Segurança da unidade

SANtricity 11.8

NetApp
January 31, 2025

Índice

Segurança da unidade

Visão geral do Drive Security

Você pode configurar o Drive Security e o gerenciamento de chaves na página Security Key Management (Gerenciamento de chaves de segurança).

O que é o Drive Security?

Drive Security é um recurso que impede o acesso não autorizado a dados em unidades habilitadas para segurança quando removido do storage array. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando as unidades FDE ou FIPS são removidas fisicamente do storage, elas não podem operar até serem instaladas em outro storage, e nesse ponto, as unidades estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida. A *security key* é uma cadeia de carateres que é compartilhada entre esses tipos de unidades e os controladores em um storage array.

Saiba mais:

- "Como funciona o recurso Segurança da Unidade"
- "Como funciona o gerenciamento de chaves de segurança"
- "Terminologia de segurança da unidade"

Como faço para configurar o gerenciamento de chaves?

Para implementar o Drive Security, é necessário ter unidades FDE ou FIPS instaladas no array. Para configurar a gestão de chaves para estas unidades, aceda ao **Definições › sistema › Gestão de chaves de segurança**, onde pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa a partir de um servidor de gestão de chaves. Por fim, você ativa a Segurança da Unidade para pools e grupos de volume selecionando "segura-capaz" nas configurações de volume.

Saiba mais:

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

Como posso desbloquear unidades?

Se você tiver configurado o gerenciamento de chaves e, em seguida, 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.

Saiba mais:

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

Informações relacionadas

Saiba mais sobre tarefas relacionadas ao gerenciamento de chaves:

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

Conceitos

Como funciona o recurso Segurança da Unidade

O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).

Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida.

Como implementar o Drive Security

Para implementar o Drive Security, execute as etapas a seguir.

1. Equipe seu storage array com unidades com capacidade segura, unidades FDE ou FIPS. (Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo ou pool de volumes totalmente FIPS.)
2. Crie uma chave de segurança, que é uma cadeia de carateres que é compartilhada pelo controlador e unidades para acesso de leitura/gravação. Você pode criar uma chave interna a partir da memória persistente do controlador ou uma chave externa 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 da unidade para pools e grupos de volumes:
   - Crie um pool ou grupo de volumes (procure **Sim** na coluna **compatível com segurança** na tabela candidatos).
   - Selecione um pool ou grupo de volumes quando criar um novo volume (procure **Sim** ao lado de **compatível com segurança** na tabela de candidatos ao grupo de grupos de volumes e pool).

Como o Drive Security funciona no nível da unidade

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

O recurso Drive Security fornece uma camada extra de proteção com unidades com capacidade de segurança. Quando grupos de volume ou pools nessas unidades são selecionados para o 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 da matriz de armazenamento

Com o recurso Segurança da unidade, você cria uma chave de segurança compartilhada entre as unidades e os controladores habilitados para segurança em um storage de armazenamento. Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança.

Se uma unidade habilitada para segurança for removida da matriz de armazenamento e reinstalada em uma matriz de armazenamento diferente, a unidade estará em um estado de segurança bloqueado. A unidade relocada procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, você aplica a chave de segurança do storage array de origem. Após um processo de desbloqueio bem-sucedido, a unidade relocada usará a chave de segurança já armazenada no storage de armazenamento de destino e o arquivo de chave de segurança importado não será mais necessário.

> Para o gerenciamento de chaves internas, a chave de segurança real é armazenada no controlador em um local não acessível. Não está em formato legível por humanos, nem é acessível ao usuário.

Como o Drive Security funciona no nível do volume

Ao criar um pool ou grupo de volumes a partir de unidades com capacidade segura, também é possível ativar a Segurança da unidade para esses pools ou grupos de volumes. A opção Segurança da unidade torna as unidades e os grupos de volume e pools associados seguros-*enabled*.

Tenha em mente as seguintes diretrizes antes de criar grupos e pools de volume habilitados para segurança:

- Os grupos de volumes e pools devem ser compostos inteiramente de unidades com capacidade de segurança. (Para volumes que exigem suporte FIPS, use apenas unidades FIPS. A combinação de unidades FIPS e FDE em um grupo de volumes ou pool resultará no tratamento de todas as unidades como unidades FDE. Além disso, uma unidade FDE não pode ser adicionada ou usada como sobressalente em um grupo ou pool de volumes totalmente FIPS.)
- Os grupos de volume e os pools devem estar em um estado ideal.

Como funciona o gerenciamento de chaves de segurança

Quando você implementa o recurso Segurança da unidade, as unidades habilitadas para segurança (FIPS ou FDE) exigem uma chave de segurança para acesso aos dados. Uma chave de segurança é uma cadeia de carateres que é compartilhada entre esses tipos de unidades e os controladores em um storage array.

Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança. Se uma unidade habilitada para segurança for removida da matriz de armazenamento, os dados da unidade serão bloqueados. Quando a unidade é reinstalada em uma matriz de armazenamento diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, tem de aplicar a chave de segurança original.

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

- Gerenciamento de chaves internas na memória persistente do controlador.

- Gerenciamento de chaves externas em um servidor de gerenciamento de chaves externo.

Gerenciamento de chaves internas

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

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Crie uma chave de segurança interna, que envolve a definição de um identificador e uma frase-passe. O identificador é uma cadeia de carateres associada à chave de segurança e é armazenada no controlador e em todas as unidades associadas à chave. A frase-passe é usada para criptografar a chave de segurança para fins de backup. Para criar uma chave interna, aceda ao **Definições › sistema › Gestão da chave de segurança › criar chave interna**.

A chave de segurança é armazenada no controlador num local oculto e não acessível. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou 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 KMIP (Key Management Interoperability Protocol). Para implementar o gerenciamento de chaves externas, execute as seguintes etapas:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você conclui e faz o download de uma solicitação de assinatura de certificado de cliente (CSR). Aceda ao **Definições › certificados › Gestão de chaves › CSR completo**.
   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 a partir do servidor de gerenciamento de chaves usando o arquivo CSR.)
   c. Depois de ter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando o 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 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.

5. Crie uma chave externa, que envolve definir o endereço IP do servidor de gerenciamento de chaves e o número da porta usada para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Para criar uma chave externa, aceda ao **Definições › sistema › Gestão da chave de segurança › criar chave externa**.

O sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

Terminologia de segurança da unidade

Saiba como os termos de segurança da unidade se aplicam à sua matriz de armazenamento.

Prazo	Descrição
Recurso de segurança da unidade	O Drive Security é um recurso de storage array que fornece uma camada extra de segurança com unidades de criptografia completa de disco (FDE) ou unidades FIPS (Federal Information Processing Standard). Quando essas unidades são usadas com o recurso Segurança da Unidade, elas precisam de uma chave de segurança para acessar seus dados. Quando as unidades são fisicamente removidas do array, elas não podem operar até serem instaladas em outro array, em que ponto, elas estarão em um estado de segurança bloqueado até que a chave de segurança correta seja fornecida.
Unidades FDE	As unidades Full Disk Encryption (FDE) executam a encriptação na unidade de disco no nível do hardware. O disco rígido contém um chip ASIC que criptografa dados durante gravações e, em seguida, descriptografa dados durante leituras.
Unidades FIPS	As unidades FIPS usam Federal Information Processing Standards (FIPS) 140-2 nível 2. Eles são essencialmente unidades FDE que aderem aos padrões do governo dos Estados Unidos para garantir algoritmos e métodos de criptografia fortes. As unidades FIPS têm padrões de segurança mais altos do que as unidades FDE.
Cliente de gestão	Um sistema local (computador, tablet, etc.) que inclui um navegador para acessar o System Manager.
Frase-passe	A frase-passe é usada para criptografar a chave de segurança para fins de backup. A mesma frase-passe 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 cabeça. Uma frase-passe pode ter entre 8 e 32 carateres. A frase-passe para o Drive Security é independente da senha do Administrador do storage.

Prazo	Descrição
Unidades com capacidade de segurança	As unidades com capacidade segura podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard), que criptografam dados durante gravações e descriptografam dados durante leituras. Essas unidades são consideradas seguras-*Capable* porque podem ser usadas para segurança adicional usando o recurso Segurança da Unidade. Se o recurso Segurança da unidade estiver habilitado para grupos de volume e pools usados com essas unidades, as unidades se tornarão seguras-*enabled*.
Unidades habilitadas para segurança	As unidades habilitadas para segurança são usadas com o recurso Segurança da unidade. Quando você ativa o recurso de Segurança da Unidade e, em seguida, aplica o Drive Security a um pool ou grupo de volume em unidades seguras-*capazes*, as unidades ficam seguras___ ativadas. 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 é fisicamente removida do storage array.
Chave de segurança	Uma chave de segurança é uma cadeia de carateres que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. Sempre que a alimentação das unidades é desligada e ligada, as unidades ativadas por segurança mudam para um estado de Segurança bloqueada até que o controlador aplique a chave de segurança. Se uma unidade habilitada para segurança for removida da matriz de armazenamento, os dados da unidade serão bloqueados. Quando a unidade é reinstalada em uma matriz de armazenamento diferente, ela procura a chave de segurança antes de tornar os dados acessíveis novamente. Para desbloquear os dados, tem de 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 — Crie e mantenha chaves de segurança em um servidor de gerenciamento de chaves externo.
Identificador da chave de segurança	O identificador da chave de segurança é uma cadeia de carateres 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

Criar chave de segurança interna

Para usar o recurso Segurança da unidade, você pode criar uma chave de segurança interna compartilhada pelos controladores e unidades seguras no storage de armazenamento. As chaves internas são mantidas na memória persistente do controlador.

Antes de começar

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

Se as unidades FDE e FIPS estiverem instaladas no storage de armazenamento, todas elas compartilharão a mesma chave de segurança.

Sobre esta tarefa

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

A frase-passe para o Drive Security é independente da senha do Administrador do storage.

Passos

1. Selecione **Definições › 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 será aberta.

3. Introduza as informações nos seguintes campos:

   - * Definir um identificador de chave de segurança* — você pode aceitar o valor padrão (nome da matriz de armazenamento e carimbo de hora, que é gerado pelo firmware do controlador) ou inserir seu próprio valor. Pode introduzir até 189 carateres alfanuméricos sem espaços, pontuação ou símbolos.

     Carateres adicionais são gerados automaticamente, anexados a ambas as extremidades da cadeia de carateres inserida. Os carateres gerados garantem que o identificador é exclusivo.

   - * Definir uma frase-passe/re-insira a frase-passe* — Digite e confirme uma frase-passe. O valor pode ter entre 8 e 32 carateres 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 **criar**.

   A chave de segurança é armazenada no controlador num local não acessível. Junto com a chave real, há um arquivo de chave criptografada que é baixado do seu navegador.

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

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

Resultados

Agora você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

> Sempre que a alimentação das unidades for desligada e novamente ligada, todas as unidades ativadas para segurança mudam para um estado de segurança bloqueado. Neste 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 Segurança bloqueada impede o acesso não autorizado aos seus dados.

Depois de terminar

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

Criar chave de segurança externa

Para usar o recurso Segurança da unidade com um servidor de gerenciamento de chaves, você deve criar uma chave externa compartilhada pelo servidor de gerenciamento de chaves e pelas unidades com capacidade segura no storage de armazenamento.

Antes de começar

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

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

- 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 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

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

Passos

1. Selecione **Definições › sistema**.
2. Em **Gerenciamento de chaves de segurança**, selecione **criar chave externa**.

   > Se o gerenciamento de chaves internas estiver configurado no momento, uma caixa de diálogo será aberta e solicitará que você confirme se deseja mudar para o gerenciamento de chaves externas.

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

3. Em **conetar ao Key Server**, insira as informações nos campos a seguir.

   - **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 comunicações KMIP. O número de porta mais comum usado para comunicações do 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 primárias não puder ser alcançado. Certifique-se de que cada servidor de chaves tenha acesso ao mesmo banco de dados de chaves; caso contrário, o array publicará erros e não poderá usar o servidor de backup.

     > Apenas um servidor de chave única é usado de cada vez. Se a matriz de armazenamento não conseguir alcançar o servidor de chave primária, a matriz entrará em Contato com o servidor de chave de backup. Esteja ciente de que você deve manter a paridade entre ambos os servidores; a falha em fazê-lo pode resultar em erros.

   - **Selecione o certificado do cliente** — clique no primeiro botão **Procurar** para selecionar o arquivo de certificado para os controladores do storage.
   - **Selecione o certificado do servidor de gerenciamento de chaves** — clique no segundo botão **Procurar** para selecionar o arquivo de certificado para o servidor de gerenciamento de chaves. Você pode escolher um certificado de raiz, intermediário ou servidor para o servidor de gerenciamento de chaves.
4. Clique em **seguinte**.
5. Em **Create/Backup Key**, você pode criar uma chave de backup para fins de segurança.

   - (Recomendado) para criar uma chave de cópia de segurança, mantenha a caixa de verificação selecionada e, em seguida, introduza e confirme uma frase-passe. O valor pode ter entre 8 e 32 carateres 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 de armazenamento, você deve saber a frase-passe para desbloquear os dados da unidade.

+

- Se não pretender criar uma chave de cópia de segurança, desmarque a caixa de verificação.

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 se elas forem migradas para outro storage array. Esta opção é o único método para criar uma chave de backup no System Manager.

6. Clique em **Finish**.

   O sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Uma cópia da chave de segurança é então armazenada no sistema local.

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

7. Grave a frase-passe e a localização do ficheiro de chave transferido e, em seguida, clique em **Fechar**.

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

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

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

   Os resultados do teste são exibidos na caixa de diálogo.

Resultados

Quando o gerenciamento de chaves externas está habilitado, você pode criar grupos ou pools de volumes habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

Sempre que a alimentação das unidades for desligada e novamente ligada, todas as unidades ativadas para segurança mudam para um estado de segurança bloqueado. Neste 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 Segurança bloqueada impede o acesso não autorizado aos seus dados.

Depois de terminar

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

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 carateres alfanuméricos sem espaços, pontuação ou símbolos.

     Os carateres adicionais são gerados automaticamente e são anexados a ambas as extremidades da cadeia de carateres inserida. Os carateres 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 carateres 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).
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 carateres 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 carateres 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 carateres 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 carateres 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 carateres 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 conete 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 carateres 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".

FAQs

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

Uma chave de segurança é compartilhada por controladores e unidades habilitadas para proteger dentro de um storage array. Se uma unidade habilitada para segurança for removida do storage array, a chave de segurança protegerá os dados contra acesso não autorizado.

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

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

Gerenciamento de chaves internas

As chaves internas são mantidas e "ocultas" em um local não acessível na memória persistente do controlador. Antes de criar uma chave de segurança interna, você deve fazer o seguinte:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.

Em seguida, você pode criar uma chave de segurança interna, que envolve a definição de um identificador e uma frase-passe. O identificador é uma cadeia de carateres associada à chave de segurança e é armazenada no controlador e em todas as unidades associadas à chave. A frase-passe é usada para criptografar a chave de segurança para fins de backup. Quando terminar, a chave de segurança é armazenada no controlador num local não acessível. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou 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 KMIP (Key Management Interoperability Protocol). Antes de criar uma chave de segurança externa, você deve fazer o seguinte:

1. Instale unidades com capacidade segura no storage de armazenamento. Essas unidades podem ser unidades com criptografia total de disco (FDE) ou unidades FIPS (Federal Information Processing Standard).
2. Certifique-se de que a funcionalidade de Segurança da unidade está ativada. Se necessário, entre em Contato com o fornecedor de armazenamento para obter instruções sobre como ativar o recurso Segurança da unidade.
3. Obtenha um arquivo de certificado de cliente assinado. Um certificado de cliente valida os controladores do storage array, para que o servidor de gerenciamento de chaves possa confiar em suas solicitações KMIP.
   a. Primeiro, você conclui e faz o download de uma solicitação de assinatura de certificado de cliente (CSR). Aceda ao **Definições › certificados › Gestão de chaves › CSR completo**.
   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 ter um arquivo de certificado de cliente, copie esse arquivo para o host onde você está acessando o 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 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.

Em seguida, você pode criar uma chave externa, que envolve a definição do endereço IP do servidor de gerenciamento de chaves e o número da porta usada para comunicações KMIP. Durante esse processo, você também carrega arquivos de certificado. Quando terminar, o sistema se coneta ao servidor de gerenciamento de chaves com as credenciais inseridas. Em seguida, você pode criar grupos de volume ou pools habilitados para segurança ou habilitar a segurança em grupos de volumes e pools existentes.

Por que eu preciso definir uma frase-passe?

A frase-passe é usada para criptografar e descriptografar o arquivo de chave de segurança armazenado no cliente de gerenciamento local. Sem a frase-passe, a chave de segurança não pode ser descriptografada e usada para desbloquear dados de uma unidade habilitada para segurança se for reinstalada em outra matriz de armazenamento.

Por que é importante Registrar informações de chave de segurança?

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

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

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

Se a chave de segurança original ficar corrompida e você não tiver um backup, perderá o acesso aos dados nas unidades se eles forem migrados de um storage array para outro.

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

- Certifique-se de que conhece o identificador da chave de segurança e a frase-passe do ficheiro de chave original.

> Somente chaves internas usam identificadores. Quando você criou o identificador, carateres adicionais foram gerados automaticamente e anexados a ambas as extremidades da cadeia de carateres do identificador. Os carateres gerados garantem que o identificador é exclusivo.

- 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.

> A frase-passe para o Drive Security não deve ser confundida com a senha de Administrador do storage. A frase-passe do Drive Security protege os backups de uma chave de segurança. A senha do administrador protege toda a matriz de armazenamento 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 fazer um Registro de onde as informações da chave de segurança estão armazenadas.

O que eu preciso saber antes de desbloquear unidades seguras?

Para desbloquear os dados de uma unidade ativada de forma segura, tem de importar a respetiva chave de segurança.

Antes de desbloquear unidades seguras, tenha em mente as seguintes diretrizes:

- O storage array já deve ter uma chave de segurança. As unidades migradas serão recodificadas para o storage de armazenamento de destino.
- Para as unidades que você está migrando, você deve saber o identificador da chave de segurança e a frase-passe que corresponde ao arquivo da chave de segurança.
- O arquivo da chave de segurança deve estar disponível no cliente de gerenciamento (o sistema com um navegador usado para acessar o System Manager).

- Se estiver a repor uma unidade NVMe bloqueada, tem de introduzir a ID de segurança da unidade. Para localizar a ID de segurança, você deve remover fisicamente a unidade e encontrar a cadeia PSID (máximo de 32 carateres) na etiqueta da unidade. Certifique-se de que a unidade é reinstalada antes de iniciar a operação.

O que é acessibilidade de leitura/escrita?

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

Para exibir os atributos de segurança da unidade, vá para a página hardware. Selecione uma unidade, clique em **View settings** e, em seguida, clique em **Show more settings** (Mostrar mais definições). Na parte inferior da página, o valor do atributo leitura/gravação acessível é **Sim** quando a unidade é desbloqueada. O valor do atributo leitura/gravação acessível é **não, chave de segurança inválida** quando a unidade está bloqueada. Pode desbloquear uma unidade segura importando uma chave de segurança (aceda ao **Definições › sistema › desbloquear unidades seguras**).

O que eu preciso saber sobre a validação da chave de segurança?

Depois de criar uma chave de segurança, você deve validar o arquivo de chave para se certificar de que ele não está corrompido.

Se a validação falhar, faça o seguinte:

- Se o identificador da chave de segurança não corresponder ao identificador no controlador, localize o ficheiro de chave de segurança correto e, em seguida, tente a validação novamente.
- Se o controlador não conseguir desencriptar a chave de segurança para validação, poderá ter introduzido incorretamente a frase-passe. Verifique novamente a frase-passe, volte a introduzi-la, se necessário, e tente a validação novamente. Se a mensagem de erro aparecer novamente, selecione uma cópia de segurança do ficheiro de chave (se disponível) e volte a tentar a validação.
- 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 a chave de segurança interna e o gerenciamento de chaves de segurança externas?

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

Uma chave de segurança é uma cadeia de carateres, que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. 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 KMIP (Key Management Interoperability Protocol).

Informações sobre direitos autorais

Informações sobre marcas comerciais