



G

SANtricity commands

NetApp
June 16, 2025

Índice

- G..... 1
 - Introdução à autenticação - SANtricity CLI 1
 - Introdução ao gerenciamento de chaves externas - SANtricity CLI 1
 - Etapas do fluxo de trabalho 1
 - Introdução ao gerenciamento de chaves internas - SANtricity CLI 2
 - Etapas do fluxo de trabalho 2

G

Introdução à autenticação - SANtricity CLI

A autenticação requer que os usuários acessem o sistema com credenciais de login atribuídas. Cada login de usuário é associado a um perfil de usuário que inclui funções específicas e permissões de acesso.

Os administradores podem implementar a autenticação do sistema da seguinte forma:

- Uso dos recursos RBAC (controle de acesso baseado em função) aplicados no storage array, que incluem usuários e funções pré-definidas.
- Conexão a um servidor LDAP (Lightweight Directory Access Protocol) e serviço de diretório, como o ativo Directory da Microsoft, e mapeando os usuários LDAP para as funções incorporadas do storage array.
- Conexão com um provedor de identidade (IDP) usando a Security Assertion Markup Language (SAML) 2,0 e, em seguida, mapeando os usuários para as funções incorporadas do storage array.



O SAML é um recurso incorporado no storage array (nível de firmware 8,42 e superior) e só é configurável a partir da interface de usuário do Gerenciador de sistemas do SANtricity.

Introdução ao gerenciamento de chaves externas - SANtricity CLI

Uma chave de segurança é uma cadeia de caracteres, que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. Ao usar o gerenciamento de chaves externas, você cria e mantém chaves de segurança em um servidor de gerenciamento de chaves

Consulte a ajuda on-line do Gerenciador de sistemas do SANtricity para obter informações conceituais sobre o uso de servidores de gerenciamento de chaves externas e chaves de segurança.

O seguinte é o fluxo de trabalho básico para a implementação de chaves de segurança externas:

1. **Gerar uma solicitação de assinatura de certificado**
2. **Obtenha certificados de cliente e servidor a partir do servidor KMIP**
3. **Instale o certificado do cliente**
4. **Defina o endereço IP e o número da porta do servidor KMIP**
5. **Teste a comunicação com o servidor KMIP**
6. * Criar uma chave de segurança de storage array*
7. **Validar a chave de segurança**

Etapas do fluxo de trabalho

Tanto o gerenciamento de certificados quanto o gerenciamento de chaves externas são novos recursos de segurança com a versão SANtricity11,40. Para começar, use as seguintes etapas básicas:

1. Gerar uma solicitação de assinatura de certificado usando o `save storageArray keyManagementClientCSR` comando. [Gerar solicitação de assinatura de certificado de Gerenciamento de chaves](#)Consulte .
2. A partir do servidor KMIP, solicite um cliente e um certificado de servidor.
3. Instale o certificado do cliente usando o `download storageArray keyManagementCertificate` comando com o `certificateType` parâmetro definido como `client`. [Instale o certificado de gerenciamento de chaves externas do storage array](#)Consulte .
4. Instale o certificado do servidor usando o `download storageArray keyManagementCertificate` comando com o `certificateType` parâmetro definido como `server`. [Instale o certificado de gerenciamento de chaves externas do storage array](#)Consulte .
5. Defina o endereço IP e o número da porta do servidor de gerenciamento de chaves usando o `set storageArray externalKeyManagement` comando. [Defina as configurações de gerenciamento de chaves externas](#)Consulte .
6. Teste a comunicação com o servidor de gerenciamento de chaves externo usando o `start storageArray externalKeyManagement test` comando. [Testar a comunicação de gerenciamento de chaves externas](#)Consulte .
7. Crie uma chave de segurança usando o `create storageArray securityKey` comando. [Criar chave de segurança](#)Consulte .
8. Valide a chave de segurança usando o `validate storageArray securityKey` comando. [Valide a chave de segurança interna ou externa](#)Consulte .

Introdução ao gerenciamento de chaves internas - SANtricity CLI

Uma chave de segurança é uma cadeia de caracteres, que é compartilhada entre as unidades e controladores habilitados para segurança em um storage array. Ao usar o gerenciamento de chaves internas, você cria e mantém chaves de segurança na memória persistente do controlador.

Consulte a ajuda on-line do Gerenciador de sistemas do SANtricity para obter informações conceituais sobre como usar chaves de segurança internas.

O seguinte é o fluxo de trabalho básico para usar chaves de segurança internas:

1. * Criar chaves de segurança*
2. * Definir chaves de segurança*
3. **Validar chave de segurança**

Etapas do fluxo de trabalho

Os seguintes comandos começam com as chaves de segurança internas:

1. Crie uma chave de segurança de storage array, usando o `create storageArray securityKey` comando. [Criando uma chave de segurança de storage array](#)Consulte .
2. Defina a chave de segurança do storage array, usando o `set storageArray securityKey` comando. [Definir uma chave de segurança de storage array](#)Consulte .

3. Valide a chave de segurança usando o `validate storageArray securityKey` comando. [Validar uma chave de segurança de storage array](#)Consulte .

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

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

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