registro do W3C é habilitado a partir da seção Sistema > Registro de Madeira. Um registro do W3C é um registro de acesso para servidores da Web no qual são gerados arquivos de texto contendo dados sobre cada pedido de acesso, inclusive o endereço do Protocolo de Internet de origem (IP), a versão HTTP, o tipo de navegador, a página de referência, e o carimbo da hora. Os registros do W3C podem se tornar muito grandes, dependendo da quantidade de dados e da categoria do registro de dados.

Na seção do W3C, o senhor pode selecionar o diário de bordo de que necessita e depois visualizá-lo ou baixá-lo.

Ver Botão

O botão View permite que o senhor veja o diário de bordo escolhido dentro da janela do editor de texto, como o Bloco de Notas.

Botão de download

Este botão permite ao senhor baixar o diário de bordo para seu depósito local para ser visto mais tarde.

O Ícone Cog

Clicando neste ícone, o senhor será levado à seção de Configurações de Log do W3C, localizada em Sistema > Logging. Discutiremos isso em detalhes na seção de Logging do guia.

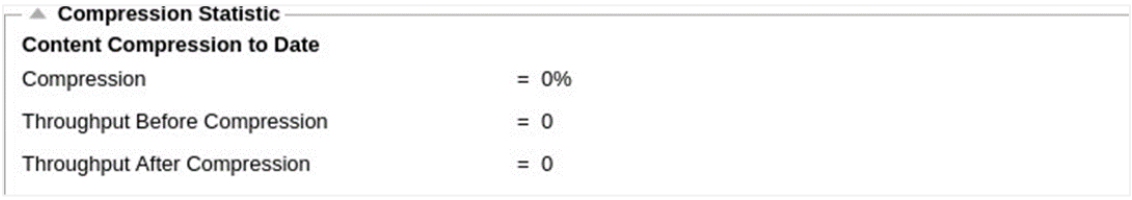
Estatísticas

A seção de estatísticas da CDA é uma área muito utilizada pelos administradores do sistema que querem assegurar que o desempenho da CDA esteja de acordo com suas expectativas.

Compressão

Toda a finalidade do ADC é monitorar os dados e direcioná-los aos Servidores Reais configurados para recebê-los. O recurso de compressão 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 de Compressão dentro da Estatística.

Compressão de conteúdo até a data



Os dados mostrados nesta seção detalham o nível de compressão alcançado pelo ADC sobre o conteúdo compressivo. Um valor de 60-80% é o que chamaríamos como típico

Compressão geral até a data

Overall Compression to Date			Current Values
Compression	= 0%		= 0%
Throughput Before Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput After Compression	= 1.93 GB		= 7.32 Mbps (data)
Throughput From Cache	= 0		= 0.00 Mbps (data)
		Total	= 14.64 Mbps (data)

Os valores fornecidos nesta seção relatam quanta compressão o ADC conseguiu em todo o conteúdo. Uma porcentagem típica para isso depende de quantas imagens pré-comprimidas estão contidas em seus serviços. Quanto maior for o número de imagens, menor será provavelmente a porcentagem de compressão total.

Entrada/saída total

Total Input	= 2.13 GB	Input/s	= 9.10 Mbps
Total Output	= 2.18 GB	Output/s	= 9.24 Mbps

Os números de Entrada/Saída Total representam a quantidade de dados brutos atravessados para dentro e para fora do ADC. A unidade de medida mudará à medida que o tamanho crescer de kbps para Mbps para Gbps.

Acertos e conexões

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

A seção de acessos e conexões contém as estatísticas gerais de acessos e transações que passam pelo ADC. Então, o que significam os hits e as conexões?

- Um acerto é definido como uma transação de Camada 7. Tipicamente usado para servidores web, é um pedido de GET para um objeto como uma imagem.
- Uma conexão é definida como uma conexão TCP de Camada 4. Muitas transações podem ocorrer em 1 conexão TCP.

Ataques totais contados

Os números dentro desta seção mostram o número cumulativo de acertos não realizados em cache desde o último reset. No lado direito, os números mostrarão o número atual de acertos por segundo.

Conexões totais

O valor total das conexões representa o número cumulativo de conexões TCP desde o último reset. A figura na segunda coluna indica as conexões TCP feitas por segundo para o ADC. O número na coluna da direita é o número de conexões TCP por segundo feitas aos Servidores Reais. Exemplo 6/8 conexões/segundo. Temos 6 conexões TCP por segundo para o Serviço Virtual e 6 conexões TCP por segundo para os Servidores Reais no exemplo mostrado.

Conexões de Pico

O valor de pico das conexões representa o número máximo de conexões TCP feitas ao ADC. O número na coluna mais à direita indica o número atual de conexões TCP ativas.

Caching

Como o senhor se lembrará, o ADC está equipado tanto com compressão quanto com caching. Esta seção mostra as estatísticas gerais relacionadas com o caching quando aplicado a um canal. Se o cache não tiver sido aplicado a um canal e configurado corretamente, o senhor verá 0 conteúdo do cache.

Caching

Content Caching	Hits	Bytes
From Cache	= 0 / **0.0%**	= 0 / **0.0%**
From Server	= 495799 / **100.0%**	= 1.97 GB / **100.0%**
Cache Contents	= 0 entries	= 0 / **0.0%**

De Cache

Acertos: A primeira coluna dá o número total de transações servidas a partir do cache do ADC desde o último reset. Uma porcentagem do total das transações também é fornecida.

Bytes: A segunda coluna dá a quantidade total de dados em Kilobytes atendidos a partir do cache do ADC. Uma porcentagem dos dados totais também é fornecida.

Do Servidor

Acertos: A coluna 1 apresenta o número total de transações servidas pelos Servidores Reais desde o último reset. Uma porcentagem do total das transações também é fornecida.

Bytes: A segunda coluna dá a quantidade total de dados em Kilobytes servidos pelos Servidores Reais. Uma porcentagem dos dados totais também é fornecida.

Conteúdo do Cache

Acertos: Esse número dá o número total de objetos contidos no cache do ADC.

Bytes: O primeiro número dá o tamanho total em Megabytes dos objetos em cache do ADC. Uma porcentagem do tamanho máximo do cache também é fornecida.

Persistência da sessão

Session Persistence

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

A seção de Persistência da sessão fornece informações sobre vários parâmetros.

Campo	Descrição
Total das sessões em curso	Isto mostra quantas sessões de persistência estão em andamento - atualizadas a cada minuto
% Utilizado (do máximo)	Isto mostra o uso que se faz do espaço total permitido para as informações da sessão
Nova sessão nesta Mina	Isto mostra, no último minuto, quantas novas sessões de persistência foram acrescentadas.
Revalidar esta mina	Isto mostra, no último minuto, quantas sessões de persistência existentes foram revalidadas por mais tráfego
Sessões expiradas nesta Mina	Isto mostra, no último minuto, quantas sessões de persistência existentes expiraram devido a não haver mais tráfego dentro do tempo limite.

Hardware

Quer o senhor esteja usando o ADC num ambiente virtual ou dentro do hardware, esta seção fornecerá ao senhor informações valiosas sobre o desempenho do aparelho.

Uso do disco

O valor fornecido na coluna 2 dá a porcentagem de espaço em disco atualmente usado e inclui informações sobre arquivos de registro e dados de cache, que são armazenados periodicamente no armazenamento.

Uso da memória

A segunda coluna dá a porcentagem da memória atualmente utilizada. O número mais significativo entre parênteses é a quantidade total de memória alocada ao ADC. Recomenda-se que o ADC seja alocado com um mínimo de 2GB de RAM.

Uso da CPU

Um dos valores críticos fornecidos é a porcentagem de CPU atualmente usada pela ADC. É natural que isso flutue.

Status

A página View > Status mostra o tráfego ao vivo que atravessa o ADC para os serviços virtuais que o senhor definiu. Mostra também o número de conexões e dados para cada servidor real, para que o senhor possa experimentar o balanceamento de carga em tempo real.

Detalhes do Serviço Virtual

VIP	VS	Name	Virtual Service	Hits/s	Cache %	Comp %	RS	Real Server	Notes	Conns	Data	Req/s	Pool
		VIP1	192.168.1.248:80	23	0	0		192.168.1.7:80		2	4.19Mb	23	0
		VS2	192.168.1.251:80	40	0	0		192.168.1.21:80	VS2 Serv...	0	7.40Mb	40	200
		VIP2	192.168.1.254:80	0	0	0		192.168.1.21:80	VIP2 Serv...	0	0	0	0
			ALB-X Total	63	0	0				0	11.60Mb	63	200

Coluna VIP

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

Status	Descrição
●	Online
●	Failover-Standby. Este serviço virtual é hot-standby
●	Indica que uma "passiva" está se segurando para uma "ativa".
●	Fora de linha. Os servidores reais são inacessíveis, ou nenhum servidor real está habilitado.
●	Situação de busca
●	Não licenciados ou licenciados IPs Virtuais excedidos

Coluna de Status VS

A cor da luz indica o estado do Serviço Virtual.

Status	Descrição
●	Online
●	Failover-Standby. Este serviço virtual é hot-standby
●	Indica que uma "passiva" está se segurando para uma "ativa".
●	O serviço precisa de atenção. Essa indicação de status pode resultar de um servidor real falhar em um monitor de saúde ou ter sido mudado manualmente para Offline. O tráfego continuará a fluir, mas com capacidade reduzida do Real Server.
●	Fora de linha. Os servidores reais são inacessíveis, ou nenhum servidor real está habilitado.
●	Situação de busca
●	Não licenciados ou licenciados IPs Virtuais excedidos

Nome

O nome do Serviço Virtual

Serviço Virtual (VIP)

O endereço IP virtual e o porto para o serviço e os usuários do endereço ou aplicações usarão.

Golpe/segundo

Transações de camada 7 por segundo no lado do cliente.

Cache%

O número aqui fornecido representa a porcentagem de objetos que foram servidos a partir do Cache de RAM da ADC.

Compressão%

Esse número representa a porcentagem de objetos que foram comprimidos entre o cliente e o ADC.

RS Status (Servidor remoto)

O quadro a seguir descreve o significado do status de Servidores Reais ligados ao VIP.

Status	Descrição
●	Conectado
●	Não monitorado
●	Drenagem ou fora de linha
●	Espera
●	Não Ligado
●	Situação de busca
●	Não licenciados ou licenciados IPs Virtuais excedidos

Servidor Real

O endereço IP e o porto do Real Server.

Notas

Esse valor pode ser qualquer nota útil para que outros entendam o propósito da inscrição.

Conns (Conexões)

A representação do número de conexões a cada servidor real permite que o senhor veja o equilíbrio de carga em ação. Muito útil para verificar se sua política de balanceamento de carga está funcionando corretamente.

Dados

O valor nessa coluna mostra a quantidade de dados que estão sendo enviados a cada servidor real.

Req/Sec (Pedidos por segundo)

O número de pedidos por segundo enviados a cada servidor real.

Sistema

O segmento Sistema da interface do usuário do ADC permite ao senhor acessar e controlar todos os aspectos do sistema do ADC.

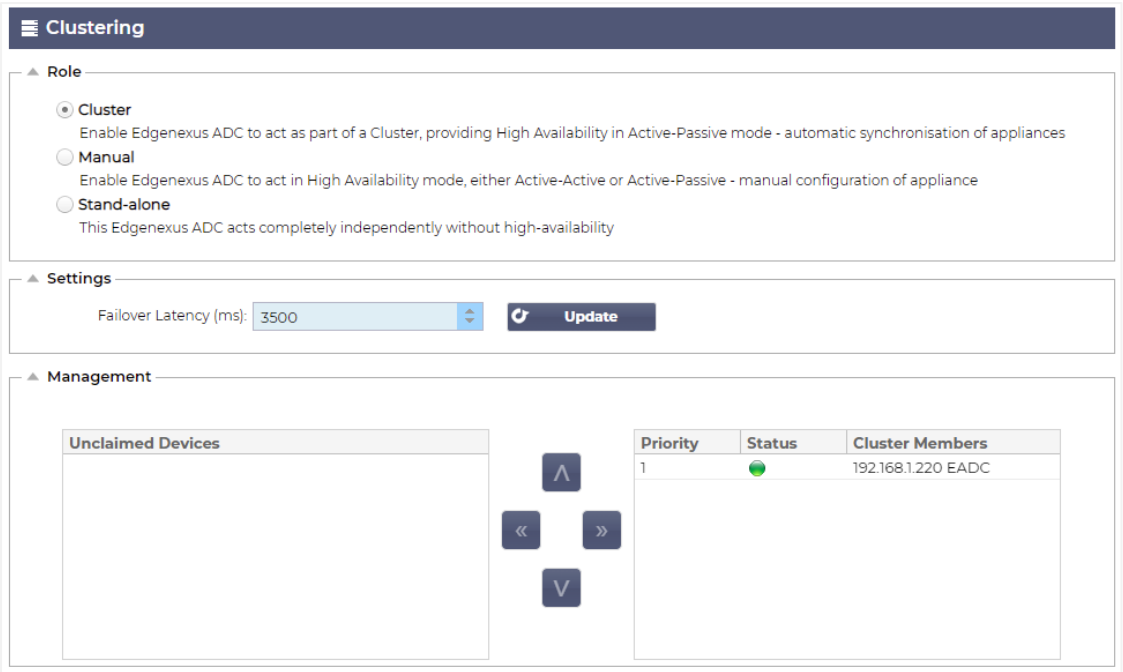
Clustering

O ADC pode ser usado como um único dispositivo autônomo, e funcionará perfeitamente bem fazendo isso. Entretanto, quando se considera que o objetivo do ADC é carregar conjuntos de servidores de equilíbrio, a necessidade de agrupar o próprio ADC se torna aparente. O projeto do ADC, de fácil navegação, torna a configuração do sistema de clustering simples.

A página Sistema > Clustering é onde o senhor vai configurar a alta disponibilidade de seus aparelhos do ADC. Esta seção está organizada em várias seções.

Nota importante

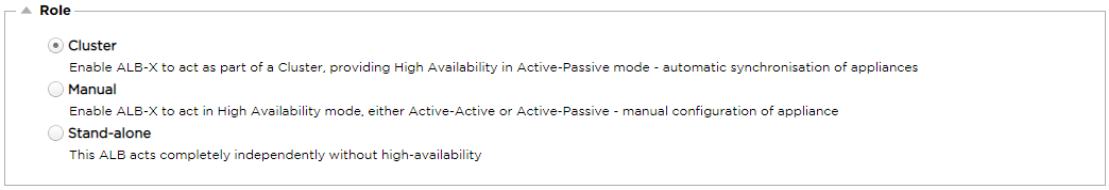
- Não há nenhuma exigência de um cabo dedicado entre o par ADC para manter um batimento cardíaco de alta disponibilidade.
- O batimento cardíaco se dá na mesma rede do Serviço Virtual que requer alta disponibilidade para ser posto em prática.
- Não há nenhuma falha de Estado entre os aparelhos do ADC.
- Quando houver alta disponibilidade em dois ou mais ADC's, cada caixa transmitirá via UDP os Serviços Virtuais que está configurada para fornecer.
- A alta disponibilidade de falhas usa mensagens unicast e ARP Gratuita para informar os novos interruptores equilibradores de carga ativos.



Papel

Há três funções de cluster disponíveis quando o senhor configura o ADC para alta disponibilidade.

Cluster



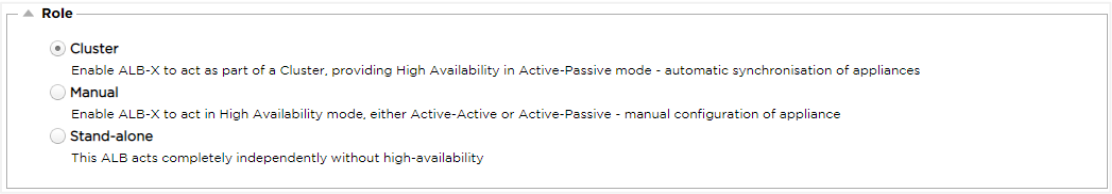
- Por padrão, um novo ADC irá energizar o uso do papel de Cluster. Nessa função, cada membro do Cluster terá a mesma "configuração de trabalho", e como tal, apenas um ADC no Cluster estará ativo a qualquer momento.
- Uma "configuração de trabalho" significa todos os parâmetros de configuração, exceto itens que precisam ser únicos, tais como o endereço IP da administração, nome ALB, configurações da rede, detalhes da interface, e assim por diante.
- O ADC na prioridade 1, a posição mais alta, da caixa dos Membros do Cluster é o Proprietário do Cluster e o Balanceador de Carga Ativo, enquanto todos os outros ADCs são Membros Passivos.
- O senhor pode editar qualquer ADC no Cluster, e as mudanças serão sincronizadas com todos os membros do Cluster.
- Quando o senhor remover um ADC do Cluster, todos os serviços virtuais serão eliminados desse ADC.
- O senhor não pode retirar o último membro do Cluster para os dispositivos não reclamados. Para remover o último membro, favor mudar a função para Manual ou autônomo.
- Os seguintes objetos não estão sincronizados:
    - Manual Seção de Data e Hora - (A seção NTP está sincronizada)
    - Latência de Failover (ms)
    - Seção de ferragens
    - Seção de aparelhos
    - Seção da rede

Falha do Proprietário do Cluster

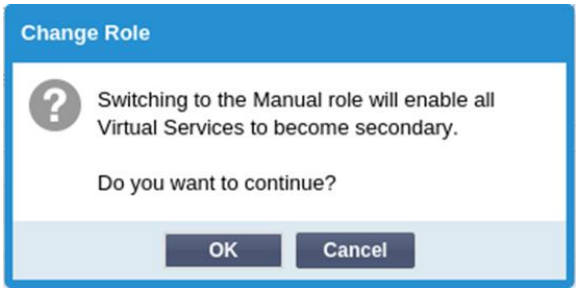
- Quando um proprietário de um agrupamento falhar, um dos membros restantes assumirá automaticamente o controle e prosseguirá com a carga equilibrando o tráfego.
- Quando o proprietário do agrupamento retornar, ele retomará o tráfego de equilíbrio de carga e assumirá o papel de proprietário.
- Vamos supor que o proprietário falhou, e que um deputado assumiu o equilíbrio da carga. Se o senhor deputado quiser que o deputado que assumiu o controle do tráfego de balanceamento de carga se torne o novo proprietário, destaque o deputado e clique na seta para cima para movê-lo para a posição de Prioridade 1.
- Se o senhor editar um dos demais membros do grupo e o proprietário estiver em baixa, o membro editado se promoverá automaticamente para o proprietário sem perda de tráfego

Mudança do papel de Cluster para o papel de Manual

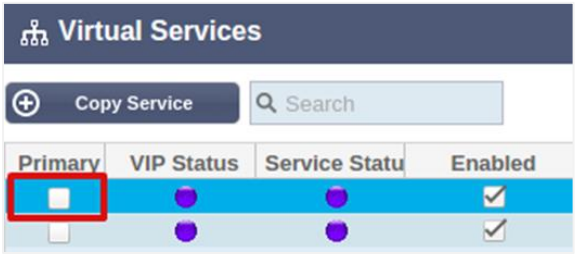
- Se desejar mudar a função de Cluster para Manual, clique no botão de rádio ao lado da opção de função Manual.



- Depois que o senhor clicar no botão do rádio, verá a seguinte mensagem:



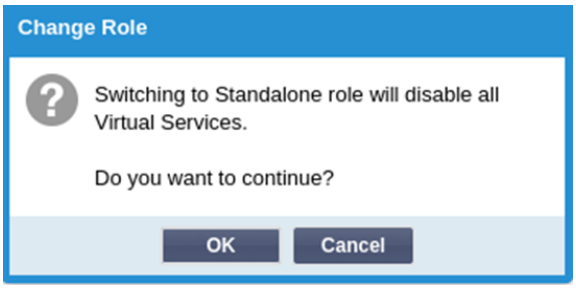
- Clique no botão OK
- Verifique a seção de Serviços Virtuais. O senhor vai ver que a coluna primária agora mostra uma caixa desmarcada.



- É uma característica de segurança e significa que se o senhor tiver outro ADC com os mesmos serviços virtuais, então não haverá interrupção do fluxo de tráfego.

Mudança do papel de Cluster para Stand-alone

- Se o senhor deseja mudar o papel de Cluster para autônomo, clique no botão de rádio ao lado da opção autônoma.
- O senhor será informado com a seguinte mensagem:



- Clique OK para mudar de função.
- Verifique seus serviços virtuais. O senhor verá que a coluna primária muda de nome para autônoma.
- O senhor verá também que todos os Serviços Virtuais estão desativados (não colados) por razões de segurança.
- Uma vez que o senhor esteja confiante de que nenhum outro ADC da mesma rede tem serviços virtuais duplicados, o senhor poderá habilitar cada um deles por sua vez.

Papel do Manual

Um CDA no papel de Manual trabalhará com outros CDA's no papel de Manual para proporcionar alta disponibilidade. A principal vantagem sobre o papel do Cluster é a capacidade de estabelecer qual ADC é Ativo para um IP Virtual. A desvantagem é que não há sincronização de configuração entre os CDA's. Quaisquer mudanças devem ser replicadas manualmente em cada caixa via GUI, ou para muitas mudanças, pode-se criar um jetPACK de um ADC e enviá-lo para o outro.

- Para fazer um endereço IP Virtual "Ativo", marque a caixa de seleção na coluna principal (página Serviços IP)
- Para fazer um endereço IP Virtual "Passivo", deixe a caixa de seleção em branco na coluna principal (página Serviços IP)
- No caso de um serviço ativo falhar, o Passivo:
    - Se ambas as Colunas Primárias forem assinaladas, então ocorre um processo eleitoral, e o endereço MAC mais baixo estará ativo.
    - Se ambos não forem colados, então o mesmo processo eleitoral ocorrerá. Além disso, se ambos forem desmarcados, não haverá uma retirada automática do ADC Ativo original.

Papel autônomo

Um CDA no papel autônomo não se comunicará com nenhum outro CDA a respeito de seus serviços, e portanto todos os Serviços Virtuais permanecerão no status Verde e conectados. O senhor deve assegurar-se de que todos os Serviços Virtuais tenham endereços IP únicos, ou haverá um conflito em sua rede.

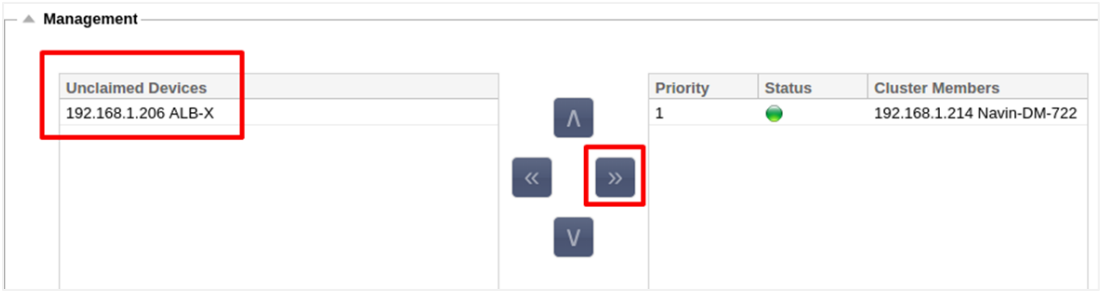
Configurações

Na seção Settings, o senhor pode definir a Latência Failover em milissegundos, o tempo que um ADC Passivo esperará antes de assumir os Serviços Virtuais depois que o ADC Ativo tiver falhado.

Recomendamos que o valor seja ajustado para 10000ms ou 10 segundos, mas o senhor poderá diminuir ou aumentar esse valor para se adequar à sua rede e às suas necessidades. Os valores aceitáveis caem entre 1500ms e 20000ms. Se o senhor experimentar instabilidade no agrupamento com uma latência menor, deverá aumentar esse valor.

Administração

Nesta seção, o senhor pode acrescentar e remover membros do agrupamento, ao mesmo tempo em que muda a prioridade de um ADC no agrupamento. A seção consiste de dois painéis e um conjunto de teclas de seta no meio. A área à esquerda são os dispositivos não reclamados, enquanto a área mais à direita é o próprio Aglomerado.

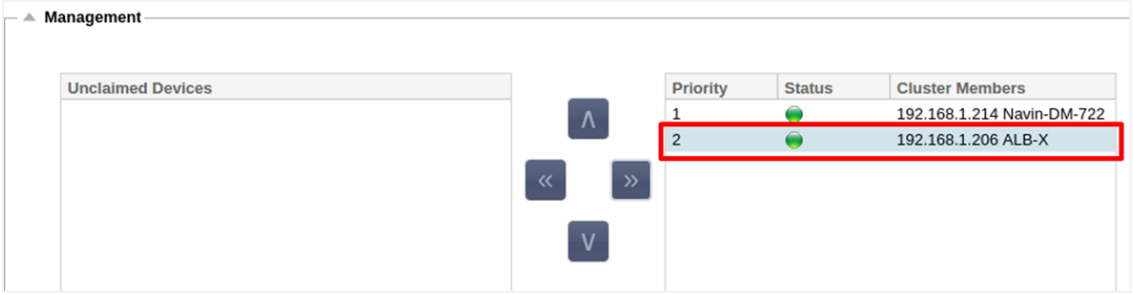


Acréscimo de um ADC ao agrupamento

- Antes de acrescentar o ADC ao agrupamento, o senhor deve assegurar-se de que todos os aparelhos do ADC tenham sido fornecidos com um nome único definido na seção Sistema > Rede.
- O senhor deve ver o ADC como Prioridade 1 com o status verde e seu nome sob a coluna Membros do Cluster na seção de administração. Esse ADC é o aparelho primário padrão.

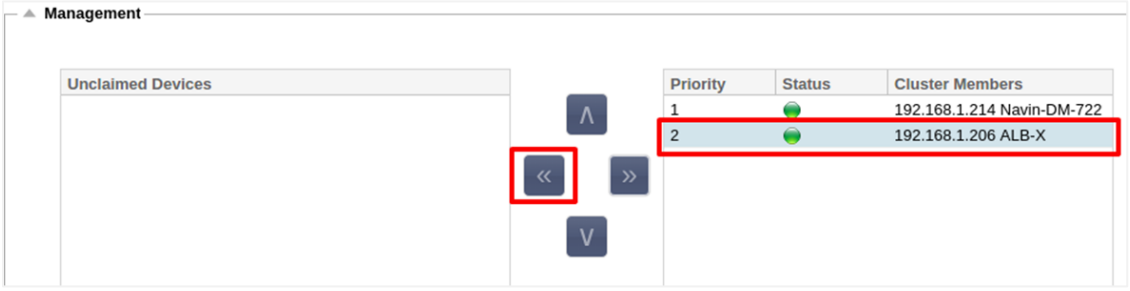
- Todos os outros ADC's disponíveis aparecerão na janela de dispositivos não reclamados dentro da seção de administração. Um dispositivo não reclamado é o ADC que foi designado na função de agrupamento, mas não tem serviços virtuais configurados.
- Destaque o ADC a partir da janela de dispositivos não reclamados e clique no botão de seta à direita.
- O senhor vai ver agora a seguinte mensagem:

- Clique OK para promover o ADC para o agrupamento.
- Seu ADC deveria agora figurar como Prioridade 2 na lista de membros do agrupamento.



Remoção de um membro do cluster

- Destaque o membro do grupo que o senhor deseja retirar do grupo.
- Clique no botão da seta à esquerda.

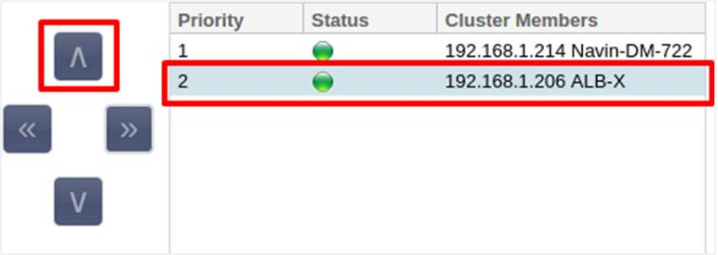


- O senhor será presenteado com um pedido de confirmação.
- Clique OK para confirmar.
- Seu ADC será removido e será mostrado no lado dos dispositivos não reclamados.

Mudança da prioridade de um ADC

Pode haver ocasiões em que o senhor deseje mudar a prioridade de um ADC dentro da lista dos membros.

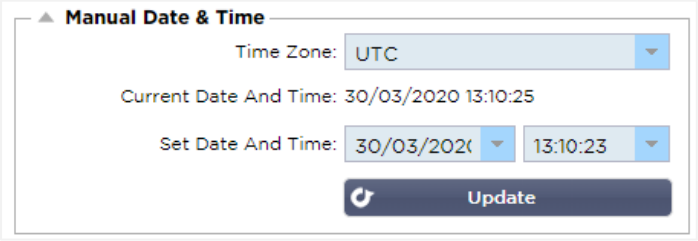
- O ADC no topo da lista de Membros do Cluster tem a Prioridade 1 e é o ADC Ativo para todos os Serviços Virtuais
- O ADC que está em segundo lugar na lista tem a Prioridade 2 e é o ADC Passivo para todos os Serviços Virtuais.
- Para mudar o que o ADC está ativo basta destacar o ADC e clicar na seta para cima até que ele esteja no topo da lista



Data e hora

A seção de data e hora permite a definição das características de data/hora do ADC, inclusive o fuso horário em que o ADC está localizado. Juntamente com o fuso horário, a data e a hora desempenham um papel vital nos processos criptográficos associados à criptografia SSL.

Manual Data e hora



Fuso horário

O valor que o senhor estabeleceu nesse campo representa o fuso horário em que se encontra o ADC.

- Clique na caixa suspensa para o fuso horário e comece a digitar sua localização.
  Por exemplo Londres
- Quando o senhor começar a digitar, o ADC mostrará automaticamente os locais que contêm a letra L.
- Continue digitando 'Lon,' e assim por diante - os locais listados serão reduzidos a locais que contenham 'Lon'. ’
- Se estiver em, digamos, Londres, então escolha Europa/Londres para definir sua localização

Se a data e a hora ainda estiverem incorretas após a mudança acima, favor mudar a data manualmente.

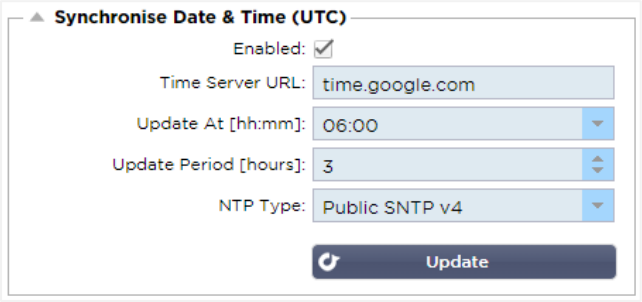
Data e hora

Esse ajuste representa a data e a hora reais.

- Escolha a data correta a partir do primeiro drop-down ou,
  alternativamente, o senhor pode digitar a data no seguinte formato DD/MM/AAAA
- Acrescentar no horário no seguinte formato hh: mm: ss, por exemplo, 06:00:10 para as 6h e 10 segundos.
- Uma vez que o senhor tenha digitado corretamente, favor clicar em Update para candidatar-se.
- O senhor deve então ver a nova data e hora em caracteres negros.

Sincronizar data e hora (UTC)

O senhor pode usar servidores NTP para sincronizar com precisão sua data e hora. Os servidores NTP estão localizados globalmente, e o senhor também pode ter seu próprio servidor NTP interno quando sua infra-estrutura tiver limitações de acesso externo.



URL do servidor de tempo

Digite 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 o uso de um FQDN.

Atualização em [hh:mm]

Selecione a hora marcada em que o senhor gostaria que o ADC se sincronizasse com o servidor do NTP.

Período de atualização [horas]:

Selecione com que freqüência o senhor deseja que a sincronização ocorra.

Tipo NTP:

- Public SNTP V4 - Este é o método atual e preferido quando se sincroniza com um servidor NTP. **RFC 5905**
- NTP v1 sobre TCP - Legado NTP versão sobre TCP. **RFC 1059**
- NTP v1 Over UDP - Legado NTP versão Over UDP. **RFC 1059**

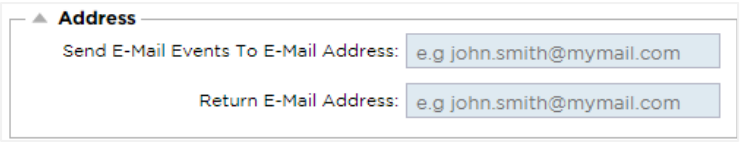
Nota: Queira observar que a sincronização é apenas em UTC. Se o senhor deseja definir uma hora local, isso só pode ser feito manualmente. Essa limitação será modificada em versões posteriores para permitir a possibilidade de selecionar um fuso horário.

Eventos por e-mail

O ADC é um aparelho crítico, e como qualquer sistema essencial, está equipado com a capacidade de informar a administração do sistema sobre quaisquer questões que possam exigir atenção.

A página Sistema > Eventos de e-mail permite que o senhor configure uma conexão de servidor de e-mail e envie notificações aos administradores do sistema. A página está organizada nas seções abaixo.

Endereço



Enviar por e-mail Eventos para Endereços de e-mail

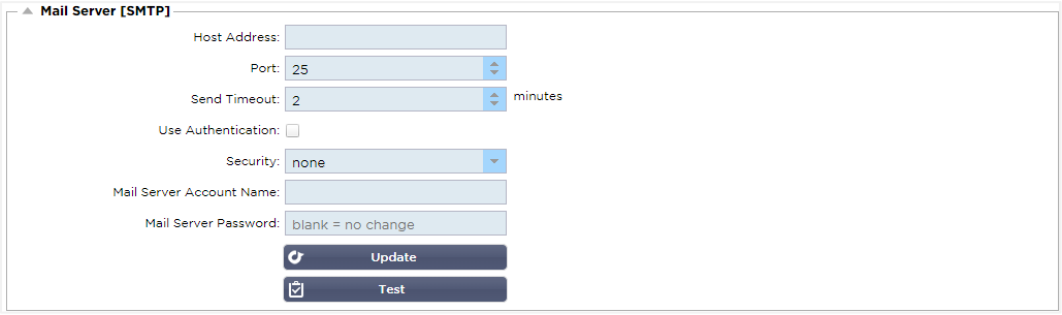
Acrescentar um endereço de e-mail válido para o envio de alertas, notificações e eventos. Exemplo: support@domain.com. O senhor também pode acrescentar vários endereços de e-mail usando um separador de vírgulas.

Devolver endereço de e-mail:

Acrescente em um endereço de e-mail que aparecerá na caixa de entrada. Exemplo adc@domain.com.

Servidor de correio (SMTP)

Nesta seção, o senhor deve acrescentar os detalhes do servidor SMTP a ser usado para enviar os e-mails. Queira certificar-se de que o endereço de e-mail que o senhor usa para o envio está autorizado a fazê-lo.



Endereço do anfitrião

Acrescente no endereço IP do seu servidor SMTP.

Porto

Acrescente no porto do seu servidor SMTP. O porto padrão para SMTP é 25 ou 587, se o senhor usar SSL.

Tempo limite de envio

Acrescente em um timeout SMTP. O tempo padrão está fixado em 2 minutos.

Usar Autenticação

Marque a caixa se seu servidor SMTP precisar de autenticação.

Segurança

- Nenhum
- A configuração padrão não é nenhuma.
- SSL - Use essa configuração se seu servidor SMTP exigir a autenticação Secure Sockets Layer.
- TLS - Use essa configuração se seu servidor SMTP exigir autenticação de segurança na camada de transporte.

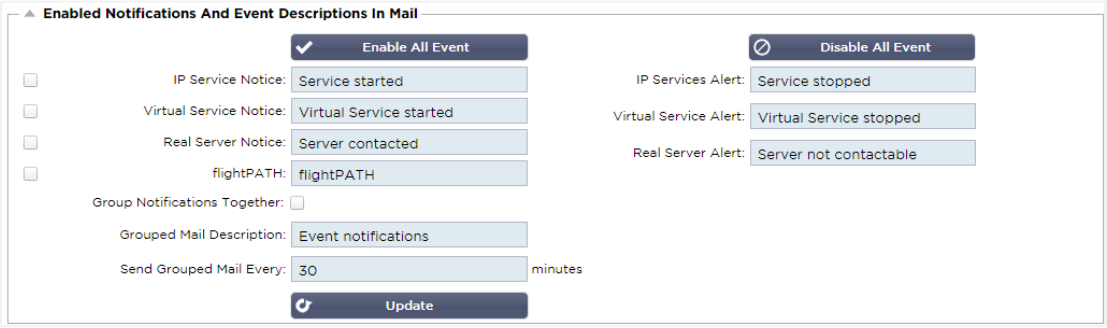
Nome da conta do servidor principal

Acrescente o nome de usuário necessário para a autenticação.

Senha do servidor de correio

Acrescentar a senha necessária para a autenticação.

Notificações e alertas



Há vários tipos de notificações de eventos que a ADC enviará às pessoas configuradas para recebê-las. O senhor pode marcar e ativar as notificações e alertas que devem ser enviados. Notificações ocorrem quando os Servidores Reais são contatados ou quando os canais são iniciados. Os alertas ocorrem quando os Servidores Reais não podem ser contatados, ou quando os canais param de funcionar.

Serviço de PI

O aviso do Serviço de PI informará o senhor quando qualquer endereço de PI virtual estiver on-line ou tiver parado de funcionar. Essa ação é realizada para todos os serviços virtuais que pertencem ao VIP.

Serviço virtual

Informa ao beneficiário que um Serviço Virtual está on-line ou que deixou de funcionar.

Servidor Real

Quando um Real Sever e um Porto estiver conectado ou não for contactável, o ADC enviará o aviso do Real Server.

vôoPATH

Esse aviso é um e-mail enviado quando uma condição foi atendida, e há uma ação configurada instruindo a ADC a enviar o evento por e-mail.

Notificações de grupo

Marque para agrupar as notificações. Com isso assinalado, todas as notificações e alertas serão agregadas em um único e-mail.

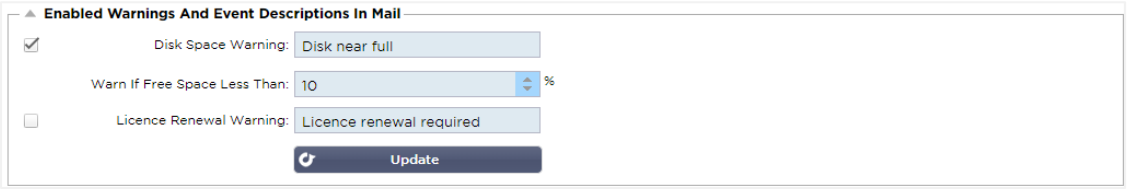
Grupo Correspondência Descrição

Especificar o assunto relevante para o e-mail de notificação do grupo.

Grupo Enviar intervalo

Estipular o tempo que o senhor deseja esperar antes de enviar um e-mail de notificação de grupo. O tempo mínimo é de 2 minutos.

Avisos



Há dois tipos de e-mails de advertência, e nenhum deles deve ser ignorado.

Espaço em disco

Fixar a porcentagem de espaço livre em disco antes da qual o aviso é enviado. Quando isso for feito, o senhor será enviado por e-mail.

Expiração da Licença

Essa configuração permite ao senhor ativar ou desativar o e-mail de aviso de expiração da licença enviado ao administrador do sistema. Quando isso for feito, o senhor será enviado por e-mail.

Histórico do sistema

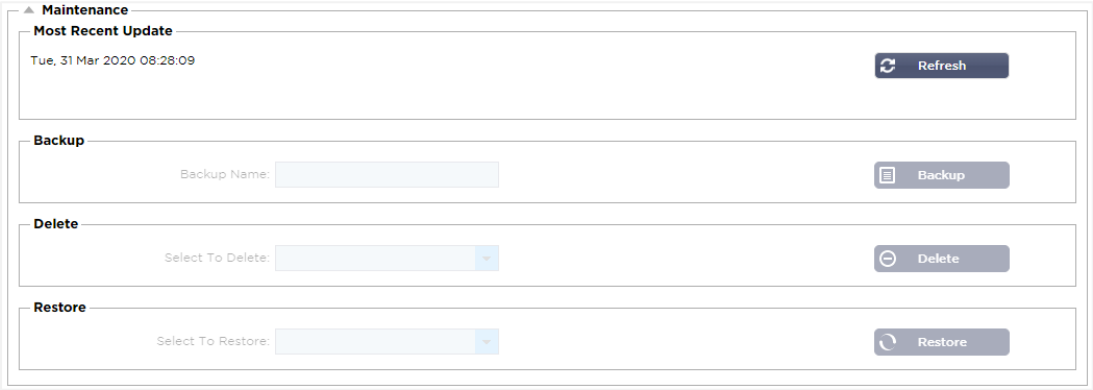
Na seção Sistema, há a opção Histórico do Sistema, permitindo a entrega de dados históricos para elementos como CPU, memória, pedidos por segundo, e outras características. Uma vez ativado, o senhor

pode ver os resultados em forma gráfica através da página View > History. Essa página também permitirá que o senhor faça backup ou restaure seus arquivos de histórico no ADC local.

Coleta de dados

- Para permitir a coleta de dados, favor assinalar a caixa de seleção.
- Em seguida, defina o intervalo de tempo em que o senhor deseja que a ADC colete os dados. Esse valor de tempo pode variar entre 1-60 segundos.

Manutenção



Esta seção ficará cinzenta se o senhor tiver permitido o corte histórico. Favor desmarcar a caixa de seleção Ativado na seção Coletar dados e clicar em Atualizar para permitir a manutenção dos registros históricos.

Cópia de segurança

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

Eliminar

Selecione um arquivo de reserva na lista suspensa. Clique em Delete para remover o arquivo de backup do ADC.

Restaurar

Selecione um arquivo de reserva previamente armazenado. Clique em Restore para preencher os dados desse arquivo de backup.

Licença

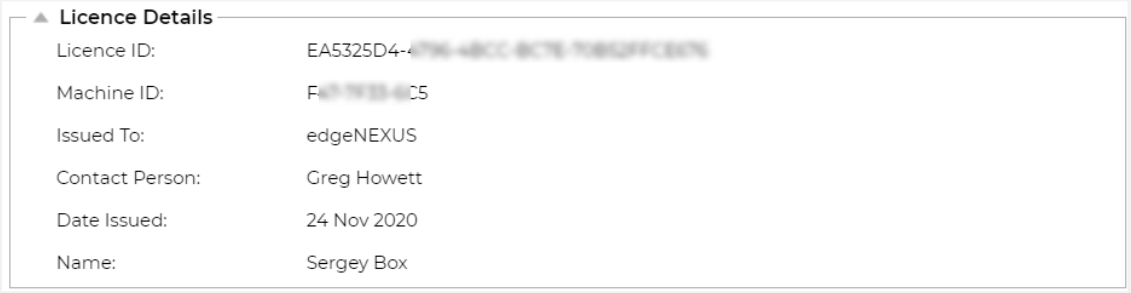
O ADC é licenciado para uso, ou usando um dos seguintes modelos, que depende dos parâmetros de compra e do tipo de cliente do senhor.

Tipo de licença	Descrição
Perpétuo	O senhor, o cliente, tem o direito de usar o ADC e outros softwares perpetuamente. Isso não impede que o senhor tenha que adquirir apoio para receber assistência e atualizações.
SaaS	SaaS ou Software-as-a-Service significa essencialmente que o senhor aluga o software de forma contínua ou pague como quiser. Nesse

	modelo, o senhor paga um aluguel anual pelo software. O senhor não tem direitos perpétuos para usar o software.
MSP	Prestadores de serviços gerenciados podem oferecer o ADC como um serviço e adquirir a licença por VIP, cobrada e paga anualmente.

Detalhes da licença

Cada licença inclui detalhes específicos pertinentes à pessoa ou organização que a adquire.



Identificação da licença

Essa identificação de licença está diretamente ligada à identificação da máquina e a outros detalhes específicos de sua compra e do ADC. Essa informação é essencial e é exigida quando o senhor deseja recuperar atualizações e outros itens da App Store.

Identificação da máquina

A identificação da máquina é gerada usando o endereço IP eth0 de um dispositivo ADC virtual e a identificação MAC de um ADC baseado em hardware. Se o senhor mudar o endereço IP de um aparelho do ADC virtual, a licença não será mais válida. O sr. terá apoio de contato para assistência. Recomendamos que o(s) aparelho(s) do CDA virtual tenha(m) endereços IP fixos com instruções para não alterá-los. O suporte técnico está disponível levantando um ticket em HTTPs://edgenexus.io.

Nota: O senhor não deve mudar o endereço IP nem o MAC ID de seus aparelhos do ADC. Se o senhor estiver em uma estrutura virtualizada, queira fixar o MAC ID e o endereço IP.

Emitido a

Esse valor contém o nome do comprador associado à identificação da máquina da ADC.

Pessoa de contato

Este valor contém a pessoa a ser contatada na empresa do cliente associada à identificação da máquina

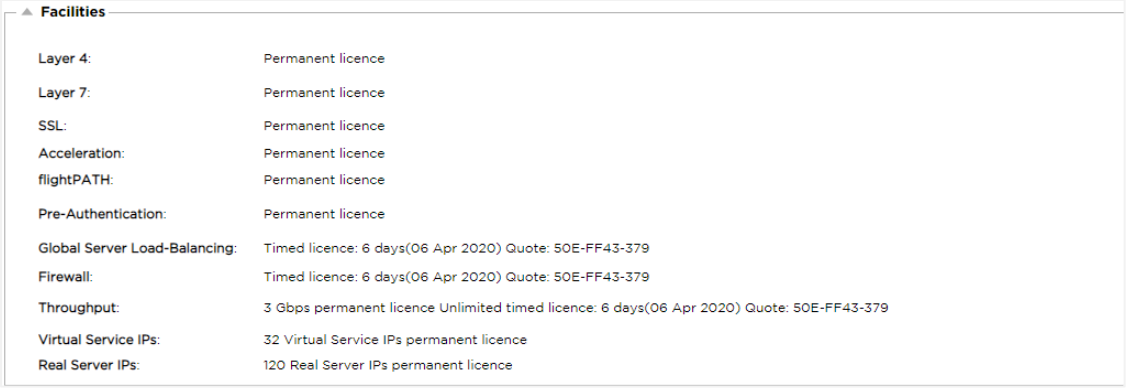
Data Questões

A data em que a licença foi emitida

Nome

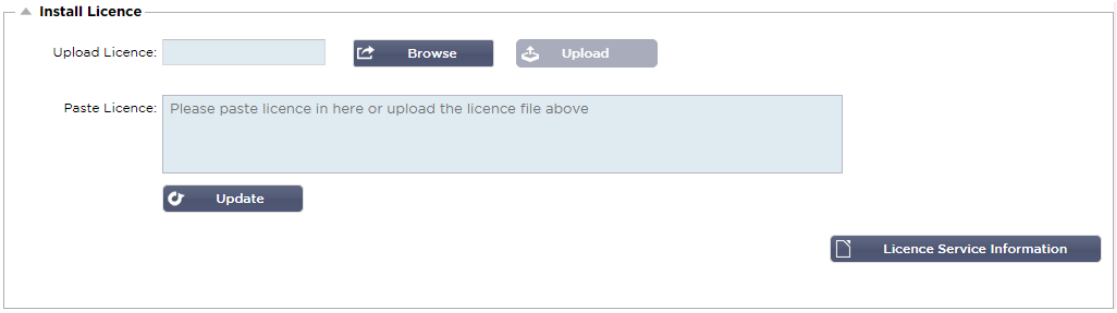
Esse valor mostra o nome descritivo para o aparelho da ADC que o senhor forneceu.

Instalações



A seção de instalações fornece ao senhor informações sobre quais funções dentro do ADC foram licenciadas para uso e a validade da licença. Também são apresentadas a produção que foi licenciada para o ADC e o número de Servidores Reais. Essa informação depende da licença que o senhor adquiriu.

Instalar Licenças e



- A instalação de uma nova licença é muito simples. Quando o senhor receber da Edgenexus sua licença nova ou de substituição, ela será enviada sob a forma de um arquivo de texto. O senhor pode abrir o arquivo e depois copiar e colar o conteúdo no campo "Licença de colar".
- O senhor também pode fazer o upload para o ADC se a cópia/colagem não for uma opção para o senhor.
- Uma vez feito isso, favor clicar no botão de atualização
- A licença está agora instalada.

Informações sobre o Serviço de Licenças

Clicando no botão "License Service Information", todas as informações sobre a licença serão exibidas. Essa função pode ser usada para enviar os detalhes para o pessoal de apoio.

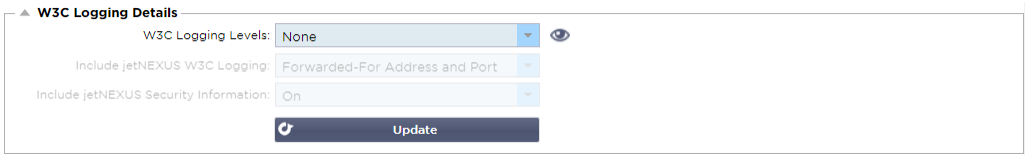
Logging

A página System > Logging permite ao senhor definir os níveis de registro do W3C e especificar o servidor remoto para o qual os registros serão automaticamente exportados. A página está organizada nas quatro seções abaixo.

W3C Detalhes de registro

A habilitação do registro do W3C fará com que o ADC comece a gravar um arquivo de registro compatível com o W3C. Um registro do W3C é um registro de acesso para servidores da Web no qual são gerados arquivos de texto contendo dados sobre cada pedido de acesso, inclusive o endereço de origem do Protocolo de Internet (IP), a versão HTTP, o tipo de navegador, a página de referência, e o carimbo de data e hora. O formato foi desenvolvido pelo World Wide Web Consortium (W3C), uma organização que promove padrões para a evolução da Web. O arquivo está em texto ASCII, com colunas delimitadas por

espaço. O arquivo contém linhas de comentário que começam com o caractere #. Uma dessas linhas de comentário é uma linha indicando os campos (fornecendo nomes de colunas) para que os dados possam ser minerados. Há arquivos separados para os protocolos HTTP e FTP.



Níveis de registro do W3C

Há diferentes níveis de registro disponíveis, e dependendo do tipo de serviço, os dados fornecidos variam.

A tabela abaixo descreve os níveis de registro para o W3C HTTP.

Valor	Descrição
Nenhum	O corte de madeira do W3C está cancelado.
Breve	Os campos presentes são: #Campos: tempo c-ip c-port s-ip método uri x-c-versão x-r-versão sc-status cs-bytes sr-bytes rs-bytes sc-bytes x-percentagem de tempo de viagem x-tempo de ida e volta cs(User-Agent) x-sc(Content-Type).
Completo	Este é um formato mais compatível com o processador, com campos de data e hora separados. Veja o resumo dos campos abaixo para informações sobre o significado dos campos. Os campos presentes são: #Campos: data hora 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 rs-bytes x-percent timetaken x-roun-trip-time x-sc(Content-Type).
Site	Esse formato é muito semelhante ao "Completo", mas tem um campo adicional. Veja o resumo dos campos abaixo para informações sobre o significado dos campos. Os campos presentes são: #Campos: data hora 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-versão x-r-versão cs-bytes sr-bytes rs-bytes rs-bytes x-percentagem do tempo de viagem x-round--trip-time x-sc(Content-Type).
Diagnóstico	Esse formato está repleto de todo tipo de informação relevante para o pessoal de desenvolvimento e apoio. Veja o resumo dos campos abaixo para informações sobre o significado dos campos. Os campos presentes são: #Campos: data hora c-ip c-port cs-username s-ip s-port x-xff x-xffcustom cs-hostes 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 rs-bytes x-percent timetaken x-round-trip-time x-trip-times (novo,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 registro para o W3C FTP.

Valor	Descrição
Breve	#Campos: data hora 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: data hora c-ip c-port s-ip s-ip s-port r-ip r-port cs-method cs-param cs-param sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes
Diagnóstico	#Campos: data hora c-ip c-port s-ip s-ip s-port r-ip r-port cs-method cs-param cs-param sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Incluir o registro do W3C

Essa opção permite ao senhor definir quais informações do ADC devem ser incluídas nos registros do W3C.

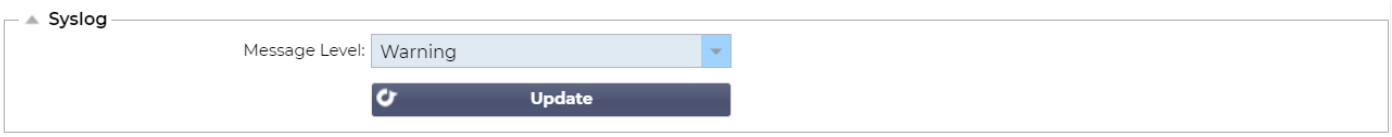
Valor	Descrição
Endereço da Rede do Cliente e Porto	O valor aqui mostrado mostra o endereço IP do cliente real junto com o porto.
Endereço da Rede do Cliente	Essa opção incluirá e mostrará apenas o endereço IP real do cliente.
Endereço e Porto	Essa opção mostrará os detalhes mantidos no cabeçalho do XFF, inclusive o endereço e o porto.
Encaminhado - Por Endereço	Essa opção mostrará os detalhes mantidos no cabeçalho do XFF, incluindo apenas o endereço.

Incluir informações de segurança

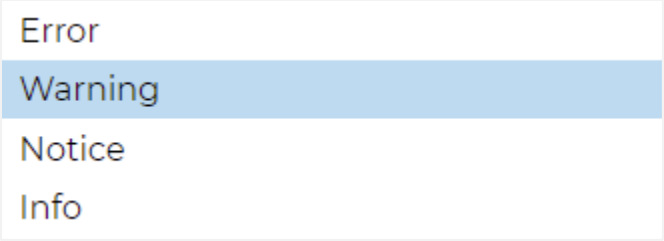
Essa ementa consiste de duas opções:

Valor	Descrição
Em	Este cenário é global. Quando ajustado para on, o nome de usuário será anexado ao registro do W3C quando qualquer Serviço Virtual estiver usando Autenticação e tiver o registro do W3C habilitado.
Off	Isso vai desligar a capacidade de registrar o nome de usuário no registro do W3C em nível global.

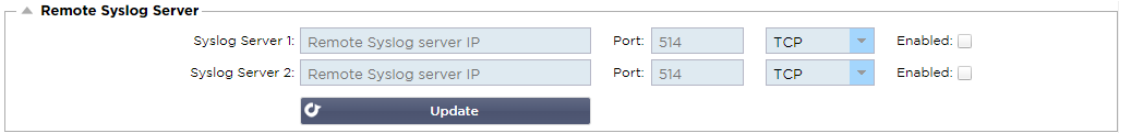
Servidor Syslog



Esta seção permite ao senhor definir o nível de registro de mensagens efetuadas no servidor SYSLOG. As opções disponíveis são as seguintes.



Servidor remoto Syslog

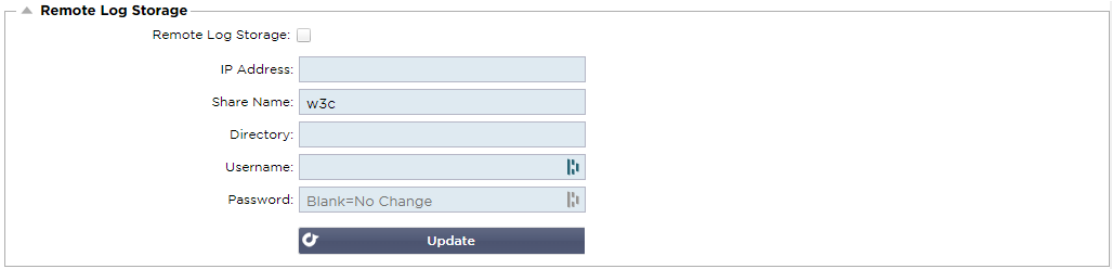


Nesta seção, o senhor pode configurar dois servidores externos de Syslog para enviar todos os logs do sistema.

- Adicionar o endereço IP do seu servidor Syslog
- Acrescentar o Porto

- Escolha se deseja usar TCP ou UDP
- Marque a caixa de seleção Ativado para iniciar o corte
- Clique em Atualizar

Armazenamento remoto de logs



Todos os registros do W3C são armazenados em forma comprimida no ADC a cada hora. Os arquivos mais antigos serão apagados quando restar 30% do espaço em disco. Caso o senhor deseje exportá-los para um servidor remoto para guarda, o senhor pode configurar isso usando uma ação SMB. Observe que o registro do W3C não será transferido para o local remoto até que o arquivo tenha sido completado e comprimido. Como os registros são escritos a cada hora, isso pode levar até duas horas em uma máquina virtual e cinco horas para uma máquina de hardware.

Incluíremos um botão de teste em futuros comunicados para dar algum feedback de que seus ajustes estão corretos.

Col1	Col2
Armazenamento remoto de logs	Assinalar a caixa para permitir o armazenamento remoto de registros
Endereço IP	Especifique o endereço IP do seu servidor SMB. Este deve estar em notação decimal pontilhada. Exemplo: 10.1.1.23
Nome da ação	Especifique o nome da ação no servidor da SMB. Exemplo: w3c.
Diretório	Especifique o diretório no servidor SMB. Exemplo: /log.
Nome de usuário	Especifique o nome de usuário para a ação da SMB.
Senha	Especificar a senha para a ação SMB

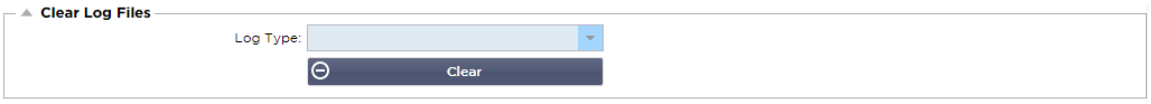
Resumo do campo

Condição	Descrição
Data	Não localizado = sempre YYYYY-MM-DD (GMT/UTC)
Hora	Não localizado = HH:MM:SS ou HH:MM:SS.ZZZ (GMT/UTC) * Nota - felizmente isto tem dois formatos (Site
	não tem .ZZZ milissegundos)
x-mil	Apenas formato do local = milissegundo de carimbo de tempo
c-ip	O melhor IP do cliente pode ser derivado da rede ou do cabeçalho X-Forwarded-For
c-porto	A melhor porta do cliente pode ser derivada da rede ou X-Forwarded-For header
cs- nome do usuário	Campo de pedido de nome de usuário do cliente
s-ip	O porto de escuta da ALB
s-port	ALB está ouvindo VIP

x-xff	Valor do cabeçalho X-Forwarded-For
x-xffcustom	Valor do cabeçalho de pedido do tipo X-Forwarded-Forwarded
cs-host	Nome do anfitrião no pedido
x-r-ip	Endereço IP do Real Server utilizado
x-r-port	Porto de Real Server usado
cs-método	Método de solicitação HTTP * exceto formato Brief
método	* Apenas um breve formato usa este nome para o método cs
cs-uri-stem	Caminho do recurso solicitado * exceto Breve formato
cs-uri-query	Consulta para o recurso solicitado * exceto Formato breve
uri	* breve formato registra um caminho combinado e um fio de consulta
sc-status	Código de resposta HTTP
cs(User-Agent)	Cadeia de usuário-agente do navegador (como enviada pelo cliente)
referir	Página de referência (como enviada pelo cliente)
x-c-versão	Pedido do cliente Versão HTTP
x-r-versão	Resposta do Content-Server versão HTTP
cs-bytes	Bytes do cliente, no pedido
sr-bytes	Bytes encaminhados ao Real Server, no pedido
rs-bytes	Bytes do Real Server, na resposta
sc-bytes	Bytes enviados ao cliente, na resposta
x-percentual	Porcentagem de compressão * = 100 * (1 - saída / entrada) incluindo cabeçalhos
tempo necessário	Quanto tempo o Real Server demorou em segundos
x-viagem novo pcon	milissegundos de conexão com a publicação na "lista de novatos". milissegundo da conexão até a colocação da conexão com o Real Server
acon	milissegundos desde a conexão até o término da colocação da conexão ao Real Server
rcon	milissegundo da conexão ao estabelecimento da conexão real-servidor
rqf	milissegundo da conexão ao recebimento do primeiro byte de pedido do cliente
rql	milissegundo da conexão ao recebimento do último byte de pedido do cliente
tqf	milissegundo da conexão ao envio do primeiro byte de pedido ao Real Server
tql	milissegundo da conexão ao envio do último byte de pedido ao Real Server
rsf	milissegundo da conexão ao recebimento do primeiro byte de resposta do Real Server
rsl	milissegundo da conexão ao recebimento do último byte de resposta do Real Server
tsf	milissegundo da conexão ao envio do primeiro byte de resposta ao cliente
tsl	milissegundo da conexão ao envio do último byte de resposta ao cliente
dis	milissegundo de conectar para desconectar (ambos os lados - último a desconectar)
log	milissegundos de ligação a este registro de registro geralmente seguido por (Política de balanço de carga e raciocínio)

x-round-trip-time	Quanto tempo levou a ALB em segundos
x-closed-by	Que ação fez com que a conexão fosse fechada (ou mantida aberta)
x-compress-acção	Como foi feita a compressão, ou evitada
x-sc(Content-Type)	Tipo de conteúdo de resposta
x-cache-acção	Como a caching respondeu, ou foi impedida
x-finish	Gatilho que causou esta fila de troncos

Limpar arquivos de log

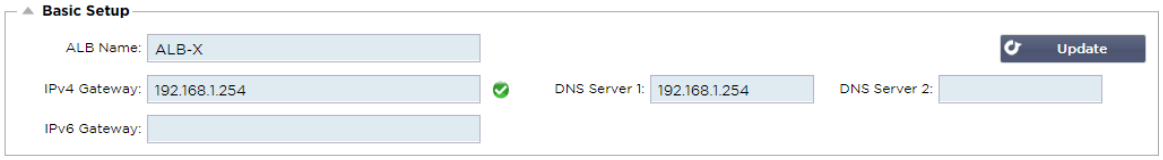


Essa característica permite que o senhor limpe os arquivos de registro do ADC. O senhor pode selecionar o tipo de registro que deseja apagar no menu suspenso e depois clicar no botão Limpar.

Rede

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

Configuração básica



ALB Nome

Especifique um nome para seu aparelho do ADC. Queira notar que isso não pode ser modificado se houver mais de um membro no agrupamento. Queira consultar a seção sobre Agrupamento.

Portão IPv4

Especifique o endereço do IPv4 Gateway. Esse endereço precisará estar na mesma sub-rede que um adaptador existente. Se o senhor acrescentar no Gateway incorretamente, verá uma Cruz Branca em um círculo vermelho. Quando o senhor acrescentar um gateway correto, verá um banner verde de sucesso no final da página e um tique branco em um círculo verde ao lado do endereço IP.

Portão IPv6

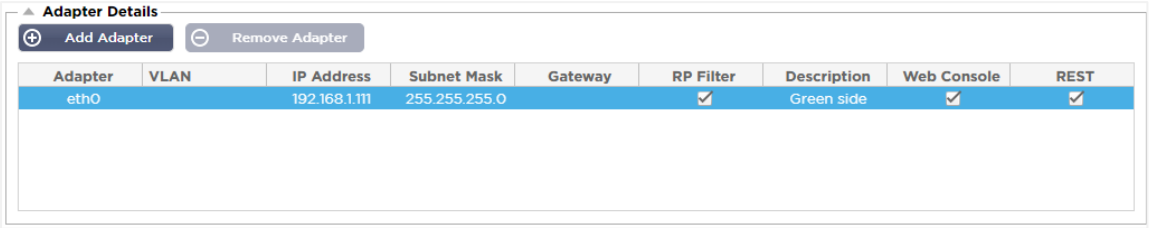
Especifique o endereço do IPv6 Gateway. Esse endereço precisará estar na mesma sub-rede que um adaptador existente. Se o senhor acrescentar no Gateway incorretamente, verá uma Cruz Branca em um círculo vermelho. Quando o usuário acrescentar um gateway correto, verá um banner verde de sucesso na parte inferior da página e uma cruz branca em um círculo verde ao lado do endereço IP.

Servidor DNS 1 e Servidor DNS 2

Adicione no endereço IPv4 do seu primeiro e segundo servidor DNS (opcional).

Detalhes do Adaptador

Esta seção do painel da Rede mostra as interfaces de rede que estão instaladas no aparelho do seu ADC. O senhor pode acrescentar e remover adaptadores, se necessário.

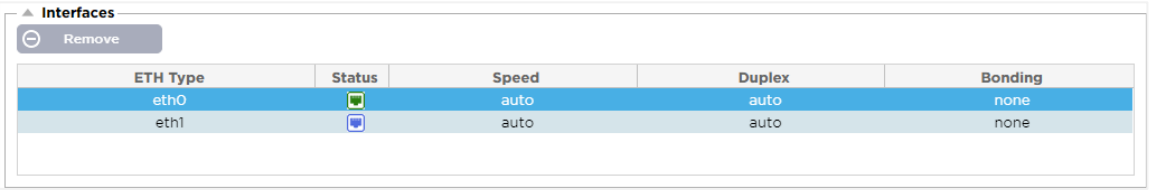


Coluna	Descrição
Adaptador	Esta coluna mostra os adaptadores físicos instalados em seu aparelho. Escolha um adaptador da lista de adaptadores disponíveis clicando sobre ele - um duplo clique colocará a linha de listagem no modo de edição.
VLAN	Clique duas vezes para acrescentar a identificação VLAN do 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 switch da rede.
Endereço IP	Clique duas vezes para acrescentar o endereço IP associado à interface do adaptador. O senhor pode acrescentar vários endereços IP à mesma interface. Esse deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 192.168.101.2
Máscara de sub-rede	Clique duplo para acrescentar a máscara de sub-rede atribuída à interface do adaptador. Esse deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 255.255.255.0
Porta de entrada	Acrescente uma porta de entrada para a interface. Quando isso for adicionado, o ADC estabelecerá uma política simples que permitirá que as conexões iniciadas a partir dessa interface sejam devolvidas, através dessa interface, ao roteador de porta de entrada especificado. Isso permite que o ADC seja instalado em ambientes de rede mais complexos sem o problema de configurar manualmente o roteamento baseado em políticas complexas.
Descrição	Faça duplo clique para acrescentar uma descrição de seu adaptador. Exemplo de interface pública. Nota: O ADC nomeará automaticamente a primeira interface Lado Verde, a segunda interface Lado Vermelho e a terceira interface Lado 3, etc. Sinta-se livre para mudar essas convenções de nomeação à sua própria escolha.
Console da Web	Clique duas vezes na coluna e depois marque a caixa para atribuir a interface como o endereço de administração para a Consola Web da Interface Gráfica do Usuário. Por favor, tenha muito cuidado ao mudar a interface que a Consola da Web irá escutar. O senhor precisará ter o roteamento correto configurado ou estar na mesma sub-rede que a nova interface, a fim de chegar ao console da Web após a mudança. A única maneira de mudar esse retorno é acessar a linha de comando e emitir o comando de configuração do lado verde. Isso eliminará todas as interfaces, exceto a eth0.

Interfaces

A seção Interfaces dentro do painel da rede permite a configuração de certos elementos relativos à interface da rede. O senhor também pode remover uma interface de rede da lista, clicando no botão

Remover. Ao usar um aparelho virtual, as interfaces que o senhor vê aqui são limitadas pela estrutura de virtualização subjacente.



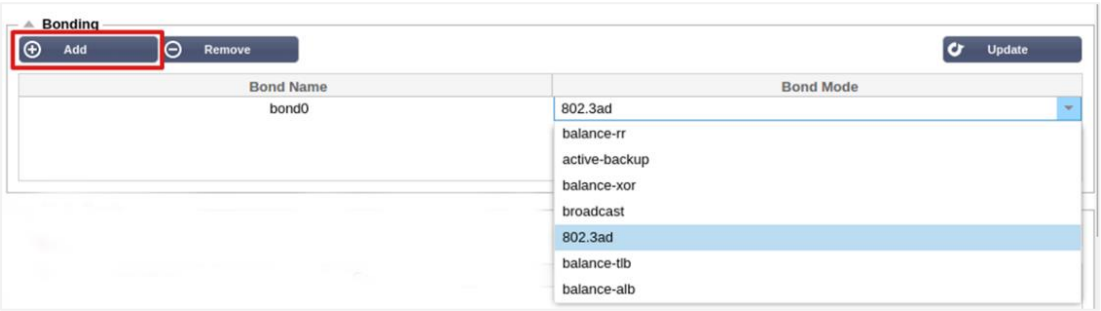
Coluna	Descrição
Tipo ETH	Esse valor indica a referência interna do sistema operacional à interface da rede. Esse campo não pode ser personalizado. Os valores começam com ETH0 e continuam em seqüência, dependendo do número de interfaces de rede.
Status	Essa indicação gráfica mostra o estado atual da interface da rede. Um status verde mostra que a interface está conectada e para cima. Outros indicadores de status são mostrados abaixo. **Adaptador UP** Adaptador Down Adaptador Desconectado Adaptador em falta
Velocidade	Por padrão, esse valor é fixado para auto-negociar a velocidade. Mas o senhor pode alterar a velocidade da rede da interface para qualquer valor disponível na queda (10/100/1000/AUTO).
Duplex	O valor desse campo é personalizável, e o senhor pode escolher entre Auto (padrão), Full-Duplex e Half-Duplex.
Ligação	O senhor pode escolher um dos tipos de vínculo que o senhor definiu. Para maiores detalhes, consulte a seção sobre as obrigações.

Ligação

Muitos nomes são usados para fazer a interface da rede de títulos: Port Trunking, Channel Bonding, Link Aggregation, NIC teaming, e outros. Bonding combina ou agrega múltiplas conexões de rede em uma única interface de canal colado. O Bonding permite que duas ou mais interfaces de rede atuem como uma só, aumentem a produção, e forneçam redundância ou failover.

O núcleo do ADC tem um driver Bonding incorporado para agregar múltiplas interfaces físicas de rede em uma única interface lógica (por exemplo, agregando eth0 e eth1 em bond0). Para cada interface bonded, o usuário pode definir o modo e as opções de monitoramento do link. Há sete opções diferentes de modo, cada uma fornecendo características específicas de balanceamento de carga e tolerância a falhas. Estas são mostradas na imagem abaixo.

NOTA: A LIGAÇÃO SÓ PODE SER CONFIGURADA PARA APARELHOS BASEADOS EM HARDWARE DO ADC.

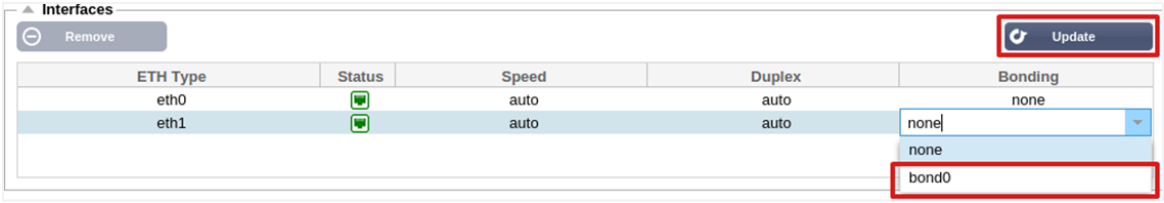


Criação de um perfil de Bonding

- Clique no botão Adicionar para adicionar uma nova Obrigação
- Fornecer um nome para a configuração do vínculo
- Escolha o modo de vinculação que deseja usar

Em seguida, na seção Interfaces, selecione o modo Bonding que deseja usar no campo Bond drop-down para a interface da rede.

No exemplo abaixo, eth0, eth1, e eth2 fazem agora parte da bond0. Enquanto o eth0 permanece por si só como interface da administração.



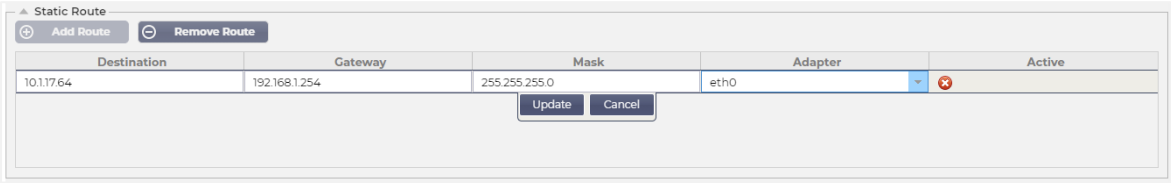
Modos de vinculação

Modo de colagem	Descrição
equilíbrio-rr:	Os pacotes são transmitidos/recebidos sequencialmente através de cada interface, um a um.
ativo de apoio:	Nesse modo, uma interface estará ativa, e a segunda interface estará em prontidão. Essa interface secundária só se tornará ativa se a conexão ativa na primeira interface falhar.
equilíbrio-xor:	Transmite com base no endereço MAC de origem XOR'd com endereço MAC de destino. Essa opção seleciona o mesmo escravo para cada endereço MAC de destino.
transmitido:	Esse modo transmitirá todos os dados sobre todas as interfaces de escravidão.
802.3ad:	Cria grupos de agregação que compartilham a mesma velocidade e configurações duplex e utiliza todos os escravos no agregador ativo, seguindo a especificação 802.3ad.
balanço-tlb:	O modo adaptativo de balanceamento de carga transmite a ligação: Fornece ligação de canal que não requer qualquer apoio especial de interruptor. O tráfego de saída é distribuído de acordo com a carga atual (computada em relação à velocidade) em cada escravo. O escravo atual recebe o tráfego de entrada. Se o escravo receptor falhar, outro escravo toma posse do endereço MAC do escravo receptor falhado.
equilíbrio - alb:	O modo de compensação de carga adaptativa: inclui também a compensação de carga de equilíbrio (rlb plus) para tráfego IPV4 e não requer qualquer suporte especial de interruptor. O balanceamento de carga de recepção é obtido pela negociação do ARP. O motorista do bonding intercepta as Respostas do ARP

	enviadas pelo sistema local na saída e sobrescreve o endereço de hardware de origem com o endereço de hardware único de um dos escravos no bond, de tal forma que diferentes pares usam endereços de hardware diferentes para o servidor.

Rota estática

Haverá momentos em que o senhor precisará criar rotas estáticas para sub-redes específicas dentro de sua rede. O ADC proporciona ao senhor a capacidade de fazer isso usando o módulo de Rotas Estáticas.



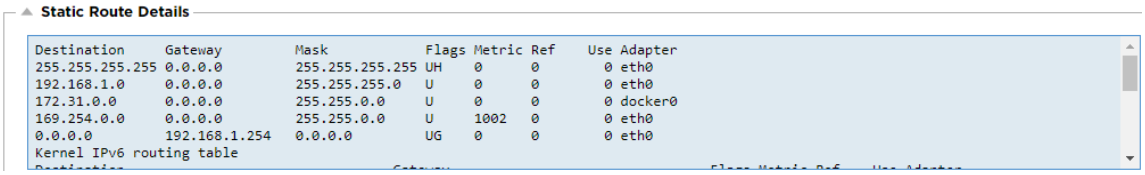
Adicionando uma rota estática

- Clique no botão Add Route
- Preencha o campo usando os detalhes da tabela abaixo como orientação.
- Clique no botão Atualizar, quando estiver pronto.

Campo	Descrição
Destino	Digite o endereço da rede de destino em notação decimal pontilhada. Exemplo 123.123.123.5
Porta de entrada	Digite o endereço IPv4 na notação decimal pontilhada. Exemplo 10.4.8.1
Máscara	Digite a máscara da sub-rede de destino em notação decimal pontilhada. Exemplo 255.255.255.0
Adaptador	Digite o adaptador em que a porta de entrada pode ser alcançada. Exemplo eth1.
Ativo	Uma caixa de seleção verde indicará que a porta de entrada pode ser alcançada. Uma cruz vermelha indicará que a porta de entrada não pode ser alcançada nessa interface. O senhor deve certificar-se de ter criado uma interface e um endereço IP na mesma rede que o portal.

Detalhes da rota estática

Esta seção fornecerá informações sobre todas as rotas configuradas no ADC.



Configurações avançadas da rede

O que é Nagle?

O algoritmo do Nagle melhora a eficiência das redes TCP/IP, reduzindo o número de pacotes que precisam ser enviados através da rede. Ver **ARTIGO DA WIKIPEDIA SOBRE O NAGLE.**

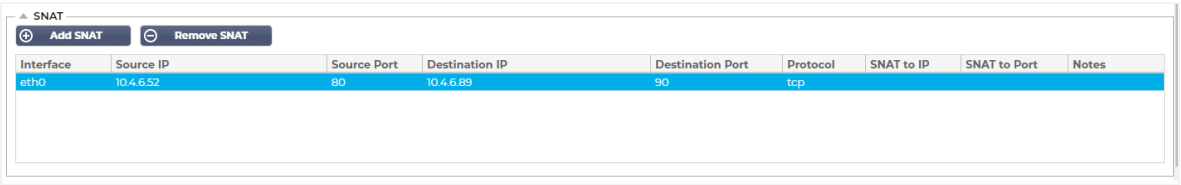
Servidor Nagle

Assinale esta caixa para permitir a configuração do Server Nagle. O Server Nagle é um meio de melhorar a eficiência das redes TCP/IP, reduzindo o número de pacotes que precisam ser enviados através da rede. Essa configuração é aplicada ao lado do Servidor da transação. Deve-se tomar cuidado com as configurações do servidor, pois o Nagle e o ACK atrasado podem ter um impacto severo no desempenho.

Cliente Nagle

Assinale a caixa para permitir o ajuste do Client Nagle. Como acima, mas aplicado ao lado do Cliente da transação.

SNAT



SNAT significa Source Network Address Translation, e diferentes fornecedores têm pequenas variações na implementação do SNAT. Uma explicação simples sobre o EdgeADC SNAT seria a seguinte.

Em circunstâncias normais, os pedidos entrantes seriam dirigidos ao VIP que veria o IP de origem do pedido. Assim, por exemplo, se um endpoint do navegador tivesse um endereço IP de 81.71.61.51, isso seria visível para o VIP.

Quando a SNAT estiver em vigor, o IP de origem original do pedido será escondido do VIP e, em vez disso, ele verá o endereço IP conforme previsto na regra da SNAT. Portanto, o SNAT pode ser usado nos modos de equilíbrio de carga de Camada 4 e Camada 7.

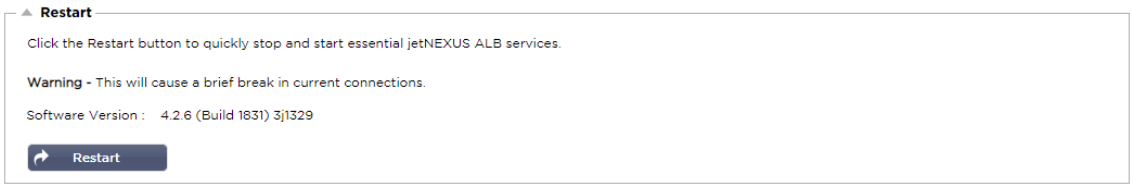
Campo	Descrição
Fonte IP	O endereço IP de origem é opcional, e pode ser ou um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser ou uma máscara de rede ou um número simples, especificando o número de 1's no lado esquerdo da máscara de rede. Assim, uma máscara de /24 é equivalente a 255.255.255.0.
PI de destino	O endereço IP de destino é opcional, e pode ser ou um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser ou 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	O porto de origem é opcional, pode ser um único número, caso em que especifica apenas esse porto, ou pode incluir dois pontos, o que especifica uma série de portos. Exemplos: 80 ou 5900:5905.
Porto de destino	O porto de destino é opcional, pode ser um único número, caso em que especifica apenas esse porto, ou pode incluir dois pontos, o que especifica uma série de portos. Exemplos: 80 ou 5900:5905.
Protocolo	O senhor pode escolher se deseja usar o SNAT em um único protocolo ou em todos os protocolos. Sugerimos ser mais específicos para ser mais precisos.
SNAT para IP	SNAT para IP é um endereço IP obrigatório ou uma gama de endereços IP. Exemplos: 10.0.0.1 ou 10.0.0.0.1-10.0.0.3.
SNAT ao Porto	O SNAT ao Porto é opcional, pode ser um número único, e nesse caso especifica apenas esse porto, ou pode incluir um traço, que especifica uma série de portos. Exemplos: 80 ou 5900-5905.

Notas	Use isso para colocar um nome amigável, para se lembrar por que as regras existem. Isso também é útil para a depuração no Syslog.

Poder

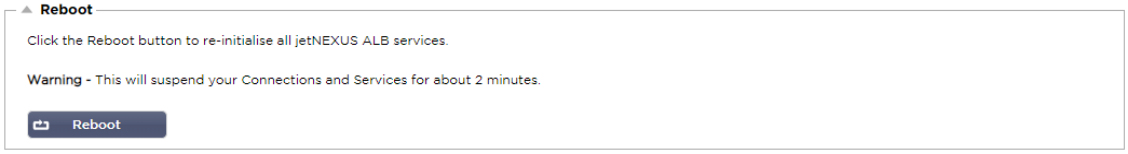
Esse sistema do ADC também permite ao senhor conduzir várias tarefas relacionadas com o poder em seu ADC.

Reinício



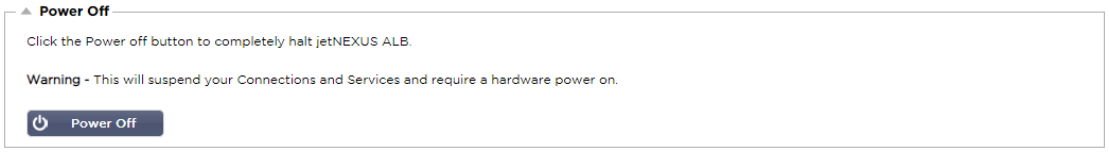
Esse cenário inicia um reinício global de todos os serviços e, conseqüentemente, quebra todas as conexões atualmente ativas. Todos os Serviços serão automaticamente retomados após um curto período, mas o tempo dependerá do número de Serviços que forem configurados. Um pop-up será exibido solicitando confirmação para a ação de reinício.

Reinicialização



Clicando no botão de reinicialização, o ADC será alimentado pelo ciclo de energia e o levará automaticamente de volta ao estado ativo. Um pop-up será exibido solicitando confirmação para a ação de reinicialização.

Desligamento



Clicando no botão de desligamento, o ADC será desligado. Se este for um aparelho de hardware, o senhor precisará de acesso físico ao dispositivo para poder ligá-lo novamente. Um pop-up será exibido solicitando confirmação para a ação de desligamento.

Segurança

Esta seção permite ao senhor alterar a senha do console da web e ativar ou desativar o acesso à Secure Shell. Ela também permite a habilitação da capacidade do REST API.

SSH

Opção	Descrição
Secure Shell Remote Conn	Marque a caixa se desejar ter acesso ao ADC usando o SSH. O "Putty" é um excelente pedido para fazer isso.

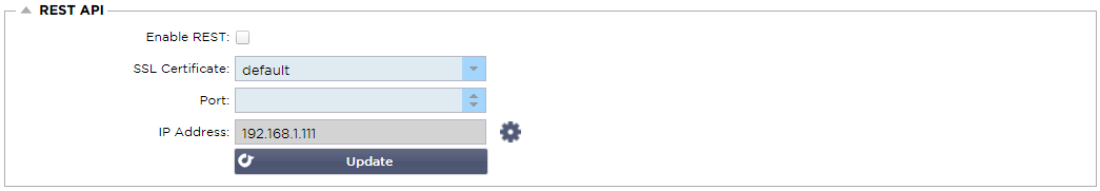
Console da Web

Certificado SSL Escolha um certificado da lista suspensa. O certificado que o senhor escolher será usado para assegurar sua conexão com a interface do usuário da ADC na Internet. O senhor pode criar um certificado autoassinado dentro do ADC ou importar um da seção de **CERTIFICADOS SSL.**

Opção	Descrição
Porto Seguro	O porto padrão para o console da web é o TCP 443. Se o senhor deseja usar um porto diferente por razões de segurança, pode mudá-lo aqui.

REST API

O REST API, também conhecido como RESTful API, é uma interface de programação de aplicações que está em conformidade com o estilo arquitetônico REST e permite a configuração do ADC ou a extração de dados do ADC. O termo REST significava transferência representativa do estado e foi criado pelo cientista da computação Roy Fielding.



Opção	Descrição
Habilitar REST	Marque esta caixa para permitir o acesso usando o REST API. Observe que o senhor também terá que configurar qual adaptador no qual o REST está habilitado. Veja a nota sobre o link Cog abaixo.
Certificado SSL	Escolha um certificado para o serviço REST. O drop-down mostrará todos os certificados instalados no ADC.
Porto	Prepare o porto para o serviço REST. É uma boa idéia usar um porto que não seja o 443.
Endereço IP	Isso mostrará o endereço IP ao qual o serviço REST está vinculado. O senhor pode clicar no link Cog para acessar a página da Rede para mudar em qual adaptador o serviço REST está habilitado.
Cog Link	Clicando neste link, o senhor será levado à página da Rede, onde poderá configurar um adaptador para o REST.

Documentação para o REST API

Documentação sobre como usar o REST API está disponível: **jetAPI | 4.2.3 | jetNEXUS | SwaggerHub**

Nota: Se o senhor receber erros na página Swagger, é porque eles têm um problema que apóia as cadeias de consulta
Passar os erros para jetNEXUS REST API

Exemplos

GUIA usando a CURL:

- Comando

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

- retornará

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

- Validade
  - O GUIA é válido por 24 horas

Detalhes da licença

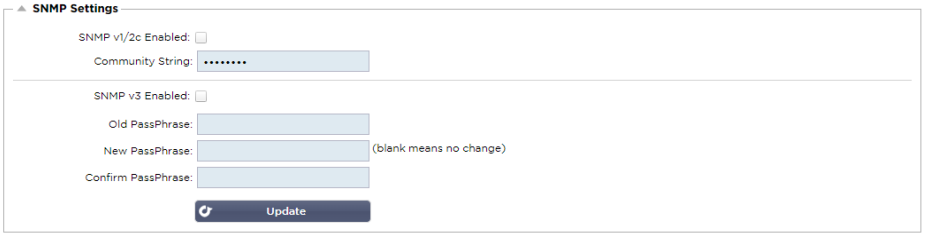
- Comando

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

SNMP

A seção SNMP permite a configuração do SNMP MIB residente dentro do ADC. A MIB pode então ser consultada por um software de terceiros capaz de se comunicar com dispositivos equipados com SNMP.

Configurações do SNMP



Opção	Descrição
SNMP v1 / V2C	Marque a caixa de seleção para habilitar o V1/V2C MIB. O SNMP v1 está em conformidade com o RFC-1157. SNMP V2c está em conformidade com o RFC-1901-1908.
SNMP v3	Marque a caixa de seleção para ativar a V3 MIB. RFC-3411-3418. O nome de usuário 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
Corda Comunitária	Esse é o conjunto de cordas apenas de leitura que é usado pelo gerente para recuperar as informações do SNMP. A cadeia padrão da comunidade é o jetnexus.
PassPhrase	Essa é a senha necessária quando o SNMP v3 está habilitado e deve ter pelo menos 8 caracteres ou mais e conter apenas as letras Aa-Zz e números 0-9. A senha padrão é **jetnexus.**

SNMP MIB

As informações visualizáveis sobre o SNMP são definidas pela Base de Informações da Administração (MIB). As MIB descrevem a estrutura dos dados da administração e usam identificadores de objeto hierárquicos (OID). Cada OID pode ser lido através de um aplicativo de administração do SNMP.

MIB Download

A MIB pode ser baixada aqui:

ADC OID

ROOT OID

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

Nossos OIDs

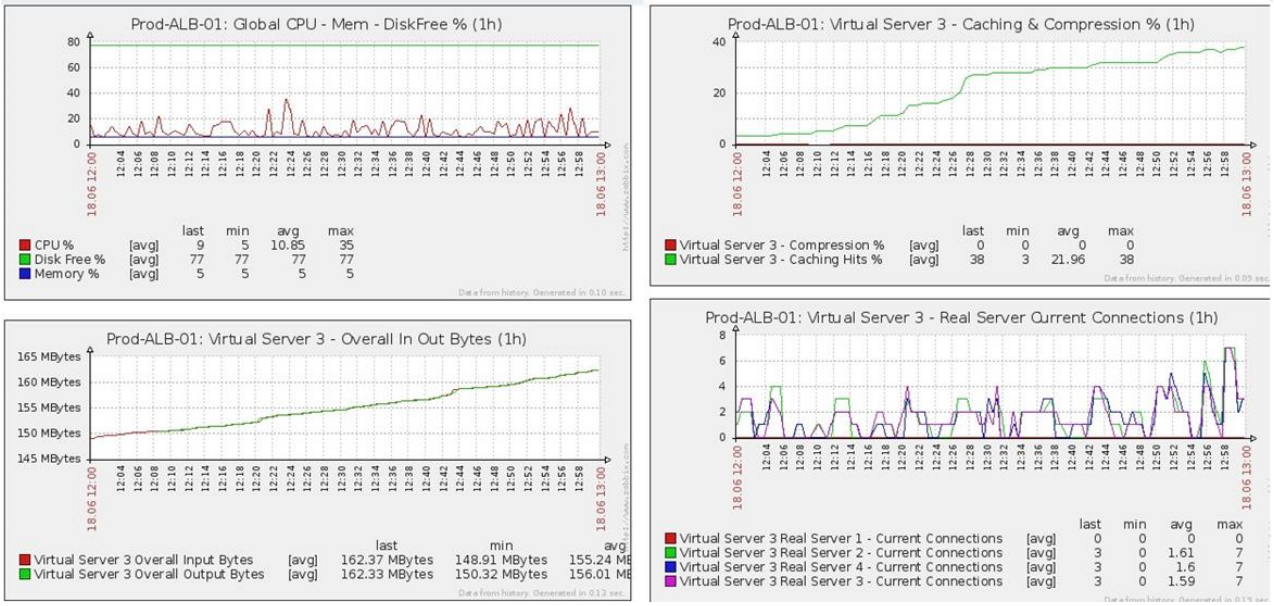
.38370 jetnexusMIB
.1 **jetnexusData (1**.3.6.1.4.1.38370.1)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.3 **jetnexusServers (1**.3.6.1.4.1.38370.1.3)
.1 **jetnexusGlobal (1**.3.6.1.4.1.38370.1.1)
.1 **jetnexusOverallInputBytes (1**.3.6.1.4.1.38370.1.1.1.1.0)
.2 **jetnexusOverallOutputBytes (1**.3.6.1.4.1.38370.1.1.1.2.0)
.3 **jetnexusCompressedInputBytes (1**.3.6.1.4.1.38370.1.1.1.3.0)
. 4 **jetnexusCompressedOutputBytes (1**.3.6.1.4.1.38370.1.1.1.4.0)
. 5 **jetnexusVersionInfo (1**.3.6.1.4.1.38370.1.1.1.5.0)
.6 **jetnexusTotalClientConnections (1**.3.6.1.4.1.38370.1.1.1.6.0)
.7 **jetnexusCpuPercent (1**.3.6.1.4.1.38370.1.1.1.7.0)
.8 **jetnexusDiskFreePercent (1**.3.6.1.4.1.38370.1.1.1.8.0)
.9 **jetnexusMemoryPercent (1**.3.6.1.4.1.38370.1.1.1.9.0)
.10 **jetnexusCurrentConnections (1**.3.6.1.4.1.38370.1.1.1.10.0)

.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**)

Gráfico Histórico

O melhor uso para o SNMP MIB personalizado do ADC é a capacidade de descarregar o gráfico histórico para um console de administração de sua escolha. Abaixo estão alguns exemplos do Zabbix que pesquisa um ADC para vários valores do OID listados acima.



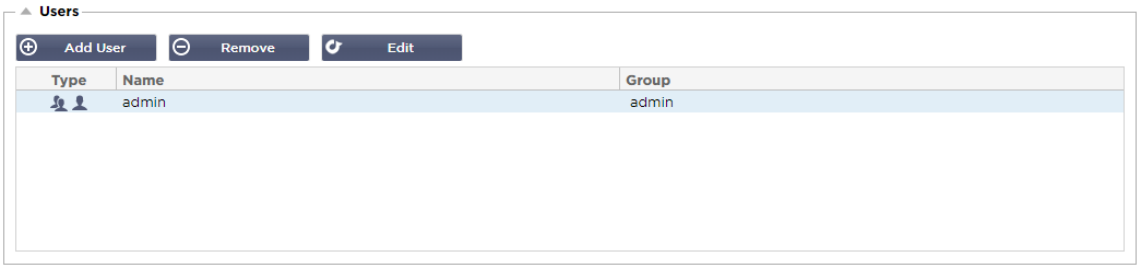
Usuários e diários de auditoria

O ADC fornece a capacidade de ter um conjunto interno de usuários para configurar e definir o que o ADC faz. Os usuários definidos dentro do ADC podem realizar uma variedade de operações, dependendo do papel a eles atribuído.

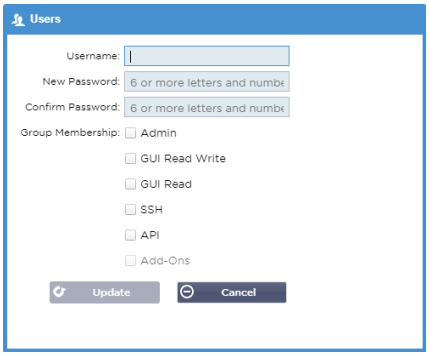
Há um usuário padrão chamado **admin** que o senhor usa quando configura o ADC pela primeira vez. A senha padrão para admin é **jetnexus**.

Usuários

A seção Usuários é fornecida para que o senhor crie, edite e remova usuários do ADC.



Adicionar Usuário



Clique no botão Adicionar Usuário, mostrado na imagem acima, para abrir o diálogo Adicionar Usuário.

Parâmetro	Descrição/uso
Nome de usuário	Digite um nome de usuário de sua escolha O nome de usuário deve estar de acordo com o seguinte: • Número mínimo de caracteres 1 • Número máximo de caracteres 32 • As cartas podem ser maiúsculas e minúsculas • Números podem ser usados • Símbolos não são permitidos
Senha	Digite uma senha **forte** que esteja de acordo com os requisitos abaixo • Número mínimo de caracteres 6 • Número máximo de caracteres 32 • Deve usar pelo menos uma combinação de letras e números • As cartas podem ser maiúsculas ou minúsculas • Os símbolos são permitidos, exceto para os do exemplo abaixo **£, %, & , < , >**
Confirmar senha	Confirmar novamente a senha para garantir que esteja correta
Participação em grupo	Assinale o grupo a que o senhor gostaria que o usuário pertencesse. • Admin - Este grupo pode fazer tudo • GUI Read Write - Os usuários deste grupo podem acessar o GUI e fazer mudanças através do GUI • GUI Read - Os usuários desse grupo podem acessar o GUI apenas para ver informações. Nenhuma alteração pode ser feita. • SSH - Os usuários desse grupo podem acessar o ADC através da Secure Shell. Essa escolha dará acesso à linha de comando, que tem um conjunto mínimo de comandos disponíveis. • API - Os usuários desse grupo terão acesso à interface programável SOAP e REST. REST estará disponível a partir da versão 4.2.1 do software.

Tipo de usuário

	Usuário local **O ADC no papel de "Stand-Alone" ou Manual H/A criará apenas Usuários Locais** **Por padrão,** um usuário local chamado "admin" **é um membro do grupo administrativo. Para compatibilidade retroativa**, **esse usuário nunca poderá ser eliminado.** **O usuário pode alterar a senha deste usuário ou apagá-la**, **mas não pode apagar o último administrador local.**
	Usuário do Cluster O ADC no papel de Cluster criará somente Cluster Users Os usuários do Cluster estão sincronizados em todos os ADCs do Cluster Qualquer mudança para um usuário do cluster mudará em todos os membros do cluster Se você estiver logado como usuário de cluster, não poderá mudar de funções de Cluster para Manual ou Stand-Alone.
	Cluster e Usuário Local Qualquer usuário criado enquanto estiver na função Stand-Alone ou Manual será copiado para o Cluster Se o ADC posteriormente deixar o Cluster, então somente os Usuários Locais permanecerão A última senha configurada para o usuário será válida

Remoção de um usuário

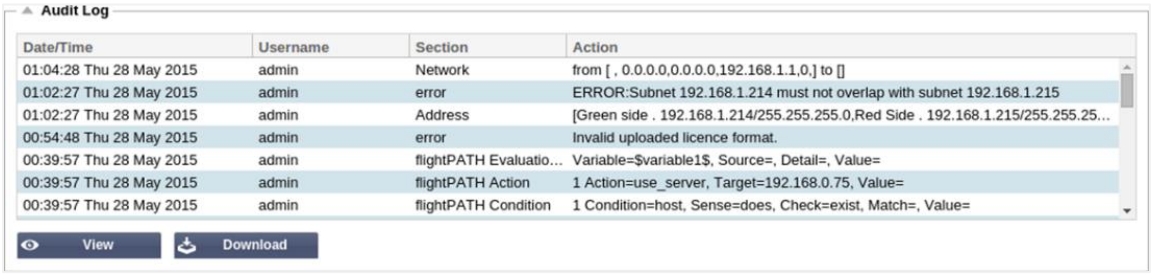
- Destacar um usuário existente
- Clique Remover
- O usuário não poderá eliminar o usuário que está atualmente assinado em
- O senhor não poderá remover o último usuário local do grupo administrativo
- O senhor não poderá remover o último usuário restante do grupo de administração.
- O senhor não poderá eliminar o usuário administrativo por compatibilidade retroativa
- Se o senhor remover o ADC do agrupamento, todos os usuários, exceto os usuários locais, serão excluídos

Edição de um usuário

- Destacar um usuário existente
- Clique em Editar
- O usuário pode mudar a composição do grupo de usuários, marcando as caixas apropriadas e atualizando
- O usuário também pode alterar a senha de um usuário, desde que tenha direitos administrativos

Diário de Auditoria

O ADC registra as mudanças feitas na configuração do ADC por usuários individuais. O registro de auditoria fornecerá as últimas 50 ações realizadas por todos os usuários. O senhor também pode ver TODAS as entradas na seção de **LOGS.** Por exemplo:



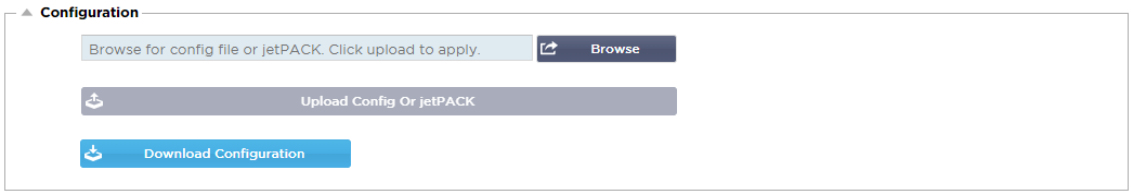
Audit Log

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

View Download

Avançado

Configuração



É sempre uma boa prática descarregar e salvar a configuração do ADC uma vez que ele esteja totalmente instalado e funcionando conforme necessário. O usuário pode usar o módulo de configuração tanto para fazer o download quanto para fazer o upload de uma configuração.

Os Jetpacks são arquivos de configuração para aplicações padrão e são fornecidos pela Edgenexus para simplificar seu trabalho. Esses também podem ser carregados para o ADC usando o módulo de configuração.

Um arquivo de configuração é essencialmente um arquivo de texto, e como tal, pode ser editado pelo senhor usando um editor de texto como o Notepad++ ou VI. Uma vez editado conforme necessário, o arquivo de configuração pode ser carregado no ADC.

Descarregar uma configuração

- Para baixar a configuração atual do ADC, pressione o botão Download Configuration.
- Aparecerá um pop-up pedindo-lhe que abra ou salve o arquivo .conf.
- Salvo em um local conveniente.
- O senhor pode abrir isto com qualquer editor de texto, como o Notepad++.

Carregamento de uma configuração

- O senhor pode fazer o upload de um arquivo de configuração salvo, navegando pelo arquivo .conf salvo.
- Clique no botão "Upload Config ou Jetpack".
- O ADC fará o upload e aplicará a configuração e depois atualizará o navegador. Se ele não atualizar o navegador automaticamente, por favor, clique em atualizar o navegador.
- O senhor será redirecionado para a página do Painel após a conclusão.

Carregar um jetPACK

- Um jetPACK é um conjunto de atualizações de configuração para a configuração existente.
- Um jetPACK pode ser tão pequeno quanto alterar o valor do TCP Timeout até uma configuração completa específica da aplicação, como o Microsoft Exchange ou o Microsoft Lync.
    - O senhor pode obter um JetPACK no portal de apoio mostrado no final deste guia.
- Procure o arquivo jetPACK.txt.
- Clique em upload.
- O navegador será atualizado automaticamente após o upload.
- O senhor será redirecionado para a página do Painel após a conclusão.
- A importação pode levar mais tempo para implantações mais complexas, como a Microsoft Lync, etc.

Configurações globais

A seção de configurações globais permite ao senhor mudar vários elementos, inclusive a biblioteca criptográfica SSL.

Timer Cache anfitrião

O Host Cache Timer é uma configuração que armazena o endereço IP de um servidor real por um determinado período quando o nome de domínio foi usado em vez de um endereço IP. O cache é descarregado em caso de falha do Servidor Real. Fixar esse valor em zero evitará que o cache seja enxaguado. Não há valor máximo para essa configuração.

Dreno

O recurso de drenagem é configurável para cada Servidor Real vinculado a um Serviço Virtual. Por padrão, a configuração Drain Clears Persistence está habilitada, permitindo que os servidores que são colocados em modo Drain terminem as sessões graciosamente para que possam ser tirados do ar para manutenção.

SSL

Essa configuração global permite que a biblioteca SSL seja modificada conforme a necessidade. A biblioteca criptográfica SSL padrão usada pela ADC é da OpenSSL. Se o senhor quisesse usar uma biblioteca criptográfica diferente, isso poderia ser mudado aqui.

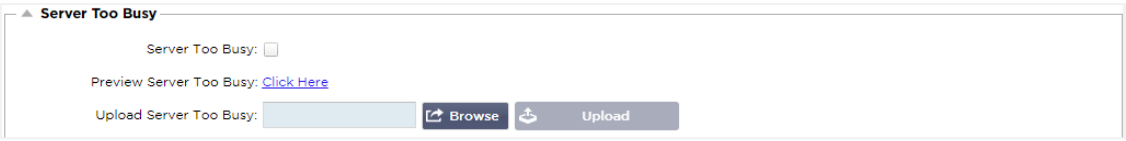
Autenticação

Esse valor estabelece o tempo limite para a autenticação, após o qual a tentativa de autenticação terá sido considerada como fracassada.

Protocolo

A seção do protocolo é usada para definir as muitas configurações avançadas para o protocolo HTTP.

Servidor muito ocupado



Suponhamos que o senhor tenha limitado as Max Connections a seus verdadeiros servidores; o senhor pode optar por apresentar uma página da internet amigável uma vez que esse limite tenha sido atingido.

- Crie uma página web simples com sua mensagem. O senhor pode incluir links externos para objetos em outros servidores e sites da web. Alternativamente, se o senhor quiser ter imagens em sua página da web, então use imagens codificadas na base64 em linha.
- Procure o arquivo HTM(L) de sua nova página web
- Clique em Upload
- Se o senhor deseja visualizar a página, pode fazê-lo com o link "Clique aqui

Encaminhado para

Forwarded For é o padrão de fato para identificar o endereço IP de origem de um cliente conectado a um servidor web por meio de equilibradores de carga de camada 7 e servidores proxy.

Encaminhados-Para Produção

Opção	Descrição
Off	O ADC não altera o cabeçalho Forwarded-For.
Acrescentar endereço e porto	Essa escolha anexará o endereço IP e o porto, do dispositivo ou cliente conectado ao ADC, ao cabeçalho Forwarded-For.
Acrescentar endereço	Essa escolha anexará o endereço IP, do dispositivo ou cliente conectado ao ADC, ao cabeçalho Forwarded-For.
Substituir Endereço e Porto	Essa escolha substituirá o valor do cabeçalho do Forwarded-For pelo endereço IP e porta do dispositivo ou cliente conectado ao ADC.
Substituir o endereço	Essa escolha substituirá o valor do cabeçalho do Forwarded-For pelo endereço IP do dispositivo ou cliente conectado ao ADC.

Encaminhado - Por Cabeçalho

Esse campo permite ao senhor especificar o nome dado ao cabeçalho Forwarded-For. Normalmente, esse é "X-Forwarded-For", mas pode ser modificado para alguns ambientes.

Logging avançado para o IIS - Logging personalizado

O senhor pode obter o X-Forwarded-For information instalando o aplicativo IIS Advanced logging 64-bit. Uma vez baixado, crie um campo de registro personalizado chamado X-Forwarded-For com as configurações abaixo.

Selecione Default da lista de Tipo de Fonte na lista de Categoria, selecione Request Header na caixa Source Name, e digite X-Forwarded-For.

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

Apache HTTPd.conf muda

O senhor vai querer fazer várias mudanças no formato padrão para registrar o endereço IP X-Forwarded-For do cliente ou o endereço IP real do cliente, se o cabeçalho X-Forwarded-For não existir.

Essas mudanças estão abaixo:

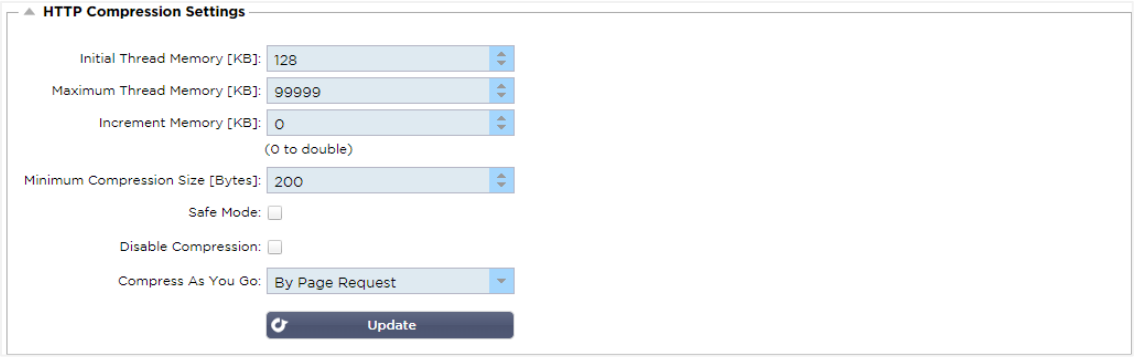
Tipo	Valor
LogFormat:	"%h %l %u %t "%r`" %>s %b {Referer}i}" \"% (Usuário-Agente) i)" combinado
LogFormat:	"% (X-Forwarded-For)i %l %u %t "%r^" %>s %b {Referer}i}" \"% (Usuário-Agente)" proxy SetEnvIf X- Forwarded-For "^.*...*...*...*" enviado
CustomLog:	"logs/access_log" combined env=!forwarded
CustomLog: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

Esse formato aproveita o apoio incorporado do Apache para o corte condicional baseado em variáveis ambientais.

- A linha 1 é a seqüência padrão combinada de caracteres de log, em formato de log, do padrão.
- A linha 2 substitui o campo %h (host remoto) pelo(s) valor(es) retirado(s) do cabeçalho do X-Forwarded-For e define o nome desse padrão de arquivo de log como "proxy".
- A linha 3 é um ajuste para a variável de ambiente "encaminhada" que contém uma expressão regular frouxa que corresponde a um endereço IP, o que está bem neste caso, já que nos preocupamos mais com a existência de um endereço IP no cabeçalho do X-Forwarded-For.
- Além disso, a linha 3 poderia ser lida como: "Se houver um valor X-Forwarded-For, use-o".
- As linhas 4 e 5 dizem ao Apache qual o padrão de tronco a ser usado. Se houver um valor X-Forwarded-For, use o padrão "proxy", ou use o padrão "combinado" para o pedido. Para a legibilidade, as linhas 4 e 5 não aproveitam o recurso de registro de logs rotativos (encanados) do Apache, mas supomos que quase todos o usam.

Essas mudanças resultarão no registro de um endereço IP para cada pedido.

Configurações de Compressão HTTP

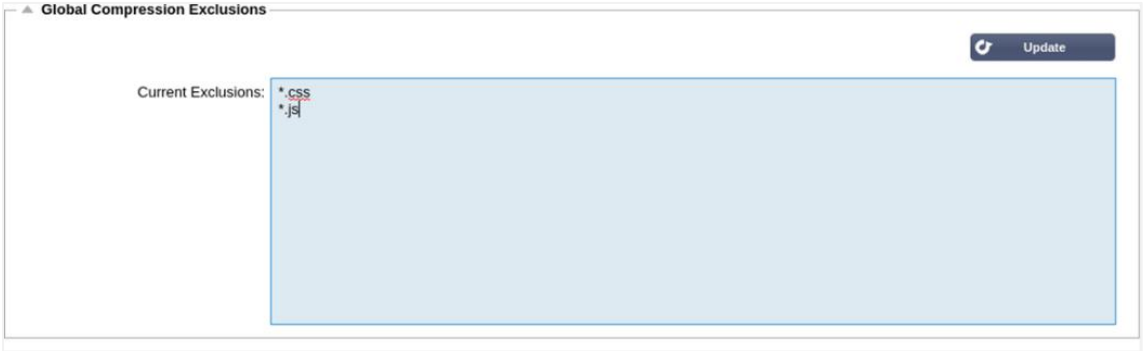


A compressão é uma característica de aceleração e está habilitada para cada Serviço na página de Serviços de PI.

AVISO - Tome extremo cuidado ao ajustar esses ajustes, pois ajustes inadequados podem afetar adversamente o desempenho do ADC

Opção	Descrição
Memória do fio inicial [KB]	Esse valor é a quantidade de memória que cada pedido recebido pela ADC pode destinar inicialmente. Para um desempenho mais eficiente, esse valor deve ser fixado em um valor que exceda o maior arquivo HTML não comprimido que os servidores da rede provavelmente enviarão.
Memória Máxima de Fio [KB]	Esse valor é a quantidade máxima de memória que o ADC alocará em um pedido. Para um desempenho máximo, o ADC normalmente armazena e comprime todo o conteúdo em memória. Se um arquivo de conteúdo excepcionalmente grande exceder essa quantidade for processado, o ADC gravará em disco e comprimirá os dados lá.
Memória de Incremento [KB]	Esse valor define a quantidade de memória adicionada à alocação inicial de memória do fio quando mais é necessário. A configuração padrão é zero. Isso significa que o ADC duplicará a alocação quando os dados excederem a alocação atual (por exemplo, 128Kb, depois 256Kb, depois 512Kb, etc.) até o limite estabelecido pelo uso máximo de memória por linha. Isso é eficiente quando a maioria das páginas é de tamanho consistente, mas ocasionalmente há arquivos maiores. (por exemplo, a maioria das páginas são de 128Kb ou menos, mas ocasionalmente há respostas de 1Mb de tamanho). No cenário onde há arquivos de grande tamanho variável, é mais eficiente estabelecer um incremento linear de tamanho significativo (por exemplo, as respostas são de 2Mb a 10Mb de tamanho, um ajuste inicial de 1Mb com incrementos de 1Mb seria mais eficiente).
Tamanho Mínimo de Compressão [Bytes]	Esse valor é o tamanho, em bytes, sob o qual o ADC não tentará comprimir. Isso é útil porque qualquer coisa muito abaixo de 200 bytes não se comprime bem e pode até crescer em tamanho devido às despesas gerais de cabeçalhos de compressão.
Modo Seguro	Marque essa opção para evitar que o ADC aplique compressão nas folhas de estilo do JavaScript. A razão para isso é que, embora a ADC esteja ciente de quais navegadores individuais podem lidar com conteúdo comprimido, alguns outros servidores proxy, embora afirmem ser compatíveis com HTTP/1.1, não conseguem transportar corretamente as folhas de estilo compactadas e o JavaScript. Se estiverem ocorrendo problemas com folhas de estilo ou JavaScript através de um servidor proxy, então use essa opção para desativar a compressão desses tipos. No entanto, isso reduzirá a quantidade total de compressão de conteúdo.
Desabilitar a Compressão	Assinale isso para impedir que a ADC comprima qualquer resposta.
Comprime enquanto você vai	ON - Use o Compress as You Go nesta página. Isso comprime cada bloco de dados recebidos do servidor em um pedaço discreto que é totalmente descomprimível. OFF - Não use Compress as You Go on this page. By Page Request - Use Compress as You Go by page request (Por pedido por página).

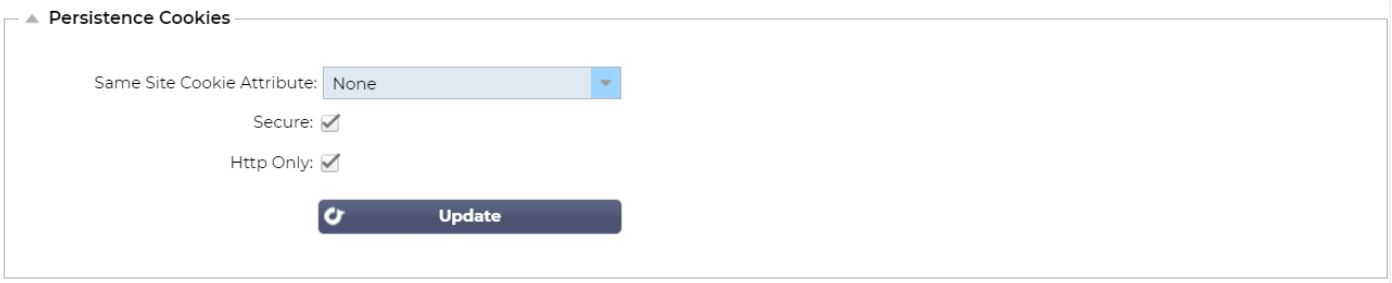
Exclusões de Compressão Global



Qualquer página com a extensão acrescentada na lista de exclusão não será comprimida.

- Digite o nome do arquivo individual.
- Clique em atualizar.
- Se o senhor deseja acrescentar um tipo de arquivo, basta digitar "*.css" para que todas as folhas de estilo em cascata sejam excluídas.
- Cada arquivo ou tipo de arquivo deve ser acrescentado a uma nova linha.

Biscoitos de persistência



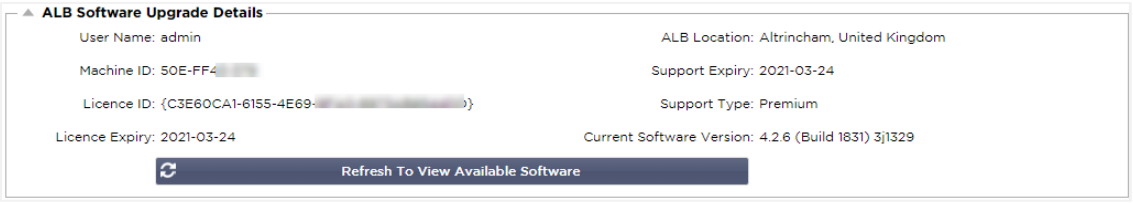
Essa configuração permite ao senhor especificar como os cookies de persistência são tratados.

Campo	Descrição
Mesmo site Atributo de Cooke	**Nenhum**: Todos os cookies são acessíveis a scripts **Lax**: Impede que cookies sejam acessados através dos sites, mas eles são armazenados para se tornarem acessíveis e submetidos ao site proprietário, caso seja visitado. **Estrito**: impede qualquer cookie para um site diferente de ser acessado ou armazenado **Desligado**: volta ao comportamento padrão do navegador
Segurança	Esta caixa de seleção, quando marcada, aplica a persistência para assegurar o tráfego
Somente HTTP	Quando verificado, isto permite Cozinheiros Persistentes somente no tráfego HTTP

Software

A seção de software permite ao senhor atualizar a configuração e o firmware de seu ADC.

Detalhes da atualização do software



As informações contidas nesta seção serão preenchidas se o senhor tiver uma conexão de Internet funcionando. Se seu navegador não tiver um link para a Internet, esta seção ficará em branco. Uma vez conectado, o senhor receberá a mensagem de banner abaixo.

We have successfully connected to Cloud Services Manager to retrieve your Software Update Details

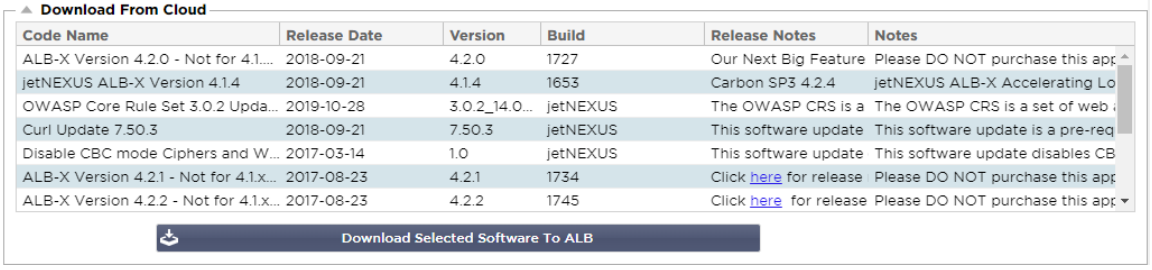
A seção Download da Nuvem mostrada abaixo será preenchida com informações mostrando as atualizações disponíveis para o senhor sob seu plano de apoio. O senhor deve prestar atenção ao tipo de apoio e à data de expiração do apoio.

Nota: Usamos a conexão do seu navegador com a Internet para ver o que está disponível no Edgenexus Cloud. O senhor só poderá baixar atualizações de software se o ADC tiver uma conexão com a Internet.

Para verificar isso:

- Advanced-- Resolução de problemas--Ping
- Endereço IP - appstore.edgenexus.io
- Clique Ping
- Se o resultado mostrar "ping: unknown host appstore.edgenexus.io". "
- O ADC NÃO poderá baixar nada da nuvem

Baixar do Cloud



Se seu navegador estiver conectado à Internet, o senhor verá detalhes do software disponível na nuvem.

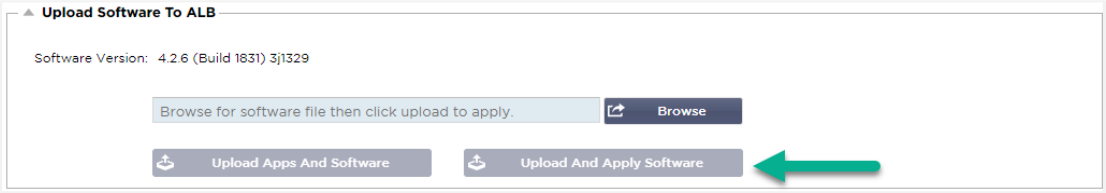
- Destaque a linha em que está interessado e clique em "Download Selected Software to ALB". botão ".
- O software selecionado será baixado para sua ALB quando clicado, o que pode ser aplicado na seção "Apply Software Stored on ALB" abaixo.

Nota: Se o ADC não tiver acesso direto à Internet, o senhor receberá um erro como o que está abaixo:

Erro de download, ALB não conseguiu acessar o ADC Cloud Services para o arquivo build1734-3236-v4.2.1-Sprint2-update-64.software.alb

Upload de software para a ALB

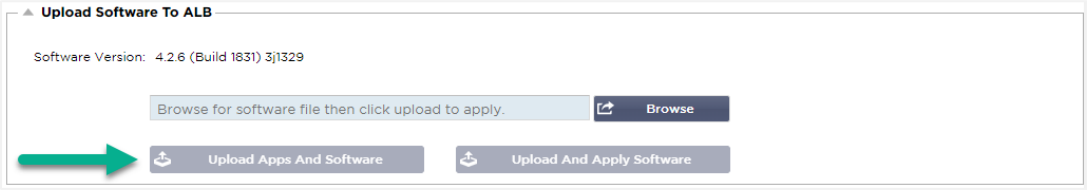
Upload de aplicativos



Se o senhor tem um arquivo App que termina com <apptype>.alb, pode usar esse método para carregá-lo.

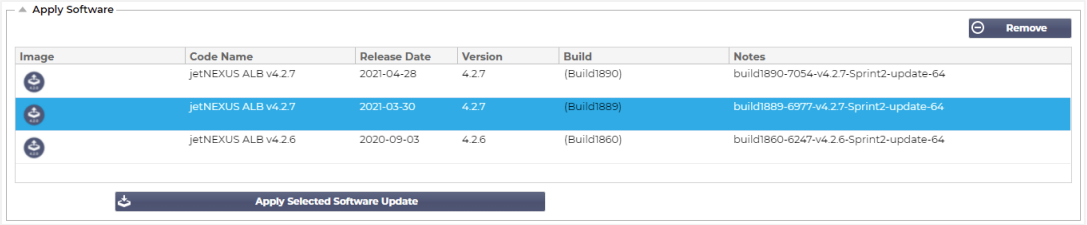
- Há cinco tipos de Apêndice
  - <appname>flightpath.alb
  - <appnome>.monitor.alb
  - <appnome>.jetpack.alb
  - <appnome>.addons.alb
  - <appnome>.featurepack.alb
- Uma vez carregados, cada app será encontrado na seção Biblioteca > Apps.
- O senhor deve, então, implantar cada Apêndice nessa seção individualmente.

Software



- Se o senhor deseja carregar o software sem aplicá-lo, então use o botão destacado.
- O Arquivo de Software é <softwarename>.software.alb.
- Em seguida, será mostrado na seção "Software Stored on ALB", de onde o senhor poderá aplicá-lo de acordo com sua conveniência.

Aplicar o software armazenado na ALB



Esta seção mostrará todos os arquivos de software armazenados na ALB e disponíveis para distribuição. A lista incluirá assinaturas atualizadas do Web Application Firewall (WAF).

- Destaque a linha de software que o senhor está interessado em usar.
- Clique em "Apply Software from Selected".
- Se esta for uma Atualização de Software da ALB, favor estar ciente de que ela fará o upload e então reiniciará a ALB para se candidatar.
- Se a atualização que o senhor está solicitando for uma atualização de assinatura da OWASP, ela será aplicada automaticamente sem reinicialização.

Solução de problemas

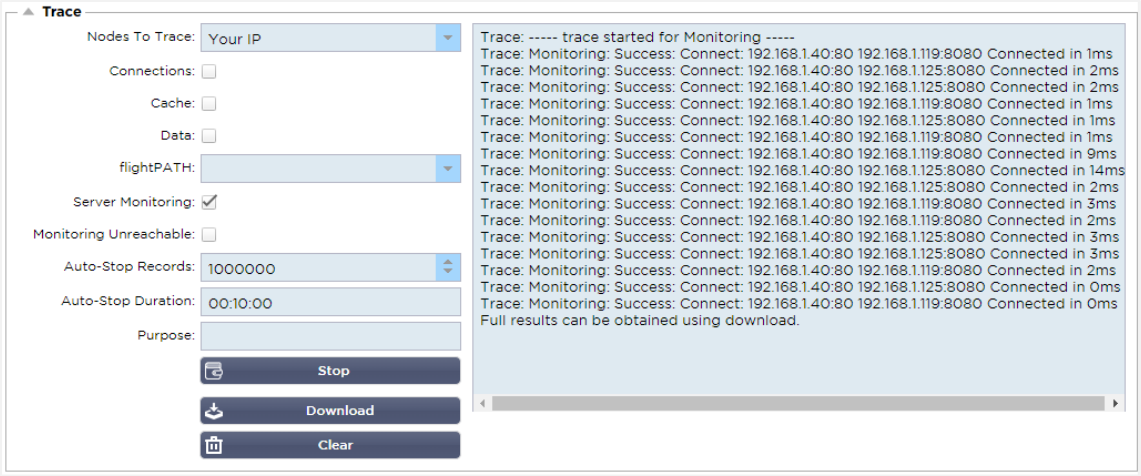
Há sempre questões que requerem solução de problemas para se chegar a uma causa e solução de raiz. Esta seção permite que o senhor faça isso.

Arquivos de apoio

Se o senhor tiver algum problema com o ADC e precisar abrir um ticket de apoio, o Suporte Técnico solicitará freqüentemente vários arquivos diferentes do aparelho do ADC. Esses arquivos foram agora agregados em um único arquivo .dat que pode ser baixado através desta seção.

- Selecione um cronograma a partir do menu suspenso: A escolha de 3, 7, 14, e Todos os dias estão à sua disposição.
- Clique em "Baixar arquivos de apoio".
- Um arquivo será baixado no formato Support-jetNEXUS-yyyymmddhh-NAME.dat
- Levantem um ticket de apoio no portal de apoio, cujos detalhes estão disponíveis no final deste documento.
- O senhor deve descrever o problema de maneira completa e anexar o arquivo .dat ao bilhete.

Trace



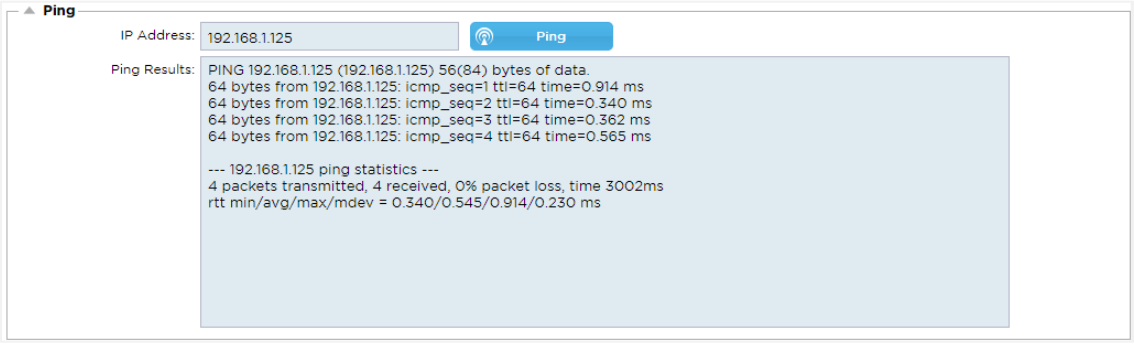
A seção Trace permitirá ao senhor examinar informações que permitam a depuração da questão. As informações entregues dependem das opções que o senhor escolher entre os drop-downs e os tick boxes.

Opção	Descrição
Nodos para rastrear	**Seu IP**: Isso filtrará a saída para usar o endereço IP de onde você está acessando o GUI (Nota: não escolha esta opção para Monitoramento, pois o Monitoramento usará o endereço de interface do ADC) **Todos os PI**: Nenhum filtro será aplicado. Deve-se observar que em uma caixa ocupada isso afetará adversamente o desempenho.
Conexões	Essa caixa de seleção, quando marcada, mostrará ao senhor informações sobre as conexões do lado do cliente e do lado do servidor.
Cache	Este campo assinalado mostrará ao senhor informações relativas aos objetos em cache.

Dados	Quando essa caixa de seleção estiver marcada, ela incluirá os bytes de dados brutos tratados pelo ADC.
vôoPATH	O menu flightPATH permite ao senhor selecionar uma regra FlightPATH específica para monitorar ou Todas as regras flightPATH.
Monitoramento do servidor	Essa caixa de seleção, quando marcada, mostrará aos monitores de saúde do servidor ativos no ADC e seus respectivos resultados.
Monitoramento Inacessível	Quando essa opção é selecionada, é muito parecida com o monitoramento do comportamento do servidor, exceto que só mostrará os monitores que falharam e assim atua como um filtro apenas para essas mensagens.
Registros de Auto-Stop	O valor padrão é de 1.000.000 de registros, após o que a instalação de Rastreamento parará automaticamente. Esse ajuste é uma precaução de segurança para evitar que o Trace seja deixado acidentalmente e afete seu desempenho no ADC.
Duração do Auto-Stop	O tempo padrão é fixado em 10 minutos, após os quais a instalação de Trace parará automaticamente. Essa característica é uma precaução de segurança para evitar que o Trace seja deixado acidentalmente ligado e afete o desempenho do ADC.
Início	Clique aqui para iniciar manualmente a instalação de Trace.
Parada	Clique para parar manualmente a instalação de Trace antes que o registro automático ou o tempo seja alcançado.
Download	Embora o senhor possa ver o espectador ao vivo no lado direito, as informações podem ser exibidas muito rapidamente. Em vez disso, o senhor pode baixar o Trace.log para ver todas as informações coletadas durante os vários traços desse dia. Esse recurso é uma lista filtrada de informações sobre os vestígios. Se o senhor deseja ver as informações de rastreamento dos dias anteriores, pode baixar o Syslog para esse dia, mas terá que filtrar manualmente.
Clear	Limpa o diário de bordo

Ping

O senhor pode verificar a conectividade de rede com servidores e outros objetos de rede em sua infra-estrutura, usando a ferramenta Ping.



Digite o endereço IP do anfitrião que deseja testar, por exemplo, o gateway padrão usando uma notação decimal pontilhada ou um endereço IPv6. O senhor poderá ter que esperar alguns segundos para que o resultado seja respondido uma vez que tenha pressionado o botão "Ping".

Se o senhor tiver configurado um servidor DNS, então poderá digitar o nome de domínio totalmente qualificado. O usuário pode configurar um servidor DNS na seção **SERVIDOR DNS 1 E SERVIDOR DNS 2.**

Talvez o senhor tenha que esperar alguns segundos para que o resultado seja respondido uma vez que tenha pressionado o botão "Ping".

Captura

Para captar o tráfego da rede, siga as instruções simples abaixo.

- Preencher as opções no formulário
- Clique Gerar
- Uma vez feita a captura, seu navegador vai aparecer e perguntar-lhe onde deseja salvar o arquivo. Ele estará no formato "jetNEXUS.cap.gz".
- Levantem um ticket de apoio no portal de apoio, cujos detalhes estão disponíveis no final deste documento.
- Certifique-se de descrever o problema de maneira completa e anexe o dossiê ao bilhete.
- O senhor também pode ver o conteúdo usando Wireshark

Opção	Descrição
Adaptador	Escolha seu adaptador a partir do drop-down, tipicamente eth0 ou eth1. O senhor também pode capturar todas as interfaces com "qualquer".
Pacotes	Esse valor é o número máximo de pacotes a serem capturados. Tipicamente, 99999
Duração	Escolha um tempo máximo para o qual a captura será feita. Um tempo típico é de 15 segundos para locais de alto tráfego. O GUI ficará inacessível durante o período de captura.
Endereço	Esse valor será filtrado em qualquer endereço IP digitado na caixa. Deixe isso em branco para que não haja filtro.

Para manter o desempenho, limitamos o arquivo de download a 10MB. Se o senhor achar que isso não é suficiente para capturar todos os dados necessários, podemos aumentar esse número.

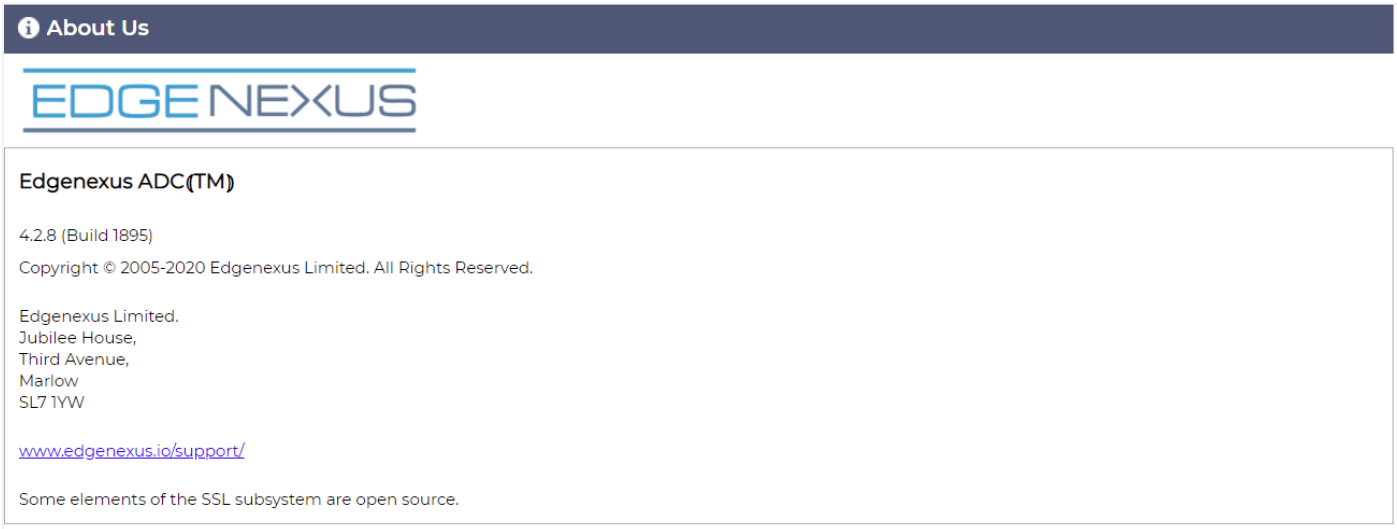
Nota: Isso terá um impacto sobre o desempenho de locais ao vivo. Para aumentar o tamanho da captura disponível, favor aplicar um jetPACK de configuração global para aumentar o tamanho da captura.

Ajuda

A seção de Ajuda fornece acesso às informações sobre o Edgenexus e acesso aos guias do usuário e outras informações úteis.

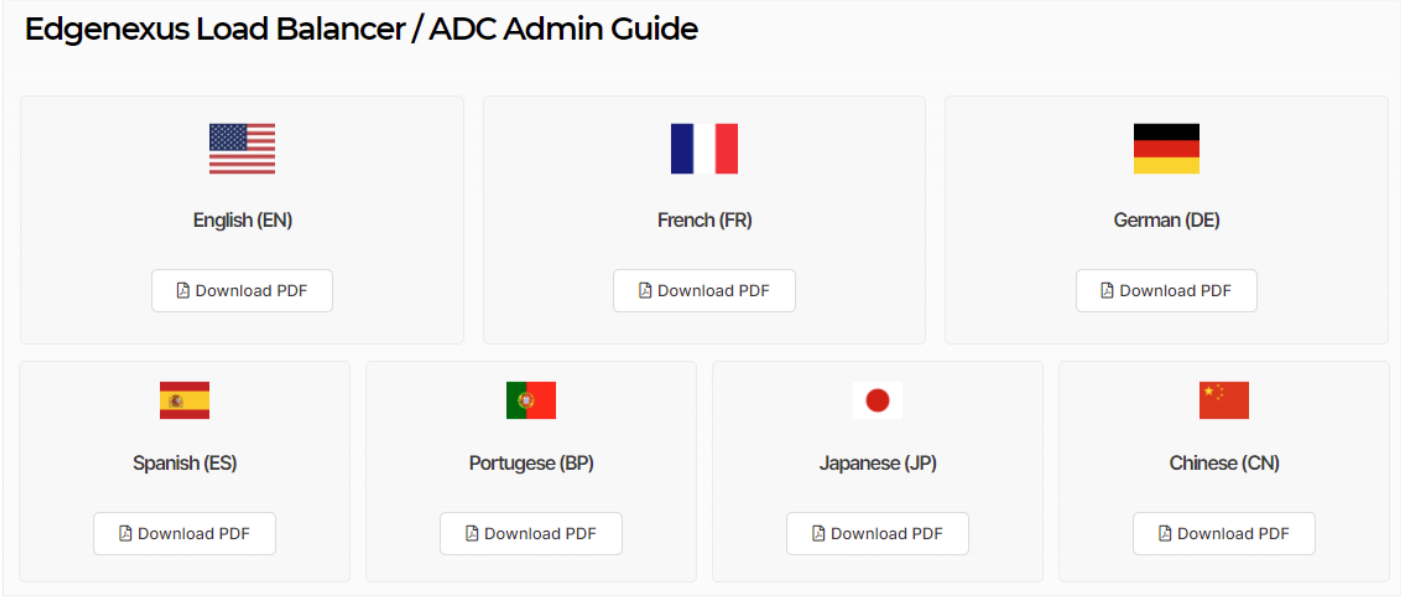
Sobre nós

Clicando na opção "Sobre nós", serão exibidas informações sobre a Edgenexus e seu escritório corporativo.



Referência

A opção de referência abrirá a página contendo guias de usuário e outros documentos úteis.



Se o senhor não encontrar o que procura, queira contatar support@edgenexus.io.

O que é um jetPACK

Os jetPACKs são um método único de configuração instantânea de seu ADC para aplicações específicas. Esses modelos fáceis de usar vêm pré-configurados e totalmente sintonizados com todas as configurações específicas de aplicações que o senhor precisa para desfrutar de uma prestação de serviços otimizada a partir de seu ADC. Alguns dos jetPACKs usam o flightPATH para manipular o tráfego, e o senhor deve ter uma licença flightPATH para que esse elemento funcione. Para saber se o senhor tem uma licença para o flightPATH, favor consultar a página da **LICENÇA.**

Descarregamento de 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 de IP Virtual de 1.1.1.1
- O senhor pode carregar esse jetPACK como está e mudar o endereço IP na GUI ou editar o jetPACK com um editor de texto como o Notepad++ e pesquisar e substituir 1.1.1.1 por seu endereço IP Virtual.
- Além disso, cada JetPACK foi criado com 2 servidores reais com endereços IP de 127.1.1.1 e 127.2.2.2.2. Novamente o senhor pode mudá-los no GUI após o upload ou antes, usando o Notepad++.
- Clique em um link jetPACK abaixo e Salve o link como um arquivo jetPACK-VIP-Application.txt em seu local escolhido

Microsoft Exchange

Aplicação	Link para download	O que é que isso faz?	O que está incluído?
Intercâmbio de 2010	jetPACK-1.1.1.1-Exchange-2010	Esse jetPACK acrescentará as configurações básicas para o balanço de carga do Microsoft Exchange 2010. Há uma regra FlightPATH incluída para redirecionar o tráfego no serviço HTTP para HTTPS, mas é uma opção. Se o senhor não tiver uma licença para o flightPATH, esse jetPACK ainda funcionará.	Configurações globais: Tempo de serviço de 2 horas Monitores: Monitor de camada 7 para o aplicativo Outlook web, e monitor de camada 4 fora da banda para o serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de serviço virtuais: 80, 443, 135, 59534, 59535 Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento do HTTP para HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	O mesmo que acima, mas acrescentará um serviço SMTP no porto 25 em conectividade por procuração inversa. O servidor SMTP verá o endereço da interface ALB-X como o IP de origem.	Configurações globais: Tempo de serviço de 2 horas Monitores: Monitor de camada 7 para a aplicação da web Outlook. Monitor de camada 4 fora da banda para o serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de serviço virtuais: 80, 443, 135, 59534, 59535, 25 (procuração inversa)

			Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento do HTTP para HTTPS
	jetPACK-1.1.1.3-Exchange-2010-SMTP-DSR	O mesmo que acima, exceto esse jetPACK irá configurar o serviço SMTP para usar a conectividade Direct Server Return. Esse jetPACK é necessário se seu servidor SMTP precisar ver o endereço IP real do cliente.	Configurações globais: Tempo de serviço de 2 horas Monitores: Monitor de camada 7 para a aplicação da web Outlook. Monitor de camada 4 fora da banda para o serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de serviço virtuais: 80, 443, 135, 59534, 59535, 25 (devolução direta ao servidor) Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTPs para HTTPs
Intercâmbio 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Essa configuração acrescenta 1 VIP e dois serviços para o tráfego HTTP e HTTPS e requer o mínimo de CPU. É possível acrescentar vários exames médicos ao VIP para verificar se cada um dos serviços individuais está funcionando.	Configurações globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS, ECP, OAB, e ADS Serviço Virtual IP: 2.2.2.2.1 Portos de serviço virtuais: 80, 443 Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento do HTTP para HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Essa instalação usa um endereço IP único para cada serviço e, portanto, usa mais recursos do que os acima mencionados. O senhor deve configurar cada serviço como uma entrada DNS individual Exemplo owa.jetnexus.com, ews.jetnexus.com, etc. Um monitor para cada serviço será adicionado e aplicado ao serviço relevante.	Configurações globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell Serviço Virtual IP: 2.2.3.1, 2.2.3.2, 2.2.3.3, 2.2.3.4, 2.2.3.5, 2.2.3.6, 2.2.3.7, 2.2.3.8, 2.2.3.9, 2.2.3.10 Portos de serviço virtuais: 80, 443 Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTPs para HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Esse jetPACK adicionará um endereço IP único e vários serviços virtuais em diferentes portos. flightPATH então mudará o contexto	Configurações globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS,

	com base no caminho de destino para o Serviço Virtual correto. Esse jetPACK requer a maior quantidade de CPU para realizar a mudança de contexto.	ECP, OAB, ADS, MAPI e PowerShell Serviço Virtual IP: 2.2.2.3 Portos de serviço virtuais: 80, 443, 1, 2, 3, 4, 5, 6, 7 Servidores de verdade: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento do HTTP para HTTPS

Microsoft Lync 2010/2013

Procuração reversa	Front End	Borda Interna	Borda Externa
jetPACK-3.3.3.3.1-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	SSL Descarga	Re-encriptação SSL	SSL Passthrough
jetPACK-4.4.4.1-Web-HTTP	jetPACK-4.4.4.4.2-Web-SSL Offload	jetPACK-4.4.4.3-Web-SSL-Re-Encryption	jetPACK-4.4.4.4-Web-SSL Passthrough

Área de trabalho remota da Microsoft

Normal
jetPACK-5.5.5.1-Remote-Desktop

DICOM - Imagem e Comunicação Digital em Medicina

HTTP normal
jetPACK-6.6.6.6.1-DICOM

Oracle e-Business Suite

SSL Descarga
jetPACK-7.7.7..1-Oracle-EBS

Vista Horizonte VMware

Servidores de conexão - SSL Offload	Servidores de Segurança - Re-encriptação SSL
jetPACK-8.8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.2-View-SSL-Re-encryption

Configurações globais

- GUI Secure Port 443 - este JetPACK mudará seu porto GUI Secure de 27376 para 443. HTTPs://x.x.x.x.x
- GUI Timeout 1 dia - o GUI solicitará que o senhor introduza sua senha a cada 20 minutos. Essa configuração aumentará esse pedido para 1 dia.
- ARP Refresh 10 - durante um failover entre aparelhos HA, este ajuste aumentará o número de **ARP's Gratuitos** para auxiliar os interruptores durante a transição

- Tamanho da captura 16MB - o tamanho padrão da captura é 2MB. Esse valor aumentará o tamanho até um máximo de 16MB.

Opções cifradas

- Cifras Fortes - Isso acrescentará a capacidade de escolher "Cifras Fortes" da lista de opções de Cifras:
    - Cipher = ALL:RC4+RSA:+RC4:+HIGH:!DES-CBC3-SHA:!SSLv2:!ADH:!EXP:!ADHexport:!MD5
- Anti-Beast - Isso acrescentará a capacidade de escolher "Anti-Beast" da lista de opções de cifras:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:RC4:HIGH:!MD5:!aNULL:!EDH
- No SSLv3 - Isso acrescentará a possibilidade de escolher "No SSLv3" da lista de opções cifradas:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- No SSLv3 no TLSv1 no RC4 - Isso acrescentará a capacidade de escolher "No-TLSv1 No-SSLv3 No-RC4" da lista de Opções Cifradas:
    - Cipher = ECDHE-RSA-AES128-SHA256:AES128-GCM-SHA256:HIGH:!MD5:!aNULL:!EDH:!RC4
- NO_TLSv1.1 - Isso acrescentará a capacidade de escolher "NO_TLSv1.1" da lista de opções da cifra:
    - Cipher= ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:RSA+AES:HIGH:!3DES:!aNULL:!MD5:!DSS:!MD5:!aNULL:!EDH:!RC4

vôosPATHs

- X-Content-Type-Options - acrescente esse cabeçalho se ele não existir e configure-o para "nosniff" - impede que o navegador automaticamente "MIME-Sniffing".
- X-Frame-Options - acrescente esse cabeçalho se ele não existir e coloque-o em "SAMEORIGIN" - páginas em seu website podem ser incluídas em quadros, mas somente em outras páginas dentro do mesmo website.
- X-XSS-Protection - adicionar este cabeçalho se ele não existir e defini-lo como "1; mode=block" - habilitar as proteções de script de cross-site do navegador
- Strict-Transport-Security - adiciona cabeçalho se não existir e define para "max-age=31536000 ; includeSubdomains" - garante ao cliente que todos os links devem ser HTTPs:// para a max-age

Aplicação de um jetPACK

O senhor pode aplicar qualquer JetPACK em qualquer ordem, mas tome cuidado para não usar um jetPACK com o mesmo endereço IP virtual. Essa ação causará uma duplicação do endereço IP na configuração. Se o senhor fizer isso por engano, poderá mudar isso na GUI.

- Navegue para Advanced > Update Software
- Seção de Configuração
- Upload Nova Configuração ou JetPACK
- Procurar por jetPACK
- Clique em Upload
- Quando a tela do navegador ficar branca, favor clicar em atualizar e esperar que a página do Painel de Controle apareça.

Criação de um jetPACK

Uma das grandes coisas do JetPACK é que o senhor pode criar o seu próprio. Pode ser que o senhor tenha criado a configuração perfeita para uma aplicação e queira usá-la em várias outras caixas de forma independente.

- Comece por copiar a configuração atual de seu ALB-X existente
  - Avançado
  - Software de atualização
  - Download da Configuração Atual
- Editar este arquivo com Notepad++
- Abrir um novo documento txt e chamá-lo "yourname-jetPACK1.txt".
- Copiar todas as seções relevantes do arquivo de configuração para "yourname-jetPACK1.txt".
- Economize uma vez concluído

IMPORTANTE: Cada jetPACK está dividido em seções diferentes, mas todos os jetPACKs devem ter #!jetpack no topo da página.

As seções que são recomendadas para edição/cópia estão listadas abaixo.

Seção 0:

```
#!jetpack
```

Essa linha precisa estar no topo do jetPACK, ou sua configuração atual será sobregravada.

Seção1:

```
[jetnexusdaemon]
```

Esta seção contém ajustes globais que, uma vez modificados, se aplicarão a todos os serviços. Algumas dessas configurações podem ser alteradas a partir do console da web, mas outras só estão disponíveis aqui.

Exemplos:

```
ConnectionTimeout=600000
```

Esse exemplo é o valor de timeout do TCP em milissegundos. Essa configuração significa que uma conexão TCP será fechada após 10 minutos de inatividade.

```
ConteúdoServidorCustomTimer=20000
```

Este exemplo é o atraso em milissegundos entre os controles de saúde dos servidores de conteúdo para monitores personalizados, como o DICOM

```
jnCookieHeader="MS-WSMAN
```

Esse exemplo vai mudar o nome do cabeçalho do cookie usado no balanceamento de carga persistente de "jnAccel" padrão para "MS-WSMAN". Essa mudança em particular é necessária para a proxy reversa Lync 2010/2013.

Seção 2:

```
[jetnexusdaemon-Csm-Rules]
```

Esta seção contém as regras personalizadas de monitoramento do servidor que são tipicamente configuradas a partir do console da web aqui.

Exemplo:

```
[jetnexusdaemon-Csm-Rules-0]
Conteúdo="Server Up" (Servidor Up)
```

Desc="Monitor 1″

Método="CheckResponse"

Name="Health Check- Is Server Up

Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html

Seção 3:

[jetnexusdaemon-LocalInterface]

Esta seção contém todos os detalhes da seção de Serviços de PI. Cada interface é numerada e inclui subinterfaces para cada canal. Se seu canal tem uma regra de flightPATH aplicada, então conterá também uma seção Path.

Exemplo:

[jetnexusdaemon-LocalInterface1] [jetnexusdaemon-LocalInterface1

1.1=”443″

1.2=”104″

1.3=”80″

1.4=”81″

Habilitado=1

Netmask="255.255.255.0″

PrimaryV2="{A28B2C99-1FFC-4A7C-AAD9-A55C32A9E913}"

[jetnexusdaemon-LocalInterface1.1]

1=">,""Secure Group"",2000,"

2="192.168.101.11:80,Y,""IIS WWW Server 1″"""

3="192.168.101.12:80,Y,""IIS WWW Server 2″"""

EndereçoResolução=0

CachePort=0

CertificateName="default" (nome do certificado)

ClientCertificateName="No SSL" (sem SSL)

Compress=1

ConexãoLimitação=0

DSR=0

DSRProto="tcp"

Habilitado=1

LoadBalancePolicy="CookieBased" (Baseado em Cookies)

MaxConnections=10000

MonitoringPolicy="1″

PassThrough=0

Protocol="Accelerate HTTP" (Acelerar HTTP)

ServiceDesc="Secure Servers VIP" (Servidores Seguros VIP)

SNAT=0

SSL=1

SSLClient=0

SSLInternalPort=27400

[jetnexusdaemon-LocalInterface1.1-Path]

1=”6″

Seção 4:

[jetnexusdaemon-Path]

Esta seção contém todas as regras do 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 esta como um exemplo abaixo.

Exemplo:

[jetnexusdaemon-Path-6]

Desc="Force to use HTTPS for certain directory" (Forçar o uso de HTTPS para certos diretórios)

Nome="Gary - Force HTTPS"

[jetnexusdaemon-Path-6-Condition-1]

Check="contain" (conter)

Condição="caminho".

Partida=

Sentido= "faz"

Valor="/secure/"

[jetnexusdaemon-Path-6-Evaluate-1]

Detalhe=

Fonte="anfitrião".

Valor=

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

Ação = "redirecionar".

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

Valor=

Introdução ao FlightPATH

O que é vôoPATH?

flightPATH é um motor de regras inteligente desenvolvido pela Edgenexus para manipular e rotear o tráfego HTTP e HTTPS. É altamente configurável, muito potente e, ao mesmo tempo, muito fácil de usar.

Embora alguns componentes do flightPATH sejam objetos de PI, tais como o IP de origem, o flightPATH só pode ser aplicado a um **tipo de serviço** igual a HTTP. Se o senhor escolher qualquer outro tipo de serviço, então a guia flightPATH em Serviços de PI ficará em branco.

Uma regra de FlightPATH tem três componentes:

Opção	Descrição
Condição	Estabelecer múltiplos critérios para acionar a regra flightPATH.
Avaliação	Permite o uso de variáveis que podem ser usadas na área de Ação.
Ação	O comportamento uma vez que a regra foi desencadeada.

O que pode fazer o FlightPATH?

flightPATH pode ser usado para modificar conteúdo e solicitações HTTP(s) de entrada e saída.

Além de usar combinações simples de cordas como "Começa com" e "Termina com", por exemplo, é possível implementar um controle completo usando expressões regulares (RegEx) compatíveis com o Perl.

Para mais informações sobre o RegEx, por favor, veja este site útil
https://www.regexbuddy.com/regex.html

Além disso, variáveis personalizadas podem ser criadas e usadas na área de **Ação**, permitindo muitas possibilidades diferentes.

Condição

Condição	Descrição	Exemplo
<form>	Os formulários HTML são usados para passar dados a um servidor	Exemplo "o formulário não tem comprimento 0".
Localização da GEO	Isto compara o endereço IP de origem com o código de país ISO 3166	GEO Localização é igual a GB OU GEO Localização é igual a Alemanha
Anfitrião	Este é o anfitrião extraído do URL	www.mywebsite.com ou 192.168.1.1
Idioma	Este é o idioma extraído do cabeçalho HTTP do idioma	Esta condição produzirá uma queda com uma lista de idiomas
Método	Esta é uma queda dos métodos HTTP	Esta é uma queda que inclui GET, POST etc.
Origem PI	Se o representante a montante apoiar X-Forwarded-for (XFF), ele usará o verdadeiro endereço de origem	Propriedade intelectual do cliente. Pode também usar múltiplos IP's ou sub-redes. 10.1.2.* é 10.1.2.0 /24 subnet10 10. 1.2.3|10.1.2.4 Utilização | para múltiplos IP's
Caminho	Este é o caminho do site	/mywebsite/index.asp

POST	Método de solicitação de pós-venda	Verificar os dados que estão sendo carregados em um website
Consulta	Este é o nome e o valor de uma consulta como tal, ela pode aceitar o nome da consulta ou um valor também	"Best=jetNEXUS" Onde a partida é melhor e o valor é edgeNEXUS
Query String	Toda a seqüência de perguntas após o ? caráter	
Solicitação Cookie	Este é o nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Pedido Cabeçalho	Este pode ser qualquer cabeçalho HTTP	Referidor, Usuário-Agente, De, Data
Versão do pedido	Esta é a versão HTTP	HTTP/1.0 OU HTTP/1.1
Órgão de resposta	Uma cadeia definida pelo usuário no corpo de resposta	Servidor UP
Código de resposta	O código HTTP para a resposta	200 OK, 304 Não modificado
Cookie de resposta	Este é o nome de um cookie enviado pelo servidor	MS-WSMAN=afYfn1CDqqCDqUD::
Resposta Cabeçalho	Este pode ser qualquer cabeçalho HTTP	Referidor, Usuário-Agente, 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, IP do servidor proxy ou algum outro endereço IP agregado	ClientIP , Proxy IP, Firewall IP. Pode também usar múltiplos IP's e sub-redes. O senhor deve escapar dos pontos, pois estes são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Jogo	**Descrição**	**Exemplo**
Aceitar	Tipos de conteúdo que são aceitáveis	Aceitar: texto/plainar
Aceitação-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>
Aceitação-Língua	Idiomas aceitáveis para a resposta	Aceitação-Língua: en-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Gama de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ====
Carga-To	Contém informações sobre os custos da aplicação do método solicitado	
Codificação do conteúdo	O tipo de codificação usada nos dados.	Codificação do conteúdo: gzip

Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (8-bit bytes)	Comprimento do conteúdo: 348
Content-Type	O tipo mímico do corpo do pedido (usado com pedidos POST e PUT)	Tipo de conteúdo: aplicação/x-www-form-urlencoded
Cookie	Um cookie HTTP previamente enviado pelo servidor com o Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Data = "Data" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, muitas vezes uma digestão de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de e-mail do usuário que faz o pedido	De: user@example.com
Se-Modificado - desde	Permite que um 304 Não modificado seja devolvido se o conteúdo não for modificado.	Se-Modified-Since: Sábado, 29 de outubro de 1994 19:43:31 GMT
Última Modificação	A última data modificada para o objeto solicitado, no formato RFC 2822	Modificado por último: Ter, 15 de novembro de 1994 12:45:26 GMT
Pragma	Os cabeçalhos específicos de implementação podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta aos pedidos.	Pragma: sem cache
Referência	Este é o endereço da página web anterior, a partir do qual foi seguido um link para a página atualmente solicitada.	Referência: 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; Versão=1
Agente-usuário	A seqüência do agente do usuário do agente do usuário	Agente-usuário: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Diz aos procuradores abaixo como combinar futuros cabeçalhos de pedidos para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova resposta do servidor de origem.	Vary: Agente-usuário
X-Powered-By	Especifica a tecnologia (por exemplo, ASP.NET, PHP, JBoss) que suporta a aplicação web	X-Powered-By: PHP/5.4.0

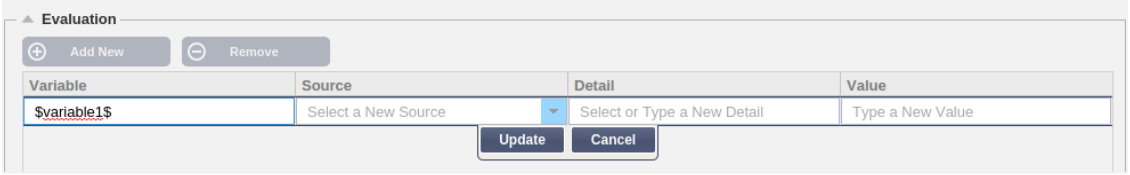
Verifique	**Descrição**	**Exemplo**
Existente	Isto não se preocupa com os detalhes da condição apenas que ela existe/não existe.	Anfitrião - Existente
Início	O cordel começa com o Valor	Caminho - Começa - /secura

Fim	O fio termina com o Valor	Caminho - Faz - Termina - .jpg
Conter	O fio contém o Valor	Solicitar Cabeçalho - Aceitar - Conter - Imagem
Igual	O fio faz igualar o valor	Anfitrião - Does - Equal - www.jetnexus.com
Ter comprimento	O fio tem o comprimento do valor	Host - Does - Have Length - 16www.jetnexus.com = TRUEwww.jetnexus.co.uk = FALSE
Partida RegEx	Isso permite que o senhor entre com uma expressão regular compatível com o Perl	Origem IP - Does - Match Regex - 10\...* | 11\...*

Exemplo

- O exemplo tem duas condições, e **AMBOS** deve ser cumprido para realizar a ação
- A primeira é verificar se o objeto solicitado é uma imagem
- A segunda é a verificação de um nome de anfitrião específico

Avaliação



Acrescentar uma variável é uma característica convincente que permitirá ao senhor extrair dados do pedido e utilizá-los nas Ações. Por exemplo, o senhor poderia registrar um nome de usuário ou enviar um e-mail se houver um problema de segurança.

- Variável: Isto deve começar e terminar com um símbolo de US$. Por exemplo, $variavel1$.
- Fonte: Selecione da caixa drop-down a fonte da variável
- Detalhe: Selecione da lista quando relevante. Se a Fonte=Cabeçalho do pedido, os Detalhes poderiam ser User-Agent
- Valor: Digite o texto ou expressão regular para afinar a variável.

Variáveis embutidas:

- As variáveis embutidas já foram codificadas com dificuldade, de modo que o senhor não precisa criar uma entrada de avaliação para elas.
- O senhor pode usar qualquer uma das variáveis listadas abaixo em sua ação
- A explicação para cada variável está localizada na tabela "Condição" acima
    - Método = $method$
    - Caminho = $caminho$$
    - Querystring = $querystring $querystring
    - Sourceip = $sourceip$
    - Código de resposta (o texto também incluía "200 OK") = $respasse$
    - Anfitrião = $host$

- Versão = $version$
- Clientport = $clientport$
- Clientip = $clientip$
- Geolocalização = $geolocalização$".

Exemplo de ação:

- Ação = Redirecionar 302
  - Alvo = HTTPs://$host$/404.html
- Ação = Log
  - Alvo = Um cliente de $sourceip$:$sourceport$ acabou de fazer um pedido $path$ página

Explicação:

- Um cliente que acesse uma página que não existe, normalmente seria apresentado com um navegador 404 página
- Neste caso, o usuário é redirecionado para o nome original do host que usou, mas o caminho errado é substituído pelo 404.html
- Uma entrada é acrescentada ao syslog dizendo "Um cliente de 154.3.22.14:3454 acaba de fazer um pedido à página wrong.html".

Fonte:	Descrição	Exemplo
Cookie	Este é o nome e o valor do cabeçalho do cookie	MS-WSMAN=afYfn1CDqqCDqUD::: Onde o nome é MS-WSMAN e o valor é afYfn1CDqqCDqUD::
Anfitrião	Este é o nome da hostname extraído do URL	www.mywebsite.com ou 192.168.1.1
Idioma	Este é o idioma extraído do cabeçalho do Idioma HTTP	Essa condição produzirá uma queda com uma lista de idiomas.
Método	Esta é uma queda dos métodos HTTP	A queda incluirá GET, POST
Caminho	Este é o caminho do site	/mywebsite/index.html
POST	Método de solicitação de pós-venda	Verificar os dados que estão sendo carregados em um website
Item de Consulta	Este é o nome e o valor de uma pergunta. Como tal, pode aceitar ou o nome da consulta ou um valor também	"Best=jetNEXUS" Onde a partida é melhor e o valor é edgeNEXUS
Query String	Este é todo o fio após o ? personagem	HTTP://servidor/percurso/programa?query_string
Pedido Cabeçalho	Este pode ser qualquer cabeçalho enviado pelo cliente	Referente, Agente-usuário, De, Data...
Resposta Cabeçalho	Este pode ser qualquer cabeçalho enviado pelo servidor	Referente, Agente-usuário, De, Data...
Versão	Esta é a versão HTTP	HTTP/1.0 ou HTTP/1.1

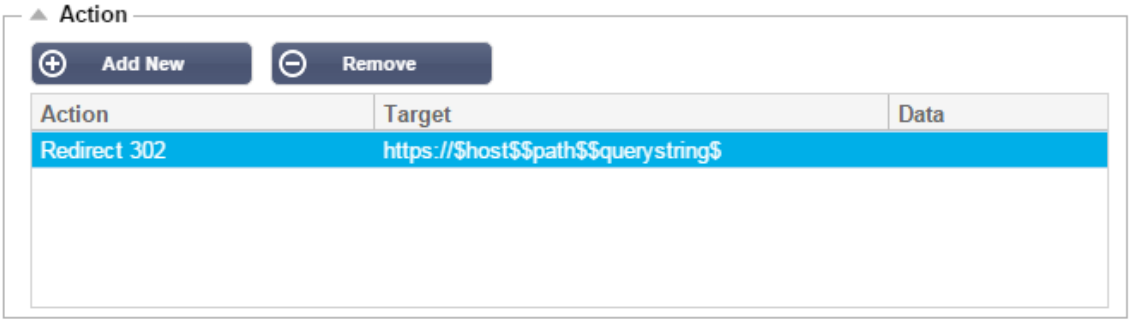
Detalhe	Descrição	Exemplo
Aceitar	Tipos de conteúdo que são aceitáveis	Aceitar: texto/plainar
Aceitação-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>

Aceitação-Língua	Idiomas aceitáveis para a resposta	Aceitação-Língua: en-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Gama de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ====
Carga-To	Contém informações sobre os custos da aplicação do método solicitado	
Codificação do conteúdo	O tipo de codificação usada nos dados.	Codificação do conteúdo: gzip
Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (8-bit bytes)	Comprimento do conteúdo: 348
Content-Type	O tipo mímico do corpo do pedido (usado com pedidos POST e PUT)	Tipo de conteúdo: aplicação/x-www-form-urlencoded
Cookie	um cookie HTTP previamente enviado pelo servidor com o Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Data = "Data" ":" HTTP-date
ETag	Um identificador para uma versão específica de um recurso, muitas vezes uma digestão de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de e-mail do usuário que faz o pedido	De: user@example.com
Se-Modificado - desde	Permite que um 304 Não modificado seja devolvido se o conteúdo não for alterado	Se-Modified-Since: Sábado, 29 de outubro de 1994 19:43:31 GMT
Última Modificação	A última data modificada para o objeto solicitado, no formato RFC 2822	Modificado por último: Ter, 15 de novembro de 1994 12:45:26 GMT
Pragma	Cabeçalhos específicos de implementação que podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta aos pedidos.	Pragma: sem cache
Referência	Este é o endereço da página web anterior, a partir do qual foi seguido um link para a página atualmente solicitada	Referência: 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; Versão=1
Agente-usuário	A seqüência do agente do usuário do agente do usuário	Agente-usuário: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Diz aos procuradores como combinar os cabeçalhos de pedidos futuros para decidir se a resposta em cache pode ser usada em	Vary: Agente-usuário

	vez de solicitar uma nova resposta do servidor de origem.	
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 habilitadas uma vez que a condição ou condições tenham sido cumpridas.



Ação

Clique duas vezes na coluna Ação para ver a lista suspensa.

Alvo

Clique duas vezes na coluna Alvo para ver a lista suspensa. A lista mudará de acordo com a Ação.

O senhor também pode digitar manualmente com algumas ações.

Dados

Clique duas vezes na coluna Dados para acrescentar manualmente seus dados que o senhor deseja acrescentar ou substituir.

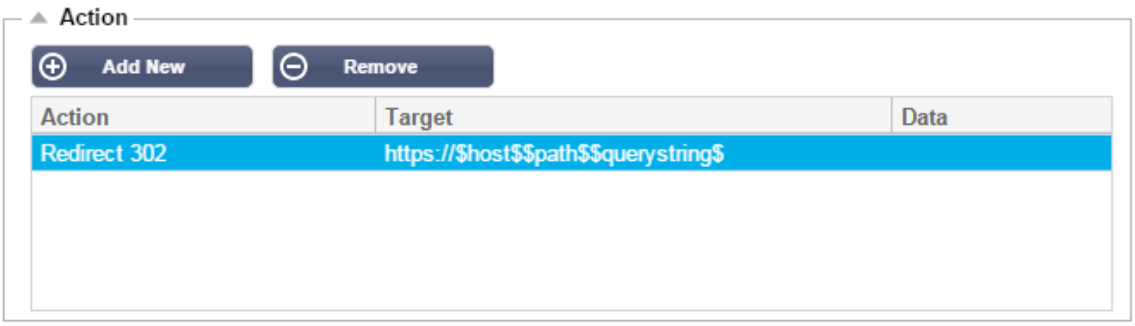
A lista de todas as ações está detalhada a seguir:

Ação	Descrição	Exemplo
Adicionar Pedido Cookie	Adicionar cookie de pedido detalhado na seção Objetivo com valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Acrescentar cabeçalho do pedido	Adicionar um cabeçalho de pedido do tipo Alvo com valor na seção Dados	Meta= Aceitar Data= imagem/png
Acrescentar Cookie de Resposta	Adicionar Cookie de Resposta detalhado na seção Objetivo com valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Acrescentar cabeçalho de resposta	Adicionar cabeçalho de pedido detalhado na seção Objetivo com valor na seção Dados	Alvo= Cache-Control Data= max-age=8888888
Corpo Substituir Todos	Revistar o Órgão de Resposta e substituir todas as instâncias	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)

Substituir primeiro o corpo	Revistar o Órgão de Resposta e substituir apenas a primeira instância	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)
Substituição do corpo Último	Revistar o Órgão de Resposta e substituir apenas a última instância	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)
Queda	Isso fará cair a conexão	Alvo= N/A Data= N/A
e-Mail	Enviará um e-mail para o endereço configurado em Eventos por e-mail. O senhor poderá usar uma variável como endereço ou como mensagem	Target= "FlightPATH enviou este evento por e-mail". Data= N/A
Log Event	Isto registrará um evento no diário de bordo do Sistema	Target= "flightPATH has logged this in syslog" Data= N/A
Redirecionar 301	Isto vai emitir um redirecionamento permanente	Target= HTTP://www.edgenexus.ioData= N/A
Redirecionamento 302	Isto vai emitir um redirecionamento temporário	Target= HTTP://www.edgenexus.ioData= N/A
Retirar Pedido Cookie	Remover cookie de pedido detalhado na seção Objetivo	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Retirar o cabeçalho do pedido	Remover o cabeçalho do pedido detalhado na seção Objetivo	Target=ServerData=N/A
Retire o Cookie de Resposta	Remover cookie de resposta detalhado na seção Objetivo	Alvo=jnAccel
Remover o cabeçalho de resposta	Remover o cabeçalho de resposta detalhado na seção Objetivo	Meta= Etag Data= N/A
Substituir Pedido Cookie	Substituir o cookie de pedido detalhado na seção Objetivo pelo valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho do pedido	Substituir o cabeçalho da solicitação no campo de destino pelo valor dos dados	Alvo= Conexão Data= keep-alive
Substituir o Cookie de Resposta	Substituir o cookie de resposta detalhado na seção Objetivo pelo valor na seção Dados	Target=jnAccel=afYfn1CDqqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho de resposta	Substituir o cabeçalho de resposta detalhado na seção Objetivo pelo valor na seção Dados	Alvo= Servidor Dados= retidos para segurança
Re-escrever o caminho	Isso permitirá que o senhor redirecione o pedido para o novo URL com base na condição	Target= /test/path/index.html$querystring$ Data= N/A
Usar Servidor Seguro	Selecione qual servidor seguro ou serviço virtual a usar	Target=192.168.101: 443Data=N/A

Use Server	Selecionar qual servidor ou serviço virtual a utilizar	Target= 192.168.101:80Data= N/A
Criptografar o Cookie	Isto irá codificar os cookies 3DES Encrypt e depois base64 codificá-los	Target= Digite o nome do cookie a ser criptografado, você pode usar o * como um wild card no finalData= Digite uma frase de passagem para a criptografia

Exemplo:



A ação abaixo emitirá um redirecionamento temporário para o navegador para um Serviço Virtual HTTPS seguro. Ele usará o mesmo hostname, o mesmo caminho, e o mesmo querystring que o pedido.

Usos comuns

Aplicação Firewall e Segurança

- Bloqueio de IPs indesejados
- Forçar o usuário a HTTPS para conteúdo específico (ou todo)
- Bloquear ou redirecionar aranhas
- Prevenir e alertar sobre os roteiros cruzados do local
- Prevenir e alertar sobre a injeção de SQL
- Ocultar a estrutura interna do diretório
- Reescrever os cookies
- Diretório seguro para usuários particulares

Características

- Redirecionar os usuários com base no caminho
- Fornecer sinal único em múltiplos sistemas
- Usuários do segmento com base no ID de usuário ou Cookie
- Acrescentar cabeçalhos para descarga de SSL
- Detecção de idiomas
- Reescrever o pedido do usuário
- Consertar URLs quebrados
- Log e e-mail de alerta 404 códigos de resposta
- Impedir o acesso ao diretório/navegação
- Enviar aranhas de conteúdo diferente

Regras pré-construídas

Extensão HTML

Muda todos os pedidos .htm para .html

Condição:

- Condição = Caminho
- Sentido = Faz
- Cheque = Partida RegEx
- Valor = \.htm$

Avaliação:

- Em branco

Ação:

- Ação = Re-escrever o caminho
- Meta = $caminho$l

Index.html

Forçar o uso de index.html em pedidos a pastas.

Condição: esta condição é uma condição geral que se ajusta à maioria dos objetos

- Condição = Anfitrião
- Sentido = Faz
- Verificação = Existente

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Meta = HTTP://$host$$$path$index.html$querystring$

Fechar Pastas

Negar pedidos a pastas.

Condição: esta condição é uma condição geral que se ajusta à maioria dos objetos

- Condição = isso precisa de uma reflexão adequada
- Sentido =
- Cheque =

Avaliação:

- Em branco

Ação:

- Ação =
- Alvo =

Ocultar CGI-BBIN:

Esconde o catálogo de cgi-bin em pedidos aos scripts do CGI.

Condição: esta condição é uma condição geral que se ajusta à maioria dos objetos

- Condição = Anfitrião
- Sentido = Faz
- Cheque = Partida RegEX
- Valor = \.cgi$

Avaliação:

- Em branco

Ação:

- Ação = Re-escrever o caminho
- Meta = /cgi-bin$caminho$

Aranha de madeira

Pedidos de aranhas de madeira de motores de busca populares.

Condição: esta condição é uma condição geral que se ajusta à maioria dos objetos

- Condição = Cabeçalho do pedido
- Partida = Usuário-Agente
- Sentido = Faz
- Cheque = Partida RegEX
- Valor = Googlebot|Slurp|bingbot|ia_archiver

Avaliação:

- Variável = $crawler$
- Fonte = Cabeçalho do pedido
- Detalhe = Usuário-Agente

Ação:

- Ação = Log Event
- Meta = [$crawler$] $host$$$path$$$querystring$

Forçar HTTPS

Forçar o uso de HTTPS para certos diretórios. Nesse caso, se um cliente estiver acessando qualquer coisa que contenha o diretório /secure/, ele será redirecionado para a versão HTTPs da URL solicitada.

Condição:

- Condição = Caminho
- Sentido = Faz
- Cheque = Conter
- Valor = /secure/

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Alvo = HTTPs://$host$$$caminho$$$querystring$

Media Stream:

Redireciona o Flash Media Stream para o serviço apropriado.

Condição:

- Condição = Caminho
- Sentido = Faz
- Cheque = Fim
- Valor = .flv

Avaliação:

- Em branco

Ação:

- Ação = Redirecionar 302
- Alvo = HTTP://$host$:8080/$path$

Trocar HTTP para HTTPS

Mude qualquer HTTP:// hardcoded para HTTPS://

Condição:

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Corpo Substituir Todos
- Alvo = HTTP://
- Dados = HTTPs://

Cartões de crédito em branco

Verifique se não há cartões de crédito na resposta e, se for encontrado um, deixe-o em branco.

Condição:

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Corpo Substituir Todos

- 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-xxxx

Expiração do conteúdo

Acrescente à página uma data sensata de expiração do conteúdo para reduzir o número de pedidos e 304s.

Condição: esta é uma condição genérica como captura de tudo. Recomenda-se focalizar esta condição em seu

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Adicionar cabeçalho de resposta
- Alvo = Cache-Control
- Dados = idade máxima=3600

Spoof Server Tipo

Arranje o tipo de servidor e mude-o para outra coisa.

Condição: esta é uma condição genérica como captura de tudo. Recomenda-se focalizar esta condição em seu

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Substituir o cabeçalho de resposta
- Alvo = Servidor
- Dados = Segredo

Nunca enviar erros

O cliente nunca recebe nenhum erro de seu site.

Condição

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Conter

- Valor = 404

Avaliação

- Em branco

Ação

- Ação = Redirecionar 302
- Alvo = HTTP//$host$/

Redirecionamento no Idioma

Encontre o código do idioma e redirecione para o domínio do país relacionado.

Condição

- Condição = Idioma
- Sentido = Faz
- Cheque = Conter
- Valor = Alemão (Padrão)

Avaliação

- Variável = $host_template$
- Fonte = Anfitrião
- Valor = .*\.

Ação

- Ação = Redirecionar 302
- Target = HTTP//$host_template$de$path$$$querystring$

Google Analytics

Insira o código requerido pelo Google para a análise - Favor mudar o valor MYGOOGLECODE para seu ID do Google UA.

Condição

- Condição = Código de resposta
- Sentido = Faz
- Cheque = Igual
- Valor = 200 OK

Avaliação

- em branco

Ação

- Ação = Corpo Substituir Último
- Alvo = </ corpo>
- Data = <scripttype= 'text/javascript'> var _gaq = _gaq || []; _gaq.push(['_setAccount', 'MY GOOGLE CODE']); _gaq.push(['_trackPageview']); (function() { var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true; ga.src = ('HTTPs' == document.location.protocol ?'HTTPs///ssl' 'HTTP//wwww') + '.google-analytics.com/ga.js'; var s =

```
document.getElementsByTagName('script')[0];s.parentNode.insertBefore(ga, s); } ()();
</script>>/body>
```

Portão IPv6

Ajustar o Host Header para Servidores IPv4 IIS em serviços IPv6. Os servidores IPv4 do IIS não gostam de ver um endereço IPV6 no pedido do cliente anfitrião, portanto essa regra substitui isso por um nome genérico.

Condição

- em branco

Avaliação

- em branco

Ação

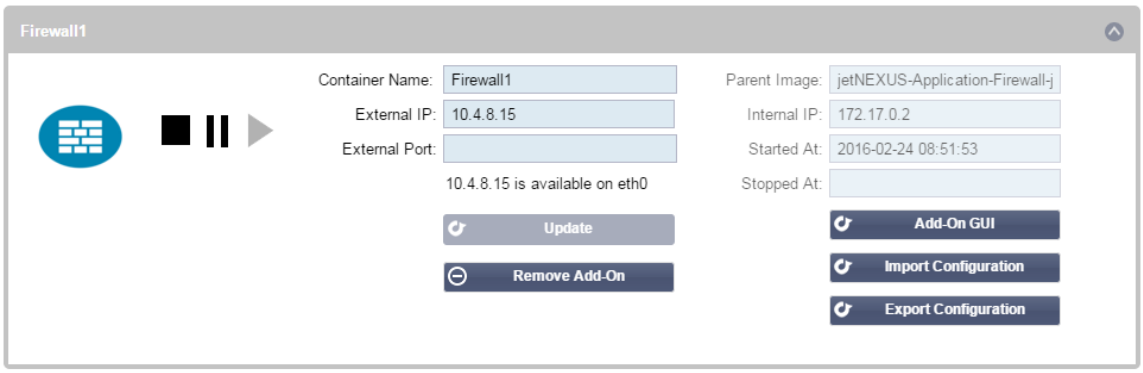
- Ação = Substituir o cabeçalho do pedido
- Alvo = Anfitrião
- Dados =ipv4.host.header

Web Application Firewall (edgeWAF)

O Web Application Firewall (WAF) está disponível mediante solicitação e é licenciado numa base anual cobrável. A instalação do WAF é feita usando a seção inbuilt Apps dentro do ADC.

Execução do WAF

Funcionando em um Docker Container, o WAF precisa que alguns parâmetros da rede sejam estabelecidos antes de iniciar.

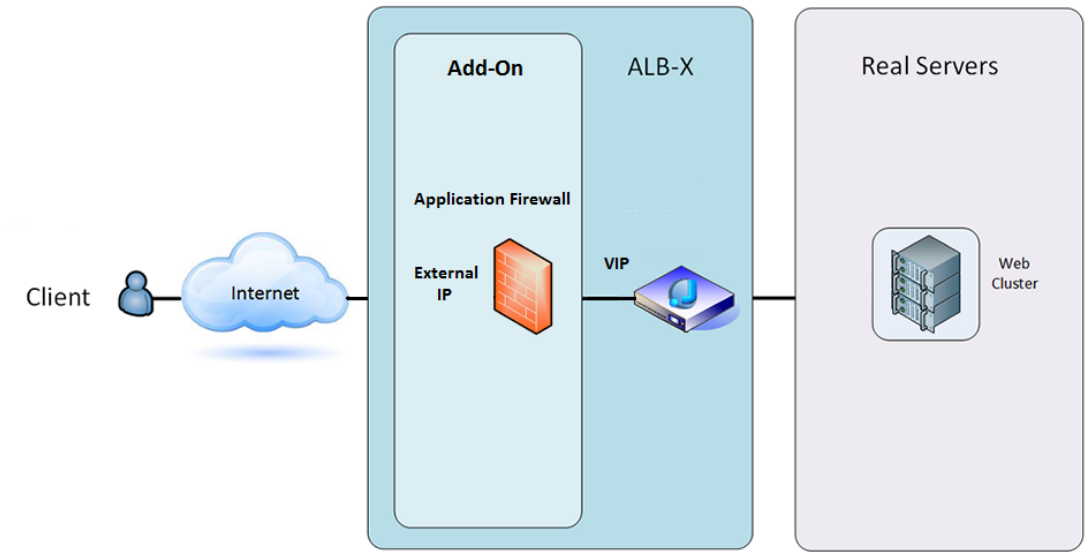


Opção	Descrição
Parada	Ficará cinzento até que se inicie um processo de Add-On. Aperte este botão para parar a instância do Docker.
Pausa	Este botão fará uma pausa no Add-On.
Jogue	Ele iniciará o Add-On com os ajustes atuais.
Nome do contêiner	Dê a seu recipiente um nome para identificá-lo a partir dos outros recipientes. Isso deve ser único. O senhor poderá usá-lo como nome de um servidor real, se desejar, e ele se resolverá automaticamente para o endereço IP interno da instância.
PI externa	Aqui o senhor pode estabelecer um IP externo para acessar seu Add-On. Isso pode ser para acessar o GUI do Add-On, bem como o serviço que funciona através do Add-On. No caso do Firewall Add-On, esse é o endereço IP de seu serviço HTTP. O Firewall pode então ser configurado para acessar um servidor ou um ALB-X VIP que contém múltiplos servidores para balanceamento de carga.
Porto externo	Se o senhor deixar isso em branco, então todos os portos serão encaminhados ao seu Firewall. Para restringir isso, basta acrescentar na lista de portos separados por vírgulas. Exemplo 80, 443, 88. Observe que o endereço do GUI do Firewall será **HTTP///[IP externo]88/waf.** Portanto, ou deixe a configuração do porto externo em branco ou acrescente na porta 88 para acessar a GUI se o senhor estiver restringindo a lista de portos.
Atualização	O senhor só pode atualizar as configurações de um Add-On depois que ele tiver sido interrompido. Uma vez parado, o senhor pode mudar o nome do contêiner, o IP externo e as configurações do porto externo.
Remover Add-On	Irá remover completamente o Add-On da página do Add-On. O senhor terá que ir à página da Biblioteca-Apps para distribuir novamente o Add-On.
Imagem dos pais	Indica a imagem do Docker a partir do qual o Add-On é construído. Pode haver várias versões de um Firewall ou mesmo outro tipo de Add-On completamente, de modo que isso ajudará a distinguir entre eles. Esta seção é apenas para fins informativos e, portanto, é cinzenta.

PI interna	O Docker cria automaticamente o endereço IP interno e, portanto, não pode ser editado. Se o senhor parar a instância do Docker e reiniciar, será emitido um novo endereço IP interno. É por essa razão que o senhor deve ou usar um endereço de IP externo para seu serviço, ou usar o Container Name para o endereço de servidor real de seu serviço.
Começou em	Isso indicará a data e a hora em que a Adenda foi iniciada. Exemplo 2016-02-16 155721
Parou em	Isso indicará a data e a hora em que o Add-On foi interrompido. Exemplo 2016-02-24 095839

Exemplo de arquitetura

WAF usando endereço IP externo

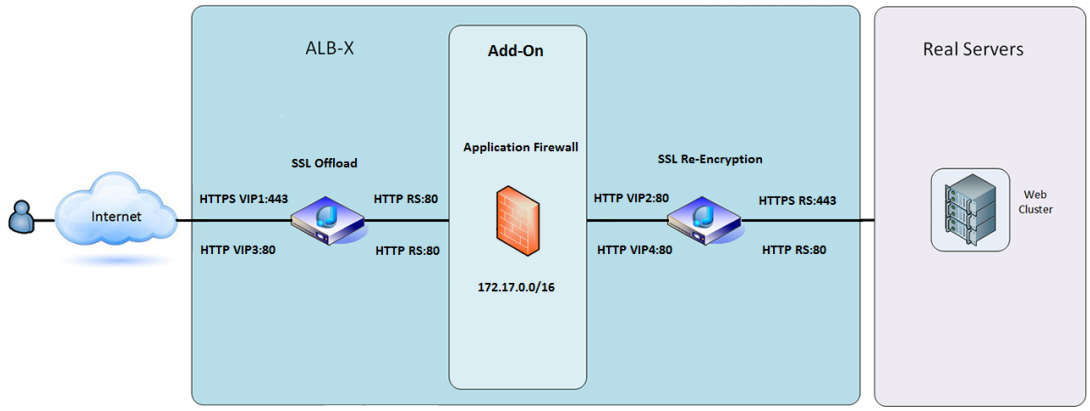


Nessa arquitetura, somente HTTP pode ser usado para seu serviço, pois o Firewall não pode inspecionar o tráfego de HTTPS.

O Firewall terá que ser configurado para enviar tráfego para o ALB-X VIP.

O ALB-X VIP, por sua vez, será configurado para carregar o tráfego de equilíbrio para o seu cluster da web.

WAF usando endereço IP interno



Nessa arquitetura, o senhor pode especificar HTTP e HTTPS.

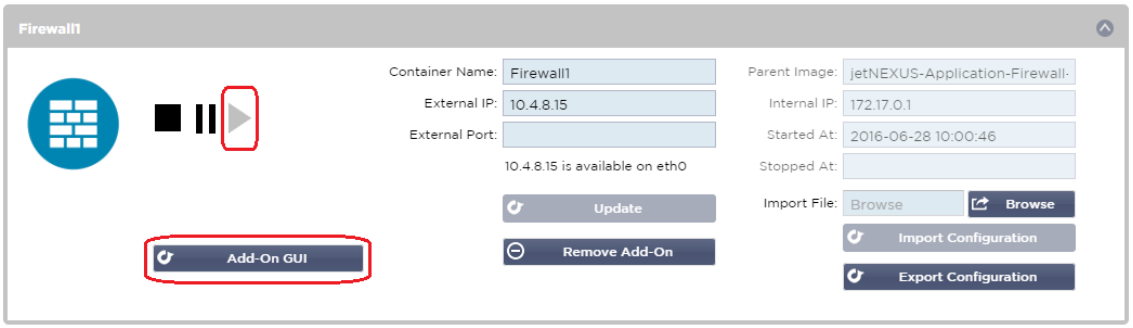
HTTPS pode ser de ponta a ponta onde as conexões do Cliente para ALB-X são criptografadas e do ALB-X para os Servidores Reais.

O tráfego do ALB-X para o endereço IP interno do firewall precisa ser descriptografado para que possa ser inspecionado.

Uma vez que o tráfego tenha passado pelo Firewall, ele é então encaminhado para outro VIP que pode então reencriptar o equilíbrio de tráfego e carga para proteger servidores ou simplesmente carregar o equilíbrio para servidores inseguros sobre HTTP.

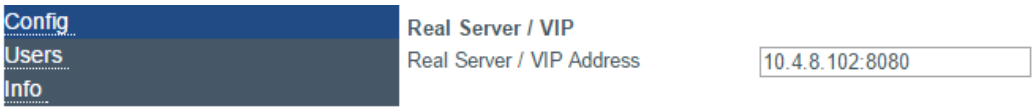
Acesso ao seu WAF add-on

- Preencha os detalhes de seu Firewall
- O senhor pode restringir seus portos ao que precisa ou deixá-los em branco para permitir todos os portos
- Clique no botão Play
- Aparecerá um botão adicional GUI

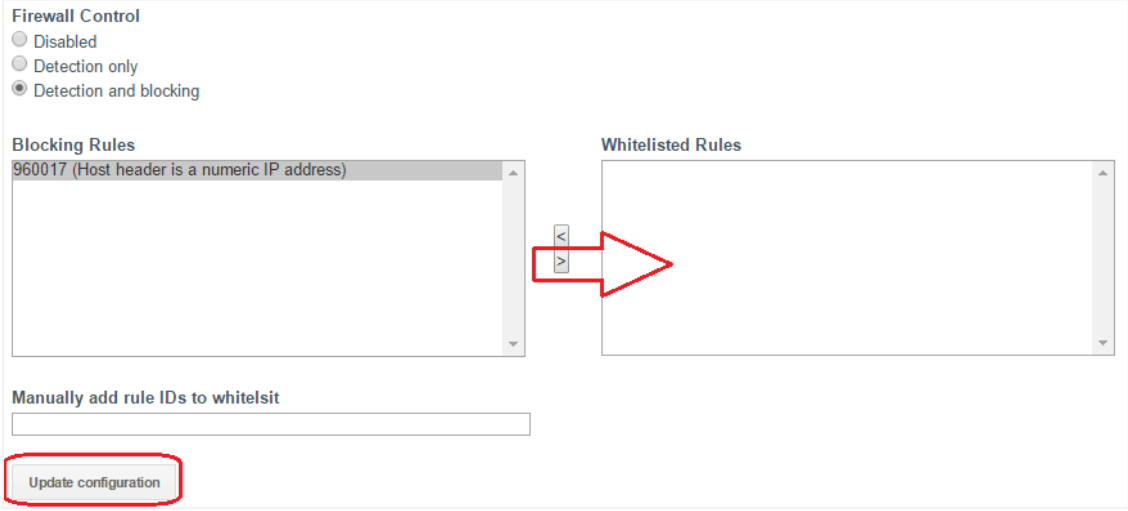


- Clique neste botão, e ele abrirá um navegador em HTTP://[External IP]:88/waf
- Neste exemplo, será HTTP://10.4.8.8.15:88/waf
- O senhor será presenteado com um diálogo de login.
- Digite as credenciais para o seu ADC.
- Ao completar um login bem sucedido, o senhor será presenteado com a página inicial do WAF.

- A página inicial apresenta um panorama gráfico dos eventos, isto é, das ações de filtragem realizadas pelo Application Firewall.
- Os gráficos provavelmente estarão em branco quando o senhor abrir a página pela primeira vez, pois não haverá tentativas de acesso através do firewall.
- O usuário pode configurar o endereço IP ou o nome de domínio do website para o qual gostaria de enviar o tráfego depois que o firewall o tiver filtrado.
- Isso pode ser alterado na seção Administração > Config



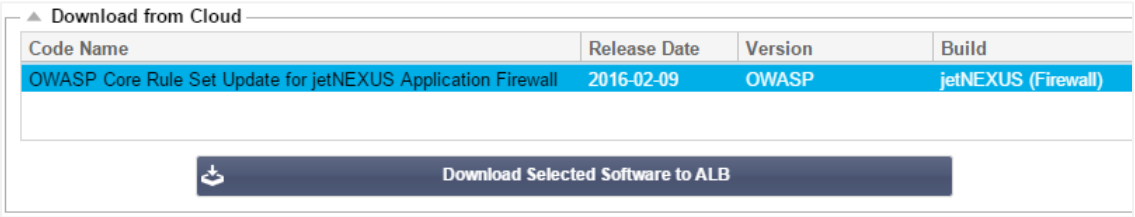
- O Firewall inspecionará o tráfego e depois o enviará para o Real Sever IP ou para o endereço VIP aqui. O senhor também pode entrar num porto junto com seu endereço de IP. Se o senhor entrar um endereço de IP por conta própria, o porto será considerado como porto 80. Clique no botão "Update Configuration" para salvar essa nova configuração.
- Quando o Firewall bloqueia um recurso de aplicação, a regra que está bloqueando o tráfego aparecerá na lista de Regras de Bloqueio na página da lista branca.
- Para evitar que o firewall bloqueie o recurso de aplicação válido, favor transferir a regra de bloqueio para a seção das Regras da Lista Branca.



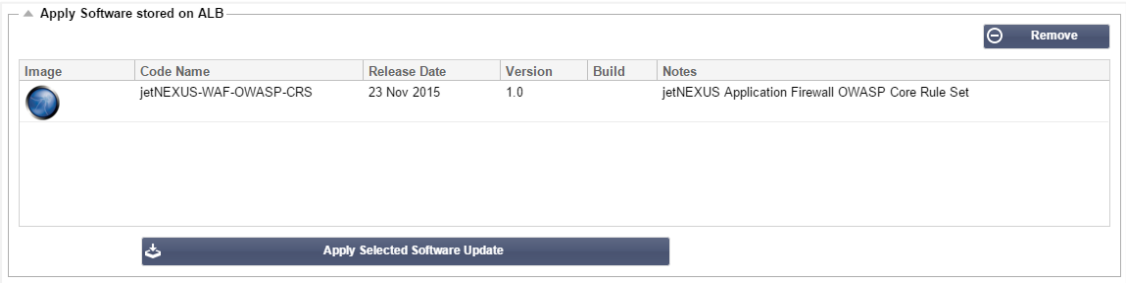
- Pressione Atualizar Configuração quando o senhor tiver transferido todas as regras da seção de Bloqueio para a seção de Lista branca.

Atualização das Regras

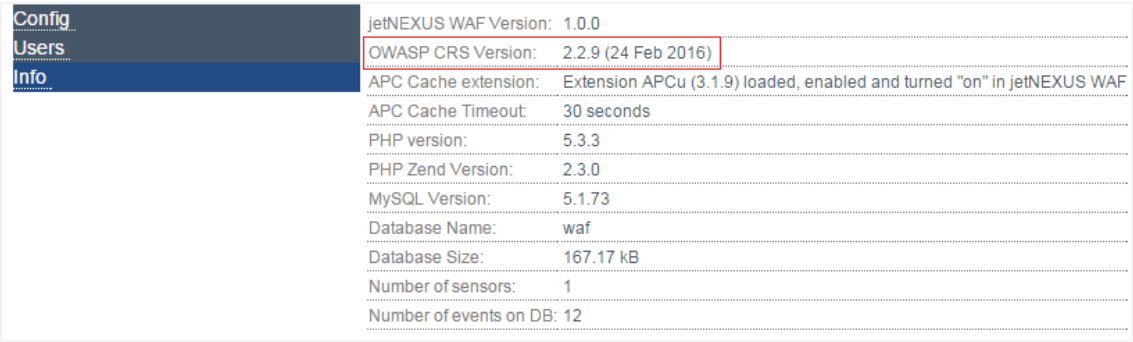
- As regras do Application Firewall podem ser atualizadas acessando a seção Advanced - Software
- Clique em Atualizar para ver o botão do software disponível na seção Detalhes de Atualização de Software
- Uma caixa adicional chamada Download from Cloud é agora exibida
- Verificar se há um conjunto de Regras Básicas da OWASP disponíveis



- Se for o caso, você pode destacar e clicar em Download Selected Software to ALB-X
- Esta ação então fará o download do arquivo inteligente para a aplicação do software armazenado na ALB.



- Destaque o jetNEXUS-WAF-OWASP-CRS e clique em Apply Selected Software Update (Aplicar Atualização de Software Selecionado) e clique em Apply
- O Firewall detectará automaticamente o conjunto de regras atualizadas, carregará e aplicará o mesmo.
- As identificações das regras da lista branca serão mantidas. No entanto, novas regras poderão começar a bloquear recursos válidos de aplicação.
- Queira verificar a lista das Regras de Bloqueio na página da lista branca, neste caso.
- O senhor também pode verificar a seção Management Info do GUI Firewall para a versão do OWASP CRS



Balanceamento de Carga do Servidor Global (edgeGSLB)

Introdução

Global Server Load Balancing (GSLB) é um termo usado para descrever métodos para distribuir o tráfego da rede pela Internet. GSLB é diferente de Server Load Balancing (SLB) ou Application Load Balancing (ALB), pois é tipicamente usado para distribuir tráfego entre múltiplos centros de dados, enquanto um ADC/SLB tradicional é usado para distribuir tráfego dentro de um único centro de dados.

A GSLB é tipicamente usada nas seguintes situações:

Resiliência e recuperação de desastres

O senhor tem vários centros de dados, e deseja dirigi-los em uma situação de Ativo-Passivo, de modo que, se um centro de dados falhar, o tráfego será enviado para o outro.

Balanceamento de carga e geo-localização

O senhor gostaria de distribuir o tráfego entre centros de dados em uma situação Ativa-Ativa com base em critérios específicos, tais como desempenho do centro de dados, capacidade do centro de dados, verificação da saúde do centro de dados, e localização física do cliente (para que o senhor possa enviá-los ao centro de dados mais próximo), etc.

Considerações comerciais

Assegurar que usuários de locais geográficos específicos sejam enviados a centros de dados específicos. Assegurar que conteúdo diferente seja servido (ou bloqueado) a outros usuários, dependendo de vários critérios, tais como o país em que o cliente está, o recurso que está solicitando, o idioma, etc.

Visão geral do sistema de nomes de domínio

A GSLB pode ser complexa; portanto, vale a pena gastar o tempo necessário para entender como funciona o misterioso sistema do Domain Name Server (DNS).

O DNS é composto de três componentes-chave:

- O resolver DNS, ou seja, o Cliente: o resolver é responsável por iniciar as consultas que, em última instância, levem a uma resolução completa do recurso necessário.
- Nameserver: este é o nameserver que o cliente inicialmente conecta para realizar a resolução DNS.
- Nome de autoridade Servidores: Incluir os servidores de nomes de domínio de primeiro nível (TLD) e os servidores de nomes de raiz.

Uma transação típica do DNS é explicada abaixo:

- Um usuário digita "exemplo.com" em um navegador da web, e a consulta viaja para a Internet e é recebida por um resolvedor recursivo do DNS.
- O resolvedor então pergunta a um servidor DNS (.).
- O servidor raiz responde então ao resolvedor com o endereço de um servidor DNS de domínio de primeiro nível (TLD) (como .com ou .net), que armazena as informações para seus domínios. Ao procurar por exemplo.com, nosso pedido é apontado para o TLD .com.
- O resolvedor então solicita o TLD .com.
- O servidor TLD responde então com o endereço IP do servidor de nomes do domínio, por exemplo.com.
- Por último, o resolvedor recursivo envia uma pergunta ao nameserver do domínio.

- O endereço IP, por exemplo.com, é então devolvido ao resolvedor pelo nameserver.
- O resolvedor DNS responde então ao web browser com o endereço IP do domínio solicitado inicialmente.
- Uma vez que os oito passos da pesquisa do DNS tenham devolvido o endereço IP, por exemplo.com, o navegador pode solicitar a página web:
- O navegador faz um pedido **HTTP** para o endereço IP.
- O servidor naquele IP retorna a página da web para ser reproduzida no navegador.

Esse processo pode ser ainda mais complicado:

Caching

A resolução de respostas de nameservers cache pode enviar a mesma resposta a muitos clientes. Resolvedores e aplicações do lado do cliente podem ter políticas de cache diferentes.

Nota: Para testes, paramos e desativamos o Cliente DNS do Windows dentro da seção de serviços do seu sistema operacional. Os nomes DNS continuarão a ser resolvidos; no entanto, não será feito o cache dos resultados nem será registrado o nome do computador. O administrador do sistema precisará decidir se essa é a melhor opção para seu ambiente, pois pode afetar outros serviços.

Tempo para viver

O resolvedor de nomes pode ignorar o Time To Live (TTL), isto é, o tempo de cache para a resposta.

Visão geral da GSLB

A GSLB se baseia no DNS e usa um mecanismo muito semelhante ao descrito acima.

O ADC pode mudar a resposta com base em vários fatores descritos mais adiante no guia. O ADC faz uso dos monitores para verificar a disponibilidade de recursos remotos, acessando o próprio recurso. No entanto, para aplicar qualquer lógica, o sistema deve primeiro receber o pedido do DNS.

Vários projetos permitem isso. O primeiro é onde a GSLB atua como um servidor de nomes autorizado.

O segundo projeto é a implementação mais comum e é semelhante à configuração autorizada do nameserver, mas usa um sub-domínio. O servidor DNS autorizado primário não é substituído pela GSLB, mas delega um sub-domínio para resolução. A delegação direta de nomes ou o uso de CNAMEs permite ao senhor controlar o que é e não é tratado pela GSLB. Nesse caso, o senhor não tem que encaminhar todo o tráfego DNS para a GSLB para sistemas que não requerem a GSLB.

A redundância é providenciada para que se um nameserver (GSLB) falhar, então o nameserver remoto faça automaticamente outro pedido a outro GSLB, impedindo que o website caia.

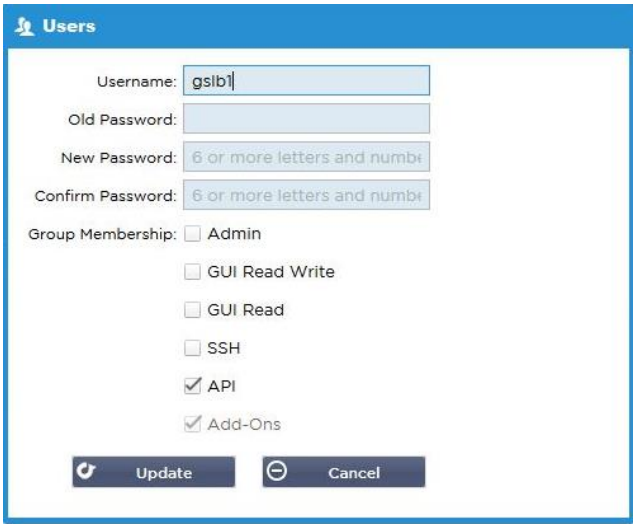
Configuração da GSLB

Depois de baixar o Add-On da GSLB, por favor, implante-o visitando a página Biblioteca > Apps do ADC GUI e clicando no botão "Deploy", como mostrado abaixo.

Após a instalação, favor configurar os detalhes do suplemento da GSLB, inclusive Nome do container, IP externo e Portos externos na Biblioteca > Página do suplemento da GUI da ADC, como mostra a figura abaixo.

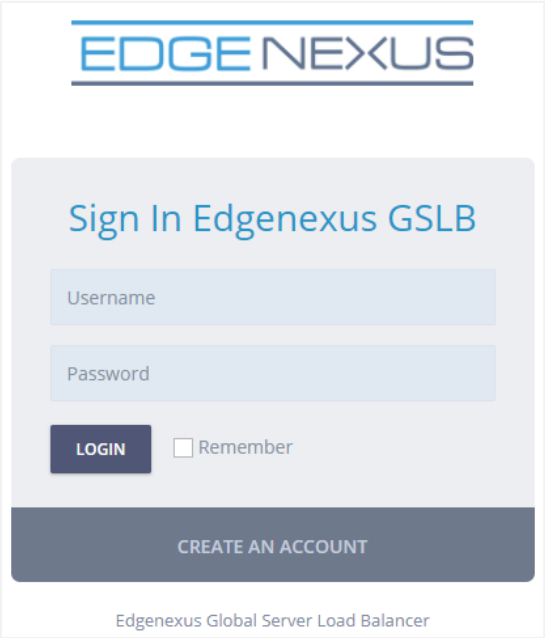
- Container Name é um nome único de um Add-On em execução, hospedado pela ADC, é usado para distinguir vários Add-Ons do mesmo tipo.
- IP externo é o IP da sua rede que será atribuído à GSLB.
- O senhor deve configurar a GSLB para ter um endereço IP externo se quiser tomar decisões baseadas na GEO, pois isso permitirá à GSLB visualizar o endereço IP real dos clientes.
- Portos externos é a lista de portos TCP e UDP da GSLB, que podem ser acessados de outros anfitriões de rede.
- Favor colocar "53/UDP, 53/TCP, 9393/TCP" na caixa de entrada Portos externos para permitir comunicações DNS (53/UDP, 53/TCP) e edgeNEXUS GSLB GUI (9393/TCP).
- Depois de configurar os detalhes do Add-On, favor clicar no botão Update.
- Comece a GSLB Add-On clicando no botão Run (Executar).

- O próximo passo é permitir que o edgeNEXUS GSLB Add-On leia e altere a configuração do ADC.
- Queira visitar a página Sistema > Usuários da ADC GUI e editar um usuário com o mesmo nome do Add-On da GSLB que o senhor implantou, como mostra a figura abaixo.
- Edite "gslb1" usuário e marque API, depois clique em Update - em versões posteriores do software pode já ter sido marcado por padrão.



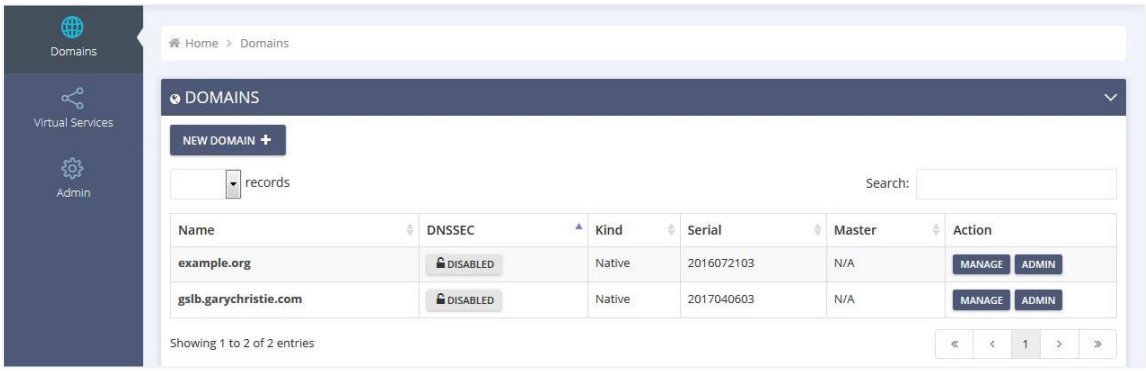
- O próximo passo só é necessário se o senhor estiver configurando a GSLB para fins de teste ou avaliação e não quiser modificar nenhum dado da zona DNS na Internet.
- Nesse caso, favor instruir a ADC a usar o GSLB Add-On como seu servidor de resolução DNS primário, alterando "DNS Server 1 na página Sistema > Rede da GUI da ADC, como mostra a figura abaixo.
- O DNS Server 2 pode ser configurado geralmente com seu servidor DNS local ou com um servidor externo na Internet, como o Google 8.8.8.8.

- Agora é o momento de fazer o log in na GSLB GUI.
- Por favor, navegue até a página Biblioteca > Add-Ons do GUI da ADC e clique no botão Add-On GUI.
- Clicando em uma nova guia do navegador que apresenta a página de login do GUI da GSLB, como mostra a seguir.

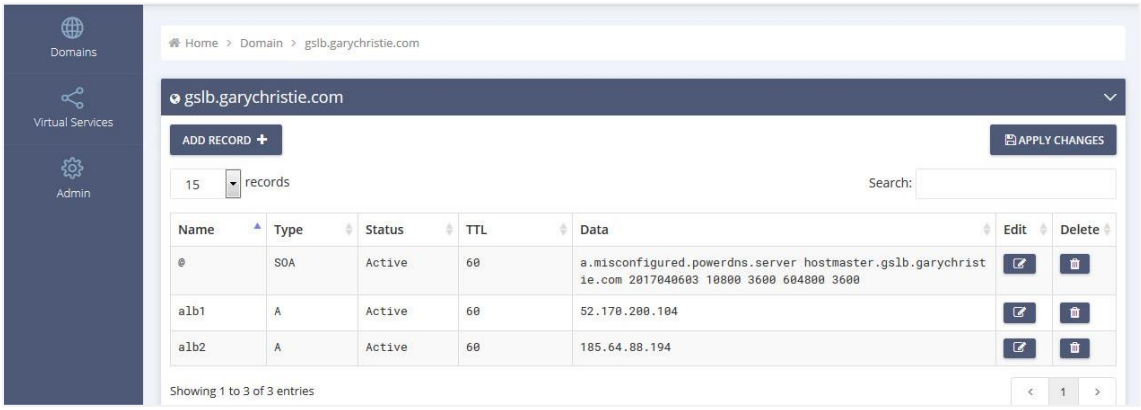


- O nome de usuário padrão é admin, e a senha padrão é jetnexus. Não se esqueça de mudar sua senha na página Administrador > Meu Perfil da GSLB GUI.
- O próximo passo na seqüência de configuração é criar uma zona DNS no servidor de nomes PowerDNS, que é uma parte da GSLB, tornando-a ou um servidor de nomes autorizado para a zona "example.org" ou uma zona de subdomínio, como o subdomínio "geo.example.org" mencionado na seção "DNS-based GSLB Overview", acima.
- Para maiores detalhes sobre a configuração da zona DNS, queira consultar a **DOCUMENTAÇÃO DO POWERDNS NAMESERVER**. Um exemplo de zona é mostrado na figura 6.

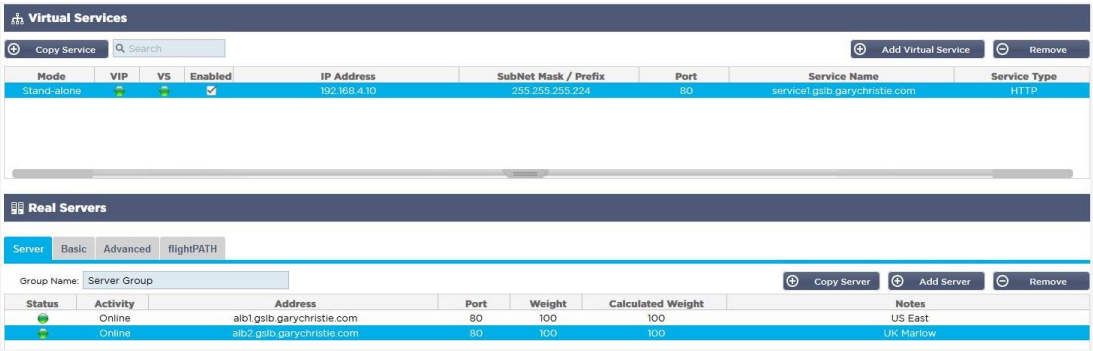
* edgeNEXUS GSLB GUI é baseado em um projeto de fonte aberta PowerDNS-Admin.



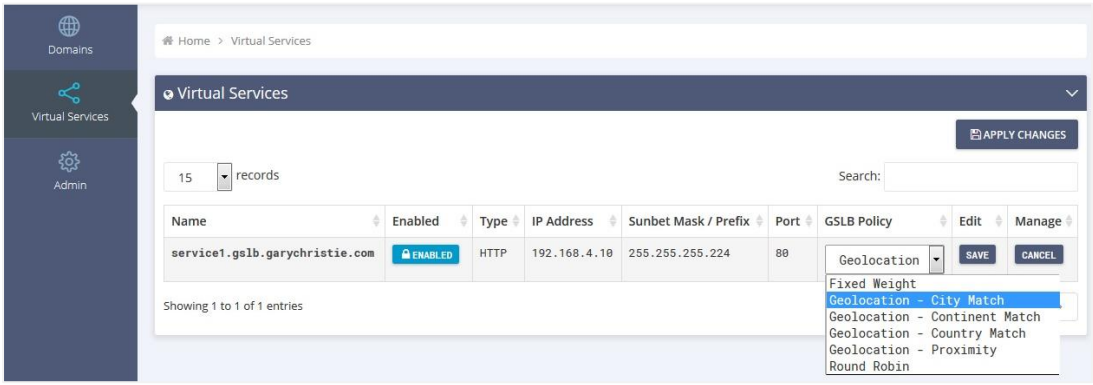
- Depois de criar uma zona DNS, favor clicar no botão Gerenciar e acrescentar nomes de hosts ao domínio, como mostra a figura abaixo.
- Após editar quaisquer registros existentes dentro da GUI da GSLB, favor pressionar o botão Salvar.
- Depois que o senhor tiver concluído a criação dos registros de hostname, favor clicar no botão Apply Changes (Solicitar mudanças). Se o senhor não clicar em Aplicar e depois emendar a página, perderá suas mudanças.
- Abaixo criamos registros que são registros de endereços IPv4.
- Queira certificar-se de criar um registro para todos os registros que deseja resolver, inclusive registros AAAA para endereços IPv6.



- Agora, voltemos à GUI da ADC e definamos um Serviço Virtual que corresponda à zona DNS que acabamos de criar.



- O Serviço Virtual será usado para a verificação da saúde dos servidores no domínio da GSLB.
- A GSLB aproveita o mecanismo de verificação de saúde da ADC, incluindo monitores personalizados. Ele pode ser usado com qualquer um dos tipos de serviços apoiados pelo ADC.
- Favor navegar até a página Serviços > IP-Serviços da GUI da ADC e criar um Serviço Virtual, como mostra a figura abaixo.
- Certifique-se de configurar o Nome de Serviço com o nome de domínio correto que o senhor deseja usar na GSLB. A GSLB lerá isso através do API e preencherá automaticamente a seção Serviços Virtuais no GUI da GSLB.
- Queira acrescentar todos os servidores no domínio da GSLB sob a seção Servidores Reais da imagem acima.
- O senhor poderá especificar servidores, seja por seus nomes de domínio ou endereços IP.
- Se o senhor especificar os nomes de domínio, então usará os registros criados em sua GSLB.
- O senhor pode escolher diferentes métodos e parâmetros de monitoramento da saúde do servidor nas guias Básica e Avançada.
- O senhor pode colocar a atividade de alguns servidores em standby para um cenário ativo-passivo.
- Nesse caso, se um servidor "Online" falhar num exame de saúde e houver um servidor "Standby" saudável, a Edgenexus EdgeGSLB resolverá o nome do domínio para um endereço do servidor "Standby".
- Queira consultar a seção de **SERVIÇOS VIRTUAIS** para obter detalhes sobre a configuração dos Serviços Virtuais.
- Agora, passemos à GUI da GSLB.
- Navegue até a página de Serviços Virtuais e selecione uma política da GSLB para o domínio da API recuperada da seção de serviços virtuais da ADC.
- Isso é mostrado na figura abaixo.



- O GSLB apóia as seguintes políticas:

Política	Descrição

Peso fixo	A GSLB seleciona o servidor com o maior peso (a ponderação do servidor pode ser atribuída pelo usuário). No caso de múltiplos servidores com o maior peso, a GSLB selecionará um desses servidores ao acaso.
Round Robin ponderado	Escolham servidores um a um, em fila. Os servidores que têm pesos maiores são selecionados com mais freqüência do que os servidores que têm pesos menores.
Geolocalização	Proximidade - escolha um servidor que esteja localizado mais próximo da localização do cliente, usando dados de latitude e longitude geográficas. Os servidores no mesmo país que o cliente são preferidos, mesmo que estejam mais distantes do que os servidores nos países vizinhos.
Geolocalização	Partida da cidade - escolha um servidor na mesma cidade que o cliente. Se não houver um servidor na cidade do cliente, selecione um servidor no país do cliente. Se não houver um servidor no país do cliente, selecione um servidor no mesmo continente. Se isso não for possível, selecione um servidor que esteja localizado mais próximo da localização do cliente, usando dados de latitude e longitude geográficas.
Geolocalização	Partida de país - escolha um servidor no mesmo país que o cliente. Se não houver um servidor no mesmo país, tente o mesmo continente, então tente o local mais próximo.
Geolocalização	Partida continental - escolha um servidor no mesmo continente que o cliente. Se não houver um servidor no mesmo continente, tente a localização mais próxima.

- Após ter selecionado uma política da GSLB, não se esqueça de clicar no botão Apply Changes (Aplicar mudanças).
- Agora o senhor pode rever e ajustar os detalhes do Serviço Virtual, clicando no botão Gerenciar.
- Isto apresentará uma página mostrada abaixo.
- Se o senhor tiver escolhido uma das políticas baseadas no peso, talvez precise ajustar os pesos do servidor GSLB.
- Se o senhor tiver selecionado uma das políticas da GSLB baseadas em geo-localização, talvez precise especificar dados geográficos para os servidores.
- Se o senhor não especificar nenhum dado geográfico para os servidores, a GSLB usará os dados fornecidos pela **BASE DE DADOS GEOLITE2 DO MAXMIND**.
- O senhor também pode modificar o nome do servidor, porto e atividade nesta página.
- Essas mudanças serão sincronizadas com o ADC quando o senhor clicar no botão "Apply Changes" (Aplicar mudanças).

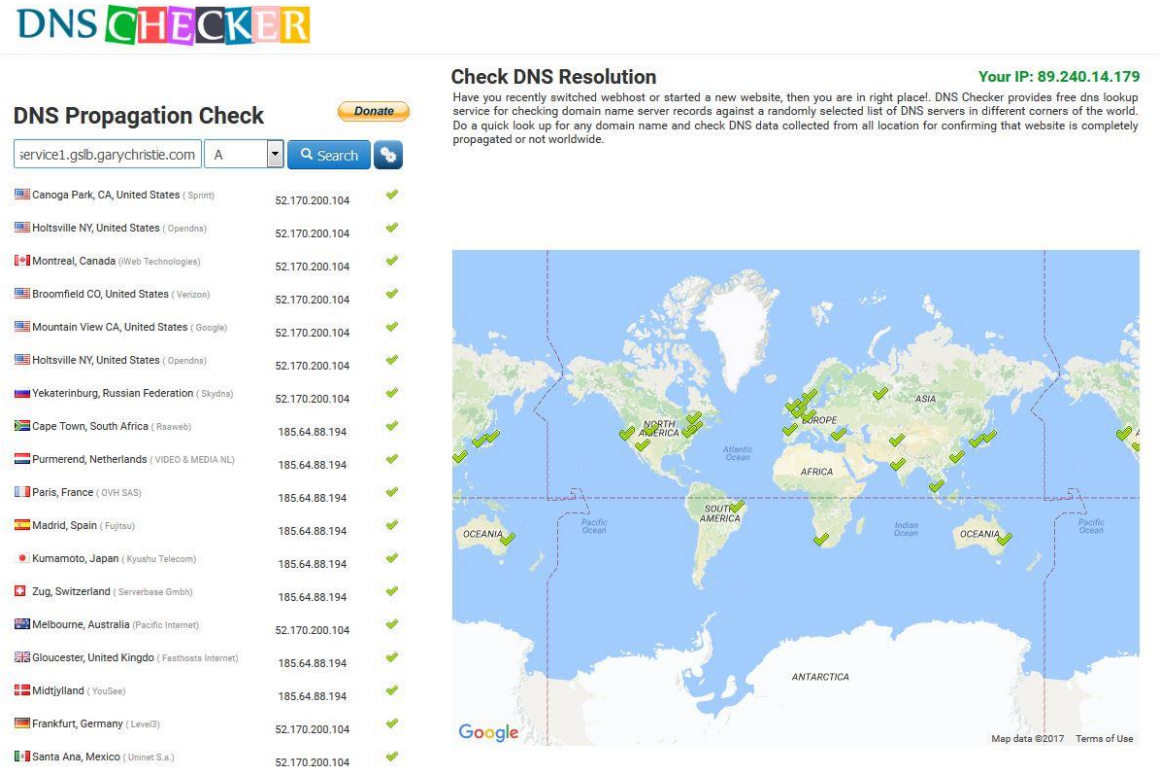
- Uma ótima maneira de verificar que respostas a GSLB enviará aos clientes é usar o NSLOOOKUP.
- Se o senhor está usando Windows, a ordem está abaixo.

```
NSLOOKUP service1.gslb.garychristie.com 192.168.4.10
```

- Onde service1.gslb.garychristie.com é o nome de domínio que o senhor deseja resolver.
- Onde 192.168.4.10 é o endereço IP externo de sua GSLB.
- Para verificar que endereço IP será devolvido na Internet, o senhor pode usar o servidor DNS do google do 8.8.8.8.

  Nslookup service1.gslb.garychristie.com 8.8.8.8.

- Alternativamente, o senhor pode usar algo como HTTPs://dnschecker.org. Exemplo HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Veja abaixo um exemplo dos resultados.



Locais personalizados

Redes Privadas

O GSLB também pode ser configurado para usar locais personalizados, de modo que o senhor possa usá-lo em redes internas "privadas". No cenário acima, a GSLB determina a localização do cliente cruzando o endereço IP público do cliente com um banco de dados para determinar sua localização. Ele também calcula a localização do endereço IP do serviço a partir do mesmo banco de dados, e se a política de balanceamento de carga for definida para uma política GEO, ele retornará o endereço IP mais próximo. Esse método funciona perfeitamente bem com endereços IP públicos, mas não existe tal base de dados para endereços privados internos que estejam de acordo com a RFC 1918 para endereços IPv4 e a RFC 4193 para endereços IPv6.

Favor ver a página da Wikipedia explicando o endereço privado
HTTPS://EN.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Como funciona

Normalmente, a idéia por trás do uso de nossa GSLB para redes internas é a de que os usuários de endereços específicos recebam uma resposta diferente para um serviço, dependendo da rede em que estiverem localizados. Portanto, vamos considerar dois centros de dados, Norte e Sul, fornecendo um serviço chamado north.service1.gslb.com e south.service1.gslb.com, respectivamente. Quando um usuário

do centro de dados do Norte consulta a GSLB, queremos que a GSLB responda com o endereço IP associado a north.service1.gslb.com, desde que o serviço esteja funcionando corretamente. Alternativamente, se um usuário do centro de dados do sul consultar a GSLB, queremos que a GSLB responda com o endereço IP associado a south.service1.gslb.com novamente, desde que o serviço esteja funcionando corretamente.

Então, o que é preciso fazer para que o cenário acima aconteça?

- Precisamos ter pelo menos dois locais personalizados, um para cada centro de dados
- Atribuir as diversas redes privadas a esses locais
- Designar cada serviço para o respectivo local

Como configuramos esse aspecto na GSLB?

Acrescentar uma localização para o Centro de Dados do Norte

- Clique em Custom Locations no lado esquerdo
- Clique em Add Location
- Nome
  - Norte
- Acrescente um endereço IP privado e uma máscara de sub-rede para sua rede do Norte. Para esse exercício, assumiremos que o serviço e os endereços IP do cliente estão na mesma rede privada.
  - 10.1.1.0/24
- Acrescentar o código do continente
  - UE
- Acrescentar o código do país
  - REINO UNIDO
- Acrescentar Cidade
  - Enfield
- Adicionar Latitude - obtido no google
  - 51.6523
- Adicionar Longitude - obtido do google
  - 0.0807

Nota, favor usar os códigos corretos que podem ser obtidos aqui.

Acrescentar uma localização para o Centro de Dados do Sul

- Clique em Custom Locations no lado esquerdo
- Clique em Add Location
- Nome
  - Sul
- Acrescente um endereço IP privado e uma máscara de sub-rede para sua rede do Sul. Assumiremos que o serviço e os endereços IP do cliente estão na mesma rede privada para esse exercício.
  - 192.168.1.0/24
- Acrescentar o código do continente
  - UE
- Acrescentar o código do país
  - REINO UNIDO
- Acrescentar Cidade
  - Croydon
- Adicionar Latitude - obtido no google
  - 51.3762
- Adicionar Longitude - obtido do google

- 0.0982

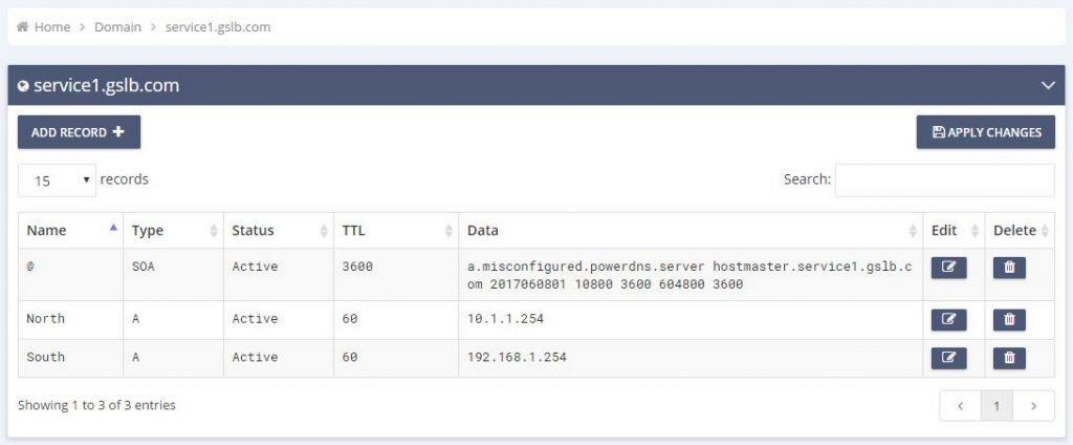
Nota, favor usar os códigos corretos que podem ser obtidos **AQUI.**

Adicionar um registro A para north.service1.gslb.com

- Clique no serviço de domínio1.gslb.com
- Clique em Add Record
- Acrescentar nome
  - Norte
- Tipo
  - A
- Status
  - Ativo
- TTL
  - 1 Minuto
- Endereço IP
  - 10.1.1.254 (Note-se que isto está na mesma rede que a localização de Enfield)

Adicionar um registro A para south.service1.gslb.com

- Clique no serviço de domínio1.gslb.com
- Clique em Add Record
- Acrescentar nome
  - Sul
- Tipo
  - A
- Status
  - Ativo
- TTL
  - 1 Minuto
- Endereço IP
  - 192.168.1.254 (Note-se que isto está na mesma rede que a localização de Croydon)



Fluxo de tráfego

Exemplo 1 - Cliente no Data-Center do Norte

- Cliente IP 10.1.1.23 consulta GSLB para serviço1.gslb.com
- A GSLB procura o endereço IP 10.1.1.23 e o combina com o Custom Location Enfield 10.1.1.0/24
- GSLB examina seus registros A para o serviço1.gslb.com e combina north.service1.gslb.com como também está na rede 10.1.1.0/24
- GSLB responde a 10.1.1.23 com o endereço IP 10.1.1.254 para serviço1.gslb.com

Exemplo 2 - Cliente no Centro de Dados do Sul

- Cliente IP 192.168.1.23 consulta GSLB para serviço1.gslb.com
- A GSLB procura o endereço IP 192.168.1.23 e o combina com o Croydon 192.168.1.0/24
- GSLB examina seus registros A para o serviço1.gslb.com e combina com South.service1.gslb.com como também está na rede 192.168.1.0/24
- GSLB responde a 192.168.1.23 com o endereço IP 192.168.1.254 para serviço1.gslb.com

Apoio técnico

Fornecemos apoio técnico a todos os nossos usuários de acordo com os termos padrão de serviço da companhia.

Forneceremos todo o apoio através do suporte técnico se o senhor tiver um contrato ativo de Suporte e Manutenção para o edgeADC, edgeWAF ou edgeGSLB.

Para levantar um ingresso de apoio, queira fazer uma visita:

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