Gerenciar chaves de segurança

SANtricity software

NetApp
March 17, 2026

Índice

Gerenciar chaves de segurança

Alterar uma chave de segurança no SANtricity System Manager

A qualquer momento, você pode substituir uma chave de segurança por uma nova. Você pode precisar trocar uma chave de segurança em casos de potencial violação de segurança na sua empresa e deseja garantir que pessoas não autorizadas não possam acessar os dados das unidades.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Alterar chave**.

   A caixa de diálogo Alterar chave de segurança é aberta.

3. Insira informações nos campos a seguir.
   - **Defina um identificador de chave de segurança** — (Apenas para chaves de segurança internas.) Aceite o valor padrão (nome do array de storage e carimbo de data/hora, que é gerado pelo firmware do controlador) ou insira seu próprio valor. Você pode inserir até 189 caracteres alfanuméricos, sem espaços, pontuação ou símbolos.

     Caracteres adicionais são gerados automaticamente e anexados às duas extremidades da sequência de caracteres que você inserir. Os caracteres gerados ajudam a garantir que o identificador seja único.

   - **Definir uma frase secreta/Inserir frase secreta novamente** — Em cada um destes campos, insira sua frase secreta. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:
     - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
     - Um número (um ou mais).
     - Um caractere não alfanumérico, como !, *, @ (um ou mais).
4. Para chaves de segurança externas, se você quiser excluir a chave de segurança antiga quando a nova for criada, selecione a caixa de seleção "Excluir chave de segurança atual…" na parte inferior da caixa de diálogo.

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

5. Clique em **Change**.

   A nova chave de segurança sobrescreve 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. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida,

clique em **Fechar**.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Altere do gerenciamento de chaves externas para internas no SANtricity System Manager

Você pode alterar o método de gerenciamento da Segurança da Unidade de um servidor de chaves externo para o método interno usado pelo array de storage. A chave de segurança previamente definida para o gerenciamento de chaves externas passa a ser usada para o gerenciamento de chaves internas.

Sobre esta tarefa

Nesta tarefa, você desativa o gerenciamento de chaves externas e baixa uma nova cópia de backup para o seu host local. A chave existente ainda é usada para Drive Security, mas será gerenciada internamente no array de storage.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Desativar External Key Management**.

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

3. Em **Definir uma frase secreta/Reinserir frase secreta**, insira e confirme uma frase secreta para o backup da chave. O valor pode ter entre 8 e 32 caracteres e deve incluir cada um dos seguintes:

   - Uma letra maiúscula (ou mais). Lembre-se de que a senha diferencia maiúsculas de minúsculas.
   - Um número (um ou mais).
   - Um caractere não alfanumérico, como !, *, @ (um ou mais).

   

   Certifique-se de registrar suas anotações para uso posterior. Se precisar mover uma unidade com segurança habilitada do array de storage, você deverá saber o identificador e a frase secreta para desbloquear os dados da unidade.

4. Clique em **Desativar**.

   A chave de backup é baixada para o seu host local.

5. Anote o identificador da chave, a frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

Resultados

A segurança da unidade agora é gerenciada internamente pelo array de storage.

Depois que você terminar

Você deve validar a chave de segurança para garantir que o arquivo de chave não esteja corrompido.

Editar as configurações do servidor de gerenciamento de chaves no SANtricity System Manager

Se você configurou o gerenciamento de chaves externo, pode visualizar e editar as configurações do servidor de gerenciamento de chaves a qualquer momento.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Visualizar/Editar configurações do servidor de gerenciamento de chaves**.
3. Edite as informações nos seguintes campos:
   - **Endereço do servidor de gerenciamento de chaves** — Insira o 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** — Insira o número da porta usado para as comunicações do Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP).

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

Faça backup das chaves de segurança no SANtricity System Manager

Após 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 que você criou anteriormente. Durante este procedimento, você cria uma nova frase secreta para o backup. Essa frase secreta não precisa ser igual à frase secreta usada quando a chave original foi criada ou alterada pela última vez. A frase secreta se aplica somente ao backup que você está criando.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Back Up Key**.

   A caixa de diálogo Back Up Security Key é aberta.
3. Nos campos **Definir uma frase secreta/Redigitar frase secreta**, insira e confirme uma frase secreta para este backup.

   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 caractere não alfanumérico, como !, *, @ (um ou mais)

Anote sua entrada para uso posterior. Você precisa da senha para acessar o backup desta chave de segurança.

4. Clique em **Back Up**.

   Um backup da chave de segurança é baixado para o seu host local e, em seguida, a caixa de diálogo **Confirmar/Registrar Backup da Chave de Segurança** é aberta.

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

5. Anote sua frase secreta em um local seguro e clique em **Fechar**.

Depois que você terminar

Você deve validar a chave de segurança de backup.

Validar chave de segurança no SANtricity System Manager

Você pode validar a chave de segurança para garantir que ela não foi corrompida e para verificar se você possui uma frase secreta correta.

Sobre esta tarefa

Esta tarefa descreve como validar a chave de segurança que você criou anteriormente. Este é um passo importante para garantir que o arquivo da chave não esteja corrompido e que a senha esteja correta, o que assegura que você poderá acessar os dados da unidade posteriormente, caso mova uma unidade com segurança habilitada de um array de storage para outro.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Validar chave**.

   A caixa de diálogo Validate Security Key é aberta.

3. Clique em **Procurar**, e selecione o arquivo de chave (por exemplo, `drivesecurity.slk`).
4. Digite a frase secreta associada à chave que você selecionou.

   Ao selecionar um arquivo de chave válido e uma senha válida, o botão **Validar** ficará disponível.

5. Clique em **Validar**.

   Os resultados da validação são exibidos na caixa de diálogo.

6. Se os resultados mostrarem "A chave de segurança foi validada com sucesso", clique em **Fechar**. Se uma mensagem de erro for exibida, siga as instruções sugeridas na caixa de diálogo.

Desbloquear unidades ao usar o gerenciamento de chaves internas no SANtricity System Manager

Se você configurou o gerenciamento de chaves internas e, posteriormente, moveu

unidades com segurança habilitada de um array de storage para outro, você deve reatribuir a chave de segurança ao novo array de storage para obter acesso aos dados criptografados nas unidades.

Antes de começar

- No array de origem (o array onde você está removendo as unidades), você exportou os grupos de volumes e removeu as unidades. No array de destino, você reinstalou 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 volume para um array de storage diferente.

  Instruções detalhadas para migrar um grupo de volume são fornecidas no "Base 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 Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.
- Você deve saber a chave de segurança associada às unidades que deseja desbloquear.
- O arquivo de chave de segurança está disponível no cliente de gerenciamento (o sistema com navegador usado para acessar o System Manager). Se você estiver movendo as unidades para um array de storage gerenciado por um sistema diferente, será necessário mover o arquivo de chave de segurança para esse cliente de gerenciamento.

Sobre esta tarefa

Ao usar o gerenciamento de chaves internas, a chave de segurança é armazenada localmente no array de storage. Uma chave de segurança é uma sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas do array e instaladas em outro, 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 a partir de um servidor de gerenciamento de chaves. Este tópico descreve o desbloqueio de dados quando o gerenciamento de chaves *interno* é utilizado. Se você utilizou o gerenciamento de chaves *externo*, consulte "Desbloqueie unidades ao usar o gerenciamento de chaves externas". Se você estiver realizando uma atualização do controlador e substituindo todos os controladores pelo hardware mais recente, você deve seguir etapas diferentes, conforme descrito no centro de documentação E-Series e SANtricity, em "Desbloquear unidades".

Após reinstalar unidades com segurança habilitada em outro array, esse array detecta as unidades e exibe a condição "Requer Atenção", juntamente com o status "Chave de Segurança Necessária". Para desbloquear os dados da unidade, você seleciona o arquivo da chave de segurança e insere a frase secreta da chave. (Essa frase secreta não é a mesma que a senha de administrador do array de storage.)

Se outras unidades com recursos de segurança habilitados estiverem instaladas no novo array de storage, elas poderão usar uma chave de segurança diferente daquela 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 for concluído com sucesso, as unidades recém-instaladas serão reassociadas à chave de segurança do array de storage de destino.

Passos

1. Selecione o menu: configurações [Sistema].
2. Em **Gerenciamento de chaves de segurança**, selecione **Desbloquear unidades seguras**.

   A caixa de diálogo Desbloquear unidades seguras é aberta. Todas as unidades que exigem uma chave de segurança são exibidas na tabela.

3. **Opcional:** passe o cursor do mouse sobre o número da unidade para ver a localização da unidade (número da prateleira e número da baia).
4. Clique em **Procurar** e, em seguida, selecione o arquivo de chave de segurança que corresponde à unidade que você deseja desbloquear.

   O arquivo de chave que você selecionou aparece na caixa de diálogo.

5. Digite a frase secreta associada a este arquivo de chave.

   Os caracteres que você inserir são mascarados.

6. Clique em **Unlock**.

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

Resultados

Quando todas as unidades são bloqueadas e depois desbloqueadas, cada controlador no array de storage será reinicializado. No entanto, se já houver algumas unidades desbloqueadas no array de storage de destino, os controladores não serão reinicializados.

Depois que você 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 volume para um array de storage diferente.

Instruções detalhadas para migrar um grupo de volume são fornecidas em "Base de Conhecimento da NetApp".

Desbloquear unidades ao usar o gerenciamento de chaves externas no SANtricity System Manager

Se você configurou o gerenciamento de chaves externas e, posteriormente, moveu unidades com segurança habilitada de um array de storage para outro, você deve reatribuir a chave de segurança ao novo array de storage para obter acesso aos dados criptografados nas unidades.

Antes de começar

- No array de origem (o array onde você está removendo as unidades), você exportou os grupos de volumes e removeu as unidades. No array de destino, você reinstalou 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 volume para um array de storage diferente.

Instruções detalhadas para migrar um grupo de volume são fornecidas no "Base 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 Drive Security deve estar ativado. Caso contrário, uma caixa de diálogo Cannot Create Security Key será exibida durante esta tarefa. Se necessário, entre em contato com o fornecedor do seu array de storage para obter instruções sobre como ativar o recurso Drive Security.
- Você deve saber o endereço IP e o número da porta do servidor de gerenciamento de chaves.
- Você possui um arquivo de certificado de cliente assinado para os controladores do array de storage e copiou esse arquivo para o host onde está acessando System Manager. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações do Key Management Interoperability Protocol (KMIP).
- Você deve obter um arquivo de certificado do servidor de gerenciamento de chaves e, em seguida, copiar esse arquivo para o host onde você está acessando System Manager. Um certificado de servidor de gerenciamento de chaves valida o servidor de gerenciamento de chaves, então o array de storage pode confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

Para obter mais informações sobre o certificado do servidor, consulte a documentação do seu key management server.

Sobre esta tarefa

Ao usar 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 sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. Quando as unidades são fisicamente removidas do array e instaladas em outro, 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 a partir de um servidor de gerenciamento de chaves. Este tópico descreve o desbloqueio de dados quando o gerenciamento de chaves *externo* é utilizado. Se você utilizou o gerenciamento de chaves *interno*, consulte "Desbloqueie unidades ao usar o gerenciamento interno de chaves". Se você estiver realizando uma atualização do controlador e substituindo todos os controladores pelo hardware mais recente, deve seguir etapas diferentes, conforme descrito na E-Series e na Central de Documentação do SANtricity, em "Desbloquear unidades".

Após reinstalar unidades com segurança habilitada em outro array, esse array detecta as unidades e exibe uma condição "Requer Atenção" juntamente com um status de "Chave de Segurança Necessária". Para desbloquear os dados da unidade, você importa o arquivo da chave de segurança e insere a frase secreta da chave. (Essa frase secreta não é a mesma que a senha de administrador do array de storage.) Durante esse processo, você configura o array de storage para usar um servidor externo de gerenciamento de chaves e então a chave de segurança ficará acessível. Você é obrigado a fornecer as informações de contato do servidor para que o array de storage possa se conectar e recuperar a chave de segurança.

Se outras unidades com recursos de segurança habilitados estiverem instaladas no novo array de storage, elas poderão usar uma chave de segurança diferente daquela 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 for concluído com sucesso, as unidades recém-instaladas serão reassociadas à chave de segurança do array de storage de destino.

Passos

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

   A caixa de diálogo Desbloquear unidades seguras é aberta. Todas as unidades que exigem uma chave de segurança são exibidas na tabela.

6. **Opcional:** passe o cursor do mouse sobre o número da unidade para ver a localização da unidade (número da prateleira e número da baia).
7. Clique em **Procurar** e, em seguida, selecione o arquivo de chave de segurança que corresponde à unidade que você deseja desbloquear.

   O arquivo de chave que você selecionou aparece na caixa de diálogo.

8. Digite a frase secreta associada a este arquivo de chave.

   Os caracteres que você inserir são mascarados.

9. Clique em **Unlock**.

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

Resultados

Quando todas as unidades são bloqueadas e depois desbloqueadas, cada controlador no array de storage será reinicializado. No entanto, se já houver algumas unidades desbloqueadas no array de storage de destino, os controladores não serão reinicializados.

Depois que você 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 volume para um array de storage diferente.

Instruções detalhadas para migrar um grupo de volume são fornecidas em "Base de Conhecimento da NetApp".

Informações sobre direitos autorais

Informações sobre marcas comerciais