G

SANtricity commands

NetApp
June 16, 2025

Índice

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 ative 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 carateres, 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 chavesConsulte .
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 arrayConsulte .
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 arrayConsulte .
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 externasConsulte .
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 externasConsulte .
7. Crie uma chave de segurança usando o `create storageArray securityKey` comando. Criar chave de segurançaConsulte .
8. Valide a chave de segurança usando o `validate storageArray securityKey` comando. Valide a chave de segurança interna ou externaConsulte .

Introdução ao gerenciamento de chaves internas - SANtricity CLI

Uma chave de segurança é uma cadeia de carateres, 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 arrayConsulte .
2. Defina a chave de segurança do storage array, usando o `set storageArray securityKey` comando. Definir uma chave de segurança de storage arrayConsulte .

3. Valide a chave de segurança usando o `validate storageArray securityKey` comando. Validar uma chave de segurança de storage arrayConsulte .

Informações sobre direitos autorais

Informações sobre marcas comerciais