Segurança de unidade

SANtricity software

NetApp
March 17, 2026

This PDF was generated from https://docs.netapp.com/pt-br/e-series-santricity-119/sm-settings/overview-drive-security.html on March 17, 2026. Always check docs.netapp.com for the latest.

Índice

Segurança de unidade

Saiba mais sobre segurança de unidades em SANtricity System Manager

Você pode configurar Drive Security e o gerenciamento de chaves na página Security Key Management.

O que é Drive Security?

Drive Security é um recurso que impede o acesso não autorizado a dados em drives com segurança habilitada quando removidos do array de storage. Esses drives podem ser Full Disk Encryption (FDE) drives ou Federal Information Processing Standard (FIPS) drives. Quando drives FDE ou FIPS são fisicamente removidos do array, eles não podem operar até serem instalados em outro array, momento em que os drives ficarão em um estado de Security Locked até que a security key correta seja fornecida. Uma *security key* é uma sequência de caracteres compartilhada entre esses tipos de drives e os controladores em um array de storage.

Saiba mais:

- "Como funciona o recurso Drive Security"
- "Como funciona o gerenciamento de chaves de segurança"
- "Terminologia de segurança de drive"

Como faço para configurar o gerenciamento de chaves?

Para implementar Drive Security, você deve ter unidades FDE ou FIPS instaladas no array. Para configurar o gerenciamento de chaves para essas unidades, acesse **Settings › Sistema › Security key management**, onde 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. Por fim, habilite Drive Security para pools e grupos de volumes selecionando "secure-capable" nas configurações do volume.

Saiba mais:

- "Criar chave de segurança interna"
- "Criar chave de segurança externa"
- "Criar pool manualmente"
- "Criar grupos de volumes"

Como faço para desbloquear unidades?

Se você configurou o gerenciamento de chaves e, posteriormente, move 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.

Saiba mais:

- "Desbloqueie unidades ao usar o gerenciamento interno de chaves"

- "Desbloqueie unidades ao usar o gerenciamento de chaves externas"

Informações relacionadas

Saiba mais sobre tarefas relacionadas à gestão de chaves:

- "Use certificados assinados por CA para autenticação com um servidor de gerenciamento de chaves"
- "Fazer backup da chave de segurança"

Conceitos

Como funciona o recurso Drive Security no SANtricity System Manager

Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS).

Quando esses discos são usados com o recurso Drive Security, eles exigem uma chave de segurança para acesso aos seus dados. Quando os discos são fisicamente removidos do array, eles não podem operar até serem instalados em outro array, momento em que ficarão em estado de Security Locked até que a chave de segurança correta seja fornecida.

Como implementar Drive Security

Para implementar a Segurança do Drive, execute as seguintes etapas.

1. Equipe seu array de storage com unidades compatíveis com segurança, sejam elas FDE drives ou FIPS drives. (Para volumes que exigem suporte a FIPS, use somente FIPS drives. Misturar FIPS drives e FDE drives em um grupo de volume ou pool fará com que todas as unidades sejam tratadas como FDE drives. Além disso, um FDE drive não pode ser adicionado ou usado como reserva em um grupo de volume ou pool composto apenas por FIPS drives.)
2. Crie uma chave de segurança, que é uma sequência de caracteres compartilhada pelo controlador e pelas unidades para acesso de leitura/gravação. 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. Para o gerenciamento de chaves externas, a autenticação deve ser estabelecida com o servidor de gerenciamento de chaves.
3. Ative a segurança de unidade para pools e grupos de volume:
   - Crie um pool ou grupo de volume (procure por **Sim** na coluna **Secure-capable** na tabela Candidates).
   - Selecione um pool ou grupo de volume ao criar um novo volume (procure por **Sim** ao lado de **Compatível com segurança** na tabela de candidatos a pool e grupo de volume).

Como o Drive Security funciona no nível da unidade

Uma unidade com recursos de segurança, seja FDE ou FIPS, criptografa os dados durante as gravações e os descriptografa durante as leituras. Essa criptografia e descriptografia não afetam o desempenho nem o fluxo de trabalho do usuário. Cada unidade possui sua própria chave de criptografia exclusiva, que nunca pode ser transferida da unidade.

O recurso Drive Security oferece uma camada extra de proteção para unidades com capacidade de segurança. Quando grupos de volumes ou pools nessas unidades são selecionados para Drive Security, as

unidades procuram uma chave de segurança antes de permitir o acesso aos dados. Você pode ativar o Drive Security para pools e grupos de volumes a qualquer momento, sem afetar os dados existentes na unidade. No entanto, não é possível desativar o Drive Security sem apagar todos os dados da unidade.

Como o Drive Security funciona no nível do array de storage

Com o recurso Drive Security, você cria uma chave de segurança que é compartilhada entre as unidades habilitadas para segurança e os controladores em um array de storage. Sempre que a energia das unidades for desligada e ligada, as unidades habilitadas para segurança mudam para o estado Security Locked até que o controlador aplique a chave de segurança.

Se uma unidade com segurança habilitada for removida do array de storage e reinstalada em um array de storage diferente, ela ficará em estado de Segurança Bloqueada. A unidade realocada procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você aplica a chave de segurança do array de storage de origem. Após um processo de desbloqueio bem-sucedido, a unidade realocada passará a usar a chave de segurança já armazenada no array de storage de destino, e o arquivo de chave de segurança importado não será mais necessário.

Para gerenciamento interno de chaves, a chave de segurança propriamente dita é armazenada no controlador em um local inacessível. Ela não está em formato legível por humanos, nem é acessível ao usuário.

Como o Drive Security funciona no nível de volume

Ao criar um pool ou grupo de volume a partir de unidades com recursos de segurança, você também pode habilitar Drive Security para esses pools ou grupos de volume. A opção Drive Security torna as unidades e os grupos de volume e pools associados secure-*enabled*.

Tenha em mente as seguintes diretrizes antes de criar grupos de volume e pools com segurança habilitada:

- Os grupos de volumes e pools devem ser compostos inteiramente por drives com capacidade de segurança. (Para volumes que exigem suporte a FIPS, use apenas drives FIPS. Misturar drives FIPS e FDE em um grupo de volume ou pool fará com que todos os drives sejam tratados como drives FDE. Além disso, um drive FDE não pode ser adicionado ou usado como reserva em um grupo de volume ou pool totalmente FIPS.)
- Os grupos de volume e os pools devem estar em um estado ideal.

Como funciona o gerenciamento de chaves de segurança no SANtricity System Manager

Ao implementar o recurso de Drive Security, as unidades com segurança habilitada (FIPS ou FDE) exigem uma chave de segurança para acesso aos dados. Uma chave de segurança é uma sequência de caracteres compartilhada entre esses tipos de unidades e os controladores em um array de storage.

Sempre que a alimentação das unidades é desligada e ligada, as unidades com segurança habilitada entram no estado Bloqueado por Segurança até que o controlador aplique a chave de segurança. Se uma unidade com segurança habilitada for removida do array de storage, os dados da unidade são bloqueados. Quando a unidade é reinstalada em um array de storage diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você deve aplicar a chave de segurança original.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento interno de chaves na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

Gerenciamento interno de chaves

As chaves internas são mantidas e "ocultas" em um local inacessível na memória persistente do controlador. Para implementar o gerenciamento de chaves internas, execute as seguintes etapas:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Crie uma chave de segurança interna, o que envolve definir um identificador e uma frase secreta. O identificador é uma sequência de caracteres associada à chave de segurança e é armazenado no controlador e em todas as unidades associadas à chave. A frase secreta é usada para criptografar a chave de segurança para fins de backup. Para criar uma chave interna, vá para **Settings › Sistema › Security key management › Create Internal Key**.

A chave de segurança é armazenada no controlador em um local oculto e inacessível. Você pode então criar grupos de volume ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volume existentes e pools existentes.

Gerenciamento de chaves externas

As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um Protocolo de Interoperabilidade de Gerenciamento de Chaves (KMIP). Para implementar o gerenciamento de chaves externas, execute as seguintes etapas:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
    a. Primeiro, você preenche e faz o download de uma Solicitação de Assinatura de Certificado (CSR) do cliente. Vá para **Settings › Certificates › Key Management › Complete CSR**.
    b. Em seguida, você solicita um certificado de cliente assinado de uma CA confiável pelo servidor de gerenciamento de chaves. (Você também pode criar e baixar um certificado de cliente do servidor de gerenciamento de chaves usando o arquivo CSR.)
    c. Depois de obter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando System Manager.
    d. Alternativamente, você pode gerar uma solicitação de assinatura de certificado externamente usando um par de chaves privada e pública.
4. Recupere um arquivo de certificado do servidor de gerenciamento de chaves e copie 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, para que o array de storage possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

5. Crie uma chave externa, o que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usado para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Para criar uma chave externa, acesse **Settings › Sistema › Security key management › Create External Key**.

O sistema se conecta ao servidor de gerenciamento de chaves com as credenciais que você inseriu. Você pode então criar grupos de volume ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volume e pools existentes.

Aprenda sobre a terminologia de segurança de unidades no software SANtricity

Saiba como os termos de segurança da unidade se aplicam ao seu array de storage.

Termo	Descrição
Recurso de segurança da unidade	Drive Security é um recurso do array de storage que fornece uma camada extra de segurança com unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS). Quando essas unidades são usadas com o recurso Drive Security, elas exigem uma chave de segurança para acesso aos seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array; nesse momento, elas estarão em um estado Security Locked até que a chave de segurança correta seja fornecida.
Unidades FDE	Unidades com criptografia de disco completa (FDE) realizam criptografia na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa os dados durante as gravações e os descriptografa durante as leituras.
Unidades FIPS	Unidades FIPS utilizam o Federal Information Processing Standards (FIPS) 140-2 nível 2. Essencialmente, são unidades FDE que seguem os padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia robustos. Unidades FIPS possuem padrões de segurança mais elevados do que unidades FDE.
Cliente de gerenciamento	Um sistema local (computador, tablet, etc.) que inclui um navegador para acessar System Manager.
Frase secreta	A frase secreta é usada para criptografar a chave de segurança para fins de backup. A mesma frase secreta usada para criptografar a chave de segurança deve ser fornecida quando a chave de segurança de backup for importada como resultado de uma migração de unidade ou troca de cabeçote. Uma frase secreta pode ter entre 8 e 32 caracteres. A senha para Segurança da Unidade é independente da senha de Administrador do array de storage.

Termo	Descrição
Unidades com capacidade de segurança	Unidades com capacidade de segurança podem ser unidades Full Disk Encryption (FDE) ou unidades Federal Information Processing Standard (FIPS), que criptografam os dados durante as gravações e descriptografam os dados durante as leituras. Essas unidades são consideradas secure-*capable* porque podem ser usadas para segurança adicional usando o recurso Drive Security. Se o recurso Drive Security estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornam secure-*enabled*.
Unidades com segurança ativada	Unidades com segurança habilitada são usadas com o recurso Drive Security. Quando você habilita o recurso Drive Security e, em seguida, aplica Drive Security a um pool ou grupo de volume em unidades secure-capable, as unidades passam a ser secure-enabled. O acesso de leitura e gravação está disponível somente por meio de um controlador configurado com a chave de segurança correta. Essa segurança adicional impede o acesso não autorizado aos dados em uma unidade que foi fisicamente removida do array de storage.
Chave de segurança	Uma chave de segurança é uma sequência de caracteres compartilhada entre as unidades e controladores com segurança habilitada em um array de storage. Sempre que a energia das unidades é desligada e ligada, as unidades com segurança habilitada entram no estado Security Locked até que o controlador aplique a chave de segurança. Se uma unidade com segurança habilitada for removida do array de storage, os dados da unidade serão bloqueados. Quando a unidade for reinstalada em um array de storage diferente, ela buscará a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você deve aplicar a chave de segurança original. Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos: • Gerenciamento de chaves internas — criar e manter chaves de segurança na memória persistente do controlador. • Gerenciamento de chaves externas — criar e manter chaves de segurança em um servidor de gerenciamento de chaves externo.
Identificador da chave de segurança	O identificador da chave de segurança é uma sequência de caracteres associada à chave de segurança durante a criação da chave. O identificador é armazenado no controlador e em todas as unidades associadas à chave de segurança.

Configurar chaves de segurança

Crie uma chave de segurança interna no SANtricity System Manager

Para usar o recurso de Segurança de Unidade, você pode criar uma chave de segurança interna que é compartilhada pelos controladores e unidades com capacidade de segurança no array de storage. As chaves internas são mantidas na memória persistente do controlador.

Antes de começar

- Unidades com capacidade de segurança devem ser instaladas no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades com o padrão Federal

Information Processing Standard (FIPS).

- 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.

> Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

Sobre esta tarefa

Nesta tarefa, você define um identificador e uma frase secreta para associar à chave de segurança interna.

> A senha para Segurança da Unidade é independente da senha de Administrador do array de storage.

Passos

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

   Se você ainda não gerou uma chave de segurança, a caixa de diálogo Criar chave de segurança é aberta.

3. Insira informações nos seguintes campos:

   - **Defina um identificador de chave de segurança** — Você pode aceitar o valor padrão (nome do array de storage e carimbo de data/hora, que é gerado pelo firmware do controlador) ou inserir seu próprio valor. Você pode inserir até 189 caracteres alfanuméricos, sem espaços, pontuação ou símbolos.

     > Caracteres adicionais são gerados automaticamente, anexados às duas extremidades da sequência que você inserir. Os caracteres gerados garantem que o identificador seja único.

   - **Definir uma frase secreta/Digitar novamente a frase secreta** — Digite e confirme uma 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).

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

4. Clique em **Create**.

   A chave de segurança é armazenada no controlador em um local inacessível. Junto com a chave real, há um arquivo de chave criptografado que é baixado do seu navegador.

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

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

Resultados

Agora você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools de volumes existentes.

> Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Security Locked impede o acesso não autorizado aos seus dados.

Depois que você terminar

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

Crie uma chave de segurança externa no SANtricity System Manager

Para usar o recurso de segurança de unidade com um servidor de gerenciamento de chaves, você deve criar uma chave externa que é compartilhada pelo servidor de gerenciamento de chaves e pelas unidades com capacidade de segurança no array de storage.

Antes de começar

- Unidades de armazenamento com capacidade de segurança devem ser instaladas no array. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).

  > Se ambas as unidades FDE e FIPS estiverem instaladas no array de storage, todas compartilharão a mesma chave de segurança.

- 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 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

Nesta tarefa, você define o endereço IP do servidor de gerenciamento de chaves e o número da porta que ele utiliza e, em seguida, carrega certificados para o gerenciamento externo de chaves.

Passos

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

> Se o gerenciamento de chaves interno estiver atualmente configurado, uma caixa de diálogo será aberta e solicitará que você confirme que deseja mudar para o gerenciamento de chaves externo.

A caixa de diálogo Criar chave de segurança externa é aberta.

3. Em **Conectar ao Key Server**, insira 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 comunicações KMIP. O número de porta mais comum usado para comunicações com o servidor de gerenciamento de chaves é 5696.

     Opcional: Se você quiser configurar um servidor de chaves de backup, clique em **Add Key Server** e insira as informações desse servidor. O segundo servidor de chaves será usado se o servidor de chaves primário não puder ser acessado. Certifique-se de que cada servidor de chaves tenha acesso ao mesmo banco de dados de chaves; caso contrário, o array exibirá erros e não poderá usar o servidor de backup.

> Apenas um servidor de chaves é usado por vez. Se o array de storage não conseguir alcançar o servidor de chaves primário, o array entrará em contato com o servidor de chaves de backup. Esteja ciente de que você deve manter a paridade entre ambos os servidores; a falha em fazê-lo pode resultar em erros.

   - **Selecionar certificado do cliente** — Clique no primeiro botão **Procurar** para selecionar o arquivo de certificado para os controladores do array de storage.
   - **Selecionar arquivo de chave privada** — Se necessário, clique no segundo botão **Procurar** para selecionar um arquivo de chave privada para os controladores do array de storage.
   - **Selecione o certificado do servidor de gerenciamento de chaves** — Clique no terceiro botão **Procurar** para selecionar o arquivo de certificado do servidor de gerenciamento de chaves. Você pode escolher um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.
4. Clique em **Next**.
5. Em **Criar/Fazer Backup da Chave**, você pode criar uma chave de backup para fins de segurança.
   - (Recomendado) Para criar uma chave de backup, mantenha a caixa de seleção marcada e, em seguida, insira e confirme uma senha. 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 anotar suas entradas para uso posterior**. Se precisar mover uma unidade com segurança habilitada do array de storage, você precisa saber a senha para desbloquear os dados da unidade.

+

- Se não quiser criar uma chave de backup, desmarque a caixa de seleção.

> Esteja ciente de que, se você perder o acesso ao servidor de chaves externo e não tiver uma chave de backup, perderá o acesso aos dados nas unidades caso elas sejam migradas para outro array de storage. Esta opção é o único método para criar uma chave de backup no System Manager.

6. Clique em **Concluir**.

   O sistema se conecta ao servidor de gerenciamento de chaves com as credenciais que você inseriu. Uma cópia da chave de segurança é então armazenada em seu sistema local.

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

7. Anote sua frase secreta e o local do arquivo de chave baixado e, em seguida, clique em **Fechar**.

   A página exibe a seguinte mensagem com links adicionais para gerenciamento externo de chaves:

   ```
   Current key management method: External
   ```

8. Teste a conexão entre o array de storage e o servidor de gerenciamento de chaves selecionando **Test Communication**.

   Os resultados dos testes são exibidos na caixa de diálogo.

Resultados

Quando o gerenciamento de chaves externas está ativado, você pode criar grupos ou pools de volumes com segurança habilitada, ou pode habilitar a segurança em grupos e pools de volumes existentes.

> Sempre que a alimentação das unidades é desligada e ligada novamente, todas as unidades com segurança habilitada passam para o estado Security Locked. Nesse estado, os dados ficam inacessíveis até que o controlador aplique a chave de segurança correta durante a inicialização da unidade. Se alguém remover fisicamente uma unidade bloqueada e instalá-la em outro sistema, o estado Security Locked impede o acesso não autorizado aos seus dados.

Depois que você terminar

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

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".

Perguntas frequentes sobre segurança de storage drive para SANtricity System Manager

Esta FAQ pode ajudar se você estiver apenas procurando uma resposta rápida para uma pergunta.

O que preciso saber antes de criar uma chave de segurança?

Uma chave de segurança é compartilhada entre controladores e unidades com segurança habilitada dentro de um array de storage. Se uma unidade com segurança habilitada for removida do array de storage, a chave de segurança protege os dados contra acesso não autorizado.

Você pode criar e gerenciar chaves de segurança usando um dos seguintes métodos:

- Gerenciamento interno de chaves na memória persistente do controlador.
- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

Gerenciamento interno de chaves

As chaves internas são mantidas e “hidden” em um local inacessível na memória persistente do controlador. Antes de criar uma chave de segurança interna, você deve fazer o seguinte:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.

Em seguida, você pode criar uma chave de segurança interna, o que envolve definir um identificador e uma frase secreta. O identificador é uma string que está associada à chave de segurança e é armazenado no controlador e em todas as unidades associadas à chave. A frase secreta é usada para criptografar a chave de segurança para fins de backup. Quando você termina, a chave de segurança é armazenada no controlador em um local inacessível. Você pode então criar grupos de volumes ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools existentes.

Gerenciamento de chaves externas

As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um Key Management Interoperability Protocol (KMIP). Antes de criar uma chave de segurança externa, você deve fazer o seguinte:

1. Instale unidades com recursos de segurança no array de storage. Essas unidades podem ser unidades com criptografia de disco completa (FDE) ou unidades Federal Information Processing Standard (FIPS).
2. Certifique-se de que o recurso de Drive Security esteja ativado. Se necessário, entre em contato com seu fornecedor de storage para obter instruções sobre como ativar o recurso de Drive Security.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do array de storage, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você preenche e faz o download de uma Solicitação de Assinatura de Certificado (CSR) do cliente. Vá para **Settings › Certificates › Key Management › Complete CSR**.
   b. Em seguida, você solicita um certificado de cliente assinado de uma CA confiável pelo servidor de gerenciamento de chaves. (Você também pode criar e baixar um certificado de cliente do servidor de gerenciamento de chaves usando o arquivo CSR baixado.)
   c. Depois de obter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando System Manager.
4. Recupere um arquivo de certificado do servidor de gerenciamento de chaves e copie 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, para que o array de storage possa confiar em seu endereço IP. Você pode usar um certificado raiz, intermediário ou de servidor para o servidor de gerenciamento de chaves.

Em seguida, você pode criar uma chave externa, o que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usado para as comunicações KMIP. Durante esse processo, você também carrega os arquivos de certificado. Ao concluir, o sistema se conecta ao servidor de gerenciamento de chaves com as credenciais inseridas. Você pode então criar grupos de volumes ou pools com segurança habilitada, ou pode habilitar a segurança em grupos de volumes e pools existentes.

Por que preciso definir uma frase secreta?

A senha é usada para criptografar e descriptografar o arquivo de chave de segurança armazenado no cliente de gerenciamento local. Sem a senha, a chave de segurança não pode ser descriptografada e usada para desbloquear dados de uma unidade com segurança habilitada, caso ela seja reinstalada em outro array de storage.

Por que é importante registrar as informações da chave de segurança?

Se você perder as informações da chave de segurança e não tiver um backup, poderá perder dados ao realocar unidades com segurança habilitada ou ao atualizar um controlador. Você precisa da chave de segurança para desbloquear dados nas unidades.

Certifique-se de registrar o identificador da chave de segurança, a frase secreta associada e o local no host local onde o arquivo da chave de segurança foi salvo.

O que preciso saber antes de fazer backup de uma chave de segurança?

Se a sua chave de segurança original for corrompida e você não tiver um backup, você perderá o acesso aos

dados nas unidades caso elas sejam migradas de um array de storage para outro.

Antes de fazer backup de uma chave de segurança, tenha em mente estas diretrizes:

- Certifique-se de conhecer o identificador da chave de segurança e a frase secreta do arquivo de chave original.

> Somente as chaves internas usam identificadores. Ao criar o identificador, caracteres adicionais foram gerados automaticamente e anexados às duas extremidades da string do identificador. Os caracteres gerados garantem que o identificador seja único.

- 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.

> A frase secreta para Drive Security não deve ser confundida com a senha de administrador do array de storage. A frase secreta para Drive Security protege os backups de uma chave de segurança. A senha de administrador protege todo o array de storage contra acesso não autorizado.

- O arquivo de chave de segurança de backup é baixado para o seu cliente de gerenciamento. O caminho para o arquivo baixado pode depender do local de download padrão do seu navegador. Certifique-se de registrar onde as informações da sua chave de segurança estão armazenadas.

O que preciso saber antes de desbloquear unidades seguras?

Para desbloquear os dados de uma unidade com segurança ativada, você deve importar sua chave de segurança.

Antes de desbloquear unidades com segurança ativada, tenha em mente as seguintes diretrizes:

- O array de storage já deve possuir uma chave de segurança. As unidades migradas serão reconfiguradas com uma nova chave para o array de storage de destino.
- Para as unidades que você está migrando, você deve saber o identificador da chave de segurança e a frase secreta que corresponde ao arquivo da chave de segurança.
- O arquivo de chave de segurança deve estar disponível no cliente de gerenciamento (o sistema com navegador usado para acessar System Manager).
- Se você estiver redefinindo uma unidade NVMe bloqueada, precisará inserir o ID de segurança da unidade. Para localizar o ID de segurança, você deve remover fisicamente a unidade e encontrar a sequência PSID (máximo de 32 caracteres) na etiqueta da unidade. Certifique-se de que a unidade esteja reinstalada antes de iniciar a operação.

O que é acessibilidade de leitura/gravação?

A janela Configurações da unidade inclui informações sobre os atributos de segurança da unidade. "Leitura/gravação acessível" é um dos atributos que indica se os dados de uma unidade foram bloqueados.

Para visualizar os atributos de segurança da unidade, acesse a página Hardware. Selecione uma unidade, clique em **Exibir configurações** e, em seguida, clique em **Mostrar mais configurações**. Na parte inferior da página, o valor do atributo Leitura/Gravação acessível é **Sim** quando a unidade está desbloqueada. O valor do atributo Leitura/Gravação acessível é **Não, chave de segurança inválida** quando a unidade está bloqueada. Você pode desbloquear uma unidade segura importando uma chave de segurança (vá para **Configurações ›**

Sistema › Desbloquear unidades seguras).

O que preciso saber sobre validar a chave de segurança?

Após criar uma chave de segurança, você deve validar o arquivo da chave para garantir que não esteja corrompido.

Se a validação falhar, faça o seguinte:

- Se o identificador da chave de segurança não corresponder ao identificador no controlador, localize o arquivo de chave de segurança correto e tente a validação novamente.
- Se o controlador não conseguir descriptografar a chave de segurança para validação, você pode ter digitado a frase secreta incorretamente. Verifique a frase secreta, digite-a novamente se necessário e tente a validação novamente. Se a mensagem de erro aparecer novamente, selecione um backup do arquivo de chave (se disponível) e tente a validação novamente.
- Se você ainda não conseguir validar a chave de segurança, o arquivo original pode estar corrompido. Crie um novo backup da chave e valide essa cópia.

Qual é a diferença entre chave de segurança interna e gerenciamento externo de chave de segurança?

Ao implementar o recurso de Segurança de Unidade, você pode usar uma chave de segurança interna ou externa para bloquear os dados quando uma unidade com segurança habilitada for removida do array de storage.

Uma chave de segurança é uma sequência de caracteres, que é compartilhada entre as unidades com segurança habilitada e os controladores em um array de storage. As chaves internas são mantidas na memória persistente do controlador. As chaves externas são mantidas em um servidor de gerenciamento de chaves separado, usando um Key Management Interoperability Protocol (KMIP).

Informações sobre direitos autorais

Copyright © 2026 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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.