



Gerenciar chaves de segurança

SANtricity 11.9

NetApp
December 16, 2024

Índice

- Gerenciar chaves de segurança 1
 - Altere a chave de segurança 1
 - Mude do gerenciamento de chaves externas para internas 2
 - Editar as configurações do servidor de gerenciamento de chaves 3
 - Faça backup da chave de segurança 3
 - Valide a chave de segurança 4
 - Desbloqueie unidades ao usar o gerenciamento de chaves internas 4
 - Desbloqueie unidades ao usar o gerenciamento de chaves externas 6

Gerenciar chaves de segurança


Altere a chave de segurança

A qualquer momento, você pode substituir uma chave de segurança por uma nova chave. Talvez seja necessário alterar uma chave de segurança nos casos em que você tenha uma potencial violação de segurança em sua empresa e queira garantir que funcionários não autorizados não possam acessar os dados das unidades.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **alterar chave**.

A caixa de diálogo alterar chave de segurança é aberta.

3. Introduza as informações nos seguintes campos.
 - **Defina um identificador de chave de segurança** — (apenas para chaves de segurança internas.) Aceite o valor padrão (nome da matriz de armazenamento e carimbo de data/hora, que é gerado pelo firmware da controladora) ou insira seu próprio valor. Pode introduzir até 189 caracteres alfanuméricos sem espaços, pontuação ou símbolos.
 -  Os caracteres adicionais são gerados automaticamente e são anexados a ambas as extremidades da cadeia de caracteres inserida. Os caracteres gerados ajudam a garantir que o identificador é exclusivo.
 - **Defina uma frase-passe/digite novamente a frase-passe** — em cada um desses campos, insira sua frase-passe. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
 - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
 - Um número (um ou mais).
 - Um caractere não alfanumérico, como !, *, at (um ou mais).
4. Para chaves de segurança externas, se você quiser excluir a chave de segurança antiga quando a nova for criada, marque a caixa de seleção "Excluir chave de segurança atual..." na parte inferior da caixa de diálogo.



Certifique-se de gravar suas entradas para uso posterior — se você precisar mover uma unidade habilitada para segurança da matriz de armazenamento, você deve saber o identificador e a frase-passe para desbloquear os dados da unidade.

5. Clique em **alterar**.

A nova chave de segurança substitui a chave anterior, que não é mais válida.



O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador.

6. Grave o identificador da chave, a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

Depois de terminar

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

Mude do gerenciamento de chaves externas para internas

Você pode alterar o método de gerenciamento de segurança de unidade de um servidor de chaves externo para o método interno usado pelo storage array. A chave de segurança definida anteriormente para o gerenciamento de chaves externas é então usada para o gerenciamento de chaves internas.

Sobre esta tarefa

Nesta tarefa, desative o gerenciamento de chaves externas e baixe uma nova cópia de backup para o host local. A chave existente ainda é usada para o Drive Security, mas será gerenciada internamente na matriz de armazenamento.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Desativar Gerenciamento de chaves externas**.

A caixa de diálogo Desativar gerenciamento de chaves externas é aberta.

3. Em **defina uma frase-passe/insira novamente a frase-passe**, insira e confirme uma frase-passe para o backup da chave. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
 - Uma letra maiúscula (uma ou mais). Tenha em mente que a frase-passe é sensível a maiúsculas e minúsculas.
 - Um número (um ou mais).
 - Um caráter não alfanumérico, como !, *, at (um ou mais).



Certifique-se de gravar suas entradas para uso posterior. Se você precisar mover uma unidade habilitada para segurança do storage, você deve saber o identificador e a frase-passe para desbloquear os dados da unidade.

4. Clique em **Desativar**.

A chave de cópia de segurança é transferida para o seu anfitrião local.

5. Grave o identificador da chave, a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

Resultados

O Drive Security agora é gerenciado internamente por meio do storage array.

Depois de terminar

Você deve validar a chave de segurança para se certificar de que o arquivo de chave não está corrompido.

Editar as configurações do servidor de gerenciamento de chaves

Se você tiver configurado o gerenciamento de chaves externas, poderá exibir e editar as configurações do servidor de gerenciamento de chaves a qualquer momento.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Exibir/Editar Configurações do servidor de gerenciamento de chaves**.
3. Edite informações nos seguintes campos:
 - **Endereço do servidor de gerenciamento de chaves** — Digite o nome de domínio totalmente qualificado ou o endereço IP (IPv4 ou IPv6) do servidor usado para o gerenciamento de chaves.
 - **Número da porta de gerenciamento de chaves** — Digite o número da porta usada para as comunicações KMIP (Key Management Interoperability Protocol).

Opcional: você pode incluir outro servidor de chaves clicando em **Add Key Server**.

4. Clique em **Salvar**.

Faça backup da chave de segurança

Depois de criar ou alterar uma chave de segurança, você pode criar uma cópia de backup do arquivo de chave caso o original seja corrompido.

Sobre esta tarefa

Esta tarefa descreve como fazer backup de uma chave de segurança criada anteriormente. Durante este procedimento, você cria uma nova frase-passe para o backup. Essa frase-passe não precisa corresponder à frase-passe usada quando a chave original foi criada ou alterada pela última vez. A frase-passe é aplicada apenas ao backup que você está criando.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Backup Key**.

A caixa de diálogo fazer backup da chave de segurança é aberta.

3. Nos campos **Definir uma frase-passe/voltar a introduzir frase-passe**, introduza e confirme uma frase-passe para esta cópia de segurança.

O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:

- Uma letra maiúscula (uma ou mais)
- Um número (um ou mais)
- Um caráter não alfanumérico, como !, *, at (um ou mais)



Certifique-se de gravar sua entrada para uso posterior. Você precisa da frase-passe para acessar o backup dessa chave de segurança.

4. Clique em **Backup**.

Um backup da chave de segurança é baixado para seu host local e a caixa de diálogo **Confirm/Record Security Key Backup** (confirmar/gravar backup da chave de segurança*) será aberta.



O caminho para o arquivo de chave de segurança baixado pode depender do local de download padrão do navegador.

5. Grave sua frase-passe em um local seguro e clique em **Fechar**.

Depois de terminar

Você deve validar a chave de segurança de backup.

Valide a chave de segurança

Você pode validar a chave de segurança para se certificar de que ela não foi corrompida e para verificar se você tem uma frase-passe correta.

Sobre esta tarefa

Esta tarefa descreve como validar a chave de segurança criada anteriormente. Esta é uma etapa importante para se certificar de que o arquivo de chave não está corrompido e a frase-passe está correta, o que garante que você possa acessar mais tarde os dados da unidade se mover uma unidade habilitada para segurança de uma matriz de armazenamento para outra.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **Validar chave**.

A caixa de diálogo Validar chave de segurança é aberta.

3. Clique em **Procurar** e selecione o ficheiro de chave (por exemplo, `drivesecurity.slk`).
4. Introduza a frase-passe associada à chave selecionada.

Quando você seleciona um arquivo de chave válido e uma frase-passe, o botão **Validar** fica disponível.

5. Clique em **Validar**.

Os resultados da validação são exibidos na caixa de diálogo.

6. Se os resultados mostrarem "a chave de segurança validada com êxito", clique em **Fechar**. Se for apresentada uma mensagem de erro, siga as instruções sugeridas apresentadas na caixa de diálogo.

Desbloqueie unidades ao usar o gerenciamento de chaves internas

Se você configurou o gerenciamento de chaves internas e depois mover unidades habilitadas para segurança de um storage array para outro, será necessário atribuir novamente a chave de segurança ao novo storage array para obter acesso aos dados criptografados nas unidades.

Antes de começar

- Na matriz de origem (a matriz onde você está removendo as unidades), você exportou grupos de volume e removeu as unidades. No array de destino, você instalou novamente as unidades.



A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no "[Base de dados de Conhecimento da NetApp](#)". Certifique-se de seguir as instruções apropriadas para arrays mais recentes gerenciados pelo System Manager ou para sistemas legados.

- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
- Você deve saber a chave de segurança que está associada às unidades que deseja desbloquear.
- O arquivo de chave de segurança está disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar o System Manager). Se você estiver movendo as unidades para um storage array gerenciado por um sistema diferente, será necessário mover o arquivo de chave de segurança para esse cliente de gerenciamento.

Sobre esta tarefa

Quando você usa o gerenciamento de chaves internas, a chave de segurança é armazenada localmente no storage array. Uma chave de segurança é uma cadeia de caracteres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas da matriz e instaladas em outra, elas não podem operar até que você forneça a chave de segurança correta.



Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Este tópico descreve como desbloquear dados quando o gerenciamento de chaves *internas* é usado. Se você usou o gerenciamento de chaves *externas*, "[Desbloqueie unidades ao usar o gerenciamento de chaves externas](#)" consulte . Se você estiver executando uma atualização de controladora e estiver trocando todos os controladores pelo hardware mais recente, siga etapas diferentes conforme descrito no centro de documentação e-Series e SANtricity, em "[Desbloquear unidades](#)".

Depois de reinstalar unidades habilitadas para segurança em outro array, esse array descobre as unidades e exibe uma condição de "precisa de atenção" junto com um status de "chave de segurança necessária". Para desbloquear os dados da unidade, selecione o ficheiro da chave de segurança e introduza a frase-passe da chave. (Esta frase-passe não é a mesma que a senha do administrador da matriz de armazenamento.)

Se outras unidades habilitadas para segurança estiverem instaladas no novo storage array, elas poderão usar uma chave de segurança diferente da que você está importando. Durante o processo de importação, a chave de segurança antiga é usada apenas para desbloquear os dados das unidades que você está instalando. Quando o processo de desbloqueio é bem-sucedido, as unidades recém-instaladas são recodificadas para a chave de segurança da matriz de armazenamento de destino.

Passos

1. Selecione **Definições > sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **desbloquear unidades seguras**.

A caixa de diálogo desbloquear unidades seguras abre-se. Todas as unidades que exigem uma chave de

segurança são mostradas na tabela.

3. **Opcional:** passe o Mouse sobre um número de unidade para ver a localização da unidade (número de prateleira e número de compartimento).
4. Clique em **Procurar** e selecione o arquivo de chave de segurança que corresponde à unidade que deseja desbloquear.

O arquivo de chave selecionado aparece na caixa de diálogo.

5. Introduza a frase-passe associada a este ficheiro de chave.

Os caracteres inseridos são mascarados.

6. Clique em **Unlock**.

Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibe: "As unidades seguras associadas foram desbloqueadas."

Resultados

Quando todas as unidades estiverem bloqueadas e, em seguida, desbloqueadas, cada controlador na matriz de armazenamento será reiniciado. No entanto, se já houver algumas unidades desbloqueadas no storage de armazenamento de destino, os controladores não serão reinicializados.

Depois de terminar

No array de destino (o array com as unidades recém-instaladas), agora você pode importar grupos de volume.



A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no "[Base de dados de Conhecimento da NetApp](#)".

Desbloqueie unidades ao usar o gerenciamento de chaves externas

Se você configurou o gerenciamento de chaves externas e depois mover unidades habilitadas para segurança de um storage array para outro, será necessário atribuir novamente a chave de segurança ao novo storage array para obter acesso aos dados criptografados nas unidades.

Antes de começar

- Na matriz de origem (a matriz onde você está removendo as unidades), você exportou grupos de volume e removeu as unidades. No array de destino, você instalou novamente as unidades.



A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no "[Base de dados de](#)

[Conhecimento da NetApp](#)". Certifique-se de seguir as instruções apropriadas para arrays mais recentes gerenciados pelo System Manager ou para sistemas legados.

- O recurso Segurança da unidade deve estar ativado. Caso contrário, uma caixa de diálogo não é possível criar chave de segurança será aberta durante esta tarefa. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
- Você deve saber o endereço IP e o número da porta do servidor de gerenciamento de chaves.
- Você tem um arquivo de certificado de cliente assinado para os controladores do storage array e copiou esse arquivo para o host onde está acessando o System Manager. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP (Key Management Interoperability Protocol).
- Você deve recuperar um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando o System Manager. Um certificado do servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, de modo que o storage array possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.



Para obter mais informações sobre o certificado do servidor, consulte a documentação do servidor de gerenciamento de chaves.

Sobre esta tarefa

Quando você usa o gerenciamento de chaves externas, a chave de segurança é armazenada externamente em um servidor projetado para proteger chaves de segurança. Uma chave de segurança é uma cadeia de caracteres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas da matriz e instaladas em outra, elas não podem operar até que você forneça a chave de segurança correta.



Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa de um servidor de gerenciamento de chaves. Este tópico descreve como desbloquear dados quando o gerenciamento de chaves *external* é usado. Se você usou o gerenciamento de chaves *internas*, ["Desbloqueie unidades ao usar o gerenciamento de chaves internas"](#) consulte . Se você estiver executando uma atualização de controladora e estiver trocando todos os controladores pelo hardware mais recente, siga etapas diferentes conforme descrito no centro de documentação e-Series e SANtricity, em ["Desbloquear unidades"](#).

Depois de reinstalar unidades habilitadas para segurança em outro array, esse array descobre as unidades e exibe uma condição de "precisa de atenção" junto com um status de "chave de segurança necessária". Para desbloquear os dados da unidade, importe o ficheiro da chave de segurança e introduza a frase-passe da chave. (Esta frase-passe não é a mesma que a senha do administrador da matriz de armazenamento.) Durante esse processo, você configura o storage array para usar um servidor de gerenciamento de chaves externo e, em seguida, a chave segura será acessível. É necessário fornecer informações de Contato do servidor para que a matriz de armazenamento se conecte e recupere a chave de segurança.

Se outras unidades habilitadas para segurança estiverem instaladas no novo storage array, elas poderão usar uma chave de segurança diferente da que você está importando. Durante o processo de importação, a chave de segurança antiga é usada apenas para desbloquear os dados das unidades que você está instalando. Quando o processo de desbloqueio é bem-sucedido, as unidades recém-instaladas são recodificadas para a chave de segurança da matriz de armazenamento de destino.

Passos

1. Selecione **Definições > sistema**.

2. Em **Gerenciamento de chaves de segurança**, selecione **criar chave externa**.
3. Conclua o assistente com as informações e certificados de conexão pré-requisito.
4. Clique em **Test Communication** para garantir o acesso ao servidor de gerenciamento de chaves externo.
5. Selecione **Unlock Secure Drives**.

A caixa de diálogo desbloquear unidades seguras abre-se. Todas as unidades que exigem uma chave de segurança são mostradas na tabela.

6. **Opcional:** passe o Mouse sobre um número de unidade para ver a localização da unidade (número de prateleira e número de compartimento).
7. Clique em **Procurar** e selecione o arquivo de chave de segurança que corresponde à unidade que deseja desbloquear.

O arquivo de chave selecionado aparece na caixa de diálogo.

8. Introduza a frase-passe associada a este ficheiro de chave.

Os caracteres inseridos são mascarados.

9. Clique em **Unlock**.

Se a operação de desbloqueio for bem-sucedida, a caixa de diálogo exibe: "As unidades seguras associadas foram desbloqueadas."

Resultados

Quando todas as unidades estiverem bloqueadas e, em seguida, desbloqueadas, cada controlador na matriz de armazenamento será reiniciado. No entanto, se já houver algumas unidades desbloqueadas no storage de armazenamento de destino, os controladores não serão reinicializados.

Depois de terminar

No array de destino (o array com as unidades recém-instaladas), agora você pode importar grupos de volume.



A função Exportar/Importar não é suportada na interface de usuário do System Manager; você deve usar a interface de linha de comando (CLI) para exportar/importar um grupo de volumes para um storage array diferente.

Instruções detalhadas para migrar um grupo de volumes são fornecidas no ["Base de dados de Conhecimento da NetApp"](#).

Informações sobre direitos autorais

Copyright © 2024 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.