Dell EMC PowerStore

Guia de configuração de segurança

1.x

July 2020
Rev. A02

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

CUIDADO: um AVISO indica possíveis danos ao hardware ou a possibilidade de perda de dados e informa como evitar o problema.

ATENÇÃO: uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

Índice

Prefácio

Como parte de um esforço contínuo de melhorias, lançamos periodicamente revisões de seu software e hardware. Algumas das funções descritas neste documento não são compatíveis com todas as versões de software ou hardware usadas no momento. As notas da versão do produto contêm as informações mais recentes sobre os recursos do produto. Entre em contato com um profissional de suporte técnico se um produto não funcionar adequadamente ou conforme descrito neste documento.

Onde obter ajuda

As informações sobre licenciamento, suporte e produtos EMC podem ser obtidas da seguinte maneira:

- **Informações sobre produtos**

  Para obter a documentação do produto e de recursos ou as notas da versão, vá para a página de documentação do PowerStore em www.dell.com/powerstoredocs.

- **Solução de problemas**

  Para obter informações sobre produtos, atualizações de software, licenciamento e serviços, acesse www.dell.com/support e localize a página de suporte ao produto apropriada.

- **Suporte técnico**

  Para suporte técnico e chamados, acesse www.dell.com/support e localize a página **Service Requests**. Para abrir um chamado, você deve ter um contrato de suporte válido. Entre em contato com o representante de vendas para saber como obter um contrato de suporte válido ou para tirar dúvidas sobre sua conta.

1

Autenticação e acesso

Este tópico contém as seguintes informações:

Tópicos:

Autenticando e gerenciando contas, funções e privilégios de usuário

A autenticação para acesso ao cluster é realizada com base nas credenciais de uma conta de usuário. As contas de usuário são criadas e posteriormente gerenciadas na página **Users**, que pode ser acessada no PowerStore Manager por meio de **Settings** > **Users** > **Users**. As autorizações aplicáveis dependem da função associada à conta de usuário. Quando o usuário especifica o endereço de rede do cluster como URL em um navegador da Web, é exibida uma página de log-in na qual ele pode fazer a autenticação como usuário local. As credenciais fornecidas pelo usuário serão autenticadas e, após a autenticação bem-sucedida, uma sessão será criada no sistema. Posteriormente, o usuário poderá monitorar e gerenciar o cluster nos recursos da função atribuída a ele.

O cluster autentica os usuários validando nomes de usuário e senhas por meio de uma conexão segura com o servidor de gerenciamento.

Gerenciamento padrão de fábrica

O equipamento vem com configurações de conta de usuário padrão de fábrica para serem usadas no acesso e na configuração.

NOTA: Com versões 1.0.x, é recomendável que você configure inicialmente o PowerStore usando a interface do usuário do PowerStore Manager em vez de usar interfaces de scripts de serviço, da CLI e da API. Isso garantirá que todas as senhas padrão sejam alteradas.

Tipo de conta	Nome de usuário	Senha	Privilégios
Gerenciamento de sistemas	admin	Password123#	Privilégios de administrador para redefinir senhas padrão, definir as configurações do equipamento e gerenciar contas de usuário.
Serviço	service	service	Para realizar operações de serviço. **NOTA:** O usuário de serviço existe para acesso de shell seguro (SSH, Secure Shell). No entanto, não é possível fazer log-in no PowerStore Manager usando o usuário de serviço.

Regras de sessão

As sessões no cluster têm as seguintes características:

- Período de expiração de uma hora.

  NOTA: O usuário é desconectado automaticamente do cluster após uma hora de inatividade da sessão.
- O tempo limite da sessão não pode ser configurado.

Uso de nome de usuário e senha

Os nomes de usuário das contas do sistema devem atender aos seguintes requisitos:

Restrição	Requisito de nome de usuário
Estrutura	Deve iniciar e terminar com um caractere alfanumérico.
Uso de maiúsculas e minúsculas	Os nomes de usuário não diferenciam maiúsculas de minúsculas
Número mínimo de caracteres alfanuméricos	1
Número máximo de caracteres alfanuméricos	64
Caracteres especiais aceitos	. (ponto)

As senhas das contas do sistema devem atender aos seguintes requisitos:

Restrição	Requisitos de senha
Número mínimo de caracteres	8
Número mínimo de caracteres maiúsculos	1
Número mínimo de caracteres minúsculos	1
Número mínimo de caracteres numéricos	1
Número mínimo de caracteres especiais ● Caracteres compatíveis: ! @ # $ % ^ * _ ~ ? **NOTA:** A senha não pode conter aspas simples ('), e comercial (&) ou caracteres de espaço.	1
Número máximo de caracteres	40

NOTA: As últimas cinco senhas não podem ser reutilizadas. Uma senha anterior pode ser reutilizada após a quinta vez em sequência.

Senhas do ESXi

A senha raiz padrão do ESXi em um equipamento PowerStore X model está no seguinte formato: ***<Service_Tag>*_123!**, em que *<Service_Tag>* é a etiqueta de serviço de sete caracteres da Dell relativa ao equipamento.

Não altere a senha padrão do ESXi enquanto a configuração inicial em cluster não estiver concluída. Para obter mais informações sobre como alterar uma senha do ESXi, consulte a documentação do VMware ESXi.

CUIDADO: Você não pode perder a senha do ESXi. Se o ESXi ficar inativo e você não tiver a senha, será preciso reinicializar o equipamento. Esse comportamento é normal no ESXi, embora a reinicialização por causa de uma senha perdida possa resultar em perda de dados.

CUIDADO: A senha padrão do ESXi é configurada de forma exclusiva para cada equipamento PowerStore X model. A senha é usada para autenticar com o host do ESXi quando os nós no equipamento são adicionados a um cluster do vCenter. Se você alterar a senha padrão antes que o cluster esteja totalmente configurado, será necessário reinicializar o equipamento.

Funções e privilégios

Os controles de acesso baseado em função permitem que os usuários tenham diferentes privilégios. Isso oferece um meio de separar as funções de administração para um melhor alinhamento com os conjuntos de habilidades e responsabilidades.

O sistema é compatível com as seguintes funções e privilégios:

NOTA: Uma ✓ em uma caixa denota um privilégio compatível com essa função, enquanto uma caixa em branco indica que o privilégio não é compatível com a função.

Tarefa	Operador	Administrador de VM	Administrador de segurança	Administrador de armazenamento	Administrador
Alterar a senha local do sistema	✓	✓	✓	✓	✓
Visualizar configurações do sistema, o status e informações de desempenho	✓		✓	✓	✓
Modificar configurações de sistema					✓
Criar, modificar, excluir recursos e políticas de proteção e habilitar/desabilitar SSH				✓	✓
Conectar-se ao vCenter		✓		✓	✓
Visualizar uma lista de contas locais			✓		✓
Adicionar, excluir ou modificar uma conta local			✓		✓
Visualizar informações de armazenamento do sistema por meio de um vCenter Server conectado ao provedor de VASA do sistema e registrar/registrar novamente o certificado da CA/autoridade de certificação VMware (VMCA)		✓			✓

Funções e privilégios relacionados a arquivo

O sistema é compatível com as seguintes funções e privilégios relacionados a arquivo:

NOTA: Uma ✓ em uma caixa denota um privilégio compatível com essa função, enquanto uma caixa em branco indica que o privilégio não é compatível com a função.

Tarefa	Operador	Administrador de VM	Administrador de segurança	Administrador de armazenamento	Administrador
Visualizar o seguinte: • Alertas de file system • Lista de servidores NAS • Lista de file systems • Lista de cotas de usuário de arquivo	✓		✓	✓	✓

Tarefa	Operador	Administrador de VM	Administrador de segurança	Administrador de armazenamento	Administrador
• Lista de rotas de interface de arquivo • Lista de interfaces de arquivo • Lista de compartilhamentos SMB • Lista de exportações NFS					
Visualizar o seguinte: • Lista de servidores DNS de arquivos ou um servidor DNS específico • Lista de servidores FTP de arquivos ou um servidor FTP específico • Lista de interfaces de arquivos ou uma interface de arquivos específica • Lista de rotas de interface de arquivos ou uma rota de interfaces específica • Lista de servidores Kerberos de arquivos ou um servidor Kerberos específico • Lista de servidores LDAP de arquivos ou um servidor LDAP específico • Lista de servidores NDMP de arquivos ou um servidor NDMP específico • Lista de servidores NIS de arquivos ou um servidor NIS específico • Lista de file systems ou um file system específico • Lista de cotas de árvore de arquivos ou uma cota de árvore de arquivos específica • Lista de cotas de usuário de arquivo ou uma cota de usuário específica • Lista de verificadores de vírus de arquivo ou um verificador de vírus de arquivo específico • Lista de servidores NAS ou um servidor NAS específico • Lista de exportações NFS ou uma exportação NFS específica • Lista de servidores NFS ou um servidor NFS específico • Lista de servidores SMB ou um servidor SMB específico • Lista de compartilhamentos SMB ou um compartilhamento SMB específico	✓		✓	✓	✓
Adicionar, modificar, excluir ou fazer ping de um servidor NAS específico ou fazer upload de				✓	✓

Tarefa	Operador	Administrador de VM	Administrador de segurança	Administrador de armazenamento	Administrador
senha, hosts ou grupos para um servidor NAS específico					
Visualizar senha ou hosts de um servidor NAS específico			✓		✓
Adicionar um file system ou modificar/excluir um file system específico em um servidor NAS atual				✓	✓
Adicionar um clone ou snapshot a um file system específico, atualizar ou restaurar um file system específico ou atualizar a cota de um file system específico				✓	✓
Adicionar uma cota de árvore de arquivos ou modificar, excluir ou atualizar uma cota de árvore de arquivos específica				✓	✓
Adicionar uma cota de usuário de arquivo ou modificar, excluir ou atualizar uma cota de usuário de arquivo específica				✓	✓
Adicionar um verificador de vírus de arquivo, modificar ou excluir um verificador de vírus de arquivo específico ou fazer upload de uma configuração específica de verificador de vírus de arquivo					✓
Fazer download de uma configuração específica de verificador de vírus de arquivo			✓		✓
Adicionar um servidor SMB ou NFS ou modificar, excluir, associar ou desfazer a associação de um servidor SMB ou NFS específico				✓	✓
Adicionar um compartilhamento SMB ou modificar/excluir um compartilhamento SMB específico				✓	✓
Adicionar uma exportação NFS ou modificar/excluir uma exportação NFS específica				✓	✓
Adicionar uma interface de arquivo ou modificar/excluir uma interface de arquivo específica				✓	✓
Adicionar uma rota de interface de arquivo ou modificar/excluir uma rota de interface de arquivo específica				✓	✓
Adicionar um servidor DNS, FTP, Kerberos, LDAP, NDMP ou NIS de arquivos ou modificar/excluir um servidor DNS, FTP, Kerberos,				✓	✓

Tarefa	Operador	Administrador de VM	Administrador de segurança	Administrador de armazenamento	Administrador
LDAP, NDMP ou NIS de arquivos específico					
Fazer upload de um arquivo keytab Kerberos					✓
Fazer download de um arquivo keytab Kerberos	✓		✓		✓
Fazer upload de uma configuração de LDAP de arquivos ou de um certificado LDAP					✓
Fazer download de um certificado LDAP de arquivos			✓		✓

Gerenciamento de contas de usuário com base em privilégios de função

Em relação ao gerenciamento de contas de usuário, um usuário com a função Administrador ou Administrador de segurança pode:

- Criar uma nova conta de usuário.
- Excluir qualquer conta de usuário, com exceção da conta de administrador integrada.

  NOTA: Não é possível excluir a conta de administrador integrada.
- Mudar outro usuário para qualquer função.
- Reconfigurar a senha de outro usuário.
- Bloquear ou desbloquear outra conta de usuário.

  NOTA: Os usuários conectados com função Administrador ou Administrador de segurança não podem bloquear sua própria conta.

Os usuários conectados não podem excluir sua própria conta de usuário. Além disso, com exceção dos usuários com a função Administrador ou Administrador de segurança, os usuários conectados só podem alterar suas próprias senhas. Os usuários devem fornecer a senha antiga para alterar a senha. Os usuários conectados não podem redefinir suas próprias senhas, alterar suas próprias funções ou bloquear/desbloquear suas próprias contas.

O perfil da conta de administrador integrada (com a função Administrador) não pode ser editado nem bloqueado.

Quando o status de bloqueio ou função de um usuário é alterado, o usuário é excluído ou sua senha é alterada por um Administrador ou Administrador de segurança. Além disso, todas as sessões vinculadas a esse usuário são invalidadas.

NOTA: Se os usuários atualizarem suas próprias senhas na sessão, a sessão permanecerá ativa.

Redefinir as senhas das contas de administrador e de serviço

O equipamento vem com uma conta de usuário administrador padrão que permite fazer a configuração inicial. Também vem com uma conta de usuário de serviço padrão que permite executar funções de serviço especializadas. É recomendável que você configure inicialmente o PowerStore usando a interface do usuário do PowerStore Manager em vez de outro método, como a REST API ou a CLI. O uso da interface do usuário do PowerStore Manager garante que todas as senhas padrão sejam alteradas. Caso esqueça das novas senhas, você poderá redefini-las com os valores padrão.

O método para redefinir essas senhas depende se o equipamento é um PowerStore T model ou um PowerStore X model. Use o método que corresponde ao seu equipamento para redefinir a senha de administrador ou de serviço, ou ambas.

Redefinir as senhas das contas de administrador e de serviço com os valores padrão em um equipamento PowerStore T model

Sobre esta tarefa

Para um equipamento PowerStore T model, o método principal para redefinir as senhas de usuário administrador ou de serviço é usar uma unidade USB. Os file systems compatíveis incluem FAT32 e ISO 9660.

NOTA: Para redefinir a senha quando o equipamento está no modo de serviço, execute as etapas a seguir com uma diferença. Aplique o processo de redefinição de USB a cada nó. Essa ação garante que, quando o sistema retornar ao modo normal e durante o log-in do PowerStore Manager, você tenha que fornecer uma nova senha tanto para o usuário de serviço como para o usuário administrador.

Etapas

1. Se a unidade USB estiver formatada, vá para a próxima etapa. Caso contrário, use um prompt de comando, como `format <d:> /FS:FAT32`, para formatá-la.

   Onde `d:` é a letra de unidade da unidade USB que você inseriu no laptop ou PC.

2. Defina o rótulo com o comando:

   ```
   label d:
   RSTPWD
   ```

   NOTA: O equipamento não montará a unidade USB sem o rótulo `RSTPWD`. Depois de rotular a unidade USB, insira um arquivo vazio para as senhas de conta que você gostaria de redefinir. Você pode redefinir a senha da conta de administrador ou de serviço, ou de ambas.

3. Para criar um arquivo vazio na unidade, use um ou ambos os comandos a seguir, conforme necessário:

   ```
   copy NUL d:\admin
   copy NUL d:\service
   ```

4. Insira a unidade USB na porta USB de um dos nós do equipamento, aguarde 10 segundos e remova a unidade.
   Agora a senha de cada conta que você redefiniu tem o valor padrão.
5. Conecte-se ao cluster por meio de um navegador usando o endereço IP do cluster e faça log-in como admin com a senha inicial padrão, que é **`Password123#`**.
   Deve ser exibido um prompt para redefinir as senhas de administrador ou de serviço, ou ambas. Se você preferir redefinir a senha de serviço usando shell seguro (SSH), a senha padrão inicial da conta de serviço é **`service`**.
6. Altere a senha de administrador do padrão para uma senha especificada pelo usuário.
7. Para definir uma senha da conta de serviço diferente da senha de administrador, desmarque a caixa de seleção relacionada.

Resultados

Se o prompt para redefinir a senha não for exibido durante a tentativa de log-in depois que você executar este procedimento, entre em contato com seu provedor de serviços.

Redefinir as senhas das contas de administrador e de serviço com os valores padrão em um equipamento PowerStore X model

Pré-requisitos

Saiba o nome do nó principal do equipamento principal (por exemplo, PSTX-44W1BW2-A e PowerStore D6013). Se necessário, gere o arquivo `reset.iso`.

Sobre esta tarefa

Para um equipamento PowerStore X model, use uma imagem ISO e monte-a no vSphere. Em www.dell.com/support, é possível fazer download de arquivos de imagem criados previamente. Você também pode criar sua própria imagem de um sistema Linux usando um ou ambos os comandos de toque a seguir, dependendo das senhas que devem ser redefinidas:

```
mkdir iso
touch iso/admin
```

```
touch iso/service
mkisofs -V RSTPWD -o reset.iso iso
```

NOTA: A imagem ISO, `reset.iso`, deve residir em um datastore para que possa ser montada como um CD virtual do vSphere.

NOTA: Para redefinir a senha quando o equipamento está no modo de serviço, execute as etapas a seguir com duas diferenças. Primeiro, você deve fazer upload da imagem ISO para o datastore PRIVATE-C9P42W2.A.INTERNAL da máquina virtual (VM) da controladora porque o datastore público não está disponível. Em segundo lugar, faça upload e aplique o arquivo `reset.iso` aos nós A e B da VM do controlador. Essa ação garante que, quando o sistema retornar ao modo normal e o acesso ao PowerStore Manager estiver disponível, você tenha que fornecer uma nova senha tanto para o usuário de serviço como para o usuário administrador.

Etapas

1. No vSphere, em **Storage**, selecione seu equipamento PowerStore X model.

   Por exemplo, **DataCenter-WX-D6013** > **PowerStore D6013**

2. Em **Files**, selecione **ISOs**.
3. Selecione **Upload** e faça upload do arquivo `reset.iso`, seja ele o arquivo de imagem criado previamente do www.dell.com/support ou seu próprio arquivo de imagem criado em um sistema Linux.
   O arquivo `reset.iso` será exibido na pasta **ISOs**.
4. No vSphere, em **Host and Clusters**, selecione o nó principal do equipamento PowerStore X model principal no cluster.

   Por exemplo, **DataCenter-WX-D6013** > **Cluster WX-D6013** > **PSTX-44W1BW2-A**

5. Em **Summary**, clique em **CD/DVD Drive 1** e selecione **Connect to datastore ISO File**.
   A janela **Choose an ISO image to mount** será exibida.
6. Em **Datastores**, clique no equipamento PowerStore X model principal no cluster e selecione a pasta **ISOs**.
   O arquivo `reset.iso` deverá ser exibido em **Contents**.
7. Selecione o arquivo `reset.iso` e clique em **OK**.
   Em **Summary**, **CD/DVD drive 1** deverá aparecer como **Connected** por cerca de 10 segundos e, em seguida, mudar para **Disconnected**. A senha de administrador do cluster, a senha de serviço ou ambas agora estão redefinidas com os valores padrão.
8. Conecte-se ao cluster por meio de um navegador usando o endereço IP do cluster e faça log-in como admin com a senha inicial padrão, que é **`Password123#`**.
   Deve ser exibido um prompt para redefinir as senhas de administrador ou de serviço, ou ambas. Se você preferir redefinir a senha de serviço usando SSH, a senha padrão inicial da conta de serviço é **`service`**.
9. Altere a senha de administrador do padrão para uma senha especificada pelo usuário.
10. Para definir uma senha da conta de serviço diferente da senha de administrador, desmarque a caixa de seleção relacionada.

Resultados

Se o prompt para redefinir a senha não for exibido durante a tentativa de log-in depois que você executar este procedimento, entre em contato com seu provedor de serviços.

Certificados

Os dados no armazenamento de certificados do PowerStore são persistentes. O armazenamento de certificados guarda os seguintes tipos de certificado:

- Certificados de CA (Certificate Authority, autoridade de certificação)
- Certificados de client
- Certificados de servidor

Visualizando certificados

Sobre esta tarefa

São exibidas as seguintes informações no PowerStore Manager para cada certificado armazenado no equipamento:

- `Service`

- Type
- Scope
- Issued by
- Valid
- Valid to
- Issued to

NOTA: Use a REST API ou a CLI para visualizar informações adicionais sobre o certificado.

Para visualizar as informações do certificado, faça o seguinte:

Etapas

1. Inicie o PowerStore Manager.
2. Clique em **Settings** e, em **Security**, clique em **Certificates**.
   As informações sobre os certificados armazenados no equipamento são exibidas.
3. Para visualizar a cadeia de certificados que compõem um certificado e as informações associadas referentes a um serviço, clique no serviço em questão.
   A opção **View Certificate Chain** é exibida e lista informações sobre a cadeia de certificados que compõem o certificado.

Comunicação segura entre equipamentos PowerStore de um cluster

Durante a criação do cluster, o nó principal do equipamento principal do cluster cria um certificado de CA (Certificate Authority, autoridade de certificação), também conhecido como CA do cluster. O equipamento principal passa o certificado CA do cluster aos equipamentos que ingressam no cluster.

Cada equipamento do PowerStore em um cluster gera seu próprio certificado IPSec exclusivo, que é assinado pelo certificado de CA do cluster. Os dados confidenciais que os equipamentos PowerStore transmitem pela rede de cluster são protegidos por IPsec e TLS para preservar a segurança e a integridade dos dados.

Comunicação segura para replicação e importação de dados

A infraestrutura de certificados e credenciais do PowerStore permite o intercâmbio de certificados de servidor e client e de credenciais de usuário. Este processo inclui:

- Recuperar e validar o certificado do servidor durante o handshake TLS
- Adicionar o certificado de CA confiável do sistema remoto ao armazenamento de credenciais
- Adicionar o certificado de servidor/client confiável ao armazenamento de credenciais
- Auxiliar no estabelecimento de conexões seguras depois que a confiança é estabelecida

O PowerStore comporta a seguinte funcionalidade de gerenciamento de certificados:

- Para a replicação, um intercâmbio de certificados entre dois clusters do PowerStore para estabelecer uma comunicação de gerenciamento confiável. Para facilitar a replicação entre os clusters do PowerStore, a confiança bidirecional deve ser estabelecida entre os clusters para permitir a autenticação TLS mútua ao emitir solicitações de controle de REST de replicação.
- Para importação de dados, um certificado e um intercâmbio de credenciais com persistência, para estabelecer uma conexão segura entre um sistema de armazenamento Dell EMC (VNX, Unity, Storage Center (SC) ou sistema de armazenamento de par (PS)) e um cluster do PowerStore.

Suporte a vSphere Storage API for Storage Awareness

O VASA (vSphere Storage API for Storage Awareness) é uma API para reconhecimento de armazenamento definida pela VMware para ser usada com qualquer fornecedor. Um VASA Provider abrange vários componentes que trabalham em cooperação para atender a solicitações de API do VASA recebidas. O gateway de API de VASA, que recebe todas as APIs de VASA de entrada, é implementado no

equipamento principal (o que possui o IP de gerenciamento flutuante) em um cluster do PowerStore. Os hosts do ESXi e o vCenter Server se conectam ao VASA Provider e obtêm informações sobre status, topologia de armazenamento e recursos disponíveis. Subsequentemente, o vCenter Server apresenta essas informações para os clients vSphere. O VASA é usado por clients VMware em vez de clients PowerStore Manager.

O usuário do vSphere deve configurar essa instância do VASA Provider como o provedor de informações do VASA para o cluster. Se o equipamento principal ficar inativo, o processo relacionado será reiniciado no equipamento que se tornará o próximo principal, junto com o VASA Provider. O endereço IP sobre failover automaticamente. Internamente, o protocolo detectará uma falha ao obter os eventos de alteração de configuração do VASA Provider recém-ativado, mas isso causará uma ressincronização automática dos objetos de VASA sem a intervenção do usuário.

O PowerStore fornece interfaces do VASA 3.0 para vSphere 6.5 e 6.7.

O VASA 3.0 é compatível com vVols (Virtual Volumes). O VASA 3.0 é compatível com interfaces para consultar abstrações de armazenamento, como vVols e contêineres de armazenamento. Essas informações ajudam o SPBM (Storage Policy-Based Management, gerenciamento baseado em políticas de armazenamento) a tomar decisões sobre posicionamento de unidade virtual e conformidade. O VASA 3.0 também dá suporte a interfaces para provisionar e gerenciar o ciclo de vida dos vVols usados para fazer backup de unidades virtuais. Essas interfaces são chamadas diretamente por hosts do ESXi.

Para obter mais informações relacionadas a VASA, vSphere e vVols, consulte a documentação da VMware e a Ajuda on-line do PowerStore Manager.

Autenticação relacionada ao VASA

Para iniciar uma conexão do vCenter com o VASA Provider do PowerStore Manager, use o client vSphere para especificar as seguintes informações:

- URL do VASA Provider, usando o seguinte formato para VASA 3.0: https://<Management IP address>:8443/version.xm.
- O nome de usuário de um usuário do PowerStore Manager (a função deve ser Administrador de VM ou Administrador).

  NOTA: A função Administrador de VM é usada estritamente como meio para registrar certificados.
- A senha associada ao usuário.

As credenciais do PowerStore Manager utilizadas aqui são usadas somente durante esta etapa inicial de conexão. Se as credenciais do PowerStore Manager forem válidas para o cluster de destino, o certificado do vCenter Server será registrado automaticamente no cluster. Esse certificado é usado para autenticar todas as solicitações subsequentes do vCenter. Não é necessária nenhuma etapa manual para instalar esse certificado no VASA Provider ou fazer upload dele. Se o certificado expirar, o vCenter deverá registrar um novo certificado para dar suporte a uma nova sessão. Se o certificado for revogado pelo usuário, a sessão será invalidada e a conexão será desfeita.

Sessão do vCenter, conexão segura e credenciais

Uma sessão do vCenter começa quando um administrador do vSphere usa o vSphere Client para fornecer ao vCenter Server as credenciais de log-in e a URL do VASA Provider. O vCenter Server usa a URL, as credenciais e o certificado SSL do VASA Provider para estabelecer uma conexão segura com o VASA Provider. Uma sessão do vCenter acaba quando um dos seguintes eventos ocorre:

- Um administrador usa o vSphere Client para remover o VASA Provider da configuração do vCenter e o vCenter Server encerra a conexão.
- O vCenter Server ou um serviço do vCenter Server apresenta falha, encerrando a conexão. Se o vCenter ou o serviço do vCenter Server não puder restabelecer a conexão SSL, será iniciada uma nova.
- O VASA Provider apresenta falha, encerrando a conexão. Quando o VASA Provider é iniciado, ele pode responder a comunicação do vCenter Server para restabelecer a conexão SSL e uma sessão do VASA.

Uma sessão do vCenter é baseada em comunicação HTTPS segura entre um vCenter Server e um VASA Provider. No VASA 3.0, o vCenter Server atua como a autoridade de certificação da VMware (VMCA). O VASA Provider transmite um certificado autoassinado na solicitação, depois de autorizar a solicitação. Ele adiciona o certificado VMCA ao truststore correspondente, emite um solicitação de assinatura de certificado e substitui o certificado autoassinado pelo certificado VMCA assinado. As futuras conexões serão autenticadas pelo VASA Provider usando o certificado do client SMS (Storage Monitoring Service) validado em relação ao certificado raiz de assinatura registrado anteriormente. Um VASA Provider gera identificadores exclusivos para objetos de entidade de armazenamento, e o vCenter Server usa o identificador para solicitar dados de uma entidade específica.

Um VASA Provider usa certificados SSL e o identificador de sessão do VASA para validar as sessões de VASA. Depois que a sessão é estabelecida, o VASA Provider deve validar o certificado SSL e o identificador de sessão do VASA associados a cada chamada de função do vCenter Server. O VASA Provider usa o certificado VMCA armazenado no truststore para validar o certificado associado a chamadas de função do SMS do vCenter. Uma sessão do VASA persiste em várias conexões SSL. Se uma conexão SSL for descartada, o vCenter Server fará um handshake de SSL com o VASA Provider para restabelecer a conexão SSL dentro do contexto da mesma sessão de VASA.

Se um certificado SSL expirar, o administrador do vSphere deverá gerar um novo certificado. O vCenter Server estabelecerá uma nova conexão SSL e registrará o novo certificado no VASA Provider.

CUIDADO: O SMS não chama a função `unregisterVASACertificate` em relação a um VASA Provider 3.0. Portanto, mesmo após o cancelamento do registro, o VASA Provider pode continuar a usar o certificado VMCA assinado obtido do SMS.

Autenticação CHAP

O CHAP (Challenge Handshake Authentication Protocol) é um método de autenticação de iniciadores iSCSI (hosts) e destinos (volumes e snapshots). O CHAP expõe o armazenamento iSCSI e garante um protocolo de armazenamento padrão seguro. A autenticação depende de um segredo, semelhante a uma senha, que é conhecido pelo autenticador e pelo par. Existem duas variantes do protocolo CHAP:

- A autenticação CHAP única permite que o destino iSCSI autentique o iniciador. Quando um iniciador tenta se conectar a um destino (modo normal ou pelo modo de detecção), ele fornece um nome de usuário e uma senha ao destino.
- A autenticação CHAP mútua é aplicada além do CHAP único. O CHAP mútuo permite que o destino iSCSI e o iniciador se autentiquem mutualmente. Cada destino iSCSI apresentado pelo grupo é autenticado pelo iniciador iSCSI. Quando um iniciador tenta se conectar a um destino, o destino fornece um nome de usuário e uma senha para ele. O iniciador compara o nome de usuário e a senha fornecidos com as informações contidas nele. Se corresponderem, o iniciador poderá se conectar ao destino.

NOTA: Se o CHAP é usado em seu ambiente, é recomendável configurar e habilitar a autenticação CHAP antes de preparar volumes para receber dados. Se você preparar unidades para receber dados antes de configurar e ativar a autenticação CHAP, poderá perder o acesso aos volumes.

O PowerStore não é compatível com o modo de detecção CHAP do iSCSI. A tabela a seguir mostra as limitações do PowerStore relacionadas ao modo de detecção CHAP do iSCSI.

Tabela 1. Limitações do modo de detecção CHAP do iSCSI

Modo CHAP	Modo único (iniciador ativado)	Modo mútuo (iniciador e destino ativados)
Detecção	O PowerStore não autenticará (desafiará) o host. A autenticação não pode ser usada para impedir a detecção de destinos. Isso não resulta em acesso indesejado a dados do usuário.	O PowerStore não responderá a uma solicitação de autenticação (desafio) de um host, e a detecção apresentará falha se o host desafiar o PowerStore.
Normal	Funciona conforme esperado. As credenciais são testadas pelo PowerStore.	Funciona conforme esperado. As credenciais são transferidas pelo PowerStore.

Para a replicação remota entre um equipamento de origem e de destino, o processo de verificação e atualização detecta alterações nos sistemas local e remoto e restabelece as conexões de dados, também levando em conta as configurações de CHAP.

Configurando o CHAP

A autenticação CHAP única (iniciador ativado) ou mútua (iniciador e destino ativados) pode ser habilitada em um cluster do PowerStore. O CHAP pode ser ativado para uma implementação de cluster de um ou de vários equipamentos PowerStore e hosts externos.

Quando a autenticação única está ativada, o nome de usuário e a senha de cada iniciador devem ser informados ao adicionar hosts externos. Se a autenticação mútua está ativada, o nome de usuário e a senha do cluster também devem ser inseridos. Ao adicionar um host e iniciadores com CHAP ativado, a senha do iniciador deve ser exclusiva, e você não pode usar a mesma senha em todos os iniciadores de um host. Os detalhes específicos sobre como fazer a configuração de CHAP de um host externo variam. Para usar este recurso, você precisa estar familiarizado com o sistema operacional do host e como configurá-lo.

NOTA: A ativação do CHAP depois que os hosts forem configurados no sistema é uma ação que causa interrupções nos hosts externos. Isso causa a interrupção de E/S até que as configurações sejam definidas no host externo e no equipamento. É recomendável que, antes de adicionar hosts externos ao equipamento, você decida qual tipo de configuração de CHAP será implementada, se for o caso.

Se você ativar o CHAP depois que os hosts forem adicionados, atualize os iniciadores de cada host. Se o CHAP estiver ativado, você não poderá adicionar um host a um grupo de hosts que não tenha credenciais de CHAP. Depois que o CHAP for ativado e você adicionar um

host mais tarde, registre o host manualmente no PowerStore Manager: em **Compute**, selecione **Hosts & Host Groups**. Você precisa inserir as credenciais no nível de iSCSI para o uso da autenticação. Nesse caso, copie o IQN do host e adicione as credenciais de CHAP relacionadas de cada iniciador.

Configure o CHAP para um cluster usando um destes meios:

- **CHAP** – Uma página de configurações de CHAP que pode ser acessada pelo PowerStore Manager (clique em **Settings** e, em **Security**, selecione **CHAP**).
- Servidor de REST API – A interface de aplicativo que pode receber solicitações de REST API para definir as configurações de CHAP. Para obter mais informações sobre a REST API, consulte *PowerStore REST API Reference Guide*.

Para determinar o status do CAHP, no PowerStore Manager, clique em **Settings** e, em **Security**, selecione **CHAP**.

Acesso SSH externo

Como opção, cada equipamento pode habilitar o acesso de shell seguro (SSH) externo à porta SSH do endereço IP do equipamento, o que leva o usuário ao recurso de serviço no nó principal de um equipamento. O endereço IP do equipamento flutua entre os dois nós dele à medida que a designação principal muda. Se o SSH externo estiver desabilitado, o acesso SSH não será permitido.

Quando um equipamento é fornecido pela primeira vez e não está configurado, o SSH é habilitado por padrão para que o equipamento possa ser atendido caso sejam identificados problemas antes que ele seja adicionado a um cluster. Quando um novo cluster é criado ou para uma operação de ingresso no cluster, o SSH deve ser definido inicialmente como desabilitado em todos os equipamentos.

Configurando o acesso SSH externo

Configure o acesso SSH externo a equipamentos de um cluster usando um dos seguintes meios:

- **SSH Management** – Uma página de configurações de SSH que pode ser acessada pelo PowerStore Manager (clique em **Settings** e, em **Security**, selecione **SSH Management**).
- Servidor de REST API – A interface de aplicativo que pode receber solicitações da REST API para definir configurações de SSH. Para obter mais informações sobre a REST API, consulte *PowerStore REST API Reference Guide*.
- `svc_service_config` – Um comando de serviço que você pode digitar diretamente como usuário de serviço no equipamento. Para obter mais informações sobre este comando, consulte o *PowerStore Service Scripts Guide*.

Para determinar o status do SSH nos equipamentos de um cluster, no PowerStore Manager, clique em **Settings** e, em **Security**, selecione **SSH Management**. Você também pode habilitar ou desabilitar SSH em um ou mais equipamentos que selecionar.

Uma vez que o serviço SSH tenha sido ativado com sucesso, use qualquer client SSH para fazer log-in no endereço IP do equipamento. O acesso ao equipamento exige credenciais de usuário de serviço.

A conta de serviço permite que os usuários executem as funções a seguir:

- Executar scripts de serviço especializados do equipamento para monitorar e solucionar problemas de operações e configurações do sistema do equipamento.
- Execute apenas um conjunto limitado de comandos atribuídos como membro de uma conta de usuário do Linux sem privilégios no modo de shell restrito. Essa conta não tem acesso aos arquivos do sistema exclusivo, arquivos de configuração ou dados de usuário ou cliente.

Para segurança máxima do equipamento, é recomendável deixar a interface do serviço SSH externo sempre desativada, a menos que ela seja especificamente necessária para executar operações de serviço no equipamento. Depois de executar as operações de serviço necessárias, desabilite a interface do SSH para garantir que o equipamento permaneça seguro.

Sessões SSH

As sessões da interface de serviço SSH do PowerStore são mantidas de acordo com as configurações estabelecidas pelo client SSH. As características da sessão são determinadas pelas definições da configuração do client SSH.

Senha da conta de serviço

A conta de serviço é uma conta que a equipe de serviço pode usar para executar comandos básicos de Linux.

Durante a configuração inicial do equipamento, você deve alterar a senha de serviço padrão. As restrições de senhas de serviço são iguais àquelas aplicadas a contas de gerenciamento do sistema (consulte Uso de nome de usuário e senha na página 7).

Autorização SSH

A autorização da conta de serviço é baseada em:

- Isolamento de aplicativos – O software PowerStore usa a tecnologia de contêineres que fornece isolamento de aplicativos. O acesso ao serviço do equipamento é fornecido pelo contêiner de serviço. Estão disponíveis apenas um conjunto de scripts de serviço e um conjunto de comandos de Linux. A conta de serviço não tem a capacidade de acessar outros contêineres que atendem ao file system e bloqueiam a E/S para usuários.
- Permissões do file system do Linux – A maioria dos utilitários e ferramentas do Linux que modificam a operação do sistema de alguma maneira não estão disponíveis para o usuário do serviço. É necessário ter privilégios de conta de superusuário. Como a conta de serviço não tem esses direitos de acesso, ela não pode usar os utilitários e ferramentas do Linux aos quais ela não tem permissões e não pode editar os arquivos de configuração que exigem acesso root para leitura e/ou modificação.
- Controles de acesso – Além do isolamento de aplicativos fornecido pela tecnologia de contêineres, o mecanismo de lista de controle de acesso (ACL, Access Control List) no equipamento usa uma lista de regras bem específicas para conceder ou negar explicitamente o acesso aos recursos do sistema pela conta de serviço. Essas regras especificam as permissões da conta de serviço a outras áreas do equipamento que não são definidas de outra forma pelas permissões do file system padrão do Linux.

Scripts de serviço do equipamento

Um conjunto de scripts para diagnóstico de problemas, configuração e recuperação do sistema é instalado na versão de software do equipamento. Esses scripts fornecem informações detalhadas e menor nível de controle do sistema do que o disponibilizado pelo PowerStore Manager. O *PowerStore Service Scripts Guide* descreve esses scripts e os casos de uso comuns.

IPMItool e porta de serviço Ethernet do nó do equipamento

O equipamento dá acesso ao console por uma porta de serviço Ethernet que está em cada nó. Esse acesso exige o uso de IPMItool. IPMItool é uma ferramenta de rede semelhante a SSH ou Telnet que usa o protocolo IPMI para fazer interface com cada nó por uma conexão Ethernet. O IPMItool é um utilitário do Windows que negocia um canal de comunicação seguro para acessar o console do nó de um equipamento. Esse utilitário exige acesso físico para ativar o console.

A interface da porta de serviço Ethernet do nó fornece os mesmos recursos e funções que a interface SSH de serviço (interface LAN de serviço) e também está sujeita às mesmas restrições. No entanto, os usuários acessam a interface por meio de uma conexão de porta Ethernet em vez de usar um client SSH. Essa interface foi projetada para a equipe de serviço em campo que pode se conectar ao equipamento sem afetar a rede. Não é necessário um console de gerenciamento dedicado.

Essa interface fornece uma conexão direta ponto a ponto e não roteável. A equipe de serviço pode usar a interface LAN de serviço para saída do console, para acesso SSH ao contêiner de serviço do PowerStore e para o PowerStore Manager, inclusive o Assistente de configuração inicial (ICW). O acesso SSH ao contêiner de serviço por meio da interface LAN de serviço está sempre ativado e não pode ser desabilitado, mas você gerencia a credencial da conta de serviço.

Para obter uma lista de scripts de serviço, consulte o *PowerStore Service Scripts Guide*.

Segurança NFS (Sistema de arquivos de rede)

A segurança NFS é o uso do Kerberos para autenticar usuários com NFSv3 e NFSv4. O Kerberos fornece integridade (assinatura) e privacidade (criptografia). A Privacidade e a integridade não precisam estar habilitadas, elas são opções de exportação NFS.

Sem o Kerberos, o servidor depende inteiramente do client para autenticar usuários: o client confia no servidor. Com o Kerberos esse não é o caso, o servidor confia no Key Distribution Center (KDC). É o KDC que lida com a autenticação e gerencia contas (principais) e senhas. Além disso, nenhuma senha em quaisquer formulários é enviada pela rede.

Sem o Kerberos, a credencial do usuário é enviada pela rede não criptografada e, portanto, pode ser falsificada com facilidade. Com o Kerberos, a identidade (principal) do usuário é incluída no tíquete do Kerberos criptografado, que pode ser lido somente pelo servidor de destino e pelo KDC. Eles são os únicos que conhecem a chave de criptografia.

Em conjunto com a segurança NFS, a criptografia AES128 e AES256 tem suporte no Kerberos. Junto com a segurança NFS, isso também afeta a SMB e o LDAP. Essas criptografias agora têm suporte por padrão pelo Windows e Linux. Essas novas criptografias são muito mais seguras No entanto, elas são válidas até o client enquanto são usadas. Com base nesse usuário principal, o servidor cria a credencial desse usuário consultando o UDS (UNIX Directory Service, serviço de diretório UNIX) ativo. Uma vez que o NIS (Serviço de informação de rede) não é protegido, não é recomendável utilizá-lo com a segurança NFS. É recomendável usar Kerberos com LDAP ou LDAPS.

A segurança NFS pode ser configurada usando o PowerStore Manager.

Relações do protocolo de arquivo

Com o Kerberos é necessário o seguinte:

- DNS - Você deve usar o nome DNS em vez de endereços IP.
- NTP- O PowerStore deve ter um servidor de NTP configurado.

  NOTA: Kerberos conta com a sincronização de hora correta entre o Key Distribution Center, servidores e o client na rede.
- UDS - Para criar credenciais.
- Nome de host - O Kerberos funciona com nomes e não com endereços IP.

A segurança NFS usa um ou dois SPNs (Service Principal Names, nomes principais de serviço), dependendo do valor do nome de host. Se o nome de host estiver no formato FQDN no domínio do host:

- O SPN curto: **`nfs/host@REALM`**
- O SPN longo: **`nfs/host.domainFQDN@REALM`**

Se o nome de host não estiver no formato FQDN, somente o SPN curto será usado.

Da mesma forma que o SMB, em que um servidor SMB pode ingressar em um domínio, um servidor NFS pode ingressar em um realm (o termo Kerberos equivalente para domínio). Existem duas opções para isso:

- usar o domínio do Windows configurado, se houver
- configurar totalmente um KDC do UNIX com base em realm Kerberos

Se o administrador escolher usar o domínio do Windows configurado, não há nada mais a fazer. Cada SPN usado pelo serviço NFS é automaticamente adicionado ou removido no KDC ao associar/retirar o servidor SMB. Observe que o servidor SMB não pode ser destruído se NFS seguro for configurado para usar a configuração do SMB.

Se o administrador selecionar para usar um UNIX com base em realm Kerberos, será necessária configuração adicional:

- Nome do realm: o nome do realm Kerberos, que geralmente é escrito em letras maiúsculas.
- configurar totalmente um KDC do UNIX com base em realm Kerberos.

Para garantir que um client monta uma exportação NFS com uma segurança específica, um parâmetro de segurança, sec, é fornecido, indicando qual a segurança mínima é permitida. Existem 4 tipos de segurança:

- `AUTH_SYS`: Segurança preexistente padrão, que não usa Kerberos. O servidor confia na credencial fornecida pelo client
- `KRB5`: Autenticação usando Kerberos v5
- `KRB5i`: Autenticação Kerberos mais integridade (assinatura)
- `KRB5p`: Autenticação Kerberos mais integridade e privacidade (criptografia)

Se um client NFS tentar montar uma exportação com uma segurança que é menor do que a segurança mínima configurada, o acesso será negado. Por exemplo, se o acesso mínimo for `KRB5i`, qualquer montagem usando `AUTH_SYS` ou `KRB5` será rejeitada.

Criando uma credencial

Quando um usuário se conecta ao sistema, ele apresenta somente a principal, **`user@REALM`**, que é extraída do tíquete Kerberos. Ao contrário da segurança `AUTH_SYS`, a credencial não está incluída na solicitação NFS. Da principal, a parte do usuário (antes da @) é extraída e usada para pesquisar o UDS para o ID exclusivo correspondente. Desse ID exclusivo, a credencial é criada pelo sistema usando o UDS ativo, semelhante a quando a credencial estendida NFS está habilitada (com a exceção de que, sem o Kerberos, o ID exclusivo é fornecido diretamente pela solicitação).

Se a principal não estiver mapeada no UDS, a credencial de usuário do UNIX padrão configurada é usada em vez disso. Se o usuário UNIX padrão não estiver definido, a credencial usada será ninguém.

Segurança em objetos do file system

Em um ambiente de vários protocolos, a política de segurança é definida no nível do file system e é independente para cada file system. Cada sistema de armazenamento usa suas políticas de acesso para determinar como reconciliar as diferenças entre a semântica de controle de acesso de NFS e SMB. Selecionar uma política de acesso determina qual mecanismo é usado para aplicar a segurança do arquivo no file system específico.

NOTA: Se o protocolo SMB1 mais antigo precisar ser compatível com seu ambiente, ele poderá ser ativado por meio do comando de serviço `svc_nas_cifssupport`. Para obter mais informações sobre este comando de serviço, consulte o *PowerStore Service Scripts Guide*.

Modelo de segurança UNIX

Quando a política do UNIX é selecionada, qualquer tentativa de alterar a segurança em nível de arquivo do protocolo SMB, como alterações em ACLs (Access Control Lists, listas de controle de acesso), é ignorada. Os direitos de acesso do UNIX são chamados de bits de modo ou ACL de NFSv4 dos objetos de um file system. Bits de modo são representados por uma string de bits. Cada bit representa um modo de acesso ou privilégio concedido ao usuário proprietário do arquivo, ao grupo associado ao objeto do file system e a todos os outros usuários. Os bits de modo do UNIX são representados como três conjuntos de definições rwx (leitura, gravação e execução) concatenadas para cada categoria de usuários (usuário, grupo ou outros). Uma ACL é uma lista de usuários e grupos de usuários pela qual o acesso ou a negação aos serviços é controlada.

Modelo de segurança Windows

O modelo de segurança do Windows é baseado principalmente nos direitos de objeto, que envolvem o uso de um SD (Security Descriptor, descritor de segurança) e sua ACL (Access Control List, lista de controle de acesso). Quando a política de SMB é selecionada, as alterações feitas nos bits de modo do protocolo NFS são ignoradas.

O acesso a um objeto do file system é baseado no fato de as permissões terem sido definidas para permitir ou negar por meio do uso de um descritor de segurança. O SD descreve o proprietário do objeto e os SIDs dos grupos do objeto, além de suas ACLs. A ACL faz parte do descritor de segurança de cada objeto. Cada ACL contém entradas de controle de acesso (ACEs). Cada ACE, por sua vez, contém um único SID, que identifica um usuário, grupo ou computador, e uma lista de direitos negados ou permitidos para esse SID.

Acesso a file systems em um ambiente multiprotocolo

O acesso a arquivos é oferecido por meio de servidores NAS. Um servidor NAS contém um conjunto de file systems em que os dados são armazenados. O servidor NAS fornece acesso a esses dados para protocolos de arquivos NFS e SMB por meio de compartilhamentos SMB e NFS. O modo de servidor NAS no compartilhamento de vários protocolos permite o compartilhamento dos mesmos dados entre SMB e NFS. Como o modo de compartilhamento de vários protocolos proporciona acesso simultâneo por SMB e NFS a um file system, devem ser levados em consideração e configurados corretamente o mapeamento de usuários do Windows para usuários do UNIX e a definição das regras de segurança a serem usadas (bits de modo, ACL e credenciais de usuários) para o compartilhamento de vários protocolos.

NOTA: Para obter informações sobre como configurar e gerenciar servidores NAS no que se refere a compartilhamento de vários protocolos, mapeamento de usuários, políticas de acesso e credenciais de usuário, consulte a ajuda on-line do PowerStore Manager.

Mapeamento de usuários

Em um contexto multiprotocolo, um usuário Windows precisa ter um usuário UNIX correspondente. No entanto, um usuário UNIX precisa ser associado a um usuário do Windows somente quando a política de acesso é Windows. Essa correspondência é necessária para que a segurança do file system possa ser aplicada, mesmo se não for nativa para o protocolo. Os seguintes componentes são envolvidos no mapeamento de usuários:

- Serviços de diretório do UNIX, arquivos locais, ou ambos
- Solucionadores Windows
- Mapeamento seguro (secmap) - um cache que contém todos os mapeamentos entre SIDs e UID ou GIDs usados por um servidor NAS.
- ntxmap

NOTA: O mapeamento de usuário não afeta os usuários ou grupos que são locais para o servidor SMB.

Serviços de diretório do UNIX e arquivos locais

Os UDS (UNIX Directory Services, serviços de diretórios do UNIX) e arquivos locais são usados para:

- Retornar o nome da conta UNIX correspondente para um ID de usuário (UID) em particular.
- Retornar o UID correspondente e o identificador de grupo primário (GID) para um nome de conta UNIX em particular.

Os serviços compatíveis são:

- LDAP
- NIS
- Arquivos locais
- Nenhum (o mapeamento só é possível é através do usuário padrão)

Deve haver um UDS habilitado, ou arquivos locais habilitados, ou arquivos locais e um UDS habilitados para o servidor NAS quando o compartilhamento multiprotocolo está habilitado. A propriedade de serviço de diretório do Unix do servidor NAS determina qual é usada para mapeamento de usuário.

Solucionadores Windows

Os solucionadores Windows são usados no mapeamento de usuário para:

- Retornar o nome da conta correspondente no Windows para um identificador de segurança (SID) em particular.
- Retornar o SID correspondente para um nome de conta em particular do Windows

Os solucionadores Windows são:

- O controlador de domínio (DC) do domínio.
- O banco de dados de grupo local (LGDB) do servidor SMB

secmap

A função de secmap é armazenar qualquer mapeamento SID-para-UID e GID primário e UID-para-SID para garantir coerência em todos os file systems do servidor NAS.

ntxmap

O ntxmap é usado para associar uma conta do Windows a uma conta UNIX de nome diferente. Por exemplo, o ntxmap é usado para criar a correlação entre uma conta chamada Gerald no Windows e uma conta, do mesmo usuário, chamada Gerry no UNIX.

SID para UID, mapeamento de GID principal

A sequência a seguir é o processo usado para resolver um SID para um UID, mapeamento de GID primário:

1. O secmap é pesquisado para o SID. Se o SID for encontrado, o mapeamento de UID e GID será resolvido.
2. Se o SID não for encontrado no secmap, o nome do Windows relacionado ao SID deve ser encontrado.
   a. Os bancos de dados do grupo local dos servidores SMB do NAS são pesquisados para o SID. Se o SID for encontrado, o nome Windows relacionado é o nome de usuário local juntamente com o nome do servidor SMB.
   b. Se o SID não for encontrado no banco de dados de grupo local, o controlador de domínio do domínio é pesquisado. Se o SID for encontrado, o nome Windows relacionado é o nome de usuário. Se o SID não for resolvido, o acesso será negado.
3. O nome do Windows é convertido em um nome do UNIX. O ntxmap é usado para essa finalidade.
   a. Se o nome do Windows for encontrado no ntxmap, a entrada é usada como o nome do UNIX.
   b. Se o nome do Windows não for encontrado no ntxmap, o nome do Windows será é usado como o nome do UNIX.
4. O UDS (servidor de NIS, servidor LDAP ou arquivos locais) é pesquisado usando o nome do UNIX.
   a. Se o nome de usuário do UNIX for encontrado, o mapeamento de UID e GID será resolvido.
   b. Se o nome do UNIX não for encontrado, mas o mapeamento automático para o recurso de contas não mapeadas do Windows estiver habilitado, o UID será automaticamente atribuído.
   c. Se o nome de usuário do UNIX não for encontrado no UDS, mas existir uma conta do UNIX padrão, o mapeamento de UID e GID será resolvido para o mapemanto da conta UNIX padrão.
   d. Se o SID não for resolvido, o acesso será negado.

Se o mapeamento for encontrado, ele será adicionado no banco de dados secmap persistente. Se o mapeamento não for encontrado, o mapeamento com falha será adicionado ao banco de dados secmap persistente.

O diagrama a seguir é o processo usado para resolver um SID para um UID, mapeamento de GID primário:

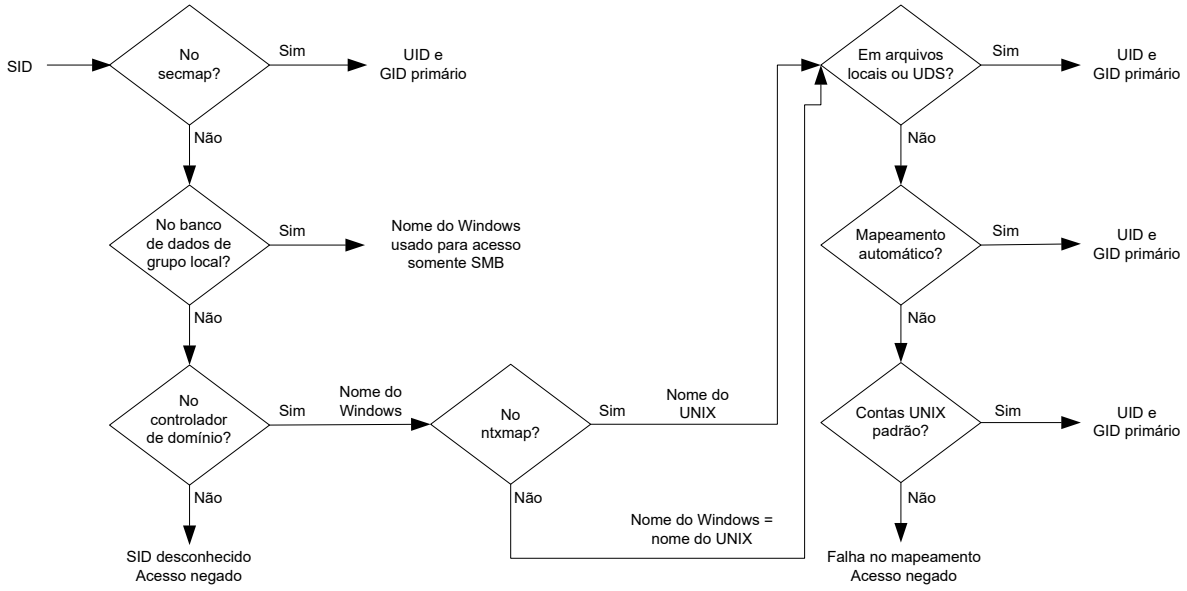

Figura 1. Processo para resolver um SID para um UID, mapeamento de GID primário

ID exclusivo para mapeamento SID

A sequência a seguir é o processo usado para resolver um ID exclusivo para um mapeamento de SID primário:

1. O secmap é pesquisado para o ID exclusivo. Se o ID exclusivo for encontrado, o mapeamento de SID será resolvido.
2. Se o ID exclusivo não for encontrado no secmap, o nome do UNIX relacionado ao ID exclusivo deve ser encontrado.
    a. O UDS (servidor NIS, servidor LDAP ou arquivos locais) é pesquisado usando o ID exclusivo. Se o ID exclusivo for encontrado, o nome Windows relacionado é o nome de usuário.
    b. Se o UID não for encontrado no UDS, mas houver uma conta do Windows padrão, o UID será associado ao SID da conta do Windows padrão.
3. Se as informações da conta Windows padrão não forem usadas, o nome do UNIX será traduzido em um nome do Windows. O ntxmap é usado para essa finalidade.
    a. Se o nome do UNIX for encontrado no ntxmap, a entrada é usada como o nome do Windows.
    b. Se o nome do UNIX não for encontrado no ntxmap, o nome do UNIX será é usado como o nome do Windows.
4. O DC do Windows ou o banco de dados do grupo local é pesquisado usando o nome do Windows.
    a. Se o nome do Windows for encontrado, o mapeamento de SID será resolvido.
    b. Se o nome do Windows contiver um ponto e a parte do nome após o último ponto (.) corresponder a um nome de servidor SMB, o banco de dados do grupo local desse servidor SMB será pesquisado para resolver o mapeamento de SID.
    c. Se o nome do Windows não for encontrado, mas houver uma conta do Windows padrão, o SID será associado ao nome da conta padrão do Windows.
    d. Se o SID não for resolvido, o acesso será negado.

Se o mapeamento for encontrado, ele será adicionado no banco de dados secmap persistente. Se o mapeamento não for encontrado, o mapeamento com falha será adicionado ao banco de dados secmap persistente.

O diagrama a seguir é o processo usado para resolver um UID para um mapeamento de SID primário:

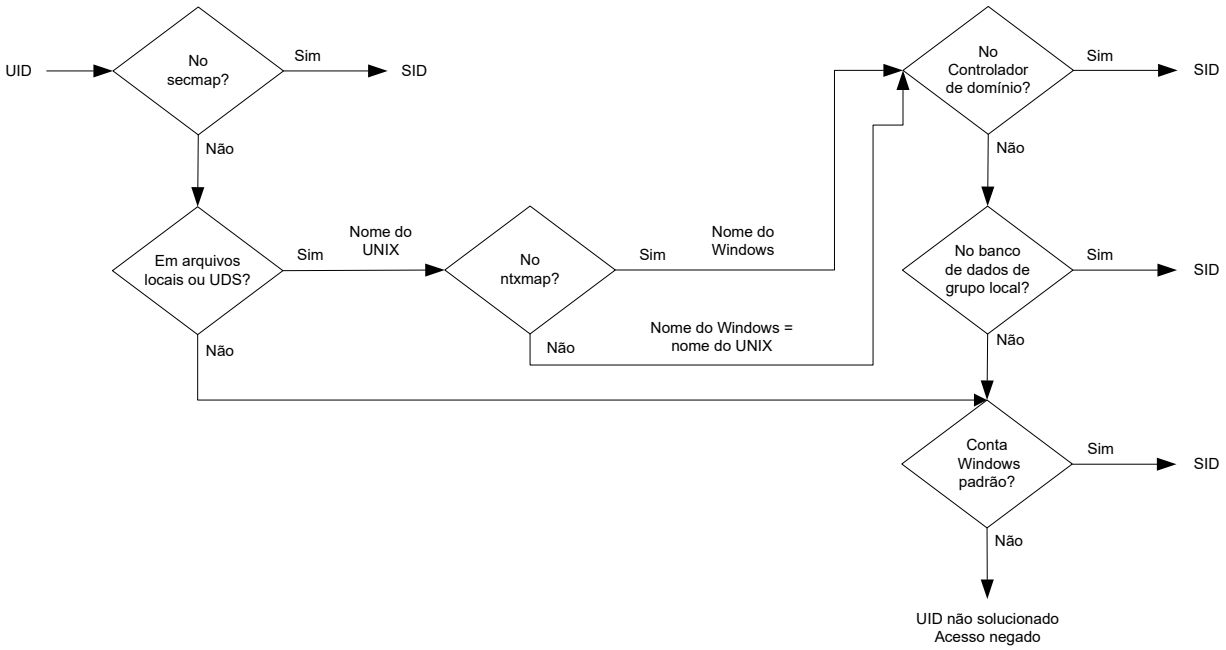

Figura 2. Processo usado para resolver um UID para o mapeamento de SID

Políticas de acesso para NFS, SMB e FTP

Em um ambiente multiprotocolo, o sistema de armazenamento usa políticas de acesso de file systems para gerenciar o controle de acesso de seus file systems. Há dois tipos de segurança, UNIX e Windows.

Para autenticação de segurança do UNIX, a credencial é criada a partir dos serviços de diretório UNIX (UDS), com a exceção de acesso de NFS não seguro, onde a credencial é fornecida pelo client do host. Os direitos do usuário são determinados pelos bits de modo e ACL de NFSv4. Os identificadores de usuário e de grupo (UID e GID, respectivamente) são usados para a identificação. Não há privilégio associado à segurança do UNIX.

Na autenticação de segurança do Windows, a credencial é criada pelo controlador de domínio (DC) do Windows e um banco de dados de grupo local (LGDB) do servidor SMB. Os direitos do usuário são determinados pelas ACLs do SMB. O identificador de segurança (SID) é usado para identificação. Existem privilégios associados à segurança do Windows, como TakeOwnership, Backup e Restore, que são concedidos pelo LGDB ou GPO (Group Policy Object, objeto de política de grupo) do servidor SMB.

A seguinte tabela descreve as políticas de acesso que definem qual segurança é usada por quais protocolos:

Access policy	Descrição
Nativa (padrão)	• Cada protocolo gerencia o acesso com a respectiva segurança nativa. • A segurança dos compartilhamentos NFS usa a credencial do UNIX associada à solicitação para verificar os bits de modo do UNIX NFSv3 ou da ACL do NFSv4. O acesso é então concedido ou negado. • A segurança dos compartilhamentos SMB usa a credencial do Windows associada à solicitação para verificar a ACL de SMB. O acesso é então concedido ou negado. • Os bits de modo do UNIX NFSv3 e as alterações de permissão da ACL NFSv4 são sincronizados entre si. • Não há nenhuma sincronização entre as permissões do Unix e do Windows.
Windows	• Protege o acesso em nível de arquivo do Windows e UNIX usando a segurança do Windows. • Usa uma credencial do Windows para verificar a ACL de SMB. • As permissões dos arquivos recém-criados são determinadas por uma conversão da ACL de SMB. As alterações de permissão da ACL de SMB são sincronizadas com os bits de modo do UNIX NFSv3 ou ACL NFSv4. • Os bits de modo de NFSv3 e as alterações de permissão da ACL NFSv4 são negados.
UNIX	• Protege o acesso em nível de arquivo do Windows e UNIX usando a segurança do UNIX. • Mediante a solicitação de acesso do SMB, a credencial do UNIX criada a partir dos arquivos locais ou UDS é usada para verificar os bits de modo de NFSv3 ou ACL NFSv4 quanto às permissões. • As permissões dos arquivos recém-criados são determinadas por UMASK. • Os bits de modo do UNIX NFSv3 ou as alterações de permissão da ACL NFSv4 são sincronizados com a ACL de SMB. • As alterações de permissão da ACL de SMB são permitidas para evitar interrupções, mas essas permissões não são mantidas.

No caso de FTP, a autenticação com Windows ou UNIX depende do formato do nome de usuário usado ao autenticar para o servidor NAS. Se a autenticação do Windows é usada, o controle de acesso ao FTP é semelhante ao do SMB. Caso contrário, a autenticação é semelhante à do NFS. Os clientes de FTP e de SFTP são autenticados quando se conectam ao servidor NAS. Pode ser uma autenticação SMB (quando o formato do nome de usuário é `domain\user` ou `user@domain`) ou uma autenticação UNIX (para outros formatos de nome de usuário único). A autenticação SMB é garantida pelo DC Windows do domínio definido no servidor NAS. A autenticação UNIX é garantida pelo DM de acordo com a senha criptografada armazenada em um servidor LDAP remoto, um servidor NIS remoto ou no arquivo local de senha do servidor NAS.

Credenciais para segurança em nível de arquivo

Para impor a segurança em nível de arquivo, o sistema de armazenamento deve criar uma credencial associada à solicitação SMB ou NFS sendo manipulada. Há dois tipos de credenciais, Windows e UNIX. As credenciais do Windows e UNIX são criadas pelo servidor NAS para os seguintes casos de uso:

- Para criar uma credencial do UNIX, com mais de 16 grupos para uma solicitação de NFS. A propriedade da credencial estendida do servidor NAS deve ser definida para fornecer essa capacidade.
- Para criar uma credencial do UNIX para uma solicitação SMB quando a política de acesso para o file system é UNIX.
- Para criar uma credencial do Windows para uma solicitação de SMB.
- Para criar uma credencial de Windows para uma solicitação de NFS quando a política de acesso para o file system é Windows.

NOTA: Para uma solicitação de NFS quando a propriedade da credencial estendida não é definida, a credencial do UNIX da solicitação de NFS é usada. Ao usar a autenticação Kerberos para uma solicitação SMB, a credencial do Windows do usuário do domínio é incluída no tíquete do Kerberos da solicitação de configuração da sessão.

Um cache persistente de credenciais é usado para:

- Credenciais do Windows criadas para o acesso a um file system, tendo uma política de acesso do Windows.
- Credenciais do Unix para o acesso por NFS se a opção de credencial estendida está habilitada.

Há uma instância de cache para cada servidor NAS.

Concedendo acesso a usuários não mapeados

O ambiente multiprotocolo exige que:

- Um usuário do Windows seja mapeado para um usuário do UNIX.
- Um usuário do UNIX seja mapeado para um usuário do Windows para criar a credencial do Windows quando o usuário está acessando um file system com política de acesso do Windows.

Duas propriedades são associadas ao servidor NAS em relação a usuários não mapeados:

- O usuário padrão do UNIX.
- O usuário padrão do Windows.

Quando um usuário não mapeado do Windows tenta se conectar a um file system multiprotocolo e a conta do usuário UNIX padrão é configurada para o servidor NAS, o identificador de usuário (UID) e o identificador de grupo (GID) primário do usuário UNIX padrão são usados na credencial do Windows. Da mesma forma, quando um usuário UNIX não mapeado tenta se conectar a um file system multiprotocolo e a conta de usuário padrão do Windows é configurada para o servidor NAS, a credencial do Windows do usuário padrão do Windows é usada.

NOTA: Se o usuário padrão do UNIX não for definido nos UDS (UNIX Directory Services, serviços de diretórios do UNIX), o acesso SMB será negado para usuários não mapeados. Se o usuário padrão do Windows não for encontrado no DC do Windows ou no LGDB, o acesso NFS em um file system que tem uma política de acesso do Windows será negado para usuários não mapeados.

NOTA: O usuário padrão do UNIX pode ser um nome de conta do UNIX existente e válido ou pode seguir o novo formato `@uid=`*`xxxx`*`,gid=`*`yyyy`*`@`, no qual *xxxx* e *yyyy* são os valores numéricos decimais do UID e do GID primário, respectivamente, e podem ser configurados no sistema por meio do PowerStore Manager.

Credencial do UNIX para solicitações NFS

Para manipular as solicitações NFS para um file system multiprotocolo com uma política de acesso nativo ou UNIX, uma credencial do UNIX deve ser usada. A credencial do UNIX sempre é incorporada em cada solicitação. No entanto, a credencial é limitada a 16 grupos adicionais. A propriedade `extendedUnixCredEnabled` do servidor NFS permite criar uma credencial com mais de 16 grupos. Se essa propriedade for definida, o UDS ativo será consultado com o UID para obter o GID e todos os GIDs a que pertence. Se o UID não for encontrado no UDS, a credencial do UNIX incorporada à solicitação será usada.

NOTA: Para acesso seguro de NFS, a credencial é sempre construída usando o UDS.

Credencial do UNIX para solicitações SMB

Para manipular as solicitações de SMB para um file system multiprotocolo com uma política de acesso UNIX, uma credencial do Windows deve ser criada primeiro para o usuário SMB no momento da configuração da sessão. O SID de usuário do Windows é usado para localizar o nome do AD. Esse nome é usado (opcionalmente pelo ntxmap) para encontrar um UID e GID do UNIX a partir do UDS ou arquivo local (arquivo passwd). O UID do proprietário está incluído na credencial do Windows. Ao acessar um sistema de arquivos com uma política de acesso do UNIX, o ID exclusivo do usuário é usado para consultar o UDS e criar a credencial do UNIX, processo semelhante ao da criação de uma credencial estendida para NFS. O UID é necessário para o gerenciamento de cotas.

Credencial do Windows para solicitações SMB

Para manipular as solicitações SMB para um file system multiprotocolo com uma política de acesso nativo ou Windows, uma credencial do Windows deve ser usada. A credencial do Windows para SMB deve ser criada apenas uma vez no momento da solicitação de configuração da sessão, quando o usuário se conecta.

Ao usar a autenticação Kerberos, a credencial do usuário será incluída no tíquete do Kerberos da solicitação de configuração da sessão, diferentemente do que ocorre ao usar o NT LAN Manager (NTLM). Outras informações são consultadas do DC do Windows ou do LGDB. No caso do Kerberos, a lista de SIDs de grupos adicionais é obtida do tíquete do Kerberos e da lista de SIDs. A lista de privilégios é extraída do LGDB (Local Group Database, banco de dados de grupos local). No caso do NTLM, a lista de SIDs de grupos adicionais é obtida do DC (Domain Controller, controlador de domínio) do Windows e da lista de SIDs. A lista de privilégios é extraída do LGDB (Local Group Database, banco de dados de grupos local).

Além disso, o UID correspondente e o GID primário também são recuperados do componente de mapeamento de usuários. O GID primário do UNIX é usado em vez do SID de grupo primário para a verificação de acesso.

NOTA: O NTLM é um conjunto mais antigo de protocolos de segurança exclusivo que fornece autenticação, integridade e confidencialidade para os usuários. Kerberos é um protocolo padrão aberto que fornece autenticação mais rápida pelo uso de um sistema de tíquetes. O Kerberos adiciona mais segurança que o NTLM aos sistemas de uma rede.

Credencial do Windows para solicitações NFS

A credencial do Windows é criada ou recuperada apenas quando um usuário acessa um file system por meio de uma solicitação NFS com uma política de acesso do Windows. O UID é extraído de solicitação NFS. Há um cache global de credenciais do Windows para ajudar a evitar a criação de credenciais em cada solicitação NFS com um período de retenção associado. Se a credencial do Windows for encontradas no cache, nenhuma outra ação será necessária. Se as credenciais do Windows não forem encontradas, o arquivo local ou UDS é consultado para encontrar o nome para o UID. O nome é usado, para localizar (opcionalmente, por meio do ntxmap) um usuário Windows, e a credencial é obtida do DC ou LGDB do Windows. Se o mapeamento não for encontrado, a credencial do Windows do usuário Windows padrão será usada ou o acesso será negado.

Noções básicas sobre CAVA (Common AntiVirus Agent)

O CAVA (Common Antivirus Agent) fornece uma solução de antivírus aos clientes que usam um servidor NAS. Ele usa um protocolo SMB padrão do setor em um ambiente do Microsoft Windows Server. O CAVA usa software antivírus de terceiros para identificar e eliminar vírus conhecidos antes que eles infectem os arquivos no sistema de armazenamento.

Por que o antivírus é importante?

O sistema de armazenamento é resistente à invasão de vírus por causa de sua arquitetura. O servidor NAS executa acesso a dados em tempo real com um sistema operacional incorporado. Não é possível executar programas com vírus neste sistema operacional. Embora o software do sistema operacional seja resistente a vírus, clients Windows que acessam o sistema de armazenamento também necessitam de proteção contra vírus. A proteção contra vírus em clients reduz a possibilidade de os clients armazenarem arquivos infectados no servidor e oferece proteção em caso de abertura de arquivos infectados. Essa solução antivírus consiste em uma combinação de software de sistema operacional, agente CAVA e um mecanismo antivírus de terceiros. O software CAVA e o mecanismo antivírus de terceiros devem ser instalados em um Windows Server no domínio.

Para obter informações adicionais sobre o CAVA, que faz parte do CEE (Common Event Enabler), consulte *Using the Common Event Enabler on Windows Platforms* em www.dell.com/powerstoredocs.

Assinatura de código

O PowerStore foi projetado para aceitar upgrades de software para versões novas e de patch. Uma chave mestra do GNU Privacy Guard (GPG) assina todos os pacotes do software PowerStore e é controlada pela Dell EMC. O processo de upgrade de software PowerStore verifica a assinatura do pacote de software e rejeita assinaturas inválidas que possam indicar uma violação ou corrupção. A etapa de verificação está integrada ao processo de upgrade, e a assinatura do pacote de software é verificada automaticamente durante a fase de pré-instalação.

2

Configurações de segurança de comunicação

Esta seção contém os seguintes tópicos:

Tópicos:

Uso de portas

As seções a seguir descrevem o conjunto de portas de rede e os serviços correspondentes que podem ser encontrados no equipamento. O equipamento funciona como um client de rede em várias circunstâncias, por exemplo, na comunicação com um vCenter Server. Nesses casos, o equipamento inicia a comunicação, e a infraestrutura de rede precisará dar suporte a essas conexões.

NOTA: Para obter mais informações sobre portas, consulte o artigo da base de conhecimento 542240, *PowerStore: regras de firewall de rede do cliente — portas TCP/UDP*. Vá para https://www.dell.com/support/kbdoc/en-us/542240. A ferramenta Regras de firewall de rede do cliente permite que você filtre e revise a lista de regras de firewall e as portas relevantes para a implementação do PowerStore.

Portas de rede do equipamento

A tabela a seguir descreve o conjunto de portas de rede e os serviços correspondentes que podem ser encontrados no equipamento.

Tabela 2. Portas de rede do equipamento

Porta	Serviço	Protocolo	Direção de acesso	Descrição
22	Client SSH, SupportAssist Connect Home	TCP	Bidirecional	• Permite o acesso pelo Secure Shell Protocol (se habilitado). • Obrigatória para o SupportAssist Connect Home. Se estiver fechada, as conexões de gerenciamento que usam SSH não estarão disponíveis.
25	SMTP	TCP	Saída	Permite que o equipamento envie e-mails. Se estiver fechada, as notificações por e-mail não estarão disponíveis.
26	Client SSH	TCP	Bidirecional	O acesso SSH à porta 22 é redirecionado para essa porta. Se estiver fechada, as conexões de gerenciamento que usam SSH não estarão disponíveis.
53	DNS	TCP/UDP	Saída	Usada para transmitir consultas DNS ao servidor DNS. Se estiver fechada, a resolução do nome de DNS não funcionará.
80, 8080, 8128	SupportAssist	TCP	Saída	Usado para conexão com o proxy do SupportAssist.
123	NTP	TCP/UDP	Saída	Sincronização de horário com NTP. Se estiver fechada, a hora não será sincronizada entre os equipamentos.

Tabela 2. Portas de rede do equipamento (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
443	HTTPS	TCP	Bidirecional	Tráfego HTTP seguro para o PowerStore Manager. Se estiver fechada, a comunicação com o equipamento não estará disponível.
500	IPsec (IKEv2)	UDP	Bidirecional	Para o IPSec funcionar nos firewalls, abra a porta UDP 500 e permita os números de protocolo IP 50 e 51 nos filtros de entrada e de saída do firewall. A porta UDP 500 deve estar aberta para permitir que o tráfego ISAKMP (Internet Security Association and Key Management Protocol) seja encaminhado pelos firewalls. O ID de protocolo IP 50 deve ser configurado para permitir que o tráfego IPSEc ESP (Encapsulating Security Protocol) seja encaminhado. O ID de protocolo IP 51 deve ser configurado para permitir que o tráfego AH (Authentication Header) seja encaminhado. Se estiver fechada, a conexão IPsec entre os equipamentos PowerStore estará indisponível.
587	SMTP	TCP	Saída	Permite que o equipamento envie e-mails. Se estiver fechada, as notificações por e-mail não estarão disponíveis.
3033	Importação	TCP/UDP	Saída	Necessária para importação de armazenamento a partir de sistemas legados EqualLogic Peer Storage e Compellent Storage Center.
3260	iSCSI	TCP	• Entrada para acesso a host e host do ESXi • Bidirecional para replicação • Saída para importação de armazenamento	Necessária para oferecer o seguinte acesso a serviços iSCSI: • Acesso iSCSI a host externo • Acesso iSCSI a host do ESXi externo ou incorporado ao PowerStore • Acesso entre clusters para replicação • Acesso à importação de armazenamento a partir de sistemas legados EqualLogic Peer Storage, Compellent Storage Center, Unity e VNX2 Se estiver fechada, os serviços iSCSI ficarão indisponíveis. Usada pela Mobilidade de dados para proporcionar desempenho de replicação razoável em conexão de baixa latência.
3261	Mobilidade de dados	TCP	Bidirecional	Usada pela Mobilidade de dados para proporcionar desempenho de replicação razoável em conexão de alta latência.
5353	DNS multicast (mDNS)	UDP	Bidirecional	Consulta de DNS multicast. Se estiver fechada, a resolução de nome de mDNS não funcionará.
8443	VASA, SupportAssist	TCP	• Entrada para VASA • Saída para SupportAssist	• Obrigatória para o VASA Provider que fornece o VASA 3.0. • Necessária para as funções relacionadas ao SupportAssist Connect Home.

Tabela 2. Portas de rede do equipamento (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
8443, 50443, 55443 ou 60443	Agentes de host de importação do Windows, do Linux e da VMware	TCP	Saída	Uma dessas portas deve ficar aberta ao importar armazenamento de dados a partir de sistemas de armazenamento legados.
9443	SupportAssist	TCP	Saída	Necessária para a REST API do SupportAssist relacionada ao Connect Home.

Portas de rede do equipamento relacionadas a arquivo

A tabela a seguir descreve o conjunto de portas de rede e os serviços correspondentes que podem ser encontrados no equipamento relacionado a arquivo.

NOTA: As portas de saída são efêmeras.

Tabela 3. Portas de rede do equipamento relacionadas a arquivo

Porta	Serviço	Protocolo	Direção de acesso	Descrição
20	FTP	TCP	Saída	Porta usada para transferências de dados FTP. Esta porta pode ser aberta ativando o FTP. A autenticação é realizada na porta 21 e definida pelo protocolo FTP.
21	FTP	TCP	Entrada	A porta 21 é a porta de controle na qual o serviço FTP monitora as solicitações recebidas de FTP.
22	SFTP	TCP	Entrada	Permite notificações de alerta por meio de SFTP (FTP por SSH). O SFTP é um protocolo client/servidor. Os usuários podem utilizar o SFTP para fazer transferências de arquivos em um equipamento da sub-rede local. Também fornece conexão de controle FTP de saída. Se estiver fechada, o FTP não estará disponível.
53	DNS	TCP/UDP	Saída	Usada para transmitir consultas DNS ao servidor DNS. Se estiver fechada, a resolução do nome de DNS não funcionará. Necessária para SMB v1.
88	Kerberos	TCP/UDP	Saída	Necessária para serviços de autenticação Kerberos.
111	Ligação RPC (para namespaces SDNAS; caso contrário, serviço de host)	TCP/UDP	Bidirecional	É aberta pelo portmapper padrão ou pelo serviço rpcbind, sendo um serviço de rede auxiliar do equipamento. Não pode ser interrompido. Por definição, se um sistema client tiver conectividade de rede com a porta, ele poderá consultá-lo. Nenhuma autenticação é realizada.
123	NTP	UDP	Saída	Sincronização de horário com NTP. Se estiver fechada, a hora não será sincronizada entre os equipamentos.
135	Microsoft RPC	TCP	Entrada	Vários objetivos para o Microsoft Client. Também é usado para protocolo de gerenciamento de dados da rede.
137	Microsoft Netbios WINS	UDP; TCP/UDP	Entrada; Saída	O Serviço de nome do NETBIOS está associado aos serviços de compartilhamento

Tabela 3. Portas de rede do equipamento relacionadas a arquivo (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
				de arquivos SMB do equipamento, sendo um componente central desse recurso (Wins). Se desativada, esta porta desativa todos os serviços relacionados a SMB.
138	Microsoft Netbios BROWSE	UDP	Saída	O Serviço de Datagrama do NETBIOS está associado aos serviços de compartilhamento de arquivos SMB do equipamento, sendo um componente central desse recurso. Somente o serviço Procurar é utilizado. Se desativada, essa porta desativa a capacidade de procura.
139	Microsoft CIFS	TCP	Bidirecional	O Serviço de sessão NETBIOS está associado aos serviços de compartilhamento de arquivos CIFS do equipamento, sendo um componente central desse recurso. Se os serviços SMB estiverem habilitados, essa porta estará aberta. É necessária especificamente para SMB v1.
389	LDAP	TCP/UDP	Saída	Consultas LDAP não seguras. Se estiver fechada, as consultas não seguras de autenticação LDAP não estarão disponíveis. O LDAP seguro pode ser configurado como alternativa.
445	Microsoft SMB	TCP	Entrada	SMB (no controlador de domínio) e porta de conectividade SMB para clients Windows 2000 e posteriores. Clientes com acesso legítimo aos serviços SMB do equipamento devem ter conectividade de rede com a porta para operação continuada. Se desativada, esta porta desativa todos os serviços relacionados a SMB. Se a porta 139 também estiver desativada, o compartilhamento de arquivos SMB (Server Message Block) estará desativado.
464	Kerberos	TCP/UDP	Saída	Necessária para SMB e serviços de autenticação Kerberos.
500	IPsec (IKEv2)	UDP	Bidirecional	Para o IPSec funcionar nos firewalls, abra a porta UDP 500 e permita os números de protocolo IP 50 e 51 nos filtros de entrada e de saída do firewall. A porta UDP 500 deve estar aberta para permitir que o tráfego ISAKMP (Internet Security Association and Key Management Protocol) seja encaminhado pelos firewalls. O ID de protocolo IP 50 deve ser configurado para permitir que o tráfego IPSEc ESP (Encapsulating Security Protocol) seja encaminhado. O ID de protocolo IP 51 deve ser configurado para permitir que o tráfego AH (Authentication Header) seja encaminhado. Se estiver fechada, a conexão IPsec entre os equipamentos PowerStore estará indisponível.
636	LDAPS	TCP/UDP	Saída	Consultas LDAP seguras. Se estiver fechada, a autenticação LDAP segura não estará disponível.

Tabela 3. Portas de rede do equipamento relacionadas a arquivo (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
1234	NFS mountd	TCP/UDP	Bidirecional	Usada para o serviço de montagem, que é um componente central do serviço NFS (versões 2, 3 e 4).
2000	SSHD	TCP	Entrada	SSHD para capacidade de serviço (opcional)
2049	E/S de NFS	TCP/UDP	Bidirecional	Usada para fornecer serviços NFS.
3268	LDAP	UDP	Saída	Consultas LDAP não seguras. Se estiver fechada, as consultas não seguras de autenticação LDAP não estarão disponíveis.
4000	STATD para NFSv3	TCP/UDP	Bidirecional	Usada para fornecer serviços statd NFS. statd é o monitor de status de bloqueio de arquivo NFS e funciona em conjunto com lockd para oferecer funções de recuperação e falha para NFS. Se estiver fechada, serviços statd NAS estarão indisponíveis.
4001	NLMD para NFSv3	TCP/UDP	Bidirecional	Usada para fornecer serviços lockd NFS. lockd é o daemon de bloqueio de arquivos NFS. Ele processa solicitações de bloqueio de clients NFS e funciona em conjunto com o daemon statd. Se estiver fechada, serviços lockd NAS estarão indisponíveis.
4002	RQUOTAD para NFSv3	TCP/UDP; UDP	Entrada; Saída	Usada para fornecer serviços rquotad NFS. O daemon de rquotad fornece informações de cota a clientes NFS que montaram um sistema de arquivos. Se estiver fechada, serviços rquotad NAS estarão indisponíveis.
4003	XATTRPD (atributo de arquivo estendido)	TCP/UDP	Entrada	Necessária para gerenciar atributos de arquivos em um ambiente multiprotocolo.
4658	PAX (arquivo do servidor NAS)	TCP	Entrada	O PAX é um protocolo de arquivo de equipamento que funciona com formatos padrão de fita UNIX.
8888	RCPD (caminho de dados de replicação)	TCP	Entrada	Usada pelo replicador (no local secundário). O replicador deixa esta porta aberta assim que dados precisam ser replicados. Após iniciado, não há como interromper este serviço.
10000	NDMP	TCP	Entrada	• Permite controlar backup e recuperação de um servidor NDMP (Network Data Management Protocol, protocolo de gerenciamento de dados de rede) por meio de um aplicativo de backup em rede, sem instalar software de terceiros no servidor. Em um equipamento, o servidor NAS funciona como um servidor NDMP. • O serviço NDMP poderá ser desabilitado se um backup em fita NDMP não for usado. • O serviço NDMP é autenticado com um par de nome de usuário/senha. O nome de usuário é configurável. A documentação do NDMP descreve como configurar a senha para uma série de ambientes.

Tabela 3. Portas de rede do equipamento relacionadas a arquivo (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
[10500,10531]	Intervalo reservado NDMP para portas dinâmicas NDMP	TCP	Entrada	Para sessões de backup/restauração de três vias, os servidores NAS usam portas 10500 para 10531.
12228	Serviço de verificação de vírus	TCP	Saída	Necessária para o serviço de verificação de vírus.

Portas de rede relacionadas a equipamentos modelo PowerStore X

A tabela a seguir descreve o conjunto de portas de rede e os serviços correspondentes que podem ser encontrados nos equipamentos PowerStore X model.

Tabela 4. Portas de rede relacionadas a equipamentos PowerStore X model

Porta	Serviço	Protocolo	Direção de acesso	Descrição
22	Servidor SSH	TCP	Entrada	Permite o acesso pelo Secure Shell Protocol (se habilitado). Se estiver fechada, as conexões de gerenciamento que usam SSH não estarão disponíveis.
80, 9000	vSphere Web Access	TCP	Entrada	Acesso para o plug-in vSphere Update Manager Web Client do vSphere Web Client.
427	SLP (Service Location Protocol) CIM	TCP/UDP	Bidirecional	Para localizar servidores CIM, o client CIM usa o SLPv2, que é a versão 2 do protocolo SLP (Service Location Protocol).
443	vSphere Web Client	TCP	Entrada	Usada para conexões com clients.
902	NFC (Network File Copy), VMware vCenter, vSphere Web Client	TCP	• Bidirecional para NFC • Saída para VMware vCenter • Entrada para vSphere Web Client	• O NFC oferece um serviço FTP com reconhecimento de tipo de arquivo para componentes do vSphere. Por padrão, o ESXi usa o NFC para operações como cópia e movimentação de dados entre datastores. • Agente do VMware vCenter • Usada no vSphere Web Client para conexões com clients.
5900, 5901, 5902, 5903, 5904	Protocolo RFB	TCP	Entrada	Acesso remoto a interfaces gráficas de usuário, como VNC.
5988	Servidor CIM (Common Information Model)	TCP	Entrada	Servidor para CIM.
5989	Servidor seguro CIM	TCP	Entrada	Servidor para CIM.
6999	Roteador virtual lógico distribuído do NSX, rabbitmqproxy	UDP	• Bidirecional para o serviço de roteador virtual distribuído do NSX • Saída para rabbitmqproxy	• Para o serviço de roteador virtual distribuído do NSX, a porta de firewall associada a esse serviço é aberta quando VIBs do NSX são instalados e o módulo VDR é criado. Se nenhuma instância do VDR estiver associada ao host, a porta não precisará ser aberta. • Para rabbitmqproxy, um proxy em execução no host do ESXi. Esse proxy permite que os aplicativos executados dentro de máquinas virtuais se comuniquem com os agentes AMQP que

Tabela 4. Portas de rede relacionadas a equipamentos PowerStore X model (continuação)

Porta	Serviço	Protocolo	Direção de acesso	Descrição
				estão em execução no domínio de rede do vCenter. A máquina virtual não precisa estar na rede, ou seja, não é necessária uma NIC. Os endereços IP da conexão de saída devem incluir pelo menos os agentes em uso ou futuros. É possível adicionar agentes posteriormente para scale-up.
8000	vMotion	TCP	Bidirecional	Necessária para a migração de máquina virtual com o vMotion. Os hosts do ESXi escutam na porta 8000 para conexões TCP de hosts remotos do ESXi para tráfego do vMotion.
8100, 8200, 8300	Fault Tolerance	TCP/UDP	Bidirecional	Usada para tráfego entre hosts do vSphere Fault Tolerance (FT).
8301, 8302	DVSSync	UDP	Bidirecional	As portas DVSSync são usadas para sincronizar estados de portas virtuais distribuídas entre hosts que tenham o recurso de repetição/gravação do VMware FT habilitado. Somente hosts que executam máquinas virtuais primárias ou de backup devem ter essas portas abertas. Em hosts que não estejam usando o VMware FT, essas portas não precisam ser abertas.
9080	Filtro de E/S	TCP	Saída	Usada pelo recurso de armazenamento de filtros de E/S.
31031	vSphere Replication, VMware Site Recovery Manager	TCP	Saída	Usada para tráfego de replicação contínua pelo vSphere Replication e pelo VMware Site Recovery Manager.
44046	vSphere Replication, VMware Site Recovery Manager	TCP	Saída	Usada para tráfego de replicação contínua pelo vSphere Replication e pelo VMware Site Recovery Manager.

3

Auditoria

Este tópico contém as seguintes informações:

Tópicos:

Auditoria

A auditoria oferece uma visualização histórica da atividade dos usuários no sistema. Um usuário com função Administrador, Administrador de segurança ou Administrador de armazenamento pode usar a REST API para pesquisar e visualizar eventos de alteração de configuração no sistema. Esses eventos auditados não estão relacionados apenas à segurança. Todas as operações do conjunto (ou seja, POST/PATCH/DELETE) são registradas para auditoria.

É possível usar outras interfaces, como a CLI e a interface do usuário do PowerStore Manager, para pesquisar e visualizar eventos de auditoria.

4

Configurações da segurança de dados

Esta seção contém os seguintes tópicos:

Tópicos:

Criptografia de dados em repouso

A criptografia de dados em repouso (D@RE) no PowerStore utiliza unidades com criptografia automática (SEDS, Self-Encrypting Drives) FIPS 140-2 validadas para armazenamento primário (SSD NVMe, SCM NVMe e SSD SAS). O dispositivo para cache NVRAM é criptografado, mas não validado com FIPS 140-2 neste momento.

A criptografia é realizada dentro de cada unidade antes que os dados sejam gravados na mídia. Isso protege os dados na unidade contra roubo ou perda e tentativas de ler a unidade diretamente por meio da desconstrução física. A criptografia também oferece um meio de apagar informações contidas em uma unidade, com rapidez e segurança, para garantir que elas não possam ser recuperadas. Além de proteger contra ameaças relacionadas à remoção física da mídia, a mídia pode ser prontamente reutilizada destruindo-se a chave de criptografia usada para proteger os dados anteriormente armazenados nessa mídia.

A leitura dos dados criptografados exige uma chave de autenticação para a SED desbloquear a unidade. Somente as SEDs autenticadas serão desbloqueadas e acessadas. Uma vez que a unidade esteja desbloqueada, a unidade SED descriptografa os dados criptografados de volta para o formato original.

O equipamento PowerStore deve conter todas as SEDs. Se você tentar adicionar a um equipamento uma unidade que não seja com criptografia automática, ele gerará um erro. Além disso, não é permitido ter equipamentos não criptografados em um cluster criptografado.

Ativação da criptografia

O recurso de criptografia de dados em repouso nos equipamentos PowerStore é definido na fábrica. Em todos os países que permitem a importação de um equipamento que dá suporte para criptografia, a criptografia é ativada por padrão. Uma vez ativada, a criptografia não pode ser desativada. Em todos os países que não permitem a importação de um equipamento que dá suporte para criptografia, o recurso de criptografia de dados em repouso fica desativado.

NOTA: Equipamentos que não dão suporte para criptografia de dados em repouso não podem ser colocados em um cluster com equipamentos criptografados.

Status de criptografia

O status de criptografia de um equipamento é informado nos seguintes níveis:

- Nível do cluster
- Nível do equipamento
- Nível da unidade

O status de criptografia no nível do cluster simplesmente indica se um equipamento está habilitado para criptografia. Ele não está relacionado ao status da unidade.

O status de criptografia de um equipamento é exibido como um dos seguintes:

- Encrypted – O recurso de criptografia está ativado no equipamento.
- Unencrypted – O recurso de criptografia não tem suporte no equipamento.
- Encrypting — Exibido durante o processo de ativação da criptografia. Quando o processo de criptografia é concluído com sucesso, o status de criptografia no nível do cluster é exibido como criptografado.

O status de criptografia no nível de unidade é informado para cada unidade de um equipamento e exibido como uma das seguintes opções:

- Encrypted – A unidade está criptografada. Esse é o estado típico de uma unidade em um equipamento com o recurso de criptografia.
- Encrypting — O equipamento está ativando a criptografia na unidade. Este status pode ser visto durante a ativação inicial da criptografia em um equipamento ou durante a inclusão de novas unidades em um equipamento configurado.
- Disabled – A unidade não pode ter criptografia ativada devido a restrições de importação específicas do país. Se alguma unidade relatar esse status, todas as unidades do cluster também relatarão o mesmo status.
- Unknown — O equipamento ainda não tentou ativar a criptografia na unidade. Este status pode ser visto durante a ativação inicial da criptografia em um equipamento ou durante a inclusão de novas unidades em um equipamento configurado.
- Unsupported – A unidade não é compatível com criptografia.
- Foreign – A unidade é compatível, mas foi bloqueada por outro equipamento. Ela precisa ser desativada para poder ser usada.

Gerenciamento de chaves

Um serviço de gerenciamento de chaves (KMS) incorporado é executado no nó ativo de cada equipamento PowerStore. Este serviço gerencia o armazenamento de lockbox do arquivo de keystore local para dar suporte ao backup automático de chaves de criptografia para unidades de inicialização e do sistema. Ele também controla o processo de bloqueio e desbloqueio da unidade com criptografia automática (SED) no equipamento e é responsável por gerenciar conteúdo do keystore local para o equipamento. O arquivo de keystore local é criptografado com uma chave AES de 256 bits, e o armazenamento de lockbox do arquivo de keystore aproveita a tecnologia BSAFE da RSA.

O KMS gera automaticamente uma chave de autenticação aleatória para SEDs durante a inicialização do equipamento. Cada unidade tem uma chave de autenticação exclusiva, incluindo aquelas que são adicionadas ao equipamento depois, e essa chave é usada nos processos de bloqueio e desbloqueio de SED. Uma chave de criptografia de chaves criptografa chaves de autenticação e de criptografia no armazenamento do arquivo de keystore e em trânsito no equipamento. As chaves de criptografia de mídia são armazenadas no hardware dedicado das SEDs e não podem ser acessadas. Quando a criptografia está ativada, todas as chaves de autenticação são armazenadas no equipamento.

Arquivo de backup de keystore

O KMS é compatível com a criação e o download de um backup fora do equipamento do arquivo de arquivamento de keystore. O backup fora do equipamento reduz as chances de uma perda de chave catastrófica, o que pode tornar um equipamento ou cluster inutilizável. Se um determinado equipamento não estiver disponível quando um backup de keystore do cluster for iniciado, a operação geral será bem-sucedida, mas será emitido um aviso informando que o backup não contém os arquivos de keystore de todos os equipamentos do cluster e que a operação deverá ser repetida quando o equipamento off-line estiver disponível.

NOTA: O equipamento principal de um cluster contém um arquivo de arquivamento de keystore do cluster que contém uma cópia de backups de keystore de cada equipamento detectado no cluster, inclusive do equipamento principal.

Quando ocorrem alterações na configuração de um sistema dentro do cluster que resultam em alterações no keystore, é recomendável que você gere um novo arquivo de arquivamento de keystore para download. Somente uma operação de download de backup do arquivo de arquivamento de keystore pode ser executada por vez.

NOTA: É altamente recomendável que você faça download do arquivo de arquivamento de keystore gerado para uma localização externa segura. Se os arquivos de keystore de um sistema se tornarem corrompidos e inacessíveis, o sistema entrará no modo de serviço. Nesse caso, o arquivo de arquivamento de keystore e um contrato de serviço serão necessários para resolução.

É necessária uma função Administrador ou Administrador de armazenamento para fazer backup do arquivo de arquivamento de keystore. Para fazer backup do arquivo de arquivamento de keystore, clique em **Settings** e, em **Security**, selecione **Encryption**. Na página **Encryption**, em **Lockbox backup**, clique em **Download Keystore Backup**.

NOTA: Para restaurar o backup do keystore em caso de falha, entre em contato com seu provedor de serviços.

Reutilizar uma unidade em um equipamento com criptografia ativada

Sobre esta tarefa

Uma unidade com criptografia automática (SED) é bloqueada quando um equipamento é inicializado ou quando é inserida em um equipamento já inicializado. A unidade não pode ser usada em outro sistema sem antes ser desbloqueada. A unidade bloqueada fica inutilizável quando inserida em outro equipamento e seu status de criptografia é exibido como `Foreign` no novo equipamento. A unidade pode ser reutilizada para o novo equipamento, mas todos os dados existentes nela serão perdidos.

Para realocar uma unidade com status de criptografia `Foreign` em um equipamento, faça o seguinte:

Etapas

1. Registre o PSID (Physical Security ID, identificação de segurança física) localizado na etiqueta na parte traseira da unidade. O PSID deve ser fornecido como parte do processo de reutilização.
2. No PowerStore Manager, clique em **Hardware**, selecione o equipamento e selecione o card **Hardware**.
3. Selecione a unidade que será reutilizada.

   O **Encryption Status** da unidade deve ser `Foreign`.
4. Clique em **Repurpose Drive**.
   O controle deslizante **Repurpose Drive** é exibido.
5. Digite o PSID da unidade e clique em **Apply**.

Resultados

A unidade será reutilizada no equipamento como uma nova unidade e o status de criptografia mudará para `Encrypted` quando o processo de reutilização for concluído.

Substituindo uma gaveta de base e os nós de um sistema com criptografia ativada

Um contrato de serviço é necessário para substituir um base enclosure e os nodes de um equipamento com criptografia ativada.

Redefinindo um equipamento com as configurações de fábrica

O script de serviço `svc_factory_reset` retorna um cluster com um único equipamento ao estado entregue pela fábrica, excluindo todos os dados do usuário e configurações persistentes.

Em clusters com vários equipamentos, não é possível executar `svc_factory_reset` nos equipamentos secundários. Em seu lugar, deve ser executado o script de serviço `svc_remove_appliance`. Esse script retorna um equipamento secundário ao estado de fábrica, excluindo todos os dados do usuário e configurações persistentes. Quando apenas o equipamento principal permanece no cluster, é possível executar `svc_factory_reset` para redefini-lo.

NOTA: É recomendável que esses scripts sejam executados somente por um provedor de serviços qualificado.

Para obter mais informações sobre esses scripts, consulte o *PowerStore Service Scripts Guide*.

5

Secure serviceability settings

Este tópico contém as seguintes informações:

Tópicos:

Descrição operacional do SupportAssist™

O recurso SupportAssist fornece uma conexão baseada em IP que permite que o Suporte Dell EMC receba arquivos de erro e alertas do equipamento e solucione problemas de maneira remota, tornando a resolução rápida e eficiente.

NOTA: É altamente recomendável que você habilite o recurso SupportAssist para agilizar o diagnóstico de problemas, solucionar problemas e acelerar o tempo de resolução. Se você não habilitar o recurso SupportAssist, talvez precise coletar informações do equipamento manualmente para ajudar o Suporte Dell EMC a solucionar os problemas no equipamento. Além disso, o recurso SupportAssist precisa estar habilitado no equipamento para que os dados sejam enviados ao CloudIQ. Para obter mais informações sobre o CloudIQ, acesse www.dell.com/support. Depois de fazer log-in, localize a página **Product Support** referente ao CloudIQ.

SupportAssist e segurança

O recurso SupportAssist emprega várias camadas de segurança em todas as etapas do processo de conectividade remota para garantir que você e a Dell EMC possam usar a solução com segurança:

- Todas as notificações enviadas à Dell EMC originam-se de seu local, e nunca de fontes externas, e são mantidas seguras com o uso da criptografia AES (Advanced Encryption Standard) de 256 bits.
- A arquitetura baseada em IP integra-se à sua atual infraestrutura e preserva a segurança do ambiente.
- As comunicações entre seu local e a Dell EMC são autenticadas bilateralmente usando certificados digitais da RSA®.
- Somente profissionais do serviço de atendimento ao cliente da Dell EMC verificados por autenticação baseada em dois fatores podem fazer download dos certificados digitais necessários para visualizar notificações do seu local.
- O aplicativo opcional Policy Manager do SupportAssist v3 permite conceder ou restringir o acesso ao Suporte Dell EMC com base em diretrizes e requisitos exclusivos e inclui um log de auditoria detalhado.

Gerenciamento do SupportAssist

O recurso SupportAssist pode ser gerenciado com o PowerStore Manager ou a REST API. Você pode habilitar ou desabilitar o serviço e fornecer as informações relevantes necessárias para a opção de SupportAssist selecionada.

NOTA: As opções **Gateway Connect with remote assist** e **Gateway Connect without remote assist** para SupportAssist centralizado não dão suporte a HA (High Availability, alta disponibilidade). Essas opções não oferecem o recurso de failover a um cluster ativo de HA do SupportAssist. Quando um equipamento PowerStore é implementado em um único servidor de gateway do cluster de HA, que é a única opção de configuração disponível, não há nenhum recurso de failover para o servidor de gateway sobrevivente no cluster. Se o servidor de gateway de HA ao qual o equipamento está conectado ficar inativo, o equipamento interromperá a transferência dos arquivos de saída, como arquivos de call home e CloudIQ, para o Suporte Dell EMC. A conectividade

de entrada do SupportAssist para acesso remoto ao equipamento ainda funcionará utilizando o servidor de gateway HA sobrevivente no cluster. Além disso, as opções SupportAssist **Gateway Connect with remote assist** e **Gateway Connect without remote assist** só devem ser configuradas no equipamento principal designado do sistema.

O equipamento propriamente dito não implementa nenhuma política. Se você precisar de mais controle sobre o acesso remoto ao equipamento, use o Policy Manager para definir permissões de autorização. O componente de software Policy Manager pode ser instalado em um servidor fornecido pelo cliente. Ele controla o acesso remoto aos dispositivos, mantém um log de auditoria de conexões remotas e dá suporte a operações de transferência de arquivos. Você pode controlar quem acessa o equipamento, o que é acessado e quando isso ocorre. Para obter mais informações sobre o Policy Manager, acesse www.dell.com/support. Depois de fazer log-in, localize a página **Support by Product** aplicável e pesquise o link para a documentação técnica específica do produto SupportAssist.

Comunicação com o SupportAssist

NOTA: O SupportAssist não pode ser habilitado em modelos PowerStore configurados com IPv6 para a rede de gerenciamento porque não é compatível com IPv6. Além disso, não é permitido reconfigurar a rede de gerenciamento de IPv4 para IPv6 quando o SupportAssist está configurado em um cluster.

Para que o recurso SupportAssist funcione, é necessário acesso a um servidor DNS.

O **Connection Status** do SupportAssist indica o estado da conexão entre o PowerStore e os serviços de suporte de back-end da Dell EMC, assim como a qualidade de serviço da conexão. O estado da conexão é determinado em até cinco minutos, e a qualidade de serviço da conexão é determinada em até 24 horas. O **Connection Status** da conexão pode ser uma das opções a seguir, com base em qualquer um dos equipamentos no cluster:

- `Unavailable` – Os dados de conectividade não estão disponíveis. Você pode ter perdido o contato com um equipamento ou o SupportAssist acabou de ser habilitado e não há dados suficientes para determinar o estado.
- `Disabled` – O SupportAssist não foi habilitado.
- `Not connected` – A conectividade foi perdida. Foram detectadas cinco falhas de keepalive consecutivas.
- `Reconnecting` – O PowerStore está tentando se reconectar após a perda de conectividade. São necessárias cinco solicitações consecutivas de keepalive bem-sucedidas para fazer a transição de volta para o status Connected.

O **Connection Status** da conexão pode ser uma das opções a seguir, com base na média de todos os equipamentos no cluster quando o PowerStore estiver conectado aos serviços de suporte de back-end da Dell EMC:

- `Evaluating` – A qualidade de serviço da conexão será indeterminada durante as primeiras 24 horas após a primeira inicialização do SupportAssist.
- `Good` – 80% ou mais das solicitações consecutivas de keepalive foram bem-sucedidas.
- `Fair` – Entre 50% e 80% das solicitações consecutivas de keepalive foram bem-sucedidas.
- `Poor` – Menos de 50% das solicitações consecutivas de keepalive foi bem-sucedida.

Opções de SupportAssist

O recurso SupportAssist fornece uma conexão baseada em IP que permite que o Suporte Dell EMC receba arquivos de erro e alertas do sistema e solucione problemas de maneira remota, tornando a resolução rápida e eficiente.

Estas são as opções de SupportAssist disponíveis para enviar informações do equipamento ao Suporte Dell EMC e realizar o processo de solução de problemas remotamente:

- Gateway Connect without remote access — Para SupportAssist centralizado, é executada em um servidor de gateway fornecido pelo cliente com transferência de arquivos bidirecional, o que inclui:
  - Call-homes
  - Suporte para CloudIQ
  - Notificações de software
  - Download do ambiente operacional/firmware do Suporte Dell EMC para o cluster

  O servidor de gateway do SupportAssist é o ponto único de entrada e saída para todas as atividades do SupportAssist baseadas em IP referentes aos equipamentos associados ao gateway.
- Gateway Connect with remote access — Para SupportAssist distribuído, é executada em um servidor de gateway fornecido pelo cliente com a mesma transferência de arquivos bidirecional que a opção Gateway Connect without remote access, juntamente com o acesso remoto para a equipe do Suporte Dell EMC.
- Direct Connect without remote access — Para SupportAssist distribuído que é executado em equipamentos individuais com a mesma transferência de arquivos bidirecional que a opção Gateway Connect without remote access.

- Direct Connect with remote access — Para SupportAssist distribuído que é executado em equipamentos individuais com a mesma transferência de arquivos bidirecional que a opção Gateway Connect without remote access, juntamente com o acesso remoto para a equipe do Suporte Dell EMC.

Existe uma outra opção (Disabled) que, embora disponível, não é recomendável. Se você selecionar esta opção, o Suporte Dell EMC não receberá notificações sobre problemas no equipamento. Talvez você precise coletar informações do equipamento manualmente para ajudar os representantes do suporte a solucionar os problemas.

Opções do SupportAssist Gateway Connect

O SupportAssist Gateway Connect é executado em um servidor de gateway. Quando você seleciona a opção **Gateway Connect without remote access** ou **Gateway Connect with remote access**, o equipamento é adicionado a outros equipamentos em um cluster do SupportAssist. O cluster reside em uma conexão segura única comum (centralizada) entre os servidores do Suporte Dell EMC e um servidor de gateway fora do array. O servidor de gateway é o ponto único de entrada e saída para todas as atividades do Dell EMC SupportAssist baseadas em IP referentes aos equipamentos associados ao gateway.

O servidor de gateway é um aplicativo de solução de suporte remoto instalado em um ou mais servidores dedicados fornecidos pelo cliente. Ele funciona como um intermediário para a comunicação entre os equipamentos associados e a empresa Dell EMC.

Para obter mais informações sobre o gateway do SupportAssist, acesse a página do produto SupportAssist no site Suporte Dell (www.dell.com/support).

Para configurar o equipamento a fim de usar a opção **Gateway Connect without remote access** ou **Gateway Connect with remote access** para o SupportAssist, você precisa informar o endereço IP e o número de porta (9443 é o padrão) do servidor de gateway. Além disso, verifique se a porta está aberta entre o servidor de gateway e o equipamento.

NOTA: O servidor de gateway deve estar ativo e em execução antes de você configurar o equipamento para usá-lo. Os equipamentos só podem ser adicionados ao gateway usando o PowerStore Manager. Se o equipamento for adicionado a partir do servidor de gateway, ele parecerá estar conectado, mas não enviará as informações do sistema.

Opções do SupportAssist Direct Connect

O SupportAssist Direct Connect é executado diretamente no nó principal de cada equipamento. Em um cluster, cada equipamento estabelecerá sua própria conexão com o Suporte Dell EMC. O tráfego não é roteado por meio do equipamento principal de um cluster. No entanto, o SupportAssist só pode ser gerenciado no nível do cluster, ou seja, todas as alterações são aplicadas a todos os equipamentos do cluster.

Habilite e configure o SupportAssist Direct Connect na página **Support Assist**, que pode ser acessada em **Settings** e está listada em **Support** no PowerStore Manager. Essas ações configuram o equipamento para usar uma conexão segura entre ele e o Suporte Dell EMC. Você pode selecionar uma das seguintes opções de conectividade de serviço remoto para o SupportAssist Direct Connect:

- **Direct Connect without remote access**
- **Direct Connect with remote access**

Quando você seleciona a opção **Direct Connect without remote access** e aceita o acordo de licença de usuário final (EULA), o equipamento configura uma conexão segura entre ele e o Suporte Dell EMC. Esta opção ativa o recurso de conectividade para transferência de arquivos bidirecional para/do Suporte Dell EMC. Se for o caso, você pode configurar a conexão do equipamento com um servidor proxy associado (opcional). Se necessário, posteriormente você pode fazer upgrade para a configuração Direct Connect with remote access.

Quando você seleciona a opção **Direct Connect with remote access** e aceita o acordo de licença de usuário final (EULA), o equipamento configura uma conexão segura entre ele e o Suporte Dell EMC. Esta opção ativa o recurso de conectividade do serviço de acesso remoto com o equipamento para/do Suporte Dell EMC, junto com a transferência de arquivos bidirecional. Se for o caso, você pode configurar a conexão do equipamento com o Policy Manager (opcional) e quaisquer servidores proxy associados (opcional) usando o PowerStore Manager.

Quando um novo equipamento é adicionado a um cluster já existente, o novo equipamento detecta as configurações do SupportAssist para o cluster e é automaticamente configurado de acordo. Se o SupportAssist Direct Connect estiver ativado, ele será habilitado automaticamente no novo equipamento. Não é necessário executar nenhuma ação a mais. Caso não seja possível ativar o SupportAssist Direct Connect, isso não impedirá que o processo de adição do equipamento seja realizado.

Requisitos do SupportAssist Gateway Connect

Os seguintes requisitos são aplicáveis às implementações **Gateway Connect without remote access** e **Gateway Connect with remote access** do SupportAssist:

- O tráfego de rede (HTTPS) deve ser permitido na porta 9443 (ou na porta especificada pelo cliente, se diferente) entre o equipamento e o servidor de gateway do SupportAssist.
- A versão do SupportAssist deve ser 4.0.5 ou 3.38.

NOTA: Nunca adicione nem remova um equipamento do servidor de gateway manualmente. Só adicione ou remova um equipamento de um servidor de gateway usando o assistente de configuração do SupportAssist do PowerStore Manager.

Requisitos do SupportAssist Direct Connect

O requisito a seguir é aplicável às implementações **Direct Connect without remote access** e **Direct Connect with remote access** do SupportAssist:

- O tráfego de rede (HTTPS) deve ser permitido nas portas 443 e 8443 (saída) para o Suporte Dell EMC. Falha ao abrir a porta 8443 resulta em impacto significativo no desempenho (30% a 45%). Falha na abertura de ambas as portas pode resultar em um atraso na solução de problemas com o dispositivo final.

O requisito a seguir é aplicável apenas à implementação **Direct Connect with remote access** do SupportAssist:

- Se a implementação incluir um Policy Manager para aumentar o controle sobre o acesso remoto ao equipamento, indique isso ao configurar o recurso SupportAssist.

Configurando o SupportAssist

Configure o SupportAssist para um equipamento usando um dos seguintes meios:

- Assistente de configuração inicial – Uma interface do usuário que orienta na configuração inicial do PowerStore Manager e prepara o sistema para uso.
- **SupportAssist** – Uma página de configurações que pode ser acessada pelo PowerStore Manager (clique em **Settings** e, em **Support**, selecione **SupportAssist**).
- Servidor de REST API – A interface de aplicativo que pode receber solicitações da REST API para definir configurações do SupportAssist. Para obter mais informações sobre a REST API, consulte PowerStore REST API Reference Guide.

Para determinar o status do recurso SupportAssist, clique em **Settings** e, em **Support**, selecione **SupportAssist** no PowerStore Manager.

Configurar o SupportAssist

Sobre esta tarefa

Para configurar o SupportAssist usando o PowerStore Manager, faça o seguinte:

NOTA: Para mudar a opção **Direct Connect with remote access** para **Direct Connect without remote access** ou **Gateway Connect**, você vai precisar da ajuda da equipe do Suporte Dell EMC.

Etapas

1. Clique em **Settings** e, em **Support**, selecione **SupportAssist**.
2. Se o status do SupportAssist for exibido como desativado, clique no ícone de controle **SupportAssist** para ativar o SupportAssist.
   Embora o recurso SupportAssist possa ser desativado, isso não é recomendado.
   O botão deverá se mover para a direita e passar a indicar `Enabled`. No entanto, o **Connection Status** só será alterado depois que você especificar as informações de configuração necessárias e clicar em **Apply**.
3. Em **SupportAssist**, a caixa de seleção **Connect to CloudIQ** fica marcada por padrão. Se você não quiser enviar arquivos ao CloudIQ, desmarque a caixa de seleção; caso contrário, deixe a caixa de seleção marcada.
4. Na lista **Type**, selecione a opção de SupportAssist que você pretende usar.

5. Dependendo do tipo de opção de SupportAssist selecionado, execute um destes procedimentos:
   - Para as opções **Gateway Connect without remote access** ou **Gateway Connect with remote access**:
     - Especifique o endereço IP do servidor de gateway.
       NOTA: O servidor de gateway deve estar ativo e em execução antes de você configurar o equipamento para usá-lo.
     - Se a porta que será usada para a conexão com o servidor de gateway for diferente do padrão (9443), use os controles para selecionar o número da porta que será usada na rede.
   - Para a opção **Direct Connect without remote access**:
     - Se sua conexão de rede usa um servidor proxy, especifique o endereço IP dele.
       NOTA: O servidor proxy deve estar ativo e em execução antes de você configurar o sistema para usá-lo.
     - Use os controles para selecionar o número da porta que será usada para a conexão com o servidor proxy na rede.
   - Para a opção **Direct Connect with remote access**:
     - Se sua conexão de rede usa um servidor proxy, especifique o endereço IP dele.
       NOTA: O servidor proxy deve estar ativo e em execução antes de você configurar o equipamento para usá-lo.
     - Use os controles para selecionar o número da porta que será usada para a conexão com o servidor proxy na rede.
     - Se você pretende usar um Policy Manager para controlar o acesso remoto ao sistema, especifique o endereço IP do Policy Manager.
       NOTA: O Policy Manager deve estar ativo e em execução antes de você configurar o equipamento para usá-lo.
     - Se a porta que será usada para a conexão com o Policy Manager for diferente do padrão (9443), digite o número da porta que será usada na rede.
6. Dependendo do tipo de opção de SupportAssist selecionado, execute um destes procedimentos:
   - Para as opções **Direct Connect without remote access** ou **Direct Connect with remote access**, vá para a próxima etapa.
   - Para as opções **Gateway Connect without remote access** ou **Gateway Connect with remote access**, selecione **Test Connection** para verificar o status da conexão com o servidor de gateway.

   NOTA: Se Connectivity Status permanecer como `Transitioning` e não mudar depois de alguns minutos (o tempo que você deve levar para testar a conectividade), entre em contato com o Suporte on-line.
7. Selecione **Send Test Alert** para enviar um alerta de teste ao Suporte Dell EMC para garantir conectividade completa.
8. Certifique-se de que as informações de contato exibidas estejam precisas. Corrija quaisquer informações incorretas ou desatualizadas.
   Suas informações de contato do SupportAssist são fundamentais para receber resposta rápida a problemas de suporte e devem estar corretas e atualizadas.
9. Selecione **Apply** para manter as informações de configuração do SupportAssist.

A

Conjuntos de codificações TLS

Este apêndice contém as seguintes informações:

Tópicos:

Conjunto de codificações TLS compatíveis

Um conjunto de codificações define um conjunto de tecnologias para proteger as comunicações TLS:

- Algoritmo de troca de chaves (como a chave secreta usada para criptografar os dados é transmitida do client ao servidor). Exemplos: chave RSA ou Diffie-Hellman (DH)
- Método de autenticação (como os hosts podem autenticar a identidade dos hosts remotos). Exemplos: certificado RSA, certificado DSS ou nenhuma autenticação
- Codificação de criptografia (como criptografar os dados). Exemplos: AES (256 ou 128 bits)
- Algoritmo de hash (dados de confirmação que fornecem uma maneira de determinar se os dados foram alterados). Exemplos: SHA-2 ou SHA-1

Os conjuntos de codificações compatíveis combinam todos esses itens.

A lista a seguir apresenta os nomes OpenSSL dos conjuntos de codificações TLS para o equipamento e as portas associadas.

Tabela 5. Conjuntos de codificações TLS padrão/compatíveis aceitos no equipamento

Conjuntos de codificações	Protocolos	Portas
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	TLSv1.2	443, 8443
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_128_GCM_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_CBC_SHA256	TLSv1.2	443, 8443
TLS_RSA_WITH_AES_256_GCM_SHA384	TLSv1.2	443, 8443