Configurar chaves de segurança

SANtricity 11.9

NetApp
December 16, 2024

Índice

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 arquivo de chave privada** — se necessário, clique no segundo botão **Procurar** para selecionar um arquivo de chave privada para os controladores do storage array.
   - **Selecione o certificado do servidor de gerenciamento de chaves** — clique no terceiro 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.

Informações sobre direitos autorais

Informações sobre marcas comerciais