EdgeADC

GUIA DE ADMINISTRAÇÃO

VERSÃO DO SOFTWARE

4.2.8.1909

Conteúdo

Propriedades do documento 7
Aviso de isenção de responsabilidade de documento 7
Direitos autorais 7
Marcas 7
Apoio Edgenexus 7
Instalando o EdgeADC 8
VMware ESXi 8
Instalando a interface VMXNET3 8
Microsoft Hyper-V 9
Citrix XenServer 10
Nutanix AHV 11
Exigências e Versões 11
Primeira Configuração de Boot 13
Primeira Bota - Detalhes da Rede Manual 13
Primeira Bota - DHCP bem-sucedido 13
Primeira Bota - Falhas do DHCP 13
Mudança do endereço IP de gerenciamento 14
Trocando a máscara de sub-rede por eth0 14
Atribuição de uma porta de entrada padrão 14
Verificação do valor padrão da porta de entrada 14
Acesso à interface web 14
Tabela de Referência de Comando 15
Lançamento do ADC Web Console 16
Credenciais de Login Padrão 16
O Painel Principal 17
Serviços 18
Serviços IP 18
Serviços virtuais 18
Servidores reais 24
Mudanças reais no servidor para retorno direto do servidor 37
Configuração do Servidor de Conteúdo Requerido 37
Mudanças reais no servidor - Modo Gateway 38
Configuração do Servidor de Conteúdo Requerido 38
Exemplo de braço único 39
Exemplo de braço duplo 39
Biblioteca 40
Suplementos 40

Apps 40
Compra de um Add-on 40
Implantação de um aplicativo 41
Autenticação 41
Configurando a Autenticação - Um Fluxo de Trabalho 42
Servidores de Autenticação 42
Regras de Autenticação 43
Assinatura única 43
Formulários 44
Cache 45
flightPATH 47
Monitores de Servidor Real 54
Tipos de monitores de servidores reais 55
A página do Monitor do Servidor Real 58
Detalhes 58
Exemplos de Monitor de Servidor Real 60
Certificados SSL 62
O que o ADC faz com o Certificado SSL? 62
Criar certificado 62
Gerenciar Certificado 64
Importação de um certificado 66
Importação de certificados múltiplos 67
Widgets 68
Ver 74
Painel de controle 74
Uso do painel de instrumentos 74
História 76
Visualização de dados gráficos 76
Logs 77
Baixar logs do W3C 78
Estatísticas 78
Compressão 78
Acertos e conexões 79
Caching 80
Persistência da sessão 80
Hardware 81
Status 81
Detalhes do Serviço Virtual 81

Sistema 84
Clustering 84
Papel 84
Configurações 87
Administração 87
Mudando a prioridade de um ADC 88
Data e hora 89
Manual Data e hora 89
Sincronizar data e hora (UTC) 89
Eventos por e-mail 90
Endereço 90
Servidor de correio (SMTP) 90
Notificações e alertas 91
Avisos 92
Histórico do sistema 92
Coleta de dados 92
Manutenção 93
Licença 93
Detalhes da licença 93
Instalações 94
Licença de instalação 95
Logging 95
Detalhes de registro do W3C 95
Servidor Syslog 97
Servidor remoto Syslog 97
Armazenamento remoto de logs 97
Limpar arquivos de log 99
Rede 99
Configuração básica 100
Detalhes do Adaptador 100
Interfaces 101
Colagem 102
Rota Estática 103
Detalhes da rota estática 104
Configurações avançadas de rede 104
SNAT 104
Energia 105
Segurança 106

SNMP 107
Configurações SNMP 107
SNMP MIB 108
MIB Download 108
ADC OID 108
Gráficos históricos 109
Usuários e logs de auditoria 109
Usuários 109
Diário de Auditoria 111
Avançado 112
Configuração 112
Download de uma configuração 112
Carregamento de uma configuração 112
Configurações globais 112
Temporizador de Cache Host 113
Drenagem 113
SSL 113
Autenticação 113
Protocolo 113
Servidor muito ocupado 114
Encaminhado para 114
Configurações de Compressão HTTP 115
Exclusões de Compressão Global 116
Biscoitos de persistência 117
Software 117
Detalhes de atualização de software 117
Baixar do Cloud 118
Upload de software para ALB 118
Aplicar o software armazenado no ALB 119
Solução de problemas 119
Arquivos de suporte 119
Trace 120
Ping 121
Captura 121
Ajuda 123
Sobre nós 123
Referência 123
O que é um jetPACK 124

Descarregamento de um jetPACK 124
Microsoft Exchange 124
Microsoft Lync 2010/2013 125
Serviços Web 126
Área de trabalho remota da Microsoft 126
DICOM - Imagem e Comunicação Digital em Medicina 126
Oracle e-Business Suite 126
Vista Horizontal VMware 126
Configurações globais 126
Opções de cifras 126
flightPATHs 127
Aplicando um jetPACK 127
Criando um jetPACK 127
Introdução ao flightPATH 130
O que é FlightPATH? 130
O que o flightPATH pode fazer? 130
Condição 130
Exemplo 133
Avaliação 133
Ação 135
Ação 135
Meta 135
Dados 136
Usos comuns 137
Firewall de Aplicação e Segurança 137
Características 137
Regras pré-construídas 138
Extensão HTML 138
Index.html 138
Fechar Pastas 138
Ocultar CGI-BBIN: 139
Aranha de madeira 139
Forçar HTTPS 139
Fluxo de mídia: 140
Trocar HTTP para HTTPS 140
Cartões de crédito em branco 140
Validade do conteúdo 141
Tipo de servidor falso 141

Firewall de Aplicação Web (edgeWAF) 144
Executando o WAF 144
Exemplo de arquitetura 145
WAF usando endereço IP externo 145
WAF usando endereço IP interno 145
Acesso ao seu WAF add-on 146
Atualização das regras 147
Balanceamento de carga do servidor global (edgeGSLB) 149
Introdução 149
Resiliência e recuperação de desastres 149
Balanceamento de carga e geo-localização 149
Considerações comerciais 149
Visão geral do sistema de nomes de domínio 149
O DNS consiste em três componentes-chave: 149
Uma transação DNS típica é explicada abaixo: 149
Caching 150
Tempo para viver 150
Visão geral da GSLB 150
Configuração da GSLB 150
Localizações personalizadas 156
Redes Privadas 156
Como funciona 156
Como configuramos este visual na GSLB? 156
Fluxo de tráfego 158
Suporte Técnico 159

Propriedades do documento

Número do documento: 2.0.11.17.21.13.11

Data de criação do documento: 30 de abril de 2021

Documento Editado por último: November 17, 2021

Autor do documento: Jay Savoor

Último documento editado por:

Indicação de documentos: EdgeADC - Versão 4.2.8.1909

Aviso de isenção de responsabilidade de documento

As imagens e gráficos neste manual podem diferir ligeiramente de seu produto devido a diferenças na versão de lançamento de seu produto. A Edgenexus garante que eles façam todo o esforço razoável para garantir que as informações contidas neste documento sejam completas e precisas. A Edgenexus não assume nenhuma responsabilidade por quaisquer erros. A Edgenexus faz alterações e correções nas informações deste documento em lançamentos futuros quando a necessidade surgir.

Direitos autorais

© 2021Todos os direitos reservados.

As informações contidas neste documento estão sujeitas a alterações 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, incluindo fotocópia e gravação, para qualquer finalidade, sem a permissão expressa por escrito do fabricante. As marcas registradas são propriedades de seus respectivos proprietários. Todos os esforços são feitos para tornar este guia o mais completo e preciso possível, mas nenhuma garantia de aptidão está implícita. Os autores e a editora não terão 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 Edgenexus

Se você tiver alguma pergunta técnica sobre este produto, por favor, levante um ticket de suporte em: support@edgenexus.io

Instalar o EdgeADC

O produto EdgeADC (referido como ADC) está disponível para instalação através de vários métodos. Cada alvo de plataforma requer seu instalador, e todos eles estão disponíveis para você.

Estes são os vários modelos de instalação disponíveis.

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

O dimensionamento da máquina virtual que você 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.

- Baixe o pacote OVA de instalação mais recente do ADC usando o link apropriado fornecido com o e-mail de download.
- Uma vez baixado, por favor, descompacte em um diretório adequado em seu host ESXi 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 dispositivo ADC irá funcionar.
- Selecione uma datastore com espaço suficiente e clique em **PRÓXIMO**
- Você então será informado sobre o produto; clique **PRÓXIMO**
- Clique **PRÓXIMO.**
- Uma vez que você tenha copiado os arquivos para o datastore, você pode 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 inicializará então, e a tela de inicialização do ADC será exibida no console.

Instalando a interface VMXNET3

O driver VMXnet3 é suportado, mas você precisará fazer alterações nas configurações do NIC primeiro.

***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 a instalação ou atualização de uma ferramenta VMware, **apenas** execute a atualização de hardware)
3. Adicionar dois DNIs e selecioná-los para serem VMXNET3
4. Iniciar o VA usando o método padrão. Ele funcionará com o VMXNET3

Habilitando a interface VMXNET3 em um VA já em execução

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

Nós apoiamos a VMware ESXi como plataforma de produção. Para fins de avaliação, você pode usar o VMware Workstation and Player.

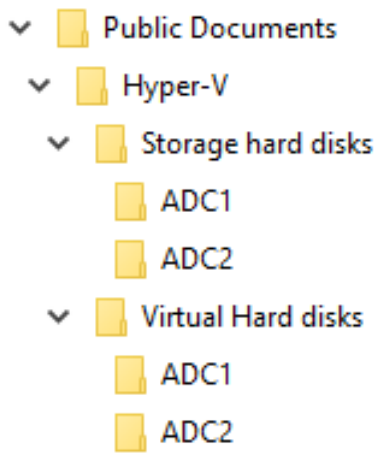
Consulte a seção **PRIMEIRA CONFIGURAÇÃO DA BOTA** para prosseguir.

Microsoft Hyper-V

O dispositivo virtual Edgenexus ADC pode ser facilmente instalado dentro de uma estrutura de virtualização Microsoft Hyper-V. Este guia assume que você especificou e configurou corretamente seu sistema Hyper-V e os 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 Hyper-V Manager.
- 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-V Discos rígidos virtuais ADC1 e C:UUSADORES Público-Documentos Hyper-V Armazenamento de discos rígidos ADC1
- **Nota**: Novas subpastas específicas do ADC para os discos rígidos virtuais e os discos rígidos de armazenamento precisam ser criados para cada instalação de instância do ADC virtual, como mostrado abaixo:

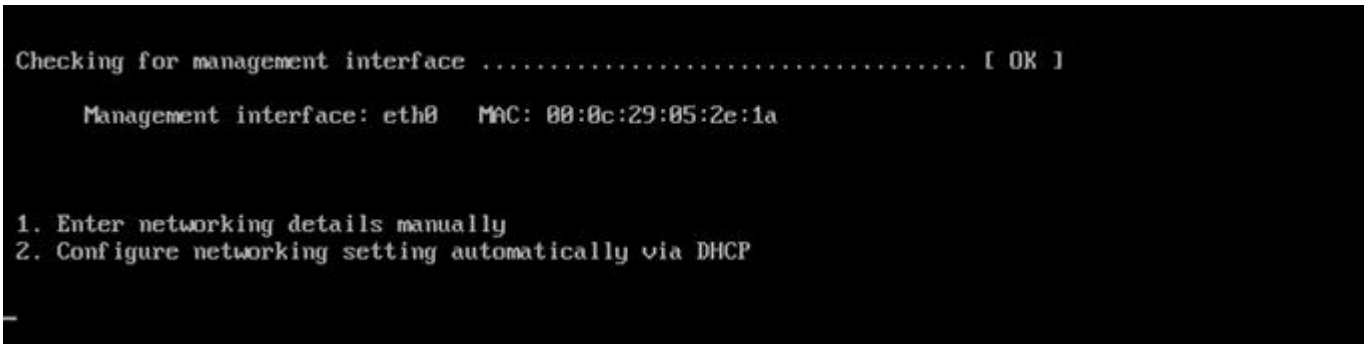


- Copie o arquivo .vhd EdgeADC extraído para a pasta 'Storage hard disk' criada acima.
- Em seu cliente Hyper-V Manager, clique com o botão direito do mouse sobre o servidor e selecione "Importar Máquina Virtual".

- 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 próximo
- 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 Concluir.
- Clique com o botão direito do mouse sobre a máquina virtual **ADC** recém importada e selecione Start

NOTA: CONFORME HTTP://SUPPORT.MICROSOFT.COM/KB/2956569, VOCÊ DEVE IGNORAR A MENSAGEM DE STATUS "DEGRADED (REQUER ATUALIZAÇÃO DE SERVIÇOS DE INTEGRAÇÃO)", QUE PODE SER EXIBIDA COMO ABAIXO APÓS O VA SER INICIADO. NENHUMA AÇÃO É NECESSÁRIA, E O SERVIÇO NÃO É DEGRADADO.

- Enquanto a VM está se inicializando, você pode clicar com o botão direito do mouse na entrada da VM e selecionar Connect...Você será então presenteado com o console EdgeADC.



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

Consulte a seção **PRIMEIRA CONFIGURAÇÃO DA BOTA** para prosseguir.

Citrix XenServer

O ADC Virtual appliance é instalável no Citrix XenServer.

- Extraia o arquivo ADC OVA ALB-VA para sua máquina ou servidor local.
- Cliente Open Citrix XenCenter.
- Em seu cliente XenCenter, selecione **"Arquivo: Importar".**
- Navegue até, e selecione o arquivo **OVA**, depois clique em **"Abrir próximo".**
- Quando solicitado, selecione o local de criação da VM.
- Escolha qual XenServer você deseja instalar e clique em **"PRÓXIMO".**
- Selecione o repositório de armazenamento (SR) para a colocação do disco virtual quando solicitado.
- Selecione um SR com espaço suficiente e clique em **"PRÓXIMO".**
- Mapeie suas interfaces de rede virtual. Ambas as interfaces dirão Eth0; no entanto, observe que a interface inferior é Eth1.
- Selecione a rede de destino para cada interface e clique em **PRÓXIMO**
- **NÃO** assinale o "Use Operating System Fixup".
- Clique em **"PRÓXIMO".**
- Escolha a interface de rede a ser utilizada para o VM de transferência temporária.
- Escolha a interface de gerenciamento, geralmente Rede 0, e deixe as configurações de rede no DHCP. Esteja ciente de que você 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 **"PRÓXIMO".**

- Revise todas as informações e verifique as configurações corretas então. Clique em **"FINISH" (finalizar).**
- Seu VM começará a transferir o disco virtual "ADC ADC" e, uma vez concluído, aparecerá sob seu XenServer.
- Dentro de seu cliente XenCenter, agora você poderá ver a nova máquina virtual.
  Clique com o botão direito do mouse no VA e clique em "**START**".
- Seu VM iniciará então, e a tela de inicialização do ADC aparecerá.

- Uma vez configurado, o logon para a VA se apresenta.

Consulte a seção **PRIMEIRA CONFIGURAÇÃO DA BOTA** para prosseguir.

Nutanix AHV

A seção seguinte mostra como instalar o EdgeADC em uma plataforma AHV da Nutanix.

Exigências e Versões

Este guia é relevante para o EdgeADC 4.2.6 e acima.

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

- O primeiro passo é entrar na Nutanix Prism Central.

Carregando a imagem do EdgeADC

- Navegar para Infra-estrutura Virtual > Imagens
- Clique no botão Adicionar imagem
- Selecione o arquivo de imagem EdgeADC que você baixou e clique no botão Abrir para carregar a imagem.
- Digite um nome para a imagem no campo Descrição da imagem.
- Selecione uma categoria apropriada
- Selecione a imagem e clique na seta para a direita
- Selecione Todas as imagens e clique em Salvar.

Criando o VM

- Navegue para Infraestrutura Virtual > VMs
- Clique no botão Criar VM
- Digite um nome para o VM, o número de CPUs que você deseja ter, e o número de núcleos que você deseja alocar para o VM.
- Em seguida, role para baixo no diálogo e digite a quantidade de memória que você deseja alocar ao VM. Você pode começar com 4GB e aumentá-la dependendo do uso.

Adicionando o disco

- A seguir, clique no link Adicionar novo disco
- Selecione a opção Clone do Serviço de Imagem dentro do menu suspenso Operação.

- Selecione a imagem do EdgeADC que você adicionou e clique no botão Adicionar.
- Selecione o disco para ser o disco de inicialização.

Acrescentando o DNI, Rede e Afinidade

- A seguir, clique no botão Add New NIC (Adicionar novo DNI). Você precisará ter dois NICS.
- Selecione a Rede e clique no botão Adicionar
- Clique no botão Definir afinidade
- Selecione os hospedeiros Nutanix nos quais o VM é permitido rodar, depois clique no botão Salvar.
- Verifique as configurações que você fez e clique no botão Salvar

Acionando o VM

- A partir da lista de VMs, clique no nome da VM que você acabou de criar
- Clique no botão Ligar para a VM
- Uma vez que a VM esteja ligada, clique no botão Launch Console

Configurando a rede EdgeADC

- Siga as instruções na seção Primeiro Ambiente de Boot.
- O EdgeADC está agora pronto para uso, e você poderá acessar sua GUI usando seu navegador e o endereço IP de gerenciamento.

Primeira Configuração de Boot

Na primeira inicialização, o ADC VA exibe a seguinte tela solicitando configuração para 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, você terá 10 segundos para interromper a atribuição automática de detalhes de IP via DHCP

Para interromper este processo, clique na janela do console e pressione qualquer tecla. Em seguida, você pode inserir os seguintes detalhes manualmente.

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

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

Primeira Bota - DHCP bem-sucedido

Se você não interromper o processo de atribuição da rede, seu ADC entrará em contato com um servidor DHCP após um intervalo de tempo para obter seus detalhes de 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 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. Aconselhamos sempre o uso de um **endereço IP FIXADO** ao usar o VA. Siga as etapas de **ALTERAÇÃO DO ENDEREÇO IP DE GERENCIAMENTO** e seções subseqüentes até ter completado a configuração da rede.

Primeira Bota - Falhas do DHCP

Se você 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 verificará novamente.

Mudança do endereço IP de gerenciamento

Você pode mudar o endereço IP do VA a qualquer momento usando o **conjunto de** comandos **greenside=n.n.n.n,** como mostrado abaixo.

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

Trocando a máscara de sub-rede por eth0

As interfaces de rede usam o prefixo 'eth'; o endereço de rede de base é chamado eth0. A máscara de sub-rede ou máscara de rede pode ser alterada usando o comando **eth0 n.n.n.n.** Você pode ver um exemplo abaixo.

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

Atribuição de uma porta de entrada padrão

A VA precisa de uma porta de entrada padrão para suas operações. Para definir o gateway padrão, use a **rota de** comando **add default gw n.n.n.n,** como mostrado no exemplo abaixo.

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

Verificação do valor padrão da porta de entrada

Para verificar se o gateway padrão é adicionado e está correto, use a **rota de** comando. Este comando exibirá as rotas da rede e o valor padrão do gateway. 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
```

Agora você pode acessar a Interface Gráfica do Usuário (GUI) para configurar o ADC para produção ou uso de avaliação.

Acesso à interface web

Você 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. Você pode mudar o ADC para usar o certificado SSL de sua própria escolha.

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

Nome de usuário predefinido = **admin** / Senha predefinida = **jetnexus**

Tabela de Referência de Comando

Comando	Parâmetro1	Parâmetro2	Descrição	Exemplo
data			Mostra a data e a hora configuradas atualmente	Ter 3 de setembro 13:00 UTC 2013
inadimplência			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]		Veja a configuração da interface para todas as interfaces	ifconfig
	eth0		Veja apenas a configuração da interface do eth0	ifconfig eth0
machineid			Este comando fornecerá o comando de máquina utilizado para licenciar o ADC ADC	EF4-3A35-F79
desista			Sair da interface da linha de comando	
reinicialização			Terminar todas as conexões e reiniciar o ADC ADC	reinicialização
reiniciar			Reinicie os serviços virtuais do ADC ADC	
rota	[em branco]		Veja a tabela de roteamento	rota
	adicionar	gw padrão	Adicionar o endereço IP padrão do gateway	rota adicionar gw padrão 192.168.100.254
conjunto	verde		Definir o endereço IP de gerenciamento para o ADC	set greenside=192.168.101.1
	máscara		Configure a máscara de sub-rede para uma interface. Os nomes das interfaces são eth0, eth1....	definir máscara eth0 255.255.255.255.0
show			Exibe as configurações globais	
desligamento			Terminar todas as conexões e desligar a energia do ADC ADC	
status			Exibe as estatísticas de dados atuais	
topo			Veja as informações do processo, como CPU e Memória	
viewlog	mensagens		Exibe as mensagens do syslog cru	Ver mensagens de log

Favor observar: os comandos não são sensíveis a maiúsculas e minúsculas. Não há histórico de comandos.

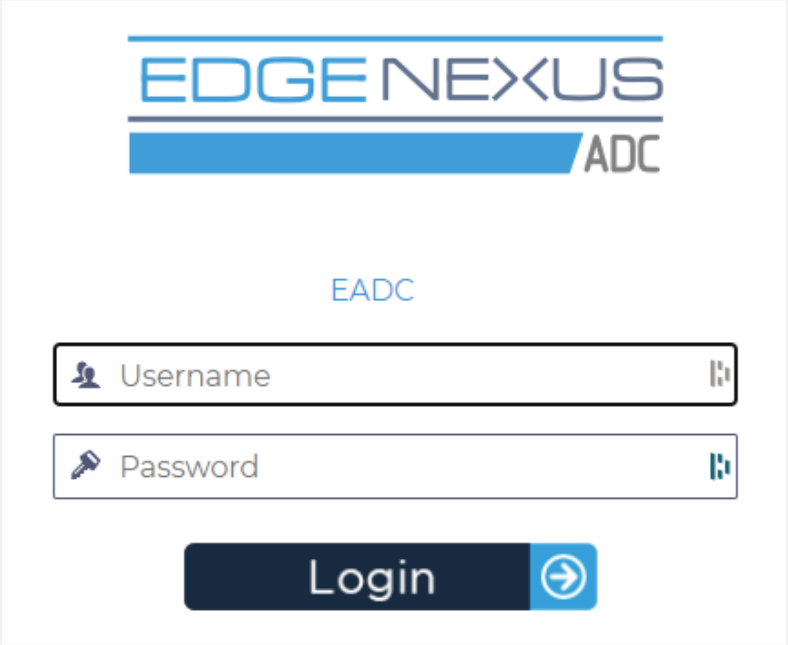
Lançamento do ADC Web Console

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

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

https://adc.company.com

Quando lançado, o console web do ADC é como mostrado abaixo, permitindo que você faça o login como usuário administrativo.



Credenciais de Login Padrão

As credenciais de login padrão são:

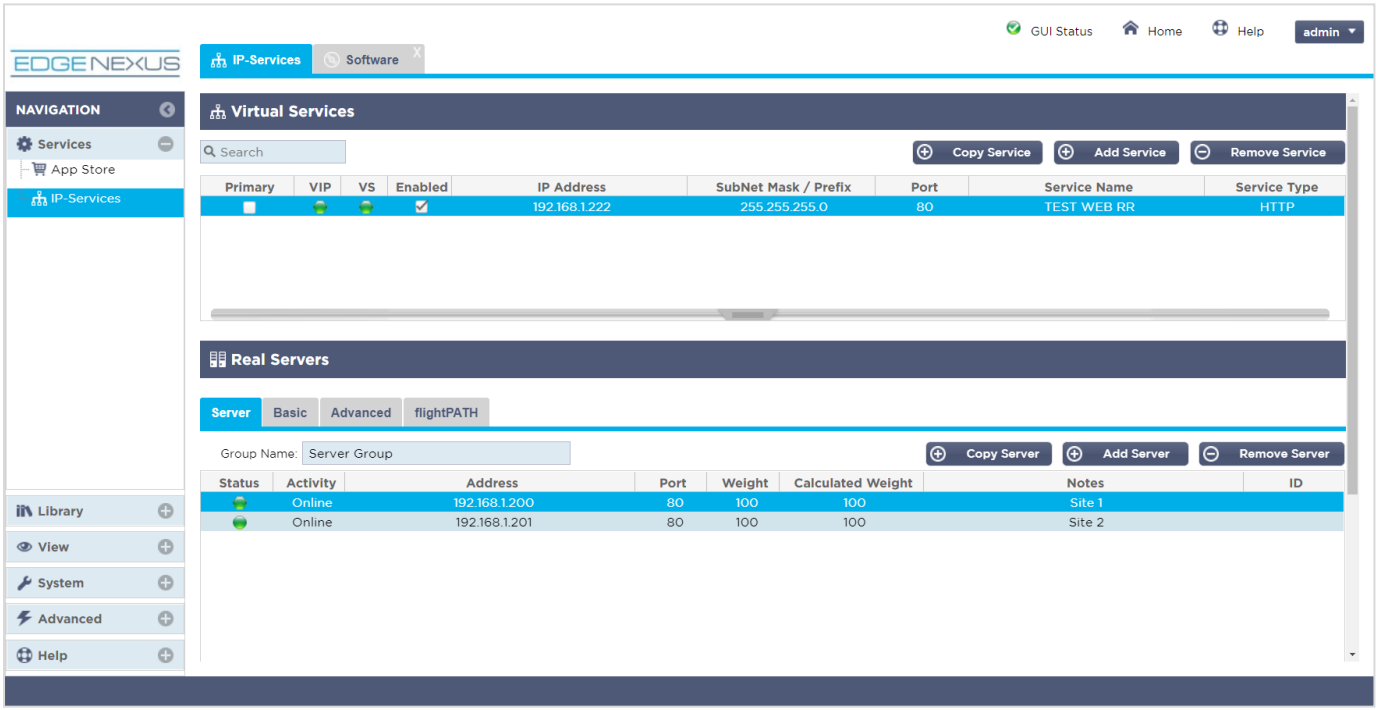
- Nome de usuário: admin
- Senha: jetnexus

Você pode alterar isto a qualquer momento usando as capacidades de configuração do usuário localizadas em *Sistema* > *Usuários*.

Uma vez conectado com sucesso, o painel principal do ADC é exibido.

O Painel Principal

A imagem abaixo ilustra como fica o 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 esta 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 do ADC. Quando você clica em uma determinada escolha dentro da Navegação, isto exibirá a seção correspondente no lado direito da tela. Você 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 do ADC tem várias áreas dentro dele. Ao clicar no item Serviço, este se expandirá para mostrar as opções disponíveis.

Serviços IP

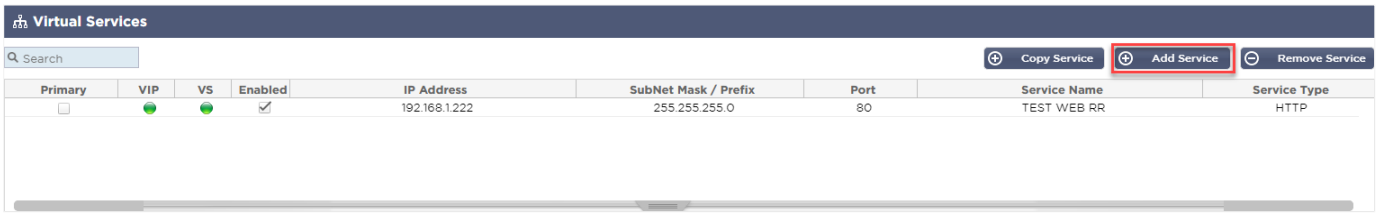
A seção Serviços IP do ADC permite adicionar, excluir e configurar os vários serviços IP virtuais necessários para seu caso particular de uso. As configurações e opções se encaixam nas seções abaixo. Estas seções estão no lado direito da tela de aplicação.

Serviços virtuais

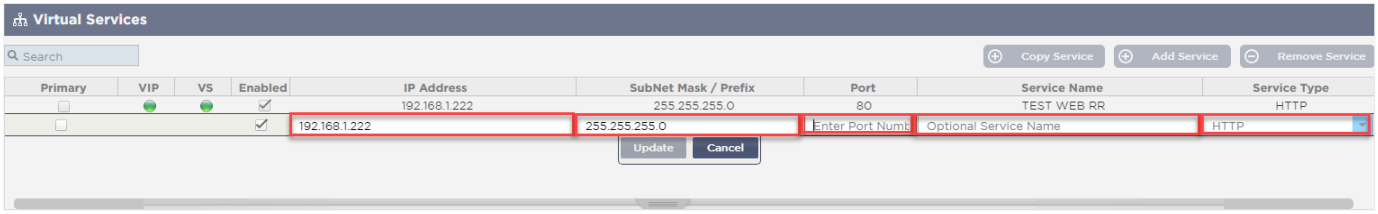
Um Serviço Virtual combina um IP Virtual (VIP) e uma porta TCP/UDP na qual o ADC ouve. O tráfego que chega ao IP do Serviço Virtual é redirecionado para um dos Servidores Reais associados a esse serviço. O endereço IP do Serviço Virtual não pode ser o mesmo que o endereço de gerenciamento do ADC, ou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

O ADC determina como o tráfego é redistribuído para os Servidores com base em uma política de balanceamento de carga definida dentro da guia Básico na seção Servidores Reais.

Criando um novo Serviço Virtual usando um novo VIP



- Clique no botão Adicionar Serviço Virtual como indicado acima.

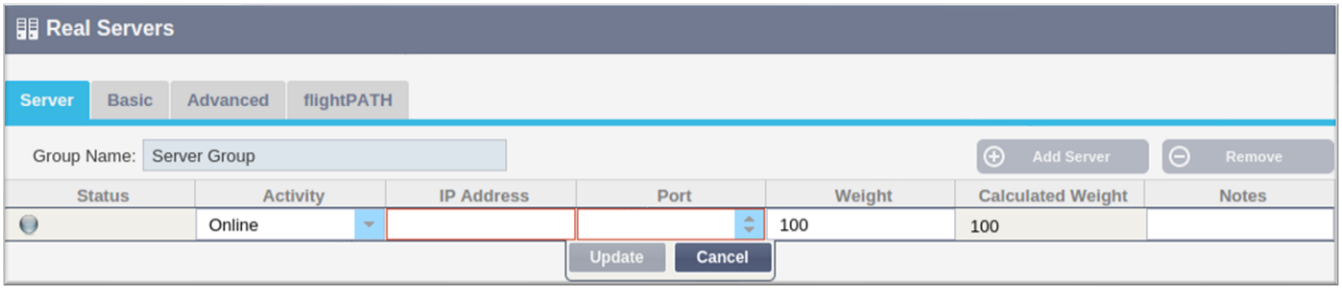


- Em seguida, você entrará no modo de **linha de edição.**
- Complete os quatro campos destacados para prosseguir, e depois clique no botão de atualização.

Favor usar a tecla TAB para navegar pelos campos.

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

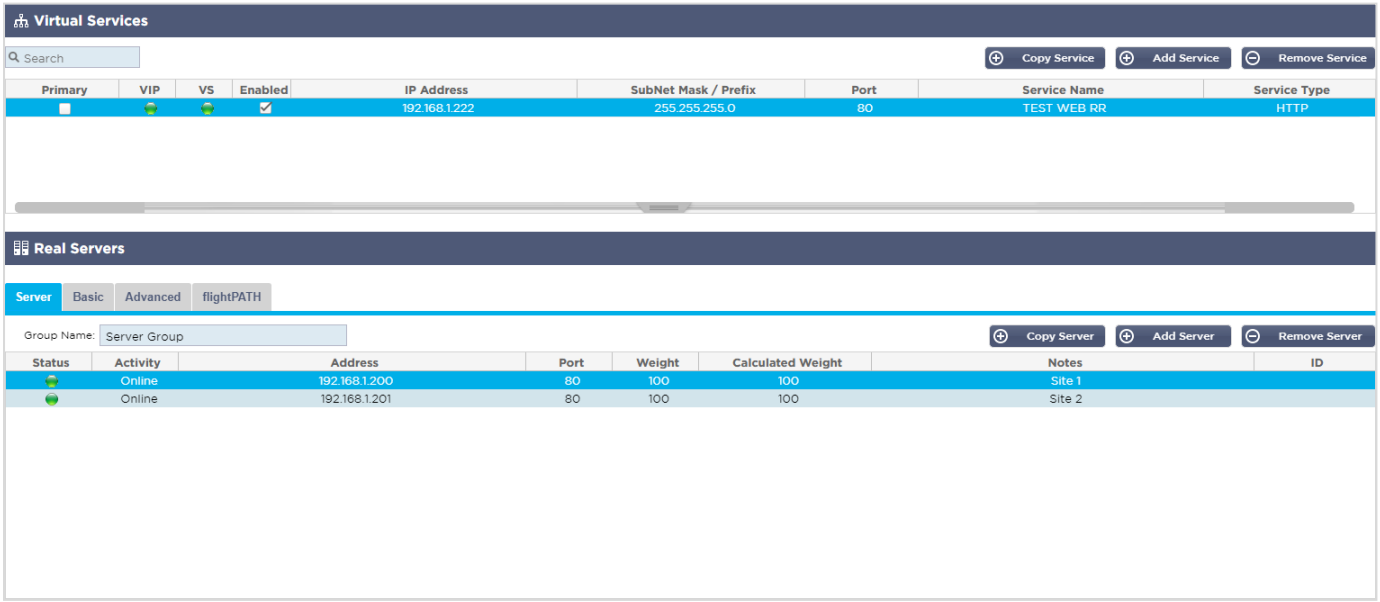
Agora você pode pressionar o botão Atualizar para salvar esta seção e pular automaticamente para a seção Servidor Real detalhada abaixo:



Campo	Descrição
Atividade	O campo de atividade pode ser usado para mostrar e alterar o status do servidor real balanceado de carga. Online - Denota que o servidor está ativo e recebendo solicitações balanceadas de carga Offline - O servidor está offline e não está recebendo solicitações Drenagem - O servidor foi colocado em modo de drenagem de modo que a persistência possa ser descarregada e o servidor movido para um estado offline sem afetar os usuários. Standby - O servidor foi colocado em estado de espera
Endereço IP	Este valor é o endereço IP do Servidor Real. Ele deve ser preciso e não deve ser um endereço DHCP.
Porto	A porta de acesso alvo no Servidor Real. Ao utilizar um proxy reverso, este pode ser diferente da porta de entrada especificada no VIP.
Ponderação	Esta configuração geralmente é configurada automaticamente pelo ADC. Você pode alterar isto se desejar alterar a ponderação de prioridade.

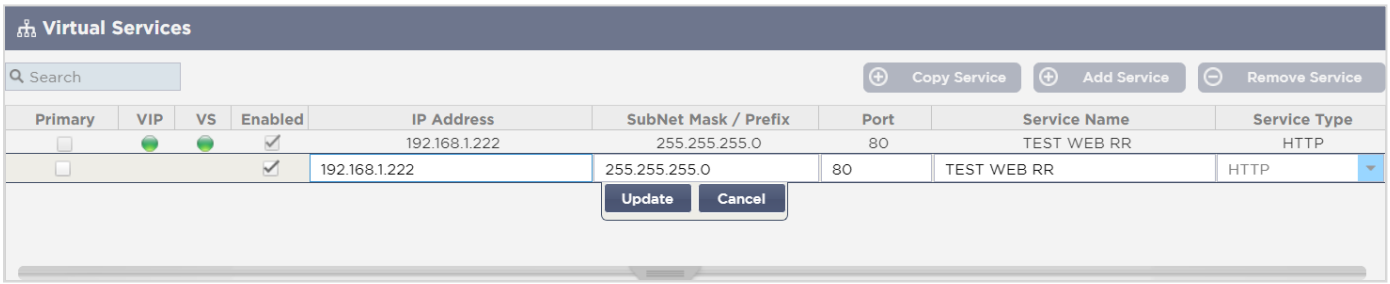
- Clique no botão Atualizar ou pressione Enter para salvar suas alterações
- A luz de status primeiro ficará cinza, seguida por verde caso o Server Health Check tenha sucesso. Ele ficará Vermelho se o Monitor do Servidor Real falhar.
- Um servidor que tenha uma luz vermelha de status não será balanceado na carga.

Exemplo de um serviço virtual completo

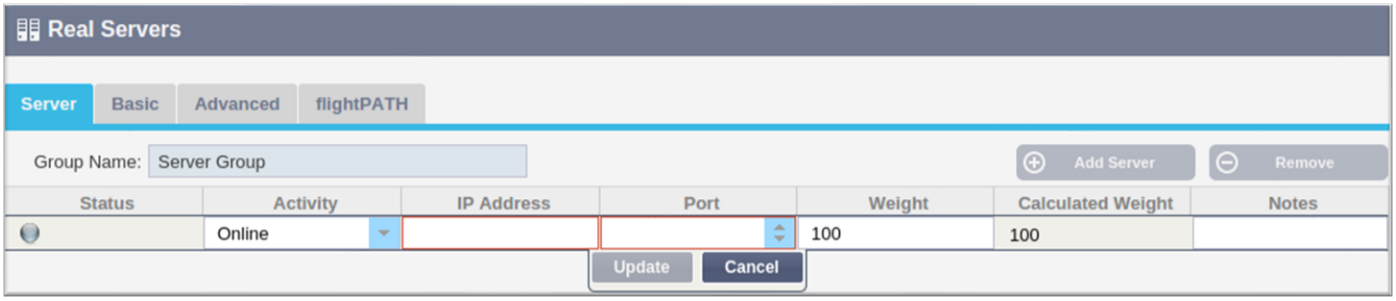


Criar um novo Serviço Virtual usando um VIP existente

- Destaque um serviço virtual que você deseja copiar
- Clique em Adicionar Serviço Virtual para entrar no modo de edição de linha



- O endereço IP e a máscara de sub-rede copiam automaticamente
- Digite o número da porta para seu serviço
- Digite um nome de serviço opcional
- Selecione um tipo de serviço
- Agora você pode 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 - isto significa que a carga será balanceada se ela passar pelo monitor de saúde padrão do TCP Connect. Esta configuração pode ser alterada posteriormente, se necessário.
- Digite um endereço IP do Servidor Real
- Digite um número de porta para o servidor real
- Digite um nome opcional para o Servidor Real

- Clique em Atualizar para salvar suas mudanças
- A luz de status primeiro ficará cinza, depois verde se o Server Health Check for bem sucedido. Ele ficará Vermelho se o Monitor do Servidor Real falhar.
- Um servidor que tenha uma luz vermelha de status não será balanceado na carga

Mudança do endereço IP de um serviço virtual

Você pode alterar o endereço IP de um Serviço Virtual ou VIP existente a qualquer momento.

- Destaque o Serviço Virtual cujo endereço IP você deseja mudar

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

- Altere o endereço IP para aquele que você 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 alteração do endereço IP de um Serviço Virtual mudará o endereço IP de todos os serviços associados com o VIP

Criando um novo serviço virtual usando o serviço de cópia

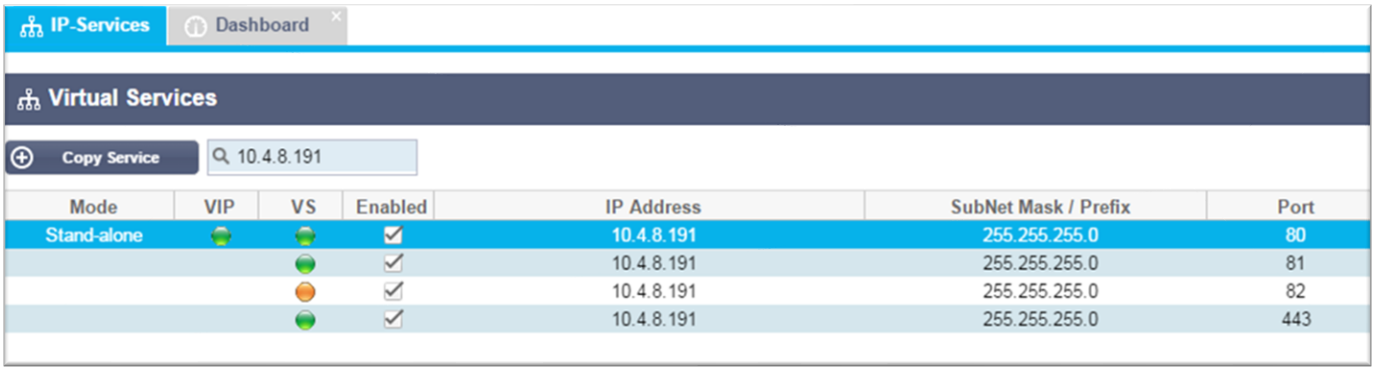
- O botão Copy Service copiará um serviço completo, incluindo todos os Servidores Reais, configurações básicas, configurações avançadas e regras flightPATH associadas a ele
- Destaque o serviço que você deseja duplicar e clique em Copy Service
- O editor de linha aparecerá com o cursor piscando na coluna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

Não se esqueça de editar cada guia se você alterar uma configuração como uma política de balanceamento de carga, o monitor do Servidor Real, ou remover uma regra do FlightPATH.

Filtragem dos dados exibidos

Procura de um termo específico

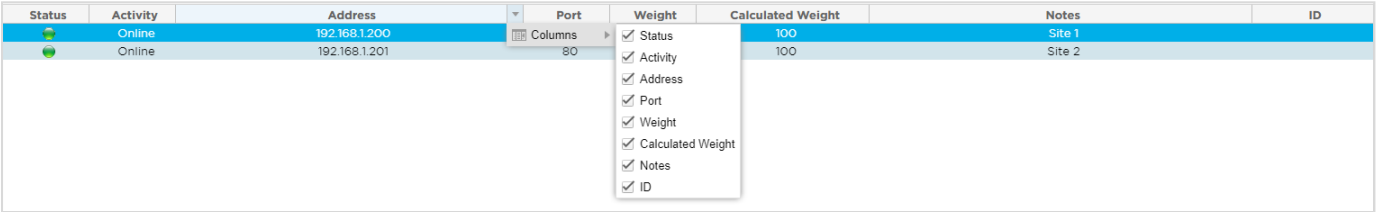
A caixa Pesquisar permite pesquisar a tabela usando qualquer valor, como os octetos do endereço IP ou o nome do serviço.



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

Seleção da visibilidade da coluna

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

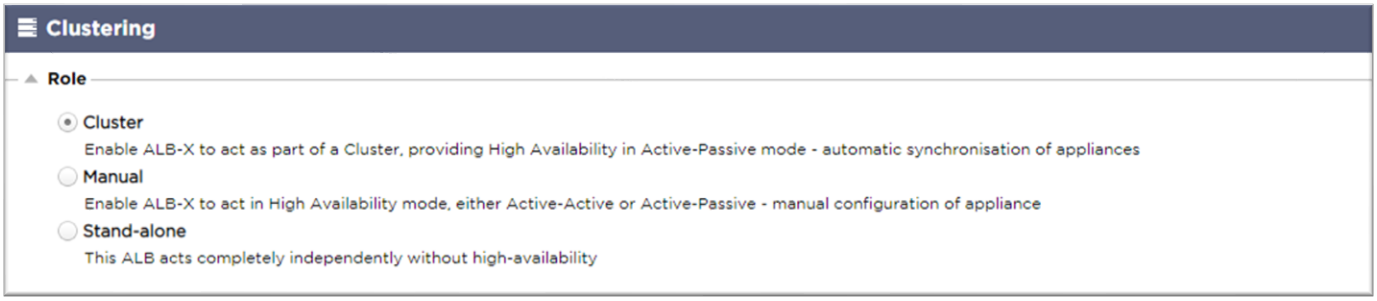


- Passe o mouse sobre qualquer uma das colunas
- Você verá uma pequena seta aparecer no lado direito da coluna
- Clicando nas caixas de seleção, selecione as colunas que você deseja ver no painel de instrumentos.

Entendendo as colunas de Serviços Virtuais

Primário/Modo

A coluna Principal/Modo indica a função de alta disponibilidade selecionada para o VIP atual. Use as opções disponíveis em Sistema > Clustering para configurar esta 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 você tiver um par de dispositivos ADC HA 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 exclusivo que é assinalável para Ativo ou não assinalável para Passivo.
Stand-Alone	O ADC está agindo como um dispositivo independente e não está no modo High Availability (Alta Disponibilidade). Como tal, a coluna primária indicará Independente.

VIP

Esta coluna fornece feedback visual sobre o status 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 segurando para um "primário".
●	O serviço precisa de atenção. Esta indicação pode resultar de um servidor real falhar em uma verificação do monitor de saúde ou ter sido alterado manualmente para fora de linha. 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
●	Encontrar o status
●	IPs virtuais não licenciados ou licenciados excedidos

Habilitado

O padrão para esta opção é Ativado, e a caixa de seleção mostra como assinalado. Você 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. Este 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".

Máscara de sub-rede/Prefixo

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

Porto

Adicione o número da porta associada ao seu serviço. A porta pode ser um número de porta TCP ou UDP. Exemplo TCP "80" para Tráfego Web e TCP "443" para Tráfego Web Seguro.

Nome do serviço

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

Tipo de serviço

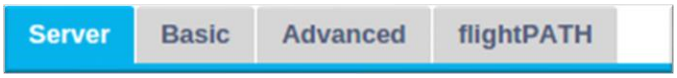
Observe que com todos os tipos de serviço de "Camada 4", o ADC não interagirá ou modificará o fluxo de dados, portanto, o flightPATH não está disponível com os tipos de serviço de Camada 4. Os serviços de Camada 4 simplesmente balanceiam o tráfego de acordo com a política de balanceamento de carga:

Tipo de serviço	Porto/Protocolo	Camada de serviço	Comentário
Camada 4 TCP	Qualquer porta 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 TCP de 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 TCP/UDP	Qualquer porta TCP ou UDP	Camada 4	É ideal se seu serviço tem um protocolo primário como o UDP, mas voltará 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	TCP/UDP	Camada 4	Usado para carregar servidores DNS de equilíbrio.
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 simples de transferência de correio	Camada 4	Usar ao equilibrar a carga dos servidores de correio
POP3	Protocolo dos Correios	Camada 4	Usar ao equilibrar a carga dos servidores de correio
IMAP	Protocolo de acesso a mensagens na Internet	Camada 4	Usar ao equilibrar a carga dos servidores de correio
RDP	Protocolo de Desktop Remoto	Camada 4	Uso em servidores de Serviços Terminais de balanceamento de carga
RPC	Chamada de procedimento remoto	Camada 4	Usar quando sistemas de balanceamento de carga usando chamadas RPC
RPC/ADS	Troca 2010 Static RPC para serviço de catálogo de endereços	Camada 4	Uso em servidores de troca de balanceamento de carga
RPC/CA/PF	Troca 2010 RPC Estático para Acesso ao Cliente e Pastas Públicas	Camada 4	Uso em servidores de troca de balanceamento de carga
DICOM	Imagens e Comunicações Digitais em Medicina	Camada 4	Uso quando servidores de balanceamento de carga usando protocolos DICOM

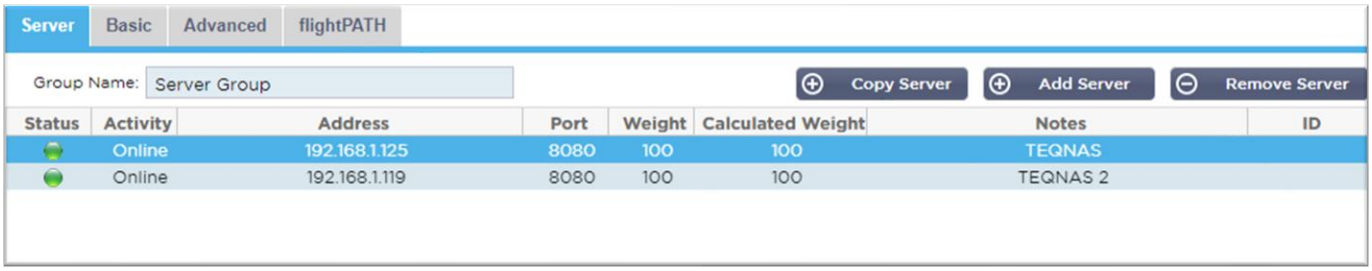
Servidores reais

Há várias guias na seção Servidores reais do painel de instrumentos: Server, Basic, Advanced, e flightPATH.



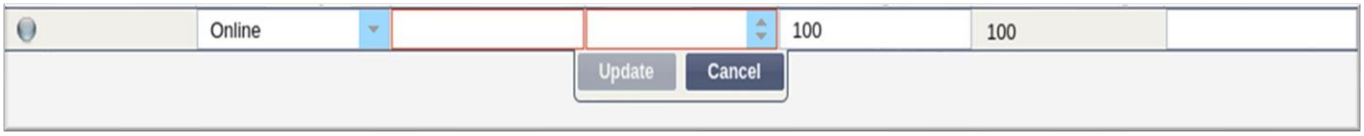
Servidor

A aba Servidor contém as definições dos verdadeiros servidores back-end emparelhados com o Serviço Virtual atualmente selecionado. É necessário adicionar pelo menos um servidor à seção Servidores Reais.



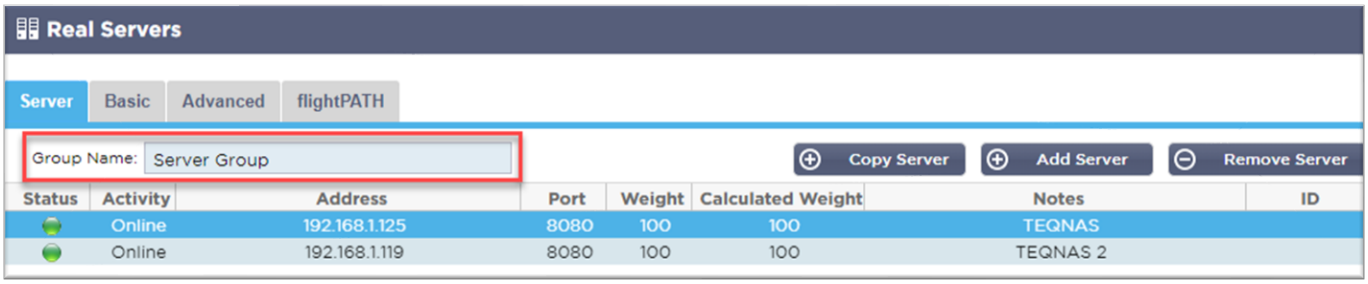
Adicionar Servidor

- Selecione o VIP apropriado que você tenha definido previamente.
- Clique em Adicionar Servidor
- 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 que seu Serviço Virtual, em qualquer rede local anexada diretamente ou em qualquer rede que seu ADC possa rotear. Exemplo "10.1.1.1".
- Tab na coluna Porta e digite o número da porta TCP/UDP de seu servidor. O número da porta pode ser o mesmo que o número da porta do Serviço Virtual ou outro número de porta para Conectividade Proxy Reversa. O ADC irá traduzir automaticamente para este número.
- Tab na seção de Notas para adicionar qualquer detalhe relevante para o servidor. Exemplo: "Servidor Web IIS 1".

Nome do grupo



Quando você tiver adicionado nos servidores que compõem o conjunto balanceado de carga, você também pode anexar um Nome de Grupo. Uma vez editado este campo, o conteúdo é salvo sem a necessidade de pressionar o botão Atualizar.

Luzes de status de servidor real

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

LED	Significado
●	Conectado
○	Não monitorado
●	Drenagem

●	Offline
●	Aguarde
●	Não Conectado
●	Status de busca
●	Servidores reais não licenciados ou licenciados excedidos

Atividade

Você pode mudar a atividade de um servidor real a qualquer momento usando o menu suspenso. Para fazer isso, clique duas vezes em uma linha de Servidor Real para colocá-la no modo de edição.

Opção	Descrição
Online	Todos os Servidores Reais designados Online receberão tráfego de acordo com a política de balanceamento de carga definida dentro da guia Básica.
Drenagem	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 processo. Uma vez que as conexões existentes tenham fechado naturalmente, os Servidores Reais ficarão offline, e a luz de Status será azul sólido. Você também pode visualizar estas conexões navegando para a seção Navegação > Monitor > Status.
Offline	Todos os Servidores Reais configurados como Offline serão imediatamente desconectados e não receberão nenhum tráfego.
Aguarde	Todos os Servidores Reais configurados como Standby permanecerão offline até que **TODOS** os servidores do grupo Online falhem suas verificações do Monitor de Saúde do Servidor. O tráfego é recebido pelo grupo Standby de acordo com a política de balanceamento de carga quando isto acontece. Se um servidor do grupo Online passar na verificação do Monitor de Saúde do Servidor, este servidor Online receberá todo o tráfego, e o grupo Standby deixará de receber tráfego.

Endereço IP

Este campo é o endereço IP de 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 tráfego Web.

Peso

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

O peso padrão para um Servidor Real é 100, e você pode inserir 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 Conexões Mínimas, e existem 200 conexões totais de clientes;

- O Server 1 terá 100 conexões simultâneas
- O Server 2 terá 50 conexões simultâneas
- O Server 3 terá 50 conexões simultâneas

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

Se acreditarmos que a política de balanceamento de carga mais rápida utiliza o menor tempo possível para obter uma resposta, o ajuste dos pesos altera o viés de forma semelhante ao das Conexões 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 balanceamento de carga.

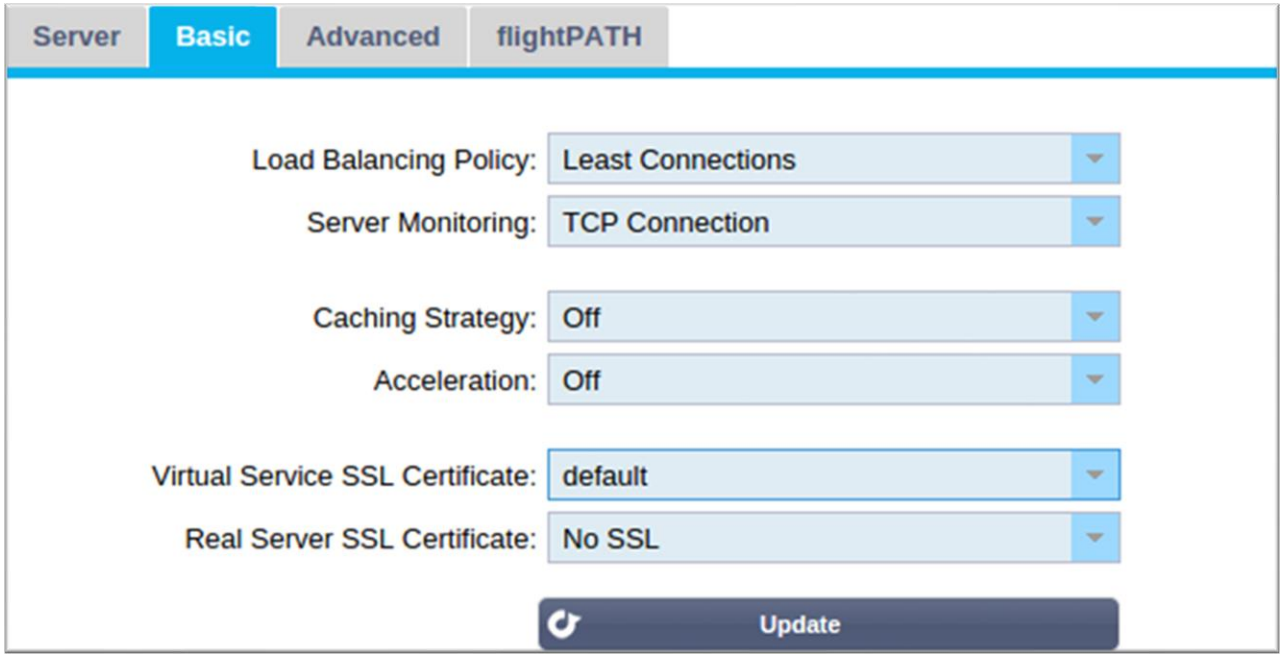
Notas

Digite qualquer nota específica útil para descrever a entrada definida no campo Notas. Exemplo "IIS Server1 - London DC".

ID

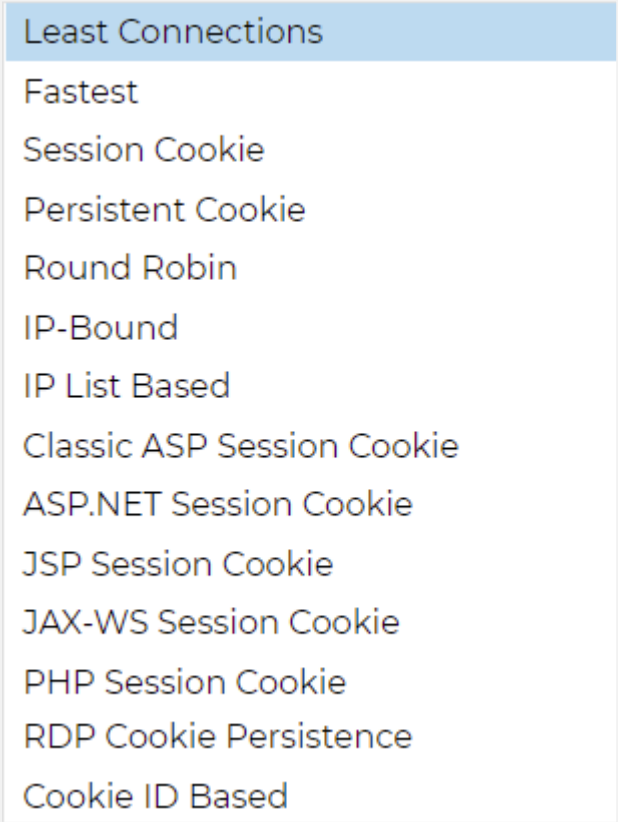
O campo ID é usado dentro da Política de balanceamento de carga do Cookie ID. O número de identificação colocado aqui é usado para identificar

Básico



Política de balanceamento de carga

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



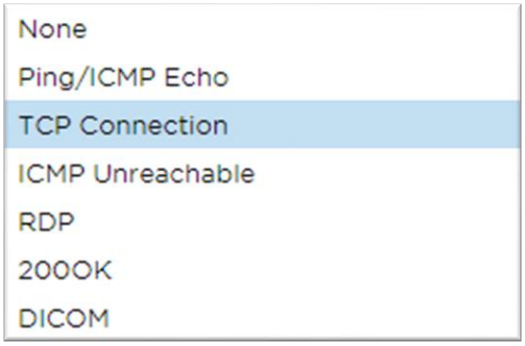
Opção	**Descrição**
Mais rápido	A política de balanceamento de carga mais rápida calcula automaticamente o tempo de resposta para todas as solicitações por servidor suavizadas ao longo do tempo. A coluna Peso Calculado contém o valor calculado automaticamente.

	A entrada manual só é possível quando se utiliza esta política de balanceamento de carga.
Round Robin	Round Robin é comumente usado em firewalls e equilibradores de carga básicos e é o método mais simples. Cada Real Server recebe um novo pedido em seqüência. Este método só é adequado quando você precisa carregar as solicitações de balanceamento de carga para servidores de forma uniforme; um exemplo seria servidores web look-up. Entretanto, quando você precisa carregar o equilíbrio baseado na carga da aplicação ou na carga do servidor, ou mesmo garantir que você use o mesmo servidor para a sessão, o método Round Robin é inadequado.
Mínimas conexões	O equilibrador de carga manterá um registro do número de conexões atuais para cada servidor real. O Servidor Real com a menor quantidade de conexões recebe o novo pedido subseqüente.
Limite IP Afinidade/Persistência de Camada 3 Sessões	Neste modo, o endereço IP do cliente forma a base para selecionar qual Servidor Real irá receber a solicitação. Esta ação proporciona persistência. Os protocolos HTTP e Layer 4 podem usar este modo. Este método é útil para redes internas onde a topologia da rede é conhecida, e você pode ter certeza de que não há "super proxies" upstream. Com a Camada 4 e proxies, todas as solicitações podem parecer como se viessem 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 proxies.
Baseado na lista IP Afinidade/Persistência de Camada 3 Sessões	A conexão com o Servidor Real inicia usando "Menos conexões" então, a afinidade da sessão é alcançada com base no endereço IP do cliente. Uma lista é mantida por padrão por 2 horas, mas isto pode ser alterado usando um jetPACK.
Sessão Cookie Afinidade/Persistência de Camada 7 Sessões	Este modo é o método de persistência mais popular para o balanceamento de carga HTTP. Neste modo, o ADC usa o balanceamento de carga baseado em lista 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. Este cookie é usado para persistência quando o cliente precisa ir ao mesmo servidor back-end a cada vez. O cookie expira quando a sessão é encerrada.
Cookie Persistente Afinidade/Persistência de Camada 7 Sessões	O modo de balanceamento de carga baseado na lista IP é usado para cada primeira solicitação. 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. Este cookie é usado para persistência quando o cliente deve ir ao mesmo servidor back-end a cada vez. O cookie expirará após 2 horas, e a conexão será balanceada de acordo com um algoritmo baseado em lista IP. Este 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 esta opção selecionada, o ADC manterá a persistência da sessão para o mesmo servidor se um cookie ASP for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie ASP, ele será balanceado de carga usando o algoritmo de Mínimas Conexões.
Cookie de sessão - Cookie de sessão ASP.NET	Este modo se aplica ao **ASP.net.** Com este modo selecionado, o ADC manterá a persistência da sessão no mesmo servidor se um cookie ASP.NET for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie ASP, ele será balanceado de carga usando o algoritmo de Mínimas Conexões.
Cookie de Sessão - Cookie de Sessão JSP	Java Server Pages (JSP) é uma tecnologia do lado do servidor Oracle. Com este modo selecionado, o ADC manterá a persistência da sessão para o mesmo servidor se um cookie JSP for detectado e encontrado em sua lista de cookies conhecidos. Na detecção de um novo cookie JSP, ele será balanceado de carga usando o algoritmo de Mínimas Conexões.

Cookie de sessão - Cookie de sessão JAX-WS	Java web services (JAX-WS) é uma tecnologia do lado do servidor Oracle. Com este modo selecionado, o ADC manterá a persistência da sessão para o 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 balanceado 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 este modo selecionado, o ADC manterá a persistência da sessão para o mesmo servidor quando um cookie PHP for detectado.
Sessão Cookie - RDP Cookie Persistência	Este método de balanceamento de carga utiliza o RDP Cookie criado pela Microsoft baseado no nome de usuário/domínio para fornecer persistência a um servidor. A vantagem deste 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 parecido com "PhpCookieBased" e outros métodos de balanceamento de carga, mas usando CookieIDBased e cookie RegEx h=[^;]+ Este método usará o valor definido no campo de notas do Real Server "ID=X;" como o valor do cookie para identificar o servidor. Isto, portanto, significa que é uma metodologia similar ao CookieListBased, mas usa um nome de cookie diferente e armazena um valor único de cookie, não o IP codificado, mas o ID do Servidor Real (lido em tempo de carga). O valor padrão é CookieIDName="h"; entretanto, se houver um valor de sobreposição na configuração avançada do servidor virtual, use-o em seu lugar. **NOTA**: Nós substituímos a expressão cookie acima para substituir h= pelo novo valor, se este valor for definido. O último bit 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 (delegar).
Lista IP compartilhada	Este tipo de serviço só está disponível quando o Modo de Conectividade está configurado para Gateway ou Direct Server Return. Ele foi adicionado principalmente para suporte com balanceamento de carga VMware.

Monitoramento de servidores

Seu ADC contém seis métodos padrão de Monitoramento de Servidor Real listados abaixo.



Escolha o método de monitoramento que você 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 você não tiver certeza de qual monitor escolher, a conexão TCP padrão é um excelente lugar para começar.

Você pode escolher vários monitores clicando em cada monitor que desejar aplicar ao serviço, por sua vez. Os monitores selecionados são executados na ordem em que você 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:

Events

Status	Date	Message
ATTENTION	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 unreachable - Echo=OK Connect=OK 200OK=FAIL
OK	10:22 26 Feb 2016	10.4.8.131:89 Real Server 172.17.0.2:88 contacted - Echo=OK Connect=OK 200OK=OK

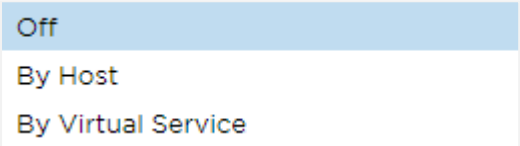
Podemos ver que a Camada 3 Ping e a Camada 4 TCP Connect tiveram sucesso se olharmos para a linha superior, mas a Camada 7 200OK falhou. Estes resultados de monitoramento fornecem informações suficientes para indicar que o roteamento está OK e que há um serviço rodando na porta relevante, mas o site não está respondendo corretamente à página solicitada. Agora é hora de olhar o webserver e a seção Library > Real Server Monitor para ver os detalhes do monitor que falhou.

Opção	**Descrição**
Nenhum	Neste modo, o Real Server não é monitorado e está sempre funcionando corretamente. A configuração Nenhum é útil para situações em que o monitoramento perturba um servidor e para serviços que não devem participar da ação de fail-over do ADC. É uma rota para hospedar sistemas não confiáveis ou legados que não são primários para as operações H/A. Use este método de monitoramento com qualquer tipo de serviço.
Ping/ICMP Echo	Neste modo, o ADC envia um pedido de eco ICMP para o IP do servidor de conteúdo. Se uma resposta de eco válida for recebida, o ADC considera o Servidor Real ativo e em funcionamento, e o fluxo de tráfego para o servidor continua. Ele também manterá o serviço disponível em um par H/A. Este método de monitoramento é utilizável com qualquer tipo de serviço.
Conexão TCP	Uma conexão TCP é feita ao Servidor Real e imediatamente quebrada sem o envio de quaisquer dados neste modo. Se a conexão for bem sucedida, o ADC considera que o Servidor Real está em funcionamento. Este método de monitoramento é utilizável com qualquer tipo de serviço, e os serviços UDP não são apropriados atualmente para o monitoramento da conexão TCP.
ICMP Inacessível	O ADC enviará um cheque de saúde UDP ao servidor e marcará o Servidor Real como indisponível se ele receber uma mensagem inalcançável de porta ICMP. Este método pode ser útil quando você precisa verificar se uma porta de serviço UDP está disponível em um servidor, tal como a porta DNS 53.
RDP	Neste modo, uma conexão TCP é inicializada como explicado no ICMP Unreachable method (método inalcançável). Após a inicialização da conexão, uma conexão RDP de Camada 7 é solicitada. Se a conexão for confirmada, o ADC considera que o Servidor Real está em funcionamento. Este método de monitoramento é utilizável com qualquer servidor de terminal Microsoft.
200 OK	Neste método, uma conexão TCP se inicializa no Servidor Real. 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". O ADC considera que o Servidor Real está funcionando se o código de resposta "200 OK" for recebido. Se o ADC não receber um código de resposta "200 OK" por qualquer motivo, incluindo timeouts, falha na conexão e outros motivos, o ADC marca o Servidor Real indisponível. Este método de monitoramento só é válido para uso com tipos de serviço HTTP e HTTP acelerado. Se um tipo de serviço Layer 4 for usado para um servidor HTTP, ele é utilizável se o SSL não estiver em uso no Servidor Real ou se for tratado apropriadamente pelo recurso "Conteúdo SSL".
DICOM	Uma conexão TCP é inicializada ao Servidor Real no modo DICOM, e uma "Solicitação de Associado" Echoscu é feita ao Servidor Real na conexão. Uma conversa que inclui uma "Associate Accept" do servidor de conteúdo, uma transferência de uma pequena quantidade de dados seguida por uma "Release Request", e depois uma "Release Response" conclui com sucesso o monitor. Se o monitor não for concluído com sucesso, então o Servidor Real é considerado como desligado por qualquer motivo.

Definido pelo usuário	Qualquer monitor configurado na seção de Monitoramento do Servidor Real aparecerá na lista.

Estratégia de Caching

Por padrão, a Estratégia de Caching é desativada e definida como Desligada. Se seu tipo de serviço é HTTP, então você pode aplicar dois tipos de Estratégia de Cache.



Consulte a página Configurar Cache para configurar configurações de cache detalhadas. 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 Host	O cache por anfitrião é baseado na aplicação por nome de anfitrião. Um Cache separado existirá para cada domínio/nome de host. Este modo é ideal para servidores web que podem servir múltiplos websites, dependendo do domínio.
Por Serviço Virtual	O cache por serviço virtual está disponível quando você escolhe esta opção. Apenas um Cache existirá para todos os domínios/nomes de domínios que passarem pelo serviço virtual. Esta opção é um cenário especializado para uso com vários clones de um único site.

Aceleração

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

Nota: Se o objeto for armazenável, o ADC armazenará uma versão compactada e a servirá estaticamente (a partir da memória) até que o conteúdo expire e seja re-validado.

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

Por padrão, a configuração é Sem SSL. Se seu tipo de serviço for "HTTP" ou "Layer4 TCP", você pode selecionar um certificado no menu suspenso para aplicar ao Serviço Virtual. Os certificados que tiverem sido criados ou importados aparecerão nesta lista. Você pode destacar vários certificados para aplicar a um serviço. Esta operação ativará automaticamente a extensão SNI para permitir um certificado baseado no "Nome de Domínio" solicitado pelo cliente.

Indicação do nome do servidor

Esta 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. Esta configuração permite que o ADC apresente vários certificados no mesmo endereço IP virtual e porta TCP.

No SSL
All
default
AnyUseCert

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

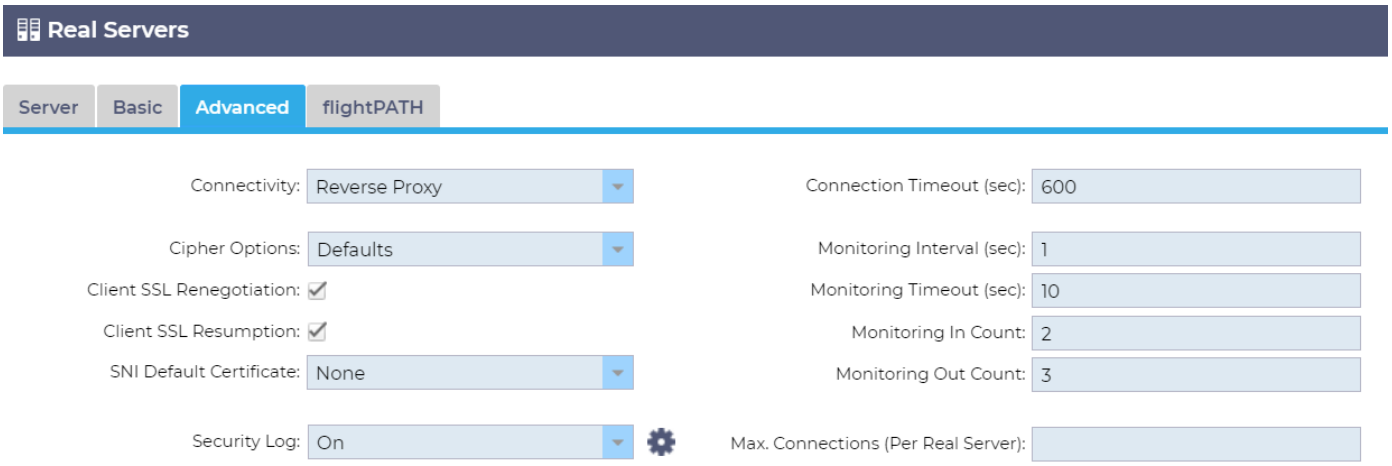
Certificado SSL do Real Server (Criptografia entre o ADC e o Real Server)

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

No SSL
Any
SNI
default
AnyUseCert

Opção	**Descrição**
Sem SSL	O tráfego do ADC para o Servidor Real 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 um cliente e aceitará qualquer certificado que o Real Server apresentar. O tráfego do ADC para o Servidor Real é criptografado quando esta 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 um 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 esta opção para habilitar o SNI no lado do servidor.
AnyUseCert	Quaisquer certificados que você tenha gerado ou importado para o ADC aparecem aqui.

Avançado



Conectividade

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

Opção	**Descrição**
Proxy Reversa	O Proxy Reverso é o valor padrão e funciona em Layer7 com compressão e cache. E na Camada4 sem caching ou compressão. Neste modo, seu ADC atua 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 que o servidor atrás do equilibrador de carga responda diretamente ao cliente contornando o ADC na resposta. O DSR é adequado apenas para uso com balanceamento de carga de Camada 4. Portanto, o Caching e a Compressão não estão disponíveis com esta opção escolhida. **Este modo só pode ser usado com os tipos de serviço TCP, UDP e TCP/UDP.** O balanceamento de carga da camada 7 não funciona com este DSR. Além disso, não há nenhum outro suporte de persistência além do baseado na lista IP. O balanceamento de carga SSL/TLS com este método não é o ideal, pois o suporte de persistência IP Source é o único tipo disponível. O DSR também requer que sejam feitas mudanças no Real Server. Consulte a seção Mudanças no Servidor Real.
Porta de entrada	O modo Gateway permite encaminhar todo o tráfego através do ADC, permitindo que os Servidores Reais sejam roteados através do ADC para outras redes através das máquinas virtuais ou interfaces de hardware do ADC. Usar o dispositivo como um dispositivo gateway para Servidores Reais é ideal quando executado em modo multi-interface. O balanceamento de carga de camada 7 com este método não funciona, pois não há outro suporte de persistência além do baseado na lista IP. Este método requer que o Real Server defina seu gateway padrão para o endereço de interface local do ADC (eth0, eth1, etc.). Favor consultar a seção Mudanças no Servidor Real. ***Favor observar que o modo Gateway não suporta failover em um ambiente de cluster.***

Opções de cifras

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

Renegociação SSL do cliente

Assinale esta caixa se você deseja permitir a renegociação SSL iniciada pelo cliente. Desabilite a renegociação SSL do cliente para prevenir qualquer possível ataque DDOS contra a camada SSL, desmarcando esta opção.

Retorno do cliente SSL

Marque esta caixa se desejar ativar as sessões do Servidor de Retorno SSL adicionadas ao cache de sessões. Quando um cliente propõe a reutilização de uma sessão, o servidor tentará reutilizar a sessão, se encontrada. Se o Resumption não for verificado, não ocorrerá cache de sessão para o cliente ou servidor.

Certificado padrão SNI

Durante uma conexão SSL com o SNI do lado do cliente habilitado, se o domínio solicitado não corresponder a nenhum dos certificados atribuídos ao serviço, o ADC apresentará o Certificado Padrão do SNI. A configuração padrão para isto é Nenhuma, o que efetivamente deixaria a conexão de lado caso não houvesse uma correspondência exata. Escolha qualquer um dos certificados instalados a partir do dropdown para apresentar caso um certificado SSL coincida exatamente.

Diário de Segurança

'On' é o valor padrão e é por serviço, permitindo o serviço de registro de informações de autenticação para os logs do W3C. Clicando no ícone Cog você será levado à página Sistema > Logging, onde você pode verificar as configurações do log do W3C.

Tempo limite de conexão

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

Configurações de monitoramento

Estas configurações estão relacionadas com os Monitores de Servidor Real na guia Básico. Há entradas globais na configuração para contar o número de monitores bem-sucedidos ou falhos 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 aguarda que um servidor responda a uma solicitação de conexão. O valor padrão é 2s. Aumente este valor para servidores ocupados.

Monitoramento em Contagem

O valor padrão para esta configuração é 2. O valor de 2 indica que o Real Server deve passar por duas verificações bem sucedidas do monitor de saúde antes de entrar on-line. Aumentar este valor aumentará a probabilidade de que o servidor possa servir o tráfego, mas levará mais tempo para entrar em serviço, dependendo do intervalo. Diminuir este valor colocará seu servidor em serviço mais cedo.

Monitorando a contagem

O valor padrão para esta 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 este valor resultará em um serviço melhor e mais confiável às custas do tempo que o ADC leva para interromper o envio de tráfego para este servidor.

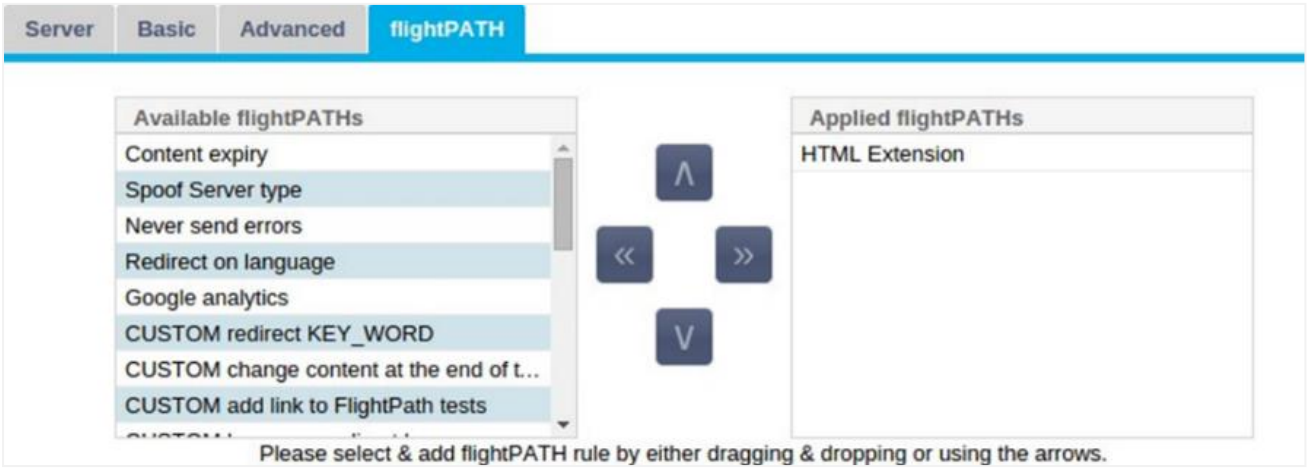
Mudar para falha de funcionamento desligado

Quando isto é verificado, os Servidores Reais que falham em seu exame de saúde são colocados offline e só podem ser configurados online manualmente.

Máx. Conexões

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

flightPATH



O 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 console de entrada de scripts. Ao invés disso, ele usa uma GUI para selecionar os diferentes parâmetros, condições e ações a serem executadas para alcançar o que eles precisam. Estas características tornam o flightPATH extremamente poderoso e permitem aos administradores de rede manipular o tráfego HTTPS de formas altamente eficazes.

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

Você 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 superior executada primeiro. Para alterar a ordem de execução, destacar a regra e mover-se para cima e para baixo usando as setas.

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

Você pode adicionar, remover e editar as regras flightPATH na seção Configurar flightPATH deste guia.

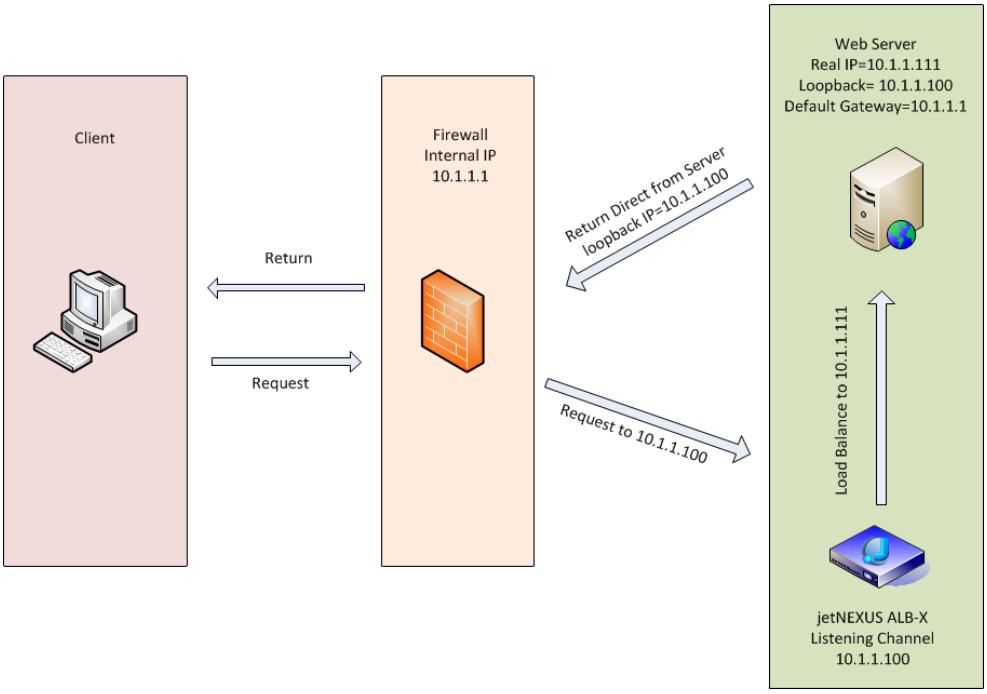
Mudanças reais no servidor para retorno direto do servidor

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 é adequado apenas para uso com balanceamento de carga de Camada 4. Caching e Compressão não estão disponíveis quando ativado.

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

Como funciona

- Cliente envia um pedido para o jetNEXUS ALB-X
- Solicitação recebida pela edgeNEXUS
- Pedido roteado para servidores de conteúdo
- Resposta enviada diretamente ao cliente sem passar pela 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

Windows

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

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

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

- Editar "/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 encaminhar todo o tráfego através do ADC, e isto permite que o tráfego proveniente dos servidores de conteúdo seja encaminhado através do ADC para outras redes através das interfaces da unidade do ADC. O uso do dispositivo como um dispositivo de gateway para servidores de conteúdo deve ser usado quando executado em modo multi-interface.

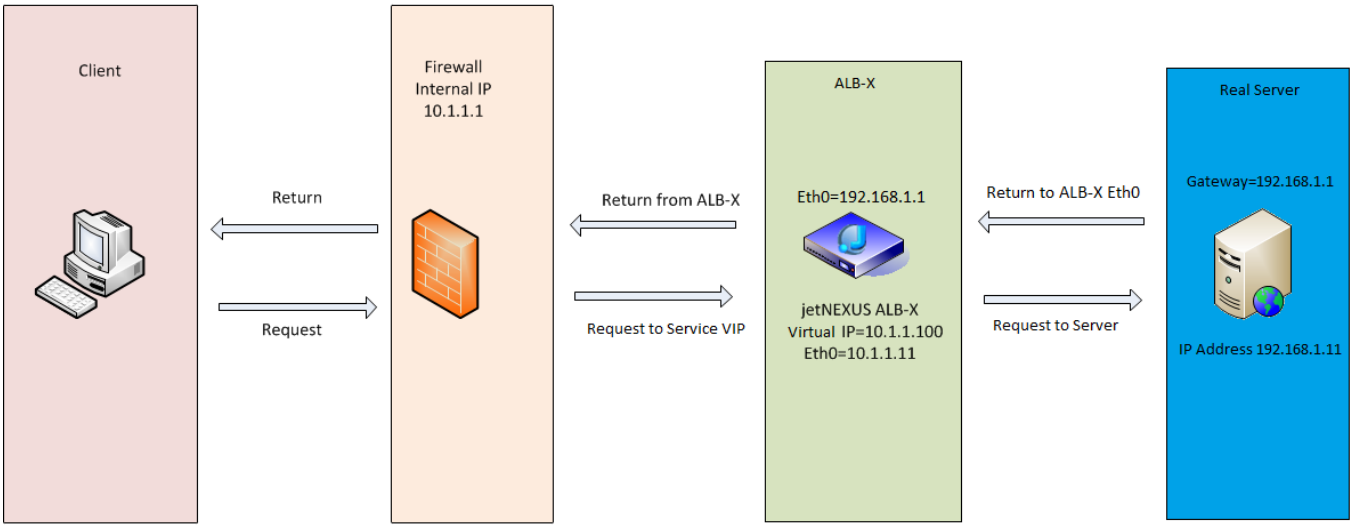
Como funciona

- O cliente envia um pedido para o jetNEXUS ALB-X
- Uma solicitação é recebida pela edgeNEXUS
- Solicitação enviada aos servidores de conteúdo
- Resposta enviada à edgeNEXUS
- ADC encaminha a resposta para o cliente

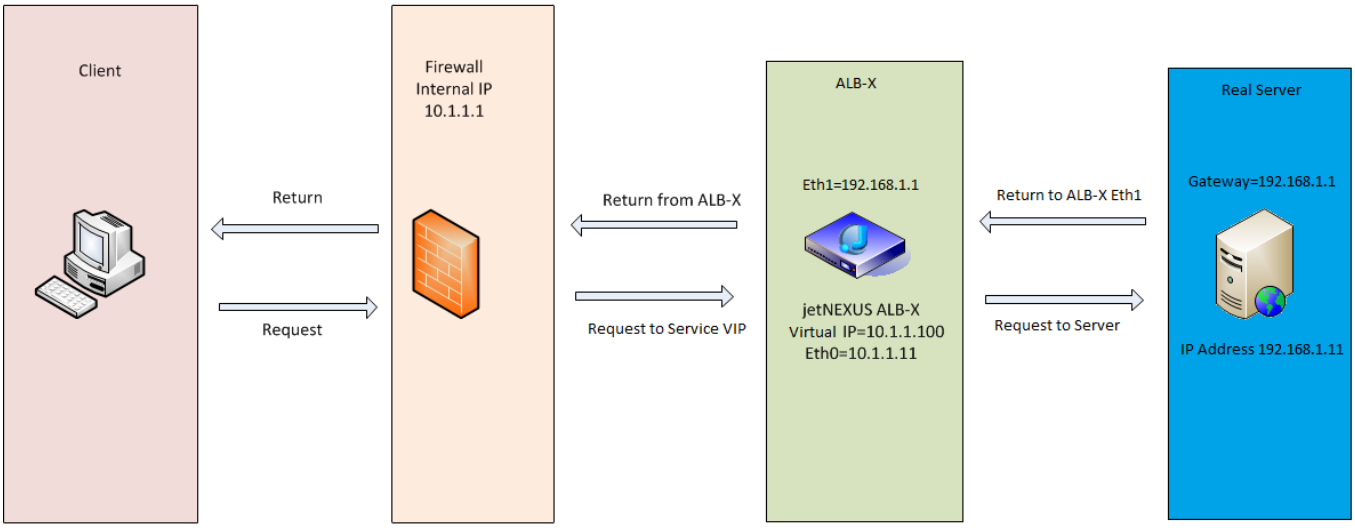
Configuração do Servidor de Conteúdo Requerido

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

Exemplo de braço único



Exemplo de braço duplo



Biblioteca

Suplementos

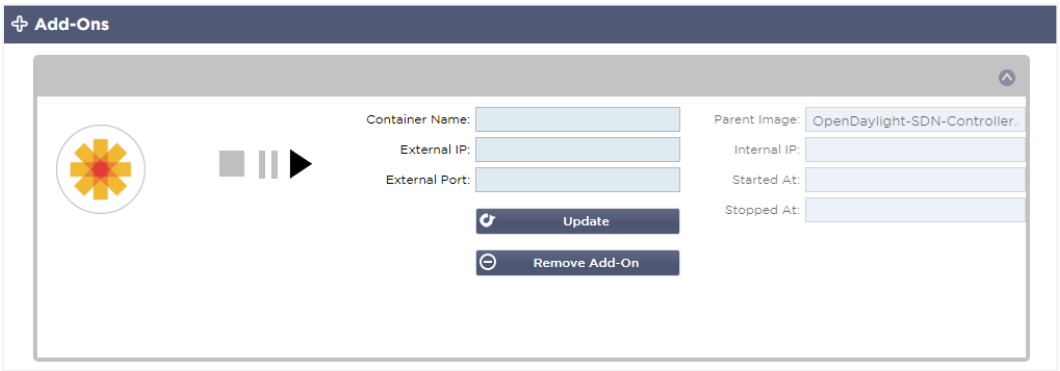
Os complementos são recipientes baseados em Docker que podem funcionar em modo isolado dentro do ADC. Exemplos de complementos podem ser um firewall de aplicação ou até mesmo uma micro instância do próprio ADC.

Apps

A seção Apps dentro dos Add-Ons detalha os Apps que você comprou, baixou e implantou.

Se não houver nenhum aplicativo presente, esta seção exibirá uma mensagem solicitando que você prossiga para a seção de aplicativos e faça o download e implante de um aplicativo.

Uma vez implantado um App, ele aparecerá na área Apps.



Compra de um Add-on

Para comprar um App, você precisa se registrar na App Store. A compra é feita usando o próprio ADC. Você encontrará

Navegue até a Biblioteca > Página de aplicativos do painel do ADC.

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

Se você estiver fazendo isso a partir do painel do ADC, por favor, selecione apenas 1 item. Você pode ser proprietário de vários conjuntos do ADC, e as aplicações precisam ser associadas ao ADC no qual elas são implantadas.

Se você acessar a App Store através de seu desktop e navegador, você pode fazer o download de quantas quiser. Por exemplo, quatro instâncias do WAF ou GSLB. Elas aparecerão na área de Aplicações Compradas do seu ADC para que você possa baixá-las.

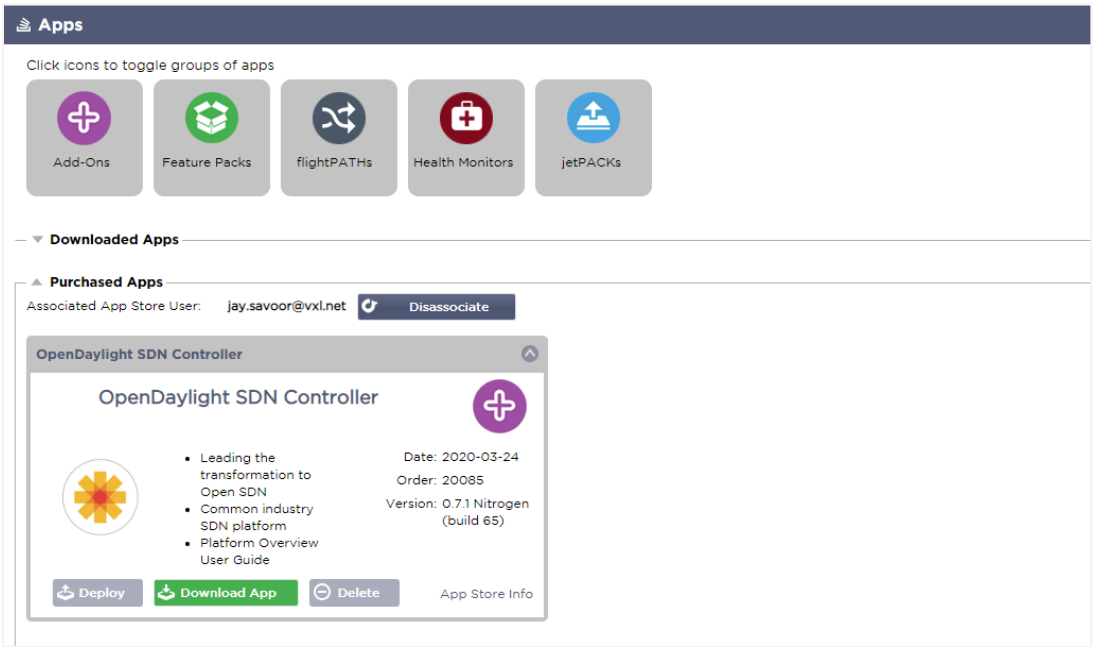
Os aplicativos associados aos ADCs que você possui e que foram registrados.

Quando você optar por baixar um Aplicativo, será solicitado o ID da Máquina, após o qual o Aplicativo é criptografado e vinculado ao ID da Máquina da ADC.

Os links para a App Store são:

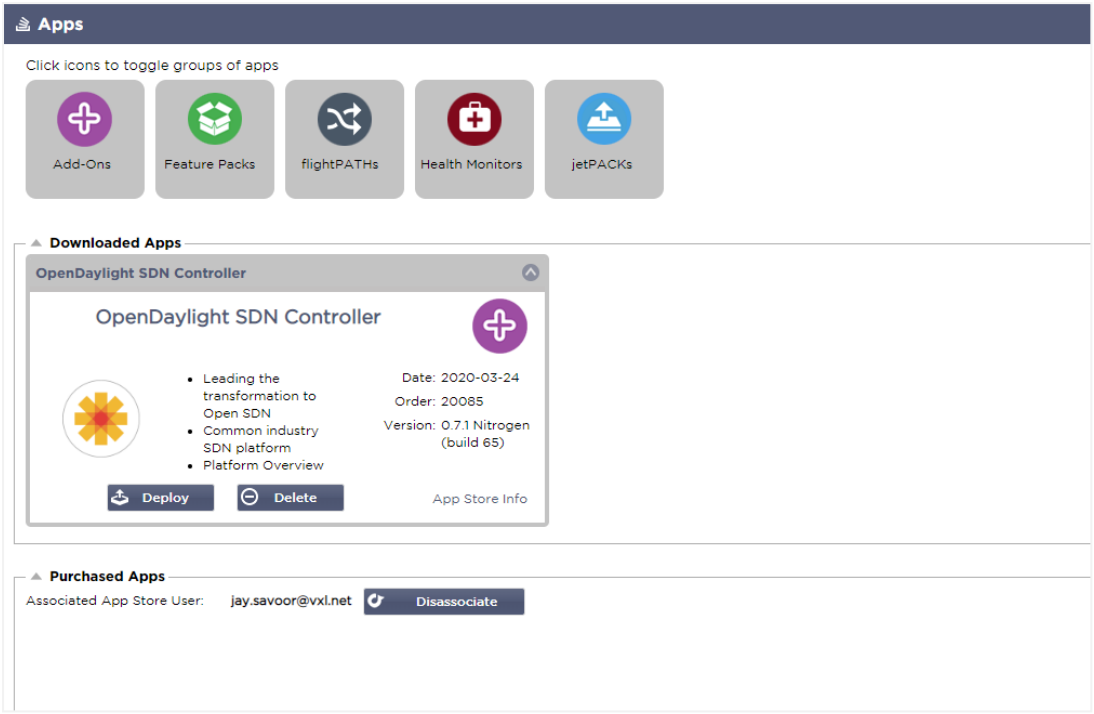
- Suplementos: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/ADD-ONS/**
- Monitores de Saúde: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/SERVER-HEALTH-MONITORS/**
- jetPACKS: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/JETPACKS/**
- Pacotes de características: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-FEATURE-PACK/**
- regras do flightPATH: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/FLIGHTPATH/**

- Atualizações de software: **HTTPS://APPSTORE.EDGENEXUS.IO/PRODUCT-CATEGORY/EDGENEXUS-SOFTWARE-UPDATE/**



Implantação de um aplicativo

Uma vez baixado para o ADC, o aplicativo será movido para a seção Downloaded Apps e implantado no ADC usando o botão Deploy. Este processo leva algum tempo, dependendo dos recursos disponíveis para o ADC. Uma vez implantado, ele aparecerá na seção de Downloads de aplicativos.



Autenticação

A Biblioteca > Página de autenticação permite configurar servidores de autenticação e criar regras de autenticação com opções para o lado do cliente Basic ou Formulários e NTLM ou BASIC do lado do servidor.

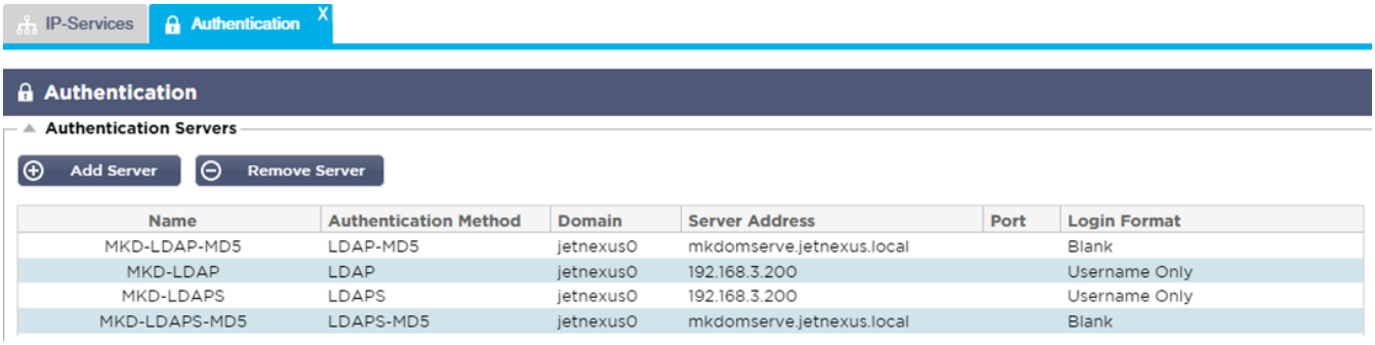
Configurando a Autenticação - Um Fluxo de Trabalho

Por favor, execute as seguintes etapas como um mínimo para aplicar a Autenticação ao seu serviço.

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

Servidores de Autenticação

Para configurar um método de autenticação funcional, é necessário primeiro configurar 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

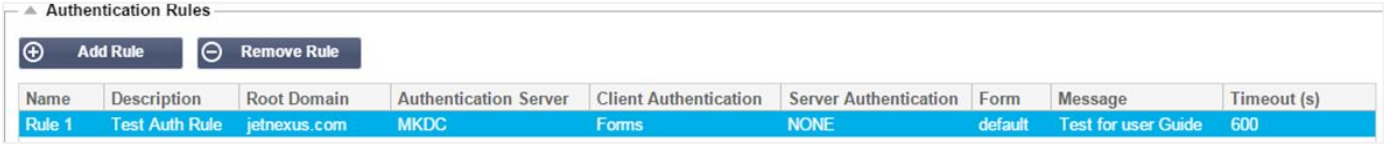
- Clique no botão Adicionar Servidor.
- Esta ação produzirá uma linha em branco pronta para ser concluída.

Opção	Descrição
Nome	Dê a seu servidor um nome para fins de identificação - este nome é usado nas regras
Descrição	Acrescentar uma descrição
Método de autenticação	Escolha um método de autenticação LDAP - LDAP básico com nomes de usuário e senhas enviadas em texto claro para o servidor LDAP. LDAP-MD5 - LDAP básico com nome de usuário em texto claro e senha MD5 hashed para maior segurança. LDAPS - LDAP sobre SSL. Envia a senha em texto claro dentro de um túnel criptografado entre o ADC e o servidor LDAP. LDAPS-MD5 - LDAP sobre SSL. A senha é MD5 hashed para maior segurança dentro de um túnel criptografado entre o ADC e o servidor LDAP.
Domínio	Adicionar 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 nome da máquina (endereço IPv4 não funcionará) LDAPS - endereço IPv4 ou hostname. LDAPS-MD5 - somente hostname (endereço IPv4 não funcionará).
Porto	Use a porta 389 para LDAP e a porta 636 para LDAPS por padrão. Não é necessário adicionar o número da porta para LDAP e LDAPS. Quando outros métodos estiverem disponíveis, você será capaz de configurá-los aqui
Condições de busca	As condições de busca devem estar em conformidade com a RFC 4515. Exemplo: (MemberOf=CN=Phone- VPN,CN=Users,DC=mycompany,DC=local).
Base de busca	Este valor é o ponto de partida para a busca no banco de dados do LDAP. Exemplo *dc=empresa microscópica,dc=local*
Formato de Login	Use o formato de login que você precisa. Nome de usuário - com este formato escolhido, você só precisa digitar o nome de usuário. Qualquer informação de usuário e domínio introduzida pelo usuário é excluída, e as informações de domínio do servidor são utilizadas. Nome de usuário e Domínio - O usuário deve digitar todo o domínio e a sintaxe do nome de usuário. Exemplo: *mycompany\gchristie\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. Esta opção é utilizada quando se utiliza MD5.
Frase de passagem	Esta opção não é utilizada nesta versão.
Tempo morto	Não utilizado nesta versão

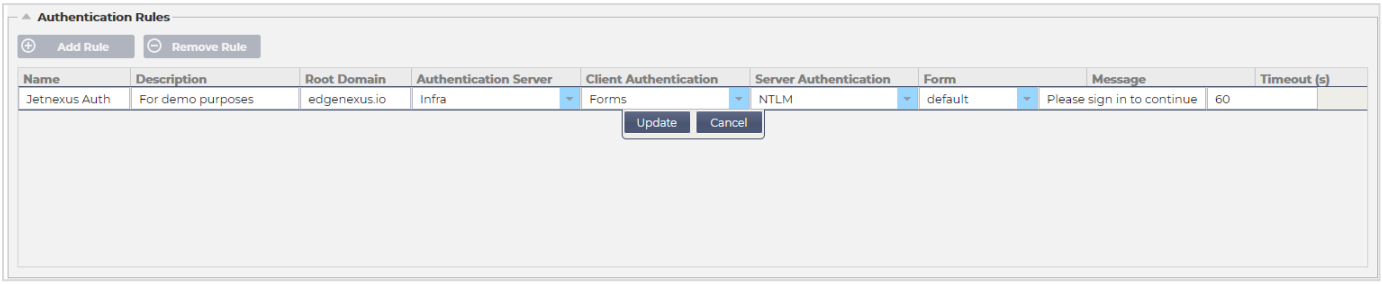
Regras de Autenticação

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



Campo	Descrição
Nome	Adicione um nome adequado para sua regra de autenticação.
Descrição	Adicione uma descrição adequada.
Domínio Raiz	Isto deve ser deixado em branco, a menos que você precise de um único sinal em todos os sub-domínios.
Servidor de Autenticação	Esta é uma caixa dropdown contendo servidores que você configurou.
Autenticação do cliente:	Escolha o valor adequado às suas necessidades: Básico (401) - Este método usa o método de autenticação padrão 401 Formulários - isto apresentará ao usuário o formulário padrão do ADC. Dentro do formulário, você pode adicionar uma mensagem. Você pode selecionar um formulário que você 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. Esta configuração significa que você pode adicionar habilidades de autenticação a um servidor que anteriormente não possuía nenhuma. Básico - se 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 Padrão - A seleção desta opção resultará no ADC usando sua forma integrada. Personalizado - você pode adicionar um formulário que você projetou e selecioná-lo aqui.
Mensagem	Acrescente uma mensagem pessoal ao formulário.
Desconto de tempo	Adicione um timeout à regra, após o qual o usuário será obrigado a se autenticar novamente. Observe que a configuração de timeout só é válida para autenticação baseada em Formulários.

Assinatura única



Se você deseja fornecer um único login para os usuários, complete a coluna Domínio Raiz com seu domínio. Neste exemplo, usamos edgenexus.io. Agora podemos ter vários serviços que utilizarão edgenexus.io como domínio raiz, e você só terá que se logar uma vez. Se considerarmos os seguintes serviços:

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

Estes serviços podem residir em um VIP ou podem ser distribuídos entre 3 VIPs. Um usuário acessando o site usercentral. mycompany.com pela primeira vez receberá um formulário solicitando que faça o login, dependendo da regra de autenticação utilizada. O mesmo usuário pode então conectar-se à appstore. mycompany.com e será autenticado automaticamente pelo ADC. Você pode definir o tempo limite, o que forçará a autenticação uma vez que este período de inatividade tenha sido alcançado.

Formulários

Esta seção permitirá que você faça o upload de um formulário personalizado.

Como criar seu formulário personalizado

Embora a forma básica que o ADC fornece seja suficiente para a maioria das finalidades, haverá ocasiões em que as empresas desejarão apresentar sua própria identidade ao usuário. Você pode criar seu formulário personalizado que será apresentado aos usuários para preencher em tais casos. Este 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 Opcional1:	%JNMESSAGE%
Mensagem Opcional2:	%JNAUTHMESSAGE%
Imagens	Se você deseja adicionar uma imagem, por favor, adicione-a em linha usando a codificação Base64.

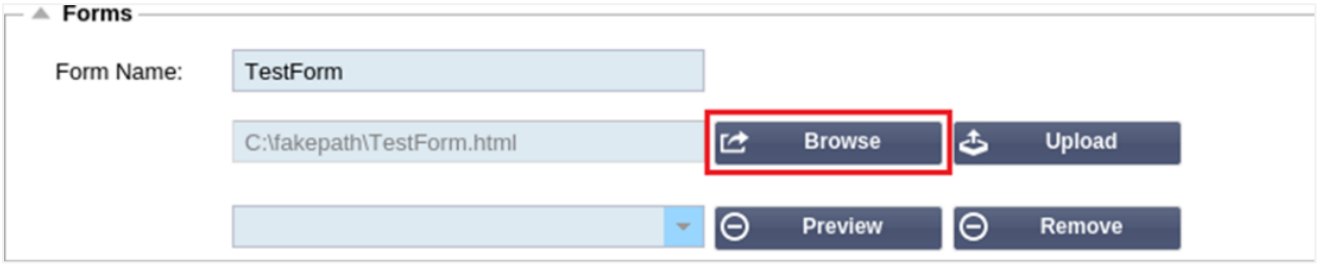
Exemplo de código html de uma forma muito básica e simples

```
<HTML>

<CABEÇA>

<TÍTULO>FORMULÁRIO DE AMOSTRA</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>

</BORBINÁRIO>
```

</HTML>

Adicionando um formulário personalizado

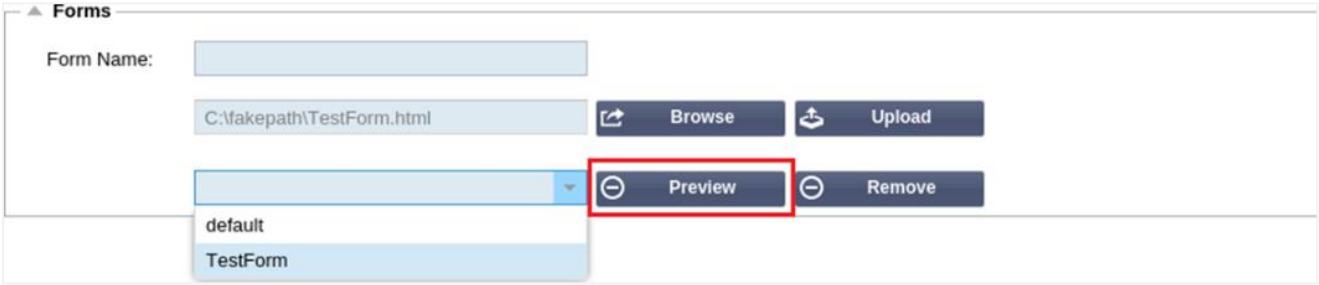
Uma vez criado um formulário personalizado, você pode adicioná-lo usando a seção Formulários.



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

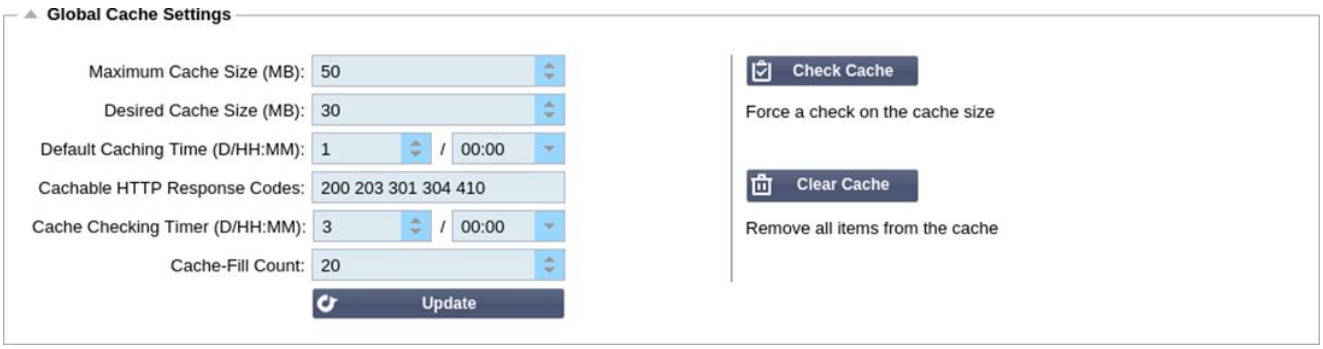
Pré-visualização de seu formulário personalizado

Para visualizar o formulário personalizado que você acabou de carregar, você o seleciona e clica em Pré-visualizar. Você também pode usar esta seção para excluir os formulários que não são mais necessários.



Cache

O ADC é capaz de armazenar dados em cache dentro de sua memória interna e periodicamente descarrega este Cache para o armazenamento interno do ADC. As configurações que gerenciam esta funcionalidade são fornecidas dentro desta seção.



Configurações de Cache Global

Tamanho Máximo do Cache (MB)

Este valor determina o máximo de RAM que o Cache pode consumir. O Cache ADC é um cache in-memory que também é periodicamente lavado no meio de armazenamento para manter a persistência do cache após reinicializações, reinicializações e operações de desligamento. Esta 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 da metade da memória disponível.

Tamanho desejado do Cache (MB)

Este valor denota a RAM ótima para a qual o Cache será aparado. Enquanto o tamanho máximo de cache representa o limite superior absoluto do Cache, o tamanho de cache desejado é pretendido como o tamanho ideal que o Cache deve tentar atingir sempre que for feita uma verificação automática ou manual do tamanho do cache. 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 para aparar 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 dimensionamento apropriado.

Tempo de Cache padrão (D/HH:MM)

O valor aqui inserido 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 diretiva "sem loja" ou tempo de expiração explícita no cabeçalho do tráfego é armazenado.

A entrada de campo toma a forma "D/HH:MM" - assim, uma entrada de "1/01:01" (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 solicitações HTTP bem sucedidas
- 203 - Os cabeçalhos não são definitivos, mas são coletados a partir de uma cópia local ou de uma cópia de terceiros
- 301 - O recurso solicitado foi atribuído a um novo URL permanente
- 304 - Não modificado desde a última solicitação e cópia em cache local deve ser usado em seu lugar
- 410 - O recurso não está mais disponível no servidor, e nenhum endereço de encaminhamento é conhecido

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

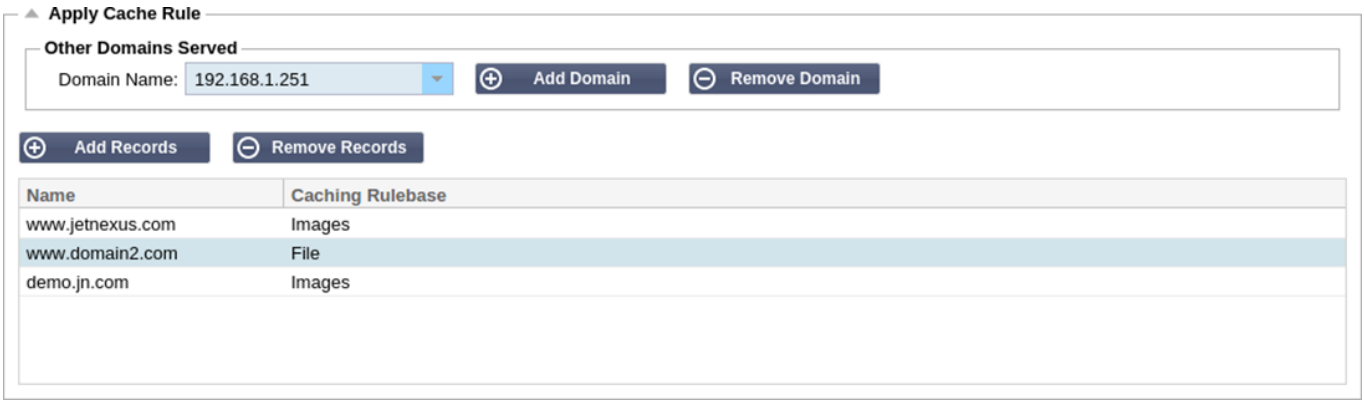
Tempo de Verificação de Cache (D/HH:MM)

Esta configuração determina o intervalo de tempo entre as operações de acabamento do cache.

Contagem de Cache-Fill

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

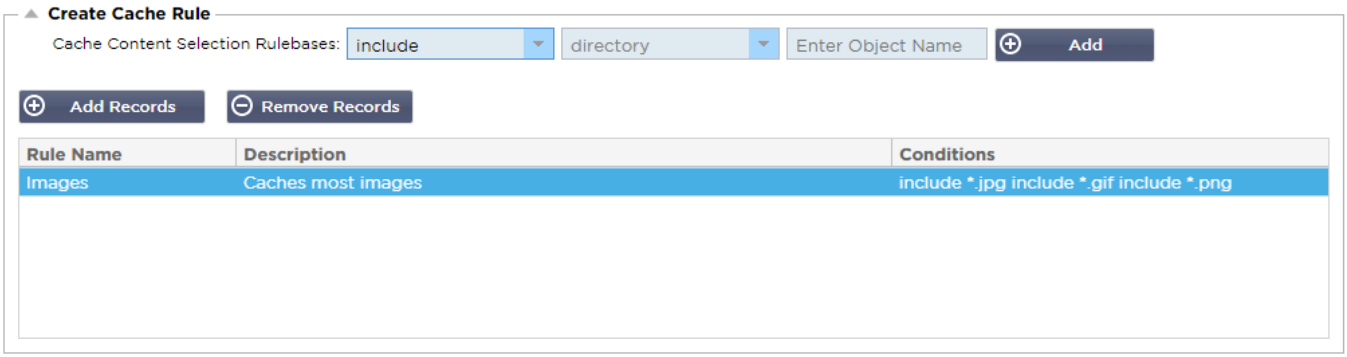
Aplicar a regra de Cache



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

- Adicionar domínio manualmente com o botão Adicionar Registros. Você 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 a partir 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 criar várias regras de cache diferentes que podem então ser aplicadas a um domínio:

- Clique em Adicionar Registros e dê um nome e descrição à sua regra
- Você pode digitar suas condições manualmente ou usar a Condição Adicional

Para adicionar uma condição usando a base de regras de seleção:

- Escolha Incluir ou Excluir
- Escolha todas as imagens JPEG
- Clique no símbolo + Adicionar
- Você verá que 'incluir *.jpg' foi agora adicionado às condições
- Você pode acrescentar mais condições. Se você optar por fazer isto manualmente, você precisa adicionar cada condição em uma NOVO linha. Observe que suas regras serão exibidas na mesma linha até que você clique na caixa Condições, então elas serão exibidas em uma linha separada

flightPATH

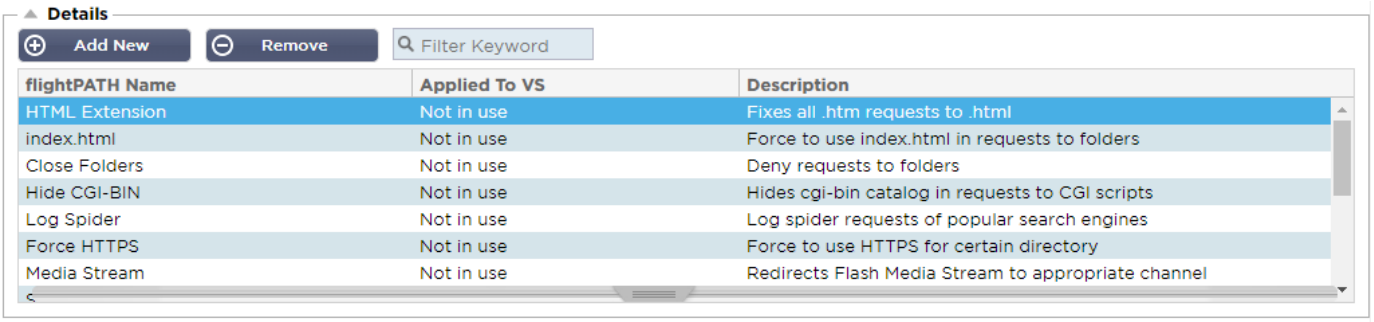
flightPATH é a tecnologia de gerenciamento de tráfego incorporada no ADC. flightPATH permite inspecionar o tráfego HTTP e HTTPS em tempo real e realizar ações baseadas em condições.

As regras do flightPATH devem ser aplicadas a um VIP quando objetos IP são utilizados dentro das regras.

Uma regra de percurso de vôo consiste em quatro elementos:

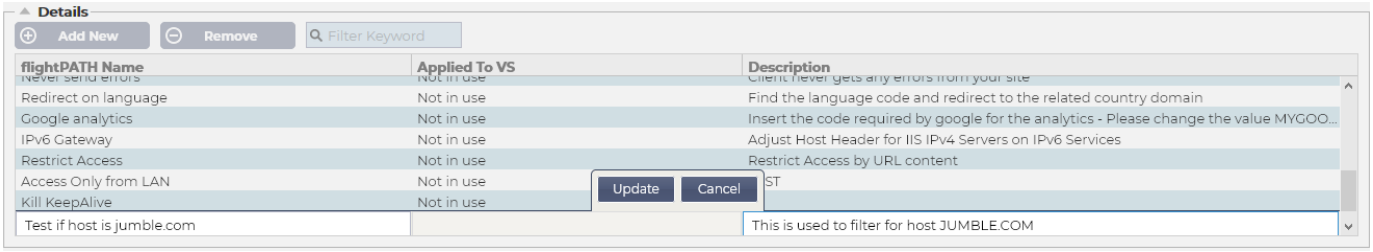
1. Detalhes, onde você define o nome do FlightPATH e o serviço ao qual ele está anexado.
2. Condição(ões) que pode(m) ser definida(s) e que provoca(m) o acionamento da regra.
3. Avaliação que permite a definição de variáveis que podem ser utilizadas dentro de Ações
4. Ações que são usadas para administrar o que deve acontecer quando as condições são cumpridas

Detalhes



A seção de detalhes mostra as regras de flightPATH disponíveis. Você pode adicionar novas regras flightPATH e remover as regras definidas desta seção.

Adicionando uma nova regra de vooPATH



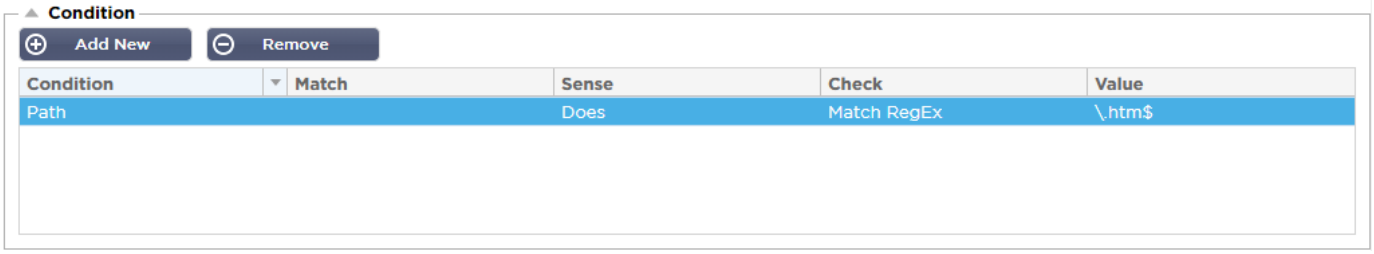
Campo	Descrição
Nome do FlightPATH	Este campo é para o nome da regra flightPATH. O nome que você fornece aqui aparece e é referenciado dentro de outras partes do ADC.
Aplicado à VS	Esta coluna é somente de leitura e mostra o VIP ao qual a regra flightPATH é aplicada.
Descrição	Valor que representa uma descrição fornecida para fins de legibilidade.

Etapas para adicionar uma regra de vooPATH

1. Primeiro, clique no botão Adicionar novo, localizado na seção 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, você verá a coluna Aplicada à autopopulação com um endereço IP e valor de porta
5. Não se esqueça de pressionar o botão Atualizar para salvar suas alterações ou, se você cometer um erro, basta pressionar cancelar e voltar ao estado anterior.

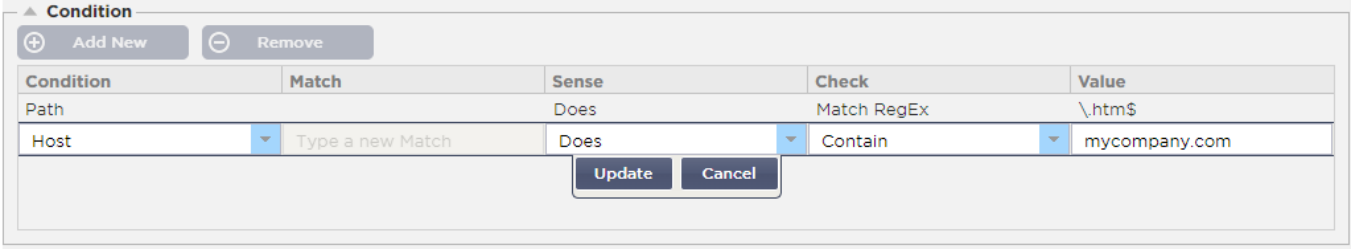
Condição

A regra flightPATH pode ter qualquer número de condições. As condições funcionam com base no "AND", permitindo estabelecer a condição na qual a ação é acionada. Se você quiser usar uma condição OR, crie uma regra flightPATH adicional e a aplique ao VIP na ordem correta.



Você também pode usar RegEx selecionando Match RegEx no campo Check e o valor RegEx no campo Value. A inclusão da avaliação do RegEx amplia tremendamente a capacidade do flightPATH.

Criando uma nova condição de vooPATH



Condição

Fornecemos várias Condições como pré-definidas dentro do dropdown e cobrimos todos os cenários previstos. Quando novas Condições são adicionadas, estas estarão disponíveis através de atualizações Jetpack.

As opções disponíveis são:

CONDIÇÃO	DESCRIÇÃO	EXEMPLO
<form>	Os formulários HTML são usados para passar dados para um servidor	Exemplo "o formulário não tem comprimento 0".
Localização GEO	Compara o endereço IP de origem com os Códigos de Países ISO 3166	GEO Location faz igual a GB, OU GEO Location faz igual à Alemanha
Anfitrião	Host 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	Desistência dos métodos HTTP	Dropdown que inclui GET, POST, etc.
Origem IP	Se o upstream proxy suporta X-Forwarded-for (XFF), ele usará o verdadeiro endereço de origem	IP do cliente. Também pode utilizar 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 POST	Verificar os dados que estão sendo carregados em um site
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
Consulta String	Toda a cadeia de consulta após o caractere ?	
Solicite um Cookie	Nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho de solicitação	Qualquer cabeçalho HTTP	Referidor, Usuário-Agente, De, Data

Versão de solicitação	A versão HTTP	HTTP/1.0 OU HTTP/1.1
Corpo 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::
Cabeçalho de resposta	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	Seja o IP de origem, IP do servidor proxy, ou algum outro endereço IP agregado	ClientIP , Proxy IP, Firewall IP. Também pode utilizar múltiplos IP e sub-redes. Você deve escapar dos pontos, pois estes são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Combinar

O campo de partida pode ser um valor drop-down ou um valor de texto e é definível dependendo do valor no campo Condição. Por exemplo, se a Condição for definida como Anfitrião, o campo Correspondência 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 os valores pertinentes.

As opções disponíveis são:

MATCH	DESCRIÇÃO	EXEMPLO
Aceitar	Tipos de conteúdo que são aceitáveis	Aceitar: texto/plainar
Aceitar-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>
Aceitar-Língua	Idiomas aceitáveis para resposta	Aceitar-Língua: pt-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Intervalos de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ=====
Carga-To	Contém informações de conta para os custos da aplicação do método solicitado	
Codificação de conteúdo	O tipo de codificação utilizada	Codificação do conteúdo: gzip
Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (bytes de 8 bits)	Comprimento do conteúdo: 348
Tipo de conteúdo	O tipo de mímica 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 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-Modificado - Desde: 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 Nov 1994 12:45:26 GMT
Pragma	Implementação: Cabeçalhos específicos que podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta ao pedido.	Pragma: sem cache
Referência	Endereço da página web anterior a partir do qual foi seguido um link para a página solicitada atualmente	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 cadeia do agente de usuário do agente de usuário	Usuário-Agente: 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 solicitação para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova solicitação do servidor de origem.	Vary: Usuário-Agente
X-Powered-By	Especifica a tecnologia (por exemplo, ASP.NET, PHP, JBoss) que suporta a aplicação web	X-Powered-By: PHP/5.4.0

Sentido

O campo Sentido é um campo booleano de queda e contém opções de Fazer ou Não Fazer.

Verifique

O campo Verificar permite a definição 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

VERIFIQUE	DESCRIÇÃO	EXEMPLO
Existente	Isto não se preocupa com o detalhe da condição apenas que ela existe/não existe	Anfitrião - Existe - Existe
Início	A cadeia começa com o Valor	Caminho - Faz - Começa - /secura
Fim	O fio termina com o Valor	Caminho - Faz - Termina - .jpg
Conter	O fio contém o Valor	Solicitar cabeçalho - Aceitar - Fazer - Conter - Imagem
Igual	O fio faz igualar o valor	Host - Does - Equal - www.edgenexus.io
Ter Comprimento	O fio tem um comprimento do valor	Hospedeiro - Tem - Tem Comprimento - 16

		www.edgenexus.io = VERDADEIRO www.edgenexus.com = FALSO
Combinar RegEx	Permite que você insira uma expressão regular totalmente compatível com Perl	Origem IP - Faz - Combina Regex - 10/11.* | 11/11.*

Passos para acrescentar uma Condição

Adicionar um novo FlightPATH Condition é muito fácil. 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 o Host. Você também pode digitar no campo, e o ADC mostrará o valor em uma caixa suspensa.
3. Escolha um Sentido. Por exemplo, o
4. Escolha um cheque. Por exemplo, Conter
5. Escolha um valor. Por exemplo, mycompany.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 host na URL é www.imagepool.com

Avaliação

A capacidade de adicionar variáveis definíveis é uma capacidade convincente. Os ADCs regulares oferecem esta capacidade usando opções de script ou linha de comando que não são ideais para ninguém. O ADC permite que você 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 - selecione valores de um drop-down ou digitados manualmente.
- Valor - o valor que a variável detém e pode ser um valor alfanumérico ou um RegEx para ajuste fino.

Variáveis incorporadas:

As variáveis embutidas já foram codificadas de forma rígida, portanto, não é necessário criar uma entrada de avaliação para elas.

Você 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") = $respresp...
- Anfitrião = $host$
- Versão = $version$

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

AÇÃO	META
Ação = Redirecionar 302	Alvo = HTTPs://$host$/404.html
Ação = Log	Meta = 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 a página de erro 404 do navegador.
- Em vez disso, o usuário é redirecionado para o hostname original que usou, mas o caminho incorreto é substituído pelo 404.html
- Uma entrada é adicionada ao Syslog dizendo: "Um cliente de 154.3.22.14:3454 acabou de solicitar a página wrong.html".

Ação

A próxima etapa do processo é acrescentar uma ação associada à regra e condição do flightPATH.

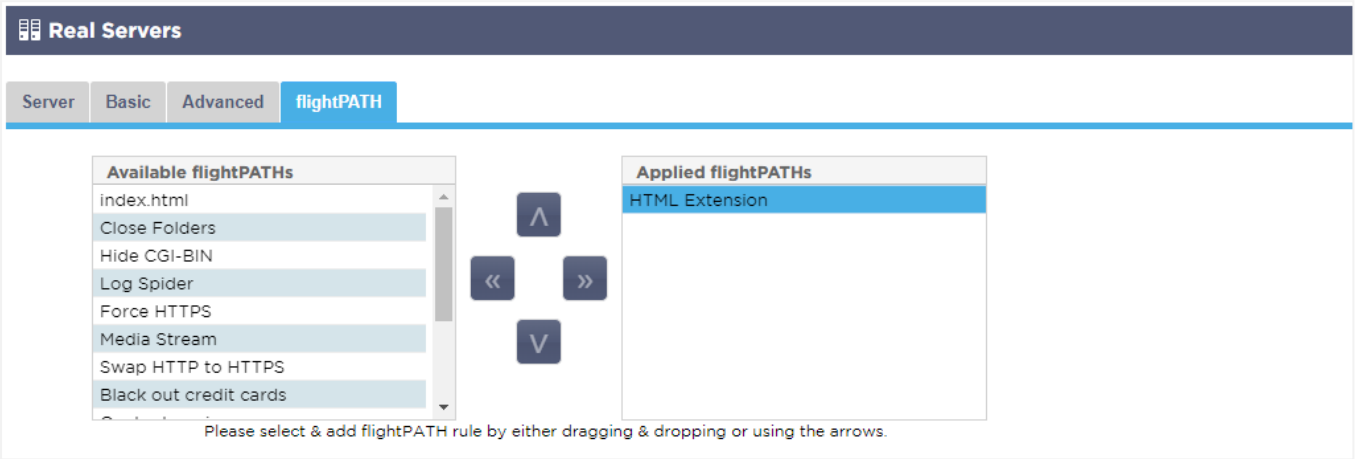
Neste exemplo, queremos reescrever a parte do caminho da URL para refletir a URL digitada pelo usuário.

- Clique em Add New (Adicionar novo)
- Escolha Rewrite Path (Reescrever caminho) no menu suspenso Action (Ação)
- No campo Alvo, digite em $path$/myimages
- Clique em Atualizar

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

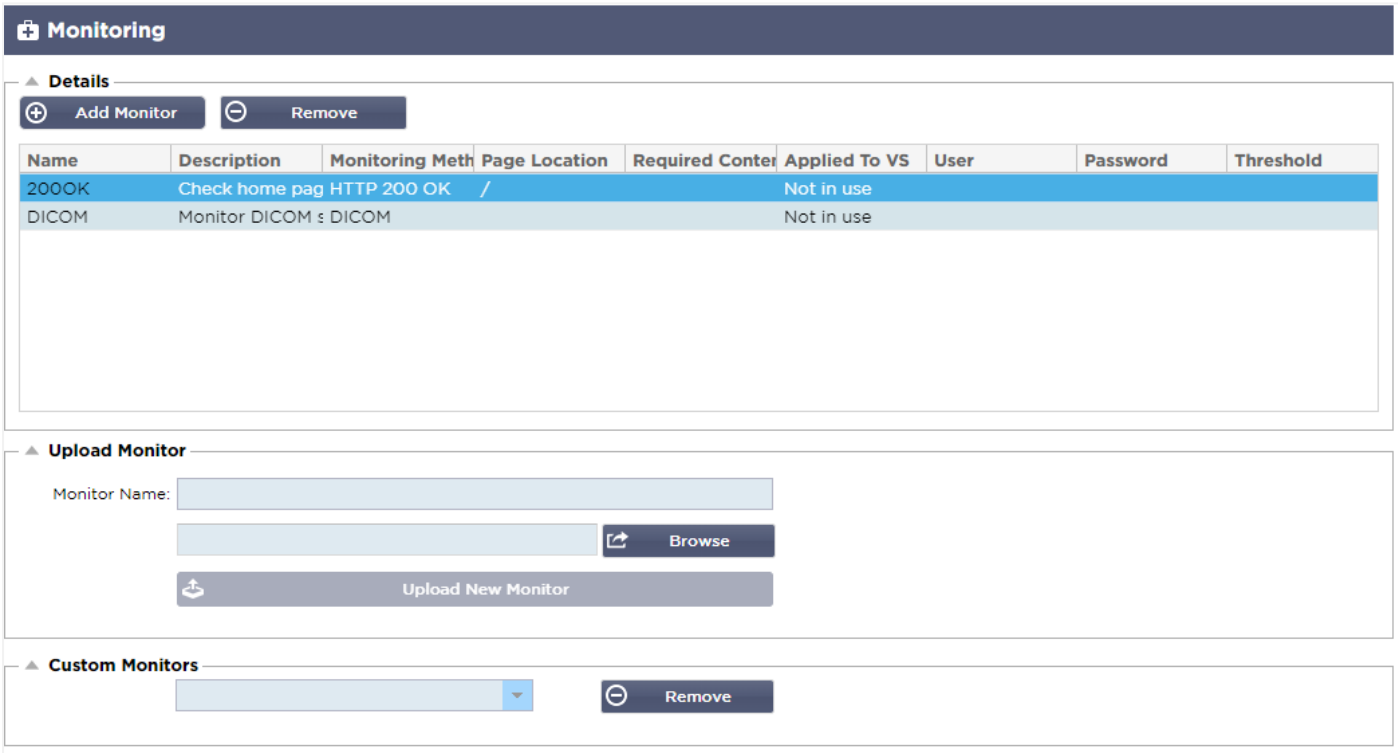
Aplicando a regra flightPATH

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



- Navegue até Serviços > Serviços IP e escolha o VIP ao qual você deseja atribuir a regra flightPATH.
- Você verá a lista de Servidores Reais mostrada abaixo
- Clique na aba flightPATH
- Selecione a regra flightPATH que você configurou ou uma das regras pré-construídas suportadas. Você pode selecionar várias regras flightPATH, se necessário.
- Arraste e solte o conjunto selecionado para a seção PAATOS DE VOOO APLICADOS ou clique no botão >> seta.
- A regra será movida para o lado certo e aplicada automaticamente.

Monitores de Servidor Real



Quando o balanceamento de carga é configurado, é útil monitorar a saúde dos servidores reais e as aplicações em execução neles. Por exemplo, em servidores web, você pode configurar uma página específica que você pode usar para monitorar o estado ou usar um dos outros sistemas de monitoramento que o ADC possui.

A página Library > Real Server Monitors permite que você adicione, visualize e edite monitoramento personalizado. Estes são os "Verificações de Saúde" do servidor Layer 7 e selecione-os no campo Monitoramento do Servidor dentro da guia Básico do serviço Virtual que você definir.

Tipos de monitores de servidores reais

Há vários Monitores de Servidor Real disponíveis, e a tabela abaixo os explica. Você pode, é claro, escrever monitores adicionais usando PERL.

Método de monitoramento	Descrição	Exemplo
HTTP 200 OK	Uma conexão TCP é feita com o Servidor Real. Após a conexão ser feita, um breve pedido HTTP é enviado ao Servidor Real. Quando a resposta é recebida, ela é verificada para a seqüência '200 OK'. Se ela estiver presente, o servidor é considerado operacional. Favor observar que a utilização deste monitor traz o conteúdo de toda a página. Este método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e Acelerado HTTP. 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 adequadamente pela instalação "Content SSL".	**Solicitação** GET / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Tipo de conteúdo: texto/html Modificado por último: Qua, 31 Jan 2018 15:08:18 GMT Intervalos de aceitação: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Ter, 13 Jul 2021 15:55:47 GMT Comprimento do conteúdo: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <estilo tipo="texto/css"> <!-- corpo { cor:#FFFFFFFFFF; ... </corpo> </html>
Cabeça HTTP 200	Uma conexão TCP é feita ao Servidor Real com o campo PATH especificando o local a ser verificado. A parte principal da resposta é buscada no servidor, com o conteúdo descartado. A resposta é verificada para 200 OK. Se ela estiver presente, o servidor é considerado operacional. Observe que o uso deste monitor só alcança a parte da cabeça. Este método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e Acelerado HTTP. 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	**Solicitação** CABEÇA / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Comprimento do conteúdo: 1364 Tipo de conteúdo: texto/html Modificado por último: Qua, 31 Jan 2018 15:08:18 GMT Intervalos de aceitação: bytes ETag: "0dd3253a59ad31:0"

	se for tratado adequadamente pela instalação "Content SSL".	Servidor: Microsoft-IIS/10.0 Data: Ter, 13 Jul 2021 15:49:19 GMT
Opções do HTTP 200	Uma conexão TCP é feita ao Real Server, e uma solicitação de Opções é feita. As Opções são devolvidas e verificadas para 200 OK de conteúdo. Se o conteúdo de 200 OK for encontrado, então o servidor é considerado como disponível.	**Solicitação** OPÇÕES / HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Permitir: OPÇÕES, TRACE, GET, HEAD, POST Servidor: Microsoft-IIS/10.0 Público: OPÇÕES, TRACE, GET, HEAD, POST Data: Ter, 13 Jul 2021 16:23:39 GMT Comprimento do conteúdo: 0
Cabeça HTTP	O monitor do cabeçote HTTP nos permite verificar um valor específico na parte do cabeçote do fluxo HTTP. Podemos inserir um Caminho e Resposta Necessária nos campos apropriados e depois verificar esse valor na resposta. Caso o valor da Resposta Necessária seja encontrado no cabeçote, o servidor é considerado como estando instalado e disponível. Também podemos usar isto em páginas especialmente protegidas que precisam de um nome de usuário e senha. Desta forma, o resultado do monitor pode ser considerado exato. Por exemplo, fornecendo **/ispagethere.html** e **200** valores **OK** nos campos Caminho e Resposta Requerida retornarão um resultado bem sucedido se o servidor estiver no ar, a página estiver disponível, e responder à solicitação. Este método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e Acelerado HTTP. 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 adequadamente pela instalação "Content SSL".	**Solicitação** HEAD /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Comprimento do conteúdo: 1364 Tipo de conteúdo: texto/html Modificado por último: Qua, 31 Jan 2018 15:08:18 GMT Intervalos de aceitação: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Qua, 14 Jul 2021 08:28:18 GMT
Opções HTTP	O monitor de Opções HTTP permite que você verifique um valor específico dentro dos dados das Opções retornadas. Inserimos um Caminho e Resposta Necessária nos campos apropriados e depois verificamos a resposta. Se a Resposta Necessária for encontrada nos dados das Opções, o servidor está disponível e em funcionamento. Os valores de Resposta Necessária podem ser qualquer um dos seguintes: OPÇÕES, TRACE, GET, HEAD, e POST.	**Solicitação** OPÇÕES /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Permitir: OPÇÕES, TRACE, GET, HEAD, POST

	Por exemplo, fornecendo **/ispagethere.html** e **GET** valores nos campos Path e Required Response retornarão um resultado bem sucedido se o servidor estiver no ar, se a página estiver disponível e se ela responder à solicitação. Este método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e Acelerado HTTP. 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 pelo recurso "Content SSL".	Servidor: Microsoft-IIS/10.0 Público: OPÇÕES, TRACE, GET, HEAD, POST Data: Qua, 14 Jul 2021 09:47:27 GMT Comprimento do conteúdo: 0
Resposta HTTP	Uma conexão e uma solicitação/resposta HTTP é feita ao Real Server e verificada como explicado nos exemplos anteriores. Mas ao invés de verificar por 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. Por exemplo, no exemplo mostrado à direita, especificamos **/ispagethere.htm** como o Caminho e **Microsoft-IIS** como a Resposta Necessária. Se o texto for encontrado, o Servidor Real é considerado como estando em funcionamento. Este método de monitoramento só pode ser realmente usado com tipos de serviço HTTP e Acelerado HTTP. 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 adequadamente pela instalação "Content SSL".	**Solicitação** GET /ispagethere.htm HTTP/1.1 Anfitrião: 192.168.159.200 Aceitar: */* Aceitar-Língua: pt-gb Usuário-Agente: Edgenexus-ADC/4.0 Conexão: Keep-Alive Cache-Control: no-cache **Resposta** HTTP/1.1 200 OK Tipo de conteúdo: texto/html Modificado por último: Qua, 31 Jan 2018 15:08:18 GMT Intervalos de aceitação: bytes ETag: "0dd3253a59ad31:0" Servidor: Microsoft-IIS/10.0 Data: Qua, 14 Jul 2021 10:07:13 GMT Comprimento do conteúdo: 1364 <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"> <html xmlns="http://www.w3.org/1999/xhtml"> <head> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>jetNEXUS</title> <estilo tipo="texto/css"> <!-- corpo { cor:#FFFFFFFFFF; …
Monitor TCP Multi-Portas	Este método é como o anterior, exceto que você pode ter vários portos diferentes. O monitor só é considerado bem-sucedido se todas as portas especificadas na seção de conteúdo exigido responderem corretamente.	Nome: Monitor Multi-Portas Descrição: Monitore múltiplos portos para o sucesso Localização da página: N/A Conteúdo Requerido: 135,59534,59535
TCP fora de faixa	O método TCP Out of Band é como um TCP Connect, exceto que você pode especificar a porta que deseja monitorar na coluna de conteúdo requerida. Esta porta normalmente não é a mesma que a porta de tráfego e é usada quando você deseja conectar serviços	Nome: TCP fora de faixa Descrição: Monitor fora de banda/ porto de tráfego Localização da página: N/A Conteúdo Requerido: 555
DICOM	Enviamos um eco DICOM usando o valor do título AE "Source Calling" na coluna de conteúdo requerido. Você também pode definir	Nome: DICOM Descrição: Exame de saúde L7 para o serviço DICOM

	o valor do título AE "Destination Calling" na seção Notes de cada servidor. Você pode encontrar a coluna Notas na seção de Serviços IP. -Virtual Services--Server page.	Método de monitoramento: DICOM Localização da página: N/A Conteúdo Requerido: Valor AET
LDAPS	Este novo exame de saúde é usado para verificar a saúde e a resposta de um servidor LDAP/AD.	Nome: LDAPS Descrição: LDAP/AD Server health check Os parâmetros de utilização são os seguintes: **Nome de usuário**: cn=nome de usuário,cn=usuários,dc=domínio,dc=local **Senha**: DomínioUserPassword **Conteúdo**: 200OK
SNMP v2	Este método de monitoramento permite verificar a disponibilidade de um servidor usando a resposta SNMP MIB do servidor. O valor da Resposta Requisitada deve conter o nome da Comunidade.	
Verificação do servidor DNS	Ao equilibrar a carga dos Servidores DNS, é útil ver se o servidor responde às consultas DNS. O monitor pode ser usado da seguinte forma: • O campo Path é usado para a FQDN que você está consultando. Por exemplo, se você desejava consultar www.edgenexus.io, então digite isto no campo Caminho. • Se você deixar isto em branco, então o monitor usará sua busca padrão para fazer a consulta. • O campo Resposta Necessária pode ser deixado em branco, e o monitor assumirá que qualquer resposta é considerada válida. Caso contrário, você deve inserir o IP esperado no campo Resposta Necessária. Por exemplo, isto pode ser 101.10.10.100. Se a consulta retornar este valor, o monitor sinalizará um sucesso; caso contrário, ele sinalizará um fracasso. Um resultado de sucesso indica que o servidor DNS que você está balanceando a carga está operacional.	

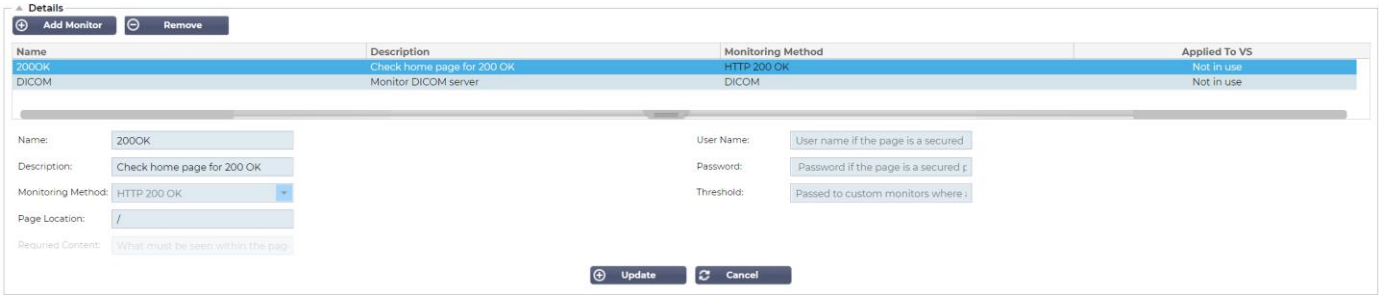
A página do Monitor do Servidor Real

A página de Monitores de Servidor Real está dividida em três seções.

- Detalhes
- Upload
- Monitores personalizados

Detalhes

A seção Detalhes é usada para adicionar novos monitores e para remover os que não forem necessários. Você 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 seja o melhor para torná-lo o mais descritivo possível.

Método de monitoramento

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

- HTTP 200 OK
- Cabeça HTTP 200
- Opções do HTTP 200
- Cabeça HTTP
- Opções HTTP
- Resposta HTTP
- Monitor TCP Multi-Portas
- TCP fora de faixa
- DICOM
- SNMP v2
- Verificação do servidor DNS
- LDAPS

Localização da página

Localização da página URL de um monitor HTTP. Este valor pode ser um link relativo, como /folder1/folder2/page1.html. Você também pode usar um link absoluto onde o site está vinculado ao nome da hostname.

Conteúdo Requerido

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

Aplicado à VS

Este campo é automaticamente preenchido com o IP/Porta do Serviço Virtual ao qual o monitor é aplicado. Você não poderá excluir nenhum Monitor que tenha sido usado com um Serviço Virtual.

Usuário

Alguns monitores personalizados podem usar este valor junto com o campo de senha para entrar em um servidor real.

Senha

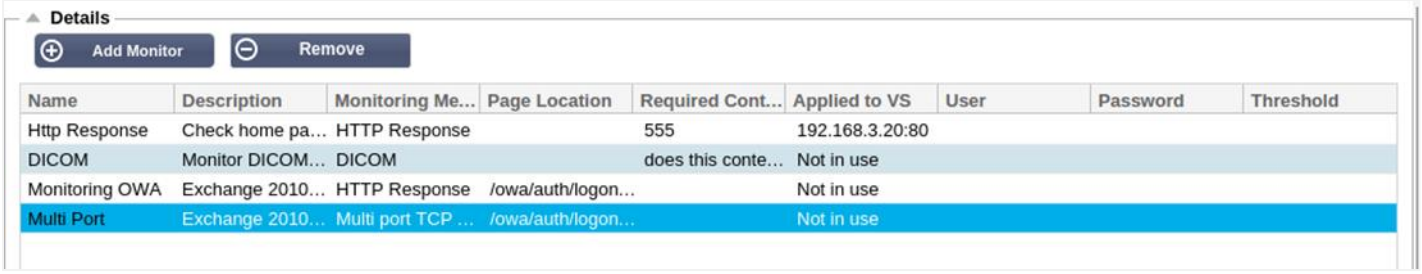
Alguns monitores personalizados podem usar este valor junto com o campo Usuário para fazer login em um Servidor Real.

Threshold

O campo Threshold é um inteiro geral usado em monitores personalizados onde um limite como o nível de CPU é necessário.

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

Exemplos de Monitor de Servidor Real



Name	Description	Monitoring Me...	Page Location	Required Cont...	Applied to VS	User	Password	Threshold
Http Response	Check home pa...	HTTP Response		555	192.168.3.20:80			
DICOM	Monitor DICOM...	DICOM		does this conte...	Not in use			
Monitoring OWA	Exchange 2010...	HTTP Response	/owa/auth/logon...		Not in use			
Multi Port	Exchange 2010...	Multi port TCP ...	/owa/auth/logon...		Not in use			

Monitor de Upload

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 de arquivo .pl.

- Dê um nome a seu monitor para que você possa identificá-lo na lista do Método de Monitoramento
- Procurar pelo 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, você pode visualizar monitores personalizados carregados e removê-los se não forem mais necessários.

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

Criando um roteiro personalizado do Monitor Perl

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

Esta seção mostra os comandos que você pode usar dentro de seu script Perl.

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

Os seguintes itens são obrigatórios:

- #Nome do monitor
- usar rigorosamente;

- usar advertência;

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

Valores dinâmicos

- meu $host = $_[0]; - Isto usa o "Endereço" da seção Serviços IP--Servidor Real
- meu $port = $_[1]; - Isto usa a seção "Port" da IP Services--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 "Notas" na seção Servidor Real de Serviços IP
- minha $página = $_[4]; - Isto usa os valores de "Page Location" da seção Library--Real Server Monitor
- meu $user = $_[5]; - Isto usa o valor "Usuário" da seção Monitor de Servidor Real da Biblioteca
- minha senha = $_[6]; - Isto usa o valor "Senha" da seção Monitor do Servidor Real da Biblioteca

Os cheques de saúde personalizados têm dois resultados

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

Exemplo de um monitor de saúde personalizado

```
#Nome do monitor HTTPS_SNI
usar rigorosamente:
usar avisos;
# O nome do monitor como acima é exibido no menu suspenso de Verificações de saúde disponíveis
# Há 6 valores passados para 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)
my Snotes=      $_[3]; #### Nome do anfitrião virtual
my Spage=       $_[4]; #### A parte da URL após o endereço do host
meu Suser=      $_[5]: ### domínio/usemame (opcional)
minha senha Spassword=          $_[6]; #### senha (opcional)
meus $resolve;
meus $auth      =;
se ($port)
{
        $resolve = "$notes:$port:$host":
}
senão {
        $resolve = "$notes:$host";
}
se ($user && $password) {
        $auth = "-u $user:$password :
}
```

```
my @lines = 'curl -s -i -retry 1 -max-time 1 -k -H "Host:$notes --resolve $resolve $auth HTTPs://${notes}${page} 2>&1';
if(join(""@linhas)=~/$content/)
        {
        imprimir "HTTPs://$notes}${página} procurando - $content - Health check successful.\n";
        retorno(1);
        }
senão
        {
        imprimir "HTTPs://${notes}${página} procurando - $content - Health check failed.\n";
        retorno(2)
        }
}
monitor(@ARGV):
```

NOTA: Monitoramento personalizado - O uso de variáveis globais não é possível. Usar somente variáveis locais - variáveis definidas dentro das funções

Certificados SSL

Para usar com sucesso o balanceamento de carga de Camada 7 com servidores usando conexões criptografadas usando SSL, o ADC deve estar equipado com os certificados SSL usados nos servidores alvo. Esta 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 desde certificados autoassinados que o ADC pode gerar até os certificados tradicionais (inclusive wildcard) disponíveis em fornecedores confiáveis. Você também pode usar certificados assinados por domínio que são gerados a partir do Active Directory.

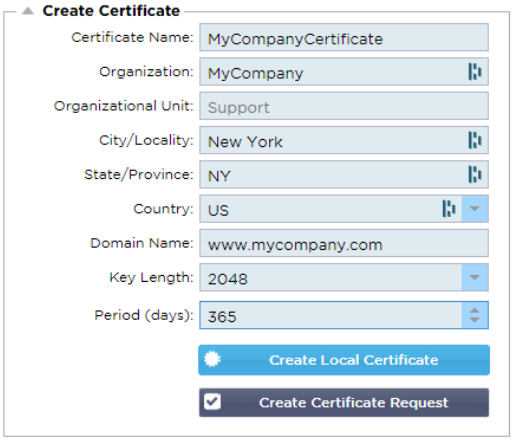
O que o ADC faz com o Certificado SSL?

O ADC pode executar regras de gerenciamento de tráfego (flightPATH) dependendo do que os dados contêm. Este gerenciamento não pode ser realizado com dados criptografados SSL. Quando o ADC tem que inspecionar os dados, ele precisa primeiro decodificá-los, e para isso, precisa ter o certificado SSL usado pelo servidor. Uma vez desencriptados, o ADC poderá então examinar e executar as regras do flightPATH. Em seguida, os dados serão re-encriptados 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 Auto-assinado. O SSL Auto-assinado é perfeito para os requisitos de equilíbrio de carga interna. Entretanto, suas políticas de TI podem exigir um certificado CA de confiança ou de domínio.

Como criar um certificado SSL local



- Preencha todos os detalhes como o exemplo acima
- Clique em Create Local Certificate (Criar certificado local)
- Uma vez clicado, você pode aplicar o certificado a um **SERVIÇO VIRTUAL.**

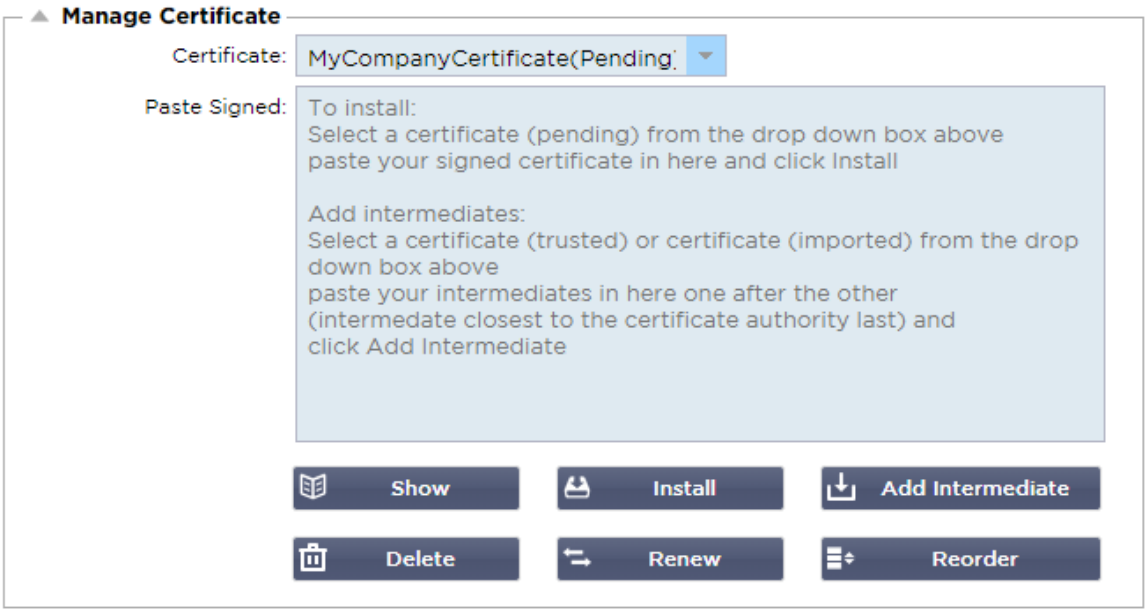
Criar uma Solicitação de Certificado (CSR)

Quando você precisar obter um SSL de confiança global de um fornecedor externo, você 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 a você o popup correspondente aos dados que você forneceu.

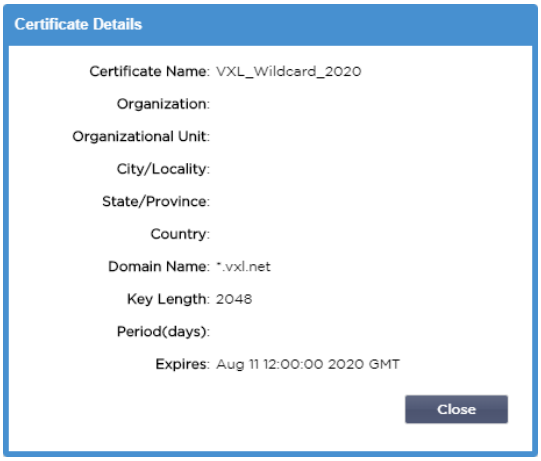
Você precisará cortar e colar o conteúdo em um arquivo TEXT e nomeá-lo com uma extensão CSR, por exemplo, *mycert.csr*. Este arquivo CSR precisará então ser fornecido à sua autoridade certificadora para criar o certificado SSL.

Gerenciar Certificado



Esta subseção contém várias ferramentas para permitir o gerenciamento dos certificados SSL que você tem dentro do ADC.

Mostrar

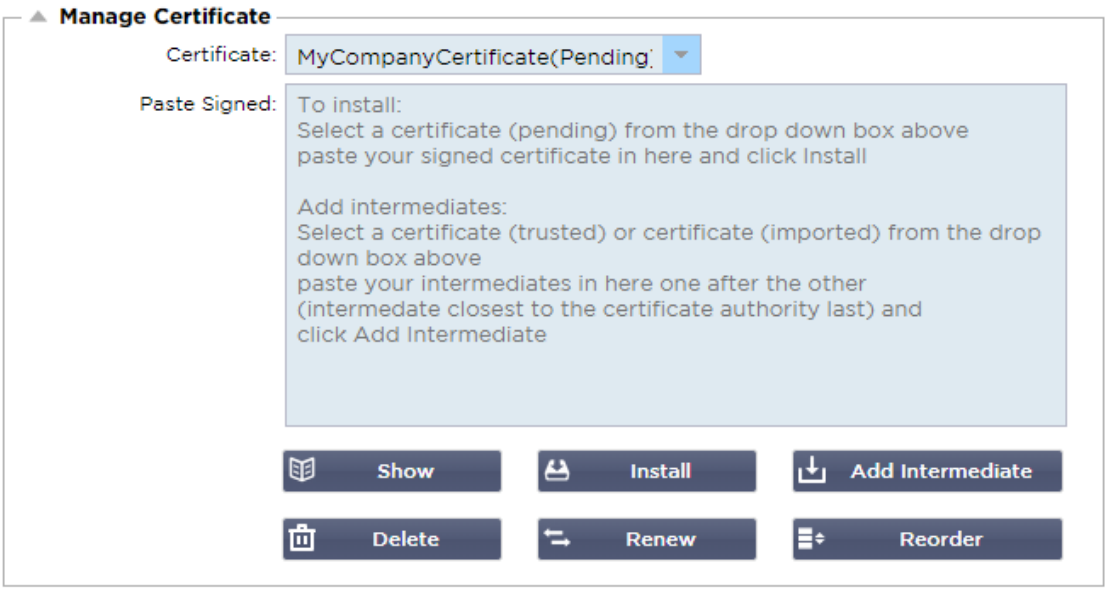


Pode haver ocasiões em que você deseje olhar os detalhes de um certificado SSL instalado.

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

Instalação de um certificado

Uma vez obtido o certificado da Autoridade de Certificação Confiável, você precisará compará-lo ao CSR gerado e instalá-lo dentro do ADC.



- Selecione um certificado que você tenha gerado nas etapas acima. Haverá um status (Pendente) fixado para o item. 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 área de transferência
- Cole o conteúdo do certificado SSL assinado que você recebeu da autoridade de confiança no campo marcado Colar Assinado.
- Você também pode colar nos Intermediários abaixo disso, tomando o cuidado de seguir a ordem correta:
  1. (TOPO) Seu Certificado Assinado
  2. (2º Desde o início) Intermediário 1
  3. (3º de cima) Intermediário 2
  4. (Fundo) Intermediário 3
  5. Autoridade de Certificado de Raiz Não há necessidade de acrescentar isto, pois eles existem nas máquinas dos clientes.
     (o ADC também contém um pacote raiz para reencriptação onde atua como um cliente para um Servidor Real)
- Clique em Instalar
- Uma vez instalado o certificado, você deve ver o status (Confiável) ao lado de seu certificado

Se você cometeu um erro ou inseriu a ordem intermediária errada, então selecione o Certificado (Trusted) e adicione os certificados (incluindo o certificado assinado) novamente na ordem correta e clique em Install

Adicionar Intermediário

É necessário, ocasionalmente, acrescentar certificados intermediários separadamente. Por exemplo, você 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 certificadora seja colado por último.
- Clique em Adicionar Intermediário.

Se você cometer um erro com o pedido, você pode repetir o processo e adicionar novamente os intermediários. Esta ação só sobregravará os intermediários anteriores.

Eliminar um certificado

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

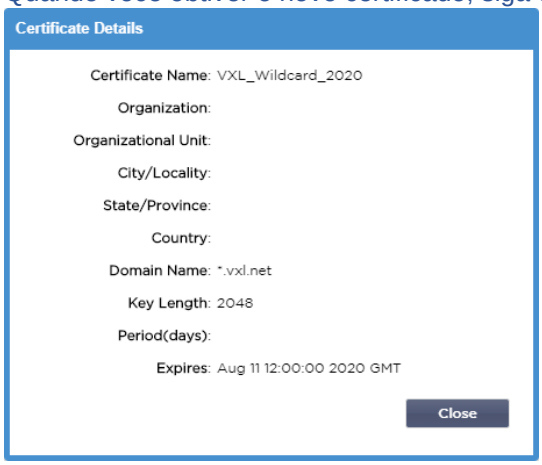
Nota: Por favor, certifique-se de que o certificado não esteja anexado a um VIP operacional antes de apagá-lo.

Renovar um certificado

O botão Renovar permite obter um novo Pedido de Assinatura de Certificado. Esta ação é necessária quando o certificado está prestes a expirar e precisa ser renovado.

- Selecione um certificado da lista suspensa; você pode escolher qualquer certificado com o status (Pendente), (Confiável), ou (Importado)
- Clique em Renovar
- Copie os novos detalhes da RSE para que você possa obter um novo certificado

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



-
- Pode haver ocasiões em que você deseje olhar os detalhes de um certificado SSL instalado.
- Selecione o certificado no 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 assinados por domínio como parte de seus regimes de segurança interna. Os certificados devem estar no formato PKCS#12, e as senhas invariavelmente protegem tais certificados.

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

- Dê um nome amigável ao seu certificado. O nome o identifica nas listas suspensas utilizadas 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 -.
- Digite a senha utilizada para criar o certificado PKCS#12
- Procurar pelo {nome do certificado}.pfx
- Clique em Importar.
- Seu certificado estará agora nos menus suspensos relevantes do ADC SSL

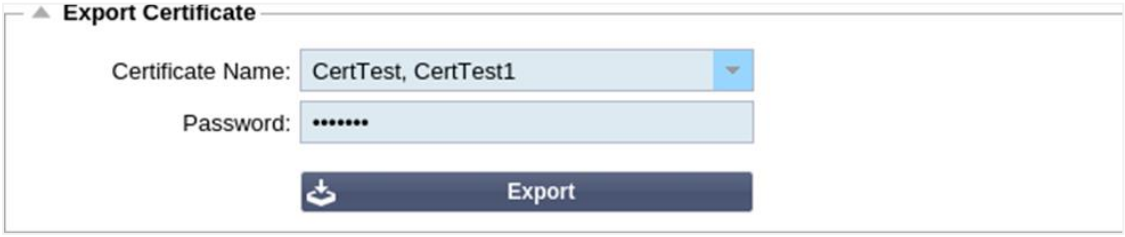
Importação de certificados múltiplos

Esta seção permite a importação de um arquivo JNBK que contém vários certificados. Um arquivo JNBK é criptografado e produzido pela ADC ao exportar múltiplos certificados.

- Navegue por seu arquivo JNBK - você pode criar um destes exportando vários certificados
- Digite a senha que você usou para criar o arquivo JNBK
- Clique em Importar.
- Seus certificados agora estarão nos menus suspensos SSL relevantes dentro do ADC

Exportação de um certificado

De tempos em tempos, você pode desejar exportar um dos certificados mantidos dentro do ADC. O ADC foi dotado da capacidade para fazer isso.



- Clique no certificado ou certificados que você deseja instalar. Todos vocês 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 % &
- Clique Exportar

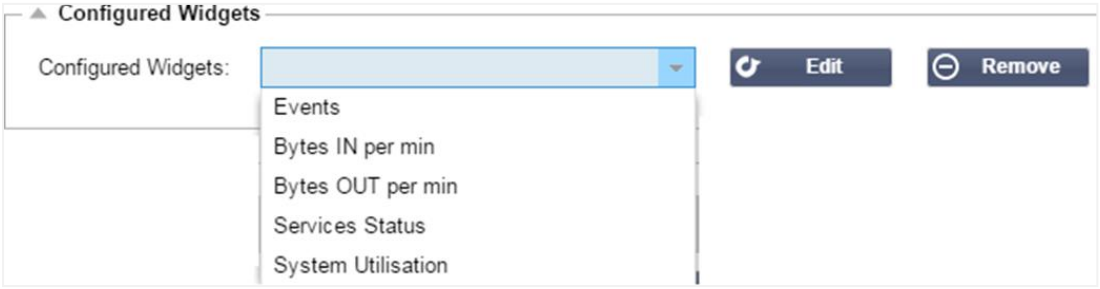
- Quando você estiver exportando um único certificado, o arquivo resultante será denominado sslcert_{certname}.pfx. Por exemplo sslcert_Test1Cert.pfx
- No caso de uma exportação com vários certificados, o arquivo resultante será um arquivo JNBK. O nome do arquivo será sslcert__pack.jnbk.

Nota: Um arquivo JNBK é um arquivo de container criptografado produzido pelo ADC e válido apenas para importação para o ADC

Widgets

A página Biblioteca > Widgets permite que você configure vários componentes visuais leves exibidos em seu painel de controle personalizado.

Widgets configurados

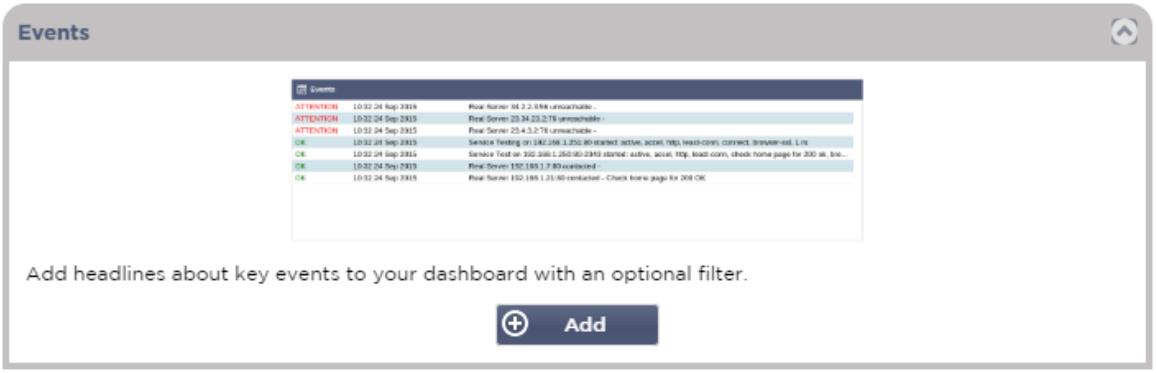


A seção Widgets Configurados permite visualizar, editar ou remover quaisquer widgets criados a partir da seção de widgets disponíveis.

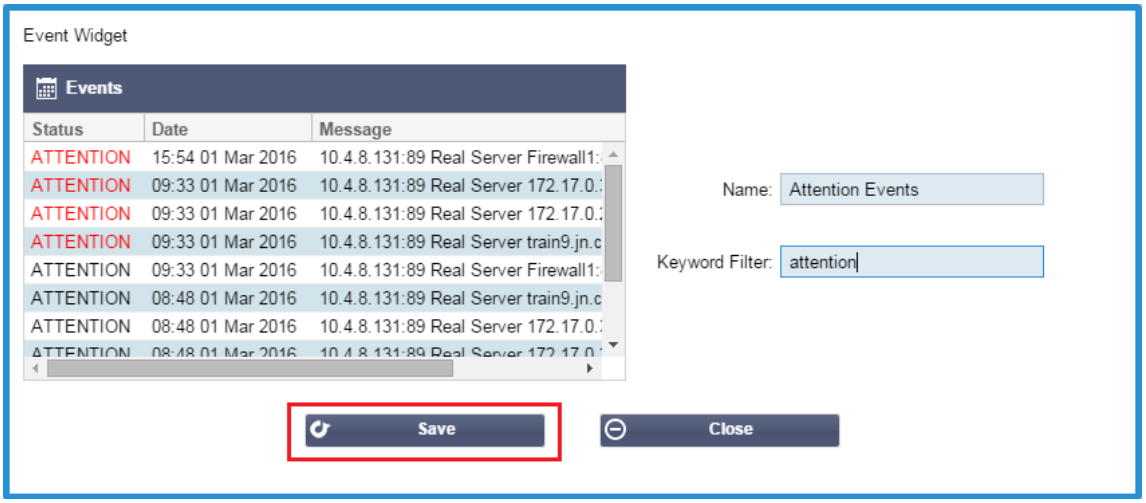
Widgets disponíveis

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

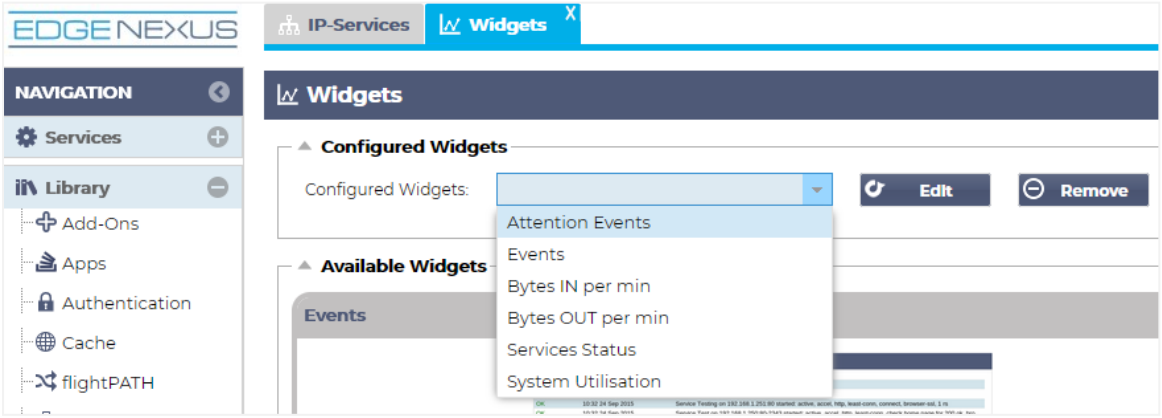
O Widget de Eventos



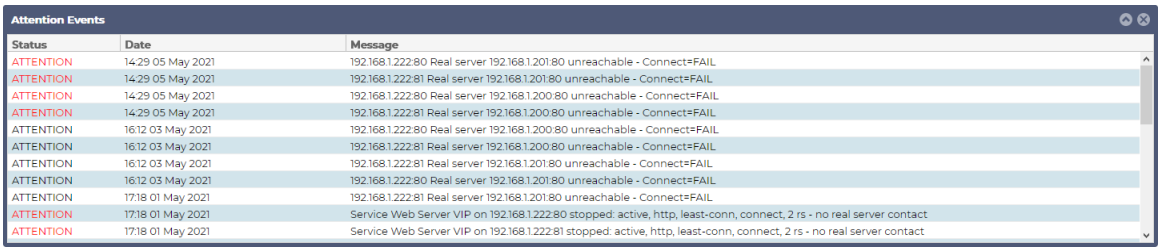
- Para adicionar um evento ao widget Eventos, clique no botão Adicionar.
- Forneça um nome para seu evento. Em nosso exemplo, acrescentamos Eventos de Atenção como o nome do evento.
- Acrescentar um filtro de palavras-chave. Também adicionamos o valor do filtro de Atenção



- Clique em Salvar, depois Fechar
- Você verá agora um Widget adicional chamado Eventos de Atenção no menu suspenso Widgets Configurados.

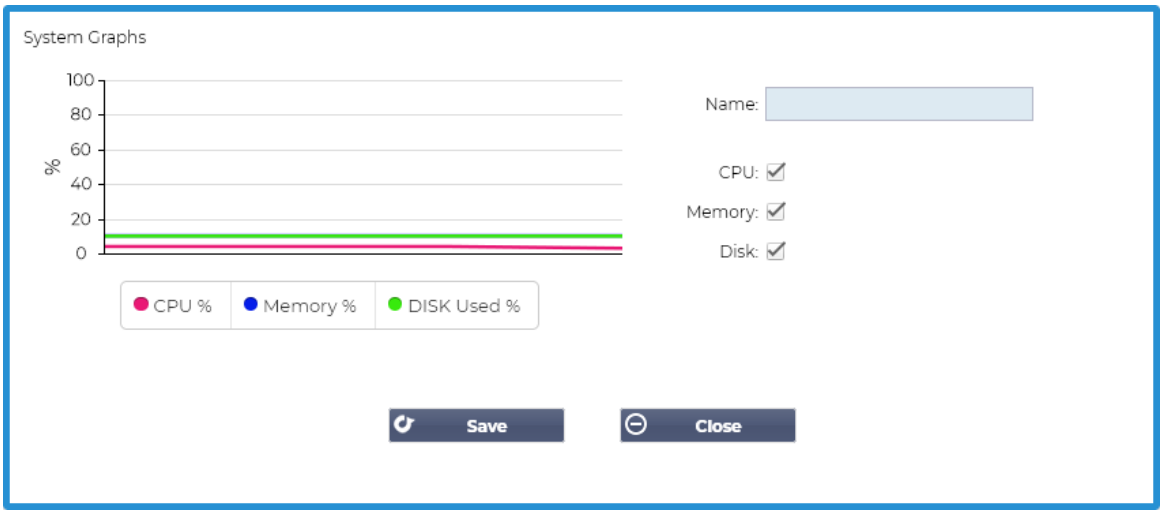


- Você pode ver que agora adicionamos este widget na seção View > Dashboard.
- Selecione o widget Atenção Eventos para exibir isto dentro do Painel de Controle. Veja abaixo.



Você também pode pausar e reiniciar a alimentação de dados ao vivo clicando no botão Pausar dados ao vivo. Além disso, você pode voltar ao painel padrão a qualquer momento clicando no botão Painel de Controle Padrão.

O sistema de gráficos Widget

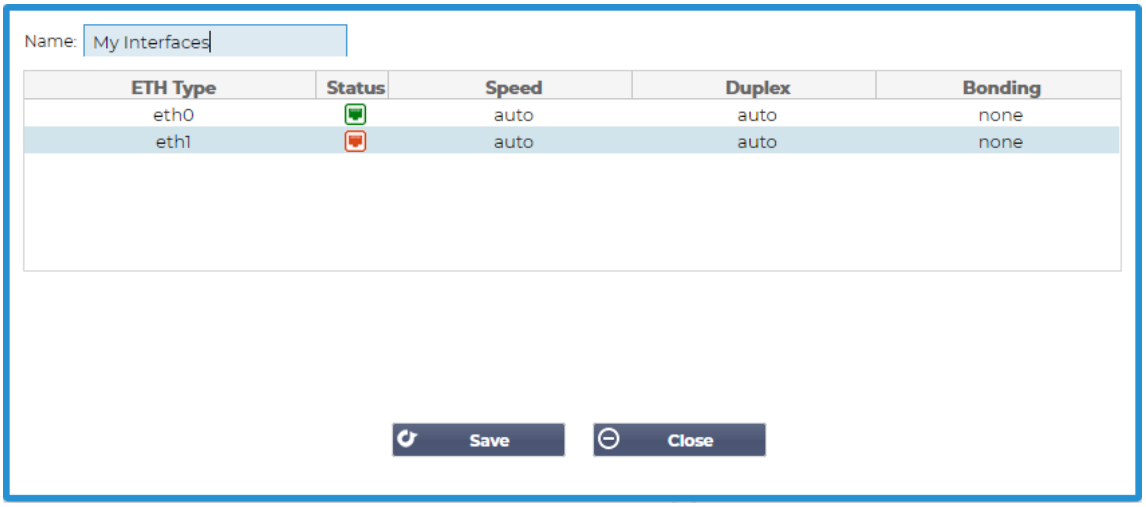


O ADC tem um widget de Gráfico de Sistema configurável. Ao clicar no botão Adicionar no widget, você pode adicionar os seguintes gráficos de monitoramento a serem exibidos.

- CPU
- MEMÓRIA
- DISCO

Uma vez adicionados, eles estarão disponíveis individualmente dentro do menu widget do Painel de Controle.

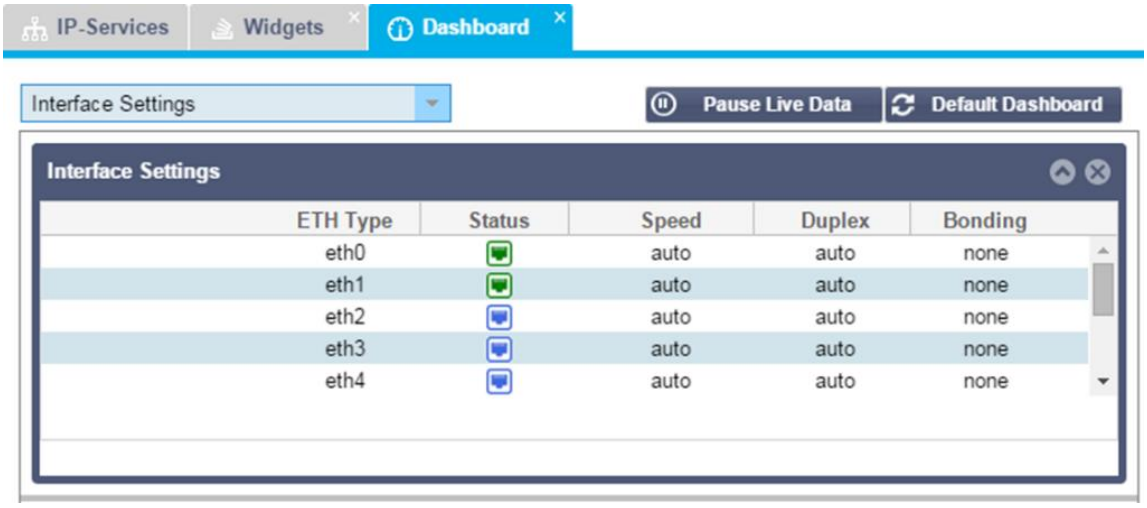
Interface Widget



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

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

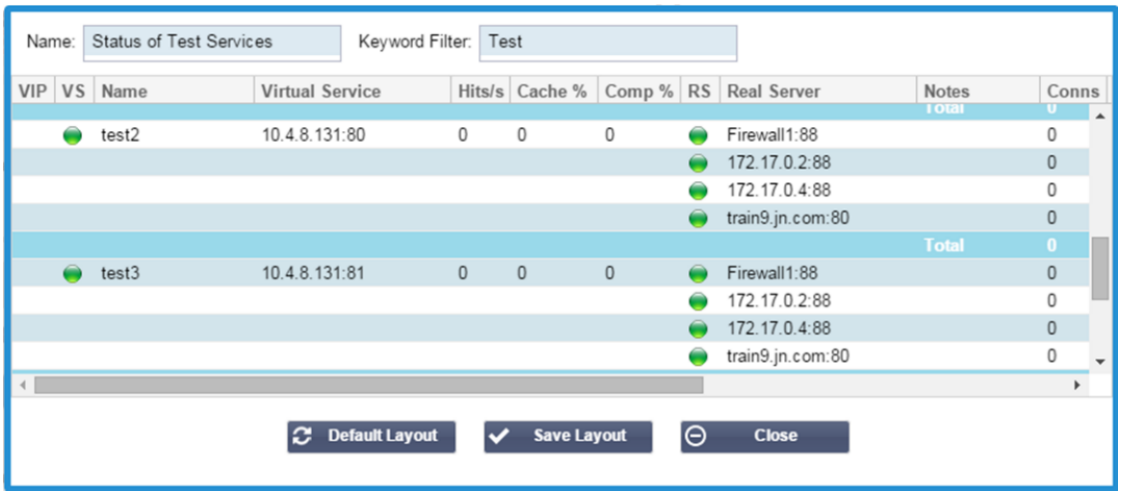
Selecione o Widget que você acabou de personalizar a partir do menu suspenso widget dentro do Painel. Você verá uma tela como a que se encontra abaixo.



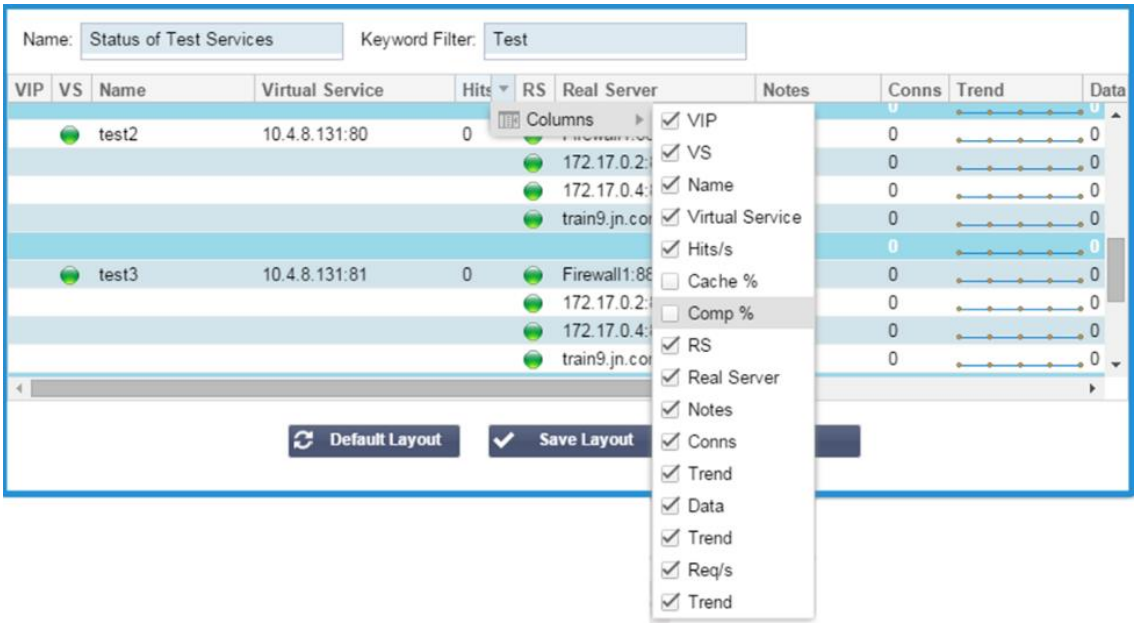
Widget de status

O widget Status permite que você veja o balanceamento de carga em ação. Você também pode filtrar a visualização para mostrar informações específicas.

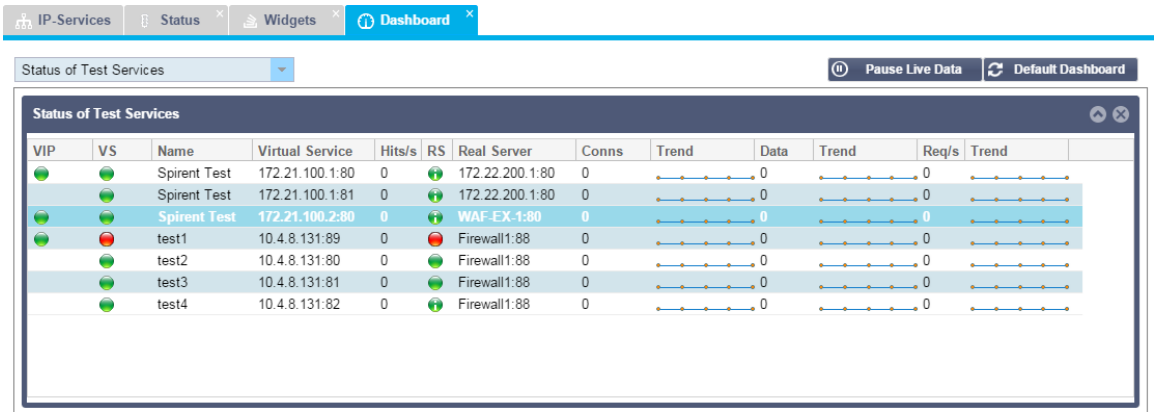
- Clique em Adicionar.



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

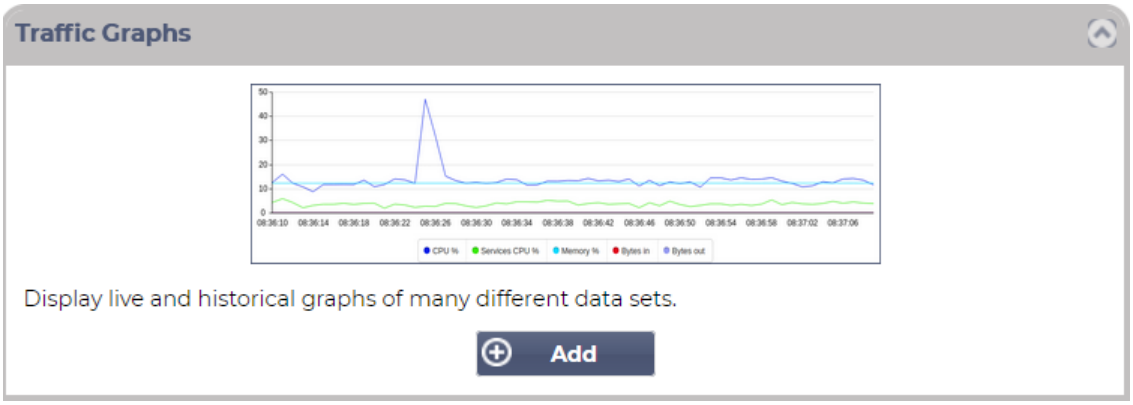


- Quando estiver satisfeito, clique em Salvar, seguido de Fechar.
- O widget Status escolhido estará disponível na seção Painel de Controle.



Widget gráfico de tráfego

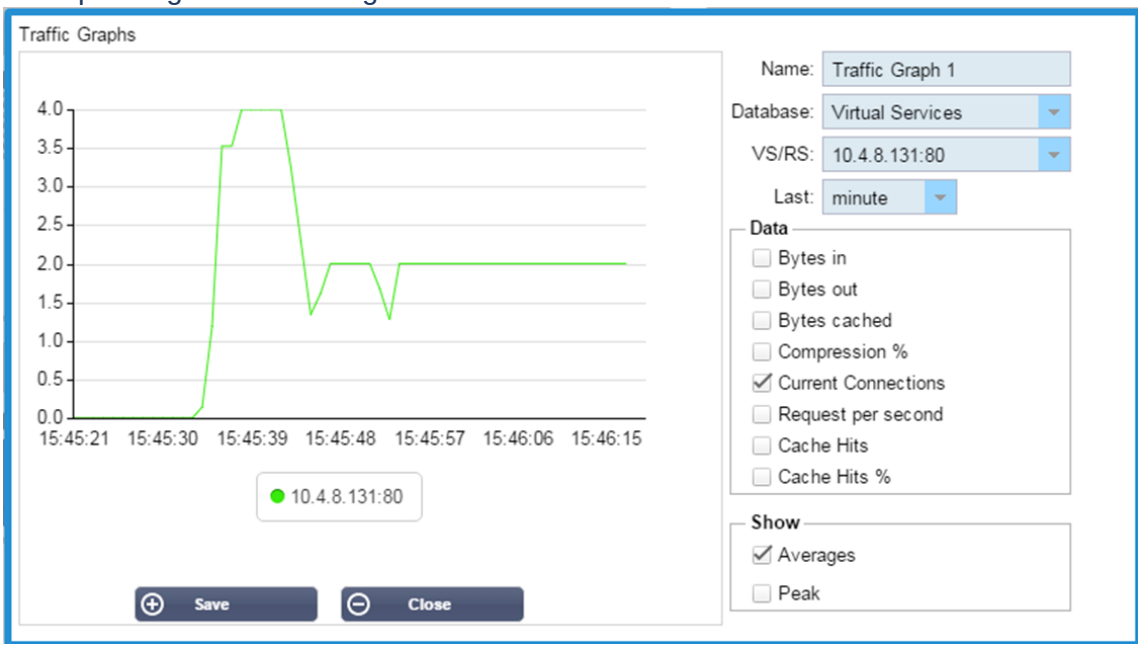
Este widget pode ser configurado para mostrar dados de tráfego atuais e históricos por Serviços Virtuais e Servidores Reais. Além disso, você pode ver os dados gerais atuais e históricos para o tráfego global



- Clique no botão Adicionar
- Dê um nome ao seu widget.
- Escolha um Banco de Dados de Serviços Virtuais, Servidores Reais, ou Sistema.
- Se você escolher Serviços Virtuais, você pode selecionar um serviço virtual a partir do menu suspenso VS/RS.

- Escolha um período de tempo a partir da última gota para baixo.
  - Minuto - 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 para fora
  - Bytes em cache
  - Compressão %
  - Conexões atuais
  - Pedidos por segundo
  - Acertos de Cache
  - Cache Hits %
- Servidores reais
  - Bytes em
  - Bytes para fora
  - Conexões atuais
  - Pedido por segundo
  - Tempo de resposta
- Sistema
  - CPU %
  - Serviços CPU
  - Memória
  - Disco livre
  - Bytes em
  - Bytes para fora
- Escolhido para mostrar valores Médios ou de Pico
- Depois de escolher todas as opções, clique em Salvar e Fechar

Exemplo de gráfico de tráfego



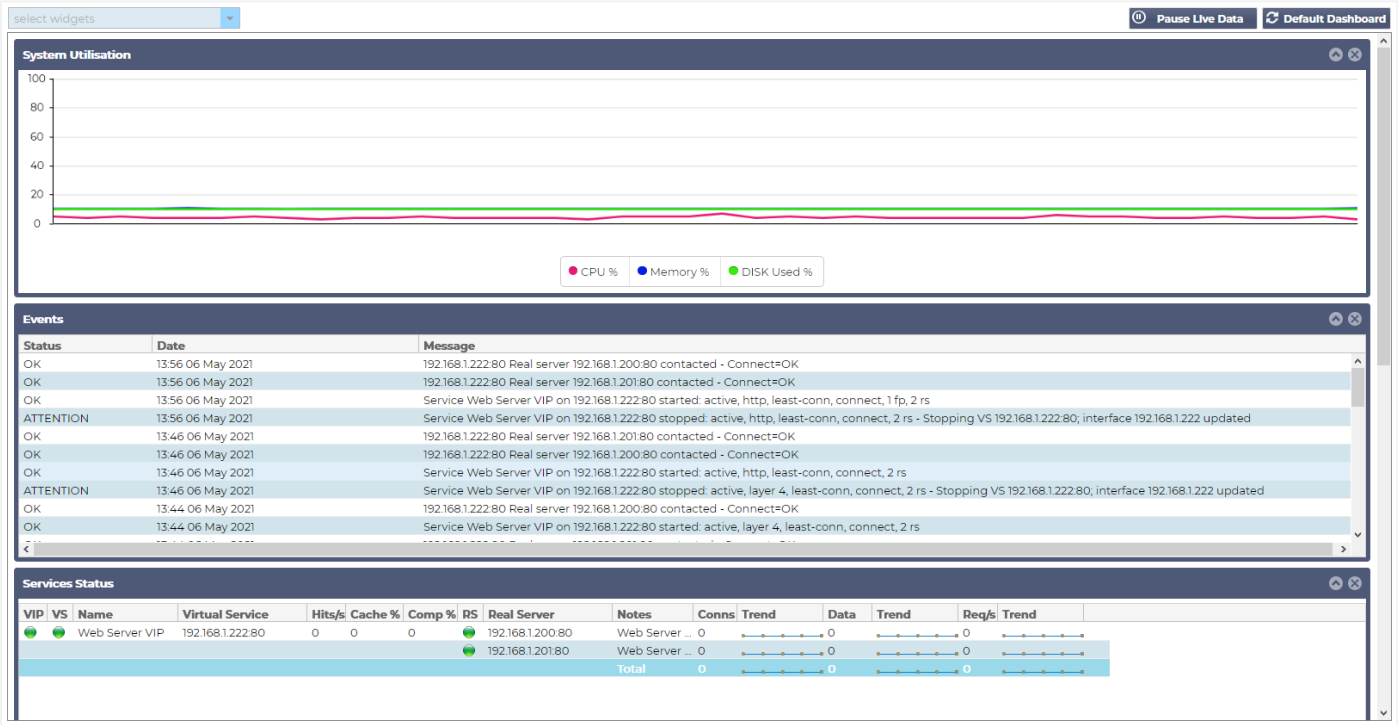
Agora você pode adicionar seu widget Gráfico de Tráfego ao View > Dashboard.

Ver

Painel de controle

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

O Painel é acessível utilizando o segmento View do painel do navegador. Quando selecionado, ele mostra vários widgets padrão e permite que você escolha qualquer um personalizado que você tenha definido.



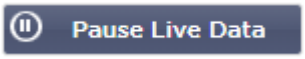
Uso do painel de instrumentos

Há quatro elementos no Painel 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 permite selecionar e adicionar qualquer widget padrão ou personalizado que você tenha definido. Para usar isto, selecione o widget a partir do menu suspenso.

Botão Pausar Dados ao Vivo



Este botão permite que você 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 que você examine o conteúdo a seu gosto. O botão muda de estado para exibir Play Live Data quando uma pausa é iniciada.

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

Botão Default Dashboard

Pode vir a ser que você deseje redefinir o layout do Painel de Controle para o padrão. Nesse caso, pressione o botão Default Dashboard. Uma vez clicado, todas as alterações feitas no Painel serão perdidas.

Redimensionamento, minimização, reordenação e remoção de widgets

Redimensionamento de um Widget

Você 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 de Controle. Você verá um retângulo pontilhado que representa o novo tamanho do widget. Solte o widget dentro do retângulo e solte o botão do mouse. Se você desejar soltar um widget redimensionado ao lado de um widget redimensionado anteriormente, você verá o retângulo aparecer ao lado do widget que deseja soltar ao lado.

Minimizando um Widget

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

Pedido de Widget móvel

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

Removendo um Widget

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

História

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

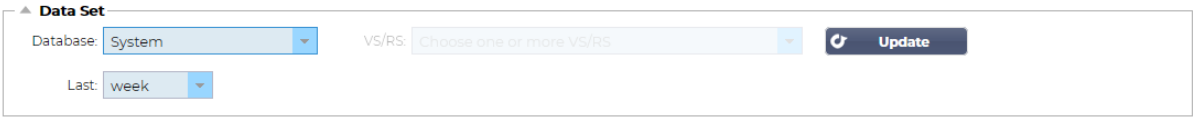
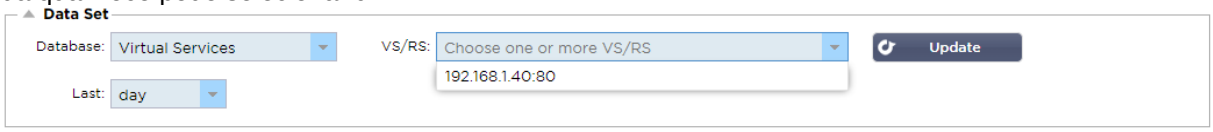
Também permite que você veja o balanceamento de carga em ação e ajuda a detectar quaisquer erros ou padrões que precisem ser investigados. Observe que você deve habilitar o registro histórico em Sistema > Histórico para fazer uso deste recurso.

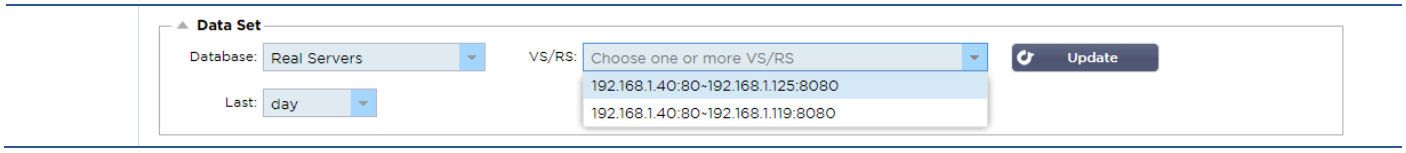
Visualização de dados gráficos

Conjunto de dados

Para visualizar os dados históricos em formato gráfico, favor proceder como a seguir:

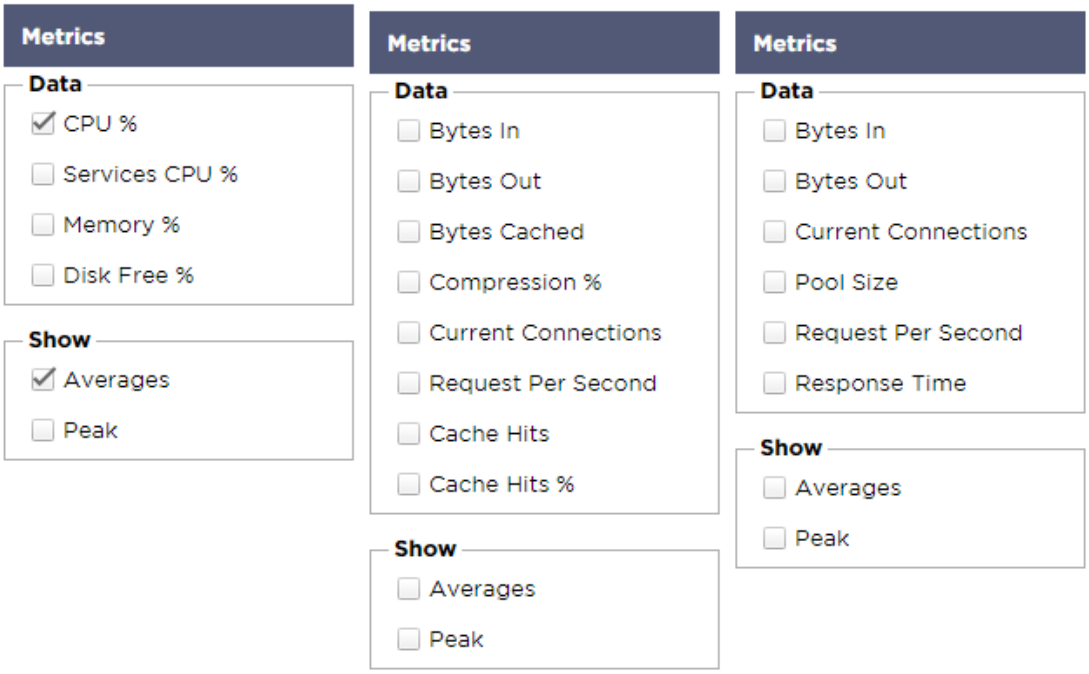
O primeiro passo é escolher o banco de dados e o período relevante para as informações que você deseja visualizar. O período que você pode selecionar no último menu suspenso é Minuto, Hora, Dia, Semana, Mês e Ano.

Base de dados	Descrição
Sistema	A seleção deste banco de dados permitirá que você veja a CPU, a memória e o espaço da unidade de disco ao longo do tempo 
Serviços virtuais	A seleção deste banco de dados permitirá que você escolha todos os serviços virtuais do banco de dados a partir de quando você começou a registrar os dados. Você verá uma lista de Serviços Virtuais da qual você pode selecionar um. 
Serviços reais	A seleção deste banco de dados permitirá que você escolha todos os Servidores Reais no banco de dados a partir de quando você começou a registrar os dados. Você verá uma lista de Servidores Reais da qual você pode selecionar um.

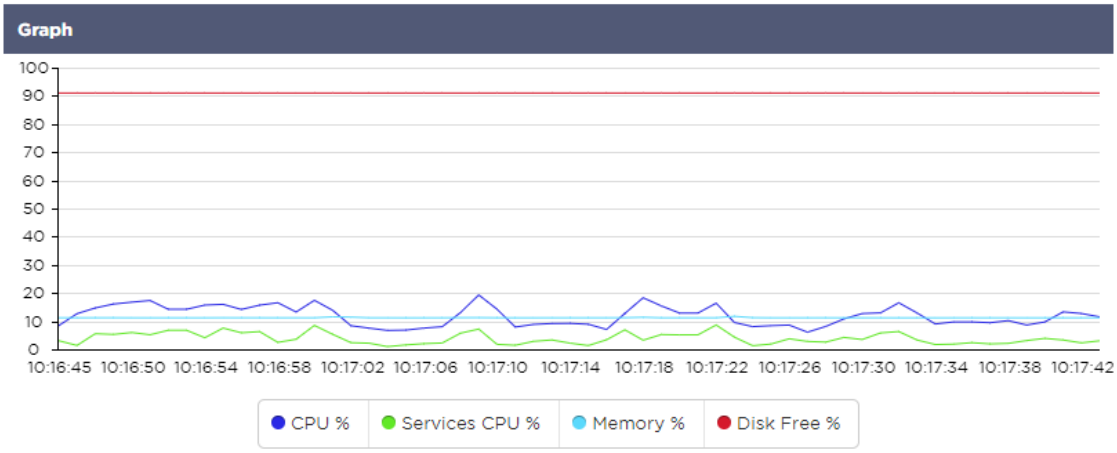


Métricas

Uma vez selecionado o Conjunto de Dados que você utilizará, é hora de escolher a Métrica que você deseja exibir. A imagem abaixo ilustra as métricas disponíveis para seleção pelo administrador: estas seleções correspondem a System, Virtual services e Real Servers (da esquerda para a direita).



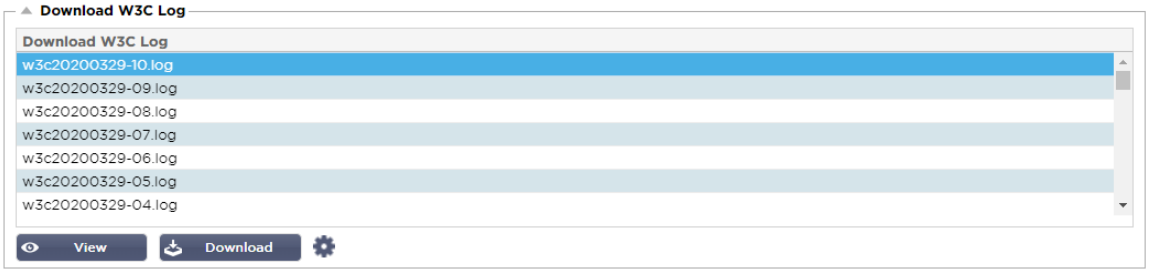
Exemplo de gráfico



Logs

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

Baixar logs do W3C



O registro W3C é habilitado na seção Sistema > Registro de dados. Um registro W3C é um registro de acesso para servidores Web no qual são gerados arquivos de texto contendo dados sobre cada solicitação de acesso, incluindo o endereço IP (Internet Protocol de origem), a versão HTTP, o tipo de navegador, a página de referência e o carimbo da hora. Os logs do W3C podem tornar-se muito grandes, dependendo da quantidade de dados e da categoria do log que está sendo registrado.

A partir da seção W3C, você pode selecionar o log que você precisa e depois visualizá-lo ou baixá-lo.

Ver Botão

O botão View permite visualizar o log escolhido dentro da janela do editor de texto, como o Bloco de Notas.

Botão de Download

Este botão permite que você faça o download do log para seu armazenamento local para visualização posterior.

O Ícone Cog

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

Estatísticas

A seção Estatísticas do ADC é uma área muito utilizada pelos administradores de sistemas que querem garantir que o desempenho do ADC esteja no mesmo nível de suas expectativas.

Compressão

O objetivo do ADC é monitorar os dados e direcioná-los para 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; estes 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 no conteúdo compressivo. Um valor de 60-80% é o que chamaríamos como típico

Compressão geral até o momento

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 atingiu 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 valores 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 Acertos e conexões contém as estatísticas gerais de acertos e transações que passam através do ADC. Então, o que significam os hits e conexões?

- Um acerto é definido como uma transação de Camada 7. Tipicamente usado para servidores web, este é um pedido 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.

Acertos totais contados

Os números dentro desta seção mostram o número cumulativo de acessos não armazenados em cache desde o último reset. No lado direito, a figura mostrará o número atual de hits por segundo.

Conexões totais

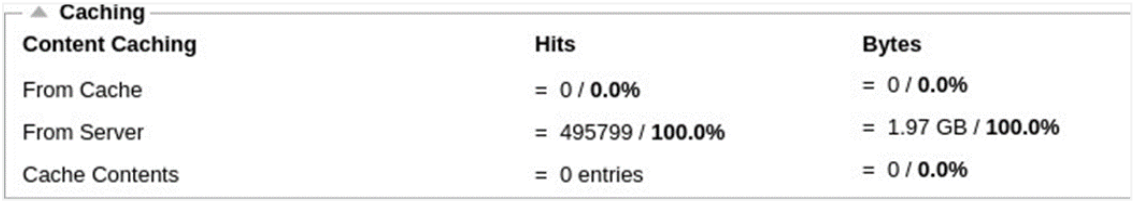
O valor Total de Conexões representa o número cumulativo de conexões TCP desde o último reset. A figura na segunda coluna indica as conexões TCP feitas por segundo para o ADC. O número na coluna do lado direito é o número de conexões TCP por segundo feitas aos Servidores Reais. Exemplo 6/8 conexões/segundo. 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 você deve se lembrar, o ADC está equipado tanto com compressão quanto com caching. Esta seção mostra as estatísticas gerais relacionadas ao caching quando aplicado a um canal. Se o cache não tiver sido aplicado a um canal e configurado corretamente, você verá 0 conteúdo de 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 fornece 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 fornece a quantidade total de dados em Kilobytes servidos a partir do cache do ADC. Uma porcentagem dos dados totais também é fornecida.

Do servidor

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

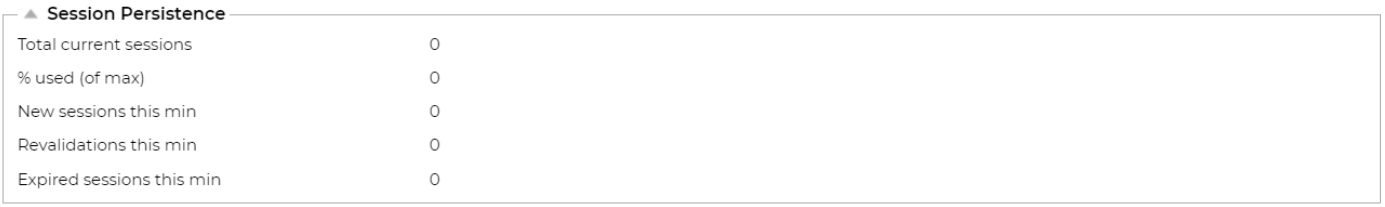
Bytes: A segunda coluna fornece a quantidade total de dados em Kilobytes servidos a partir dos Servidores Reais. Uma porcentagem dos dados totais também é fornecida.

Conteúdo do Cache

Acertos: Este 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 Persistência da sessão fornece informações para vários parâmetros.

Campo	Descrição
Total das sessões atuais	Isto mostra quantas sessões de persistência estão em andamento - atualizadas a cada minuto
% Utilizado (do máximo)	Isto mostra quanto uso há 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 esta min	Isto mostra, no último minuto, quantas sessões de persistência existentes expiraram devido a não haver mais tráfego dentro do tempo limite.

Hardware

Quer você esteja utilizando o ADC em um ambiente virtual ou dentro do hardware, esta seção lhe fornecerá informações valiosas sobre o desempenho do aparelho.

Hardware

Disk Usage	= 22%
Memory Usage	= 18.9%(277.5MB of 1465.1MB)
CPU Usage	= 11.0%

Uso do disco

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

Uso da memória

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

Utilização da CPU

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

Status

A página View > Status exibe o tráfego ao vivo que atravessa o ADC para os Serviços virtuais que você definiu. Também mostra o número de conexões e dados para cada Servidor Real para que você possa experimentar o balanceamento de carga em tempo real.

Detalhes do Serviço Virtual

Virtual Service Details

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 um "passivo" está se segurando por um "ativo".
●	Fora de linha. Os servidores reais são inacessíveis, ou nenhum servidor real está habilitado
●	Encontrar o status
●	IPs virtuais não licenciados ou licenciados 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 um "passivo" está se segurando por um "ativo".
●	O serviço precisa de atenção. Esta indicação de status pode resultar de um servidor real falhar em um monitor de saúde ou ter sido alterado manualmente para fora de linha. O tráfego continuará a fluir mas com capacidade reduzida do Servidor Real.
●	Fora de linha. Os servidores reais são inacessíveis, ou nenhum servidor real está habilitado
●	Encontrar o status
●	IPs virtuais não licenciados ou licenciados excedidos

Nome

O nome do Serviço Virtual

Serviço Virtual (VIP)

O endereço IP Virtual e a porta para o serviço e os usuários de endereço ou aplicações usarão.

Golpe/segundo

Transações de camada 7 por segundo no lado do cliente.

Cache%

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

Compressão%

Esta figura representa a porcentagem de objetos que foram comprimidos entre o cliente e o ADC.

RS Status (Servidor Remoto)

A tabela abaixo descreve o significado do status dos Servidores Reais vinculados ao VIP.

Status	Descrição
●	Conectado
●	Não monitorado
●	Drenagem ou fora de linha
●	Aguarde
●	Não Conectado
●	Encontrar o status
●	IPs virtuais não licenciados ou licenciados excedidos

Servidor Real

O endereço IP e a porta do Real Server.

Notas

Este valor pode ser qualquer nota útil para que outros entendam o propósito da entrada.

Conns (Conexões)

Representar o número de conexões a cada Servidor Real permite que você veja o balanceamento de carga em ação. Muito útil para verificar se sua política de balanceamento de carga está funcionando corretamente.

Dados

O valor nesta coluna mostra a quantidade de dados sendo enviada para cada Servidor Real.

Req/Sec (Pedidos por segundo)

O número de solicitações por segundo enviadas a cada Servidor Real.

Sistema

O segmento Sistema da interface de usuário do ADC permite que você acesse e controle todos os aspectos do sistema do ADC.

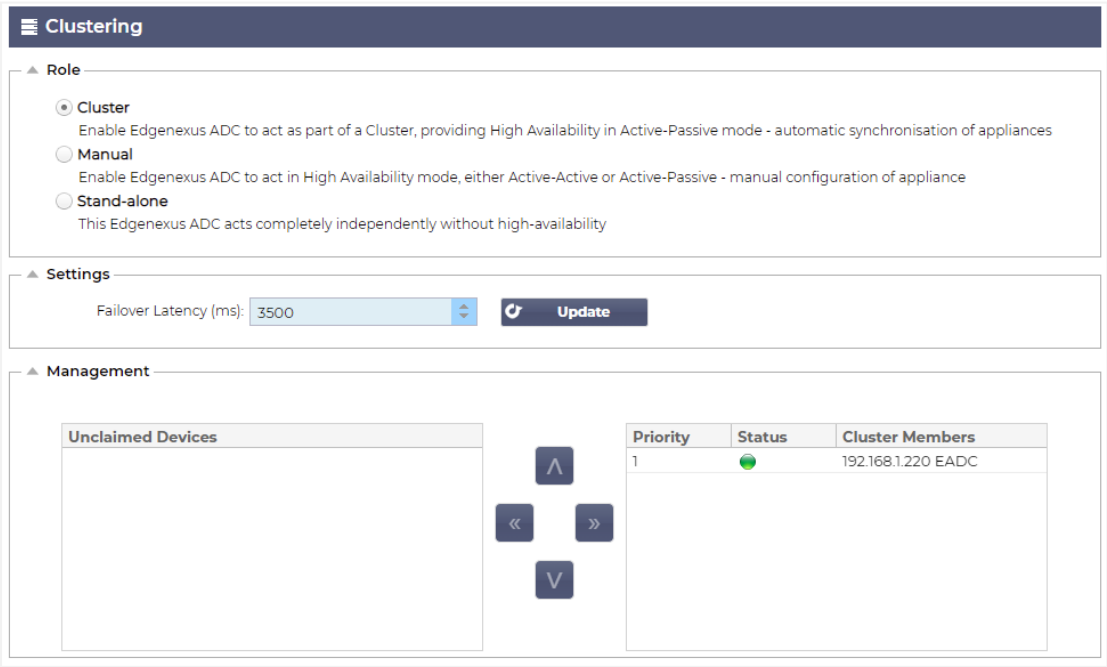
Clustering

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 torna-se aparente. O projeto do ADC de fácil navegação da interface de usuário torna a configuração do sistema de cluster simples.

A página Sistema > Clustering é onde você irá configurar a alta disponibilidade de seus aparelhos ADC. Esta seção está organizada em várias seções.

Nota importante

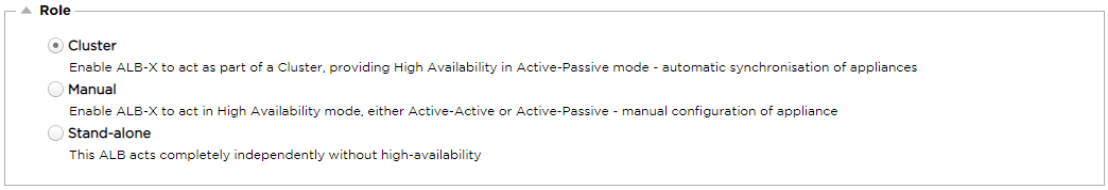
- Não há nenhuma exigência de um cabo dedicado entre o par ADC para manter um batimento cardíaco de alta disponibilidade.
- O batimento cardíaco ocorre na mesma rede que o Serviço Virtual que requer alta disponibilidade para ser implantado.
- Não há falhas de estado entre os aparelhos do ADC.
- Quando houver alta disponibilidade em dois ou mais ADC's, cada caixa transmitirá via UDP os Serviços Virtuais que está configurada para fornecer.
- O fail-over de alta disponibilidade utiliza mensagens unicast e ARP Gratuito para informar os novos interruptores balanceadores de carga ativos.



Papel

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

Cluster



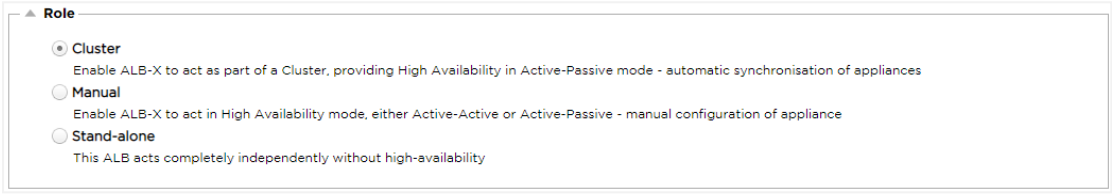
- Por padrão, um novo ADC irá alimentar o uso do papel de Cluster. Nesta função, cada membro do Cluster terá a mesma "configuração funcional" e, como tal, somente um ADC no Cluster estará ativo a qualquer momento.
- Uma "configuração funcional" significa todos os parâmetros de configuração, exceto itens que precisam ser únicos, tais como o endereço IP de gerenciamento, nome ALB, configurações de rede, detalhes da interface, etc.
- 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.
- Você pode editar qualquer ADC no Cluster, e as mudanças serão sincronizadas com todos os membros do Cluster.
- Quando você remove um ADC do Cluster, todos os Serviços Virtuais serão excluídos desse ADC.
- Você não pode remover o último membro do Cluster para dispositivos não reclamados. Para remover o último membro, favor mudar a função para Manual ou Autônomo.
- Os seguintes objetos não estão sincronizados:
    - Seção Manual de Data e Hora - (A seção NTP é sincronizada)
    - Latência de Failover (ms)
    - Seção de ferragens
    - Seção de eletrodomésticos
    - Seção de rede

Falha do Proprietário do Cluster

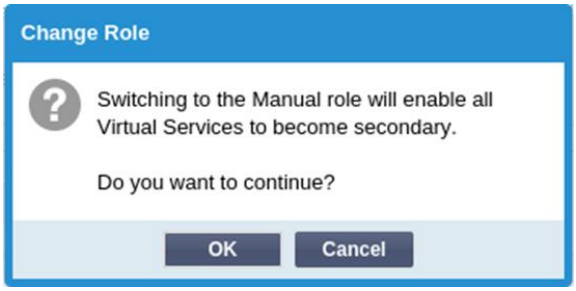
- Quando um proprietário de um cluster falha, um dos membros restantes assumirá automaticamente o controle e continuará equilibrando a carga do tráfego.
- Quando o proprietário do cluster retornar, ele retomará o tráfego de balanceamento de carga e assumirá o papel de proprietário.
- Vamos supor que o Proprietário falhou e que um Membro assumiu o equilíbrio de carga. Se você gostaria que o Membro que assumiu o tráfego de balanceamento de carga se tornasse o novo proprietário, destaque o membro e clique na seta para cima para movê-lo para a posição de Prioridade 1.
- Se você editar um dos membros restantes do cluster e o proprietário estiver em baixa, o membro editado se promoverá automaticamente para o proprietário sem perda de tráfego

Mudança do papel do Cluster para o papel manual

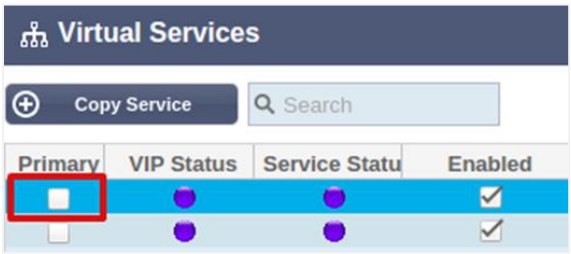
- Se você deseja mudar a função de Cluster para Manual, clique no botão de rádio ao lado da opção Função Manual



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



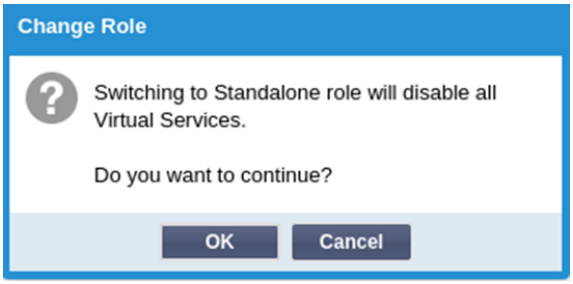
- Clique no botão OK
- Verifique a seção de Serviços Virtuais. Você verá que a coluna primária agora mostra uma caixa desmarcada.



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

Mudando o papel de Cluster para Stand-alone

- Se você deseja mudar o papel de Cluster para Autônomo, clique no botão de rádio ao lado da opção Autônomo.
- Você será avisado com a seguinte mensagem:



- Clique em OK para mudar de função.
- Verifique seus Serviços Virtuais. Você verá que a coluna primária muda o nome para Stand-alone
- Você verá também que todos os Serviços Virtuais estão desativados (não colados) por razões de segurança.
- Quando você estiver confiante de que nenhum outro ADC na mesma rede tem serviços virtuais duplicados, você pode habilitar cada um deles por sua vez.

Papel Manual

Um ADC no papel do Manual trabalhará com outros ADCs no papel do Manual para proporcionar alta disponibilidade. A principal vantagem sobre o papel de Cluster é a capacidade de definir qual ADC é Ativo para um IP Virtual. A desvantagem é que não há sincronização de configuração entre os ADC's. Quaisquer mudanças devem ser replicadas manualmente em cada caixa através do 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, um serviço Ativo falha no Passivo:

- Se ambas as Colunas Primárias forem assinaladas, então ocorre um processo eleitoral, e o endereço MAC mais baixo estará ativo.
- Se ambos forem desmarcados, então ocorre o mesmo processo eleitoral. Além disso, se ambos forem desmarcados, não haverá uma retirada automática para o ADC Ativo original.

Papel autônomo

Um ADC no papel autônomo não se comunicará com nenhum outro ADC em relação a seus serviços e, portanto, todos os Serviços Virtuais permanecerão no status Verde e conectados. Você deve garantir que todos os Serviços Virtuais tenham endereços IP únicos, ou haverá um conflito em sua rede.

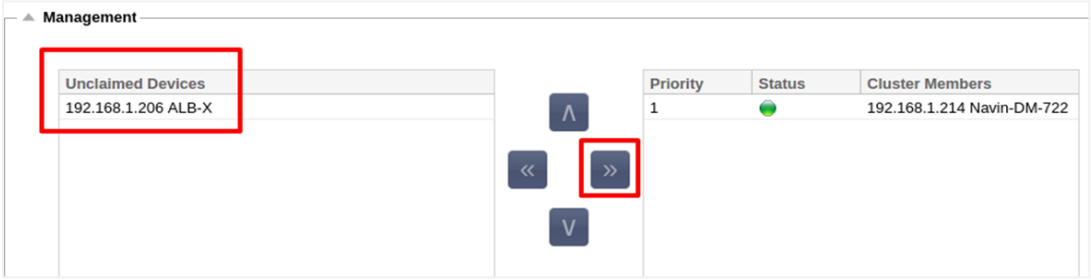
Configurações

Na seção Configurações, você pode definir a Latência de Failover em milissegundos, o tempo que um ADC Passivo esperará antes de assumir os Serviços Virtuais após o ADC Ativo ter falhado.

Recomendamos que você ajuste este valor para 10000ms ou 10 segundos, mas pode diminuir ou aumentar este valor para se adequar à sua rede e às suas necessidades. Os valores aceitáveis caem entre 1500ms e 20000ms. Se você experimentar instabilidade no cluster em uma latência mais baixa, você deve aumentar este valor.

Administração

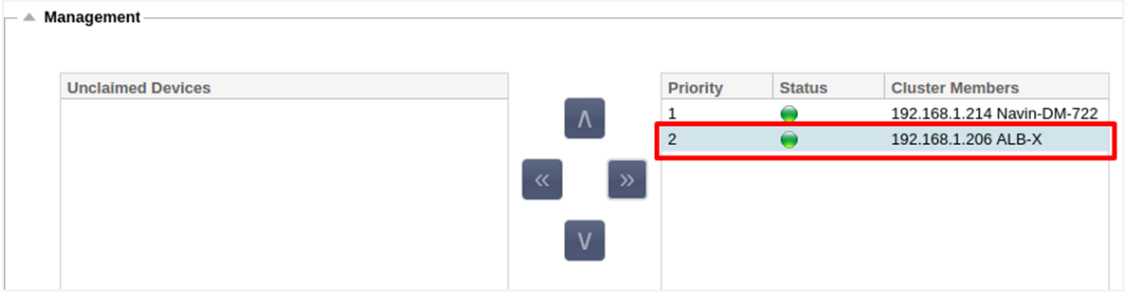
Nesta seção, você pode adicionar e remover membros do cluster e ao mesmo tempo alterar a prioridade de um ADC no cluster. A seção consiste de dois painéis e um conjunto de teclas de seta no meio. A área à esquerda são os Dispositivos não reclamados, enquanto a área mais à direita é o próprio Aglomerado.



Adicionando um ADC ao conjunto

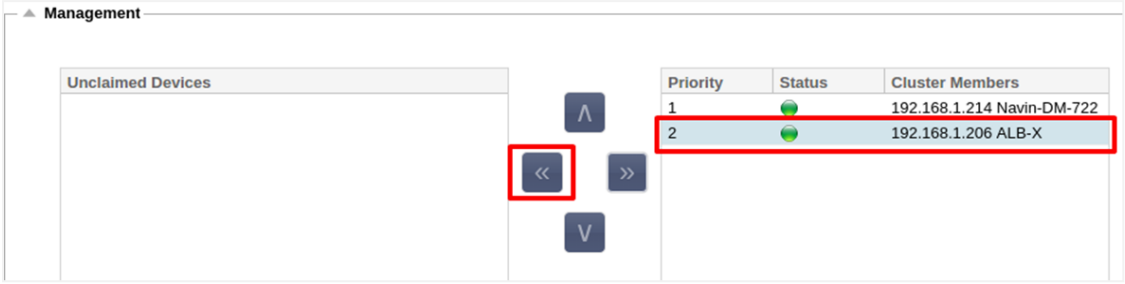
- Antes de adicionar o ADC ao conjunto, você deve se certificar de que todos os aparelhos do ADC tenham sido fornecidos com um nome único definido na seção Sistema > Rede.
- Você deve ver o ADC como Prioridade 1 com status verde e seu nome sob a coluna Membros do Cluster na seção de gerenciamento. Este ADC é o dispositivo primário padrão.
- Todos os outros ADC's disponíveis aparecerão na janela de Dispositivos não reclamados dentro da seção de gerenciamento. Um Dispositivo não reclamado é o ADC que foi designado no Cluster Role, mas não tem serviços virtuais configurados.
- Destaque o ADC a partir da janela Dispositivos não reclamados e clique no botão de seta para a direita.
- Você verá agora a seguinte mensagem:

- Clique OK para promover o ADC para o agrupamento.
- Seu ADC deve agora aparecer como Prioridade 2 na lista de membros do cluster.



Remoção de um membro do cluster

- Destaque o Membro do Cluster que você deseja remover do cluster.
- Clique no botão de seta à esquerda.



- Será apresentado a você um pedido de confirmação.
- Clique OK para confirmar.
- Seu ADC será removido e será mostrado no lado dos dispositivos não reclamados.

Mudando a prioridade de um ADC

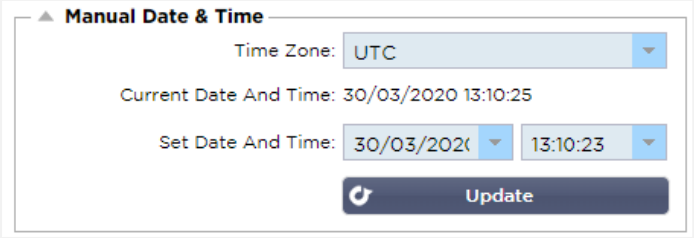
Pode haver ocasiões em que você deseje mudar a prioridade de um ADC dentro da lista de membros.

- 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 ADC que 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, incluindo 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 definido neste campo representa o fuso horário em que o ADC está localizado.

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

Se a Data e Hora ainda estiverem incorretas após a mudança acima, favor alterar a data manualmente.

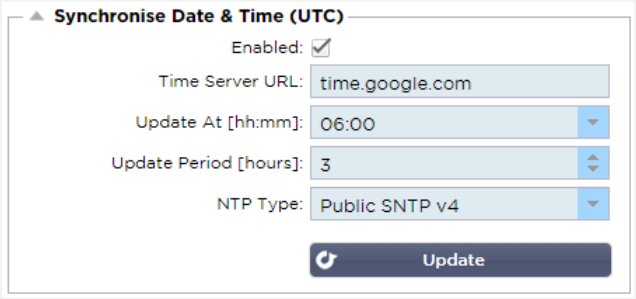
Data e hora definidas

Esta configuração representa a data e a hora reais.

- Escolha a data correta a partir do primeiro drop-down ou,
  alternativamente, você pode digitar a data no seguinte formato DD/MM/AAAA
- Adicione no tempo no seguinte formato hh: mm: ss, por exemplo, 06:00:10 por 6 am e 10 segundos.
- Uma vez que você tenha inserido corretamente, por favor clique em Atualizar para aplicar.
- Você deve então ver a nova Data e Hora em caracteres em negrito.

Sincronizar data e hora (UTC)

Você pode usar servidores NTP para sincronizar sua data e hora com precisão. Os servidores NTP estão localizados globalmente, e você também poderá 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 o horário programado em que você gostaria que o ADC se sincronizasse com o servidor NTP.

Período de atualização [horas]:

Selecione com que freqüência você gostaria que a sincronização ocorresse.

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 - Versão legada do NTP sobre TCP. **RFC 1059**
- NTP v1 sobre UDP - Versão legada do NTP sobre UDP. **RFC 1059**

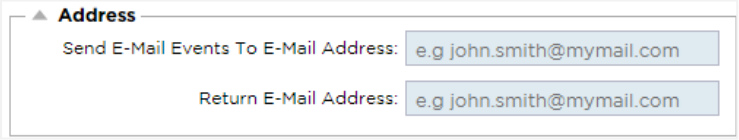
Nota: Favor observar que a sincronização é somente em UTC. Se você deseja definir uma hora local, isto só pode ser feito manualmente. Esta limitação será alterada em versões posteriores para permitir a possibilidade de selecionar um fuso horário.

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 configurar uma conexão de servidor de e-mail e enviar notificações aos administradores do sistema. A página está organizada nas seções abaixo.

Endereço



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

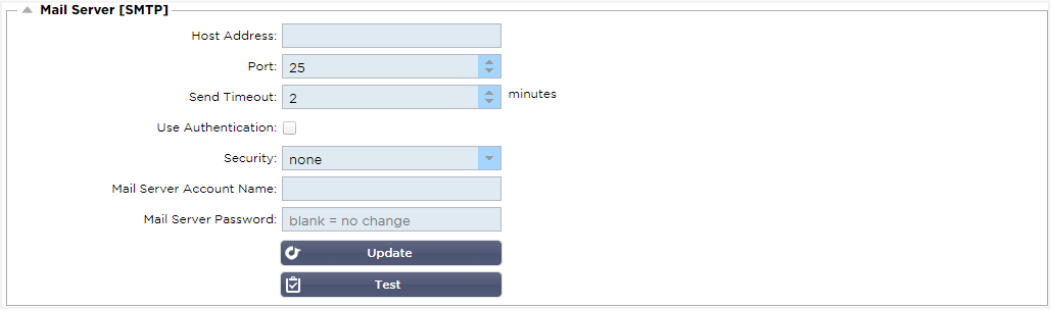
Adicione um endereço de e-mail válido para enviar os alertas, notificações e eventos. Exemplo support@domain.com. Você também pode adicionar vários endereços de e-mail usando um separador de vírgulas.

Endereço de e-mail de retorno:

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

Servidor de correio (SMTP)

Nesta seção, você deve adicionar os detalhes do servidor SMTP a ser usado para enviar os e-mails. Por favor, certifique-se de que o endereço de e-mail que você usa para o envio esteja autorizado a fazê-lo.



Endereço do anfitrião

Adicione no endereço IP do seu servidor SMTP.

Porto

Adicione no Porto de seu servidor SMTP. A porta padrão para SMTP é 25 ou 587 se você usar SSL.

Tempo limite de envio

Acrescente em um tempo limite SMTP. O tempo padrão está definido para 2 minutos.

Autenticação de uso

Assinale a caixa se seu servidor SMTP requer autenticação.

Segurança

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

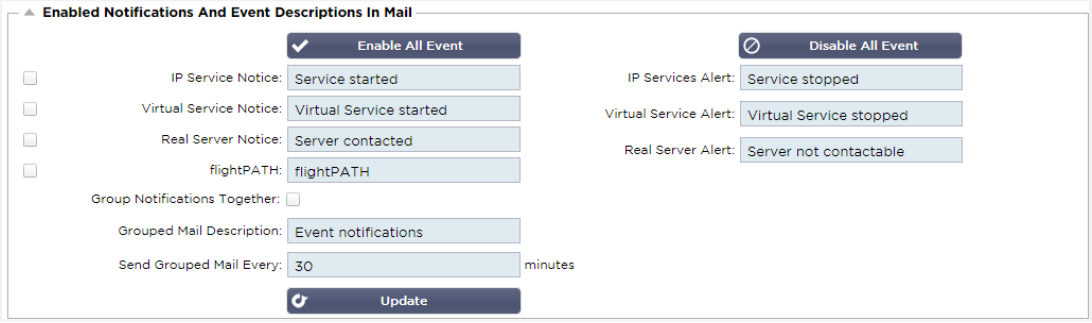
Nome da conta do servidor principal

Adicionar o nome de usuário necessário para a autenticação.

Senha do servidor de correio

Adicionar a senha necessária para a autenticação.

Notificações e alertas



Há vários tipos de notificações de eventos que o ADC enviará às pessoas configuradas para recebê-las. Você 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 IP

O aviso de Serviço IP o informará quando qualquer endereço IP Virtual estiver online ou tiver parado de funcionar. Esta ação é realizada para todos os serviços Virtuais que pertencem ao VIP.

Serviço Virtual

Informa ao destinatário que um Serviço Virtual está online ou que parou de funcionar.

Servidor Real

Quando uma Real Sever e Porta está conectada ou não é contatável, o ADC enviará o aviso de Servidor Real.

flightPATH

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

Notificações de grupo

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

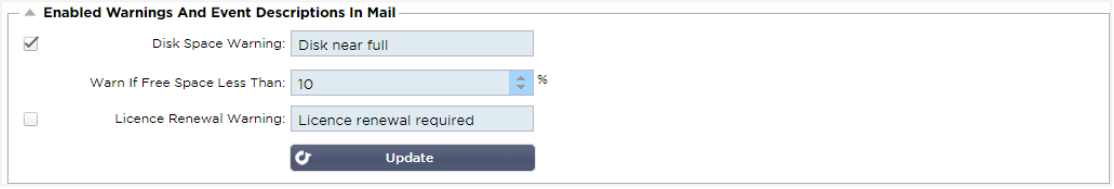
Descrição do correio do grupo

Especifique o assunto relevante para o e-mail de notificação de grupo.

Intervalo de envio do grupo

Estipular o tempo que você 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

Defina a porcentagem de espaço livre em disco antes da qual o aviso é enviado. Quando isto for alcançado, você será enviado por e-mail.

Validade da Licença

Esta configuração permite ativar ou desativar o e-mail de aviso de expiração da licença enviado ao administrador do sistema. Quando isto for alcançado, você será enviado por e-mail.

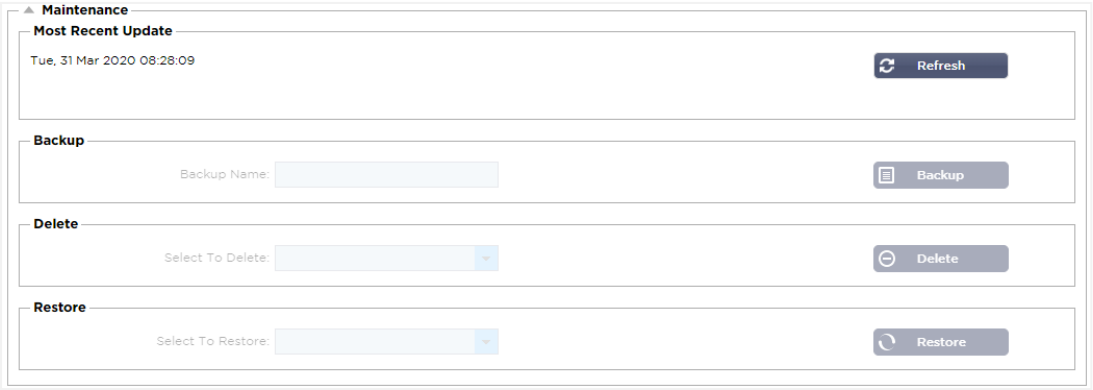
Histórico do sistema

Na seção Sistema, há a opção Histórico do Sistema, permitindo a entrega de dados históricos para elementos como CPU, memória, solicitações por segundo e outras características. Uma vez ativado, você pode visualizar os resultados em forma gráfica através da página View > History. Esta página também permitirá que você faça backup ou restaure seus arquivos de histórico para o ADC local.

Coleta de dados

- Para permitir a coleta de dados, assinale a caixa de seleção.
- Em seguida, defina o intervalo de tempo no qual você deseja que o ADC colete os dados. Este valor de tempo pode variar entre 1-60 segundos.

Manutenção



Esta seção será desativada se você tiver ativado 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 um nome descritivo ao seu backup. Clique em Backup para fazer o backup de todos os arquivos para o ADC

Excluir

Selecione um arquivo de backup a partir da lista suspensa. Clique em Excluir para remover o arquivo de backup do ADC

Restaurar

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

Licença

O ADC é licenciado para uso em um dos seguintes modelos, o que depende de seus parâmetros de compra e tipo de cliente.

Tipo de licença	Descrição
Perpétuo	Você, o cliente, tem o direito de usar o ADC e outros softwares perpetuamente. Isso não impede que você tenha que adquirir suporte para receber assistência e atualizações.
SaaS	SaaS ou Software-as-a-Service significa essencialmente que você aluga o software de forma contínua ou pague o que quiser. Neste modelo, você paga um aluguel anual pelo software. Você não tem direitos perpétuos para usar o software.
MSP	Os Provedores 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.

Licence Details

Licence ID:	EA5325D4-[illegible]
Machine ID:	F[illegible]C5
Issued To:	edgeNEXUS
Contact Person:	Greg Howett
Date Issued:	24 Nov 2020
Name:	Sergey Box

Identificação da licença

Esta ID de licença está diretamente ligada à ID da máquina e a outros detalhes específicos de sua compra e do ADC. Esta informação é essencial e é necessária quando você deseja recuperar atualizações e outros itens da App Store.

Identificação da máquina

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

Nota: Você não deve alterar o endereço IP ou o MAC ID de seus aparelhos ADC. Se você estiver em uma estrutura virtualizada, então, por favor, conserte o MAC ID e o endereço IP.

Emitido para

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

Pessoa de contato

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

Data Emissões

A data em que a licença foi emitida

Nome

Este valor mostra o nome descritivo do aparelho da ADC que você forneceu.

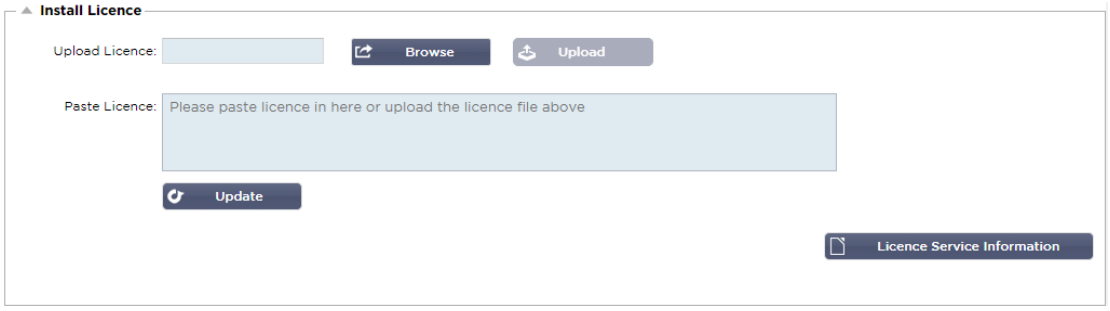
Instalações

Facilities

Layer 4:	Permanent licence
Layer 7:	Permanent licence
SSL:	Permanent licence
Acceleration:	Permanent licence
flightPATH:	Permanent licence
Pre-Authentication:	Permanent licence
Global Server Load-Balancing:	Timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Firewall:	Timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Throughput:	3 Gbps permanent licence Unlimited timed licence: 6 days(06 Apr 2020) Quote: 50E-FF43-379
Virtual Service IPs:	32 Virtual Service IPs permanent licence
Real Server IPs:	120 Real Server IPs permanent licence

A seção de instalações fornece informações sobre quais funções dentro do ADC foram licenciadas para uso e a validade da licença. Também é exibida a produtividade que foi licenciada para o ADC e o número de Servidores Reais. Estas informações dependem da licença que você adquiriu.

Instalar Licençase



- A instalação de uma nova licença é muito simples. Quando você receber sua nova licença ou licença de substituição da Edgenexus, ela será enviada na forma de um arquivo de texto. Você pode abrir o arquivo e depois copiar e colar o conteúdo no campo Paste License.
- Você também pode carregá-lo para o ADC se copiar/colar não for uma opção para você.
- Uma vez feito isso, por favor clique no botão atualizar
- A licença está agora instalada.

Informações sobre o serviço de licença

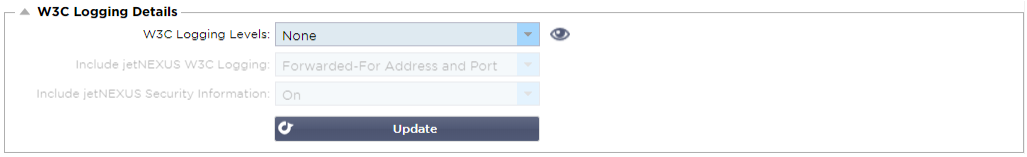
Clicando no botão Informações de Serviço de Licença, todas as informações sobre a licença serão exibidas. Esta função pode ser usada para enviar os detalhes para o pessoal de suporte.

Logging

A página Sistema > Logging permite definir os níveis de log do W3C e especificar o servidor remoto para o qual os logs serão automaticamente exportados. A página está organizada nas quatro seções abaixo.

Detalhes de registro do W3C

A ativação do registro W3C fará com que o ADC comece a gravar um arquivo de registro compatível com o W3C. Um registro W3C é um registro de acesso para servidores Web no qual são gerados arquivos de texto contendo dados sobre cada solicitação de acesso, incluindo o endereço IP (Internet Protocol) de origem, 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 registro do W3C está desligado.
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 do 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 obter 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	Este formato é muito semelhante ao "Completo", mas tem um campo adicional. Veja o resumo dos campos abaixo para obter 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	Este formato é preenchido com todos os tipos de informações relevantes para o pessoal de desenvolvimento e suporte. Consulte o resumo dos campos abaixo para obter 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-versão x-r-versão cs-bytes sr-bytes rs-bytes rs-bytes x-percentual do tempo de viagem x-round-trip-time x-trip-times(novo,rcon,rqf,rql,tqf,tql,rsf,rsl,tsf,tsl,dis,log) x-fechado por x- compress-action x-sc(Content-Type) x-cache-action X-finish

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

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-bytes 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-bytes sc-status sc-param sc-bytes sr-method sr-param sr-bytes rs-status rs-param rs-bytes

Incluir o registro do W3C

Esta opção permite definir quais informações do ADC devem ser incluídas nos registros do W3C.

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

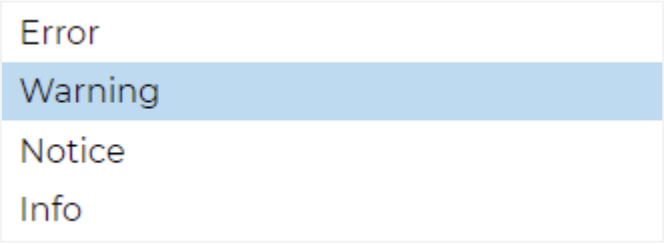
Incluir informações de segurança

Este menu consiste de duas opções:

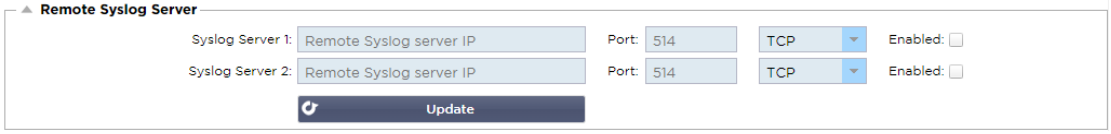
Valor	Descrição
Em	Este cenário é global. Quando ajustado para on, o nome de usuário será anexado ao log do W3C quando qualquer Serviço Virtual estiver usando Autenticação e tiver o log do W3C habilitado.
Fora	Isto desligará a capacidade de registrar o nome de usuário no registro do W3C em nível global.

Servidor Syslog

Esta seção permite que você defina o nível de registro de mensagens realizadas no servidor SYSLOG. As opções disponíveis são as seguintes.



Servidor remoto Syslog



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

- Adicione o endereço IP do seu servidor Syslog
- Adicionar o Porto
- Escolha se você deseja usar TCP ou UDP
- Marque a caixa de seleção Ativado para iniciar o registro
- Clique em Atualizar

Armazenamento remoto de logs

Todos os registros W3C são armazenados em forma comprimida no ADC a cada hora. Os arquivos mais antigos serão apagados quando 30% do espaço em disco estiver restante. Caso você deseje exportar estes arquivos para um servidor remoto para guarda segura, você pode configurar isto usando um compartilhamento 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, isto pode levar até duas horas em um equipamento de Máquina Virtual e cinco horas para um equipamento de hardware.

Incluiremos um botão de teste em futuros lançamentos para fornecer algum feedback de que suas configurações

Col1	**Col2**
Armazenamento remoto de logs	Assinale 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 SMB. Exemplo: w3c.
Diretório	Especifique o diretório no servidor SMB. Exemplo: /log.
Nome de usuário	Especifique o nome de usuário para a ação SMB.
Senha	Especifique a senha para a ação SMB

estão corretas.

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 site = 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 para o cliente pode ser derivada da rede ou do cabeçalho X-Forwarded-For
cs- nome do usuário	Campo de solicitação de nome de usuário do cliente
s-ip	Porta de escuta da ALB
s-port	ALB's ouvindo VIP
x-xff	Valor do cabeçalho X-Forwarded-For
x-xffcustom	Valor do cabeçalho de solicitação do tipo X-Forwarded-Forwarded
cs-host	Nome do anfitrião no pedido
x-r-ip	Endereço IP do Servidor Real utilizado
x-r-port	Porto de Servidor Real utilizado
cs-método	Método de solicitação HTTP * exceto formato Brief
método	* Apenas um breve formato utiliza 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 Usuário-Agente do Navegador (conforme enviado pelo cliente)
referir	Página de referência (como enviada pelo cliente)
x-c-versão	Solicitação 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, na solicitação
rs-bytes	Bytes do Real Server, na resposta
sc-bytes	Bytes enviados ao cliente, na resposta
x-percente	Porcentagem de compressão * = 100 * (1 - saída / entrada) incluindo cabeçalhos
tempo necessário	Quanto tempo o Real Server demorou em segundos
x-trip-times novo pcon	milissegundos de conexão para postagem na "lista de novatos". milissegundos desde a conexão até a colocação da conexão com o Real Server
acon	milissegundos desde a conexão até o acabamento da colocação da conexão ao Real Server
rcon	milissegundos desde a conexão até o estabelecimento da conexão real-servidor
rqf	milissegundos desde a conexão até o recebimento do primeiro byte de solicitação do cliente
rql	milissegundos desde a conexão até o recebimento do último byte de solicitação do cliente
tqf	milissegundos desde a conexão até o envio do primeiro byte de solicitação para o Real Server
tql	milissegundos desde a conexão até o envio do último byte de solicitação para o Real Server
rsf	milissegundos desde a conexão até o recebimento do primeiro byte de resposta do Real Server
rsl	milissegundos desde a conexão até o recebimento do último byte de resposta do Real Server
tsf	milissegundos desde a conexão até o envio do primeiro byte de resposta ao cliente
tsl	milissegundos desde a conexão até o envio do último byte de resposta ao cliente
dis	milissegundo de conectar para desconectar (ambos os lados - último a desconectar)
log	milissegundos de conexão a este registro de registro geralmente seguido por (política de equilíbrio de carga e raciocínio)
x-round-trip-time	Quanto tempo levou o ALB em segundos
x-closed-by	Que ação fez com que a conexão fosse fechada (ou mantida aberta)
x-compress-acção	Como a compressão foi realizada, ou evitada
x-sc(Content-Type)	Tipo de conteúdo de resposta
x-cache-acção	Como o cache respondeu, ou foi impedido
x-finish	Gatilho que causou esta fila de troncos

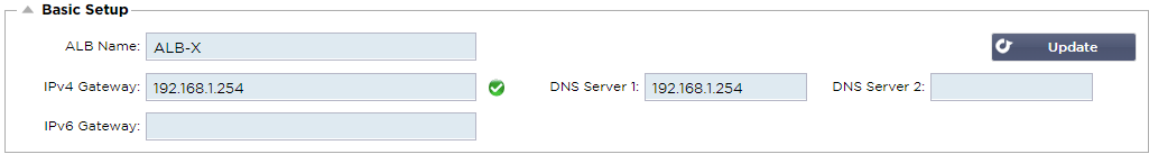
Limpar arquivos de log

Este recurso permite limpar os arquivos de registro do ADC. Você pode selecionar o tipo de registro que deseja excluir do 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.

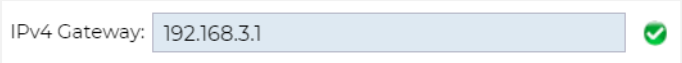
Configuração básica



Nome ALB

Especifique um nome para seu aparelho ADC. Observe que isto não pode ser alterado se houver mais de um membro no agrupamento. Favor ver a seção sobre Clustering.

Gateway IPv4



Especifique o endereço do IPv4 Gateway. Este endereço precisará estar na mesma sub-rede que um adaptador existente. Se você adicionar o Gateway incorretamente, você verá uma Cruz Branca em um círculo vermelho. Ao adicionar um gateway correto, você verá um banner verde de sucesso na parte inferior da página e uma cruz branca em um círculo verde ao lado do endereço IP.

Portal IPv6

Especifique o endereço IPv6 Gateway. Este endereço precisará estar na mesma sub-rede que um adaptador existente. Se você adicionar o Gateway incorretamente, você verá uma Cruz Branca em um círculo vermelho. Ao adicionar um gateway correto, você verá um banner verde de sucesso na parte inferior da página e um tick branco em um círculo verde ao lado do endereço IP.

Servidor DNS 1 & Servidor DNS 2

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

Detalhes do Adaptador

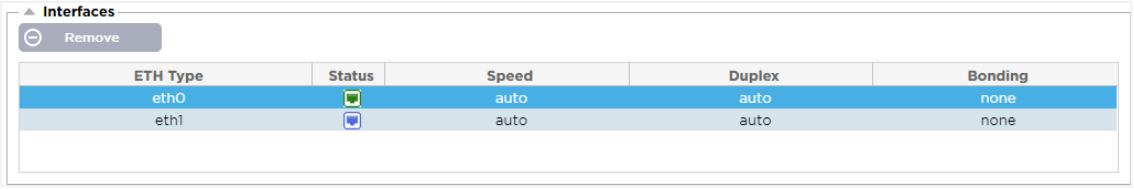
Esta seção do painel Rede mostra as interfaces de rede que são instaladas em seu aparelho ADC. Você pode adicionar e remover adaptadores, conforme necessário.

Coluna	**Descrição**
Adaptador	Esta coluna exibe os adaptadores físicos instalados em seu aparelho. Escolha um adaptador da lista de adaptadores disponíveis clicando nele - um duplo clique colocará a linha de listagem no modo de edição.
VLAN	Clique duas vezes para adicionar a identificação da VLAN para o adaptador. A VLAN é uma Rede Local Virtual que cria um domínio de transmissão distinto. Uma VLAN tem os mesmos atributos da LAN física, mas permite que as estações finais sejam agrupadas mais facilmente se não estiverem no mesmo switch da rede.
Endereço IP	Clique duplo para adicionar o endereço IP associado com a interface do adaptador. Você pode adicionar vários endereços IP à mesma interface. Este deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 192.168.101.2

Máscara de sub-rede	Clique duas vezes para adicionar a máscara de sub-rede atribuída à interface do adaptador. Este deve ser um número IPv4 de 32 bits em notação decimal com quatro pontos. Exemplo 255.255.255.0
Porta de entrada	Adicionar uma porta de entrada para a interface. Quando isto for adicionado, o ADC estabelecerá uma política simples que permitirá que as conexões iniciadas a partir desta interface sejam retornadas através desta interface para o roteador de gateway especificado. Isto 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	Clique duas vezes para adicionar uma descrição para 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. Por favor, sinta-se à vontade para mudar estas convenções de nomenclatura para sua própria escolha.
Console Web	Clique duas vezes na coluna e depois marque a caixa para atribuir a interface como o endereço de gerenciamento para a Consola Web da Interface Gráfica do Usuário. Tenha muito cuidado ao alterar a interface que o Console da Web irá escutar. Você precisará ter o roteamento correto configurado ou estar na mesma sub-rede da nova interface para poder chegar ao Console Web após a mudança. A única maneira de alterar este retorno é acessar a linha de comando e emitir o comando set greenside. Isto apagará todas as interfaces, exceto a eth0.

Interfaces

A seção Interfaces dentro do painel Rede permite a configuração de certos elementos pertencentes à interface de rede. Você também pode remover uma interface de rede da lista, clicando no botão Remover. Ao utilizar um dispositivo virtual, as interfaces que você vê aqui são limitadas pela estrutura de virtualização subjacente.



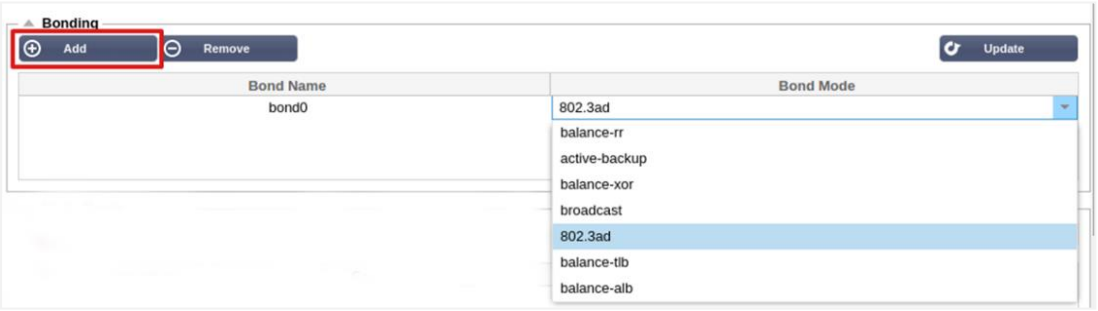
Coluna	Descrição
Tipo ETH	Este valor indica a referência interna do SO à interface da rede. Este campo não pode ser personalizado. Os valores começam com ETH0 e continuam em seqüência, dependendo do número de interfaces de rede.
Status	Esta indicação gráfica mostra o status atual da interface da rede. 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, este valor é definido para auto-negociar a velocidade. Mas você pode alterar a velocidade da rede da interface para qualquer valor disponível no drop-down (10/100/1000/AUTO).
Duplex	O valor deste campo é personalizável, e você pode escolher entre Auto (padrão), Full-Duplex, e Half-Duplex.
Colagem	Você pode escolher um dos tipos de colagem que você definiu. Consulte a seção sobre Colagem para obter mais detalhes.

Colagem

Muitos nomes são usados para denominar a ligação de interface de rede: 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 o rendimento 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, você pode definir o modo e as opções de monitoramento de 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 COLAGEM SÓ PODE SER CONFIGURADA PARA APARELHOS ADC BASEADOS EM HARDWARE.

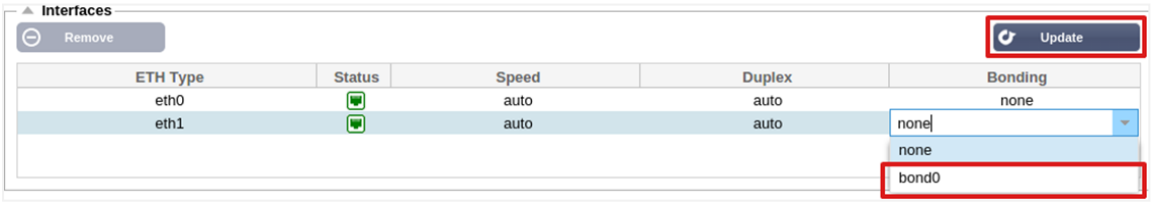


Criando um perfil de Bonding

- Clique no botão Adicionar para adicionar uma nova Obrigação
- Fornecer um nome para a configuração da colagem
- Escolha o modo de ligação que você deseja usar

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

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

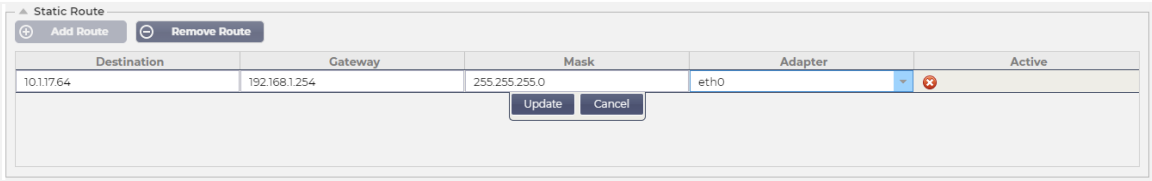


Modos de colagem

Modo de colagem	Descrição
equilíbrio-rr:	Os pacotes são transmitidos/recebidos sequencialmente através de cada interface, um a um.
backup ativo:	Neste modo, uma interface estará ativa, e a segunda interface estará em espera. Esta interface secundária só ficará ativa se a conexão ativa na primeira interface falhar.
balance-xor:	Transmite com base no endereço MAC de origem XOR'd com endereço MAC de destino. Esta opção seleciona o mesmo escravo para cada endereço MAC de destino.
transmitido:	Este modo transmitirá todos os dados em todas as interfaces escravas.
802.3ad:	Cria grupos de agregação que compartilham as mesmas configurações de velocidade e duplex e utiliza todos os escravos no agregador ativo, seguindo a especificação 802.3ad.
balanço-tlb:	O modo de ligação de balanceamento de carga adaptável transmite: Fornece ligação de canal que não requer qualquer suporte 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 assume o endereço MAC do escravo receptor falhado.
equilíbrio-alb:	O modo de ligação de balanceamento de carga adaptativo: também inclui balanceamento de carga (rlb plus) para tráfego IPV4 e não requer qualquer suporte especial de interruptor. O balanceamento de carga de recepção é obtido através de negociação ARP. O driver de bonding intercepta as Respostas 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 forma que diferentes pares usam endereços de hardware diferentes para o servidor.

Rota Estática

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



Adicionando uma rota estática

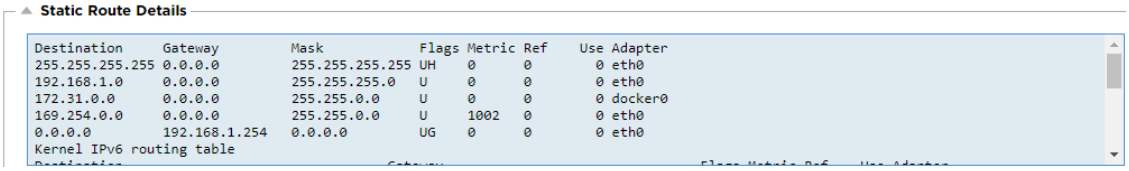
- Clique no botão Adicionar Rota
- Preencha o campo usando os detalhes da tabela abaixo como orientação.
- Clique no botão Atualizar quando estiver pronto.

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 do gateway em notação decimal pontilhada. Exemplo 10.4.8.1
Máscara	Insira a máscara da sub-rede de destino em notação decimal pontilhada. Exemplo 255.255.255.0
Adaptador	Digite o adaptador em que o portal pode ser alcançado. 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. Certifique-se de ter configurado uma interface e um endereço IP na mesma rede que o gateway.

Detalhes da rota estática

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



Configurações avançadas de rede

O que é Nagle?

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

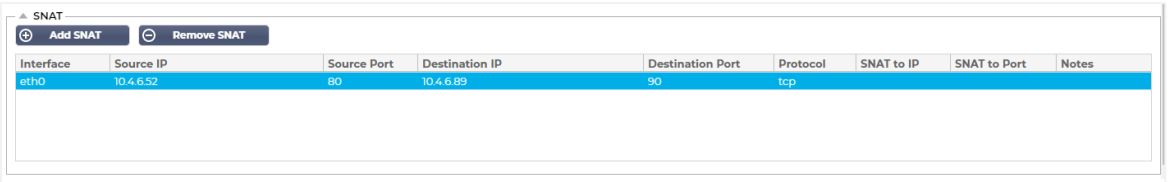
Servidor Nagle

Assinale esta caixa para ativar 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. Esta 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.

Nagle cliente

Marque a caixa para habilitar 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 para o EdgeADC SNAT seria a seguinte.

Em circunstâncias normais, os pedidos entrantes seriam direcionados 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, isto seria visível para o VIP.

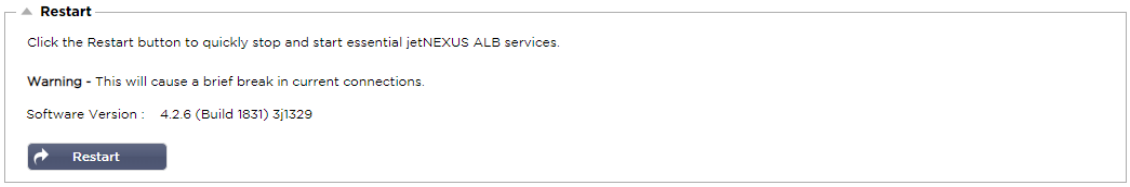
Quando o SNAT estiver em vigor, o IP de origem original do pedido será escondido do VIP, e em vez disso, ele verá o endereço IP conforme previsto na regra SNAT. Assim, o SNAT pode ser usado nos modos de balanceamento de carga de Camada 4 e Camada 7.

Campo	Descrição
Fonte IP	O endereço IP de origem é opcional, e pode ser um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser tanto uma máscara de rede quanto um número simples, especificando o número de 1's no lado esquerdo da máscara de rede. Assim, uma máscara de /24 é equivalente a 255.255.255.255.0.
IP de destino	O endereço IP de destino é opcional, e pode ser um endereço IP de rede (com /mask) ou um endereço IP simples. A máscara pode ser tanto uma máscara de rede quanto um número simples, especificando o número de 1's no lado esquerdo da máscara de rede. Assim, uma máscara de /24 é equivalente a 255.255.255.255.0.
Porto de origem	A porta de origem é opcional, pode ser um único número, em cujo caso especifica apenas essa porta, ou pode incluir dois pontos, o que especifica uma gama de portas. Exemplos: 80 ou 5900:5905.
Porto de destino	O porto de destino é opcional, pode ser um único número, em cujo caso especifica apenas esse porto, ou pode incluir dois pontos, o que especifica uma gama de portos. Exemplos: 80 ou 5900:5905.
Protocolo	Você pode escolher entre usar o SNAT em um único protocolo ou todos os protocolos. Sugerimos ser 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 para Porta é opcional, pode ser um único número, neste caso especifica apenas aquela porta, ou pode incluir um traço, que especifica uma gama de portas. Exemplos: 80 ou 5900-5905.
Notas	Use isto para colocar um nome amigável para se lembrar por que as regras existem. Isto também é útil para a depuração no Syslog.

Energia

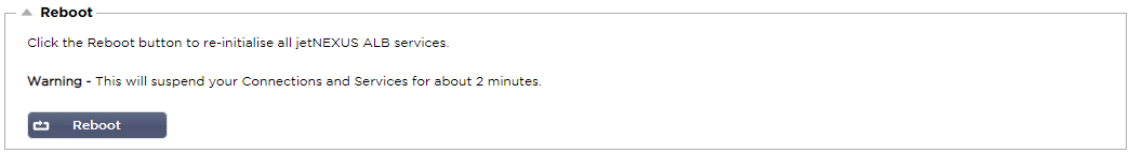
Esta característica do sistema ADC também permite a realização de várias tarefas relacionadas ao poder em seu ADC.

Reinicie



Esta configuração 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 de quantos Serviços forem configurados. Um pop-up será exibido solicitando confirmação para a ação de reinício.

Reinicialização



Clicando no botão Reiniciar (Reboot), o ADC será alimentado e automaticamente retornará a um estado ativo. Um pop-up será exibido solicitando confirmação para a ação de reinicialização.

Desligar a energia

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

Segurança

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

SSH

Opção	Descrição
Comando Remoto Seguro Shell	Marque a caixa se você deseja ter acesso ao ADC usando SSH. O "Putty" é uma excelente aplicação para fazer isto.

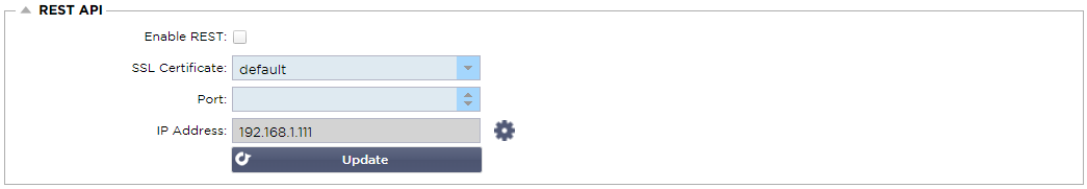
Console Web

Certificado SSL Escolha um certificado a partir da lista suspensa. O certificado que você escolher será usado para proteger sua conexão com a interface do usuário da ADC na web. Você pode criar um certificado autoassinado dentro do ADC ou importar um da seção de **CERTIFICADOS SSL.**

Opção	Descrição
Porto Seguro	A porta padrão para o console web é TCP 443. Se você desejar usar uma porta diferente por razões de segurança, você pode alterá-la aqui.

REST API

O REST API, também conhecido como RESTful API, é uma interface de programação de aplicação 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 utilizando a API REST. Observe que você também terá que configurar qual adaptador no qual o REST está habilitado. Veja a nota no link Cog abaixo.
Certificado SSL	Escolha um certificado para o serviço REST. O drop-down mostrará todos os certificados instalados no ADC.
Porto	Defina o porto para o serviço REST. É uma boa idéia usar um porto que não seja o 443.
Endereço IP	Isso exibirá o endereço IP ao qual o serviço REST está vinculado. Você pode clicar no link Cog para acessar a página da Rede para mudar qual adaptador o serviço REST está habilitado.
Cog Link	Clicando neste link, você será conduzido à página da Rede, onde você poderá configurar um adaptador para o REST.

Documentação para REST API

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

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

Exemplos

GUIA usando 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

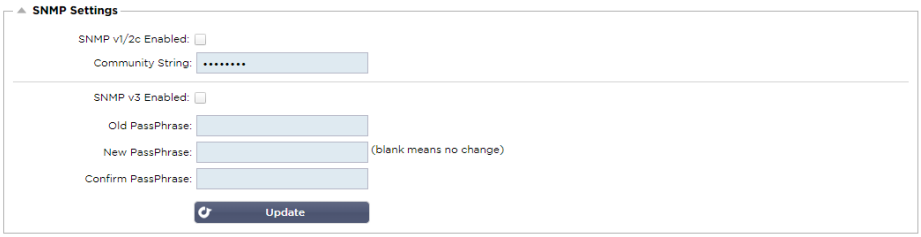
- Comando

```
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 SNMP



Opção	Descrição
SNMP v1/ V2C	Marque a caixa de seleção para ativar 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 o 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	Este é o conjunto de cordas somente leitura no agente e usado pelo gerente para recuperar as informações do SNMP. A cadeia de caracteres padrão da comunidade é jetnexus
PassPhrase	Esta é a senha necessária quando o SNMP v3 está habilitado e deve ter pelo menos 8 caracteres ou mais e conter letras Aa-Zz e números 0-9 apenas. A senha padrão é **jetnexus**

SNMP MIB

As informações visíveis sobre o SNMP são definidas pela Base de Informações Gerenciais (MIB). As MIB descrevem a estrutura dos dados gerenciais e utilizam identificadores de objetos hierárquicos (OID). Cada OID pode ser lido através de um aplicativo de gerenciamento SNMP.

MIB Download

O MIB pode ser baixado 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 **jetnexusOveralllnputBytes (1**.3.6.1.4.1.38370.1.1.1.1.0)
.2 **jetnexusOveralllOutputBytes (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**.3.6.1.4.1.38370.1.1.7.0)
.8 **jetnexusDiskFreePercent (1**.3.6.1.4.1.38370.1.1.8.0)
.9 **jetnexusMemoryPercent (1**.3.6.1.4.1.38370.1.1.1.9.0)
.10 **jetnexusCurrentConnections (1**.3.6.1.4.1.38370.1.1.1.10.0)

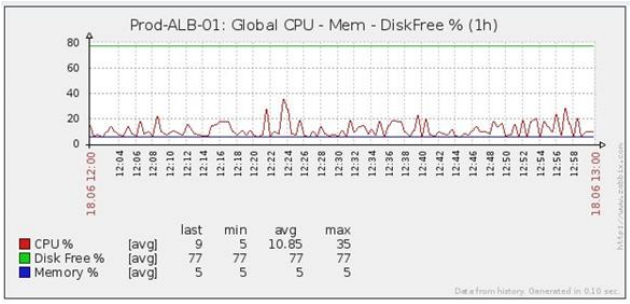
.2 **jetnexusVirtualServices (1**.3.6.1.4.1.38370.1.2)
.1 **jnvirtualserviceEntry (1**.3.6.1.4.1.38370.1.2.1)
.1 **jnvirtualserviceIndexvirtualservice (1**.3.6.1.4.1.38370.1.2.1.**1**)
.2 **jnvirtualserviceVSAddrPort (1**.3.6.1.4.1.38370.1.2.1.**2**)
.3 **jnvirtualserviceOveralllnputBytes (1**.3.6.1.4.1.38370.1.2.1.**3**)
.4 **jnvirtualserviceOveralllOutputBytes (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**)

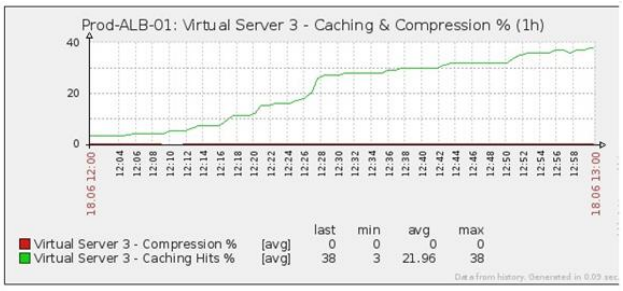
.3 **jetnexusRealServers (1**.3.6.1.4.1.38370.1.3)
.1 **jnrealserverEntry (1**.3.6.1.4.1.38370.1.3.**1**)
.1 **jnrealserverIndexVirtualService (1**.3.6.1.4.1.38370.1.3.1.**1**)

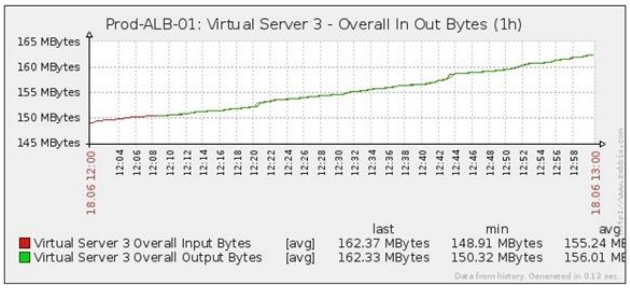
.2 **jnrealserverIndexRealServer** (1.3.6.1.4.1.38370.1.3.1.2)
.3 **jnrealserverChAddrPort** (1.3.6.1.4.1.38370.1.3.1.3)
. 4 **jnrealserverCSAddrPort** (1.3.6.1.4.1.38370.1.3.1.4)
.5 **jnrealserverOveralllnputBytes** (1.3.6.1.4.1.38370.1.3.1.5)
.6 **jnrealserverOveralllOutputBytes** (1.3.6.1.4.1.38370.1.3.1.6)
.7 **jnrealserverCompressionPercent** (1.3.6.1.4.1.38370.1.3.1.7)
.8 **jnrealserverPresentClientConnections** (1.3.6.1.4.1.38370.1.3.1.8)
. 9 **jnrealserverPoolUsage** (1.3.6.1.4.1.38370.1.3.1.9)
.10 **jnrealserverHitCount** (1.3.6.1.4.1.38370.1.3.1.10)
. 11 **jnrealserverRSStatus** (1.3.6.1.4.1.38370.1.3.1.11)

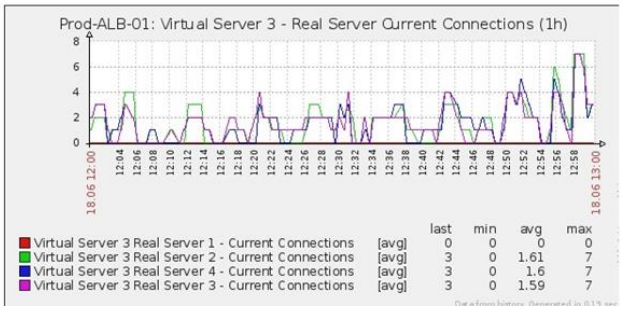
Gráficos históricos

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









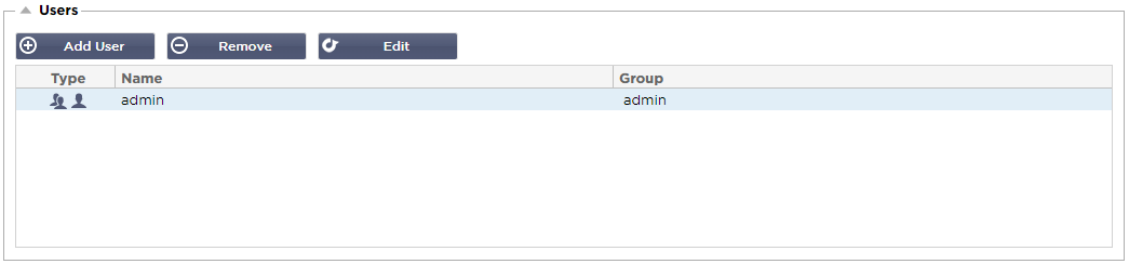
Usuários e logs de auditoria

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 da função a eles ligada.

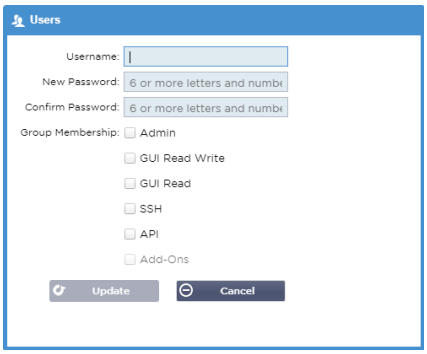
Há um usuário padrão chamado **admin** que você usa quando configura o ADC pela primeira vez. A senha padrão para admin é **jetnexus**.

Usuários

A seção Usuários é fornecida para que você possa criar, editar e remover 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 letras podem ser maiúsculas e minúsculas • Números podem ser utilizados • 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 letras podem ser maiúsculas ou minúsculas • Os símbolos são permitidos, exceto para os do exemplo abaixo **£, %, & , < , >**
Confirmar senha	Confirmar a senha novamente para garantir que esteja correta
Participação em grupo	Assinale o grupo ao qual você gostaria que o usuário pertencesse. • Admin - Este grupo pode fazer tudo • GUI Read Write - Os usuários deste grupo podem acessar a GUI e fazer alterações através da GUI • GUI Read - Os usuários deste grupo podem acessar a GUI para visualizar apenas informações. Nenhuma alteração pode ser feita • SSH - Os usuários deste grupo podem acessar o ADC através da Secure Shell. Esta escolha dará acesso à linha de comando, que tem um conjunto mínimo de comandos disponíveis • API - Os usuários deste 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 H/A Stand-Alone ou Manual criará somente Usuários Locais** **Por padrão,** um usuário local chamado "admin" **é um membro do grupo admin. Para compatibilidade retroativa**, **este usuário nunca pode ser excluído.** **Você 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 apenas Usuários do Cluster Os usuários do Cluster são sincronizados em todos os ADCs do Cluster Qualquer mudança em um usuário do cluster mudará em todos os membros do cluster Se você estiver logado como um usuário de cluster, não poderá mudar de funções de Cluster para Manual ou Stand-Alone
	Cluster e usuário local Qualquer usuário criado enquanto estiver no papel Stand-Alone ou Manual será copiado para o Cluster Se o ADC subseqüentemente deixar o Cluster, então somente os Usuários Locais permanecerão A última senha configurada para o usuário será válida

Removendo um usuário

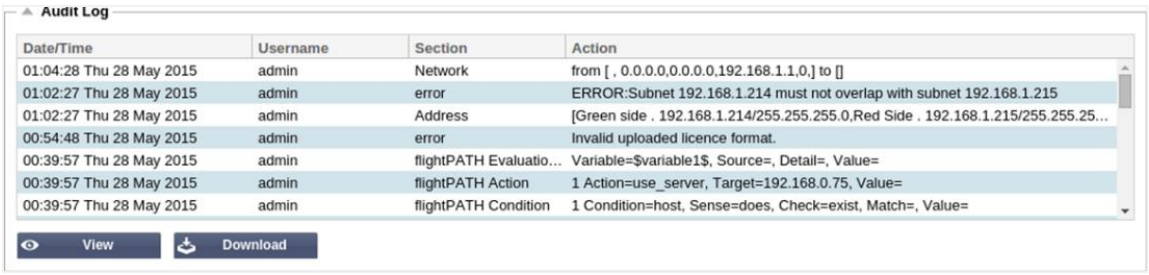
- Destacar um usuário existente
- Clique em Remover
- Você não poderá excluir o usuário que está atualmente conectado
- Você não poderá remover o último usuário local do grupo administrativo
- Você não será capaz de remover o usuário final restante do cluster no grupo de administração
- Você não poderá excluir o usuário administrador para compatibilidade retroativa
- Se você remover o ADC do cluster, todos os usuários, exceto os usuários locais, serão excluídos

Edição de um usuário

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

Diário de Auditoria

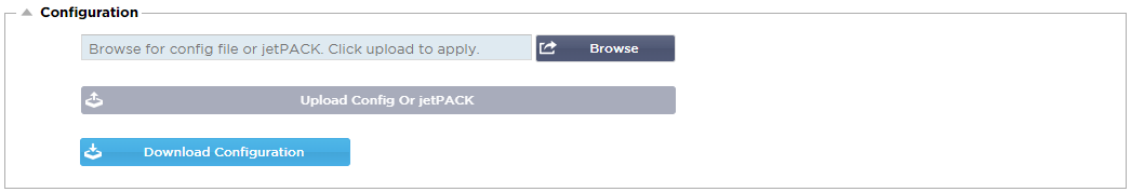
O ADC registra alterações feitas na configuração do ADC por usuários individuais. O registro de auditoria fornecerá as últimas 50 ações realizadas por todos os usuários. Você também pode ver TODAS as entradas na seção **LOGS.** Por exemplo, o ADC:



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=

Avançado

Configuração



É sempre a melhor prática descarregar e salvar a configuração do ADC uma vez que ele esteja totalmente configurado e funcionando conforme necessário. Você pode usar o módulo Configuração tanto para baixar quanto para carregar uma configuração.

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

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

Download de uma configuração

- Para baixar a configuração atual do ADC, pressione o botão Download Configuration.
- Um pop-up aparecerá pedindo que você abra ou salve o arquivo .conf.
- Economize em um local conveniente.
- Você pode abrir isto com qualquer editor de texto, como o Notepad++.

Carregamento de uma configuração

- Você pode carregar um arquivo de configuração salvo, navegando pelo arquivo .conf salvo.
- Clique no botão 'Upload Config ou Jetpack'.
- O ADC carregará e aplicará a configuração e então atualizará o navegador. Se ele não atualizar o navegador automaticamente, por favor clique em atualizar no navegador.
- Você será redirecionado para a página do Painel de Controle 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.
    - Você pode obter um jetPACK no portal de suporte mostrado no final deste guia.
- Procure o arquivo jetPACK.txt.
- Clique em upload.
- O navegador será atualizado automaticamente após o upload.
- Você será redirecionado para a página do Painel de Controle após a conclusão.
- A importação pode levar mais tempo para implantações mais complexas, como Microsoft Lync, etc.

Configurações globais

A seção Configurações globais permite alterar vários elementos, incluindo a biblioteca criptográfica SSL.

Temporizador de Cache Host

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 tiver sido usado em vez de um endereço IP. O cache é descarregado em caso de falha do Servidor Real. Definindo este valor como zero, evitará que o cache seja lavado. Não há um valor máximo para esta configuração.

Drenagem

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

SSL

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

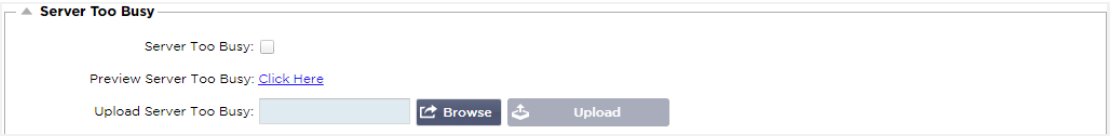
Autenticação

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

Protocolo

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

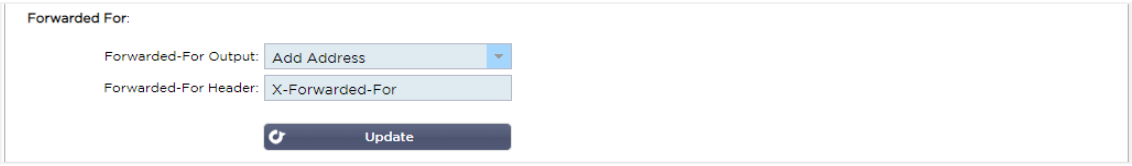
Servidor muito ocupado



Suponha que você tenha limitado as Max Connections a seus Servidores Reais; você pode optar por apresentar uma página web amigável uma vez que este limite tenha sido atingido.

- Crie uma página web simples com sua mensagem. Você pode incluir links externos para objetos em outros servidores e sites da web. Alternativamente, se você quiser ter imagens em sua página da web, então use imagens codificadas na base64 em linha
- Procure seu arquivo HTM(L) recém-criado para a página web
- Clique em Upload
- Se você deseja visualizar a página, você 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 através de equilibradores de carga Layer- 7 e servidores proxy.

Encaminhado - Para saída

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

Cabeçalho de Forwarded-For

Este campo permite que você especifique o nome dado ao cabeçalho Forwarded-For. Tipicamente, este é "X-Forwarded-For", mas pode ser alterado para alguns ambientes.

Logging avançado para IIS - Logging personalizado

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

Selecione Default da lista Tipo de Fonte da lista 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

Mudanças no Apache HTTPd.conf

Você 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 "%b" "% (Refrigerador)i" "\Combinado de "% (Usuário-Agente)".
LogFormat:	"%{X-Forwarded-For}i %l %u %t "%r" %>s %b {Referer}i "\Conjunto de Proxy de "% (Usuário-Agente)i" Se X- Encaminhado-Para "^.*...*...*" Encaminhado
CustomLog:	"logs/access_log" combined env=!forwarded
CustomLog:	proxy "logs/access_log" env=forwarded

Este formato aproveita o suporte incorporado do Apache para o registro condicional baseado em variáveis ambientais.

- A linha 1 é a seqüência padrão combinada de log formatada a partir do padrão.
- A linha 2 substitui o campo %h (host remoto) pelo(s) valor(es) tirado(s) do cabeçalho X-Forwarded-For e define o nome deste padrão de arquivo de log como "proxy".
- A linha 3 é uma configuração para a variável de ambiente "encaminhada" que contém uma expressão regular frouxa que corresponde a um endereço IP, o que é ok neste caso, já que nos preocupamos mais se existe um endereço IP no cabeçalho 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 padrão de tronco a ser utilizado. Se um valor X-Forwarded-For existe, 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 assumimos que quase todos o utilizam.

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

Configurações de Compressão HTTP

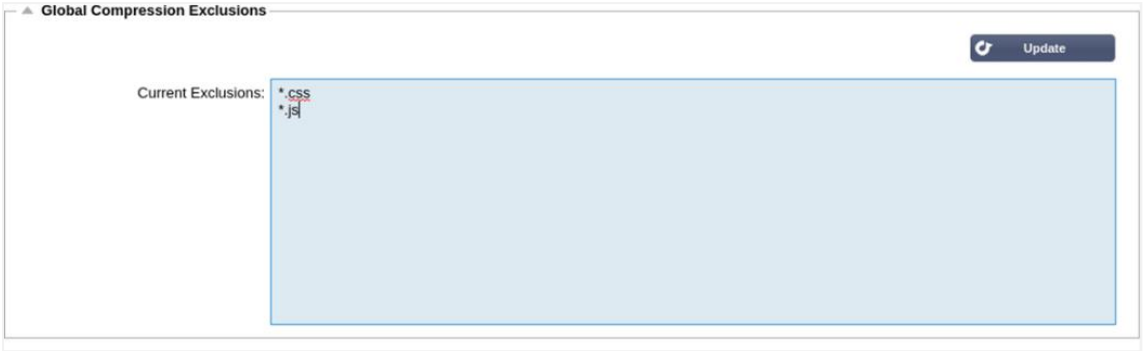
A compressão é uma característica de aceleração e está habilitada para cada Serviço na página de Serviços IP.

AVISO - Tome extremo cuidado ao ajustar essas configurações, pois configurações inadequadas podem afetar negativamente o desempenho do ADC

Opção	Descrição
Memória de rosca inicial [KB]	Este valor é a quantidade de memória que cada pedido recebido pelo ADC pode inicialmente alocar. Para um desempenho mais eficiente, este valor deve ser definido para um valor que exceda o maior arquivo HTML não comprimido que os servidores web provavelmente irão enviar.

Memória máxima de rosca [KB]	Este 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 na memória. Se um arquivo de conteúdo excepcionalmente grande exceder esta quantidade for processado, o ADC gravará em disco e comprimirá os dados lá.
Memória de Incremento [KB]	Este valor define a quantidade de memória adicionada à Alocação Inicial de Memória de Rosca quando mais é necessário. A configuração padrão é zero. Isto 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 thread. Isto é eficiente quando a maioria das páginas tem um 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 definir um incremento linear de um 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]	Este valor é o tamanho, em bytes, sob o qual o ADC não tentará comprimir. Isto é útil porque qualquer coisa muito abaixo de 200 bytes não comprime bem e pode até crescer em tamanho devido às despesas gerais dos cabeçotes de compressão.
Modo Seguro	Assinale esta opção para evitar que o ADC aplique compressão em folhas de estilo de 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 estar em conformidade 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 esta opção para desativar a compressão destes tipos. Entretanto, isto reduzirá a quantidade total de compressão de conteúdo.
Desativar Compressão	Assinale isto para impedir que o ADC comprima qualquer resposta.
Comprima Enquanto Você Vai	ON - Use Compress as You Go nesta página. Isto comprime cada bloco de dados recebidos do servidor em um pedaço discreto que é totalmente descompactável. OFF - Não use Compress as You Go on this page. By Page Request - Use Compress as You Go by page request.

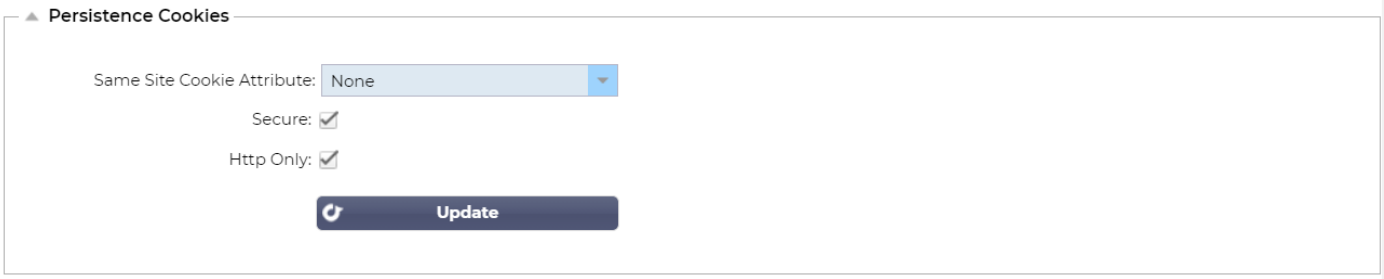
Exclusões de Compressão Global



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

- Digite o nome do arquivo individual.
- Clique em atualizar.
- Se você deseja adicionar um tipo de arquivo, simplesmente digite "*.css" para que todas as folhas de estilo em cascata sejam excluídas.
- Cada arquivo ou tipo de arquivo deve ser adicionado a uma nova linha.

Biscoitos de persistência



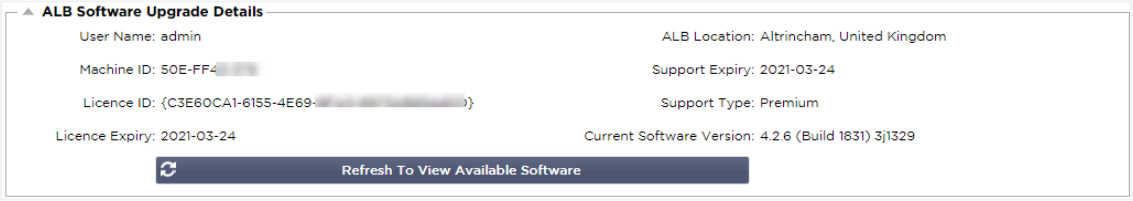
Esta configuração permite que você especifique como os Cookies de Persistência são tratados.

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

Software

A seção Software permite atualizar a configuração e o firmware de seu ADC.

Detalhes de atualização de software



As informações desta seção serão preenchidas se você tiver uma conexão de Internet funcionando. Se seu navegador não tiver um link para a Internet, esta seção estará em branco. Uma vez conectado, você 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 você sob seu plano de suporte. Você deve prestar atenção ao tipo de suporte e à data de validade do suporte.

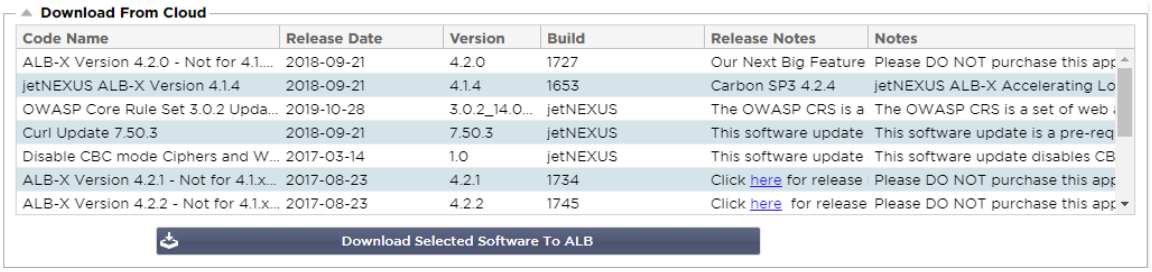
Nota: Usamos a conexão de internet de seu navegador para ver o que está disponível na Nuvem Edgenexus. Você só poderá baixar atualizações de software se o ADC tiver uma conexão com a Internet.

Para verificar isto:

- Avançado-- Resolução de problemas- Ping
- Endereço IP - appstore.edgenexus.io
- Clique em Ping

- Se o resultado mostrar "ping: unknown host appstore.edgenexus.io". "
- O ADC NÃO poderá baixar nada da nuvem

Baixar do Cloud



Code Name	Release Date	Version	Build	Release Notes	Notes
ALB-X Version 4.2.0 - Not for 4.1....	2018-09-21	4.2.0	1727	Our Next Big Feature	Please DO NOT purchase this app
jetNEXUS ALB-X Version 4.1.4	2018-09-21	4.1.4	1653	Carbon SP3 4.2.4	jetNEXUS ALB-X Accelerating Lo
OWASP Core Rule Set 3.0.2 Upda...	2019-10-28	3.0.2_14.0...	jetNEXUS	The OWASP CRS is a	The OWASP CRS is a set of web
Curl Update 7.50.3	2018-09-21	7.50.3	jetNEXUS	This software update	This software update is a pre-req
Disable CBC mode Ciphers and W...	2017-03-14	1.0	jetNEXUS	This software update	This software update disables CB
ALB-X Version 4.2.1 - Not for 4.1.x...	2017-08-23	4.2.1	1734	Click here for release	Please DO NOT purchase this app
ALB-X Version 4.2.2 - Not for 4.1.x...	2017-08-23	4.2.2	1745	Click here for release	Please DO NOT purchase this app

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

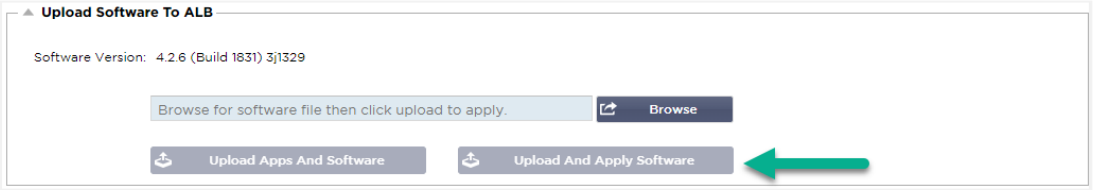
- Destaque a linha em que você está interessado e clique no botão "Download Selected Software to ALB". botão "Download do software selecionado
- O software selecionado será baixado para seu ALB quando clicado, o qual pode ser aplicado na seção "Apply Software Stored on ALB" abaixo.

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

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

Upload de software para ALB

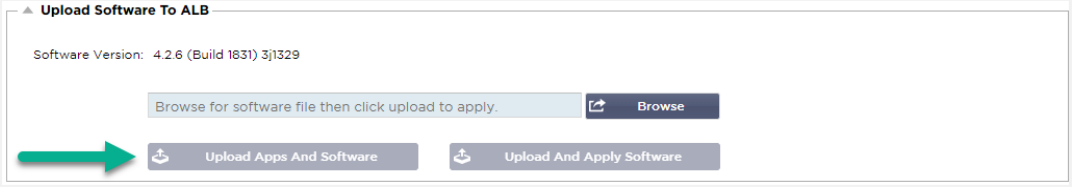
Upload de aplicativos



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

- Há cinco tipos de aplicativos
  - <appname>flightpath.alb
  - <appnome>.monitor.alb
  - <appnome>.jetpack.alb
  - <appnome>.addons.alb
  - <appnome>.featurepack.alb
- Uma vez carregado, cada aplicativo será encontrado na seção Biblioteca > Aplicativos.
- Em seguida, você deve implantar cada aplicativo nessa seção individualmente.

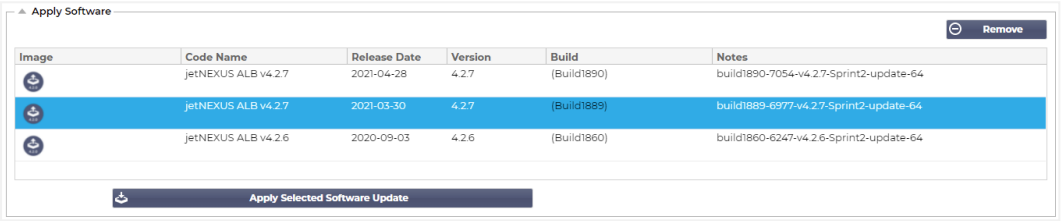
Software



- Se você deseja carregar o software sem aplicá-lo, então use o botão destacado.
- O Arquivo de Software é <softwarename>.software.alb.

- Em seguida, ele será exibido na seção "Software Stored on ALB", de onde você poderá aplicá-lo conforme sua conveniência.

Aplicar o software armazenado no ALB



Esta seção mostrará todos os arquivos de Software armazenados no ALB e disponíveis para implantação. A lista incluirá assinaturas de Web Application Firewall (WAF) atualizadas.

- Destaque a linha de Software que você está interessado em usar.
- Clique em "Apply Software from Selected" (Aplicar software da Selected)
- Se esta for uma Atualização de Software ALB, esteja ciente de que ela será carregada e então reinicializada para ser aplicada.
- Se a atualização que você está aplicando for uma atualização de assinatura OWASP, ela será aplicada automaticamente sem reinicialização.

Solução de problemas

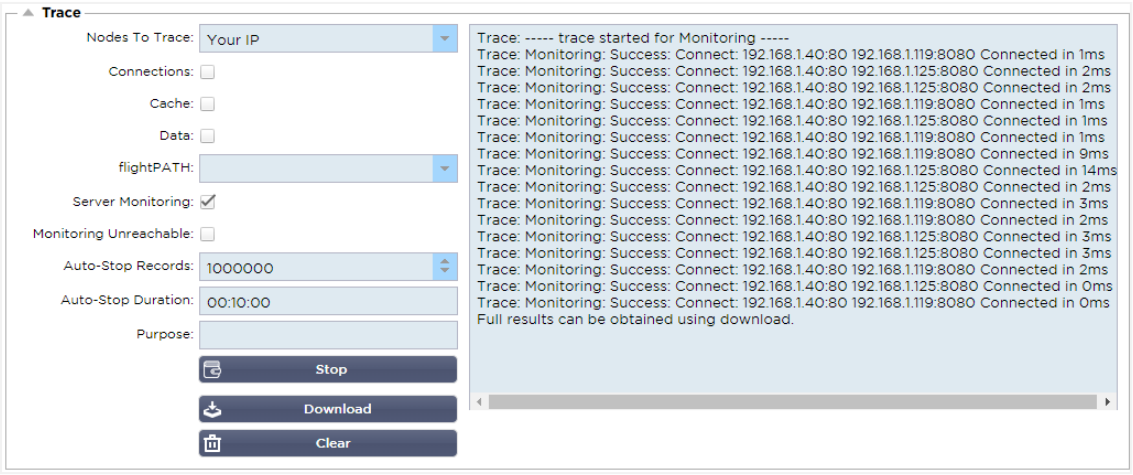
Há sempre questões que requerem solução de problemas para chegar a uma causa e solução de raiz. Esta seção permite que você faça isso.

Arquivos de suporte

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

- Selecione um período de tempo a partir do menu suspenso: Uma escolha de 3, 7, 14, e Todos os dias estão disponíveis para você.
- Clique em "Baixar arquivos de suporte".
- Um arquivo será baixado no formato Support-jetNEXUS-yyyyymmddhh-NAME.dat
- Levante um ticket de suporte no portal de suporte, cujos detalhes estão disponíveis no final deste documento.
- Certifique-se de descrever o problema minuciosamente e anexar o arquivo .dat ao bilhete.

Trace



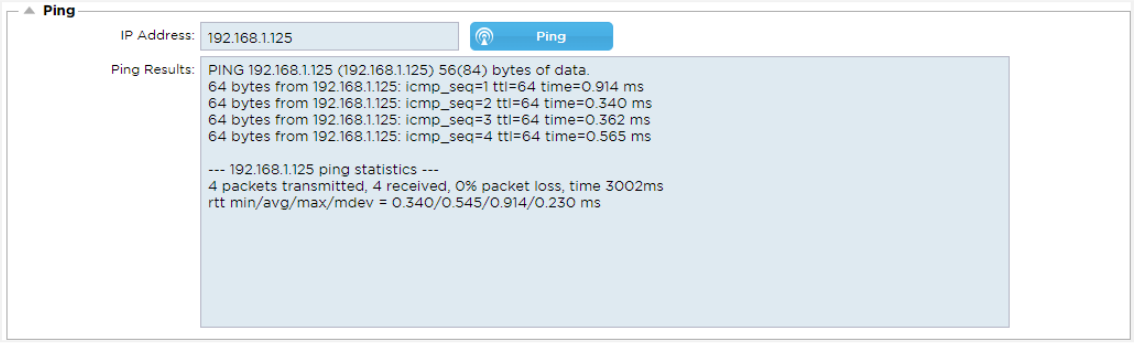
A seção Trace permitirá que você examine informações que permitam a depuração do problema. As informações entregues dependem das opções que você escolher entre as drop-downs e as caixas de seleção.

Opção	**Descrição**
Nodos para rastrear	**Seu IP**: Isto filtrará a saída para usar o endereço IP de onde você está acessando a GUI (Nota: não escolha esta opção para Monitoramento, pois o Monitoramento usará o endereço de interface do ADC) **Todos os IP**: Nenhum filtro será aplicado. Deve-se observar que em uma caixa ocupada isto afetará adversamente o desempenho.
Conexões	Esta caixa de seleção, quando marcada, mostrará informações sobre as conexões do lado do cliente e do lado do servidor.
Cache	Esta caixa de seleção assinalada mostrará informações com relação aos objetos em cache.
Dados	Quando esta caixa de seleção for marcada, ela incluirá os bytes de dados brutos tratados por dentro e por fora pelo ADC.
flightPATH	O menu flightPATH permite selecionar uma determinada regra flightPATH para monitorar ou Todas as regras flightPATH.
Monitoramento de servidores	Esta caixa de seleção, quando marcada, mostrará os monitores de saúde do servidor ativos no ADC e seus respectivos resultados.
Monitoramento inatingível	Quando esta opção é selecionada, é muito parecida com o monitoramento de comportamento do servidor, exceto que ele só mostrará os monitores que falharam e assim atua como um filtro apenas para estas mensagens.
Registros de Auto-Stop	O valor padrão é de 1.000.000 de registros, após o que a instalação Trace irá parar automaticamente. Esta configuração é uma precaução de segurança para evitar que o Trace seja deixado acidentalmente ligado e afete seu desempenho do ADC.
Duração da Auto-Stop	O tempo padrão é ajustado para 10 minutos, após os quais a instalação Trace parará automaticamente. Esta característica é uma precaução de segurança para evitar que Trace seja deixado acidentalmente ligado e afete o desempenho do ADC.
Início	Clique aqui para iniciar a instalação de rastreamento manualmente.
Parada	Clique para parar manualmente a instalação Trace antes que o registro automático ou o tempo seja alcançado.
Download	Embora você possa ver o espectador ao vivo no lado direito, as informações podem ser exibidas muito rapidamente. Em vez disso, você pode baixar o

	Trace.log para ver todas as informações coletadas durante os vários traços naquele dia. Este recurso é uma lista filtrada de informações de traços. Se você desejar visualizar as informações de rastreamento dos dias anteriores, você pode baixar o Syslog para aquele dia, mas terá que filtrar manualmente.
Limpar	Limpa o registro de rastreamento

Ping

Você 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 host que você deseja testar, por exemplo, o gateway padrão usando uma notação decimal pontilhada ou um endereço IPv6. Você pode ter que esperar alguns segundos para que o resultado seja respondido uma vez que você tenha pressionado o botão "Ping".

Se você tiver configurado um servidor DNS, então você pode digitar o nome de domínio totalmente qualificado. Você pode configurar um servidor DNS na seção **SERVIDOR DNS 1 E SERVIDOR DNS 2**. Você pode ter que esperar alguns segundos para que o resultado seja respondido uma vez que você tenha pressionado o botão "Ping".

Captura

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

- Preencha as opções no formulário
- Clique em Gerar
- Uma vez que a captura tenha sido executada, seu navegador irá aparecer e perguntar onde você deseja salvar o arquivo. Ele estará no formato "jetNEXUS.cap.gz".
- Levante um ticket de suporte no portal de suporte, cujos detalhes estão disponíveis no final deste documento.
- Certifique-se de descrever o problema minuciosamente e anexar o arquivo ao bilhete.
- Você também pode ver o conteúdo usando Wireshark

Opção	**Descrição**
Adaptador	Escolha seu adaptador a partir do drop-down, tipicamente eth0 ou eth1. Você também pode capturar todas as interfaces com "qualquer"
Pacotes	Este 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. A GUI ficará inacessível durante o período de captura.

Endereço	Este valor será filtrado em qualquer endereço IP inserido na caixa. Deixe isto em branco para que não haja filtro.

Para manter o desempenho, limitamos o arquivo de download a 10MB. Se você descobrir que isto não é suficiente para capturar todos os dados necessários, podemos aumentar este número.

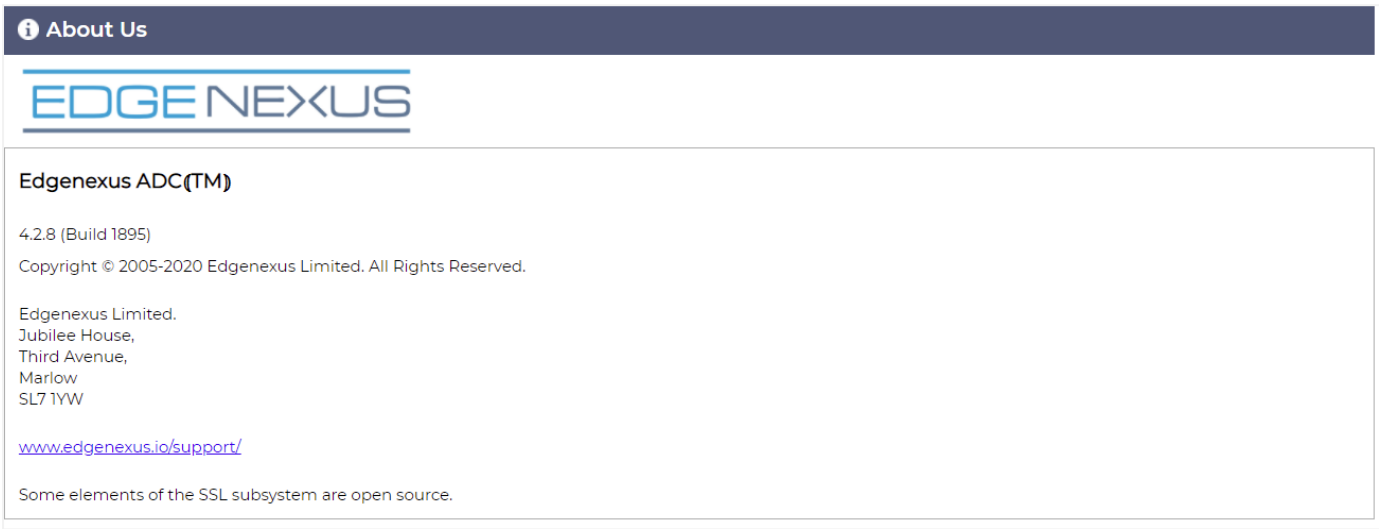
Nota: Isto terá um impacto sobre o desempenho de sites ao vivo. Para aumentar o tamanho de captura disponível, favor aplicar um jetPACK de configuração global para aumentar o tamanho da captura.

Ajuda

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

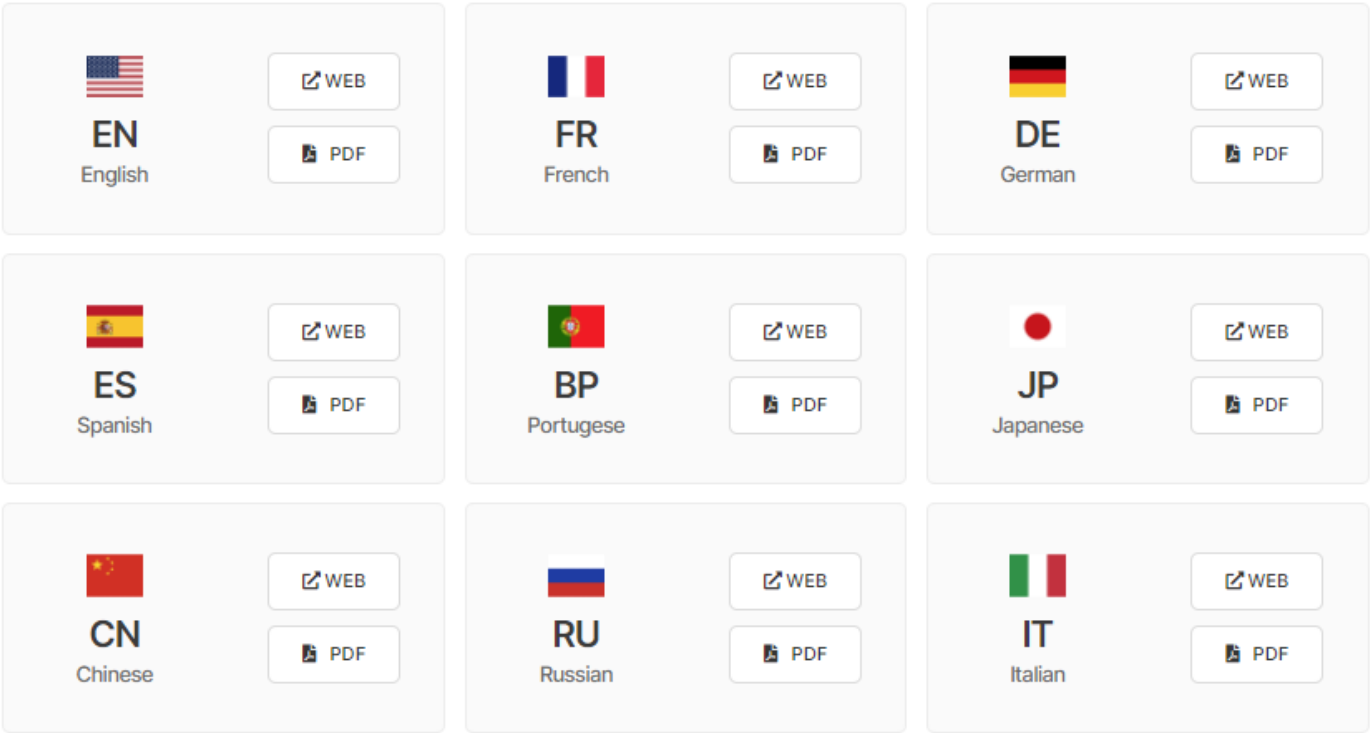
Sobre nós

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 do usuário e outros documentos úteis.



Se você não encontrar o que está procurando, por favor, entre em contato com support@edgenexus.io.

O que é um jetPACK

jetPACKs são um método único de configuração instantânea de seu ADC para aplicações específicas. Estes modelos fáceis de usar vêm pré-configurados e totalmente sintonizados com todas as configurações específicas da aplicação que você 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 você deve ter uma licença flightPATH para que este elemento funcione. Para saber se você tem uma licença para o flightPATH, consulte a página de **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 IP Virtual de 1.1.1.1
- Você pode carregar este jetPACK como está e alterar o endereço IP na GUI ou editar o jetPACK com um editor de texto como o Notepad++ e 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 você pode alterá-los na 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 ele faz?	O que está incluído?
Intercâmbio 2010	jetPACK-1.1.1.1-Exchange-2010	Este jetPACK adicionará 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 você não tiver uma licença para o flightPATH, este jetPACK ainda funcionará.	Configurações globais: Tempo de serviço de 2 horas Monitores: Monitor de camada 7 para o aplicativo web Outlook, e monitor de camada 4 fora da banda para serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de Serviço Virtual: 80, 443, 135, 59534, 59535 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTP para HTTPS
	jetPACK-1.1.1.2-Exchange-2010-SMTP-RP	O mesmo que acima, mas adicionará um serviço SMTP na porta 25 em conectividade proxy reversa. 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 o aplicativo web Outlook. Monitor de camada 4 fora de banda para o serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de Serviço Virtual: 80, 443, 135, 59534, 59535, 25 (proxy reverso) Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTP para HTTPS
	jetPACK-1.1.1.3-Exchange-	O mesmo que acima, exceto que este jetPACK irá configurar o serviço SMTP para usar a conectividade Direct Server	Configurações globais: Tempo de serviço de 2 horas

	2010-SMTP-DSR	Return. Este jetPACK é necessário se seu servidor SMTP precisar ver o endereço IP real do cliente.	Monitores: Monitor de camada 7 para o aplicativo web Outlook. Monitor de camada 4 fora de banda para o serviço de acesso do cliente Serviço Virtual IP: 1.1.1.1.1 Portos de Serviço Virtual: 80, 443, 135, 59534, 59535, 25 (retorno direto do servidor) Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTPs para HTTPs
Intercâmbio 2013	jetPACK-2.2.2.1-Exchange-2013-Low-Resource	Esta configuração adiciona 1 VIP e dois serviços para o tráfego HTTP e HTTPS e requer o mínimo de CPU. É possível adicionar vários exames de saúde 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: 2.2.2.1 Portos de Serviço Virtual: 80, 443 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTP para HTTPS
	jetPACK-2.2.3.1-Exchange-2013-Med-Resource	Esta configuração utiliza um endereço IP único para cada serviço e, portanto, utiliza mais recursos do que os acima. Você deve configurar cada serviço como uma entrada DNS individual Exemplo owa. edgenexus.com, ews. edgenexus.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 Virtual: 80, 443 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTPs para HTTPs
	jetPACK-2.2.2.3-Exchange2013-HIgh-Resource	Este jetPACK adicionará um único endereço IP e vários serviços virtuais em diferentes portos. flightPATH então mudará o contexto com base no caminho de destino para o Serviço Virtual correto. Este jetPACK requer a maior quantidade de CPU para realizar a mudança de contexto	Configurações globais: Monitores: Monitor de camada 7 para OWA, EWS, OA, EAS, ECP, OAB, ADS, MAPI e PowerShell Serviço Virtual IP: 2.2.2.3 Portos de Serviço Virtual: 80, 443, 1, 2, 3, 4, 5, 6, 7 Servidores reais: 127.1.1.1 127.2.2.2 flightPATH: Adiciona redirecionamento de HTTP para HTTPS

Microsoft Lync 2010/2013

Proxy 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	Descarga SSL	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

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

Vista Horizontal VMware

Servidores de conexão - SSL Offload	Servidores de segurança - Re-encriptação SSL
jetPACK-8.8.8.8.1-View-SSL-Offload	jetPACK-8.8.8.8.2-View-SSL-Re-encryption

Configurações globais

- GUI Secure Port 443 - este jetPACK mudará sua porta GUI segura de 27376 para 443. HTTPs://x.x.x.x.x
- GUI Timeout 1 dia - a GUI solicitará que você digite sua senha a cada 20 minutos. Esta configuração aumentará essa solicitação para 1 dia.
- ARP Refresh 10 - durante uma falha entre aparelhos HA, este ajuste aumentará o número de **ARP's Gratuitos** para auxiliar os interruptores durante a transição
- Tamanho de captura de 16MB - o tamanho padrão de captura é de 2MB. Este valor aumentará o tamanho a um máximo de 16MB

Opções de cifras

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

flightPATHs

- X-Content-Type-Options - adicionar este cabeçalho se ele não existir e configurá-lo para "nosniff" - impede que o navegador automaticamente "MIME-Sniffing".
- X-Frame-Options - adicione este cabeçalho se ele não existir e configure-o para "SAMEORIGIN" - páginas em seu website podem ser incluídas em Frames, 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-o para "max-age=31536000 ; includeSubdomains" - garante ao cliente que todos os links devem ser HTTPs:// para a max-age

Aplicando um jetPACK

Você pode aplicar qualquer jetPACK em qualquer ordem, mas tenha cuidado para não usar um jetPACK com o mesmo endereço IP Virtual. Esta ação causará uma duplicação do endereço IP na configuração. Se você fizer isto por engano, você pode mudar isto na GUI.

- Navegue para Avançado > Atualizar Software
- Seção de Configuração
- Carregar Nova Configuração ou JetPACK
- Procurar por jetPACK
- Clique em Upload
- Quando a tela do navegador ficar branca, por favor clique em atualizar e aguarde que a página do Painel de Controle apareça.

Criando um jetPACK

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

- Comece copiando a configuração atual de seu ALB-X existente
  - Avançado
  - Software de atualização
  - Download da configuração atual
- Edite este arquivo com o Notepad++
- Abra um novo documento txt e chame-o de "yourname-jetPACK1.txt".
- Copiar todas as seções relevantes do arquivo de configuração para "yourname-jetPACK1.txt".
- Economize uma vez concluído

IMPORTANTE: Cada jetPACK é 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
```

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

Seção1:

```
[jetnexusdaemon]
```

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

Exemplos:

ConnectionTimeout=600000

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

ContentServerCustomTimer=20000

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

jnCookieHeader="MS-WSMAN

Este exemplo mudará o nome do cabeçalho do cookie usado no balanceamento de carga persistente de "jnAccel" padrão para "MS-WSMAN". Esta mudança em particular é necessária para Lync 2010/2013 proxy reverso.

Seção 2:

[jetnexusdaemon-Csm-Regras]

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

Exemplo:

[jetnexusdaemon-Csm-Rules-0]
Content="Server Up" (Servidor Up)
Desc="Monitor 1″
Método="CheckResponse" (VerificarResposta)
Name="Health Check- Is Server Up
Url="HTTP://demo.jetneus.com/healthcheck/healthcheck.html

Seção 3:

[jetnexusdaemon-LocalInterface]

Esta seção contém todos os detalhes na seção de Serviços IP. Cada interface é numerada e inclui sub-interfaces para cada canal. Se seu canal tem uma regra flightPATH aplicada, então ele também conterá uma seção Path.

Exemplo:

[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=">",""Grupo Seguro"",2000,"
2="192.168.101.11:80,Y,""IIS WWW Server 1″"""
3="192.168.101.12:80,Y,""IIS WWW Server 2″"""
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 este como exemplo abaixo.

Exemplo:

[jetnexusdaemon-Path-6]
Desc="Force to use HTTPS for certain directory" (Forçar o uso de HTTPS para determinado diretório)
Name="Gary - Forçar HTTPS"
[jetnexusdaemon-Path-6-Condition-1]
Check="contain" (conter)
Condição="caminho".
Match=
Sentido="faz".
Value="/secure/"
[jetnexusdaemon-Path-6-Evaluate-1]
Detalhe=
Fonte="host" (hospedeiro)
Valor=
Variable="$host$"[jetnexusdaemon-Path-6-Function-1]
Action="redirecionar"
Target="HTTPs://$host$$$path$$$querystring$"
Valor=

Introdução ao flightPATH

O que é FlightPATH?

flightPATH é um motor de regras inteligente desenvolvido pela Edgenexus para manipular e rotear o tráfego HTTP e HTTPS. Ele é altamente configurável, muito potente e, no entanto, muito fácil de usar.

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

A regra flightPATH tem três componentes:

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

O que o flightPATH pode fazer?

flightPATH pode ser usado para modificar o conteúdo e as solicitações HTTP de entrada e saída.

Além de utilizar 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, consulte este site útil https://www.regexbuddy.com/regex.html

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

Condição

Condição	Descrição	Exemplo
<form>	Os formulários HTML são usados para passar dados para um servidor	Exemplo "o formulário não tem comprimento 0".
Localização GEO	Isto compara o endereço IP de origem com o código de país ISO 3166	Localização GEO é igual a GB OU Localização GEO é igual a Alemanha
Anfitrião	Este é o hospedeiro 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 gota abaixo dos métodos HTTP	Esta é uma queda que inclui GET, POST etc.
Origem IP	Se o upstream proxy suporta X-Forwarded-for (XFF), ele usará o verdadeiro endereço de origem	IP do cliente. Também pode utilizar 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 POST	Verificar os dados que estão sendo carregados em um site

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=edgeNEXUS" Onde a partida é melhor e o valor é edgeNEXUS
Consulta String	Toda a cadeia de consulta após o caractere ?	
Solicite um Cookie	Este é o nome de um cookie solicitado por um cliente	MS-WSMAN=afYfn1CDqqCDqUD::
Cabeçalho de solicitação	Este pode ser qualquer cabeçalho HTTP	Referidor, Usuário-Agente, De, Data
Versão de solicitação	Esta é a versão HTTP	HTTP/1.0 OU HTTP/1.1
Corpo 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::
Cabeçalho de resposta	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, o IP do servidor proxy ou algum outro endereço IP agregado	ClientIP , Proxy IP, Firewall IP. Também pode utilizar múltiplos IP's e sub-redes. Você deve escapar dos pontos, pois estes são RegEX. Exemplo 10\.1\.2\.3 é 10.1.2.3

Combinar	**Descrição**	**Exemplo**
Aceitar	Tipos de conteúdo que são aceitáveis	Aceitar: texto/plainar
Aceitar-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>
Aceitar-Língua	Idiomas aceitáveis para resposta	Aceitar-Língua: pt-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Intervalos de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ=====
Carga-To	Contém informações de conta para os custos da aplicação do método solicitado	
Codificação de conteúdo	O tipo de codificação usada nos dados.	Codificação do conteúdo: gzip
Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (bytes de 8 bits)	Comprimento do conteúdo: 348
Tipo de conteúdo	O tipo de mímica 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 Set-Cookie (abaixo)	Cookie: $Version=1; Skin=new;
Data	Data e hora em que a mensagem foi originada	Data = "Data" ":" HTTP-date

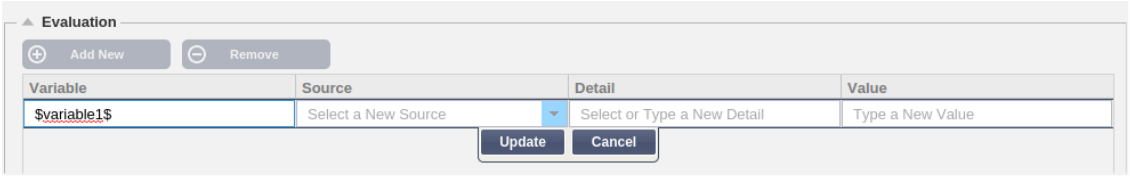
ETag	Um identificador para uma versão específica de um recurso, muitas vezes uma digestão de mensagem	ETag: "aed6bdb8e090cd1:0"
De	O endereço de e-mail do usuário que faz o pedido	De: user@example.com
Se-Modificado - desde	Permite que um 304 Não modificado seja devolvido se o conteúdo não for alterado	Se-Modificado - Desde: 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 Nov 1994 12:45:26 GMT
Pragma	Os cabeçalhos específicos da Implementação podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta ao pedido.	Pragma: sem cache
Referência	Este é o endereço da página web anterior a partir do qual um link para a página atualmente solicitada foi seguido	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 cadeia do agente de usuário do agente de usuário	Usuário-Agente: 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 solicitação para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova solicitação do servidor de origem.	Vary: Usuário-Agente
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 o detalhe da condição apenas que ela existe/não existe	Anfitrião - Existe - Existe
Início	A cadeia começa com o Valor	Caminho - Faz - Começa - /secura
Fim	O fio termina com o Valor	Caminho - Faz - Termina - .jpg
Conter	O fio contém o Valor	Solicitar cabeçalho - Aceitar - Fazer - Conter - imagem
Igual	O fio faz igualar o valor	Host - Does - Equal - www.edgenexus.io
Ter Comprimento	A corda tem o comprimento do valor	Hospedeiro - Tem - Tem Comprimento - 16 www.edgenexus.io = VERDADEIRO www.edgenexus.com = FALSO
Combinar RegEx	Isto permite que você entre em uma expressão regular compatível com Perl completa.	Origem IP - Faz - Combina Regex - 10/11.* | 11/11.*

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 verificar um nome específico de host

Avaliação



Adicionar uma variável é uma característica convincente que lhe permitirá extrair dados da solicitação e utilizá-los nas Ações. Por exemplo, você pode 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 $. Por exemplo, $variavel1$
- Fonte: Selecione na caixa drop-down a fonte da variável
- Detalhe: Selecione da lista quando relevante. Se a Fonte=Cabeçalho do Pedido, os Detalhes podem ser User-Agent
- Valor: Digite o texto ou expressão regular para afinar a variável.

Variáveis incorporadas:

- As variáveis embutidas já foram codificadas de forma difícil, portanto, não é necessário criar uma entrada de avaliação para elas.
- Você 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") = $respresp...
    - Anfitrião = $host$
    - Versão = $version$
    - Clientport = $clientport$
    - Clientip = $clientip$
    - Geolocalização = $geolocalização$".

Exemplo de ação:

- Ação = Redirecionar 302
    - Alvo = HTTPs://$host$/404.html
- Ação = Log
    - Meta = 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 de host original que usou, mas o caminho errado é substituído pelo 404.html

- Uma entrada é adicionada ao syslog dizendo "Um cliente de 154.3.22.14:3454 acabou de fazer um pedido à página wrong.html".

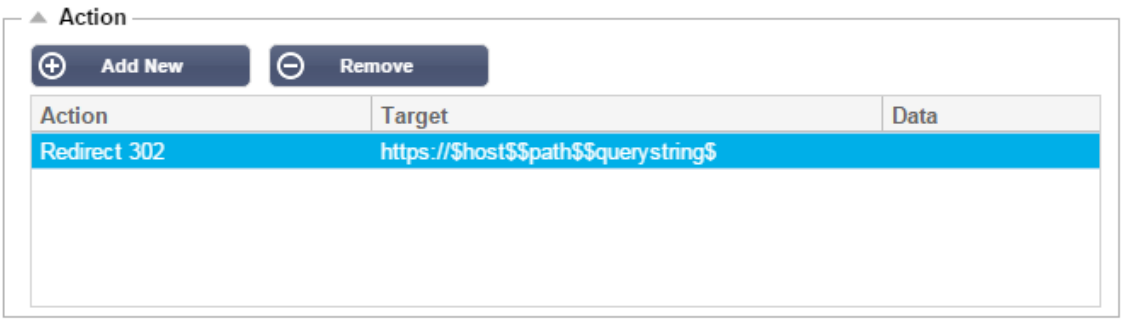
Fonte	Descrição	Exemplo
Cookie	Este é o nome e o valor do cabeçalho do cookie	MS-WSMAN=afYfn1CDqqCDqUD::Onde o nome é MS-WSMAN e o valor é afYfn1CDqqCDqUD::
Anfitrião	Este é o nome da hostname extraído do URL	www.mywebsite.com ou 192.168.1.1
Idioma	Este é o idioma extraído do cabeçalho do Idioma HTTP	Esta condição produzirá uma queda com uma lista de idiomas.
Método	Esta é uma gota abaixo dos métodos HTTP	O dropdown incluirá GET, POST
Caminho	Este é o caminho do site	/mywebsite/index.html
POST	Método de solicitação POST	Verificar os dados que estão sendo carregados em um site
Item de Consulta	Este é o nome e o valor de uma consulta. Como tal, ele pode aceitar o nome da consulta ou um valor também	"Best=jetNEXUS" Onde a partida é melhor e o valor é edgeNEXUS
Consulta String	Este é o fio inteiro após o ? caractere	HTTP://servidor/percurso/programa?query_string
Cabeçalho de solicitação	Isto pode ser qualquer cabeçalho enviado pelo cliente	Referidor, Usuário-Agente, De, Data...
Cabeçalho de resposta	Este pode ser qualquer cabeçalho enviado pelo servidor	Referidor, Usuário-Agente, 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
Aceitar-Codificação	Codificações aceitáveis	Aceitar-Codificação: <comprimir | gzip | esvaziar | sdch | identidade>
Aceitar-Língua	Idiomas aceitáveis para resposta	Aceitar-Língua: pt-US
Aceito-Alterações	Que tipo de conteúdo parcial este servidor suporta	Intervalos de aceitação: bytes
Autorização	Credenciais de autenticação para autenticação HTTP	Autorização: Básico QWxhZGRpbjpvcGVuIHNlc2FtZQ=====
Carga-To	Contém informações de conta para os custos da aplicação do método solicitado	
Codificação de conteúdo	O tipo de codificação usada nos dados.	Codificação do conteúdo: gzip
Comprimento do conteúdo	O comprimento do corpo de resposta em Octets (bytes de 8 bits)	Comprimento do conteúdo: 348
Tipo de conteúdo	O tipo de mímica 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 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-Modificado - Desde: 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 Nov 1994 12:45:26 GMT
Pragma	Cabeçalhos específicos de implementação que podem ter vários efeitos em qualquer lugar ao longo da cadeia de resposta ao pedido.	Pragma: sem cache
Referência	Este é o endereço da página web anterior, a partir do qual um link para a página atualmente solicitada foi seguido	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 cadeia do agente de usuário do agente de usuário	Usuário-Agente: Mozilla/5.0 (compatível; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)
Vary	Diz aos procuradores como combinar futuros cabeçalhos de solicitação para decidir se a resposta em cache pode ser usada em vez de solicitar uma nova solicitação do servidor de origem.	Vary: Usuário-Agente
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.

Meta

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

Você também pode digitar manualmente com algumas ações.

Dados

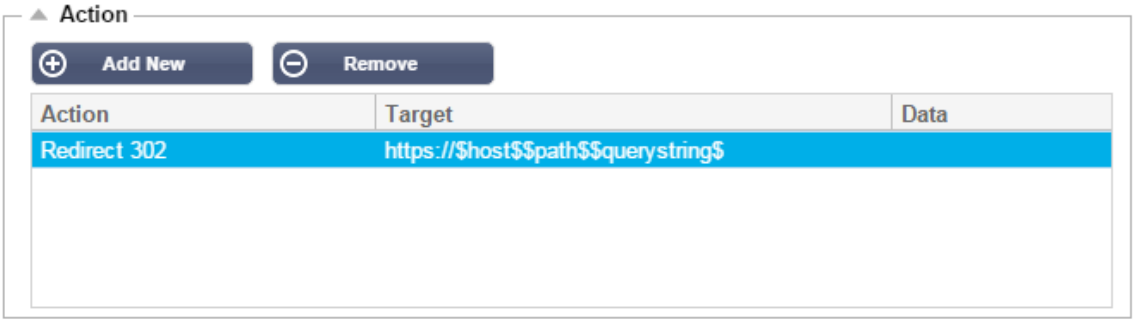
Clique duas vezes na coluna Dados para adicionar manualmente seus dados que você deseja adicionar ou substituir.

A lista de todas as ações está detalhada abaixo:

Ação	Descrição	Exemplo
Adicionar Pedido de Cookie	Adicionar cookie de solicitação detalhado na seção Objetivo com valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar cabeçalho de pedido	Adicionar um cabeçalho de solicitação do tipo Alvo com valor na seção Dados	Alvo= Aceitar Data= imagem/png
Adicionar bolinho de resposta	Adicionar Cookie de Resposta detalhado na seção Objetivo com valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Adicionar 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	Pesquisar o órgão de resposta e substituir todas as instâncias	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)
Substituir primeiro o corpo	Pesquisar o Órgão de Resposta e substituir apenas a primeira instância	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)
Substituir Body Replace Last	Pesquisar o Órgão de Resposta e substituir apenas em última instância	Target= HTTP:// (Cadeia de busca) Data= HTTPs:// (Cadeia de substituição)
Queda	Isto irá soltar a conexão	Alvo= N/A Data= N/A
e-Mail	Enviará um e-mail para o endereço configurado em Eventos por e-mail. Você pode usar uma variável como o endereço ou a mensagem	Target= "flightPATH enviou este evento por e-mail". Data= N/A
Log Event	Isto registrará um evento no registro do Sistema	Target= "flightPATH logou isto no syslog". Data= N/A
Redirecionar 301	Isto irá emitir um redirecionamento permanente	Target= HTTP://www.edgenexus.ioData= N/A
Redirecionar 302	Isto irá emitir um redirecionamento temporário	Target= HTTP://www.edgenexus.ioData= N/A
Retirar Pedido Cookie	Remover cookie de solicitação detalhado na seção Objetivo	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii
Remover cabeçalho de solicitação	Remover o cabeçalho do pedido detalhado na seção Objetivo	Target=ServerData=N/A
Remover Cozinheiro de Resposta	Remover cookie de resposta detalhado na seção Objetivo	Target=jnAccel
Remover cabeçalho de resposta	Remover o cabeçalho de resposta detalhado na seção Objetivo	Meta= Etag Data= N/A
Substituir Pedido de Cookie	Substituir o cookie de solicitação detalhado na seção Objetivo pelo valor na seção Dados	Alvo= Cookie Data= MS-WSMAN=afYfn1CDqqCDqCVii

Substituir o cabeçalho de solicitação	Substituir o cabeçalho da solicitação no campo de destino pelo valor dos dados	Alvo= Conexão Data= manter vivo
Substituir o Cookie de Resposta	Substituir o cookie de resposta detalhado na seção Objetivo pelo valor na seção Dados	Target=jnAccel=afYfn1CDqqCDqCViiDate=MS-WSMAN=afYfn1CDqqCDqCVii
Substituir o cabeçalho de resposta	Substituir o cabeçalho de resposta detalhado na seção Objetivo pelo valor na seção Dados	Alvo= Servidor Data= Retenção de dados para segurança
Re-escrever o caminho	Isso permitirá que você redirecione o pedido para uma nova URL, com base na condição	Target= /test/path/index.html$querystring$ Data= N/A
Use o Servidor Seguro	Selecione qual servidor seguro ou serviço virtual a ser utilizado	Target=192.168.101: 443Data=N/A
Usar Servidor	Selecione o servidor ou serviço virtual a ser utilizado	Target= 192.168.101:80Data= N/A
Cookie Encriptado	Isto irá criptografar os cookies 3DES e depois codificá-los com base64	Target= Digite o nome do cookie a ser criptografado, você pode usar o * como um curinga no finalData= Digite uma frase de passe 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, caminho e querystring que a solicitação.

Usos comuns

Firewall de Aplicação e Segurança

- Bloquear IPs indesejados
- Forçar o usuário a HTTPS para conteúdo específico (ou todo)
- Bloquear ou redirecionar aranhas
- Prevenir e alertar sobre roteiros cruzados no local
- Prevenir e alertar a injeção SQL
- Ocultar a estrutura interna do diretório
- Reescrever cookies
- Diretório seguro para usuários específicos

Características

- Redirecionar os usuários com base no caminho
- Fornecer sinal único em múltiplos sistemas
- Usuários do segmento com base em User ID ou Cookie
- Adicionar cabeçalhos para descarregar SSL

- Detecção de idiomas
- Reescrever solicitação do usuário
- Consertar URLs quebradas
- Códigos de resposta Log e Email Alert 404
- 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 = Combinar RegEx
- Valor = \.htm$

Avaliação:

- Em branco

Ação:

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

Index.html

Forçar a utilização 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
- Alvo = 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 = isto precisa de uma reflexão adequada
- Sentido =
- Verificação =

Avaliação:

- Em branco

Ação:

- Ação =
- Alvo =

Ocultar CGI-BBIN:

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

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

- Condição = Anfitrião
- Sentido = Faz
- Verificar = Combinar RegEX
- Valor = \.cgi$

Avaliação:

- Em branco

Ação:

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

Aranha de madeira

Pedidos de aranha de registro de motores de busca populares.

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

- Condição = Cabeçalho de solicitação
- Combinação = Usuário-Agente
- Sentido = Faz
- Verificar = Combinar RegEX
- Valor = Googlebot|Slurp|bingbot|ia_archiver

Avaliação:

- Variável = $crawler$
- Fonte = Cabeçalho de solicitação
- Detalhe = Usuário-Agente

Ação:

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

Forçar HTTPS

Forçar a utilização de HTTPS para determinados diretórios. Neste 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
- Verificar = Conter
- Valor = /secure/

Avaliação:

- Em branco

Ação:

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

Fluxo de mídia:

Redireciona o Flash Media Stream para o serviço apropriado.

Condição:

- Condição = Caminho
- Sentido = Faz
- Verificação = 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
- Verificação = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Body Replace All
- 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
- Verificação = Igual
- Valor = 200 OK

Avaliação:

- Em branco

Ação:

- Ação = Body Replace All
- 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

Validade do conteúdo

Adicionar uma data de validade de conteúdo sensata à página para reduzir o número de solicitações e 304s.

Condição: esta é uma condição genérica como um "catch all". É recomendável focalizar esta condição em sua

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

Avaliação:

- Em branco

Ação:

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

Tipo de servidor falso

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

Condição: esta é uma condição genérica como um "catch all". É recomendável focalizar esta condição em sua

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

Avaliação:

- Em branco

Ação:

- Ação = Substituir cabeçalho de resposta
- Alvo = Servidor
- Dados = Secreto

Nunca enviar erros

O cliente nunca recebe nenhum erro de seu site.

Condição

- Condição = Código de resposta
- Sentido = Faz

- Verificar = Conter
- Valor = 404

Avaliação

- Em branco

Ação

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

Redirecionar no idioma

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

Condição

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

Avaliação

- Variável = $modelo_de_anfitrião$
- 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 alterar o valor MYGOOGLECODE para seu ID do Google UA.

Condição

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

Avaliação

- em branco

Ação

- Ação = Body Replace Last
- 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>

Portal IPv6

Ajuste o Header Host para Servidores IPv4 IIS em Serviços IPv6. Os servidores IPv4 IIS não gostam de ver um endereço IPV6 no pedido do cliente host, portanto, esta regra substitui este por um nome genérico.

Condição

- em branco

Avaliação

- em branco

Ação

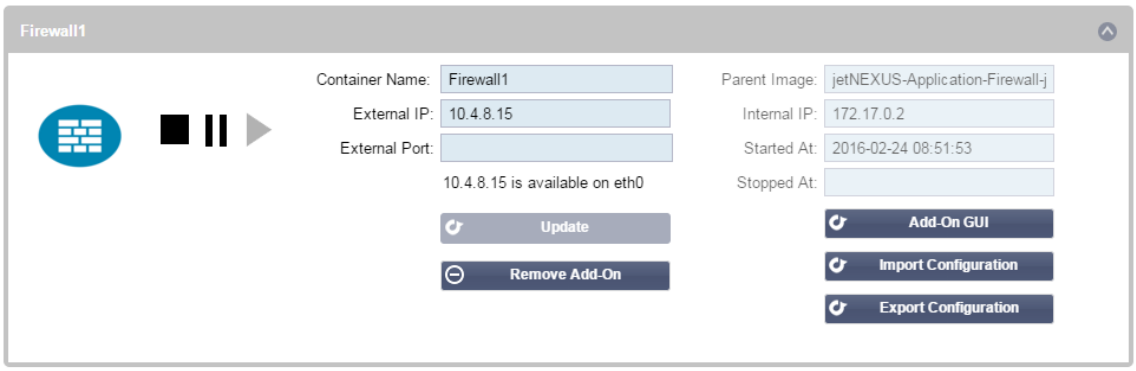
- Ação = Substituir cabeçalho de solicitação
- Alvo = Anfitrião
- Dados =ipv4.host.header

Firewall de Aplicação Web (edgeWAF)

O Web Application Firewall (WAF) está disponível mediante solicitação e é licenciado anualmente. A instalação do WAF é feita utilizando a seção inbuilt Apps dentro do ADC.

Executando o WAF

Operando em um Docker Container, o WAF precisa de alguns parâmetros de rede a serem definidos antes de ser iniciado.

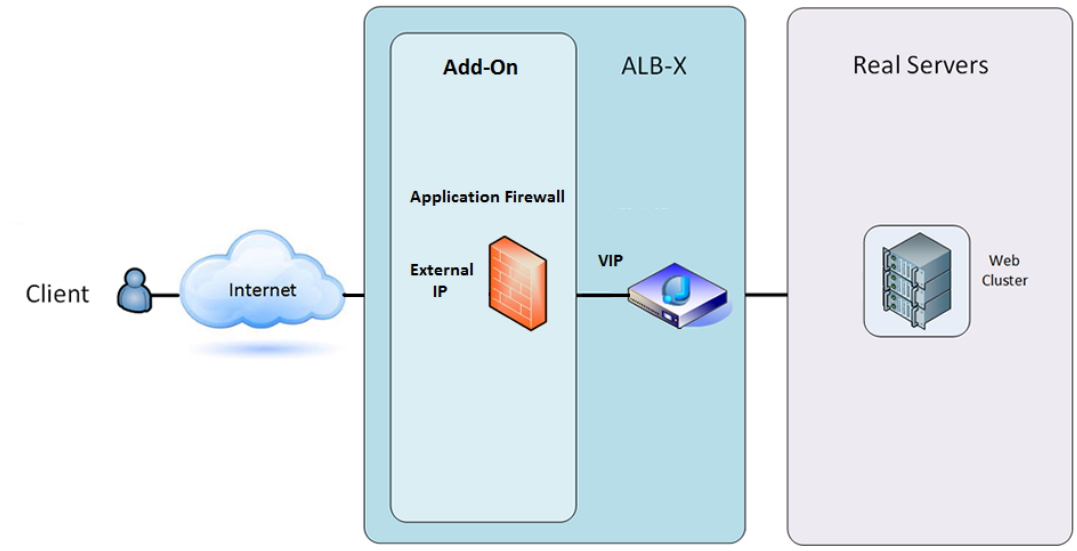


Opção	**Descrição**
Parada	Ficará cinzento até que se inicie uma instância de Add-On. Pressione este botão para parar a instância do Docker.
Pausa	Este botão fará uma pausa no Add-On.
Reproduzir	Ele iniciará o Add-On com as configurações atuais.
Nome do contêiner	Dê um nome ao seu container para identificá-lo a partir dos outros containers. Isto deve ser único. Você pode usá-lo como o nome de um servidor real se desejar e ele se resolverá automaticamente para o endereço IP interno da instância.
PI externa	Aqui você pode definir um IP externo para acessar seu Add-On. Isto pode ser para acessar a GUI do Add-On, bem como o serviço que roda através do Add-On. No caso do Firewall Add-On, este é o endereço IP do seu serviço HTTP. O Firewall pode então ser configurado para acessar um servidor ou um ALB-X VIP que contenha vários servidores para balanceamento de carga.
Porto externo	Se você deixar isto em branco, então todas as portas serão encaminhadas para seu Firewall. Para restringir isto, basta adicionar na lista de portas separadas por vírgulas. Exemplo 80, 443, 88. Observe que o endereço GUI do Firewall será **HTTP///[IP externo]88/waf.** Portanto, deixe a configuração da Porta Externa em branco ou adicione a porta 88 para acessar a GUI se você estiver restringindo a lista de portas.
Atualização	Você só pode atualizar as configurações de um Add-On uma vez que ele tenha sido interrompido. Uma vez parada sua instância, você pode mudar o nome do Container, o IP externo e as configurações da porta externa.
Remover Add-On	Irá remover completamente o Add-On da página Add-On. Você precisará ir à página Library-Apps para implantar o Add-On novamente.
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 isto ajudará a distinguir entre eles. Esta seção é apenas para fins informativos e, portanto, é cinzenta.
IP interno	O Docker cria automaticamente o endereço IP interno e, portanto, não pode ser editado. Se você parar a instância do Docker e reiniciar, um novo endereço IP interno será emitido. É por esta razão que você deve usar um endereço IP externo para seu serviço ou usar o Container Name para o endereço real do servidor de seu serviço.

Começou em	Isto indicará a data e a hora em que o Add-On foi iniciado. Exemplo 2016-02-16 155721
Parou em	Isto 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

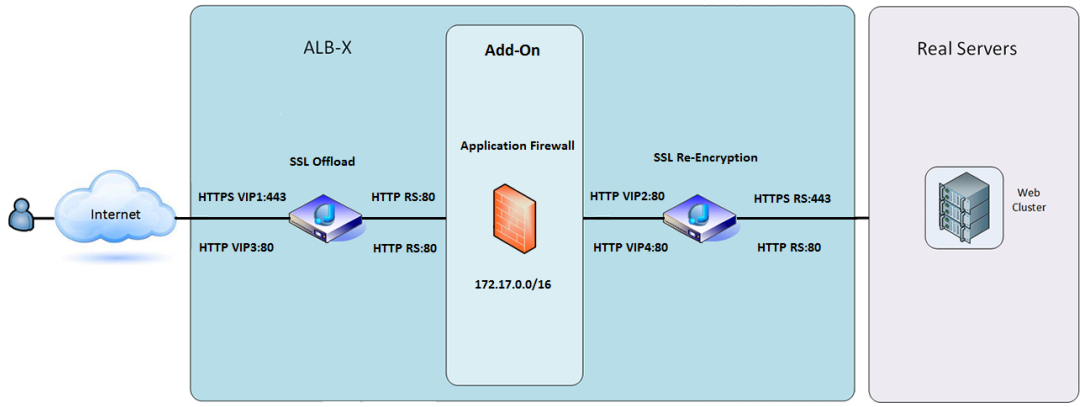


Nesta arquitetura, somente HTTP pode ser usado para seu serviço, pois o Firewall não pode inspecionar o tráfego HTTPS.

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 seu cluster web.

WAF usando endereço IP interno



Nesta arquitetura, você pode especificar HTTP e HTTPS.

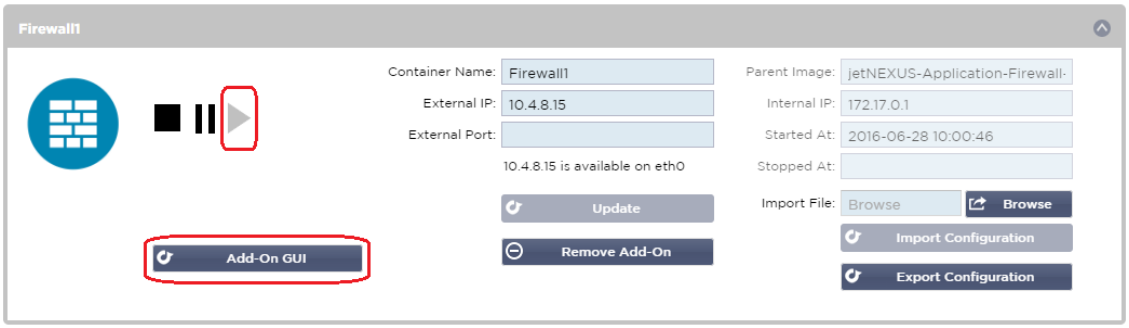
HTTPS pode ser de ponta a ponta onde as conexões do Cliente ao ALB-X são criptografadas e do ALB-X para os Servidores Reais.

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

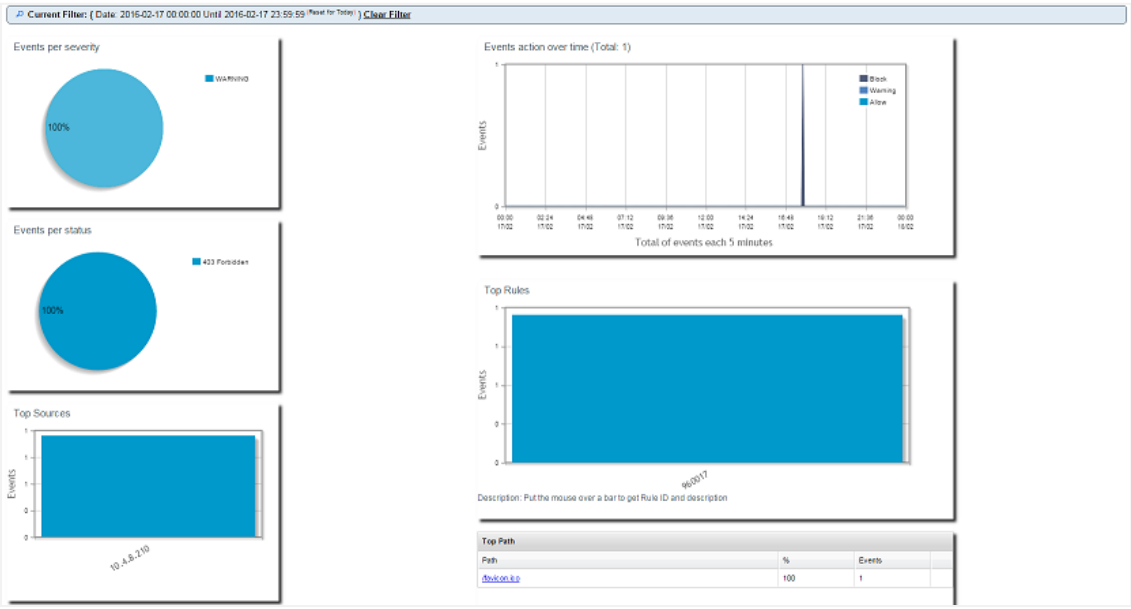
Uma vez que o tráfego tenha passado pelo Firewall, ele é então encaminhado para outro VIP que pode então reencriptar o tráfego e o equilíbrio de carga para proteger os servidores ou simplesmente carregar o equilíbrio para servidores inseguros através de HTTP.

Acesso ao seu WAF add-on

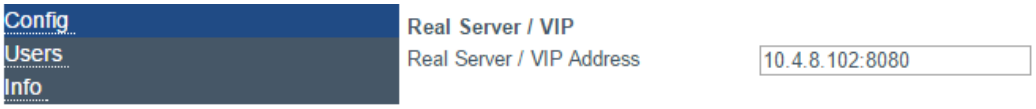
- Preencha os detalhes para seu Firewall
- Você pode restringir seus portos ao que você precisa ou deixá-los em branco para permitir todos os portos
- Clique no botão Play
- Aparecerá um botão GUI Add-On



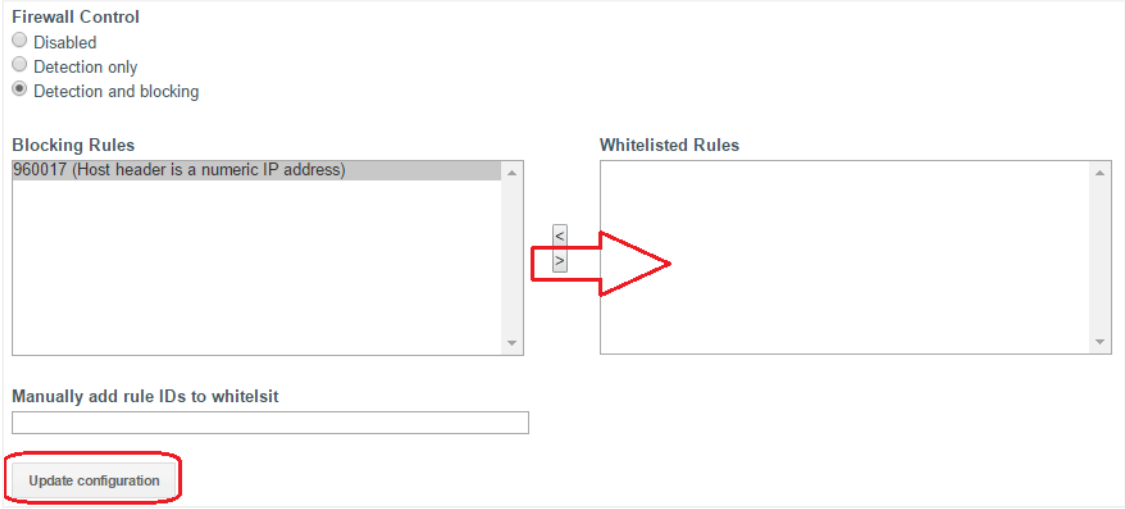
- Clique neste botão, e ele abrirá um navegador em HTTP://[IP externo]:88/waf
- Neste exemplo, será HTTP://10.4.8.8.15:88/waf
- Você será presenteado com um diálogo de login.
- Digite as credenciais para seu ADC.
- Após a conclusão de um login bem sucedido, você será presenteado com a página inicial do WAF.



- A página inicial apresenta uma visão gráfica dos eventos, ou seja, as ações de filtragem realizadas pelo Firewall de Aplicação.
- Os gráficos muito provavelmente estarão em branco quando você abrir a página pela primeira vez, pois não haverá tentativas de acesso através do firewall.
- Você pode configurar o endereço IP ou o nome de domínio do site para o qual você gostaria de enviar o tráfego após o firewall ter filtrado o mesmo.
- Isto pode ser alterado na seção Administração > Config



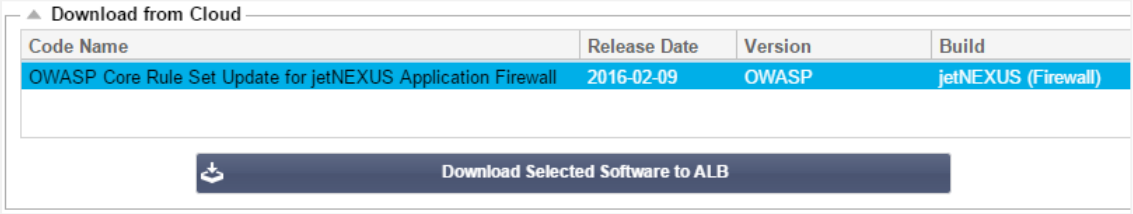
- O Firewall inspecionará o tráfego e depois o enviará para o endereço IP ou VIP do Real Sever aqui. Você também pode entrar em uma porta junto com seu endereço IP. Se você digitar um endereço IP por conta própria, a porta será assumida como porta 80. Clique no botão "Atualizar Configuração" para salvar esta 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 Lista Branca.
- Para evitar que o firewall bloqueie o recurso de aplicação válido, favor mover a regra de bloqueio para a seção Regras da Lista Branca.



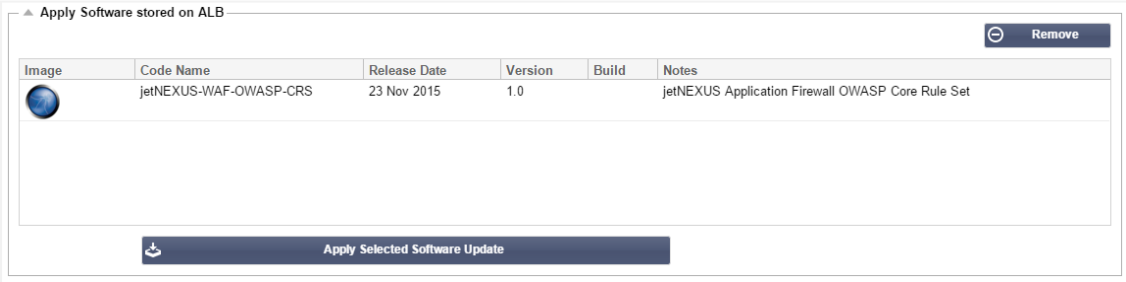
- Pressione Atualizar Configuração quando você tiver transferido todas as regras da seção Bloqueio para a seção Lista Branca.

Atualização das regras

- As regras de Firewall de Aplicação podem ser atualizadas acessando a seção Avançado - Software
- Clique em Atualizar para ver o botão de software disponível na seção Detalhes de Atualização de Software
- Uma caixa adicional chamada Download from Cloud é agora exibida
- Verifique se há um conjunto de regras centrais OWASP disponíveis

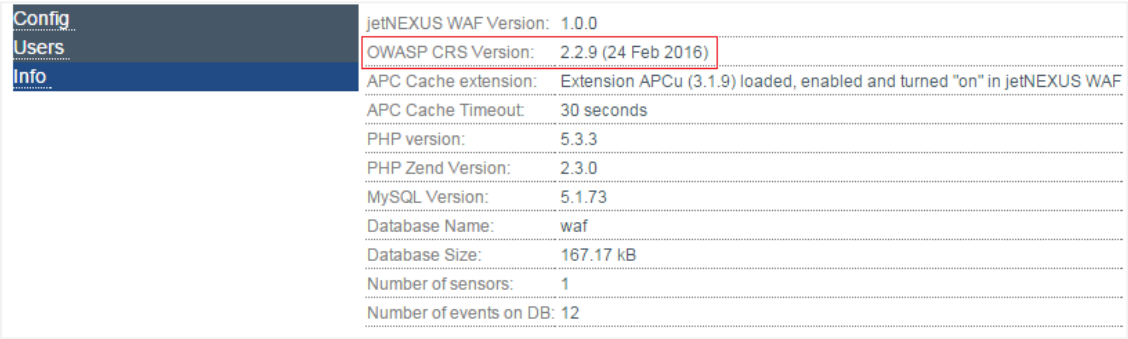


- Se for o caso, você pode destacar e clicar em Download Selected Software to ALB-X
- Esta ação fará o download do arquivo inteligente para o software Apply Software armazenado no ALB



- 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 atualizado, carregará e o aplicará.

- As identificações das regras da Whitelist serão mantidas. Entretanto, novas regras podem começar a bloquear recursos de aplicação válidos.
- Favor verificar a lista de Regras de Bloqueio na página da Lista Branca neste caso.
- Você também pode verificar a seção Informações Gerenciais da GUI Firewall para a versão OWASP CRS



Balanceamento de carga do servidor global(edgeGSLB)

Introdução

Global Server Load Balancing (GSLB) é um termo usado para descrever métodos de distribuição do tráfego de rede pela Internet. O GSLB é diferente do Equilíbrio de Carga do Servidor (SLB) ou Equilíbrio de Carga de Aplicações (ALB), pois é tipicamente usado para distribuir tráfego entre vários centros de dados, enquanto um ADC/SLB tradicional é usado para distribuir tráfego dentro de um único centro de dados.

A GSLB é tipicamente utilizada nas seguintes situações:

Resiliência e recuperação de desastres

Você tem vários centros de dados, e deseja executá-los em uma situação Ativa-Passiva para que, se um centro de dados falhar, o tráfego seja enviado para o outro.

Balanceamento de carga e geo-localização

Você gostaria de distribuir o tráfego entre centros de dados em uma situação Active-Active 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 você possa enviá-los para seu centro de dados mais próximo), etc.

Considerações comerciais

Assegurar que usuários de locais geográficos específicos sejam enviados a centros de dados específicos. Assegurar que conteúdos diferentes sejam servidos (ou bloqueados) a outros usuários, dependendo de vários critérios, 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; assim, vale a pena gastar o tempo para entender como funciona o misterioso sistema DNS (Domain Name Server).

O DNS consiste em três componentes-chave:

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

Uma transação DNS típica 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 consulta um servidor de nomes raiz 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 domínio .com TLD.
- O servidor TLD responde então com o endereço IP do servidor de nomes do domínio, exemplo.com.
- Finalmente, o resolvedor recursivo envia uma consulta ao servidor de nomes do domínio.
- O endereço IP, por exemplo.com, é então devolvido ao resolvedor a partir do nameserver.

- O resolvedor DNS responde então ao navegador web com o endereço IP do domínio solicitado inicialmente.
- Uma vez que as oito etapas da pesquisa DNS tenham retornado o endereço IP, por exemplo.com, o navegador pode solicitar a página web:
- O navegador faz uma solicitação **HTTP** para o endereço IP.
- O servidor naquele IP retorna a página da web para ser renderizada no navegador.

Este processo pode ser ainda mais complicado:

Caching

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

Nota: Para testes, paramos e desativamos o Cliente DNS do Windows dentro da seção de serviços de seu sistema operacional. Os nomes DNS continuarão a ser resolvidos; no entanto, ele não armazenará os resultados nem registrará o nome do computador. Seu administrador de sistema precisará decidir se esta 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), ou seja, o tempo de cache para a resposta.

Visão geral da GSLB

A GSLB é baseada no DNS e utiliza 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. Entretanto, para aplicar qualquer lógica, o sistema deve primeiro receber a solicitação DNS.

Vários projetos permitem isso. O primeiro é onde a GSLB atua como o servidor de nomes autorizado.

O segundo projeto é a implementação mais comum e é semelhante à configuração autorizada do nameserver, mas utiliza 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 controlar o que é e o que não é tratado pela GSLB. Neste caso, você não precisa encaminhar todo o tráfego DNS para a GSLB para sistemas que não requerem a GSLB.

A redundância é fornecida para que, se um servidor de nomes (GSLB) falhar, então o servidor de nomes remoto emite automaticamente outro pedido para outro GSLB, impedindo que o website caia.

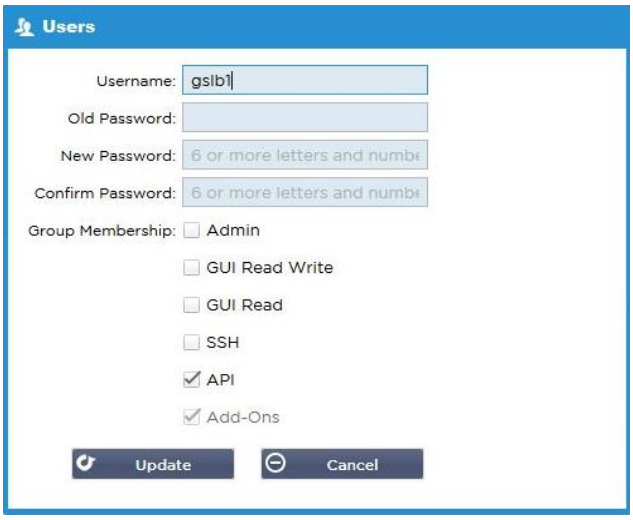
Configuração da GSLB

Após baixar o GSLB Add-On, por favor, implante-o visitando a página Library > Apps da GUI do ADC e clicando no botão "Deploy" como mostrado abaixo.

Após a instalação, por favor, configure os detalhes do GSLB Add-On, incluindo Nome do Container, IP Externo e Portos Externos na Biblioteca > Página Add-Ons do ADC GUI, como mostrado na figura abaixo.

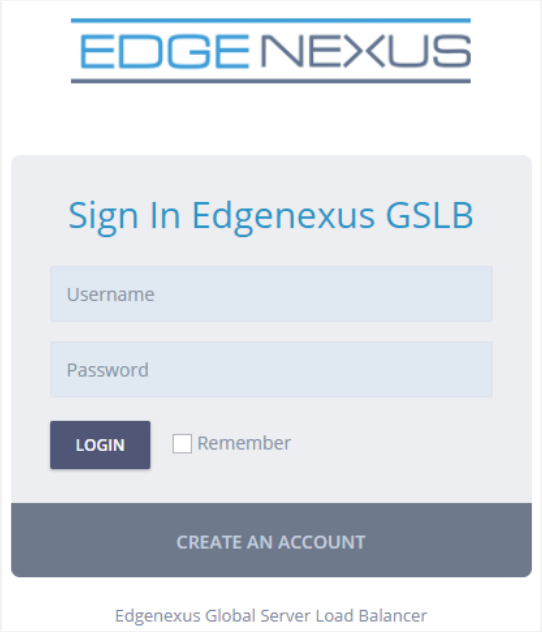
- Container Name é um nome único de um Add-On em execução, hospedado pela ADC, é usado para distinguir vários Add-Ons de um mesmo tipo.
- IP externo é o IP em sua rede que será atribuído à GSLB.
- Você deve configurar a GSLB para ter um endereço IP externo se quiser tomar decisões baseadas na GEO, pois isto permitirá que a GSLB veja o endereço IP real dos clientes.
- Portos externos é a lista de portas TCP e UDP da GSLB, que podem ser acessadas de outros hosts 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).
- Após configurar os detalhes do Add-On, clique no botão Update (Atualizar).
- Inicie o 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.
- Por favor, visite a página Sistema > Usuários do ADC GUI e edite um usuário com o mesmo nome do GSLB Add-On que você implantou, como mostrado na figura abaixo.
- Edite o usuário "gslb1" e marque API, depois clique em Atualizar - em versões posteriores do software pode já ter sido marcado por padrão.



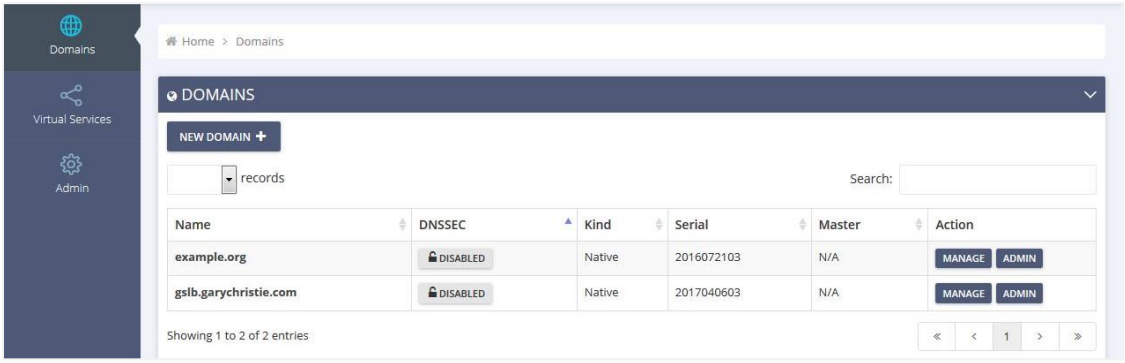
- O próximo passo só é necessário se você estiver configurando a GSLB para fins de teste ou avaliação e não quiser modificar nenhum dado da zona DNS na Internet.
- Neste caso, favor instruir o ADC a usar o GSLB Add-On como seu servidor de resolução DNS primário alterando "DNS Server 1 na página Sistema > Rede da GUI do ADC, como mostrado na figura abaixo.
- O DNS Server 2 pode ser configurado geralmente com seu servidor DNS local ou um na Internet, como o Google 8.8.8.8.

- Agora é a hora de fazer o login na GSLB GUI.
- Navegue até a página Biblioteca > Add-Ons da GUI do ADC e clique no botão Add-On GUI.
- Clicando em uma nova guia do navegador que apresenta a página de login da GSLB GUI, como mostrado abaixo.

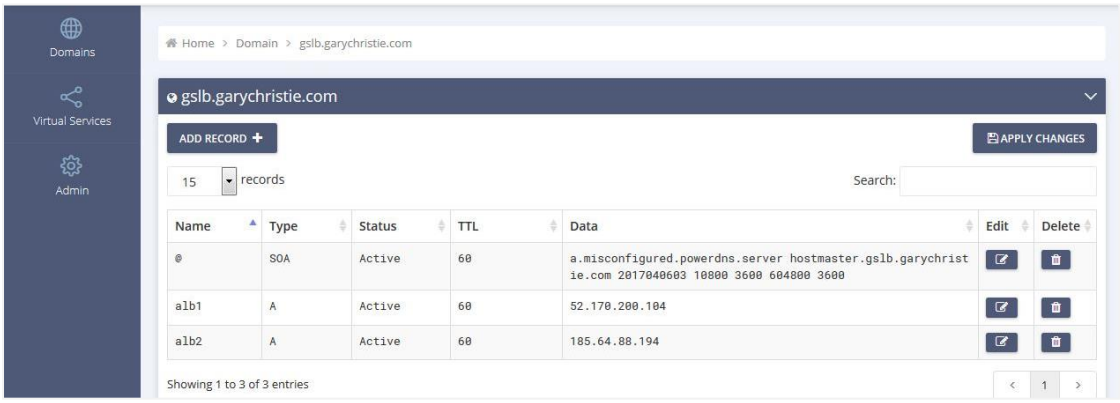


- O nome de usuário padrão é admin, e a senha padrão é jetnexus. Por favor, não esqueça de mudar sua senha na página Administrador > Meu perfil da GUI GSLB.
- O próximo passo na seqüência de configuração é criar uma zona DNS no servidor de nomes PowerDNS, que faz parte da GSLB, tornando-a ou um servidor de nomes autorizado para a zona "example.org" ou uma zona de subdomínios, como o subdomínio "geo.example.org" mencionado na seção "DNS-based GSLB Overview" acima.
- Para maiores detalhes sobre a configuração da zona DNS, consulte a **DOCUMENTAÇÃO DO POWERDNS NAMESERVER**. Uma zona de exemplo é mostrada na Figura 6.

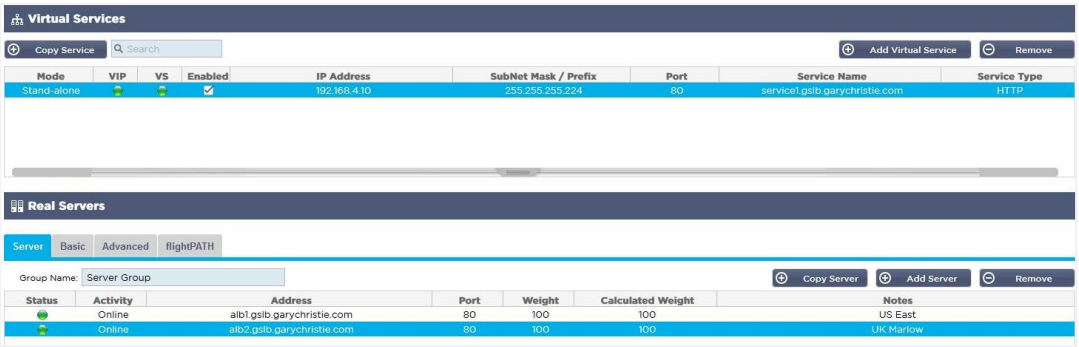
* edgeNEXUS GSLB GUI é baseado em um projeto de código aberto PowerDNS-Admin.



- Após criar uma zona DNS, clique no botão Gerenciar e adicione nomes de host ao domínio, como mostrado na figura abaixo.
- Depois de editar qualquer registro existente dentro do GUI da GSLB, por favor pressione o botão Salvar.
- Depois de concluir a criação de registros de nomes de host, clique no botão Aplicar mudanças. Se você não clicar em Aplicar e depois emendar a página, você perderá suas mudanças.
- Abaixo criamos registros que são registros de endereços IPv4.
- Certifique-se de criar um registro para todos os registros que você deseja ter resolvido, incluindo registros AAAA para endereços IPv6.

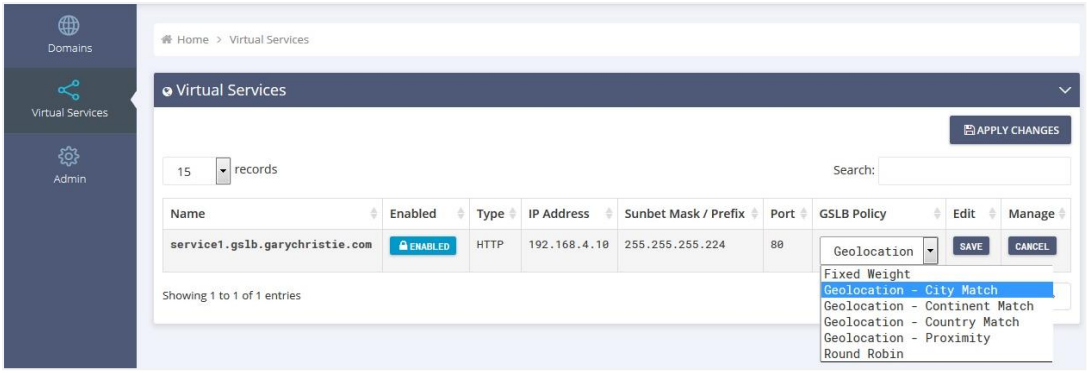


- Agora, vamos voltar à GUI do ADC e definir um Serviço Virtual que corresponda à zona DNS que acabamos de criar.



- O Serviço Virtual será usado para verificação da saúde dos servidores no domínio da GSLB.
- A GSLB utiliza o mecanismo de verificação da saúde do ADC, incluindo monitores personalizados. Ele pode ser usado com qualquer um dos tipos de serviço suportados pelo ADC.
- Navegue até a página Serviços > Serviços IP da GUI da ADC e crie um Serviço Virtual, como mostrado na figura abaixo.
- Certifique-se de configurar o Nome de Serviço com o nome de domínio correto que você deseja usar na GSLB. A GSLB lerá isto através da API e preencherá automaticamente a seção Serviços Virtuais na GUI da GSLB.
- Favor adicionar todos os servidores no domínio GSLB sob a seção Servidores Reais da imagem acima.
- Você pode especificar os servidores, seja por seus nomes de domínio ou endereços IP.

- Se você especificar os nomes de domínio, então utilizará os registros criados em seu GSLB.
- Você pode escolher diferentes métodos e parâmetros de monitoramento da saúde do servidor nas abas Básica e Avançada.
- Você pode definir a atividade de alguns servidores como Standby para um cenário Ativo-Passivo.
- Neste caso, se um servidor "Online" falhar uma verificação de saúde e houver um servidor Standby saudável, a Edgenexus EdgeGSLB resolverá o nome de domínio para um endereço do servidor Standby.
- Consulte a seção **SERVIÇOS VIRTUAIS** para obter detalhes sobre a configuração dos Serviços Virtuais.
- Agora, vamos passar para a 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.
- Isto é mostrado na figura abaixo.



- A 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 aleatoriamente.
Ponderada Round Robin	Escolha os 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	City match - 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 isto não for possível, selecione um servidor que esteja localizado mais próximo da localização do cliente usando dados de latitude e longitude geográficas.
Geolocalização	Combinação de países - escolha um servidor no mesmo país que o cliente. Se não houver um servidor no mesmo país, tente o mesmo continente, então tente a localização mais próxima.
Geolocalização	Combinação 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 GSLB, não esqueça de clicar no botão Apply Changes (Aplicar mudanças).
- Agora você pode rever e ajustar os detalhes do Serviço Virtual, clicando no botão Gerenciar.
- Isto apresentará uma página mostrada abaixo.
- Se você selecionou uma das políticas baseadas no peso, talvez seja necessário ajustar os pesos do servidor GSLB.
- Se você selecionou uma das políticas GSLB baseadas em geo-localização, talvez seja necessário especificar dados geográficos para os servidores.

- Se você não especificar nenhum dado geográfico para os servidores, a GSLB usará os dados fornecidos pelo **BANCO DE DADOS GEOLITE2 DO MAXMIND**.
- Você também pode modificar o nome do servidor, porta e atividade nesta página.
- Estas mudanças serão sincronizadas com o ADC quando você clicar no botão "Apply Changes" (Aplicar Mudanças).

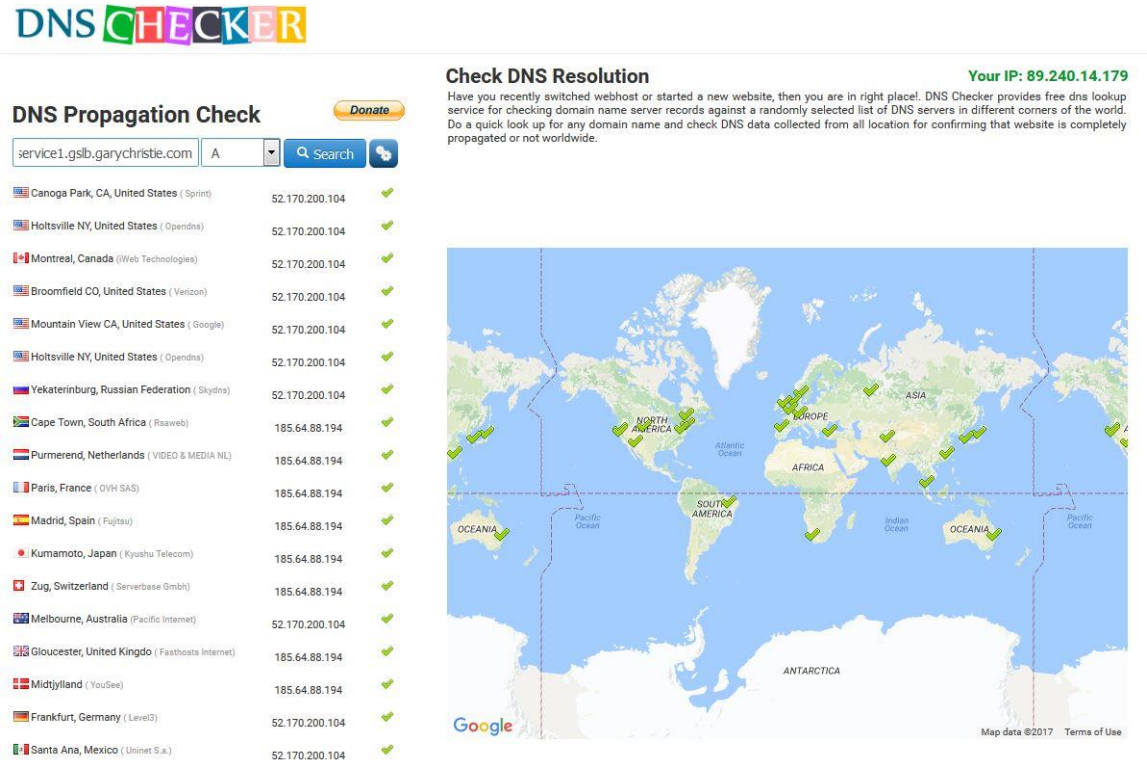
- Uma ótima maneira de verificar as respostas que a GSLB enviará aos clientes é usar o NSLOOKUP.
- Se você estiver usando Windows, o comando está abaixo.

NSLOOKUP service1.gslb.garychristie.com 192.168.4.10

- Onde service1.gslb.garychristie.com é o nome de domínio que você deseja resolver.
- Onde 192.168.4.10 é o endereço IP externo de sua GSLB.
- Para verificar qual endereço IP será devolvido na Internet, você pode usar o servidor DNS do google do 8.8.8.8.

Nslookup service1.gslb.garychristie.com 8.8.8.8.8.

- Alternativamente, você pode usar algo como HTTPs://dnschecker.org. Exemplo HTTPs://dnschecker.org/#A/service1.gslb.garychristie.com.
- Veja abaixo um exemplo dos resultados.



Localizações personalizadas

Redes Privadas

O GSLB também pode ser configurado para usar locais personalizados para que você 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. Este método funciona perfeitamente bem com endereços IP públicos, mas não existe tal banco de dados para endereços privados internos que estejam em conformidade com a RFC 1918 para endereços IPv4 e a RFC 4193 para endereços IPv6.

Favor ver a página da Wikipedia explicando os endereços privados
HTTPS://PT.WIKIPEDIA.ORG/WIKI/PRIVATE_NETWORK

Como funciona

Normalmente, a idéia por trás do uso de nosso GSLB para redes internas é para que os usuários de endereços específicos recebam uma resposta diferente para um serviço, dependendo da rede em que estão 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 precisamos 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
- Atribuir cada serviço ao respectivo local

Como configuramos este visual na GSLB?

Adicionar um local para o Centro de Dados do Norte

- Clique em Localizações personalizadas no lado esquerdo
- Clique em Adicionar local
- Nome
  - Norte
- Adicione um endereço IP privado e uma máscara de sub-rede para sua rede do Norte. Para este exercício, assumiremos que o serviço e os endereços IP do cliente estão na mesma rede privada
  - 10.1.1.0/24
- Adicionar o código do continente
  - UE
- Adicionar o código do país
  - REINO UNIDO
- Adicionar Cidade
  - Enfield
- Adicionar Latitude - obtido no google
  - 51.6523
- Adicionar Longitude - obtido no google
  - 0.0807

Nota, por favor use os códigos corretos que podem ser obtidos aqui

Adicionar um local para o Centro de Dados do Sul

- Clique em Localizações personalizadas no lado esquerdo
- Clique em Adicionar local
- Nome
  - Sul
- Adicione um endereço IP privado e uma máscara de sub-rede para sua rede Sul. Assumiremos que o serviço e os endereços IP do cliente estão na mesma rede privada para este exercício.
  - 192.168.1.0/24
- Adicionar o código do continente
  - UE
- Adicionar o código do país
  - REINO UNIDO
- Adicionar Cidade
  - Croydon
- Adicionar Latitude - obtido no google
  - 51.3762
- Adicionar Longitude - obtido no google
  - 0.0982

Nota, por favor use os códigos corretos que podem ser obtidos **AQUI**

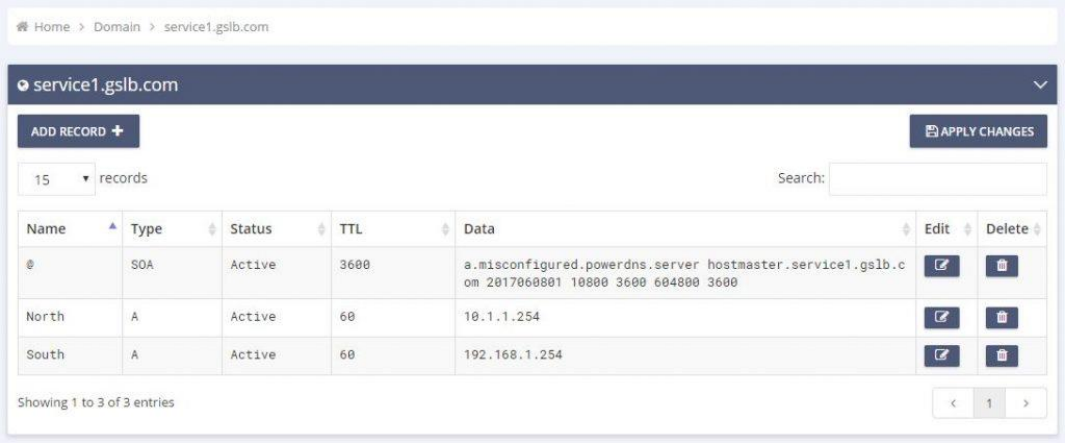
Adicionar um registro A para north.service1.gslb.com

- Clique no serviço de domínio1.gslb.com
- Clique em Adicionar registro
- Adicionar nome
  - Norte
- Tipo
  - A
- Status
  - Ativo
- TTL
  - 1 Minuto
- Endereço IP
  - 10.1.1.254 (Note que isto está na mesma rede que a localização Enfield)

Adicionar um registro A para south.service1.gslb.com

- Clique no serviço de domínio1.gslb.com
- Clique em Adicionar registro
- Adicionar nome
  - Sul
- Tipo
  - A
- Status
  - Ativo

- TTL
  - 1 Minuto
- Endereço IP
  - 192.168.1.254 (Note 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
- A GSLB analisa seus registros A para o service1.gslb.com e combina com o north.service1.gslb.com como também está na rede 10.1.1.0/24
- GSLB responde ao 10.1.1.23 com o endereço IP 10.1.1.254 para service1.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 Custom Location
- A GSLB examina seus registros A para o service1.gslb.com e combina 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 service1.gslb.com

Suporte Técnico

Fornecemos suporte técnico a todos os nossos usuários de acordo com os termos de serviço padrão da empresa.

Forneceremos todo o suporte via suporte técnico se você tiver um contrato de Suporte e Manutenção ativo para o edgeADC, edgeWAF ou edgeGSLB.

Para levantar um ticket de apoio, favor visitar:

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