# Implantação e configuração do VMware Unified Access Gateway

Unified Access Gateway 3.0

vmware®

Você pode encontrar a documentação técnica mais atualizada no site da VMware, em:

https://docs.vmware.com/br/

O site da VMware também fornece as atualizações mais recentes de produtos.

Caso tenha comentários sobre esta documentação, envie seu feedback para:

docfeedback@vmware.com



**VMware, Inc.**
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

# Conteúdo

# Implantação e configuração do VMware Unified Access Gateway

A *Implantando e configurando o Unified Access Gateway* fornece informações sobre a implantação do projeto do VMware Horizon®, do VMware Identity Manager™ e do VMware AirWatch® que utiliza o VMware Unified Access Gateway™ para acesso externo seguro aos aplicativos de sua organização. Esses aplicativos podem ser aplicativos do Windows, aplicativos de software como um serviço (SaaS) e áreas de trabalho. Este guia também fornece instruções para implementar os appliances virtuais do Unified Access Gateway e alterar as definições de configuração após a implementação.

## Público-alvo

Estas informações são concebidas para qualquer pessoa que deseja implementar e utilizar os appliances do Unified Access Gateway. As informações foram escritas para administradores de sistema experientes do Linux e do Windows que estejam familiarizados com a tecnologia de máquina virtual e operações de centro de dados.

# Preparando-se para implantar o VMware Unified Access Gateway 1

O Unified Access Gatewayfunciona como um gateway seguro para usuários que desejam acessar áreas de trabalho e aplicativos remotos fora do firewall corporativo.

**Observação** O VMware Unified Access Gateway® anteriormente se chamava VMware Access Point.

Este capítulo inclui os seguintes tópicos:



## Unified Access Gateway como um gateway seguro

O Unified Access Gateway é um appliance de segurança normalmente instalado em uma zona desmilitarizada (DMZ). O Unified Access Gateway é usado para garantir que o único tráfego entrando no centro de dados corporativo seja o tráfego em nome de um usuário remoto fortemente autenticado.

O Unified Access Gateway direciona solicitações de autenticação ao servidor apropriado e descarta qualquer solicitação não autorizada. Os usuários podem acessar somente os recursos que têm autorização para acessar.

O Unified Access Gateway também garante que o tráfego de um usuário autenticado possa ser direcionado somente para os recursos da área de trabalho e de aplicativos para os quais o usuário estiver realmente qualificado. Esse nível de proteção envolve a inspeção específica de protocolos de área de trabalho e a coordenação de potenciais endereços de rede e políticas de mudança rápida para controlar o acesso de maneira precisa.

O Unified Access Gateway atua como um host de proxy para conexões dentro da rede segura da empresa. Esse design fornece uma camada extra de segurança ao proteger áreas de trabalho virtuais, hosts de aplicativos e servidores da Internet voltada para o público.

O Unified Access Gateway é projetado especificamente para a DMZ. As seguintes configurações de proteção são implementadas.

- Linux Kernel e patches de software atualizados

- Suporte múltiplo de NIC para tráfego de Internet e intranet
- SSH desabilitado
- Serviços desabilitados de FTP, Telnet, Rlogin ou Rsh
- Serviços indesejados desabilitados

# Usando o Unified Access Gateway ao invés de uma rede virtual privada

O Unified Access Gateway e as soluções de VPN genéricas são semelhantes, pois ambos garantem que o tráfego seja encaminhado para uma rede internal somente em nome de usuários fortemente autenticados.

As vantagens do Unified Access Gateway sobre a VPN genérica incluem o seguinte.

- Access Control Manager. O Unified Access Gateway aplica regras de acesso automaticamente. O Unified Access Gateway reconhece as qualificações dos usuários e o endereçamento exigido para a conexão interna. Uma VPN faz a mesma coisa, porque a maioria das VPNs permite que um administrador configure as regras de conexão de rede para cada usuário ou grupo de usuários individualmente. Primeiro, isso funciona bem com uma VPN, mas exige um esforço administrativo significativo para manter as regras exigidas.
- Interface do Usuário. O Unified Access Gateway não altera a interface do usuário simples do Horizon Client. Com o Unified Access Gateway, quando o Horizon Client é iniciado, os usuários autenticados estão no ambiente do View deles e têm acesso controlado aos respectivos aplicativos e áreas de trabalho. Uma VPN exige que você configure o software VPN primeiro e o autentique separadamente antes de iniciar o Horizon Client.
- Desempenho. O Unified Access Gateway é projetado para maximizar a segurança e o desempenho. Com o Unified Access Gateway, os protocolos PCoIP, HTML access e WebSocket ficam seguros sem exigir encapsulamento adicional. VPNs são implementadas como VPNs SSL. Essa implantação atende aos requisitos de segurança e, com a Segurança de Camada de Transporte (Transport Layer Security, TLS) habilitada, é considerada segura, mas o protocolo subjacente com SSL/TLS é baseado em TCP. Com protocolos modernos de vídeo remoto que exploram transportes baseados em UDP sem conexão, os benefícios de desempenho podem se deteriorar significativamente quando forçados sobre um transporte com base em TCP. Isso não se aplica a todas as tecnologias de VPN, tendo em vista que aqueles que também podem funcionar com DTLS ou IPsec em vez de SSL/TLS podem funcionar bem com protocolos de área de trabalho do View.

# Requisitos de sistema e de rede do Unified Access Gateway

Para implementar o appliance do Unified Access Gateway, certifique-se de que seu sistema atenda aos requisitos de hardware e software.

## Versões de produtos VMware compatíveis

Você deve utilizar versões específicas dos produtos VMware com versões específicas do Unified Access Gateway. Consulte as notas da versão do produto para obter as informações mais recentes sobre compatibilidade e consulte a Matriz de Interoperabilidade de Produto da VMware em http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

## Requisitos de hardware do servidor ESXi

O appliance do Unified Access Gateway deve ser implantado em uma versão do vSphere que seja a mesma versão compatível para produtos e versões da VMware que esteja utilizando.

Se você planeja utilizar o vSphere Web Client, certifique-se de que o plug-in de integração do cliente esteja instalado. Para obter mais informações, consulte a documentação do vSphere. Se você não instalar esse plug-in antes de iniciar o assistente de implementação, o assistente solicitará a instalação do plug-in. Isso exige o fechamento do navegador e a saída do assistente.

**Observação** Configure o relógio (UTC) no appliance do Unified Access Gateway para que ele esteja com a hora correta. Por exemplo, abra uma janela de console na máquina virtual do Unified Access Gateway e utilize os botões de seta para selecionar o fuso horário correto. Verifique também se o horário do host do ESXi está sincronizado com o servidor NTP e verifique se as VMware Tools, que são executadas na máquina virtual do appliance, sincronizam o horário na máquina virtual com o horário no host do ESXi.

## Requisitos do appliance virtual

O pacote OVF para o appliance do Unified Access Gateway seleciona automaticamente a configuração da máquina virtual que o Unified Access Gateway exige. Embora você possa alterar estas configurações , a VMware recomenda que não altere o CPU, memória ou espaço em disco para valores inferiores às configurações padrão do OVF.

- O requisito mínimo da CPU é de 2000 MHz
- Memória mínima de 4GB

Certifique-se de que o repositório de dados usado para o appliance tenha espaço livre em disco suficiente e atenda aos outros requisitos do sistema.

- O tamanho de download do appliance virtual é de 1.4 GB
- O requisito mínimo de disco com provisionamento dinâmico é de 2.6 GB
- O requisito mínimo de disco com provisionamento estático é de 20 GB

As seguintes informações são necessárias para implantar o appliance virtual.

- Endereço IP estático (recomendado)
- Endereço IP do servidor DNS
- Senha para o usuário raiz
- Senha para o usuário administrador
- URL da instância do servidor ou balanceador de carga para onde o appliance do Unified Access Gateway aponta

## Versões de navegador compatíveis

Os navegadores compatíveis para a inicialização da IU do administrador são o Chrome, o Firefox e o Internet Explorer. Use a versão mais atual do navegador.

## Requisitos de hardware ao usar o Servidor Hyper-V Windows

Ao usar o Unified Access Gateway para uma implantação do AirWatch Tunnel por aplicativo, é possível instalar o appliance do Unified Access Gateway em um servidor Hyper-V Microsoft.

Os servidores Microsoft compatíveis são o Windows Server 2012 R2 e o Windows Server 2016.

### Requisitos de configuração de rede

É possível utilizar uma, duas ou três interfaces de rede e o Unified Access Gateway necessita de um endereço IP estático separado para cada uma. Muitas implementações do DMZ utilizam redes separadas para proteger tipos de tráfego diferentes. Configure o Unified Access Gateway de acordo com o design da rede do DMZ no qual está implementado.

- Uma interface de rede é apropriada para POCs (prova de conceitos) ou testes. Com um NIC, os tráfegos externo, interno e de gerenciamento ficam todos na mesma sub-rede.
- Com duas interfaces de rede, o tráfego externo está em uma sub-rede e o tráfego interno e de gerenciamento estão em outra.
- Utilizar três interfaces de rede é a opção mais segura. Com um terceiro NIC, os tráfegos externo, interno e de gerenciamento têm suas próprias sub-redes.

---

**Importante** Verifique se atribuiu um pool de IPs para cada rede. O appliance do Unified Access Gateway pode então captar a máscara de sub-rede e as configurações do gateway. Para adicionar um pool de IPs, no vCenter Server, se estiver utilizando o vSphere Client nativo, vá até a guia **Pools de IPs** do centro de dados. Alternativamente, se estiver utilizando o vSphere Web Client, você poderá criar um perfil de protocolo de rede. Vá até a guia **Gerenciar** do centro de dados e selecione a guia **Perfis de Protocolo de Rede**. Para obter mais informações, consulte Configurando Perfis de Protocolo para Redes de Máquinas Virtuais.

Se o Unified Access Gateway for implantado sem os pools de IP (vCenter Server), a implantação será bem sucedida, mas ao tentar acessar o Unified Access Gateway usando a IU do administrador no navegador, o serviço da IU do administrador não iniciará.

---

### Requisitos de retenção de registro

Os arquivos de registro são configurados por padrão para utilizar certa quantidade de espaço, que é menor do que o tamanho total do disco no agregado. Os logs para o Unified Access Gateway são alternados por padrão. Você deve utilizar syslog para preservar estas entradas de registro. Consulte "Coletando logs do appliance do Unified Access Gateway", na página 73.

## Regras de firewall para appliances do Unified Access Gateway baseados em DMZ

Appliances do Unified Access Gatewaybaseados em DMZ exigem certas regras de firewall nos firewalls front-end e back-end. Durante a instalação, os serviços do Unified Access Gatewaysão configurados para ouvir em certas portas de rede por padrão.

A implementação de um appliance do Unified Access Gatewaybaseado em DMZ normalmente inclui dois firewalls.

- É necessário um firewall front-end externo voltado para a rede para proteger o DMZ e a rede interna. Configure este firewall para permitir que o tráfego de rede externo chegue até o DMZ.
- É necessário um firewall back-end, entre o DMZ e a rede interna, para fornecer uma segunda camada de segurança. Configure este firewall para aceitar tráfego que se origina somente dos serviços dentro do DMZ.

A política de firewall controla estritamente comunicações de entrada de serviço DMZ, o que reduz amplamente o risco de comprometimento da rede interna.

Para permitir que dispositivos cliente externos se conectem a um appliance do Unified Access Gateway dentro da DMZ, o firewall front-end deve permitir tráfego em determinadas portas. Por padrão, os dispositivos cliente externos e clientes Web externos (HTML Access) conectam-se a um appliance do Unified Access Gateway dentro da DMZ na porta TCP 443. Se for usado o protocolo Blast, a porta 8443 deve estar aberta no firewall, mas é possível configurar também o Blast para a porta 443.

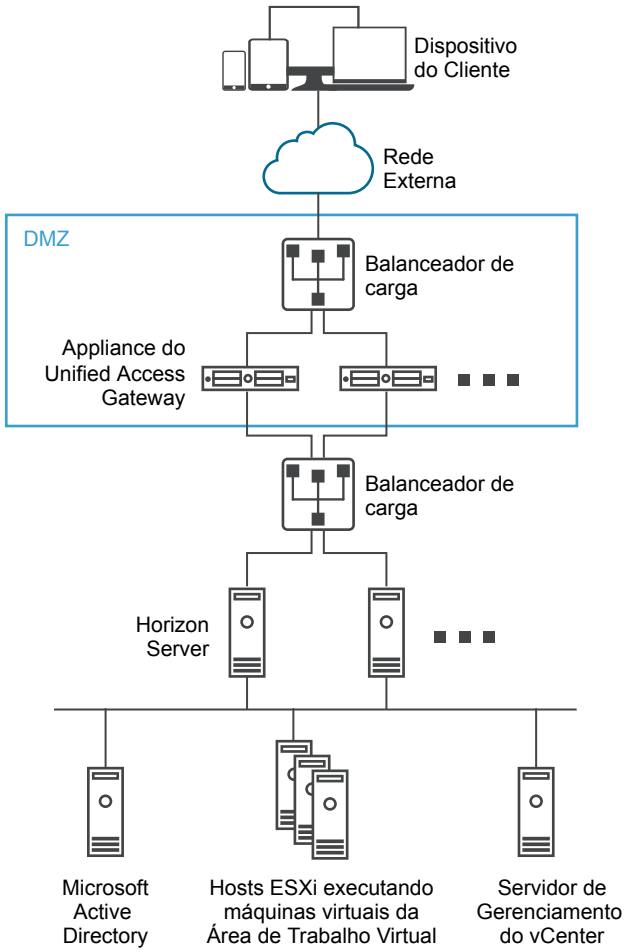
**Tabela 1-1.** Requisitos de porta

| Porta | Portal | Fonte | Destino | Descrição |
|---|---|---|---|---|
| 443 | TCP | Internet | Unified Access Gateway | Para o tráfego da Web, XML Horizon Client - API, túnel do Horizon e Blast Extreme |
| 443 | UDP | Internet | Unified Access Gateway | UDP (opcional) |
| 8443 | UDP | Internet | Unified Access Gateway | Blast Extreme (opcional) |
| 8443 | TCP | Internet | Unified Access Gateway | Blast Extreme |
| 4172 | TCP e UDP | Internet | Unified Access Gateway | PCoIP (opcional) |
| 443 | TCP | Unified Access Gateway | Agente Horizon | Horizon Client XML-API |
| 22443 | TCP e UDP | Unified Access Gateway | Áreas de trabalho e hosts RDS | Blast Extreme |
| 4172 | TCP e UDP | Unified Access Gateway | Áreas de trabalho e hosts RDS | PCoIP (opcional) |
| 32111 | TCP | Unified Access Gateway | Áreas de trabalho e hosts RDS | Canal de estrutura para redirecionamento USB |
| 9427 | TCP | Unified Access Gateway | Áreas de trabalho e hosts RDS | MMR e CDR |
| 9443 | TCP | IU do administrador | Unified Access Gateway | Interface de gerenciamento |

**Observação** Para que sejam permitidas, todas as portas UDP exigem diagramas de dados de encaminhamento e diagramas de dados de resposta.

A figura a seguir mostra um exemplo de uma configuração que inclui firewalls front-end e back-end.

**Figura 1-1.** Na topologia de DMZ Unified Access Gateway



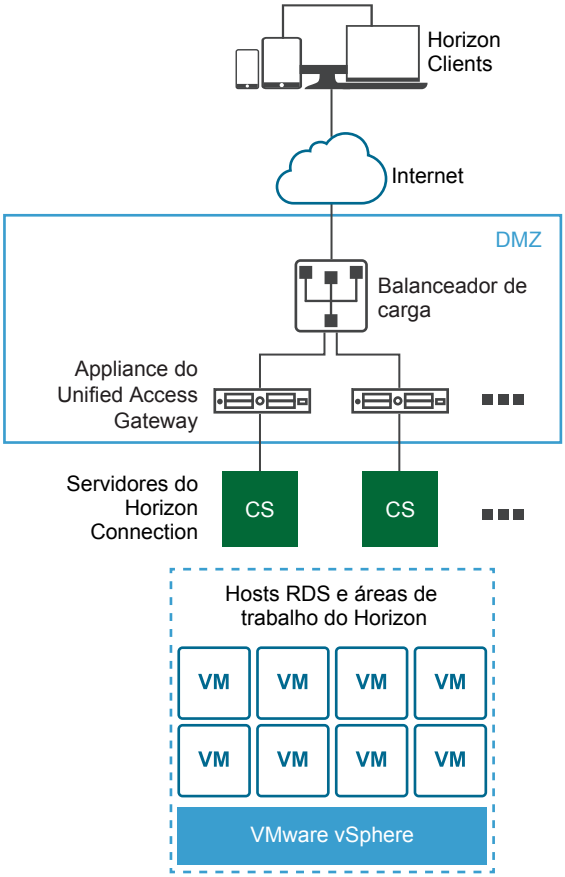

# Topologias do balanceamento de carga do Unified Access Gateway

Um appliance do Unified Access Gateway na DMZ pode ser configurado para apontar para um servidor ou para um balanceador de carga que vá de encontro a um grupo de servidores. Os appliances do Unified Access Gateway funcionam com soluções de balanceamento de carga padrão de terceiros que são configuradas para HTTPS.

Se o appliance do Unified Access Gateway apontar para um balanceador de carga na frente de servidores, a seleção da instância do servidor será dinâmica. Por exemplo, o balanceador de carga poderá fazer uma seleção com base na disponibilidade e no conhecimento dele sobre o número de sessões atuais em cada instância do servidor. As instâncias do servidor dentro do firewall corporativo normalmente têm um balanceador de carga para suportar o acesso interno. Com o Unified Access Gateway, você pode apontar o appliance do Unified Access Gateway para este mesmo balanceador de carga que está já sendo utilizado com frequência.

Você pode, alternativamente, ter um ou mais appliances doUnified Access Gateway apontando para uma instância individual do servidor. Em ambas as abordagens, utilize um balanceador de carga na frente de dois ou mais appliances do Unified Access Gateway no DMZ.

**Figura 1-2.** Vários appliances do Unified Access Gateway atrás de um balanceador de carga




## Protocolos Horizon

Quando um usuário do Horizon Client se conecta a um ambiente Horizon, são utilizados vários protocolos diferentes. A primeira conexão é sempre o protocolo XML-API primário sobre o HTTPS. Após a autenticação bem-sucedida, são criados um ou mais protocolos secundários.

- Protocolo Horizon primário

  O usuário insere um nome do host no Horizon Client e isso inicia o protocolo Horizon primário. Esse é um protocolo de controle para a autorização de autenticação e o gerenciamento de sessão. O protocolo usa mensagens XML estruturadas sobre HTTPS. Esse protocolo também é conhecido como protocolo de controle Horizon XML-API. Em um ambiente com carga balanceada como exibido na figura, os vários appliances do Unified Access Gateway atrás de um balanceador de carga, o balanceador de carga direciona essa conexão a um dos appliances do Unified Access Gateway. No geral, o balanceador de carga seleciona o appliance com base primeiramente na disponibilidade e, em seguida, escolhe a partir dos tráfegos de rotas de appliances disponíveis com base no menor número de sessões atuais. Essa configuração distribui uniformemente o tráfego de diferentes clientes no conjunto disponível de appliances do Unified Access Gateway

- Protocolos Horizon secundários

Após o Horizon Client estabelecer a comunicação segura com um dos appliances do Unified Access Gateway, o usuário faz a autenticação. Se essa tentativa de autenticação for bem-sucedida, uma ou mais conexões secundárias são feitas do Horizon Client. Essas conexões secundárias podem incluir o seguinte

- Túnel HTTPS usado para encapsulamento dos protocolos TCP, como o RDP, o MMR/CDR e o canal de estrutura do cliente. (TCP 443)
- Protocolo de exibição Blast Extreme (TCP 443, TCP 8443, UDP 443 e UDP 8443)
- Protocolo de exibição PCoIP (TCP 443, UDP 443)

Esses protocolos Horizon secundários devem ser encaminhados ao mesmo appliance do Unified Access Gateway ao qual o protocolo Horizon primário foi encaminhado. O Unified Access Gateway pode então autorizar os protocolos secundários com base na sessão de usuário autenticada. Uma capacidade importante de segurança do Unified Access Gateway é que o Unified Access Gateway somente encaminha o tráfego ao centro de dados corporativo se o tráfego estiver em nome de um usuário autenticado. Se o protocolo secundário for encaminhado erroneamente a um appliance do Unified Access Gateway diferente do appliance do protocolo primário, ele não será autorizado e será colocado na DMZ. A conexão falha. O encaminhamento incorreto de protocolos secundários será um problema comum se o balanceador de carga não estiver configurado corretamente.

# Design da DMZ para o Unified Access Gateway com várias placas de interface de rede

Uma das definições de configuração para o Unified Access Gateway é o número de placas de interface de rede (Network Interface Cards, NICs) virtuais a serem utilizadas. Ao implantar o Unified Access Gateway, você seleciona uma configuração de implantação para sua rede.

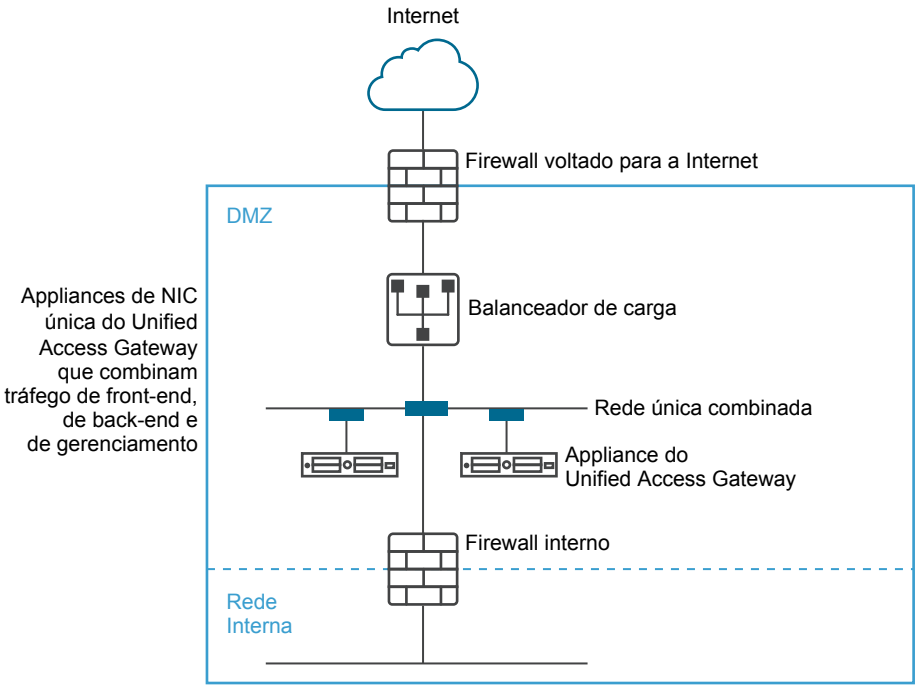
É possível especificar uma, duas ou três configurações de NICS que são especificadas como onenic, twonic ou threenic.

Reduzir o número de portas abertas em cada LAN virtual e separar os tipos diferentes de tráfego de rede pode melhorar a segurança de forma significativa. Os benefícios são principalmente em termos de separação e isolamento dos tipos diferentes de tráfego de rede como parte de uma estratégia de design de segurança da DMZ de defesa em profundidade. Isso pode ser conquistado ao implementar comutadores físicos separados dentro da DMZ, com várias LANs virtuais dentro da DMZ ou como parte de uma DMZ totalmente gerenciada pelo VMware NSX.

## Implementação típica da DMZ com NIC única

A implantação mais simples de um Unified Access Gateway é com uma única NIC, onde todo o tráfego de rede é combinado em uma única rede. O tráfego do firewall voltado para a Internet é direcionado a um dos appliances disponíveis do Unified Access Gateway. O Unified Access Gateway então encaminha o tráfego autorizado através do firewall interno aos recursos na rede interna. O Unified Access Gateway descarta o tráfego não autorizado.

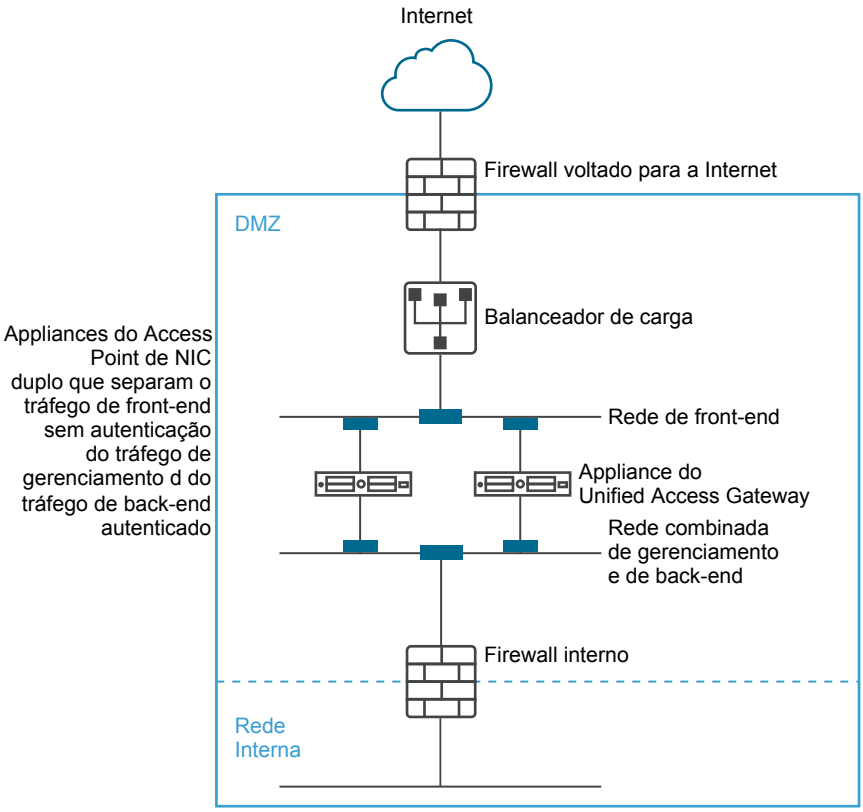
**Figura 1-3.** Opção NIC única do Unified Access Gateway




## Separando o tráfego de usuário não autenticado do tráfego de back-end e de gerenciamento

Uma melhoria sobre a implementação de NIC única é especificar duas NICs. A primeira ainda é usada para Internet voltada para o acesso não autenticado, mas o tráfego autenticado de back-end e o tráfego de gerenciamento são separados em uma rede diferente.

**Figura 1-4.** Opção com duas NICs do Unified Access Gateway




Em uma implantação com duas NICs, o Unified Access Gateway deve autorizar o tráfego que para a rede interna pelo firewall interno. O tráfego não autorizado não está nessa rede de back-end. O tráfego de gerenciamento como a API REST para o Unified Access Gateway está somente nesta segunda rede

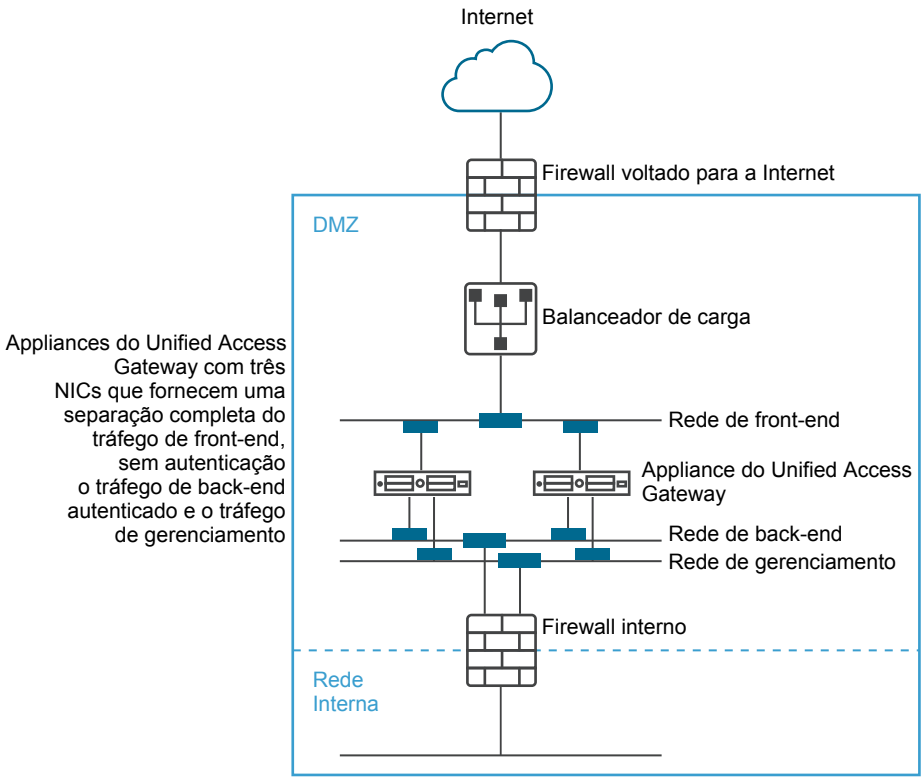
Se um dispositivo na rede de front-end sem autenticação foi comprometido, como o balanceador de carga, então a reconfiguração do dispositivo para ignorar o Unified Access Gateway não é possível nesta implantação com duas NICs. Ela combina as regras de firewall da camada 4 com a segurança do Unified Access Gateway da camada 7. De maneira semelhante, se o firewall voltado para a Internet foi configurado de maneira errada para permitir a passagem pela porta 9443 TCP, isso ainda não deixaria a API REST de gerenciamento do Unified Access Gateway exposta a usuários da Internet. Um princípio de defesa em profundidade utiliza vários níveis de proteção, como saber que um único erro de configuração ou ataque de sistema não cria necessariamente uma vulnerabilidade geral

Em uma implantação com duas NICs, é possível colocar sistemas de infraestrutura adicionais, como servidores DNS, servidores de Gerenciador de Autenticação do RSA SecurID na rede de back-end dentro da DMZ para que estes servidores não estejam visíveis na rede voltada para a Internet. Colocar sistemas de infraestrutura dentro da DMZ protege contra ataques de camada 2 da LAN voltada para a Internet a partir de um sistema de front-end comprometido e reduz efetivamente a superfície geral de ataque.

A maior parte do tráfego de rede do Unified Access Gateway consiste nos protocolos de exibição para Blast e PCoIP. Com uma NIC única, o tráfego de protocolo de exibição de e para a Internet é combinado com tráfego de e para os sistemas de back-end. Quando duas ou mais NICs são utilizadas, o tráfego é espalhado em NICs de front-end e back-end e em redes. Isso reduz o potencial de gargalo de uma NIC única e resulta em benefícios de desempenho.

O Unified Access Gateway suporta uma separação adicional ao permitir também a separação do tráfego de gerenciamento em uma LAN de gerenciamento específico. O tráfego de gerenciamento HTTPS para a porta 9443 só é possível a partir da LAN de gerenciamento.

**Figura 1-5.** Opção com três NICs do Unified Access Gateway




# Atualização com zero tempo de inatividade

As atualizações com zero tempo de inatividade permitem atualizar o Unified Access Gateway sem que haja tempo de inatividade para os usuários. Antes de atualizar um appliance do Unified Access Gateway, o modo quiesce nas páginas de configuração do sistema do Unified Access Gateway é alterado de NÃO para SIM.

Quando o valor do modo quiesce for SIM, o appliance do Unified Access Gateway será mostrado como indisponível quando o balanceador de carga verificar a integridade do appliance. As solicitações que chegam ao balanceador de carga são enviadas ao próximo appliance do Unified Access Gateway que está atrás do balanceador de carga.

### Pré-requisitos

- Dois ou mais appliances do Unified Access Gateway configurados atrás do balanceador de carga
- A definição da URL de verificação de integridade configurada com uma URL com a qual o balanceador de carga se conecta para verificar a integridade do appliance do Unified Access Gateway
- Verifique a integridade do appliance no balanceador de carga. Digite o comando API REST do `GET https://mycoUnifiedAccessGateway.com:443/favicon.ico`.

  A resposta é `HTTP/1.1 200 OK`, se o modo quiesce estiver definido como Não ou `HTTP/1.1 503`, se o modo quiesce estiver definido como Sim.

### Procedimentos

1 Na seção Configurar manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações avançadas, clique no ícone de engrenagem **Configuração do Sistema**.

3 Na linha do **Modo quiesce**, habilite **SIM** para pausar o appliance do Unified Access Gateway.

   Quando o appliance for parado, as sessões existentes que o appliance atendia são mantidas durante 10 horas. As sessões serão fechadas após esse período.

4 Clique em **Salvar**.

As novas solicitações que chegam ao balanceador de carga são enviadas ao próximo appliance do Unified Access Gateway.

### Próximo passo

Exporte as configurações do appliance do Unified Access Gateway pausado. Implante uma nova versão do Unified Access Gateway e importe as configurações. A nova versão do appliance do Unified Access Gateway pode ser adicionada ao balanceador de carga.

# Implementação do appliance do Unified Access Gateway 2

O Unified Access Gateway é colocado em um pacote como um OVF e é implantado em um host vSphere ESX ou ESXi como um appliance virtual pré-configurado.

Podem ser usados dois métodos primários para instalar o appliance do Unified Access Gateway em um vSphere ESX ou um host de ESXi. As funções do Microsoft Server 2012 e do Hyper-V 2016 são compatíveis.

- O vSphere Client ou o vSphere Web Client podem ser utilizados para implementar o modelo do OVF do Unified Access Gateway. Você recebe um aviso para configurações básicas, incluindo a configuração de implementação da NIC, endereço IP e senhas da interface de gerenciamento. Após o OVF ser implementado, faça o login na interface de usuário administrador do Unified Access Gateway para ajustar as configurações de sistema do Unified Access Gateway, definir os serviços de borda seguros em vários casos de uso e configurar a autenticação na DMZ. Consulte "Implementar o Unified Access Gateway usando o assistente modelo do OVF", na página 20.
- Os scripts PowerShell podem ser usados para implementar o Unified Access Gateway e definir serviços de borda seguros em vários casos de uso. Você pode baixar o arquivo compactado, configurar o script do PowerShell para o seu ambiente e executar o script para implantar o Unified Access Gateway. Consulte "Usando o PowerShell para implementar o appliance do Unified Access Gateway", na página 28.

**Observação** Para os casos de uso do Tunnel e proxy por aplicativo do AirWatch, você pode implementar o Unified Access Gateway em ambientes ESXi ou Microsoft Hyper-V.

Este capítulo inclui os seguintes tópicos:



## Usando o assistente modelo do OVF para implantar o Unified Access Gateway

Para implementar o Unified Access Gateway, implante o modelo do OVF usando o vSphere Client ou o vSphere Web Client, ative o appliance e defina as configurações.

Ao implantar o OVF, você configura o número necessário de interfaces de rede (NIC), o endereço IP e as senhas do administrador e de raiz.

Após a implantação do Unified Access Gateway, vá para a interface de usuário de administração (IU) para configurar o ambiente do Unified Access Gateway. Na IU do administrador, configure os recursos da área de trabalho e do aplicativo e os métodos de autenticação a serem usados na DMZ. Para fazer logon nas páginas IU do administrador, vá para `https://<mycoUnifiedGatewayAppliance>.com:9443/admin/index.html`.

## Implementar o Unified Access Gateway usando o assistente modelo do OVF

Você pode implementar o appliance do Unified Access Gatewayefetuando logon no vCenter Server e utilizando o assistente Implementar Modelo OVF.

Há duas versões do OVA do Unified Access Gateway disponíveis, OVA padrão e versão FIPS do OVA. A versão FIPS 140-2 é executada com o conjunto de cifras e hashes do certificado FIPS e tem serviços restritivos habilitados que são compatíveis com bibliotecas FIPS certificadas. Quando o Unified Access Gateway é implantado no modo FIPS, o appliance não pode ser alterado para o modo de implantação OVA padrão.

**Observação** Se você utilizar o vSphere Client nativo, certifique-se de que atribuiu um pool de IPs para cada rede. Para adicionar um pool de IPs no vCenter Server utilizando o vSphere Client original, vá até a guia Pools de IPs do centro de dados. Alternativamente, se estiver utilizando o vSphere Web Client, você poderá criar um perfil de protocolo de rede. Vá até a guia Gerenciar do centro de dados e selecione a guia Perfis de Protocolo de Rede.

### Pré-requisitos

- Revise as opções de implantação disponíveis no assistente. Consulte "Requisitos de sistema e de rede do Unified Access Gateway", na página 8.
- Determine quantas interfaces de rede e endereços IP estáticos devem ser configurados para o appliance do Unified Access Gateway. Consulte "Requisitos de configuração de rede", na página 10.
- Faça o download do arquivo do instalador `.ova` para o appliance do Unified Access Gatewayno site da VMware em https://my.vmware.com/web/vmware/downloads ou determine a URL a ser utilizado (exemplo: `http://exemplo.com/vapps/euc-access-point-`*`Y.Y`*`.0.0-`*`xxxxxxx`*`_OVF10.ova`), onde *Y.Y* é o número da versão e *xxxxxxx* é o número de compilação.

### Procedimentos

1 Utilize o vSphere Client nativo ou o vSphere Web Client para efetuar logon em uma instância do vCenter Server.

Para uma rede IPv4, utilize o Cliente vSphere nativo ou o Cliente Web vSphere. Para uma rede IPv6, utilize o cliente Web vSphere.

2 Selecione um comando de menu para iniciar o assistente **Implantar modelo OVF**.

| Opção | Comando de Menu |
|---|---|
| **vSphere Client** | Selecione **Arquivo > Implementar Modelo OVF**. |
| **vSphere Web Client** | Selecione um objeto de inventário que seja um objeto parente válido de uma máquina virtual, como um centro de dados, pasta, cluster, pool de recursos ou host e, no menu **Ações**, selecione **Implementar Modelo OVF**. |

3 Na página Selecionar origem, navegue até a localização do arquivo `.ova` que baixou ou insira uma URL e clique em **Avançar**.

Revise os detalhes do produto, a versão e os requisitos de tamanho.

4 Siga as indicações do assistente e leve em consideração as seguintes orientações à medida que conclui o assistente.

| Opção | Descrição |
| --- | --- |
| **Nome e localização** | Insira um nome para o appliance virtual do Unified Access Gateway. O nome deve ser exclusivo na pasta do inventário. Os nomes diferenciam maiúsculas de minúsculas.<br>Selecionar uma localização para o appliance virtual. |
| **Configuração da implantação** | Para uma rede IPv4, você pode utilizar uma, duas ou três interfaces de rede (NICs). Para uma rede IPv6, utilize três NICs. O Unified Access Gateway exige um endereço IP estático separado para cada NIC. Muitas implementações do DMZ utilizam redes separadas para proteger tipos de tráfego diferentes. Configure o Unified Access Gateway de acordo com o design da rede do DMZ no qual está implementado. |
| **Host/Cluster** | Selecione o host ou o cluster no qual executar o appliance virtual. |
| **Formato do disco** | Para ambientes de avaliação e teste, selecione o formato de Provisionamento Dinâmico. Para ambientes de produção, selecione um dos formatos de Provisionamento Estático. O Thick Provision Eager Zeroed é um tipo de formato de disco virtual estático que suporta recursos de cluster como tolerância a falhas, mas demora muito mais para ser criado do que outros tipos de discos virtuais. |

| Opção | Descrição |
|---|---|
| **Configurar Redes/Mapeamento de Rede** | Se estiver utilizando o vSphere Web Client, a página Configurar Redes permitirá o mapeamento de cada NIC a uma rede e especifica configurações de protocolo.<br>Mapeie as redes usadas no modelo OVF para as redes no seu inventário.<br>a Selecione IPv4 ou IPv6 na lista suspensa de **protocolo IP**.<br>b Selecione a primeira linha na tabela **Internet** e, em seguida, clique na seta para baixo para selecionar a rede de destino. Se você selecionar IPv6 como o protocolo IP, será preciso selecionar a rede que possui recursos IPv6.<br>Após selecionar a linha, você pode também inserir os endereços IP para o servidor DNS, o gateway e a máscara de rede na porção inferior da janela.<br>c Se estiver utilizando mais de um NIC, selecione a fileira seguinte **Rede de Gerenciamento**, selecione a rede de destino e, em seguida, poderá inserir os endereços IP para o servidor DNS, gateway e máscara de rede para aquela rede.<br>Se estiver utilizando somente um NIC, todas as linhas serão mapeadas para a mesma rede.<br>d Se possuir um terceiro NIC, selecione também a terceira linha e conclua as configurações.<br>Se estiver utilizando somente dois NICs, para esta terceira linha **Rede Back-end**, selecione a mesma rede que utilizou para **Rede de Gerenciamento**.<br>Com o vSphere Web Client, um perfil de protocolo de rede será criado automaticamente após a conclusão do assistente, se ainda não existir.<br>Se você utiliza o vSphere Client nativo, a página Mapeamento de rede permite mapear cada NIC a uma rede, mas não há campos para especificar os endereços do servidor DNS, do gateway e da máscara de rede. Como descrito nos pré-requisitos, você precisa ter atribuído um pool de IPs para cada rede ou ter criado um perfil de protocolo de rede. |
| **Personalizar propriedades de rede** | As caixas de texto na página Propriedades são específicas ao Unified Access Gateway e podem não ser necessárias para outros tipos de appliance virtuais. O texto na página do assistente explica cada configuração. Se o texto estiver truncado no lado direito do assistente, redimensione a janela arrastando-a partir do canto inferior direito.<br>■ **IPMode:STATICV4/STATICV6**. Se digitar STATICV4, será necessário inserir o endereço IPv4 para o NIC. Se digitar STATICV6, será necessário inserir o endereço IPv6 para o NIC.<br>■ **Lista separada por vírgula das regras de encaminhamento com o formato {tcp\|udp}/listening-port-number/destination-ip-address:destination-port-nu**<br>■ **Endereço IPv4 para o NIC 1 (ETH0)**. Insira o endereço IPv4 para o NIC se digitou STATICV4 para o modo NIC.<br>■ **Lista separada por vírgula das rotas personalizadas IPv4 para NIC 1 (eth0) com o formato ipv4-network-address/bits.ipv4-gateway-address**<br>■ **Endereço IPv6 para o NIC 1 (eth0)**. Insira o endereço IPv6 para o NIC se digitou STATICV6 para o modo NIC.<br>■ **Endereços de servidor DNS**. Insira os endereços IPv4 ou IPv6 separados por espaço dos servidores do nome de domínio para o appliance do Unified Access Gateway . O exemplo de entrada do IPv4 é 192.0.2.1 192.0.2.2. O exemplo de entrada do IPv6 é fc00:10:112:54::1<br>■ **Gateway padrão**Insira um valor padrão definido pelos perfis de protocolo de rede do vSphere (Observação: Insira um valor de gateway padrão somente se o modo IP for STATICV4/STATICV6).<br>■ **Endereço IPv4 para o NIC 2 (eth1)**. Insira o endereço IPv4 para o NIC se digitou STATICV4 para o modo NIC. |

| Opção | Descrição |
|---|---|
| | ■ **Lista separada por vírgula das rotas personalizadas IPv4 para NIC 2 (eth1) com o formato ipv4-network-address/bits.ipv4-gateway-address**<br>■ **Endereço IPv6 para o NIC 2 (eth1)**. Insira o endereço IPv6 para o NIC se digitou STATICV6 para o modo NIC.<br>■ **Endereço IPv4 para o NIC 3 (eth2)**. Insira o endereço IPv4 para o NIC se digitou STATICV4 para o modo NIC.<br>■ **Lista separada por vírgula das rotas personalizadas IPv4 para NIC 3 (eth2) com o formato ipv4-network-address/bits.ipv4-gateway-address**<br>■ **Endereço IPv6 para o NIC 3 (eth2)**. Insira o endereço IPv6 para o NIC se digitou STATICV6 para o modo NIC.<br>■ **Opções de senha**. Insira a senha para o usuário raiz desta VM e a senha para o usuário administrador que acessa o console de administração e habilita o acesso à API REST.<br>■ **Opções de senha**. Insira a senha para o usuário administrador que faz logon na IU do administrador para configurar o Unified Access Gateway e que pode habilitar o acesso à API REST.<br>As outras configurações são opcionais ou já têm uma configuração padrão inserida. |

5 Na página Pronto para Concluir, selecione **Ligar após implementação** e clique em **Concluir**.

Uma tarefa de Implementar Modelo OVF aparece na área de status do vCenter Server para que você possa monitorar a implementação. Você pode também abrir um console na máquina virtual para visualizar as mensagens do console que são exibidas durante a inicialização do sistema. Um registro destas mensagens também está disponível no arquivo `/var/log/boot.msg`.

6 Quando a implementação for concluída, certifique-se de que os usuários finais possam se conectar ao appliance abrindo um navegador e inserindo a seguinte URL:

`https://`*`FQDN-of-UAG-appliance`*

Nessa URL, *FQDN-of-UAG-appliance* é o nome de domínio totalmente qualificado do appliance do Unified Access Gateway que pode ser resolvido por DNS.

Se a implementação for bem-sucedida, você verá a página da Web fornecida pelo servidor para o qual o Unified Access Gateway estiver apontado. Se a implementação não foi bem sucedida, você pode excluir a máquina virtual do appliance e implementá-lo novamente. O erro mais comum é não inserir as impressões digitais do certificado corretamente.

O appliance do Unified Access Gatewayé implementado e iniciado automaticamente.

### Próximo passo

Faça o logon na interface do usuário administrador (IU) do Unified Access Gateway e configure os recursos da área de trabalho e do aplicativo para permitir acesso remoto da Internet por meio do Unified Access Gateway e os métodos de autenticação a serem usados na DMZ. A URL do console de administração está no formato `https://<mycoUnified Access Gatewayappliance.com:9443/admin/index.html`.

**Observação** Se não for possível acessar o logon da UI do administrador na tela, verifique para observar se a máquina virtual tem o endereço IP exibido durante a instalação do OVA. Se o endereço IP não estiver configurado, use o comando vami mencionado na UI para reconfigurar as NICs. Execute o comando como "`cd /opt/vmware/share/vami`" depois o comando "`./vami_config_net`".

# Configurando o Unified Access Gateway a partir das páginas de configuração do administrador

Após implantar o OVF e o appliance do Unified Access Gateway estiver ativado, faça logon na interface do usuário do administrador do Unified Access Gateway para definir as seguintes configurações.

As páginas de configurações gerais e configurações avançadas incluem o seguinte:

- Configuração do sistema e certificado de servidor SSL do Unified Access Gateway
- Configurações do Serviço de Borda do Horizon, Proxy reverso e o VMware Tunnel
- Configurações de autenticação para o RSA SecurID, RADIUS, Certificado X.509 e RSA Adaptive Authentication
- Configurações para provedor de identidade SAML e provedor de serviços
- Configuração da ponte de identidade

As opções a seguir podem ser acessadas a partir das páginas Configurações de suporte.

- Baixe os arquivos de log compactados do Unified Access Gateway
- Exporte as configurações do Unified Access Gateway para recuperar as definições de configuração
- Defina as configurações do nível de log
- Importe as configurações do Unified Access Gateway para criar e atualizar uma configuração inteira do Unified Access Gateway

## Configurar as definições de sistema do Unified Access Gateway

É possível configurar os protocolos de segurança e os algoritmos criptográficos usados para criptografar as comunicações entre os clientes e o appliance do Unified Access Gateway a partir das páginas de configuração do administrador.

### Pré-requisitos

- Revisar as propriedades de implementação do Unified Access Gateway. São necessárias as seguintes informações de configurações.
  - Endereço IP estático para o appliance do Unified Access Gateway
  - Endereço IP do servidor DNS
  - Senha para o console de administração
  - URL da instância do servidor ou balanceador de carga para o qual o appliance do Unified Access Gateway aponta
  - URL do servidor Syslog para salvar os arquivos de log de evento

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Avançadas, clique no ícone de engrenagem **Configuração do Sistema**.

3 Edite os seguintes valores de configuração do appliance do Unified Access Gateway.

| Opção | Valor padrão e descrição |
|---|---|
| **Localidade** | Especifica o local a ser utilizado ao gerar mensagens de erro.<br>■ **`en_US`** para inglês<br>■ **`ja_JP`** para japonês<br>■ **`fr_FR`** para francês<br>■ **`de_DE`** para alemão<br>■ **`zh_CN`** para chinês simplificado<br>■ **`zh_TW`** para chinês tradicional<br>■ **`ko_KR`** para coreano |
| **Senha do administrador** | Esta senha foi definida quando você implementou o appliance. É possível redefini-la.<br>As senhas devem ter pelo menos 8 caracteres de comprimento, conter pelo menos uma letra maiúscula e uma letra minúscula, um dígito e um caractere especial, que inclui ! @ # $ % * ( ). |
| **Conjuntos de criptografia** | Na maioria dos casos, as configurações padrão não precisam ser alteradas. Esses são os algoritmos criptográficos usados para criptografar as comunicações entre os clientes e o appliance do Unified Access Gateway. As configurações de criptografia são usadas para ativar vários protocolos de segurança. |
| **Obedecer ordem de criptografia** | O padrão é NÃO. Selecione **SIM** para ativar o controle de ordem da lista de criptografia TLS. |
| **SSL 3.0 ativado** | O padrão é NÃO. Selecione **SIM** para ativar o protocolo de segurança SSL 3.0. |
| **TLS 1.0 ativado** | O padrão é NÃO. Selecione **SIM** para ativar o protocolo de segurança TLS 1.0. |
| **TLS 1.1 ativado** | O padrão é SIM. O protocolo de segurança TLS 1.1 está ativado. |
| **TLS 1.2 ativado** | O padrão é SIM. O protocolo de segurança TLS 1.2 está ativado. |
| **URL do Syslog** | Insira a URL do servidor Syslog utilizado para registrar eventos do Unified Access Gateway. Este valor pode ser uma URL ou um nome do host ou endereço IP. Se você não definir a URL do servidor syslog, nenhum evento será registrado. Digite como `syslog://server.example.com:514`. |
| **URL de verificação de integridade** | Insira um URL pelo qual o balanceador de carga se conecta e verifica a integridade do Unified Access Gateway |
| **Cookies a serem armazenados em cache** | O conjunto de cookies que o Unified Access Gateway armazena em cache. O padrão é nenhum. |
| **Modo do IP** | Selecione modo do IP estático, STATICV4 OU STATICV6. |
| **Tempo limite da sessão** | O valor padrão é **36000000** milissegundos. |
| **Modo quiesce** | Ative **SIM** para pausar o appliance do Unified Access Gateway a fim de alcançar um estado consistente para realizar tarefas de manutenção |
| **Intervalo do monitor** | O valor padrão é **60**. |

4 Clique em **Salvar**.

### Próximo passo

Defina as configurações do serviço de borda para os componentes com os quais o Unified Access Gateway é implantado. Após definir as configurações de borda, defina as configurações de autenticação.

# Atualizar certificados assinados de servidor SSL

É possível substituir os certificados assinados após a expiração.

Para ambientes de produção, a VMware recomenda enfaticamente a substituição do certificado padrão o mais rápido possível. O certificado padrão do servidor TLS/SSL que é gerado ao implementar um appliance do Unified Access Gatewaynão é assinado por uma Autoridade de Certificação Confiável.

### Pré-requisitos

- Novo certificado assinado e chave privada salvos em um computador que possa ser acessado.
- Converta o certificado em arquivos de formato PEM e converta os arquivos .pem no formato de uma linha. Consulte Converter arquivos de certificado para o formato PEM de uma linha.

### Procedimentos

1 No console de administração, clique em **Selecionar**.

2 Na seção Configurações Avançadas, clique no ícone de engrenagem Configurações do Certificado do Servidor SSL.

3 Selecione um tipo de certificado de **PEM** ou de **PFX**.

4 Se o tipo de certificado for **PEM**:

   a Na linha Chave Privada, clique em **Selecionar** e navegue até o arquivo da chave privada.

   b Clique em **Abrir** para carregar o arquivo.

   c Na linha Cadeia de certificados, clique em **Selecionar** e navegue até o arquivo da cadeia de certificados.

   d Clique em **Abrir** para carregar o arquivo.

5 Se o tipo de certificado for **PFX**:

   a Na linha Atualizar PFX, clique em **Selecionar** e navegue até o arquivo pfx.

   b Clique em **Abrir** para carregar o arquivo.

   c Insira a senha do certificado PFX.

   d Insira o pseudônimo do certificado PFX. Isso é usado quando vários certificados estão presentes no armazenamento de certificados.

6 Clique em **Salvar**.

### Próximo passo

Se a CA que assinou o certificado não tiver reputação renomada, configure clientes para confiar nos certificados raiz e intermediário.

# Usando o PowerShell para implantar o Unified Access Gateway 3

Um script do PowerShell pode ser usado para implantar o Unified Access Gateway. O script do PowerShell é entregue como um script de amostra que pode ser adaptado às necessidades específicas do ambiente.

Quando for usado o script do PowerShell para implantar o Unified Access Gateway, o script chamará o comando da OVF Tool e validará as configurações para construir automaticamente a sintaxe de linha de comando correta. Esse método também permite configurações avançadas, como a configuração do certificado do servidor TLS/SSL a ser aplicado no momento da implementação.

Este capítulo inclui os seguintes tópicos:



## Requisitos do sistema para a implantação do Unified Access Gateway com o PowerShell

Para implantar o Unified Access Gateway usando script do PowerShell, você deve usar versões específicas dos produtos VMware.

- Host do vSphere ESX com um vCenter Server.
- O script do PowerShell é executado em máquinas com Windows 8.1 ou versões posteriores ou no Windows Server 2008 R2 ou versões posteriores.

  A máquina também pode ser um vCenter Server executado no Windows ou em uma máquina separada do Windows.
- A máquina com Windows que executar o script deve ter um comando de VMware OVF Tool instalado.

  Você deve instalar o OVF Tool 4.0.1 ou versão posterior do https://www.vmware.com/support/developer/ovf/.

Você deve selecionar o repositório de dados e a rede do vSphere a serem usados.

Um Perfil do Protocolo de Rede do vSphere deve ser associado a cada nome de rede de referência. Esse Perfil de Protocolo de Rede especifica as configurações de rede, como máscara de sub-rede IPv4, gateway etc. A implantação do Unified Access Gateway usa esses valores, então verifique se os valores estão corretos.

# Usando o PowerShell para implementar o appliance do Unified Access Gateway

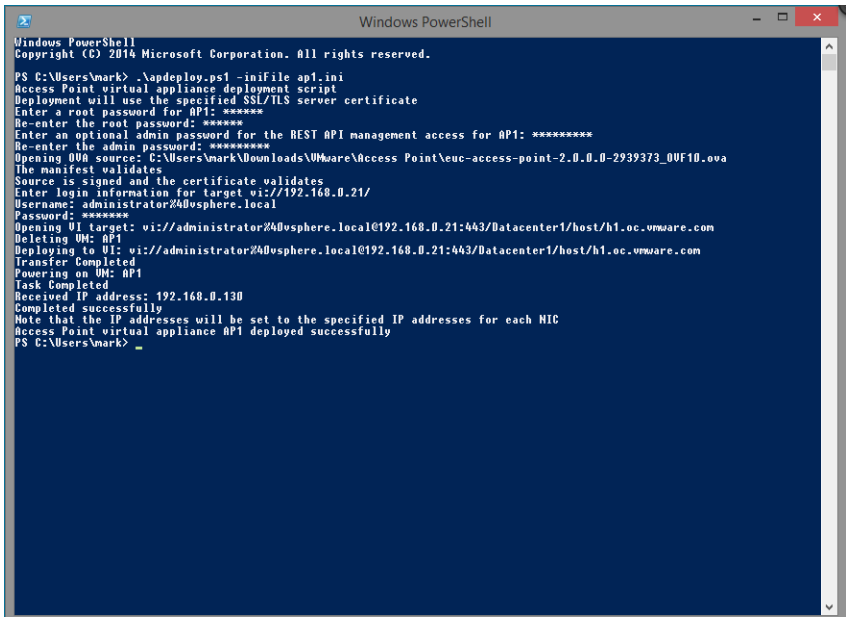
Os scripts do PowerShell preparam seu ambiente com todas as definições de configuração. Ao executar o script do PowerShell para implementar o Unified Access Gateway, a solução está pronta para produção na primeira inicialização do sistema.

### Pré-requisitos

- Verifique se os requisitos do sistema são apropriados e se estão disponíveis para uso.

  Este é um script de amostra para implementar o Unified Access Gateway no seu ambiente.

  **Figura 3-1.** Script de amostra do PowerShell




### Procedimentos

1. Faça o download do OVA do Unified Access Gateway no My VMware para sua máquina Windows.
2. Faça o download dos arquivos ap-deploy-XXX.zip em uma pasta na máquina Windows.

   Os arquivos zip estão disponíveis em https://communities.vmware.com/docs/DOC-30835.
3. Abra um script do PowerShell e modifique o diretório do local do seu script.
4. Crie um arquivo de configuração .INI para o appliance virtual do Unified Access Gateway.

   Por exemplo: implemente um novo appliance AP1 do Unified Access Gateway. O arquivo de configuração é nomeado como ap1.ini. Esse arquivo contém todas as definições de configuração para AP1. É possível usar os arquivos .INI de amostra no arquivo apdeploy .ZIP para criar o arquivo .INI e modificar as configurações adequadamente.

---

**Observação** Você pode ter arquivos .INI exclusivos para várias implementações do Unified Access Gateway no seu ambiente. Você deve alterar os Endereços IP e os parâmetros de nome no arquivo .INI adequadamente para implantar vários appliances.

---

Exemplo do arquivo .INI a ser modificado.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 Para assegurar que a execução do script seja bem-sucedida, digite o comando `set-executionpolicy` do PowerShell.

```
set-executionpolicy -scope currentuser unrestricted
```

Você deve executar esse comando uma vez e somente se ele estiver restrito no momento.

Se houver um aviso para o script, execute o comando para desbloquear o aviso:

```
unblock-file -path .\apdeploy.ps1
```

6 Execute o comando para iniciar a implementação. Se você não especificar o arquivo .INI, o script será padronizado para ap.ini.

```
.\apdeploy.ps1 -iniFile ap1.ini
```

7 Insira as credenciais quando receber o aviso e conclua o script.

---

**Observação** Se você receber um aviso para adicionar a impressão digital da máquina de destino, digite **sim**.

---

O appliance do Unified Access Gateway está implementado e disponível para produção.

Para obter mais informações sobre scripts do PowerShell, consulte https://communities.vmware.com/docs/DOC-30835.

# Casos de uso de implantação para o Unified Access Gateway 4

Os cenários de implantação descritos neste capítulo podem auxiliar a identificar e organizar a implantação do Unified Access Gateway em seu ambiente.

É possível implantar o Unified Access Gateway com o Horizon View, o Horizon Cloud com infraestrutura local, o VMware Identity Manager e o VMware AirWatch.

Este capítulo inclui os seguintes tópicos:



## Implementação com o Horizon View e o Horizon Cloud com infraestrutura local

É possível implantar o Unified Access Gateway com o Horizon View e o Horizon Cloud com infraestrutura local. Para o componente View do VMware Horizon, os appliances do Unified Access Gateway cumprem a mesma função que foi anteriormente desempenhada pelos servidores de segurança do View.

### Cenário de implementação

O Unified Access Gateway fornece acesso remoto seguro a áreas de trabalho e aplicativos virtuais no local em um centro de dados do cliente. Isso funciona com uma implantação local do Horizon View ou do Horizon Cloud para o gerenciamento unificado.

O Unified Access Gateway fornece à empresa uma garantia de preservação da identidade do usuário e controla de forma precisa o acesso às áreas de trabalho e aplicativos autorizados.

Os appliances virtuais do Unified Access Gateway são implementados, geralmente, em uma zona desmilitarizada (DMZ) da rede. A implementação na DMZ assegura que todo o tráfego entrando no centro de dados para os recursos da área de trabalho e do aplicativo é tráfego em nome de um usuário fortemente autenticado. Os appliances virtuais do Unified Access Gateway também garantem que o tráfego de um usuário autenticado possa ser direcionado somente para os recursos da área de trabalho e de aplicativos para os quais o usuário estiver autorizado. Esse nível de proteção envolve a inspeção específica de protocolos de área de trabalho e a coordenação de potenciais endereços de rede e políticas de mudança rápida para controlar o acesso de maneira precisa.

Você deve verificar os requisitos para a implementação contínua do Unified Access Gateway com o Horizon.

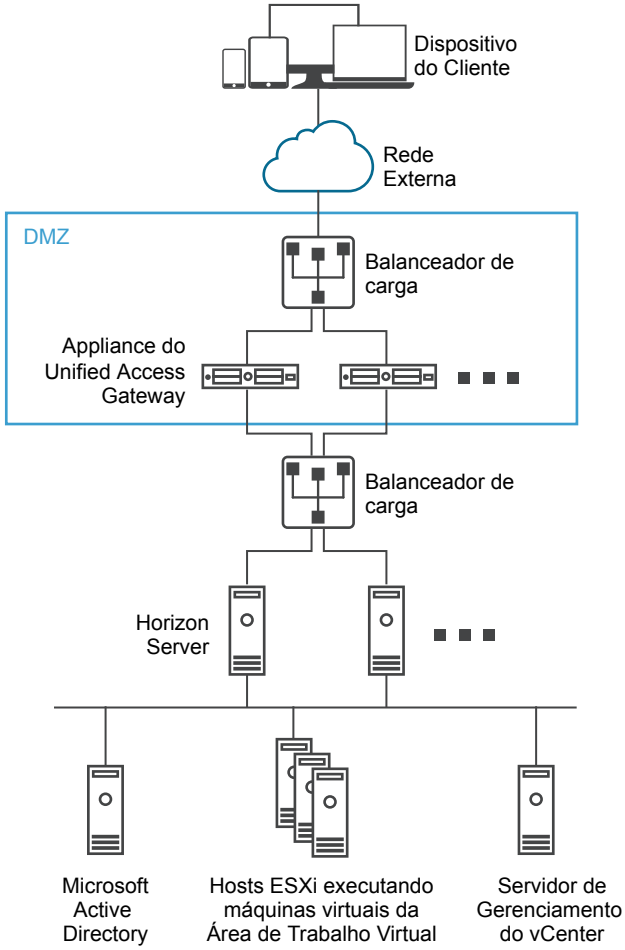
- Se o appliance do Unified Access Gateway apontar para um balanceador de carga na parte frontal dos servidores Horizon, a seleção da instância do servidor será dinâmica.

- O Unified Access Gateway substitui o servidor de segurança Horizon.
- Por padrão, a porta 8443 deve estar disponível para Blast TCP/UDP. No entanto, a porta 443 também pode ser configurada para Blast TCP/UDP.
- O gateway seguro e o gateway seguro PCoIP devem ser habilitados quando o Unified Access Gateway estiver implantado com o Horizon. Isso garante que os protocolos de exibição possam servir como proxies automaticamente por meio do Unified Access Gateway. As configurações do BlastExternalURL e pcoipExternalURL especificam endereços de conexão usados pelos clientes do Horizon para encaminhar essas conexões de protocolo de exibição por meio dos gateways apropriados no Unified Access Gateway. Isso oferece uma segurança melhorada, tendo em vista que esses gateways garantem que o tráfego do protocolo de exibição seja controlado em nome de um usuário autenticado. O tráfego do protocolo de exibição não autorizado é desconsiderado pelo Unified Access Gateway.
- Desative os gateways seguros (gateway seguro Blast e o gateway seguro PCoIP) nas instâncias do servidor de conexão do View e ative esses gateways nos appliances do Unified Access Gateway.

A principal diferença do servidor de segurança do View é que o Unified Access Gateway apresenta-se como se segue.

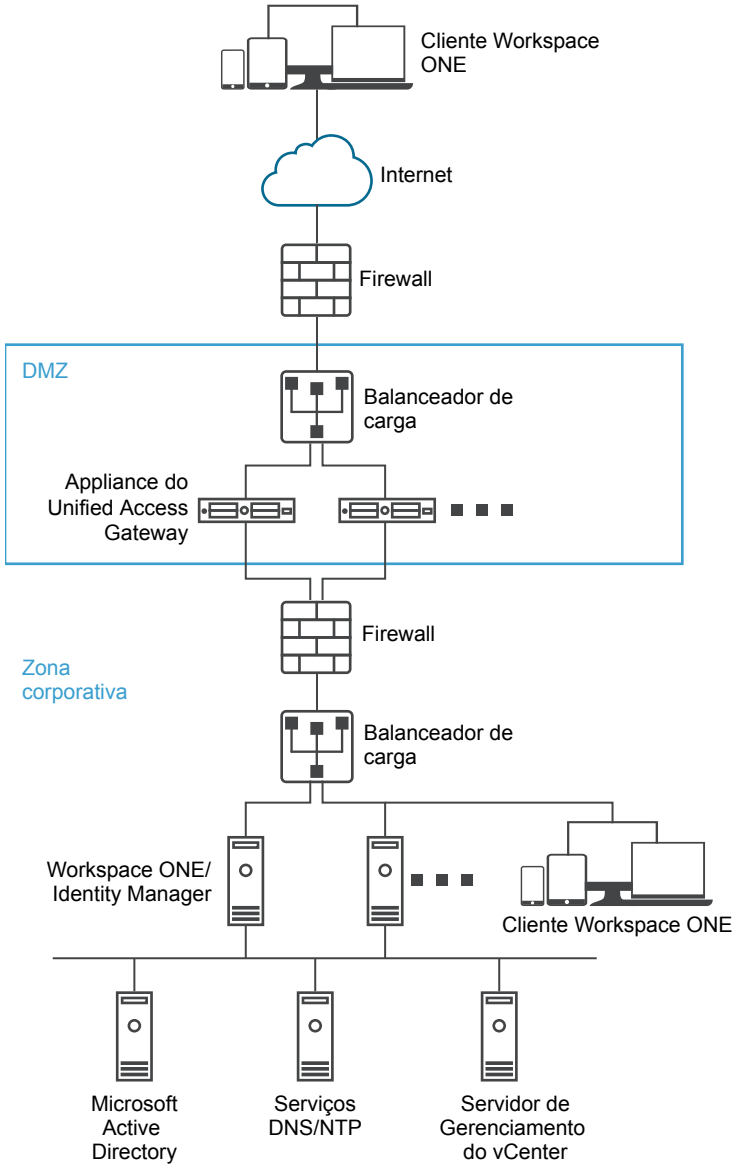
- Implementação segura. O Unified Access Gateway é implementado como uma máquina virtual pré-configurada, protegida e bloqueada, baseada em Linux.
- Escalável. Você pode conectar o Unified Access Gateway com um servidor de conexão do view individual, ou você pode conectá-lo por meio de um balanceador de carga na frente de vários servidores de conexão do view, oferecendo alta disponibilidade aprimorada. Ele age como uma camada entre o Horizon Clients e os Servidores de Conexão do View de back-end. Como a implementação é rápida, ele pode rapidamente ser ampliado ou reduzido para atender as demandas de empresas em constante mudança.

**Figura 4-1.** Appliance do Unified Access Gateway apontando para um balanceador de carga




De modo alternativo, é possível ter um ou mais appliances do Unified Access Gateway apontando para a instância de um servidor individual. Em ambas as abordagens, utilize um balanceador de carga na frente de dois ou mais appliances do Unified Access Gateway na DMZ.

**Figura 4-2.** Appliance do Unified Access Gateway apontando para uma instância do servidor Horizon




## Autenticação

A autenticação do usuário é similar ao servidor de segurança do View. Os métodos compatíveis de autenticação do usuário no Unified Access Gateway incluem o seguinte.

- O nome de usuário e a senha do Active Directory
- Modo Kiosk. Para obter mais detalhes sobre o modo de quiosque, consulte a documentação do Horizon
- Autenticação de dois fatores do RSA SecurID, formalmente certificada pela RSA para SecurID
- RADIUS por meio de diversas soluções de dois fatores de fornecedores de segurança terceirizados.
- Cartão inteligente, CAC ou certificados de usuário PIV X.509
- SAML

Esses métodos de autenticação são compatíveis com o servidor de conexão do View. Não é obrigatório que o Unified Access Gateway tenha comunicação direta com o Active Directory. Essa comunicação serve como um proxy por meio do Servidor de Conexão do View, que pode acessar diretamente o Active Directory. Após a sessão do usuário ser autenticada de acordo com a política de autenticação, o Unified Access Gateway pode encaminhar as solicitações para informações de qualificação, e a área de trabalho e o aplicativo iniciam solicitações para o servidor de conexão do View. O Unified Access Gateway também gerencia a área de trabalho e os manipuladores de protocolo de aplicação para permitir que encaminhem somente tráfego de protocolo autorizado.

O Unified Access Gateway identifica sozinho a autenticação de cartões inteligentes. Isso inclui opções para que o Unified Access Gateway se comunique com os servidores do protocolo de status do certificado online (OCSP) e para verificar a revogação do certificado X.509, e assim por diante.

## Definir configurações do Horizon

É possível implantar o Unified Access Gateway a partir do Horizon View e do Horizon Cloud with On-Premises Infrastructure. Para o componente do View do VMware Horizon, o appliance do Unified Access Gateway cumpre a mesma função que foi anteriormente desempenhada pelo servidor de segurança do View.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.

3 Clique no ícone de engrenagem **Configurações do Horizon**.

4 Na página Configurações do Horizon, altere o NÃO para **SIM** para ativar o Horizon

5 Defina os seguintes recursos de configurações do serviço de borda para o Horizon

| Opção | Descrição |
|---|---|
| **Identificador** | Definido como padrão para o View. O Unified Access Gateway pode se comunicar com os servidores que usam o protocolo XML do View, como o servidor de conexão do View, o Horizon Cloud, e o Horizon Cloud with On-Premises Infrastructure. |
| **URL do servidor de conexão** | Insira o endereço do servidor Horizon ou do balanceador de carga. Insira-o como https://00.00.00.00 |
| **Impressões digitais da URL de destino do proxy** | Insira a lista de impressões digitais do servidor do Horizon<br>Se você não fornecer uma lista das impressões digitais, os certificados do servidor deverão ser emitidos por uma CA confiável. Insira os dígitos da impressão digital hexadecimal. Por exemplo, sha1= C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 |

6 Para configurar a regra do método de autenticação e outras configurações avançadas, clique em **Mais**.

| Opção | Descrição |
|---|---|
| **Métodos de autenticação** | Selecione os métodos de autenticação a serem utilizados.<br>O padrão é utilizar a autenticação de passagem do nome de usuário e senha. Os métodos de autenticação configurados no Unified Access Gateway estão listados nos menus suspensos.<br>Para configurar uma autenticação que inclui aplicar um segundo método de autenticação caso a primeira tentativa de autenticação não seja bem-sucedida.<br>a Selecione um método de autenticação no primeiro menu suspenso.<br>b Clique no + e selecione E ou OU.<br>c Selecione o segundo método de autenticação no terceiro menu suspenso.<br>Para exigir que os usuários façam a autenticação através de dois métodos de autenticação, altere OU para E no menu suspenso. |
| **URL de verificação de integridade** | Se um balanceador de carga estiver configurado, insira a URL que o balanceador de carga utiliza para se conectar e verifique a integridade do appliance do Unified Access Gateway. |
| **SAML SP** | Insira o nome do provedor de serviços SAML para o agente do View XMLAPI. Esse nome deve corresponder ao nome de um metadado de um provedor de serviços configurado ou ser o valor especial DEMO. |
| **PCOIP ativado** | Altere NÃO para **SIM** para especificar se o gateway seguro PCoIP está habilitado. |
| **URL externa do proxy** | Insira a URL externa do appliance do Unified Access Gateway. Os clientes utilizam essa URL para conexões seguras por meio do Gateway seguro PCoIP. Esta conexão é utilizada para o tráfego PCoIP. O padrão é o endereço IP do Unified Access Gateway e a porta 4172. |
| **Aviso de dica do cartão inteligente** | Altere o NÃO para **SIM** para habilitar o appliance do Unified Access Gateway para que seja compatível com o recurso de sugestões de nome de usuário de cartão inteligente. Com o recurso de sugestões de cartão inteligente, o certificado de cartão inteligente de um usuário pode mapear várias contas de usuário do domínio Active Directory. |
| **Blast ativado** | Para usar o Gateway seguro Blast, altere o NÃO para **SIM**. |
| **URL externa de Blast** | Insira a URL do FQDN do appliance do Unified Access Gateway que os usuários utilizam para fazer uma conexão segura a partir dos navegadores da Web através do gateway seguro Blast. Insira-o como https://exampleappliance:443 |
| **Servidor do túnel UDP habilitado** | Ative isto se os Horizon Clients usarem uma condição de rede deficiente. |
| **Túnel ativado** | Se o túnel seguro do View for utilizado, altere NÃO para **SIM**. O Client utiliza a URL externa para conexões de túnel através do Gateway seguro do View. O túnel é utilizado para tráfego RDP, USB e de redirecionamento de multimídia (multimedia redirection, MMR). |
| **URL externa do túnel** | Insira a URL externa do appliance do Unified Access Gateway. O valor padrão será usado se não estiver configurado. |
| **Padrão de proxy** | Insira a expressão regular que corresponde aos URIs que estão relacionados à URL do servidor Horizon (proxyDestinationUrl). Para o servidor de conexão do View, uma barra (/) é um valor típico para fornecer o redirecionamento ao cliente Web HTML Access Web ao utilizar o appliance do Unified Access Gateway. |
| **Corresponder nome do usuário do Windows** | Altere o NÃO para **SIM** para corresponder ao RSA SecurID e ao nome do usuário Windows. Quando definido para SIM, o securID-auth está definido como verdadeiro e a correspondência de nomes de usuário SecurID e Windows é aplicada. |
| **Localização do gateway** | Altere o NÃO para **SIM** para ativar a localização de onde as solicitações se originam. O servidor de segurança e o Unified Access Gateway definem a localização do gateway. O local pode ser externo ou interno. |

| Opção | Descrição |
|---|---|
| **Windows SSO ativado** | Altere o NÃO para **SIM** para ativar a autenticação RADIUS. O login do Windows utiliza as credenciais utilizadas na primeira solicitação de acesso RADIUS bem-sucedida. |
| **Entradas de host** | Insira uma lista separada por vírgulas das entradas de host a serem adicionadas no arquivo de /etc/hosts. Cada entrada inclui um IP, um nome de host e um pseudônimo de nome de host opcional nesta ordem, separados por um espaço. Por exemplo, **`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**. |

7 Clique em **Salvar**.

## Opções de configuração de URL externa de TCP e UDP Blast

O gateway seguro Blast inclui a rede Blast Extreme Adaptive Transport (BEAT), que ajusta dinamicamente as condições da rede, como variações de velocidade e perda de pacotes. No Unified Access Gateway, é possível configurar as portas usadas pelo protocolo BEAT.

O Blast usa as portas padrão TCP 8443 e UDP 8443. A UDP 443 também pode ser usada para acessar a área de trabalho através do servidor de túnel UDP. A configuração da porta é ajustada adequadamente através da URL externa do Blast.

**Tabela 4-1.** Opções de porta do BEAT

| URL externa de Blast | Porta TCP usada pelo cliente | Porta UDP usada pelo cliente | Descrição |
|---|---|---|---|
| https://ap1.myco.com | 8443 | 8443 | Este formato é o padrão e exige que a TCP 8443 e opcionalmente a UDP 8443 sejam abertas no firewall para permitir conexões à internet para o Unified Access Gateway |
| https://ap1.myco.com:443 | 443 | 8443 | Usar este formato quando for necessário abrir a TCP 443 ou UDP 8443. |
| https://ap1.myco.com:xxxx | xxxx | 8443 | |
| https://ap1.myco.com:xxxx/?UDPPort=yyyy | xxxx | yyyy | |

Para configurar portas diferentes do padrão, deve ser adicionada uma regra interna de encaminhamento de IP para o respectivo protocolo quando for implantado. As regras de encaminhamento devem ser especificadas na implantação do modelo do OVF ou por meio dos arquivos INI que são inseridos por meio de comandos PowerShell.

# Implementação como proxy reverso

O Unified Access Gateway pode ser usado como um proxy reverso da web e pode agir como um proxy reverso comum ou como um proxy reverso de autenticação na DMZ.

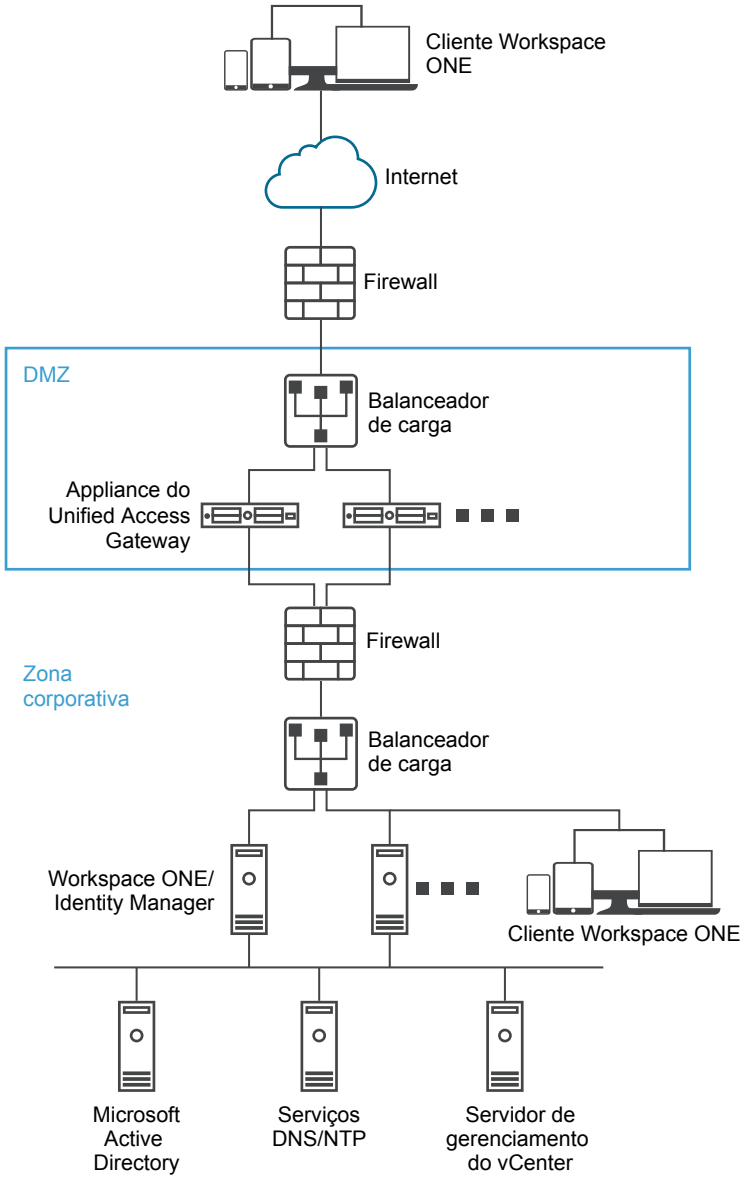
## Cenário de implementação

O Unified Access Gateway fornece acesso remoto para a implantação local do VMware Identity Manager. Os appliances do Unified Access Gateway são implantados, geralmente, em uma zona desmilitarizada (DMZ) da rede. Com o VMware Identity Manager, o appliance do Unified Access Gateway opera como um proxy reverso da Web entre um navegador do usuário e o serviço VMware Identity Manager no centro de dados. OUnified Access Gateway também habilita o acesso remoto ao catálogo do Workspace ONE para iniciar aplicativos do Horizon.

Requisitos para a implantação do Unified Access Gateway com o VMware Identity Manager.

- DNS dividido
- O appliance do VMware Identity Manager deve ter um nome de domínio totalmente qualificado (fully qualified domain name, FQDN) como nome do host.
- O Unified Access Gateway deve usar DNS interno. Isso significa que a URL de destino de proxy deve usar um FQDN.

**Figura 4-3.** Appliance Unified Access Gateway Indicando o VMware Identity Manager



## Entendendo o proxy reverso

O Unified Access Gateway, como uma solução, fornece acesso ao portal de aplicativos para usuários remotos para single sign-on e acesso aos recursos. Você habilita o proxy reverso de autenticação em um service manager de borda. Atualmente, os métodos de autenticação do RSA SecureID e RADIUS são compatíveis.

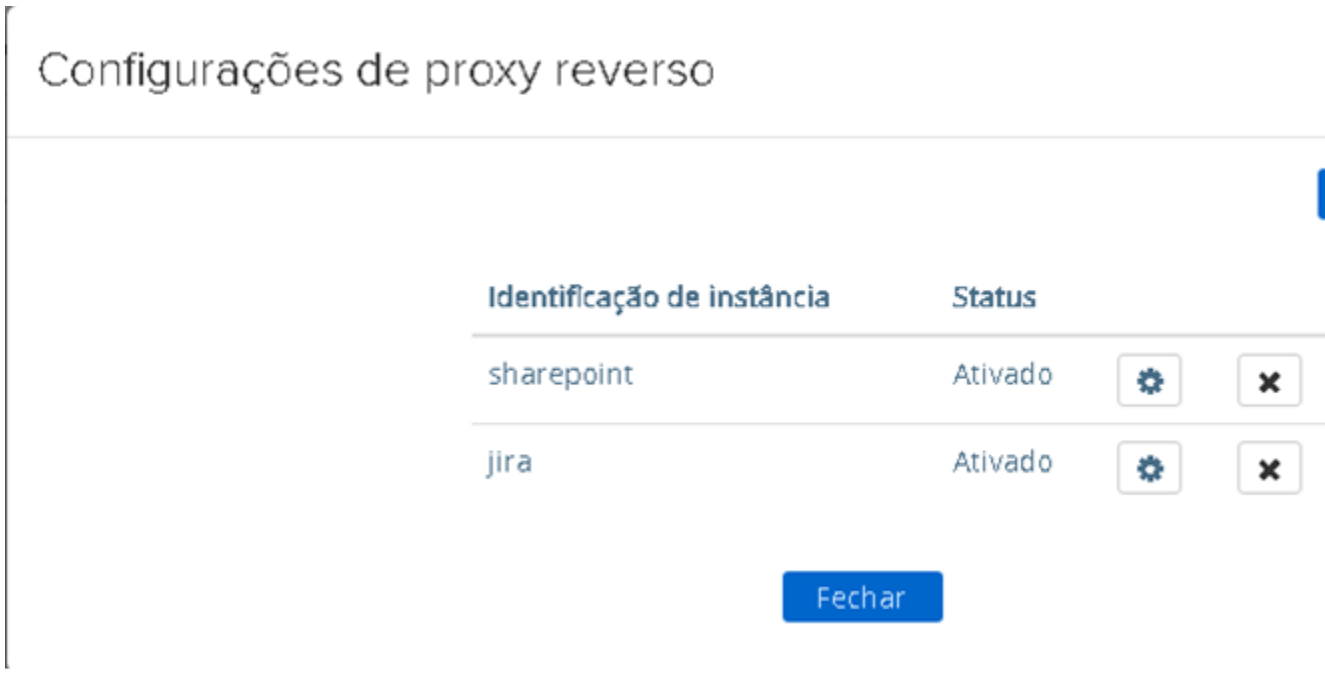
**Observação** Você deve gerar metadados do provedor de identidade antes de habilitar a autenticação no proxy reverso da web.

OUnified Access Gateway fornece acesso remoto ao VMware Identity Manager e aos aplicativos da web com ou sem autenticação do cliente baseado no navegador e, em seguida, inicia a área de trabalho do Horizon.

- Os clientes baseados em navegadores são suportados usando o RADIUS e o RSA SecurID como métodos de autenticação.

É possível configurar várias instâncias de proxy reverso e cada instância configurada pode ser excluída.

**Figura 4-4.** Vários Proxies Reversos Configurados




## Configurar proxy reverso

É possível configurar o serviço de proxy reverso da Web para utilizar o Unified Access Gateway com o VMware Identity Manager.

### Pré-requisitos

Requisitos para a implantação com o VMware Identity Manager.

- DNS dividido. O DNS dividido pode ser usado para resolver o nome para endereços IP diferentes, dependendo se o IP é interno ou externo.
- O serviço do VMware Identity Manager deve ter um nome de domínio totalmente qualificado (fully qualified domain name, FQDN) como o nome do host.
- O Unified Access Gateway deve usar DNS interno. Isso significa que a URL de destino do proxy deve usar um FQDN.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.

3 Clique no ícone de engrenagem **Configurações de Proxy Reverso**.

4 Na página de configuração do proxy reverso, clique em **Adicionar**.

5 Na seção Configurações de proxy reverso, altere o NÃO para **SIM** para habilitar o proxy reverso.

6 Configurar as configurações do serviço de borda.

| Opção | Descrição |
|---|---|
| **Identificador** | O identificador do serviço de borda é configurado como proxy reverso da Web. |
| **Identificação de instância** | O nome exclusivo para identificar e diferenciar uma instância de proxy reverso da Web de todas as demais instâncias de proxy reverso da Web. |
| **URL de destino do proxy** | Insira o endereço do aplicativo da Web. |
| **Impressões digitais da URL de destino do proxy** | Insira uma lista das impressões digitais do certificado do servidor SSL aceitáveis para a URL de destino do proxy. Se você incluir um curinga*, qualquer certificado será permitido. Uma impressão digital tem o formato [alg=]xx:xx, onde alg pode ser sha1, o padrão ou md5. Os 'xx' são dígitos hexadecimais. O separador ':' também pode ser um espaço ou estar ausente. O caso em uma impressão digital é ignorado. Por exemplo:<br>sha1=B6 77 DC 9C 19 94 2E F1 78 F0 AD 4B EC 85 D1 7A F8 8B DC 34,<br>sha256=ad:5c:f1:48:47:94:7e:80:82:73:13:6c:83:52:be:78:ed:ff:50:23:56:a8:42:8a:d9:30:fc:3a:33:d6:c6:db<br>Se você não configurar as impressões digitais, os certificados do servidor deverão ser emitidos por uma Autoridade de Certificação (Certificate Authority, CA) confiável. |
| **Padrão de proxy** | Insira os caminhos de URI correspondentes que encaminham para a URL de destino. Por exemplo, insira como **`(/\|/SAAS(.*)\|/hc(.*)\|/web(.*)\|/catalog-portal(.*))`**.<br>**Observação** Ao configurar vários proxies reversos, forneça o nome do host no padrão de host do proxy. |

7 Para definir outras configurações avançadas, clique em **Mais**.

| Opção | Descrição |
|---|---|
| **Métodos de autenticação** | O padrão é utilizar a autenticação de passagem do nome de usuário e senha. Os métodos de autenticação configurados no Unified Access Gateway estão listados nos menus suspensos. |
| **Caminho de URI para verificação de integridade** | O Unified Access Gateway se conecta a este caminho de URI para verificar a integridade de seu aplicativo Web. |
| **SAML SP** | Esse campo é necessário ao configurar o UAG como proxy reverso autenticado para o VMware Identity Manager. Insira o nome do provedor de serviços SAML para o agente do View XML API. Esse nome deve corresponder ao nome de um provedor de serviços configurado com o Unified Access Gatewayou ser o valor especial **`DEMO`**. Se houver vários provedores de serviços configurados com oUnified Access Gateway, seus nomes deverão ser únicos. |
| **Código de ativação** | Insira o código de ativação gerado pelo serviço do VMware Identity Manager e importado no Unified Access Gateway para configurar a confiança entre o VMware Identity Manager e o Unified Access Gateway. Observe que o código de ativação não é necessário para implantações on-premise (local). Para obter detalhes sobre como gerar um código de ativação, consulte *Implantação em nuvem do VMware Identity Manager*. |

| Opção | Descrição |
|---|---|
| **URL externa** | O valor padrão é a URL do host do Unified Access Gateway e a porta 443. É possível inserir uma outra URL externa. Digite como `https://<host:port>`. |
| **Padrão desprotegido** | Insira o padrão de redirecionamento conhecido do VMware Identity Manager. Por exemplo: `(/catalog-portal(.*)\|/\|/SAAS/\|/SAAS\|/SAAS/API/1.0/GET/image(.*)\|/SAAS/horizon/css(.*)\|/SAAS/horizon/angular(.*)\|/SAAS/horizon/js(.*)\|/SAAS/horizon/js-lib(.*)\|/SAAS/auth/login(.*)\|/SAAS/jersey/manager/api/branding\|/SAAS/horizon/images/(.*)\|/SAAS/jersey/manager/api/images/(.*)\|/hc/(.*)/authenticate/(.*)\|/hc/static/(.*)\|/SAAS/auth/saml/response\|/SAAS/auth/authenticatedUserDispatcher\|/web(.*)\|/SAAS/apps/\|/SAAS/horizon/portal/(.*)\|/SAAS/horizon/fonts(.*)\|/SAAS/API/1.0/POST/sso(.*)\|/SAAS/API/1.0/REST/system/info(.*)\|/SAAS/API/1.0/REST/auth/cert(.*)\|/SAAS/API/1.0/REST/oauth2/activate(.*)\|/SAAS/API/1.0/GET/user/devices/register(.*)\|/SAAS/API/1.0/oauth2/token(.*)\|/SAAS/API/1.0/REST/oauth2/session(.*)\|/SAAS/API/1.0/REST/user/resources(.*)\|/hc/t/(.*)/(.*)/authenticate(.*)\|/SAAS/API/1.0/REST/auth/logout(.*)\|/SAAS/auth/saml/response(.*)\|/SAAS/(.*)/(.*)auth/login(.*)\|/SAAS/API/1.0/GET/apps/launch(.*)\|/SAAS/API/1.0/REST/user/applications(.*)\|/SAAS/auth/federation/sso(.*)\|/SAAS/auth/oauth2/authorize(.*)\|/hc/prepareSaml/failure(.*)\|/SAAS/auth/oauthtoken(.*)\|/SAAS/API/1.0/GET/metadata/idp.xml\|/SAAS/auth/saml/artifact/resolve(.*)\|/hc/(.*)/authAdapter(.*)\|/hc/authenticate/(.*)\|/SAAS/auth/logout\|/SAAS/common.js\|/SAAS/auth/launchInput(.*)\|/SAAS/launchUsersApplication.do(.*)\|/hc/API/1.0/REST/thinapp/download(.*)\|/hc/t/(.*)/(.*)/logout(.*))` |
| **Cookie de autenticação** | Insira o nome do cookie de autenticação. Por exemplo: **`HZN`** |
| **URL de redirecionamento de logon** | Se o usuário fizer logout do portal, digite o URL de redirecionamento para efetuar login novamente. Por exemplo: **`/SAAS/auth/login?dest=%s`** |
| **Padrão de host de proxy** | Nome de host externo usado para verificar o host que entra para verificar se combina com o padrão para aquela instância em particular. O padrão do host é opcional ao configurar instâncias de proxy reverso da Web. |
| **Entradas de host** | Insira uma lista separada por vírgulas das entradas de host a serem adicionadas no arquivo de /etc/hosts. Cada entrada inclui um IP, um nome de host e um pseudônimo de nome de host opcional nesta ordem, separados por um espaço. Por exemplo, **`10.192.168.1 example1.com, 10.192.168.2 example2.com example-alias`**. |

**Observação** Padrão desprotegido, Cookie de autenticação e as opções de URL de redirecionamento de logon são aplicáveis apenas com o VMware Identity Manager. Os valores fornecidos aqui também são aplicáveis ao Access Point 2.8 e ao Unified Access Gateway 2.9.

**Observação** As propriedades do Cookie de autenticação e do Padrão desprotegido não são válidas para proxy reverso de autenticação. Você deve usar a propriedade Métodos de autenticação para definir o método de autenticação.

8 Clique em **Salvar**.

### Próximo passo

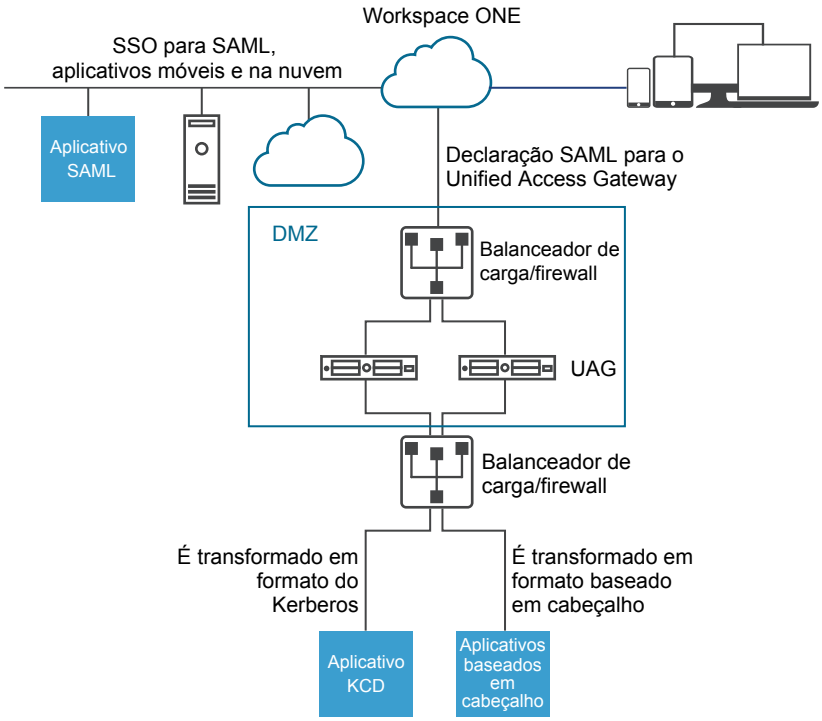
Para habilitar a ponte de identidade, consulte "Configurando as definições da ponte de identidade", na página 45.

# Implementação para acesso single sign-on para aplicativos da Web locais herdados.

O recurso de ponte de identidade do Unified Access Gateway pode ser configurado para fornecer single sign-on (SSO) para aplicativos da internet herdados que usam a delegação restrita do Kerberos (KCD) ou a autenticação baseada no cabeçalho.

O Unified Access Gateway em modo de ponte de identidade atua como o provedor de serviços que passa a autenticação do usuário para os aplicativos herdados configurados. O VMware Identity Manager atua como um provedor de identidade e fornece SSO nos aplicativos SAML. O Identity Manager autentica o usuário quando os aplicativos herdados de acesso dos usuários exigem a autenticação KCD ou baseada em cabeçalho. A declaração SAML com as informações do usuário é enviada ao Unified Access Gateway. O Unified Access Gateway usa essa autenticação para permitir que os usuários acessem o aplicativo.

**Figura 4-5.** Modo de ponte de identidade do Unified Access Gateway




## Cenários de implantação de ponte de identidade

O modo de ponte de identidade do Unified Access Gateway pode ser configurado para trabalhar com o VMware Workspace® ONE® em nuvem ou em um ambiente local.

### Usando a ponte de identidade do Unified Access Gateway com clientes do Workspace ONE na nuvem

O modo de ponte de identidade pode ser configurado para trabalhar com o Workspace ONE na nuvem para autenticar usuários. Quando um usuário solicita acesso para um aplicativo da Web herdado, o provedor de identidade aplica as políticas aplicáveis de autenticação e autorização.

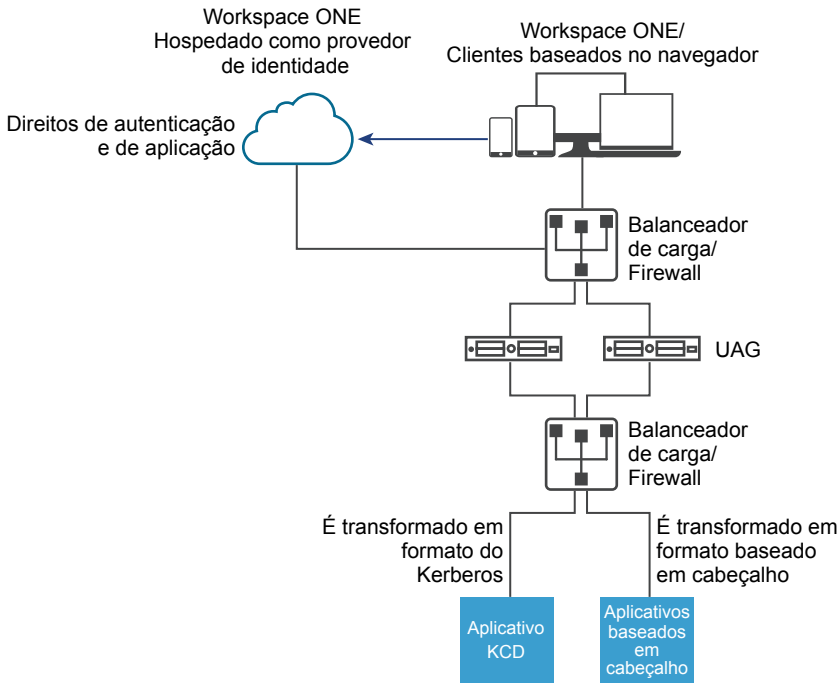
Se o usuário for validado, o provedor de identidade cria um token SAML e o envia ao usuário. O usuário passa o token SAML ao Unified Access Gateway na DMZ. O Unified Access Gateway valida o token SAML e recupera o nome da entidade do usuário do token.

Se a solicitação for para a autenticação no Kerberos, a delegação restrita do Kerberos será usada para negociar com o servidor do Active Directory. O Unified Access Gateway representa o usuário para recuperar o token do Kerberos para autenticar com o aplicativo.

Se a solicitação for para autenticação baseada em cabeçalho, o nome de cabeçalho do usuário é enviado ao servidor de internet para solicitar a autenticação com o aplicativo.

O aplicativo envia a resposta de volta ao Unified Access Gateway A resposta é devolvida ao usuário.

**Figura 4-6.** Ponte de identidade do Unified Access Gateway com os clientes do Workspace ONE na nuvem




## Usando a ponte de identidade com os clientes do Workspace ONE local

Quando o modo de ponte de identidade é configurado para os usuários de autenticação com o Workspace ONE em um ambiente local, os usuários inserem a URL para acessar o aplicativo de internet herdado local por meio do proxy do Unified Access Gateway. O Unified Access Gateway redireciona a solicitação ao provedor de identidade para autenticação. O provedor de identidade aplica as políticas de autenticação e autorização à solicitação. Se o usuário for validado, o provedor de identidade criará um token SAML e o enviará ao usuário.

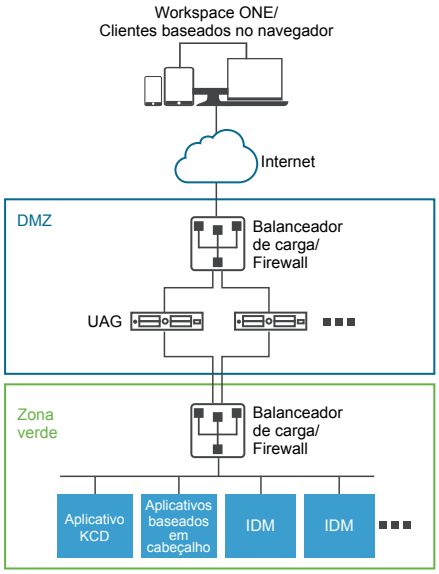
O usuário passa o token SAML ao Unified Access Gateway. O Unified Access Gateway valida o token SAML e recupera o nome da entidade do usuário do token.

Se a solicitação for para a autenticação no Kerberos, a delegação restrita do Kerberos será usada para negociar com o servidor do Active Directory. O Unified Access Gateway representa o usuário para recuperar o token do Kerberos para autenticar com o aplicativo.

Se a solicitação for para autenticação baseada em cabeçalho, o nome de cabeçalho do usuário é enviado ao servidor de internet para solicitar a autenticação com o aplicativo.

O aplicativo envia a resposta de volta ao Unified Access Gateway A resposta é devolvida ao usuário.

**Figura 4-7.** Ponte de identidade do Unified Access Gateway local.




## Configurando as definições da ponte de identidade

Quando o Kerberos é configurado na aplicação de back-end, para configurar a ponte de identidade no Unified Access Gateway, é necessário carregar os metadados do provedor de identidade e o arquivo keytab e configurar as definições de território do KCD.

**Observação** Esta versão de ponte de identidade é compatível apenas com uma configuração de domínio único. Isso significa que o usuário e o SPN devem estar no mesmo território/domínio.

Quando a ponte de identidade está habilitada com a autenticação baseada em cabeçalho, as configurações de keytab e as configurações de território do KCD não são necessárias.

Antes de configurar as definições da ponte de identidade para a autenticação do Kerberos, certifique-se de que o seguinte esteja disponível.

- Um provedor de identidade é configurado e os metadados SAML do provedor de identidade são salvos. O arquivo de metadados SAML é carregado para o Unified Access Gateway (apenas cenários de SAML).
- Para a autenticação do Kerberos, um servidor com o Kerberos habilitado com os nomes dos territórios para os centros de distribuição de chaves para o uso identificado.
- Para a autenticação do Kerberos, carregar o arquivo keytab para o Unified Access Gateway. O arquivo keytab inclui as credenciais para a conta do serviço de Active Directory que é configurada para obter o ticket do Kerberos em nome de qualquer usuário no domínio para um determinado serviço de back-end.

### Carregar metadados do provedor de identidade

Para configurar o recurso de ponte de identidade, é necessário carregar o arquivo XML de metadados do certificado SAML do provedor de identidade para o Unified Access Gateway

#### Pré-requisitos

É possível acessar o arquivo XML de metadados SAML salvo em um computador.

Se for usado o VMware Identity Manager como provedor de identidade, baixe e salve o arquivo de metadados SAML do console de administrador do VMware Identity Manager, Catálogo > Metadados SAML de configurações > Link de metadados do provedor de identidade (IdP).

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção **Configurações avançadas > Configurações de ponte de identidade,** selecionar o ícone de engrenagem de **Carregar metadados do provedor de identidade**.

3 Insira a ID da entidade para o provedor de identidade na caixa de texto **ID da entidade** .

Se não for inserido um valor na caixa de texto ID da entidade, o nome no provedor de identidade no arquivo de metadados será analisado e usado como a ID da entidade do provedor de identidade.

4 Na seção **Metadados IDP** , clique em **Selecionar** e navegue até o arquivo de metadados salvo. Clique em **Abrir**.

5 Clique em **Salvar**.

### Próximo passo

Para a autenticação KDC, configure as configurações de território e as configurações keytab.

Para autenticação baseada em cabeçalho, quando você configurar o recurso de ponte de identidade, preencha a opção Nome de cabeçalho do usuário com o nome do cabeçalho HTTP que inclui a ID do usuário.

## Definir configurações do território

Configure o nome do território do domínio, os centros de distribuição de chaves para o território e o tempo limite KDC.

O território é o nome de uma entidade administrativa que mantém os dados de autenticação. É importante selecionar um nome descritivo para o território de autenticação Kerberos. Configure o território, saiba também o nome do domínio e o serviço KDC correspondente no Unified Access Gateway. Quando a solicitação UPN vai para um território específico, o Unified Access Gateway resolve internamente o KDC para usar o ticket de serviço do Kerberos.

A convenção é fazer com que o nome do território seja o mesmo que o seu nome de domínio, inserido em letras maiúsculas. Por exemplo, um nome de território é EXAMPLE.NET. O nome do território é usado por um cliente Kerberos para gerar nomes DNS.

Começando com o UAG 3.0, você pode excluir territórios definidos anteriormente.

### Pré-requisitos

Um servidor com o Kerberos habilitado com os nomes dos territórios para os centros de distribuição de chaves para o uso identificado.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção **Configurações avançadas > Configurações de ponte de identidade,** selecione o ícone de engrenagem **Configurações do território**.

3 Clique em **Adicionar**.

4 Preencha o formulário.

| Etiqueta | Descrição |
|---|---|
| Nome do território | Insira o território com o nome do domínio. Insira o território em letras maiúsculas. O território deve ser correspondente ao nome do domínio configurado no Active Directory. |
| Centros de distribuição de chaves | Inserir os servidores KDC para o território. Separe com vírgula a lista se for adicionado mais de um servidor. |
| Tempo limite do KDC (em segundos) | Insira o tempo de espera para a resposta do KDC. O padrão é de 3 segundos. |

5 Clique em **Salvar**.

### Próximo passo

Configure as definições de keytab.

## Carregar configurações Keytab

Um keytab é um arquivo que contém pares de chaves principais e criptografadas do Kerberos. Um arquivo keytab é criado para aplicações que exigem single sign-on. A ponte de identidade do Unified Access Gateway usa um arquivo keytab para que seja autenticado em sistemas remotos usando o Kerberos sem inserir uma senha.

Quando um usuário é autenticado no Unified Access Gateway a partir de um provedor de identidade, o Unified Access Gateway solicita um tíquete do Kerberos do controlador de domínio do Kerberos para autenticar o usuário.

O Unified Access Gateway usa um arquivo keytab para representar o usuário a autenticar o domínio do Active Directory. O Unified Access Gateway deve ter uma conta de serviço do usuário do domínio no domínio do Active Directory. O Unified Access Gateway não fica ligado diretamente ao domínio.

**Observação** Se o administrador regenerar o arquivo keytab para uma conta de serviços, o arquivo keytab deverá ser carregado novamente no Unified Access Gateway.

### Pré-requisitos

Acesse o arquivo keytab do Kerberos para carregar para o Unified Access Gateway. O arquivo keytab é um arquivo binário. Se possível, use SCP ou outro método seguro para transferir o keytab entre os computadores.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção **Configurações avançadas > Configurações de ponte de identidade,** selecione o ícone de engrenagem **Carregar configurações keytab**.

3 (Opcional) Insira o nome da entidade do Kerberos na caixa de texto **Nome da entidade**.

Cada identidade sempre é totalmente qualificada com o nome do território. O território sempre deve estar em letras maiúsculas.

Certifique-se de que o nome da entidade inserido aqui é o primeiro nome da entidade encontrado no arquivo keytab. Se o mesmo nome da entidade não estiver no arquivo keytab que foi carregado, o carregamento do arquivo keytab falhará.

4 No campo **Selecionar arquivo keytab**, clique em **Selecionar** e navegue até o arquivo keytab salvo. Clique em **Abrir**.

Se o nome da entidade não foi inserido, é usado o primeiro nome da entidade encontrado no keytab. É possível fundir diversos keytabs em um arquivo.

5 Clique em **Salvar**.

### Próximo passo

Configure um proxy reverso da Web para a ponte de identidade do Unified Access Gateway

## Configurar um proxy reverso da Web para a ponte de identidade

Ative a ponte de identidade, configure o nome do host externo para o serviço e baixe o arquivo de metadados do provedor de serviços do Unified Access Gateway.

Esse arquivo de metadados é carregado para a página Configuração de aplicativo na internet no serviço do VMware Identity Manager.

### Pré-requisitos

Configurações da ponte de identidade configuradas na IU do administrador do Unified Access Gateway na seção Configurações avançadas. As configurações a seguir devem ser definidas.

- Metadados do provedor de identidade carregados para o Unified Access Gateway.
- O nome principal do Kerberos configurado e o arquivo keytab carregado para o Unified Access Gateway.
- O nome do território e as informações do centro de distribuição de chaves.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.

3 Clique no ícone de engrenagem **Configurações de Proxy Reverso**.

4 Na página de configurações do proxy reverso, clicar em **Adicionar** para criar uma nova configuração de proxy.

5 Configurar as configurações do serviço de borda.

| Opção | Descrição |
|---|---|
| **Identificador** | O identificador do serviço de borda é configurado como proxy reverso da Web. |
| **Identificação de instância** | Nome exclusivo da instância do proxy reverso da Web. |
| **URL de destino do proxy** | Especifique o URI interno do aplicativo da Web. É obrigatório que o Unified Access Gateway leia e acesse esta URL. |
| **Impressões digitais da URL de destino do proxy** | Insira a URI para combinar com esta configuração de proxy. Uma impressão digital tem o formato [alg=]xx:xx, onde alg pode ser sha1, o padrão ou md5. Os 'xx' são dígitos hexadecimais. Por exemplo, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3<br>Se você não configurar as impressões digitais, os certificados do servidor deverão ser emitidos por uma Autoridade de Certificação (Certificate Authority, CA) confiável. |
| **Padrão de proxy** | (Opcional) Especifique um padrão de host. O padrão de host informa o Unified Access Gateway quando encaminhar o tráfego usando esta configuração de proxy se o padrão de proxy não for exclusivo. Isso é decidido usando a URL usada pelo navegador da Web do cliente. Por exemplo, insira como **`(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`**. |

6 Na seção Ativar ponte de identidade, altere de NÃO para **SIM**.

7 Configurar as seguintes configurações do serviço de borda.

| Opção | Descrição |
|---|---|
| **Provedor de identidade** | No menu suspenso, selecione o provedor de identidade a ser utilizado. |
| **Keytab** | No menu suspenso, selecione o keytab configurado para este proxy reverso. |
| **Nome da identidade do serviço de destino** | Insira o nome principal do serviço Kerberos. Cada identidade sempre é totalmente qualificada com o nome do território. Por exemplo, **`myco_hostname@MYCOMPANY`**. Digite o nome do território em letras maiúsculas. Se não for adicionado um nome na caixa de texto, o nome principal do serviço será derivado do nome do host da URL de destino do proxy. |
| **Página de aterrissagem de serviço** | Insira a página para a qual os usuários são redirecionados no provedor de identidade após a validação da declaração. A configuração padrão é `/`. |
| **Nome de cabeçalho do usuário** | Para a autenticação baseada em cabeçalho, insira o nome do cabeçalho HTTP que inclui a ID do usuário derivada da declaração. |

8 Na seção Baixar metadados SP, clicar em **Download**.

Salve o arquivo de metadados do provedor de serviços.

9 Clique em **Salvar**.

### Próximo passo

Adicione o arquivo de metadados do provedor de serviços do Unified Access Gateway à página Configuração de aplicativo da Web no serviço do VMware Identity Manager.

## Adicionar o arquivo de metadados do provedor de serviços do Unified Access Gateway ao serviço do VMware Identity Manager

O arquivo de metadados do provedor de serviços do Unified Access Gateway que foi baixado deve ser carregado na página Configuração de aplicativo de internet no serviço do VMware Identity Manager.

O certificado SSL usado deve ser o mesmo certificado usado em servidores do Unified Access Gateway com carga balanceada.

### Pré-requisitos

Arquivo de metadados do provedor de serviços do Unified Access Gateway salvo no computador

### Procedimentos

1 Faça logon no console de administração do VMware Identity Manager.

2 Na guia Catálogo, clique em **Adicionar Aplicativo** e selecione **Criar um novo**.

3 Na página Detalhes do aplicativo, insira um nome de usuário final amigável na caixa de texto Nome.

4 Selecione o perfil de autenticação **SAML 2.0 POST** .

Também é possível adicionar uma descrição desse aplicativo e um ícone para ser exibido aos usuários finais no portal Workspace ONE.

5 Clique em **Avançar** e na página Configuração de aplicativo, role até a seção **Configurar Via**.

6 Selecione o botão de opção XML de metadados e cole o texto dos metadados do provedor de serviços do Unified Access Gateway na caixa de texto de XML de metadados.

7 (Opcional) Na seção Mapeamento de atributos, mapeie os seguintes nomes de atributos para os valores de perfil de usuário. O valor do campo FORMATO é Básico. Os nomes de atributos devem ser inseridos em letras minúsculas.

| Nome | Valor configurado |
|---|---|
| upn | userPrincipalName |
| userid | ID de usuário do Active Directory |

8 Clique em **Salvar**.

### Próximo passo

Autorize usuários e grupos a usar este aplicativo.

**Observação** O Unified Access Gateway é compatível apenas com usuários de domínio único. Se o provedor de identidade estiver configurado com vários domínios, o aplicativo poderá ser qualificado apenas para usuários em um único domínio.

## VMware Tunnel no Unified Access Gateway

A implantação do VMware Tunnel usando o appliance do Unified Access Gateway fornece um método seguro e eficaz para aplicativos individuais para acessar recursos corporativos. O Unified Access Gateway é compatível com a implantação em ambientes ESXi ou Microsoft Hyper-V.

O VMware Tunnel é composto por dois componentes independentes: o Tunnel Proxy e o Per-App Tunnel. Você implanta o VMware Tunnel usando qualquer um dos dois modelos de arquitetura de rede: de uma ou várias camadas.

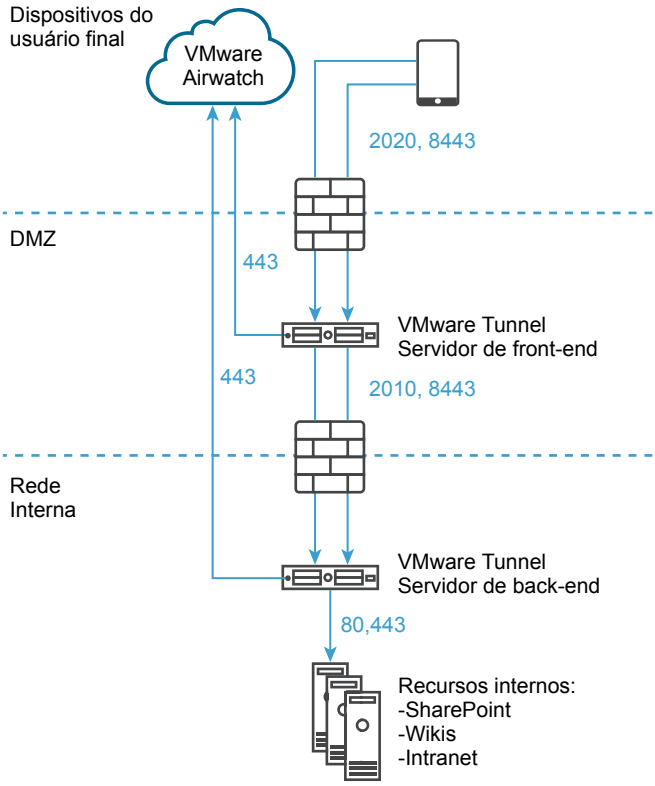
Os dois modelos de implantação, o Tunnel Proxy e Per-App Tunnel, podem ser usados para uma rede de várias camadas no appliance UAG. A implantação consiste em um servidor de front-end do Unified Access Gateway implantado no DMZ e em um servidor de back-end implantado na rede interna.

O componente do Tunnel Proxy garante o tráfego de rede entre um dispositivo de usuário final e um site por meio do VMware Browser ou qualquer aplicativo habilitado para SDK implantado a partir do AirWatch. O aplicativo móvel cria uma conexão HTTPS com o servidor do proxy de túnel e protege os dados confidenciais. Os dispositivos são autenticados para o Tunnel Proxy com um certificado emitido pelo SDK conforme configurado no Console de administração do AirWatch. Normalmente, esse componente deve ser usado quando há dispositivos não gerenciados que precisam de acesso seguro a recursos internos.

Para dispositivos totalmente registrados, o componente Per-App Tunnel permite que os dispositivos se conectem a recursos internos sem precisar do SDK do AirWatch. Esse componente aproveita os recursos nativos da VPN por aplicativo dos sistemas operacionais iOS, Android, Windows 10 e MacOS. Para obter mais informações sobre essas plataformas e recursos do componente do VMware Tunnel, consulte o *Guia do VMware Tunnel* em https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en

A implantação do VMware Tunnel para o seu ambiente AirWatch envolve a configuração do hardware inicial, a configuração do nome do host do VMware Tunnel e as informações da porta no Console de administração do AirWatch, o download e a implantação do modelo OVF do Unified Access Gateway e a configuração manual do VMware Tunnel. Consulte "Definir as configurações do VMware Tunnel para o AirWatch", na página 51 para obter mais detalhes.

**Figura 4-8.** Desenvolvimento multicamadas do VMware Tunnel: Proxy e Per-App Tunnel




O AirWatch v9.1 e posterior é compatível com o modo Cascata como o modelo de implantação de várias camadas para o VMware Tunnel. O modo Cascata requer uma porta de entrada dedicada para cada componente do Tunnel, que vai da Internet ao servidor front-end do Tunnel. Os servidores front-end e back-end devem poder se comunicar com a API do AirWatch e com os servidores AWCM. O modo Cascata do VMware Tunnel é compatível com a arquitetura de várias camadas do componente do Per-App Tunnel.

Para obter mais detalhes, incluindo aqueles na implantação do endpoint de relê para uso com o componente Proxy do túnel, consulte a documentação do *VMware Tunnel* em https://resources.air-watch.com/view/yr8n5s2b9d6qqbcfjbrw/en

## Definir as configurações do VMware Tunnel para o AirWatch

A implementação do proxy de túnel garante o tráfego de rede entre um dispositivo de usuário final e um site por meio do aplicativo móvel do Navegador do VMware.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Serviços de Borda, clique em **Mostrar**.

3 Clique no ícone **configurações do VMware Tunnel Settings**.

4 Altere o NÃO para **SIM** para ativar o proxy de túnel.

5 Defina os seguintes recursos de configurações do serviço de borda.

| Opção | Descrição |
|---|---|
| **URL do servidor da API** | Insira a URL do servidor da API do AirWatch. Por exemplo, insira como https://example.com:<port>. |
| **Nome de usuário do servidor da API** | Insira a nome de usuário para fazer login no servidor da API. |

| Opção | Descrição |
|---|---|
| **Senha do servidor da API** | Insira a senha para fazer login no servidor da API. |
| **ID do grupo de organização** | Insira a organização do usuário. |
| **Nome do host do servidor do túnel** | Digite o nome de host externo do VMware Tunnel configurado no console do administrador do AirWatch. |

6 Para definir outras configurações avançadas, clique em **Mais**.

| Opção | Descrição |
|---|---|
| **Host do proxy de saída** | Insira o nome do host onde o proxy de saída está instalado.<br>**Observação** Este não é o Proxy de Túnel. |
| **Porta do proxy de saída** | Insira o número da porta do proxy de saída. |
| **Nome de usuário do proxy de saída** | Insira a nome de usuário para fazer login no proxy de saída. |
| **Senha do proxy de saída** | Insira a senha para fazer login no proxy de saída. |
| **Autenticação NTLM** | Altere o NÃO para **SIM** para especificar que a solicitação de proxy de saída exige a autenticação NTLM. |
| **Utilizar para o proxy do VMware Tunnel** | Altere de NÃO para **SIM** para usar esse proxy como um proxy de saída para o VMware Tunnel. Se não estiver habilitado, o Unified Access Gateway utilizará esse proxy para a chamada da API inicial a fim de obter a configuração do console de administração do AirWatch. |
| **Entradas de host** | Insira uma lista separada por vírgulas das entradas de host a serem adicionadas no arquivo de /etc/hosts. Cada entrada inclui um IP, um nome de host e um pseudônimo de nome de host opcional nesta ordem, separados por um espaço. Por exemplo, **`10.192.168.1 example1.com, 10.192.168.2 example2.com exemplo-pseudônimo`**. |
| **Certificados confiáveis** | Selecionar os arquivos de certificados confiáveis a serem adicionados ao armazenamento de confiança. |

7 Clique em **Salvar**.

Para obter mais informações sobre a implantação do Unified Access Gateway com o AirWatch, consulte a documentação do VMware Tunnel https://my.air-watch.com/help/9.1/en/Content/Expert_Guides/EI/AW_Tunnel/C/Tunnel_Introduction.htm.

## Implantação do VMware Tunnel para o Watch usando o PowerShell

É possível usar o PowerShell para implantar o VMware Tunnel para o AirWatch.

Para obter informações sobre a implantação do VMware Tunnel com o PowerShell, assista este vídeo:

Implantação do PowerShell do VMware AirWatch Tunnel (http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_airwatch_tunnel_powershell)

# Configuração do Unified Access Gateway usando certificados TLS/SSL

5

Você deve configurar os Certificados TLS/SSL para os appliances do Unified Access Gateway.

**Observação** A configuração dos certificados TLS/SSL para o appliance do Unified Access Gateway aplica-se somente ao Horizon View, Horizon Cloud e ao proxy reverso da Web.

## Configurando certificados TLS/SSL para appliances do Unified Access Gateway

O TLS/SSL é necessário para conexões de clientes aos appliances do Unified Access Gateway. Appliances do Unified Access Gatewaye servidores intermediários voltados para o cliente que terminam conexões TLS/SSL necessitam de certificados de servidor TLS/SSL.

Certificados de servidor TLS/SSL são assinados por uma Autoridade de Certificação (CA). Uma CA é uma entidade confiável que garante a identidade do certificado e de seu criador. Quando um certificado é assinado por uma CA confiável, os usuários passam a não receber mensagens pedindo a verificação do certificado e os dispositivos cliente leves podem se conectar sem necessitar de configurações adicionais.

Um certificado de servidor TLS/SSL padrão é gerado ao implantar um appliance do Unified Access Gateway. Para ambientes de produção, a VMware recomenda a substituição do certificado padrão o mais rápido possível. O certificado padrão não é assinado por uma CA confiável. Utilize o certificado padrão somente em um ambiente que não é de produção.

### Selecionando o tipo correto de certificado

Você pode utilizar vários tipos de certificados TLS/SSL com o Unified Access Gateway. É crucial selecionar o tipo de certificado correto para a sua implementação. Tipos diferentes de certificado variam em termos de custo, dependendo do número de servidores nos quais podem ser utilizados.

Siga as recomendações de segurança da VMware utilizando nomes de domínio totalmente qualificados (FQDNs) para os certificados, independentemente do tipo selecionado. Não utilize um nome de servidor ou endereço IP simples, mesmo para comunicações dentro de seu domínio interno.

#### Certificado de nome de servidor único

Você pode gerar um certificado com um nome da entidade para um servidor específico. Por exemplo: `dept.exemplo.com`.

Este tipo de certificado será útil se, por exemplo, apenas um appliance do Unified Access Gatewayprecisar de um certificado.

Ao enviar uma solicitação de assinatura de certificado, forneça o nome de servidor que estará associado ao certificado. Certifique-se de que o appliance do Unified Access Gateway possa resolver o nome de servidor fornecido para que ele corresponda ao nome associado com o certificado.

### Nomes Alternativos da Entidade

Um Nome Alternativo da Entidade (Subject Alternative Name, SAN) é um atributo que pode ser adicionado a um certificado quando ele está sendo emitido. Você utiliza este atributo para adicionar nomes de entidade (URLs) a um certificado para que ele possa validar mais de um servidor

Por exemplo, três certificados podem ser emitidos para os appliances do Unified Access Gatewayque estejam atrás de um balanceador de carga: `ap1.exemplo.com`, `ap2.exemplo.com` e `ap3.exemplo.com`. Ao adicionar um Nome alternativo da entidade que representa o nome de host do balanceador de carga, como `horizon.exemplo.com` neste exemplo, o certificado é válido, pois será correspondente ao nome de host especificado pelo cliente.

Ao enviar uma solicitação de assinatura de certificado para um Certificado de CA (autoridade de certificação), forneça o endereço IP virtual (VIP) do balanceador de carga da interface externa como o nome em comum e o nome SAN. Certifique-se de que o appliance do Unified Access Gateway possa resolver o nome de servidor fornecido para que ele corresponda ao nome associado com o certificado.

O certificado é usado na porta 443.

### Certificado Curinga

Um certificado curinga é gerado para que possa ser utilizado para vários serviços. Por exemplo: `*.exemplo.com`.

Um curinga será útil se muitos servidores precisarem de um certificado. Se outros aplicativos no ambiente além dos appliances do Unified Access Gatewayprecisarem de certificados TLS/SSL, você também poderá utilizar um certificado curinga para estes servidores. No entanto, se você utilizar um certificado curinga que esteja compartilhado com outros serviços, a segurança do produtoVMware Horizontambém dependerá da segurança destes outros serviços.

---

**Observação** Você pode utilizar um certificado curinga somente em um nível único de domínio. Por exemplo, um certificado curinga com o nome de entidade `*.exemplo.com` pode ser utilizado para o subdomínio `dept.exemplo.com` mas não para `dept.it.exemplo.com`.

---

Os certificados importados para o appliance do Unified Access Gatewaydevem ser confiáveis para as máquinas clientes e também devem ser aplicáveis a todas as instâncias do Unified Access Gatewaye de qualquer balanceador de carga, utilizando curingas ou utilizando certificados de Nome Alternativo de Entidade (SAN).

## Converter arquivos de certificado para o formato PEM de uma linha

Para utilizar a API REST do Unified Access Gatewaypara configurar definições de certificado ou para utilizar os scripts do PowerShell, você deve converter o certificado em arquivos de formato PEM para a cadeia de certificados e a chave privada, e deve converter os arquivos `.pem` em um formato de uma linha que inclua caracteres newline integrados.

Ao configurar o Unified Access Gateway, há três tipos possíveis de tipos de certificados que talvez seja preciso converter.

- Você deve sempre instalar e configurar um certificado de servidor TLS/SSL para o appliance do Unified Access Gateway.
- Se planeja utilizar a autenticação com cartão inteligente, você deve instalar e configurar o certificado do emissor de CA confiável para o certificado que será colocado no cartão inteligente.
- Se planeja utilizar a autenticação com cartão inteligente, a VMware recomenda a instalação e configuração de um certificado raiz para o certificado de autoridade de certificação de assinatura do certificado de servidor SAML que está instalado no appliance do Unified Access Gateway.

Para todos estes tipos de certificados, realize o mesmo procedimento para converter o certificado para o arquivo de formato PEM que contém a cadeia de certificados. Para os certificados de servidor TSL/SSL e certificados raiz, também é possível converter cada arquivo para o arquivo PEM que contém a chave privada. Você deve converter cada arquivo `.pem` para um formato de uma linha que possa ser passado em uma cadeia de caracteres de JSON à API REST do Unified Access Gateway.

### Pré-requisitos

- Verifique se possui o arquivo do certificado. O arquivo pode estar no formato PKCS#12 (`.p12` ou `.pfx`) ou no formato Java JKS ou JCEKS.
- Familiarize-se com a ferramenta de linha de comando do `openssl` que você usará para converter o certificado. Consulte https://www.openssl.org/docs/apps/openssl.html.
- Se o certificado estiver no formato Java JKS ou JCEKS, familiarize-se com a ferramenta de linha de comando `keytool` do Java para converter o certificado primeiramente para o formato `.p12` ou `.pks` antes de convertê-lo para arquivos `.pem`.

### Procedimentos

1 Se seu certificado estiver no formato Java JKS ou JCEKS, utilize o `keytool` para converter o certificado para o formato `.p12` ou `.pks`.

**Importante** Utilize a mesma senha de origem e destino durante essa conversão.

2 Se seu certificado estiver no formato PKCS#12 (`.p12` ou `.pfx`) ou após o certificado ser convertido para o formato PKCS#12, utilize o `openssl` para converter o certificado para arquivos `.pem`.

Por exemplo, se o nome do certificado é `mycaservercert.pfx`, utilize os seguintes comandos para converter o certificado:

```
openssl pkcs12 –in mycaservercert.pfx –nokeys –out mycaservercert.pem
openssl pkcs12 –in mycaservercert.pfx –nodes –nocerts –out mycaservercertkey.pem
openssl rsa –in mycaservercertkey.pem –check –out mycaservercertkeyrsa.pem
```

3 Edite `mycaservercert.pem` e remova quaisquer entradas de certificado desnecessárias. Ele deve conter o certificado de servidor SSL seguido por quaisquer certificados de autoridade de certificação intermediários necessários e o certificado de autoridade de certificação raiz.

4 Utilize o seguinte comando UNIX para converter cada arquivo `.pem` para um valor que possa ser passado em uma cadeia de caracteres de JSON à API REST do Unified Access Gateway:

```
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' cert–name.pem
```

Neste exemplo, *`cert–name`*`.pem` é o nome do arquivo do certificado. O certificado parece semelhante a este exemplo.

**Figura 5-1.** Arquivo do certificado em uma única linha


O novo formato coloca todas as informações do certificado em uma única linha com caracteres integrados de nova linha. Se você possui um certificado intermediário, esse certificado deve também estar no formato de uma linha e adicionar-se ao primeiro certificado para que ambos os certificados estejam na mesma linha.

Você pode agora configurar certificados para o Unified Access Gatewayutilizando estes arquivos `.pem` com os scripts do PowerShell anexados à publicação do blog "Utilizando o PowerShell para Implementar o VMware Unified Access Gateway", disponível em https://communities.vmware.com/docs/DOC-30835. De forma alternativa, você pode criar e utilizar uma solicitação JSON para configurar o certificado.

### Próximo passo

Se você converteu um certificado de servidor TLS/SSL, consulte "Substituir o certificado padrão do servidor TLS/SSL pelo Unified Access Gateway", na página 56. Para certificados de cartão inteligente, consulte "Configurando a autenticação de certificado ou de cartão inteligente no appliance do Unified Access Gateway", na página 59.

## Substituir o certificado padrão do servidor TLS/SSL pelo Unified Access Gateway

Para armazenar um certificado de servidor TLS/SSL assinado pela CA confiável no appliance do Unified Access Gateway você deve converter o certificado para o formato correto e utilizar a IU do administrador ou os scripts do PowerShell para configurar o certificado.

Para ambientes de produção, a VMware recomenda enfaticamente a substituição do certificado padrão o mais rápido possível. O certificado padrão do servidor TLS/SSL que é gerado ao implementar um appliance do Unified Access Gatewaynão é assinado por uma Autoridade de Certificação Confiável.

**Importante** Utilize também este procedimento para a substituição periódica de um certificado que foi assinado por uma CA confiável antes da expiração do certificado, o que pode acontecer a cada dois anos.

Esse procedimento descreve como utilizar a API REST para substituir o certificado.

### Pré-requisitos

- A menos que já possua um certificado de servidor TLS/SSL válido e sua chave privada, obtenha um novo certificado assinado de uma Autoridade de Certificação. Ao gerar uma solicitação de assinatura de certificado (certificate signing request, CSR) para obter um certificado, certifique-se de que também seja gerada uma chave privada. Não gere certificados para servidores utilizando um valor KeyLength inferior a 1024.

  Para gerar o CSR, é preciso conhecer o nome de domínio totalmente qualificado (FQDN) que os dispositivos cliente utilizam para se conectar ao appliance do Unified Access Gatewaye a unidade organizacional, organização, cidade, estado e país para preencher o nome da Entidade.

- Converta o certificado para arquivos de formato PEM-e converta os arquivos `.pem` para o formato de uma linha. Consulte "Converter arquivos de certificado para o formato PEM de uma linha", na página 54.

### Procedimentos

1 Na seção Configurar manualmente a IU do administrador, clique em Selecionar.

2 Em Configurações avançadas > Configurações do certificado de servidor TLS, clique no ícone de engrenagem.

3 Clicar em **Selecionar** para a Chave privada e navegue até o arquivo da chave privada. Clique em **Abrir** para carregar o arquivo.

4 Clique em **Selecionar** para a Cadeia de certificados e navegue até o arquivo do certificado. Clique em **Abrir** para carregar o arquivo.

5 Clique em **Salvar**.

  Se o certificado for aceito, será exibida uma mensagem de sucesso.

### Próximo passo

Se a CA que assinou o certificado não tiver reputação renomada, configure clientes para confiar nos certificados raiz e intermediário.

## Alterar os protocolos de segurança e os conjuntos de codificação utilizados para a comunicação TLS ou SSL

Embora na maioria dos casos, as configurações padrão não precisem ser alteradas, você pode configurar protocolos de segurança e algoritmos de criptografia que são utilizados para codificar as comunicações entre clientes e o appliance doUnified Access Gateway.

A configuração padrão inclui conjuntos de criptografia que utilizam a Criptografia AES de 128 ou 256 bits, exceto para algoritmos DH anônimos e os classifica por força. Por padrão, o TLS v.1.1 e o TLS v1.2 estão ativados. O TLS v1.0 e o SSL v3.0 estão desabilitados.

### Pré-requisitos

- Familiarize-se com a API REST doUnified Access Gateway. A especificação para esta API está disponível na seguinte URL na máquina virtual onde o Unified Access Gateway está instalado: `https://access-point-appliance.exemplo.com:9443/rest/swagger.yaml`.

- Familiarize-se com as propriedades específicas para configurar os protocolos e conjuntos de criptografia: `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` e `tls12Enabled`.

### Procedimentos

1 Crie uma solicitação JSON para especificar os protocolos e conjuntos de criptografia a serem utilizados.

O exemplo a seguir possui as configurações padrão.

```
{
"cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

2 Utilize um cliente REST, como o `curl` ou o `postman`, para utilizar a solicitação JSON invocar a API REST do Unified Access Gateway e configurar os protocolos e conjuntos de criptografia.

No exemplo, *access-point-appliance.exemplo.com* é o nome de domínio totalmente qualificado do appliance do Unified Access Gateway .

```
curl –k –d @– –u 'admin' –H "Content–Type: application/json" –X PUT https://access–point–
appliance.exemplo.com:9443/rest/v1/config/system < ~/ciphers.json
```

*ciphers*.json é a solicitação JSON criada nada etapa anterior.

São utilizados os conjuntos e protocolos de criptografia que você especificou.

# Configuração da autenticação em DMZ 6

Ao implantar o Unified Access Gateway inicialmente, a autenticação da senha do Active Directory está definida como o padrão. Os usuários inserem o nome de usuário e a senha do Active Directory e essas credenciais são enviadas por um sistema de back-end para autenticação.

É possível configurar o serviço do Unified Access Gateway para realizar a autenticação de Certificado/Cartão Inteligente, autenticação do RSA SecurID, autenticação RADIUS e RSA Adaptive Authentication.

**Observação** A autenticação da senha com o Active Directory é o único método de autenticação que pode ser usado com uma implementação do AirWatch.

Este capítulo inclui os seguintes tópicos:



## Configurando a autenticação de certificado ou de cartão inteligente no appliance do Unified Access Gateway

É possível configurar a autenticação de certificado x509 no Unified Access Gateway para permitir que os clientes façam a autenticação com certificados em sua área de trabalho ou dispositivos móveis ou usem um adaptador de cartão inteligente para autenticação.

A autenticação com base no certificado é baseada no que o usuário tem (a chave privada ou o cartão inteligente) e no que a pessoa sabe (a senha para a chave privada ou o PIN do cartão inteligente). A autenticação de cartão inteligente fornece a autenticação de dois fatores verificando o que a pessoa possui (o cartão inteligente) e o que a pessoa sabe (o PIN). Os usuários finais podem utilizar os cartões inteligentes para efetuar logon em um sistema operacional de área de trabalho remota do View e para acessar aplicativos ativados por cartão inteligente, como um aplicativo de e-mail que utiliza o certificado para assinar e-mails e provar a identidade do remetente.

Com este recurso, a autenticação de certificado de cartão inteligente é realizada em oposição ao serviço do Unified Access Gateway. O Unified Access Gateway usa a asserção SAML para comunicar informações sobre o certificado X.509 de usuário final e o PIN do cartão inteligente ao servidor Horizon.

É possível configurar a verificação de revogação de certificado para evitar que os usuários com certificados de usuário revogados façam a autenticação. Os certificados são frequentemente revogados quando um usuário deixa uma organização, perde um cartão inteligente ou muda de um departamento para outro. Há suporte para a verificação de revogação de certificados com as listas de certificados revogados (certificate revocation lists, CRLs) e com o Protocolo de status de certificado on-line (Online Certificate Status Protocol, OCSP). Uma CRL é uma lista de certificados revogados publicados pela CA que emitiu os certificados. O OCSP é um protocolo de validação de certificado utilizado para obter o status de revogação de um certificado.

É possível definir ambos CRL e OCSP na mesma configuração do adaptador de autenticação de certificado. Ao configurar os dois tipos de verificação de revogação de certificado e a caixa de seleção Usar CRL em caso de falha do OCSP for habilitada, o OCSP será verificado primeiro e, se o OCSP falhar, a verificação de revogação fará fallback para a CRL. A revogação de verificação não utilizará o OCSP se a CRL falhar.

Você também pode configurar a autenticação, de modo que o Unified Access Gateway exija a autenticação do cartão inteligente, mas, então, a autenticação também passará pelo servidor, exigindo a autenticação do Active Directory.

**Observação** Para o VMware Identity Manager, a autenticação é sempre passada através do Unified Access Gateway ao serviço do VMware Identity Manager. Será possível configurar a autenticação do cartão inteligente para que seja realizada no appliance do Unified Access Gateway somente se o Unified Access Gateway estiver sendo utilizado com o Horizon 7.

## Configurar a autenticação de certificado no Unified Access Gateway

Você habilita e configura a autenticação de certificado a partir do console de administração do Unified Access Gateway.

### Pré-requisitos

- Obtenha o certificado raiz e os certificados intermediários da Autoridade de Certificação (Certificate Authority, CA) que assinou os certificados apresentados por seus usuários. Consulte "Obter Certificados de Autoridade de Certificação", na página 62
- Verifique se os metadados SAML do Unified Access Gateway estão adicionados no provedor de serviços e se os metadados SAML do provedor de serviço são copiados para o appliance do Unified Access Gateway.
- (Opcional) Lista de Identificadores de Objeto (Object Identifier, OID) das políticas de certificado válidas para a autenticação de certificado.
- Para a verificação de revogação, a localização do arquivo da CRL e a URL do servidor OCSP.
- (Opcional) Localização do arquivo de certificado de assinatura de resposta OCSP.
- Conteúdo do formulário de consentimento se aparecer um formulário de consentimento antes da autenticação.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do Certificado X.509.

4 Configure o formulário do Certificado X.509.

Um asterisco indica uma caixa de texto obrigatória. Todas as outras caixas de texto são opcionais.

| Opção | Descrição |
|---|---|
| **Ativar Certificado X.509** | Altere o NÃO para **SIM** para ativar a autenticação do certificado. |
| ***Nome** | Nomeie este método de autenticação. |
| ***Certificados de CA raiz e intermediária** | Clique em **Selecionar** para selecionar os arquivos de certificado a serem carregados. É possível selecionar vários certificados de CA intermediária e de CA raiz codificados como DER ou PEM. |
| **Tamanho do cache CRL** | Insira o tamanho do cache da lista de revogação de certificado. O padrão é 100. |
| **Ativar revogação de certificado** | Altere o NÃO para **SIM** para ativar a verificação de revogação de certificado. A verificação de revogação impede a autenticação dos usuários que têm certificados de usuário revogados. |
| **Usar CRL dos certificados** | Marque a caixa de seleção para usar a lista de revogação de certificados (certificate revocation list, CRL) publicada pela CA que emitiu os certificados para validar o status de um certificado revogado ou não revogado. |
| **Local da CRL** | Digite o caminho do arquivo do servidor ou o caminho do arquivo local a partir do qual recupera-se a CRL. |
| **Ativar a revogação do OCSP** | Marque a caixa de seleção para usar o protocolo de validação de certificado do Protocolo de status de certificado on-line (Online Certificate Status Protocol, OCSP) a fim de obter o status de revogação de um certificado. |
| **Usar a CRL em caso de falha do OCSP** | Se você configurar a CRL e o OCSP, poderá marcar esta caixa para fazer fallback ao uso da CRL se a verificação do OCSP não estiver disponível. |
| **Enviar nonce do OCSP** | Marque esta caixa de seleção se deseja que o identificador único da solicitação do OCSP seja enviado na resposta. |
| **URL do OCSP** | Se você ativou a revogação do OCSP, digite o endereço do servidor do OCSP para a verificação de revogação. |
| **Certificado de assinatura do respondente do OCSP** | Insira o caminho ao certificado OCSP para o respondente, */path/to/file.cer*. |
| **Ativar formulário de consentimento antes da autenticação** | Marque esta caixa de seleção para incluir uma página do formulário de consentimento que aparecerá antes de os usuários fazerem login no Workspace Portal ONE usando a autenticação de certificado. |
| **Conteúdo do formulário de consentimento** | Digite aqui o texto que será exibido no formulário de consentimento. |

5 Clique em **Salvar**.

### Próximo passo

Quando a autenticação do Certificado X.509 é definida e o appliance do Unified Access Gateway é configurado atrás de um balanceador de carga, certifique-se de que o Unified Access Gateway esteja configurado com uma passagem do SSL no balanceador de carga e não esteja configurado para encerrar o SSL no balanceador de carga. Essa configuração assegura que o handshake do SSL esteja entre o Unified Access Gateway e o cliente para passar o certificado ao Unified Access Gateway.

## Obter Certificados de Autoridade de Certificação

Você deve obter todos os certificados de CA (autoridade de certificação) para todos os certificados de usuários confiáveis nos cartões inteligentes apresentados por seus usuários e administradores. Esses certificados incluem certificados raiz e podem incluir certificados intermediários, se o certificado de cartão inteligente do usuário foi emitido por uma autoridade de certificado intermediária.

Se você não possui o certificado raiz ou intermediário da CA que assinou os certificados nos cartões inteligente apresentados por seus usuários e administradores, é possível exportar os certificados de um certificado de usuário assinado pela CA ou de um cartão inteligente que contenha um certificado assinado pela CA. Consulte "Obter o certificado de CA do Windows", na página 62.

### Procedimentos

- Obtenha os certificados CA de uma das seguintes origens.
  - Um servidor Microsoft IIS que esteja executando Serviços de Certificado da Microsoft. Consulte o site da Microsoft TechNet para obter informações sobre como instalar o Microsoft IIS, emitir certificados e distribuí-los em sua organização.
  - O certificado raiz público de uma CA confiável. Esta é a origem mais comum de um certificado raiz em ambientes que já possuem uma infraestrutura de cartão inteligente e uma abordagem padronizada para a distribuição e autenticação de cartões inteligentes.

### Próximo passo

Adicione o certificado raiz, certificado intermediário ou ambos a um arquivo confiável do servidor.

## Obter o certificado de CA do Windows

Se você possui um certificado de usuário assinado por uma autoridade de certificação ou um cartão inteligente que contém um certificado assinado por uma autoridade de certificação e o Windows confia no certificado raiz, é possível exportar o certificado raiz do Windows. Se o emissor do certificado de usuário é uma autoridade de certificação intermediária, é possível exportar este certificado.

### Procedimentos

1. Se um certificado de usuário está em um cartão inteligente, insira o cartão inteligente em um leitor para adicionar o certificado de usuário ao seu armazenamento pessoal.

   Se o certificado de usuário não aparecer em seu armazenamento pessoal, utilize o software de leitura para exportá-lo para um arquivo. Este arquivo é usado na Etapa 4 deste procedimento.
2. No Internet Explorer, selecione **Ferramentas > Opções de Internet**.
3. Na guia **Conteúdo**, clique em **Certificados**.
4. Na guia **Pessoal**, selecione o certificado que deseja utilizar e clique em **Visualizar**.

   Se o certificado de usuário não aparecer na lista, clique em **Importar** para importá-lo manualmente de um arquivo. Após o certificado ser importado, você pode selecioná-lo na lista.
5. Na guia **Caminho de Certificação**, selecione o certificado no topo da árvore e clique em **Visualizar Certificado**.

   Se o certificado de usuário estiver assinado como parte de uma hierarquia de confiança, o certificado assinado poderá ser assinado por outro certificado de nível superior. Selecione o certificado de parente (aquele que assinou o certificado de usuário) como seu certificado raiz. Em alguns casos, o emissor pode ser uma autoridade de certificação intermediária.
6. Na guia **Detalhes**, clique em **Copiar para Arquivo**.

   O Assistente de Exportação de Certificado aparece.

7 Clique em **Avançar > Avançar** e digite um nome e localização para o arquivo que deseja exportar.

8 Clique em **Avançar** para salvar o arquivo como um certificado raiz em um local especificado.

### Próximo passo

Adicione o certificado CA a um arquivo confiável do servidor.

## Configurar a autenticação do RSA SecurID no Unified Access Gateway

Após a configuração do appliance do Unified Access Gateway como o agente de autenticação no servidor RSA SecurID, é necessário adicionar as informações de configuração do RSA SecurID no appliance do Unified Access Gateway.

### Pré-requisitos

- Verifique se o Gerenciador da Autenticação RSA (o servidor RSA SecurID) está instalado e adequadamente configurado.
- Faça o download do arquivo compactado sdconf.rec a partir do servidor RSA SecurID e extraia o arquivo de configuração do servidor.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do RSA SecurID.

4 Configure a página do RSA SecurID.

As informações usadas e os arquivos gerados no servidor do RSA SecurID são necessários ao configurar a página do SecurID.

| Opção | Ação |
|---|---|
| Ativar RSA SecurID | Altere o NÃO para **SIM** para ativar a autenticação do SecurID. |
| *Nome | O nome é securid-auth. |
| *Número de iterações | Insira o número de tentativas de autenticação permitidas. Este é o número máximo de tentativas de login com falha ao usar o token do RSA SecurID. O padrão é de 5 tentativas.<br>**Observação** Quando mais de um diretório é configurado e você implementa a autenticação do RSA SecurID com diretórios adicionais, configure o **Número de tentativas de autenticação permitidas** com o mesmo valor para cada configuração do RSA SecurID. Se o valor não for o mesmo, haverá falha na autenticação do SecurID. |
| *Nome do HOST externo | Digite o endereço IP da instância do Unified Access Gateway. O valor inserido deve corresponder ao valor usado quando você adicionou o appliance do Unified Access Gateway como um agente de autenticação ao servidor do RSA SecurID. |
| *Nome do HOST interno | Digite o valor atribuído ao prompt do **Endereço IP** no servidor do RSA SecurID. |
| *Configuração do servidor | Clique em Alterar para carregar o arquivo de configuração do servidor do RSA SecurID. Primeiro, você deve baixar o arquivo compactado do servidor do RSA SecurID e extrair o arquivo de configuração do servidor, que, por padrão, é denominado `sdconf.rec`. |
| *Sufixo da ID do nome | Insira o nameId que permite que o View forneça a experiência TrueSSO. |

# Configuração do RADIUS para o Unified Access Gateway

É possível configurar o Unified Access Gateway para que os usuários sejam obrigados a usar a autenticação RADIUS. Você configura as informações do servidor RADIUS no appliance do Unified Access Gateway.

O suporte do RADIUS oferece uma ampla gama de opções de autenticação alternativa de dois fatores baseada em token. Como soluções de autenticação de dois fatores, como o RADIUS, trabalham com gerenciadores de autenticação instalados em servidores separados, é necessário ter o servidor RADIUS configurado e acessível ao serviço do gerenciador de identidade

Quando os usuários fazem o login e a autenticação RADIUS é habilitada, uma caixa de diálogo de login especial aparece no navegador. Os usuários inserem seu nome de usuário e senha da autenticação RADIUS na caixa de diálogo de login. Se o servidor RADIUS emitir um desafio de acesso, o Unified Access Gateway exibirá uma caixa de diálogo solicitando uma segunda senha. Atualmente, o suporte para desafios do RADIUS é limitado à solicitação para inserção de texto.

Após os usuários inserirem as credenciais na caixa de diálogo, o servidor RADIUS pode enviar uma mensagem de texto SMS ou e-mail ou texto utilizando algum outro mecanismo de banda externa ao telefone celular do usuário com um código. O usuário pode inserir este texto e código na caixa de diálogo de login para concluir a autenticação.

Se o servidor RADIUS fornecer a habilidade de importar usuários do Active Directory, os usuários finais poderão primeiramente ser solicitados a fornecer as credenciais do Active Directory antes da solicitação do nome de usuário e senha de autenticação RADIUS.

## Configurar a autenticação RADIUS

No appliance do Unified Access Gateway, deve-se ativar a autenticação RADIUS, inserir as definições de configuração do servidor RADIUS e alterar o tipo de autenticação para a autenticação RADIUS.

### Pré-requisitos

- Verifique se o servidor a ser utilizado como o servidor do gerenciador da autenticação possui o software RADIUS instalado e configurado. Defina o servidor RADIUS e, em seguida, configure as solicitações do RADIUS a partir do Unified Access Gateway. Consulte as guias de configuração do fornecedor do RADIUS para obter mais informações sobre como configurar o servidor RADIUS.

São necessárias as seguintes informações do servidor RADIUS.

- Endereço IP ou nome DNS do servidor RADIUS.
- Números das portas de autenticação. A porta de autenticação é normalmente 1812.
- Tipo de autenticação. Os tipos de autenticação incluem PAP, Password Authentication Protocol (Protocolo de autenticação de senha), CHAP, Challenge Handshake Authentication Protocol (Protocolo de autenticação por desafios de identidade), MSCHAP1, MSCHAP2, Microsoft Challenge Handshake Authentication Protocol versões 1 e 2 (Protocolo de autenticação por desafios de identidade).
- Segredo compartilhado do RADIUS utilizado para criptografia e descriptografia nas mensagens do protocolo do RADIUS.
- Tempo limite específico e valores de novas tentativas necessários para a autenticação RADIUS

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Nas Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do RADIUS.

| Opção | Ação |
|---|---|
| Ativar RADIUS | Altere o NÃO para **SIM** para ativar a autenticação RADIUS. |
| Nome* | O nome é radius-auth |
| Tipo de autenticação* | Insira o protocolo de autenticação suportado pelo servidor RADIUS. PAP, CHAP, MSCHAP1 OU MSCHAP2. |
| Segredo compartilhado* | Insira o segredo compartilhado do RADIUS. |
| Número de tentativas de Autenticação permitidas * | Digite o número máximo de tentativas de login falhas ao usar o RADIUS para fazer o login. O padrão é de três tentativas. |
| Número de tentativas para o servidor RADIUS* | Insira o número total de novas tentativas. Se o servidor primário não responder, o serviço aguardará o tempo configurado antes de tentar novamente. |
| Tempo limite do servidor em segundos* | Insira o tempo limite do servidor RADIUS em segundos. Depois disso, uma nova tentativa será enviada se o servidor RADIUS não responder. |
| Nome do host do servidor Radius * | Insira o nome do host ou o endereço IP do servidor RADIUS. |
| Porta de autenticação* | Insira o número da porta de autenticação do Radius. A porta é normalmente 1812. |
| Prefixo de território | (Opcional) A localização da conta do usuário é chamada território.<br>Se você especificar uma cadeia de prefixo de território, a cadeia de caracteres será colocada no começo do nome de usuário quando o nome for enviado ao servidor RADIUS. Por exemplo, se o nome de usuário for inserido como jdoe e o prefixo de território DOMAIN-A\ for especificado, o nome de usuário DOMAIN-A\jdoe será enviado ao servidor RADIUS. Se você não configurar esses campos, somente o nome de usuário inserido será enviado. |
| Sufixo de território | (Opcional) Se você configurar um sufixo de território, a cadeia de caracteres será colocada no final do nome de usuário. Por exemplo, se o sufixo for @myco.com, o nome de usuário jdoe@myco.com será enviado ao servidor RADIUS. |
| Sufixo da ID do nome | Insira o nameId que permite que o View forneça a experiência True SSO. |
| Dica de senha da página de logon | Insira a cadeia de caracteres de texto a ser exibida na mensagem na página de logon do usuário para direcioná-los a inserir a senha Radius correta. Por exemplo, se este campo estivesse configurado com a **senha AD primeiro e, em seguida, a senha SMS**, a mensagem da página de logon seria **Insira sua senha AD primeiro e, em seguida, a senha SMS.** A cadeia de caracteres de texto padrão é **Senha RADIUS**. |
| Ativar servidor secundário | Altere o NÃO para **SIM** para configurar um servidor RADIUS secundário para alta disponibilidade. Configure as informações de servidor secundário conforme descrito na etapa 3. |

4 Clique em **Salvar**.

# Configurar o RSA Adaptive Authentication no Unified Access Gateway

O RSA Adaptive Authentication pode ser implementado para fornecer uma autenticação multifator mais forte do que apenas a autenticação de nome de usuário e senha em relação ao Active Directory. O Adaptive Authentication monitora e autentica as tentativas de login do usuário com base em níveis e políticas de risco.

Quando a Adaptive Authentication está habilitada, os indicadores de risco especificados nas políticas de risco estabelecidas no aplicativo de Gerenciamento da Política da RSA e na configuração do Unified Access Gateway da autenticação adaptativa são usados para determinar se um usuário é autenticado com o nome de usuário e a senha ou se são necessárias informações adicionais para autenticar o usuário.

## Métodos de autenticação do RSA Adaptive Authentication suportados

Os métodos de autenticação forte do RSA Adaptive Authentication suportados no Unified Access Gateway são a autenticação de banda externa via telefone, e-mail ou mensagem de texto SMS e perguntas de desafio. Você habilita no serviço os métodos do RSA Adaptive Authentication que podem ser fornecidos. As políticas do RSA Adaptive Authentication determinam o método de autenticação secundário a ser usado.

A autenticação de banda externa é um processo que exige o envio de verificação adicional em conjunto com o nome de usuário e senha. Quando os usuários se inscrevem no servidor do RSA Adaptive Authentication, fornecem um endereço de e-mail, um número de telefone ou ambos, dependendo da configuração do servidor. Se for necessária alguma verificação adicional, o servidor de autenticação adaptativa da RSA enviará um código de acesso de uso único por meio do canal fornecido. Os usuários digitam esse código de acesso junto com o nome de usuário e a senha.

As perguntas de desafio exigem que o usuário responda a uma série de perguntas quando se inscreve no servidor do RSA Adaptive Authentication. É possível configurar quantas perguntas de inscrição serão feitas e quantas perguntas de desafio serão apresentadas na página de login.

## Inscrevendo usuários no servidor do RSA Adaptive Authentication

Os usuários devem ser provisionados no banco de dados do RSA Adaptive Authentication para utilizar a autenticação adaptativa para autenticação. Os usuários serão adicionados ao banco de dados do RSA Adaptive Authentication quando fizerem o login pela primeira vez com seu nome de usuário e senha. Dependendo de como você configurou o RSA Adaptive Authentication no serviço, quando os usuários fazem o login, podem ser solicitados a fornecer o endereço de e-mail, o número de telefone e o número do serviço de envio de mensagens (SMS) deles ou podem ser solicitados a configurar respostas para as perguntas de desafio.

**Observação** O RSA Adaptive Authentication não permite caracteres internacionais nos nomes de usuário. Se você pretende permitir caracteres de vários bytes nos nomes de usuário, entre em contato com o suporte da RSA para configurar o RSA Adaptive Authentication e o RSA Authentication Manager.

## Configurar o RSA Adaptive Authentication no Unified Access Gateway

Para configurar o RSA Adaptive Authentication no serviço, habilite o RSA Adaptive Authentication, selecione os métodos de autenticação adaptativa a serem aplicados e adicione as informações de conexão do Active Directory e o certificado.

### Pré-requisitos

- RSA Adaptive Authentication configurado corretamente com os métodos de autenticação a serem usados para autenticação secundária.

- Detalhes sobre o endereço de endpoint do SOAP e o nome de usuário do SOAP.
- Informações de configuração do Active Directory e certificado SSL disponível do Active Directory.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Gerais > Configurações de Autenticação, clique em **Mostrar**.

3 Clique na engrenagem na linha do RSA Adaptive Authentication.

4 Selecione as configurações apropriadas para o seu ambiente.

**Observação** Um asterisco indica um campo obrigatório. Os outros campos são opcionais.

| Opção | Descrição |
|---|---|
| **Habilitar o RSA AA Adapter** | Altere o NÃO para **SIM** para ativar o RSA Adaptive Authentication. |
| **Nome*** | O nome é rsaaa-auth. |
| **Endpoint do SOAP*** | Insira o endereço do endpoint do SOAP para integração entre o adaptador do RSA Adaptive Authentication e o serviço. |
| **Nome do usuário do SOAP*** | Insira o nome de usuário e a senha utilizados para assinar mensagens do SOAP. |
| **Senha do SOAP*** | Insira a senha da SOAP API do RSA Adaptive Authentication. |
| **Domínio RSA** | Insira o endereço de domínio do servidor Adaptive Authentication. |
| **Habilitar e-mail para OOB** | Selecione SIM para habilitar a autenticação de banda externa que envia uma senha única ao usuário final por uma mensagem de e-mail. |
| **Habilitar SMS para OOB** | Selecione SIM para habilitar a autenticação de banda externa que envia uma senha única ao usuário final por uma mensagem de texto SMS. |
| **Ativar o SecurID** | Selecione SIM para ativar o SecurID. Os usuários são solicitados a inserir seu token e senha RSA. |
| **Habilitar pergunta secreta** | Selecione SIM se você estiver usando as perguntas de inscrição e de desafio para autenticação. |
| **Número de perguntas de inscrição*** | Insira o número de perguntas que o usuário precisará configurar ao se inscrever no servidor Authentication Adapter. |
| **Número de perguntas de desafio*** | Insira o número de perguntas de desafio que os usuários devem responder corretamente ao fazer login. |
| **Número de tentativas de autenticação permitidas*** | Insira o número de vezes para exibir as perguntas de desafio a um usuário que tenta fazer login antes que a autenticação falhe. |
| **Tipo de diretório*** | O único diretório suportado é o Active Directory. |
| **Usar SSL** | Selecione SIM se utilizar o SSL para sua conexão de diretório. Você adiciona o certificado SSL do Active Directory no campo Certificado de Diretório. |
| **Host do servidor*** | Insira o nome do host do Active Directory. |
| **Porta do servidor** | Insira o número da porta do Active Directory. |
| **Usar localização do serviço DNS** | Marque SIM se a localização do serviço DNS for usada para conexão de diretório. |
| **DN Base** | Insira o DN do qual se deseja iniciar as pesquisas de conta. Por exemplo, OU=myUnit,DC=myCorp,DC=com. |
| **Vincular DN*** | Insira a conta que pode procurar usuários. Por exemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com |
| **Senha de associação** | Insira a senha para a conta de DN de associação. |
| **Atributo de pesquisa** | Insira o atributo de conta que contém o nome de usuário. |

| Opção | Descrição |
|---|---|
| **Certificado do diretório** | Para estabelecer conexões SSL seguras, adicione o certificado do servidor de diretório à caixa de texto. No caso de vários servidores, adicione o certificado raiz da autoridade de certificação. |
| **Usar STARTTLS** | Altere o NÃO para **SIM** para usar STARTTLS. |

5 Clique em **Salvar**.

# Gerar metadados SAML do Unified Access Gateway

Você deve gerar os metadados SAML no appliance do Unified Access Gateway e trocar metadados com o servidor para estabelecer a confiança mútua necessária para a autenticação de cartão inteligente.

A Security Assertion Markup Language (SAML) é um padrão baseado em XML que é utilizado para descrever e trocar informações de autenticação e autorização entre domínios de segurança diferentes. SAML passa informações sobre usuários entre fornecedores de identidade e fornecedores de serviço em documento chamados de asserções SAML. Neste cenário, o Unified Access Gateway é o fornecedor de identidade e o servidor no provedor de serviços.

### Pré-requisitos

- Configure o relógio (UTC) no appliance doUnified Access Gatewaypara que ele esteja com a hora correta. Por exemplo, abra uma janela de console na máquina virtual do Unified Access Gateway e utilize os botões de seta para selecionar o fuso horário correto. Verifique também se o horário do host ESXi está sincronizado com um servidor NTP. Verifique se as VMware Tools, executadas na máquina virtual do appliance, sincronizam o horário na máquina virtual com o horário no host ESXi.

  **Importante** Se o relógio do appliance do Unified Access Gateway não corresponder ao relógio do host do servidor, a autenticação de cartão inteligente poderá não funcionar.

- Obtenha um certificado de autenticação SAML que possa utilizar para assinar os metadados do Unified Access Gateway.

  **Observação** A VMware recomenda a criação e utilização de um certificado de autenticação SAML específico quando há mais de um appliance doUnified Access Gatewayem sua configuração. Neste caso, todos os appliances devem estar configurados com o mesmo certificado de autenticação para que o servidor possa aceitar as asserções de qualquer um dos appliances do Unified Access Gateway. Com um certificado de autenticação SAML específico, os metadados SAML de todos os appliances são os mesmos.

- Se você ainda não o fez, converta o certificado de autenticação SAML para arquivos de formato PEM e converta os arquivos `.pem` para o formato de uma linha. Consulte "Converter arquivos de certificado para o formato PEM de uma linha", na página 54.

### Procedimentos

1 Na seção Configurar Manualmente a IU do administrador, clique em **Selecionar**.

2 Na seção Configurações Avançadas, clique no ícone de engrenagem **Configurações do Provedor de Identidade SAML**.

3 Selecione a caixa de seleção **Fornecer Certificado**.

4 Para adicionar um arquivo de Chave privada, clique em **Selecionar** e navegue até o arquivo da chave privada para o certificado.

5 Para adicionar o arquivo de Cadeia de certificados, clique em **Selecionar** e navegue até o arquivo da cadeia de certificados.

6 Clique em **Salvar**.

7 Na caixa de texto Nome do Host, insira o nome do host e faça o download das configurações do provedor de identidade.

## Criando um autenticador SAML utilizado por outros provedores de serviço

Após gerar os metadados SAML no appliance do Unified Access Gateway, você pode copiar estes dados para o provedor de serviços de back-end. Copiar estes dados no provedor de serviços é parte do processo de criação de um autenticador SAML para que o Unified Access Gatewaypossa ser utilizado como um fornecedor de identidade.

Para um servidor Horizon Cloud, consulte a documentação do produto para obter instruções específicas.

## Copiar metadados SAML do provedor de serviços para o Unified Access Gateway

Após criar e ativar o autenticador SAML para que o Unified Access Gatewaypossa ser utilizado como um fornecedor de identidade, você pode gerar metadados SAML nesse sistema de back-end e utilizar os metadados para criar um provedor de serviços no appliance do Unified Access Gateway. Esta troca de dados estabelece confiança entre o fornecedor de identidade (Unified Access Gateway) e o provedor de serviços de back-end, como o Servidor de Conexão do View.

### Pré-requisitos

Verifique se você criou um autenticador SAML para o Unified Access Gateway no servidor do provedor de serviços de back-end.

### Procedimentos

1 Recupere os metadados SAML do provedor de serviços, que estão geralmente na forma de um arquivo XML.

Para obter instruções, consulte a documentação para o provedor de serviços.

Provedores de serviços diferentes têm procedimentos diferentes. Por exemplo, você deve abrir um navegador e digitar uma URL, como: https://*connection-server.example.com*/SAML/metadata/sp.xml

Você pode então utilizar um comando **Salvar como** para salvar a página da Web em um arquivo XML. O conteúdo deste arquivo começa com o seguinte texto:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

2 Na seção Configurar Manualmente a IU do administrador do Unified Access Gateway, clique em **Selecionar**.

3 Na seção Configurações Avançadas, clique no ícone de engrenagem **Configurações do Provedor do Servidor SAML**.

4 Na caixa de texto Nome do Provedor de Serviços, insira o nome do provedor de serviços.

5 Na caixa de texto XML de Metadados, cole o arquivo de metadados criado na etapa 1.

6 Clique em **Salvar**.

O Unified Access Gatewaye o provedor de serviços podem agora trocar informações de autenticação e autorização.

# Implantação da resolução de problemas do Unified Access Gateway

7

Você pode usar vários procedimentos para diagnosticar e corrigir problemas encontrados durante a implantação do Unified Access Gateway em seu ambiente.

Você pode usar os procedimentos de resolução de problemas para investigar as causas de tais problemas e tentar corrigi-los sozinho, ou você pode obter assistência do Suporte Técnico da VMware.

Este capítulo inclui os seguintes tópicos:



## Monitoramento da integridade dos serviços implantados

É possível observar rapidamente que os serviços implantados estão configurados e operando com sucesso a partir da IU do administrador para as configurações de borda.

**Figura 7-1.** Verificação de integridade


É exibido um círculo antes do serviço. O código de cores é o seguinte:

- Um círculo em branco significa que a definição não está configurada.
- Um círculo vermelho significa que o serviço está inoperante.
- Um círculo âmbar significa que o serviço funciona parcialmente.
- Um círculo verde significa que o serviço funciona sem nenhum problema.

# Resolução de erros de implementação

Talvez você enfrente dificuldades ao implantar o Unified Access Gateway em seu ambiente. Você pode usar vários procedimentos para diagnosticar e corrigir problemas da sua implementação.

## Aviso de segurança ao executar scripts baixados da Internet

Verifique se o script do PowerShell é o script que você deseja executar e, em seguida, no console do PowerShell, execute o seguinte comando:

```
unblock-file .\apdeploy.ps1
```

## comando ovftool não encontrado

Verifique se você instalou o software OVF Tool no Windows e se ele está instalado no local esperado pelo script.

## Rede inválida na netmask1 da propriedade

- A mensagem pode indicar netmask0, netmask1 ou netmask2. Verifique se o valor foi definido no arquivo .INI para cada uma das três redes, como netInternet, netManagementNetwork e netBackendNetwork.
- Verifique se um Perfil do Protocolo de Rede do vSphere foi associado a cada nome de rede de referência. Isso especifica as configurações de rede, como máscara de sub-rede IPv4, gateway e assim por diante. Verifique se o Perfil do Protocolo de Rede associado tem valores corretos para cada uma das configurações.

## Mensagem de aviso sobre o identificador do sistema operacional não compatível

A mensagem de aviso exibe se o identificador do sistema operacional especificado SUSE Linux Enterprise Server 12.0 64-bit (id:85) não é compatível com o host selecionado. Ele é mapeado com o seguinte identificador de SO: Outro Linux (64-bit).

Ignore esta mensagem de aviso. Ele é mapeado automaticamente para um sistema operacional compatível.

## Configurar a autenticação do RSA SecurID do Unified Access Gateway

Adicione as seguintes linhas à seção do Horizon do arquivo .INI.

```
authMethods=securid-auth && sp-auth
matchWindowsUserName=true
```

Adicione uma nova seção no final do seu arquivo .INI.

```
[SecurIDAuth]
serverConfigFile=C:\temp\sdconf.rec
externalHostName=192.168.0.90
internalHostName=192.168.0.90
```

Os endereços IP devem ser configurados com o endereço IP do Unified Access Gateway. O arquivo sdconf.rec é obtido a partir de um Gerenciador de Autenticações RSA que deve estar totalmente configurado. Verifique se você está usando o Access Point 2.5 ou uma versão mais recente e se o servidor do Gerenciador de Autenticações RSA é acessível na rede do Access Point. Execute novamente o comando de implementação do Powershell para implementar novamente seu Access Point configurado para RSA SecurID.

### O localizador não se refere a um erro de objeto

O erro notifica se o valor de destino que é usado pelo vSphere OVF Tool não está correto para o seu ambiente vCenter. Use a tabela listada em https://communities.vmware.com/docs/DOC-30835 para ver exemplos de formato de destino usado para consultar um host ou cluster do vCenter. O objeto de nível superior é especificado a seguir:

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

O objeto agora lista os nomes possíveis a serem usados no próximo nível.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

Os nomes da pasta, nomes do host e nomes do cluster usados no destino diferenciam letras maiúsculas e minúsculas.

## Coletando logs do appliance do Unified Access Gateway

Baixe o arquivo AP-Log Archieve.zip das configurações de suporte da IU do administrador. O arquivo ZIP contém todos os logs do appliance do Unified Access Gateway.

### Configurar o nível de log

É possível gerenciar as configurações de nível de log na IU do administrador. Vá para a página Configurações de suporte e selecione Configurações de nível de log. Os níveis de log que podem ser gerados são INFORMAÇÕES, AVISO, ERRO e DEPURAÇÃO. O nível de log é configurado por padrão como INFORMAÇÕES.

Segue seguir uma descrição do tipo de informações que os níveis de log coletam.

**Tabela 7-1.** Níveis de log

| Nível | Tipo de informações coletadas |
|---|---|
| INFORMAÇÕES | O nível INFORMAÇÕES indica as mensagens informativas que destacam o andamento do serviço. |
| ERRO | O nível ERRO indica eventos de erro que ainda podem permitir que o serviço continue sendo executado. |
| AVISO | O nível AVISO indica situações potencialmente perigosas, mas normalmente recuperáveis ou que podem ser ignoradas. |
| DEPURAÇÃO | Eventos que geralmente seriam úteis para a depuração de problemas. Você pode habilitar o modo de depuração para visualizar ou manipular o estado interno do appliance. O modo de depuração permite testar o cenário de implantação no seu ambiente. |

### Coletar logs

Baixe os arquivos ZIP de log da seção de configurações de suporte da IU do administrador.

Estes arquivos de registro são coletados do diretório `/opt/vmware/gateway/logs` no appliance.

As tabelas a seguir contêm descrições dos vários arquivos inclusos no arquivo ZIP.

**Tabela 7-2.** Arquivos que contêm informações de sistema para auxiliar na resolução de problemas

| Nome do Arquivo | Descrição |
|---|---|
| `df.log` | Contém informações sobre a utilização do espaço em disco. |
| `netstat.log` | Contém informações sobre conexões de rede. |
| `ap_config.json` | Contém as definições de configurações atuais para o appliance do Unified Access Gateway>. |
| `ps.log` | Inclui a lista de processos. |
| `ifconfig.log` | Contém informações sobre interfaces de rede. |
| `free.log` | Contém informações sobre a utilização da memória. |

**Tabela 7-3.** Arquivos de Registro para o Unified Access Gateway

| Nome do Arquivo | Descrição |
|---|---|
| `esmanager.log` | Contém mensagens de registro do processo do Edge Service Manager, que escuta as portas 443 e 80. |
| `authbroker.log` | Contém mensagens de registros do processo AuthBroker, que manipula adaptadores de autenticação. |
| `admin.log` | Contém mensagens de registros do processo que fornece a API REST do Unified Access Gateway na porta 9443. |
| `admin-zookeeper.log` | Contém mensagens de registros relacionadas à camada de dados que é utilizada para armazenar as informações de configuração do Unified Access Gateway . |
| `tunnel.log` | Contém mensagens de registros do processo de túnel que é utilizado como parte do processamento da XML API. |
| `bsg.log` | Contém mensagens de registro do Gateway Seguro Blast. |
| `SecurityGateway_*.log` | Contém mensagens de registro do Gateway Seguro PCoIP. |

Os arquivos de registro que terminam em "-std-out.log"`-std-out.log`" contêm informações escritas para o `stdout` de vários processos e são normalmente arquivos vazios.

Arquivos de log do Unified Access Gateway para o AirWatch

- `/var/log/airwatch/tunnel/vpnd`

  O tunnel-init.log e o tunnel.log são capturados neste diretório.

- `/var/log.airwatch/proxy`

  O proxy.log é capturado neste diretório.

- `/var/log/airwatch/appliance-agent`

  O appliance-agent.log é capturado neste diretório.

# Índice