



Diretrizes de endurecimento do ONTAP

ONTAP 9

NetApp
January 17, 2025

Índice

Diretrizes de endurecimento do ONTAP	1
Visão geral do fortalecimento da segurança do ONTAP	1
Validação de imagem ONTAP	1
Contas de administrador de armazenamento local	2
Métodos de administração do sistema	18
Proteção autônoma contra ransomware da ONTAP	24
Auditoria de sistema administrativo de storage	24
Criptografia de storage	26
Criptografia de replicação de dados	28
Criptografia de dados em trânsito IPsec	29
Modo FIPS e gerenciamento TLS e SSL	30
Crie um certificado digital assinado pela CA	32
Protocolo de estado do certificado online	33
Gerenciamento do SSHv2	33
NetApp AutoSupport	34
Protocolo de hora de rede	35
Contas locais do sistema de arquivos nas (grupo de trabalho CIFS)	36
Auditoria do sistema de arquivos nas	36
Configure e ative a assinatura e a vedação CIFS SMB	38
Proteção do NFS	39
Ative a assinatura e a vedação do protocolo Lightweight Directory Access	41
Crie e use um FPolicy do NetApp	42
Segurança LIF	44
Segurança de protocolo e porta	44

Diretrizes de endurecimento do ONTAP

Visão geral do fortalecimento da segurança do ONTAP

O ONTAP fornece um conjunto de controles que permitem proteger o sistema operacional de storage ONTAP, o software de gerenciamento de dados líder do setor. Use as orientações e as configurações do ONTAP para ajudar sua organização a cumprir os objetivos de segurança prescritos para confidencialidade, integridade e disponibilidade do sistema de informações.

A evolução do cenário atual de ameaças apresenta uma organização com desafios únicos para proteger seus ativos mais valiosos: Dados e informações. As ameaças e vulnerabilidades avançadas e dinâmicas que enfrentamos estão cada vez mais aumentando em sofisticação. Juntamente com um aumento na eficácia das técnicas de ofuscação e reconhecimento por parte de potenciais intrusos, os gestores de sistemas devem abordar a segurança de dados e informações de forma proativa.



A partir de julho de 2024, o conteúdo de relatórios técnicos publicados anteriormente como PDFs foi integrado à documentação do produto ONTAP. A documentação de segurança do ONTAP agora inclui conteúdo de *TR-4569: Guia de proteção de segurança para ONTAP*.

Validação de imagem ONTAP

O ONTAP fornece mecanismos para garantir que a imagem ONTAP seja válida na atualização e no momento da inicialização.

Atualizar validação de imagem

A assinatura de código ajuda a verificar se as imagens ONTAP instaladas por meio de atualizações de imagem sem interrupções ou atualizações automatizadas de imagem sem interrupções, CLIs ou APIs ONTAP são autenticamente produzidas pela NetApp e não foram adulteradas. A validação da imagem de atualização foi introduzida no ONTAP 9.3.

Esse recurso é um aprimoramento de segurança sem toque para atualização ou reversão do ONTAP. Não se espera que o usuário faça nada de diferente, exceto para opcionalmente verificar a assinatura de nível superior `image.tgz`.

Validação de imagem no momento da inicialização

A partir do ONTAP 9.4, a inicialização segura da interface de firmware extensível unificada (UEFI) é ativada para sistemas NetApp AFF A800, AFF A220, FAS2750 e FAS2720 e sistemas subsequentes de próxima geração que utilizam BIOS UEFI.

Durante a ativação, o bootloader valida o banco de dados da lista de permissões de chaves de inicialização seguras com a assinatura associada a cada módulo carregado. Depois que cada módulo é validado e carregado, o processo de inicialização continua com a inicialização do ONTAP. Se a validação da assinatura falhar para qualquer módulo, o sistema será reinicializado.



Esses itens se aplicam às imagens do ONTAP e ao BIOS da plataforma.

Contas de administrador de armazenamento local

Funções, aplicativos e autenticação

O ONTAP fornece à empresa com consciência de segurança a capacidade de fornecer acesso granular a diferentes administradores por meio de diferentes aplicativos e métodos de login. Isso ajuda os clientes a criar um modelo de confiança zero centrado nos dados.

Estas são as funções disponíveis para administradores de máquinas virtuais de administração e armazenamento. Os métodos de aplicação de início de sessão e os métodos de autenticação de início de sessão são especificados.

Funções

Com o controle de acesso baseado em funções (RBAC), os usuários têm acesso apenas aos sistemas e opções necessários para suas funções e funções de trabalho. A solução RBAC no ONTAP limita o acesso administrativo dos usuários ao nível concedido para sua função definida, o que permite que os administradores gerenciem os usuários por função atribuída. O ONTAP fornece várias funções predefinidas. Os operadores e administradores podem criar, modificar ou excluir funções de controle de acesso personalizadas e podem especificar restrições de conta para funções específicas.

Funções predefinidas para administradores de cluster

Esta função...	Tem este nível de acesso...	Para os seguintes comandos ou diretórios de comandos
admin	Tudo	Todos os diretórios de comando (DEFAULT)
admin-no-fsa (Disponível a partir de ONTAP 9.12,1)	Leitura/escrita	<ul style="list-style-type: none">• Todos os diretórios de comando (DEFAULT)• security login rest-role• security login role

Somente leitura	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Nenhum
volume file show-disk-usage	autosupport	Tudo
<ul style="list-style-type: none"> • set • system node autosupport 	Nenhum	Todos os outros diretórios de comando (DEFAULT)
backup	Tudo	vserver services ndmp
Somente leitura	volume	Nenhum
Todos os outros diretórios de comando (DEFAULT)	readonly	Tudo

<ul style="list-style-type: none"> • security login password <p>Apenas para gerir a palavra-passe local da conta de utilizador e as informações das chaves</p> <ul style="list-style-type: none"> • set 	Nenhum	security
Somente leitura	Todos os outros diretórios de comando (DEFAULT)	none



A `autosupport` função é atribuída à conta predefinida `autosupport`, que é usada pelo AutoSupport OnDemand. O ONTAP impede que você modifique ou exclua a `autosupport` conta. O ONTAP também impede que você atribua `autosupport` a função a outras contas de usuário.

Funções predefinidas para administradores de máquina virtual de storage (SVM)

Nome da função	Recursos
<code>vsadmin</code>	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Gerenciar LUNs • Executar operações SnapLock, exceto exclusão privilegiada • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede • Monitorar a integridade do SVM

vsadmin-volume	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, incluindo movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Gerenciar LUNs • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Monitorar a interface de rede • Monitorar a integridade do SVM
vsadmin-protocol	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurar serviços: DNS, LDAP e NIS • Gerenciar LUNs • Monitorar a interface de rede • Monitorar a integridade do SVM
vsadmin-backup	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Gerenciar operações NDMP • Faça uma leitura/gravação de volume restaurada • Gerencie relacionamentos do SnapMirror e cópias Snapshot • Exibir volumes e informações de rede
vsadmin-snaplock	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Gerencie volumes, exceto movimentos de volume • Gerencie cotas, qtrees, cópias Snapshot e arquivos • Executar operações SnapLock, incluindo exclusão privilegiada • Configurar protocolos: NFS e SMB • Configurar serviços: DNS, LDAP e NIS • Monitorizar trabalhos • Monitore conexões de rede e interface de rede

vsadmin-readonly	<ul style="list-style-type: none"> • Gerencie a senha local da própria conta de usuário e as informações chave • Monitorar a integridade do SVM • Monitorar a interface de rede • Visualizar volumes e LUNs • Exibir serviços e protocolos
------------------	---

Métodos de aplicação

O método de aplicação especifica o tipo de acesso do método de início de sessão. Os valores possíveis incluem `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, e `telnet`.

Definir este parâmetro para `service-processor` conceder ao utilizador acesso ao processador de serviço. Quando este parâmetro está definido como `service-processor`, o `-authentication-method` parâmetro tem de ser definido como `password` porque o processador de serviço suporta apenas `password` a autenticação. As contas de usuário do SVM não podem acessar o processador de serviços. Portanto, os operadores e administradores não podem usar o `-vserver` parâmetro quando este parâmetro está definido como `service-processor`.

Para restringir ainda mais o acesso ao `service-processor` use o comando `system service-processor ssh add-allowed-addresses`. O comando `system service-processor api-service` pode ser usado para atualizar as configurações e certificados.

Por motivos de segurança, o Telnet e o Shell remoto (RSH) são desativados por padrão porque o NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro. Se houver um requisito ou necessidade exclusiva para Telnet ou RSH, eles devem ser ativados.

O `security protocol modify` comando modifica a configuração existente em todo o cluster do RSH e Telnet. Ative o RSH e o Telnet no cluster definindo o campo ativado para `true`.

Métodos de autenticação

O parâmetro método de autenticação especifica o método de autenticação usado para logins.

Método de autenticação	Descrição
<code>cert</code>	Autenticação de certificado SSL
<code>community</code>	Strings de comunidade SNMP
<code>domain</code>	Autenticação do Active Directory
<code>nsswitch</code>	Autenticação LDAP ou NIS
<code>password</code>	Palavra-passe
<code>publickey</code>	Autenticação de chave pública
<code>usm</code>	Modelo de segurança do utilizador SNMP



O uso de NIS não é recomendado devido a falhas de segurança do protocolo.

A partir do ONTAP 9.3, a autenticação de dois fatores encadeada está disponível para contas SSH locais `admin` usando `publickey` e `password` como os dois métodos de autenticação. Além do `-authentication-method` campo no `security login` comando, um novo campo chamado `-second-authentication-method` foi adicionado. `publickey` ou `password` pode ser especificado como `-authentication-method` ou `-second-authentication-method`. No entanto, durante a autenticação SSH, a ordem é sempre `publickey` com autenticação parcial, seguida pelo prompt de senha para autenticação completa.

```
[user@host01 ~]$ ssh ontap.netapp.local
Authenticated with partial success.
Password:
cluster1::>
```

Começando com ONTAP 9.4, `nsswitch` pode ser usado como um segundo método de autenticação com `publickey`.

A partir do ONTAP 9.12,1, o FIDO2 também pode ser usado para autenticação SSH usando um dispositivo de autenticação de hardware YubiKey ou outros dispositivos compatíveis com o FIDO2.

Começando com ONTAP 9.13,1:

- `domain` as contas podem ser usadas como um segundo método de autenticação com `publickey`.
- Senha única baseada no tempo (`totp`) é uma senha temporária gerada por um algoritmo que usa a hora atual do dia como um de seus fatores de autenticação para o segundo método de autenticação.
- A revogação de chaves públicas é suportada com chaves públicas SSH, bem como certificados que serão verificados para expiração/revogação durante o SSH.

Para obter mais informações sobre autenticação multifator (MFA) para Gerenciador de sistemas, Active IQ Unified Manager e SSH da ONTAP, ["TR-4647: Autenticação multifator no ONTAP 9"](#) consulte .

Contas administrativas padrão

A conta de administrador deve ser restrita porque a função de administrador tem acesso permitido usando todos os aplicativos. A conta `diag` permite o acesso ao shell do sistema e deve ser reservada apenas para o suporte técnico para executar tarefas de solução de problemas.

Existem duas contas administrativas padrão: `admin` e `diag`.

As contas órfãs são um grande vetor de segurança que muitas vezes leva a vulnerabilidades, incluindo a escalação do Privileges. Estas são contas desnecessárias e não utilizadas que permanecem no repositório de contas de usuário. São principalmente contas padrão que nunca foram usadas ou para as quais senhas nunca foram atualizadas ou alteradas. Para resolver esse problema, o ONTAP suporta a remoção e renomeação de contas.



O ONTAP não pode remover ou renomear contas internas. No entanto, o NetApp recomenda bloquear quaisquer contas internas desnecessárias com o comando `LOCK`.

Embora as contas órfãs sejam um problema de segurança significativo, o NetApp recomenda fortemente

testar o efeito da remoção de contas do repositório de contas local.

Listar contas locais

Para listar as contas locais, execute o `security login show` comando.

```
cluster1::*> security login show -vserver cluster1

Vserver: cluster1

User/Group Name      Application      Authentication Method      Role Name      Acct Locked      Is-Nsswitch Group
-----
admin                console         password      admin          no           no
admin                http           password      admin          no           no
admin                ontapi        password      admin          no           no
admin                service-processor password      admin          no           no
admin                ssh           password      admin          no           no
autosupport         console         password      autosupport    no           no
6 entries were displayed.
```

Definir a palavra-passe da conta de diagnóstico (diag)

Uma conta de diagnóstico nomeada `diag` é fornecida com o sistema de storage. Você pode usar a `diag` conta para executar tarefas de solução de problemas no `systemshell`. A `diag` conta é a única conta que pode ser usada para acessar o `systemshell` através do `diag` comando ``systemshell`` privilegiado .



O `systemshell` e a conta associada `diag` destinam-se a fins de diagnóstico de baixo nível. Seu acesso requer o nível de privilégio de diagnóstico e é reservado apenas para ser usado com orientação do suporte técnico para executar tarefas de solução de problemas. Nem a `diag` conta nem o `systemshell` destinam-se a fins administrativos gerais.

Antes de começar

Antes de aceder ao `systemshell`, tem de definir a `diag` palavra-passe da conta utilizando o `security login password` comando . Você deve usar princípios de senha fortes e alterar a `diag` senha em intervalos regulares.

Passos

1. Defina a `diag` senha do usuário da conta:

```
cluster1::> set -privilege diag
```

```
Warning: These diagnostic commands are for use by NetApp personnel only.  
Do you want to continue? \{y|n\}: y
```

```
cluster1::*> systemshell -node node-01  
      (system node systemshell)  
diag@node-01's password:
```

```
Warning: The system shell provides access to low-level  
diagnostic tools that can cause irreparable damage to  
the system if not used properly. Use this environment  
only when directed to do so by support personnel.
```

```
node-01%
```

Verificação multi-admin

A partir do ONTAP 9.11,1, é possível usar a verificação multiadministrador (MAV) para permitir que determinadas operações, como a exclusão de volumes ou cópias Snapshot, sejam executadas somente após aprovações de administradores designados. Isso impede que administradores comprometidos, maliciosos ou inexperientes façam alterações indesejáveis ou excluam dados.

A configuração do MAV consiste no seguinte:

- ["Criando um ou mais grupos de aprovação de administrador."](#)
- ["Habilitando a funcionalidade de verificação de vários administradores."](#)
- ["Adicionar ou modificar regras."](#)

Após a configuração inicial, somente os administradores de um grupo de aprovação MAV (administradores MAV) podem modificar esses elementos.

Quando o MAV está ativado, a conclusão de cada operação protegida requer três passos:

1. Quando um utilizador inicia a operação, a ["a solicitação é gerada."](#)
2. Antes de poder ser executado, o número necessário de ["Os administradores do MAV devem aprovar."](#)
3. Após a aprovação, o utilizador conclui a operação.

O MAV não se destina a ser usado com volumes ou fluxos de trabalho que envolvam automação pesada, pois cada tarefa automatizada requer aprovação antes que a operação possa ser concluída. Se você quiser usar automação e MAV juntos, a NetApp recomenda que você use consultas para operações MAV específicas. Por exemplo, você pode aplicar `volume delete` regras MAV apenas a volumes em que a automação não está envolvida e pode designar esses volumes com um esquema de nomenclatura específico.

Para obter informações mais detalhadas sobre o MAV, consulte o ["Documentação de verificação de vários administradores do ONTAP"](#).

Bloqueio de cópias snapshot

O bloqueio de cópias snapshot é uma funcionalidade do SnapLock em que as cópias Snapshot são tornadas indelévels manual ou automaticamente, com um período de retenção na política de Snapshot de volume. O objetivo do bloqueio de cópias Snapshot é impedir que administradores desonestos ou não confiáveis excluam snapshots em sistemas ONTAP primário ou secundário.

O bloqueio de cópia Snapshot foi introduzido no ONTAP 9.12.1. O bloqueio de cópias snapshot também é conhecido como bloqueio instantâneo à prova de violação. Embora isso exija a licença SnapLock e a inicialização do relógio de conformidade, o bloqueio de cópias snapshot não está relacionado ao SnapLock Compliance ou ao SnapLock Enterprise. Não há administrador de storage confiável, assim como o SnapLock Enterprise e ele não protege a infraestrutura de storage físico subjacente, como o SnapLock Compliance. Isso é uma melhoria em relação às cópias Snapshot do SnapVaulting para um sistema secundário. A recuperação rápida de snapshots bloqueados em sistemas primários pode ser obtida para restaurar volumes corrompidos por ransomware.

Para obter mais detalhes sobre o bloqueio de cópias instantâneas, consulte "[Documentação do ONTAP](#)".

Configure o acesso à API baseado em certificado

Em vez de autenticação de ID de usuário e senha para acesso à API REST ou à API SDK de gerenciamento do NetApp ao ONTAP, a autenticação baseada em certificado deve ser usada.



Como alternativa à autenticação baseada em certificado para API REST, use "[Autenticação baseada em token OAuth 2,0](#)".)

Você pode gerar e instalar um certificado autoassinado no ONTAP conforme descrito nestas etapas.

Passos

1. Usando OpenSSL, gere um certificado executando o seguinte comando:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout test.key
-out test.pem \> -subj "/C=US/ST=NC/L=RTP/O=NetApp/CN=cert_user"
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'test.key'
```

Este comando gera um certificado público nomeado `test.pem` e uma chave privada chamada `key.out`. O nome comum, CN, corresponde ao ID de usuário do ONTAP.

2. Instale o conteúdo do certificado público no formato pem (Privacy Enhanced mail) no ONTAP executando o seguinte comando e colando o conteúdo do certificado quando solicitado:

```
security certificate install -type client-ca -vserver cluster1
```

Please enter Certificate: Press <Enter> when done

3. Ative o ONTAP para permitir o acesso do cliente através de SSL e definir a ID do usuário para acesso à API.

```
security ssl modify -vserver cluster1 -client-enabled true
security login create -user-or-group-name cert_user -application ontapi
-authmethod cert -role admin -vserver cluster1
```

No exemplo a seguir, o ID de usuário `cert_user` agora está habilitado para usar o acesso à API autenticado por certificado. Um script Python simples do SDK para gerenciamento usando `cert_user` para exibir a versão do ONTAP aparece da seguinte forma:

```
#!/usr/bin/python

import sys
sys.path.append("/home/admin/netapp-manageability-sdk-9.5/netapp-
manageability-sdk-9.5/lib/python/NetApp")
from NaServer import *

cluster = "cluster1"
transport = "HTTPS"
port = 443
style = "CERTIFICATE"
cert = "test.pem"
key = "test.key"

s = NaServer(cluster, 1, 30)
s.set_transport_type(transport)
s.set_port(port)
s.set_style(style)
s.set_server_cert_verification(0)
s.set_client_cert_and_key(cert, key)

api = NaElement("system-get-version")
output = s.invoke_elem(api)
if (output.results_status() == "failed"):
    r = output.results_reason()
    print("Failed: " + str(r))
    sys.exit(2)

ontap_version = output.child_get_string("version")
print ("V: " + ontap_version)
```

A saída do script exibe a versão do ONTAP.

```
./version.py
```

```
V: NetApp Release 9.5RC1: Sat Nov 10 05:13:42 UTC 2018
```

4. Para executar a autenticação baseada em certificado com a API REST do ONTAP, execute as seguintes etapas:

a. No ONTAP, defina a ID do usuário para acesso http:

```
security login create -user-or-group-name cert_user -application http
-authmethod cert -role admin -vserver cluster1
```

b. No seu cliente Linux, execute o seguinte comando que produz a versão ONTAP como saída:

```
curl -k --cert-type PEM --cert ./test.pem --key-type PEM --key ./test.key -X GET "https://cluster1/api/cluster?fields=version"
{
  "version": {
    "full": "NetApp Release 9.7P1: Thu Feb 27 01:25:24 UTC 2020",
    "generation": 9,
    "major": 7,
    "minor": 0
  },
  "_links": {
    "self": {
      "href": "/api/cluster"
    }
  }
}
```

Mais informações

- ["Autenticação baseada em certificado com o SDK de gerenciamento do NetApp para ONTAP"](#).

Autenticação baseada em token ONTAP OAuth 2,0 para API REST

Como alternativa à autenticação baseada em certificado, você pode usar a autenticação baseada em token OAuth 2,0 para API REST.

A partir do ONTAP 9.14,1, você tem a opção de controlar o acesso aos clusters do ONTAP usando a estrutura autorização aberta (OAuth 2,0). Você pode configurar esse recurso usando qualquer uma das interfaces administrativas do ONTAP, incluindo a CLI do ONTAP, o Gerenciador do sistema e a API REST. No entanto, as decisões de autorização e controle de acesso do OAuth 2,0 só podem ser aplicadas quando um cliente acessa o ONTAP usando a API REST.

Os tokens OAuth 2,0 substituem senhas para autenticação de conta de usuário.

Para obter mais informações sobre como usar o OAuth 2,0, consulte ["Documentação do ONTAP sobre autenticação e autorização usando OAuth 2,0"](#).

Parâmetros de login e senha

Uma postura de segurança eficaz adere às políticas organizacionais estabelecidas, diretrizes e qualquer governança ou padrões que se apliquem à organização. Exemplos desses requisitos incluem vida útil do nome de usuário, requisitos de comprimento de senha, requisitos de caracteres e o armazenamento de tais contas. A solução ONTAP fornece recursos e funções para lidar com essas construções de segurança.

Novos recursos de conta local

Para oferecer suporte às políticas, diretrizes ou padrões de contas de usuário de uma organização, incluindo governança, a seguinte funcionalidade é suportada no ONTAP:

- Configurando políticas de senha para impor um número mínimo de dígitos, caracteres minúsculos ou caracteres maiúsculos
- Exigindo um atraso após uma tentativa de login com falha
- Definir o limite inativo da conta
- A expirar uma conta de utilizador
- Exibindo uma mensagem de aviso de expiração de senha
- Notificação de um login inválido



As configurações configuráveis são gerenciadas usando o comando `security login role config modify`.

Suporte SHA-512

Para melhorar a segurança da senha, o ONTAP 9 suporta a função hash de senha SHA-2 e usa o padrão SHA-512 para hashing de senhas recém-criadas ou alteradas. Os operadores e administradores também podem expirar ou bloquear contas conforme necessário.

As contas de usuário pré-existentes do ONTAP 9 com senhas inalteradas continuam a usar a função hash MD5 após a atualização para o ONTAP 9.0 ou posterior. No entanto, a NetApp recomenda fortemente que essas contas de usuário migrem para a solução SHA-512 mais segura, fazendo com que os usuários alterem suas senhas.

A funcionalidade hash de senha permite executar as seguintes tarefas:

- Exibir contas de usuário que correspondem à função hash especificada:

```
cluster1::*> security login show -user-or-group-name NewAdmin -fields
hash-function
vserver user-or-group-name application authentication-method hash-
function
-----
-----
cluster1 NewAdmin          console    password    sha512
cluster1 NewAdmin          ontapi     password    sha512
cluster1 NewAdmin          ssh        password    sha512
```

- As contas expiram que usam uma função hash especificada (por exemplo, MD5), que força os usuários a alterar suas senhas no próximo login:

```
cluster1::*> security login expire-password -vserver * -username * -hash
-function md5
```


- Bloqueie contas com senhas que usam a função hash especificada.

```
cluster1::*> security login lock -vserver * -username * -hash-function md5
```

A função hash de senha é desconhecida para o usuário interno `autosupport` no SVM administrativo do cluster. Esta questão é cosmética. A função hash é desconhecida porque este usuário interno não tem uma senha configurada por padrão.

- Para exibir a função hash de senha para `autosupport` o usuário, execute os seguintes comandos:

```
::> set advanced
::> security login show -user-or-group-name autosupport -instance

                Vserver: cluster1
User Name or Group Name: autosupport
          Application: console
Authentication Method: password
Remote Switch IP Address: -
                Role Name: autosupport
Account Locked: no
          Comment Text: -
Whether Ns-switch Group: no
Password Hash Function: unknown
Second Authentication Method2: none
```

- Para definir a função hash de senha (padrão: SHA512), execute o seguinte comando:

```
::> security login password -username autosupport
```

Não importa para que a senha está definida.

```
security login show -user-or-group-name autosupport -instance
```

```
          Vserver: cluster1
User Name or Group Name: autosupport
          Application: console
          Authentication Method: password
Remote Switch IP Address: -
          Role Name: autosupport
          Account Locked: no
          Comment Text: -
Whether Ns-switch Group: no
          Password Hash Function: sha512
Second Authentication Method2: none
```

Parâmetros da palavra-passe

A solução ONTAP suporta parâmetros de senha que atendem e suportam requisitos e diretrizes de políticas organizacionais.

Atributo	Descrição	Padrão	Alcance
username-minlength	É necessário um comprimento mínimo do nome de utilizador	3	3-16
username-alphanum	Nome de utilizador alfanumérico	desativado	Ativado/desativado
passwd-minlength	É necessário um comprimento mínimo da palavra-passe	8	3-64
passwd-alphanum	Palavra-passe alfanumérica	ativado	Ativado/desativado
passwd-min-special-chars	Número mínimo de caracteres especiais necessários na senha	0	0-64
passwd-expiry-time	Tempo de expiração da senha (em dias)	Ilimitado, o que significa que as senhas nunca expiram	0-ilimitado 0 expiram agora
require-initial-passwd-update	Requer atualização inicial de senha no primeiro login	Desativado	Ativado/desativado Alterações permitidas através de console ou SSH
max-failed-login-attempts	Número máximo de tentativas falhadas	0, não bloqueie a conta	-

Atributo	Descrição	Padrão	Alcance
lockout-duration	Período máximo de bloqueio (em dias)	O padrão é 0, o que significa que a conta está bloqueada por um dia	-
disallowed-reuse	Não permitir as últimas palavras-passe N.	6	O mínimo é 6
change-delay	Atraso entre alterações de senha (em dias)	0	-
delay-after-failed-login	Atraso após cada tentativa de início de sessão falhada (em segundos)	4	-
passwd-min-lowercase-chars	Número mínimo de caracteres alfabéticos minúsculos necessário na senha	0, que não requer caracteres minúsculos	0-64
passwd-min-uppercase-chars	Número mínimo de caracteres alfabéticos maiúsculos necessário	0, que não requer caracteres maiúsculos	0-64
passwd-min-digits	Número mínimo de dígitos necessário na senha	0, que não requer dígitos	0-64
passwd-expiry-warn-time	Apresentar mensagem de aviso antes da expiração da palavra-passe (em dias)	Ilimitado, o que significa nunca avisar sobre a expiração da senha	0, o que significa avisar o usuário sobre a expiração da senha após cada login bem-sucedido
account-expiry-time	A conta expira em N dias	Ilimitado, o que significa que as contas nunca expiram	O tempo de expiração da conta deve ser maior que o limite inativo da conta
account-inactive-limit	Duração máxima de inatividade antes da expiração da conta (em dias)	Ilimitado, o que significa que as contas inativas nunca expiram	O limite inativo da conta deve ser inferior ao tempo de expiração da conta

Exemplo

```
cluster1::*> security login role config show -vserver cluster1 -role admin

                                Vserver: cluster1
                                Role Name: admin
                                Minimum Username Length Required: 3
                                    Username Alpha-Numeric: disabled
                                Minimum Password Length Required: 8
                                    Password Alpha-Numeric: enabled
                                Minimum Number of Special Characters Required in the Password: 0
                                    Password Expires In (Days): unlimited
                                Require Initial Password Update on First Login: disabled
                                Maximum Number of Failed Attempts: 0
                                    Maximum Lockout Period (Days): 0
                                        Disallow Last 'N' Passwords: 6
                                    Delay Between Password Changes (Days): 0
                                        Delay after Each Failed Login Attempt (Secs): 4
                                Minimum Number of Lowercase Alphabetic Characters Required in the
                                Password: 0
                                Minimum Number of Uppercase Alphabetic Characters Required in the
                                Password: 0
                                Minimum Number of Digits Required in the Password: 0
                                Display Warning Message Days Prior to Password Expiry (Days): unlimited
                                    Account Expires in (Days): unlimited
                                Maximum Duration of Inactivity before Account Expiration (Days): unlimited
```



A partir de 9.14.1, há maior complexidade e regras de bloqueio para senhas. Isso se aplica apenas a novas instalações do ONTAP.

Métodos de administração do sistema

Estes são parâmetros importantes para fortalecer a administração do sistema ONTAP.

Acesso à linha de comando

Estabelecer acesso seguro aos sistemas é uma parte essencial da manutenção de uma solução segura. As opções de acesso de linha de comando mais comuns são SSH, Telnet e RSH. Destes, o SSH é a melhor prática mais segura e padrão do setor para acesso remoto à linha de comando. A NetApp recomenda fortemente o uso de SSH para acesso de linha de comando à solução ONTAP.

Configurações SSH

O `security ssh show` comando mostra as configurações dos algoritmos de troca de chaves SSH, cifras e algoritmos MAC para o cluster e SVMs. O método de troca de chaves usa esses algoritmos e cifras para especificar como as chaves de sessão únicas são geradas para criptografia e autenticação e como a autenticação do servidor ocorre.

```
cluster1::> security ssh show
```

Vserver	Ciphers	Key Exchange Algorithms	MAC Algorithms
nsadhanacluster-2	aes256-ctr, aes192-ctr, aes128-ctr	diffie-helman-group- exchange-sha256, ecdh-sha2-nistp384	hmac-sha2-256 hmac-sha2-512
vs0	aes128-gcm	curve25519-sha256	hmac-sha1
vs1	aes256-ctr, aes192-ctr, aes128-ctr, 3des-cbc, aes128-gcm	diffie-hellman-group- exchange-sha256 ecdh-sha2-nistp384 ecdh-sha2-nistp512	hmac-sha1-96 hmac-sha2-256 hmac-sha2-256- etm hmac-sha2-512

3 entries were displayed.

Banners de login

Os banners de login permitem que uma organização apresente quaisquer operadores, administradores e até mesmo errantes com termos e condições de uso aceitável, e eles indicam quem é permitido o acesso ao sistema. Esta abordagem é útil para estabelecer expectativa de acesso e uso do sistema. O `security login banner modify` comando modifica o banner de login. O banner de login é exibido imediatamente antes da etapa de autenticação durante o processo de login do dispositivo SSH e console. O texto do banner deve estar em aspas duplas (" "), como mostrado no exemplo a seguir.

```
cluster1::> security login banner modify -vserver cluster1 -message  
"Authorized users ONLY!"
```

Parâmetros de banner de login

Parâmetro	Descrição
<code>vserver</code>	Use este parâmetro para especificar o SVM com o banner modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster. A mensagem no nível do cluster é usada como padrão para SVMs de dados que não têm uma mensagem definida.

Parâmetro	Descrição
message	<p>Este parâmetro opcional pode ser usado para especificar uma mensagem de banner de login. Se o cluster tiver um conjunto de mensagens de banner de login, o banner de login do cluster também será usado por todos os SVMs de dados. A configuração de um banner de login do SVM substitui a exibição do banner de login do cluster. Para redefinir um banner de login SVM de dados para usar o banner de login do cluster, use este parâmetro com o valor "-".</p> <p>Se você usar esse parâmetro, o banner de login não poderá conter novas linhas (também conhecidas como extremidades de linhas [EOLS] ou quebras de linha). Para inserir uma mensagem de banner de login com novas linhas, não especifique nenhum parâmetro. Você é solicitado a inserir a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas.</p> <p>Carateres não ASCII devem usar Unicode UTF-8.</p>
uri	<p>`(ftp`</p>
http://(hostname	<p>IPv4`</p> <p>Use este parâmetro para especificar o URI a partir do qual o banner de login é baixado.</p> <p>A mensagem não deve exceder 2048 bytes de comprimento. Carateres não ASCII devem ser fornecidos como Unicode UTF-8.</p>

Mensagem do dia

O `security login motd modify` comando atualiza a mensagem do dia (MOTD).

Existem duas categorias de MOTD: O MOTD em nível de cluster e os dados SVM-nível MOTD. Um usuário que faz login no clustershell de um SVM de dados pode ver duas mensagens: O MOTD de nível de cluster seguido pelo MOTD de nível SVM para esse SVM.

O administrador do cluster pode ativar ou desativar o MOTD no nível do cluster em cada SVM individualmente, se necessário. Se o administrador do cluster desativar o MOTD no nível do cluster para um SVM, um usuário que faz login no SVM não verá a mensagem no nível do cluster. Apenas um administrador de cluster pode ativar ou desativar a mensagem de nível de cluster.

Parâmetro MOTD	Descrição
SVM	Use este parâmetro para especificar o SVM para o qual o MOTD é modificado. Use o nome do administrador do cluster SVM para modificar a mensagem no nível do cluster.

Parâmetro MOTD	Descrição
mensagem	<p>Este parâmetro opcional pode ser usado para especificar uma mensagem. Se você usar este parâmetro, o MOTD não pode conter novas linhas. Se você não especificar nenhum parâmetro além do <code>-vserver</code> parâmetro, será solicitado que você insira a mensagem interativamente. As mensagens inseridas interativamente podem conter novas linhas. Caracteres não ASCII devem ser fornecidos como Unicode UTF-8. A mensagem pode conter conteúdo gerado dinamicamente usando as seguintes sequências de escape:</p> <ul style="list-style-type: none"> • <code>\</code> - Um único caráter de reação • <code>\b</code> - Sem saída (suportado apenas para compatibilidade com Linux) • <code>\C</code> - Nome do cluster • <code>\d</code> - Data atual como definido no nó de login • <code>\t</code> - Hora atual como definido no nó de login • <code>\I</code> - Endereço IP de LIF de entrada (imprime console para um <code>console login</code>) • <code>\l</code> - Nome do dispositivo de login (imprime console para um <code>console login</code>) • <code>\L</code> - Último login para o usuário em qualquer nó no cluster • <code>\m</code> - Arquitetura da máquina • <code>\n</code> - Nome do nó ou data SVM • <code>\N</code> - Nome do usuário que faz login • <code>\o</code> - O mesmo que <code>o</code>. Fornecido para compatibilidade com Linux. • <code>\O</code> - Nome de domínio DNS do nó. Observe que a saída depende da configuração da rede e pode estar vazia. • <code>\r</code> - Número de versão do software • <code>\s</code> - Nome do sistema operacional • <code>\u</code> - Número de sessões ativas de clustershell no nó local. Para o administrador do cluster: Todos os usuários do clustershell. Para os dados SVM admin: Apenas sessões ativas para esses dados SVM. • <code>\U</code> - Igual a <code>\u</code>, mas tem <code>user</code> ou <code>users</code> anexa • <code>\v</code> - String de versão de cluster eficaz • <code>\W</code> - Sessões ativas em todo o cluster para o usuário que faz (<code>`who`login</code>)

Para obter mais informações sobre como configurar a mensagem do dia no ONTAP, consulte "[Documentação do ONTAP na mensagem do dia](#)".

Tempo limite da sessão da CLI

O tempo limite padrão da sessão da CLI é de 30 minutos. O tempo limite é importante para evitar sessões obsoletas e piggybacking da sessão.

Use o `system timeout show` comando para exibir o tempo limite atual da sessão da CLI. Para definir o

valor de tempo limite, use o `system timeout modify -timeout <minutes>` comando.

Acesso à Web com o Gerenciador do sistema NetApp ONTAP

Se um administrador do ONTAP preferir usar uma interface gráfica em vez da CLI para acessar e gerenciar um cluster, use o Gerenciador do sistema do NetApp ONTAP. Ele é incluído com o ONTAP como um serviço da Web, habilitado por padrão e acessível usando um navegador. Aponte o navegador para o nome do host se estiver usando DNS ou o endereço IPv4 ou IPv6 através de `https://cluster-management-LIF` do .

Se o cluster usar um certificado digital autoassinado, o navegador pode exibir um aviso indicando que o certificado não é confiável. Você pode reconhecer o risco de continuar o acesso ou instalar um certificado digital assinado pela autoridade de certificação (CA) no cluster para autenticação do servidor.

A partir do ONTAP 9.3, a autenticação SAML (Security Assertion Markup Language) é uma opção para o Gerenciador de sistemas do ONTAP.

Autenticação SAML para o Gerenciador de sistemas do ONTAP

O SAML 2,0 é um padrão amplamente adotado do setor que permite que qualquer provedor de identidade (IDP) compatível com SAML de terceiros execute MFA usando mecanismos exclusivos para o IDP escolhido pela empresa e como fonte de logon único (SSO).

Há três funções definidas na especificação SAML: O principal, o IDP e o provedor de serviços. Na implementação do ONTAP, um dos principais é o administrador de cluster que obtém acesso ao ONTAP por meio do Gerenciador de sistemas do ONTAP ou do NetApp Active IQ Unified Manager. O IDP é um software IDP de terceiros. A partir do ONTAP 9.3, os Serviços Federados do Microsoft Active Directory (ADFS) e o IDP Shibboleth de código aberto são IDPs suportados. A partir do ONTAP 9.12,1, o Cisco DUO é um IDP suportado. O fornecedor de serviços é a funcionalidade SAML incorporada ao ONTAP usada pelo Gerenciador de sistemas do ONTAP ou pela aplicação Web do Active IQ Unified Manager.

Ao contrário do processo de configuração de dois fatores SSH, depois que a autenticação SAML é ativada, o ONTAP System Manager ou o ONTAP Service Processor Access requer que todos os administradores existentes se autenticuem através do IDP SAML. Não são necessárias alterações nas contas de utilizador do cluster. Quando a autenticação SAML está ativada, um novo método de autenticação de `saml` é adicionado aos usuários existentes com funções de administrador para `http` aplicativos e `ontapi` .

Depois que a autenticação SAML estiver ativada, novas contas adicionais que exigem acesso SAML IDP devem ser definidas no ONTAP com a função de administrador e o método de autenticação `saml` para `http` aplicativos e `ontapi`. Se a autenticação SAML estiver desativada em algum momento, essas novas contas exigirão que o `password` método de autenticação seja definido com a função de administrador `http` e `ontapi` os aplicativos e a adição `console` do aplicativo para autenticação ONTAP local ao Gerenciador do sistema do ONTAP.

Depois que o IDP SAML é ativado, o IDP executa a autenticação para o acesso do Gerenciador de sistema do ONTAP usando métodos disponíveis para o IDP, como LDAP (Lightweight Directory Access Protocol), AD (Active Directory), Kerberos, senha e assim por diante. Os métodos disponíveis são exclusivos do IDP. É importante que as contas configuradas no ONTAP tenham IDs de usuário mapeadas para os métodos de autenticação IDP.

Os IDPs que foram validados pelo NetApp são Microsoft ADFS, Cisco DUO e IDP de código aberto Shibboleth.

A partir do ONTAP 9.14,1, o Cisco DUO pode ser usado como um segundo fator de autenticação para SSH.

Para obter mais informações sobre o MFA para Gerenciador de sistemas ONTAP, Active IQ Unified Manager e SSH, "[TR-4647: Autenticação multifator no ONTAP 9](#)" consulte .

Insights do Gerenciador de sistemas da ONTAP

A partir do ONTAP 9.11.1, o Gerenciador de sistemas do ONTAP fornece insights para ajudar os administradores de cluster a otimizar suas tarefas diárias. Os insights de segurança são baseados nas recomendações deste relatório técnico.

Insight de segurança	Determinação
O Telnet está ativado	A NetApp recomenda o Shell seguro (SSH) para acesso remoto seguro.
O Remote Shell (RSH) está ativado	O NetApp recomenda SSH para acesso remoto seguro.
O AutoSupport está usando um protocolo inseguro	O AutoSupport não está configurado para ser enviado por xref:./ontap-security-hardening/HTTPS.
O banner de login não está configurado no cluster ao nível do cluster	Aviso se o banner de login não estiver configurado para o cluster.
O SSH está usando cifras inseguras	Aviso se o SSH usa cifras inseguras.
Poucos servidores NTP estão configurados	Aviso se o número de servidores NTP configurados for inferior a três.
Usuário de administrador padrão não bloqueado	Quando não estiver usando nenhuma conta administrativa padrão (admin ou diag) para fazer login no System Manager e essas contas não estiverem bloqueadas, a recomendação é bloqueá-las.
Defesa contra ransomware: Os volumes não têm políticas de Snapshot	Nenhuma política de snapshot adequada é anexada a um ou mais volumes.
Defesa de ransomware: Desative a exclusão automática do Snapshot	A eliminação automática de instantâneos está definida para um ou mais volumes.
Os volumes não estão sendo monitorados para ataques de ransomware	A proteção autônoma contra ransomware é compatível com vários volumes, mas ainda não está configurada.
Os SVMs não estão configurados para proteção autônoma contra ransomware	A proteção autônoma contra ransomware é compatível com vários SVMs, mas ainda não está configurada.
FPolicy nativo não está configurado	O FPolicy não está definido para SVMs nas.
Ative o modo ativo de proteção autônoma contra ransomware	Vários volumes concluíram o modo de aprendizagem e você pode ativar o modo ativo
A conformidade com o FIPS 140-2 global está desativada	A conformidade com o FIPS 140-2 global não está ativada.
O cluster não está configurado para notificações	E-mails, webhooks ou traposts SNMP não estão configurados para receber notificações.

Para obter mais informações sobre os insights do Gerenciador de sistemas do ONTAP, consulte "[Documentação do ONTAP System Manager Insights](#)".

Proteção autônoma contra ransomware da ONTAP

Para complementar a análise de comportamento do usuário para a segurança de workloads de workloads de storage, a proteção autônoma contra ransomware do ONTAP analisa workloads de volume e entropia para detectar ransomware e captura Snapshot e notifica o administrador quando houver suspeita de um ataque.

Além da detecção e prevenção de ransomware usando análise comportamental do usuário (UBA) do FPolicy externo com o NetApp Cloud Insights/Cloud Secure e o ecossistema de parceiros do NetApp FPolicy, o ONTAP 9.10,1 introduz proteção autônoma contra ransomware. A proteção autônoma contra ransomware da ONTAP usa uma funcionalidade de aprendizado de máquina (ML) incorporada on-box que analisa a atividade do workload de volume e entropia de dados para detectar automaticamente ransomware. Ele monitora a atividade que é diferente da UBA para que ele possa detectar ataques que a UBA não faz.

Para obter informações mais detalhadas sobre essa capacidade, "[Soluções da NetApp para ransomware](#)" consulte ou "[Documentação autônoma de proteção de ransomware da ONTAP](#)".

Auditoria de sistema administrativo de storage

Garanta a integridade da auditoria de eventos transferindo eventos do ONTAP para um servidor syslog remoto. Esse servidor pode ser um sistema de gerenciamento de eventos de informações de segurança, como Splunk.

Envie syslog

As informações de log e auditoria são inestimáveis para uma organização do ponto de vista de suporte e disponibilidade. Além disso, as informações e detalhes contidos em logs (syslog) e relatórios de auditoria e saídas são geralmente de natureza sensível. Para manter a postura e os controles de segurança, é imperativo que as organizações gerenciem dados de log e auditoria de maneira segura.

O descarregamento de informações do syslog é necessário para limitar o escopo ou a pegada de uma violação a um único sistema ou solução. Portanto, a NetApp recomenda descarregar com segurança as informações do syslog para um local seguro de armazenamento ou retenção.

Crie um destino de encaminhamento de registros

Use o `cluster log-forwarding create` comando para criar destinos de encaminhamento de log para o log remoto.

Parâmetros

Use os seguintes parâmetros para configurar o `cluster log-forwarding create` comando:

- *** Anfitrião de destino.*** Esse nome é o nome do host ou o endereço IPv4 ou IPv6 do servidor para o qual encaminhar os logs.

```
-destination <Remote InetAddress>
```

- **Porto de destino.** Esta é a porta na qual o servidor de destino escuta.

```
[-port <integer>]
```

- **Protocolo de encaminhamento de registos.** Este protocolo é utilizado para enviar mensagens para o destino.

```
[-protocol \{udp-unencrypted|tcp-unencrypted|tcp-encrypted} ]
```

O protocolo de encaminhamento de registos pode utilizar um dos seguintes valores:

- `udp-unencrypted`. User Datagram Protocol sem segurança.
 - `tcp-unencrypted`. TCP sem segurança.
 - `tcp-encrypted`. TCP com Transport Layer Security (TLS).
- **Verifique a identidade do servidor de destino.** Quando esse parâmetro é definido como verdadeiro, a identidade do destino de encaminhamento de log é verificada validando seu certificado. O valor só pode ser definido como verdadeiro quando o `tcpencrypted` valor é selecionado no campo protocolo.

```
[-verify-server \{true|false} ]
```

- *** Syslog facilidade.*** Esse valor é o recurso syslog a ser usado para os logs encaminhados.

```
[-facility <Syslog Facility>]
```

- **Ignorar o teste de conectividade.** Normalmente, o `cluster log-forwarding create` comando verifica se o destino está acessível enviando um ping ICMP (Internet Control Message Protocol) e falha se não estiver acessível. Definir este valor para `true` ignorar a verificação de ping para que você possa configurar o destino quando ele não estiver acessível.

```
[-force [true]]
```



O NetApp recomenda usar o `cluster log-forwarding` comando para forçar a conexão a um `-tcp-encrypted` tipo.

Notificação de evento

Proteger as informações e os dados que saem de um sistema é vital para manter e gerenciar a postura de segurança do sistema. Os eventos gerados pela solução ONTAP fornecem uma riqueza de informações sobre o que a solução está encontrando, as informações processadas e muito mais. A vitalidade desses dados destaca a necessidade de gerenciá-los e migrá-los de forma segura.

O `event notification create` comando envia uma nova notificação de um conjunto de eventos definido por um filtro de eventos para um ou mais destinos de notificação. Os exemplos a seguir descrevem a configuração de notificação de eventos e o `event notification show` comando, que exibe os filtros e

destinos de notificação de eventos configurados.

```
cluster1::> event notification create -filter-name filter1 -destinations
email_dest,syslog_dest,snmp-traphost

cluster1::> event notification show
ID      Filter Name      Destinations
-----  -
1 filter1 email_dest, syslog_dest, snmp-traphost
```

Criptografia de storage

Para proteger dados confidenciais em caso de um disco que seja roubado, devolvido ou reutilizado, use a criptografia de storage NetApp baseada em hardware ou a criptografia de volume NetApp/NetApp agregada baseada em software. Ambos os mecanismos são validados pelo FIPS-140-2 e, ao usar mecanismos baseados em hardware com mecanismos baseados em software, a solução se qualifica para o Programa soluções comerciais para classificados (CSfC). Ele permite maior proteção de segurança para dados secretos e secretos em repouso nas camadas de hardware e software.

A criptografia de dados em repouso é importante para proteger dados confidenciais em caso de um disco que seja roubado, retornado ou reutilizado.

A ONTAP 9 tem três soluções de criptografia de dados em repouso compatíveis com FIPS (Federal Information Processing Standard) 140-2:

- O NetApp Storage Encryption (NSE) é uma solução de hardware que usa unidades com autocriptografia.
- O NetApp volume Encryption (NVE) é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele esteja habilitado com uma chave exclusiva para cada volume.
- O NetApp Aggregate Encryption (NAE) é uma solução de software que permite a criptografia de qualquer volume de dados em qualquer tipo de unidade onde ele é habilitado com chaves exclusivas para cada agregado.

O NSE, NVE e NAE podem usar o gerenciamento de chaves externas ou o OKM (Onboard Key Manager). O uso de NSE, NVE e NAE não afeta os recursos de eficiência de storage da ONTAP. No entanto, os volumes NVE são excluídos da deduplicação agregada. Os volumes NAE participam e se beneficiam da deduplicação agregada.

O OKM fornece uma solução de criptografia autônoma para dados em repouso com NSE, NVE ou NAE.

NVE, NAE e OKM usam o ONTAP CryptoMod. O CryptoMod está listado na lista de módulos validados do CMVP FIPS 140-2. ["FIPS 140-2 Cert no. 4144"](#)Consulte .

Para iniciar a configuração OKM, use o `security key-manager onboard enable` comando. Para configurar gerenciadores de chaves KMIP (Key Management Interoperability Protocol) externos, use o `security key-manager external enable` comando. A partir do ONTAP 9.6, a alocação a vários clientes é suportada para gerentes de chaves externos. Use o `-vserver <vserver name>` parâmetro para habilitar o gerenciamento de chaves externas para uma SVM específica. Antes de 9,6, o `security key-`

`manager setup` comando foi usado para configurar os gerenciadores OKM e de chaves externas. Para o gerenciamento de chaves integradas, essa configuração orienta o operador ou o administrador pela configuração da senha e parâmetros adicionais para configurar o OKM.

Uma parte da configuração é fornecida no exemplo a seguir:

```
cluster1::> security key-manager setup
Welcome to the key manager setup wizard, which will lead you through
the steps to add boot information.

Enter the following commands at any time
"help" or "?" if you want to have a question clarified,
"back" if you want to change your answers to previous questions, and
"exit" if you want to quit the key manager setup wizard. Any changes
you made before typing "exit" will be applied.

Restart the key manager setup wizard with "security key-manager setup". To
accept a default
or omit a question, do not enter a value.

Would you like to configure onboard key management? {yes, no} [yes]:
Enter the cluster-wide passphrase for onboard key management. To continue
the configuration, enter the passphrase, otherwise
type "exit":
Re-enter the cluster-wide passphrase:
After configuring onboard key management, save the encrypted configuration
data
in a safe location so that you can use it if you need to perform a manual
recovery
operation. To view the data, use the "security key-manager backup show"
command.
```

A partir do ONTAP 9.4, você pode usar a `-enable-cc-mode` opção `True` com `security key-manager setup` para exigir que os usuários inseram a senha após uma reinicialização. Para o ONTAP 9.6 e posterior, a sintaxe de comando é `security key-manager onboard enable -cc-mode-enabled yes`.

A partir do ONTAP 9.4, você pode usar o `secure-purge` recurso com privilégios avançados para "esfregar" dados em volumes habilitados para NVE sem interrupções. A análise de dados em um volume criptografado garante que ele não possa ser recuperado da Mídia física. O seguinte comando limpa com segurança os arquivos excluídos no vol1 no SVM VS1:

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume vol1
```

A partir do ONTAP 9.7, NAE e NVE são ativados por padrão se a licença VE estiver em vigor, os gerenciadores de chaves externos ou OKM são configurados e NSE não é usado. Os volumes NAE são criados por padrão em agregados NAE e os volumes NVE são criados por padrão em agregados não-naE. Você pode substituir isso digitando o seguinte comando:

```
cluster1::*> options -option-name
encryption.data_at_rest_encryption.disable_by_default true
```

A partir do ONTAP 9.6, você pode usar um escopo SVM para configurar o gerenciamento de chaves externas para um SVM de dados no cluster. Isso é melhor para ambientes com alocação a vários clientes nos quais cada locatário usa um SVM diferente (ou conjunto de SVMs) para servir dados. Somente o administrador do SVM de um determinado locatário tem acesso às chaves desse locatário. Para obter mais informações, consulte ["Habilite o gerenciamento de chaves externas no ONTAP 9.6 e posterior"](#) a documentação do ONTAP.

A partir do ONTAP 9.11,1, é possível configurar a conectividade com servidores de gerenciamento de chaves externas em cluster, designando servidores de chaves primárias e secundárias em um SVM. Para obter mais informações, consulte ["configurar servidores de chaves externas em cluster"](#) a documentação do ONTAP.

A partir do ONTAP 9.13,1, você pode configurar servidores de gerenciador de chaves externos no gerenciador de sistema. Para obter mais informações, consulte ["Gerenciar gerenciadores de chaves externos"](#) a documentação do ONTAP.

Criptografia de replicação de dados

Para complementar os dados em repouso, é possível criptografar o tráfego de replicação de dados do ONTAP entre clusters usando o TLS 1,2 com uma chave pré-compartilhada para SnapMirror, SnapVault ou FlexCache.

Ao replicar dados para recuperação de desastre, armazenamento em cache ou backup, você precisa proteger esses dados durante o transporte por cabo de um cluster ONTAP para outro. Isso evita ataques intermediários maliciosos contra dados confidenciais quando eles estão em trânsito.

A partir do ONTAP 9.6, a criptografia de peering de cluster fornece suporte de criptografia TLS 1,2 AES-256 GCM para recursos de replicação de dados do ONTAP, como SnapMirror, SnapVault e FlexCache. A criptografia é configurada por meio de uma chave pré-compartilhada (PSK) entre dois pares de cluster.

Clientes que usam tecnologias como NSE, NVE e NAE para proteger dados em repouso também podem usar criptografia de dados completa atualizando para o ONTAP 9.6 ou posterior para usar a criptografia de peering de cluster.

O peering de cluster criptografa todos os dados entre os pares do cluster. Por exemplo, ao usar o SnapMirror, todas as informações de peering, bem como todas as relações SnapMirror entre o peer de cluster de origem e destino são criptografadas. Não é possível enviar dados de texto não criptografado entre pares de cluster com criptografia de peering de cluster ativada.

A partir do ONTAP 9.6, as novas relações de cluster-peer têm a encriptação ativada por predefinição. Para habilitar a criptografia em relacionamentos de pares de cluster que foram criados antes do ONTAP 9.6, você deve atualizar o cluster de origem e destino para 9,6. Além disso, você deve usar o `cluster peer modify` comando para alterar os pares de cluster de origem e destino para usar a criptografia de peering de cluster.

Você pode converter um relacionamento de pares existente para usar a criptografia de peering de cluster no ONTAP 9.6, conforme mostrado no exemplo a seguir:

On the Destination Cluster Peer

```
cluster2::> cluster peer modify cluster1 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter a passphrase.

On the Source Cluster Peer

```
cluster1::> cluster peer modify cluster2 -auth-status-admin use-  
authentication -encryption-protocol-proposed tls-psk
```

When prompted enter the same passphrase you created in the previous step.

Criptografia de dados em trânsito IPsec

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec. O IPsec fornece uma alternativa à criptografia NFS ou SMB/CIFS e é a única opção de criptografia em voo para tráfego iSCSI.

Em algumas situações, pode haver um requisito para proteger todos os dados do cliente transportados por cabo (ou em trânsito) para o SVM do ONTAP. Isso impede a repetição e ataques maliciosos contra dados confidenciais em trânsito.

A partir do ONTAP 9.8, a Segurança de Protocolo de Internet (IPsec) oferece suporte de criptografia de ponta a ponta para todo o tráfego IP entre um cliente e um SVM do ONTAP. A criptografia de dados IPsec para todo o tráfego IP inclui protocolos NFS, iSCSI e SMB/CIFS. O IPsec fornece a única opção de criptografia em voo para tráfego iSCSI.

Fornecer criptografia NFS por cabo é um dos principais casos de uso do IPsec. Antes do ONTAP 9.8, a criptografia por cabo NFS exigiu a configuração e configuração do Kerberos para utilizar o krb5p para criptografar dados NFS em trânsito. Isso nem sempre é simples ou fácil de realizar em todos os ambientes do cliente.

Os clientes que usam tecnologias de criptografia de dados em repouso, como criptografia de storage NetApp (NSE) ou criptografia de volume NetApp (NVE) e criptografia de peering de cluster (CPE) para tráfego de replicação de dados, agora podem usar criptografia de ponta a ponta entre o cliente e o storage em seu data fabric de multicloud híbrida, atualizando para o ONTAP 9 ou posterior e usando IPsec.

IPsec é um padrão IETF. O ONTAP usa IPsec no modo de transporte. Ele também aproveita o protocolo IKE (Internet Key Exchange) versão 2, que usa uma chave pré-compartilhada (PSK) para negociar material chave entre o cliente e o ONTAP com IPv4 ou IPv6. Por padrão, o IPsec usa criptografia de 256 bits AES-GCM do Suite-B. Suite-B AES-GMAC256 e AES-CBC256 com encriptação de 256 bits também são suportados.

Embora o recurso IPsec deva estar habilitado no cluster, ele se aplica a endereços IP SVM individuais por

meio do uso de uma entrada SPD (Security Policy Database). A entrada SPD (diretiva) contém o endereço IP do cliente (sub-rede IP remota), o endereço IP SVM (sub-rede IP local), o conjunto de codificação de criptografia a ser usado e o segredo pré-compartilhado (PSK) necessário para autenticar via IKEv2 e estabelecer a conexão IPsec. Além da entrada de diretiva IPsec, o cliente deve ser configurado com as mesmas informações (IP local e remoto, PSK e conjunto de codificação) antes que o tráfego possa fluir pela conexão IPsec. A partir do ONTAP 9.10,1, o suporte à autenticação de certificado IPsec é adicionado. Isso remove os limites de diretiva IPsec e habilita o suporte do sistema operacional Windows para IPsec.

Se houver um firewall entre o cliente e o endereço IP SVM, ele deverá permitir que os protocolos ESP e UDP (portas 500 e 4500), tanto de entrada (entrada) quanto de saída (saída), para que a negociação IKEv2 seja bem-sucedida e, assim, permita o tráfego IPsec.

Para criptografia de tráfego de peering de cluster e NetApp SnapMirror, a criptografia de peering de cluster (CPE) ainda é recomendada por IPsec para garantir o trânsito seguro por cabo. O CPE tem melhor desempenho para essas cargas de trabalho do que o IPsec. Você não precisa de uma licença para IPsec e não há restrições de importação ou exportação.

Você pode ativar o IPsec no cluster e criar uma entrada SPD para um único cliente e um único endereço IP SVM, conforme mostrado no exemplo a seguir:

```
On the Destination Cluster Peer
```

```
cluster1::> security ipsec config modify -is-enabled true
```

```
cluster1::> security ipsec policy create -vserver vs1 -name test34 -local  
-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
```

```
When prompted enter and confirm the pre shared secret (PSK).
```

Modo FIPS e gerenciamento TLS e SSL

O padrão FIPS 140-2 especifica requisitos de segurança para módulos criptográficos dentro de sistemas de segurança que protegem informações confidenciais em sistemas de computador e telecomunicações. O padrão FIPS 140-2 aplica-se *especificamente* ao módulo criptográfico, em vez do produto, arquitetura, dados ou ecossistema. O módulo criptográfico é o componente específico (hardware, software, firmware ou uma combinação dos três) que implementa funções de segurança aprovadas pelo NIST.

A ativação da conformidade com o FIPS 140-2 tem efeitos em outros sistemas e comunicações internas e externas ao ONTAP 9. A NetApp recomenda fortemente testar essas configurações em um sistema que não seja de produção com acesso ao console.

A partir do suporte a ONTAP 9.11,1 e TLS 1,3, é possível validar o FIPS 140-3.



A configuração FIPS se aplica ao ONTAP e ao Platform BMC.

Configuração do modo FIPS do NetApp ONTAP

O NetApp ONTAP tem uma configuração do modo FIPS que instancia um nível adicional de segurança ao

plano de controle:

- A partir do ONTAP 9.11.1, quando o modo de conformidade com o FIPS 140-2 estiver ativado, TLSv1, TLSv1,1 e SSLv3 serão desativados e apenas TLSv1,2 e TLSv1,3 permanecerão ativados. Afeta outros sistemas e comunicações que são internos e externos ao ONTAP 9. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativar, TLSv1, TLSv1,1 e SSLv3 permanecerão desativados. O TLSv1,2 ou o TLSv1,3 permanecerão ativados dependendo da configuração anterior.
- Para versões do ONTAP anteriores a 9.11.1, quando o modo de conformidade com FIPS 140-2 estiver ativado, tanto o TLSv1 quanto o SSLv3 são desativados e apenas o TLSv1,1 e o TLSv1,2 permanecem ativados. O ONTAP impede que você ative o TLSv1 e o SSLv3 quando o modo de conformidade FIPS 140-2 estiver ativado. Se você ativar o modo de conformidade FIPS 140-2 e, em seguida, desativá-lo, o TLSv1 e o SSLv3 permanecerão desativados, mas o TLSv1,2 ou o TLSv1,1 e o TLSv1,2 serão ativados dependendo da configuração anterior.
- "[Módulo de segurança criptográfica NetApp \(NCSM\)](#)", Validado pelo FIPS 140-2 nível 1, fornece conformidade com software.



O NIST enviou um padrão FIPS-140-3 e o NCSM terá validações FIPS-140-2 e FIPS-140-3. Todas as validações do FIPS 140-2 serão transferidas para o status histórico em 21 de setembro de 2026, ou seja, cinco anos após o último dia para novos envios de certificados.

Ative o modo de conformidade FIPS-140-2 e FIPS-140-3

A partir do ONTAP 9, é possível habilitar o modo de conformidade FIPS-140-2 e FIPS-140-3 para interfaces do plano de controle em todo o cluster.

- "[Ativar FIPS](#)"
- "[Exibir status FIPS](#)"

Protocolos e capacitação FIPS

O `security config modify` comando permite modificar a configuração de segurança existente em todo o cluster. Se ativar o modo compatível com FIPS, o cluster selecionará automaticamente apenas protocolos TLS.

- Use o `-supported-protocols` parâmetro para incluir ou excluir protocolos TLS independentemente do modo FIPS. Por padrão, o modo FIPS é desativado e o ONTAP oferece suporte aos protocolos TLSv1,2, TLSv1,1 e TLSv1.
- Para compatibilidade com versões anteriores, o ONTAP suporta a adição de SSLv3 à lista de protocolos compatíveis quando o modo FIPS está desativado.

Capacitação FIPS e cifras

- Utilize o `-supported-cipher-suites` parâmetro para configurar apenas o AES (Advanced Encryption Standard) ou AES e 3DES.
- Você pode desativar cifras fracas, como RC4, especificando `!RC4`. Por padrão, a configuração de codificação suportada é `ALL:!LOW:!aNULL:!EXP:!eNULL`. Essa configuração significa que todos os conjuntos de criptografia suportados para os protocolos estão ativados, exceto aqueles que usam algoritmos de criptografia de 64 bits ou 56 bits sem autenticação, criptografia, sem exportação e pacotes de criptografia de baixa criptografia.
- Selecione um conjunto de codificações que esteja disponível com o protocolo selecionado

correspondente. Uma configuração inválida pode fazer com que algumas funcionalidades não funcionem corretamente.

- Para obter a sintaxe correta da cadeia de caracteres de cifra, consulte "[página de cifras](#)" On OpenSSL (publicado pela fundação do software OpenSSL). A partir do ONTAP 9.9,1 e versões posteriores, não é mais necessário reiniciar todos os nós manualmente depois de modificar a configuração de segurança.

Proteção de segurança SSH e TLS

A administração SSH do ONTAP 9 requer um cliente OpenSSH 5,7 ou posterior. Os clientes SSH devem negociar com o algoritmo de chave pública ECDSA (Elliptic Curve Digital Signature Algorithm) para que a conexão seja bem-sucedida.

Para proteger a segurança TLS, ative apenas o TLS 1,2 e use conjuntos de codificação capazes de Perfect Forward Secrecy (PFS). O PFS é um método de troca de chaves que, quando usado em combinação com protocolos de criptografia como o TLS 1,2, ajuda a impedir que um invasor descriptografe todas as sessões de rede entre um cliente e um servidor.

Ative os conjuntos de codificação compatíveis com TLSv1,2 e PFS

Para ativar apenas conjuntos de encriptação compatíveis com TLS 1,2 e PFS, utilize o `security config modify` comando a partir do nível de privilégio avançado.



Antes de alterar a configuração da interface SSL, certifique-se de que o cliente suporta as cifras DHE e ECDHE ao se conectar ao ONTAP para manter a conectividade com o ONTAP.

Exemplo

```
cluster1::*> security config modify -interface SSL -supported-protocols
TLSv1.2 -supported-cipher-suites
PSK:DHE:ECDHE:!LOW:!aNULL:!EXP:!eNULL:!3DES:!kDH:!kECDH
```

Confirme `y` para cada prompt. Para obter mais informações sobre PFS, consulte este "[NetApp blog](#)".

Informações relacionadas

["Publicação Federal Information Processing Standard \(FIPS\) 140"](#)

Crie um certificado digital assinado pela CA

Para muitas organizações, o certificado digital auto-assinado para o acesso à Web ONTAP não é compatível com suas políticas INFOSEC. Em sistemas de produção, é uma prática recomendada do NetApp instalar um certificado digital assinado pela CA para uso na autenticação do cluster ou SVM como um servidor SSL.

Você pode usar o `security certificate generate-csr` comando para gerar uma solicitação de assinatura de certificado (CSR) e o `security certificate install` comando para instalar o certificado recebido de volta da CA.

Passos

1. Para criar um certificado digital assinado pela CA da organização, faça o seguinte:

- a. Gerar um CSR.
- b. Siga o procedimento da sua organização para solicitar um certificado digital usando a CSR da CA da sua organização. Por exemplo, usando a interface da Web do Microsoft Active Directory Certificate Services, vá para <CA_server_name>/certsrv e solicite um certificado.
- c. Instale o certificado digital no ONTAP.

Protocolo de estado do certificado online

O OCSP (Online Certificate Status Protocol) permite que aplicativos ONTAP que usam comunicações TLS, como LDAP ou TLS, recebam status de certificado digital quando o OCSP está ativado. O aplicativo recebe uma resposta assinada significando que o certificado solicitado é bom, revogado ou desconhecido.

O OCSP permite determinar o status atual de um certificado digital sem exigir listas de revogação de certificados (CRLs).

Por padrão, a verificação do status do certificado OCSP está desativada. Ele pode ser ativado com o comando `security config ocsf enable -app name`, onde o nome do aplicativo pode ser `autosupport`, `audit_log`, `fabricpool ems`, `knip`, `ldap_ad`, `ldap_nis_namemap`, `all` ou `.` O comando requer nível de privilégio avançado.

Gerenciamento do SSHv2

O `security ssh modify` comando substitui as configurações existentes dos algoritmos de troca de chaves SSH, cifras ou algoritmos MAC para o cluster ou um SVM com as configurações especificadas.

A NetApp recomenda o seguinte:



- Use senhas para sessões de usuário.
- Use uma chave pública para acesso à máquina.

Cifras suportadas e trocas de chaves

Cifras	Troca de chaves
aes256-ctr	diffie-hellman-group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-group-Exchange-SHA1 (SHA-1)
aes128-ctr	diffie-hellman-group14-SHA1 (SHA-1)
aes256-cbc	diffie-hellman-group1-SHA1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-gcm	-
aes256-gcm	-

Cifras	Troca de chaves
3des-cbc	-

Criptografia simétrica AES e 3DES suportada

O ONTAP também suporta os seguintes tipos de criptografia simétrica AES e 3DES (também conhecidos como cifras):

- hmac-sha1
- hmac-sha1-96
- hmac-md5
- hmac-md5-96
- hmac-ripemd160
- umac-64
- umac-64
- umac-128
- hmac-sha2-256
- hmac-sha2-512
- hmac-sha1-etm
- hmac-sha1-96-etm
- hmac-sha2-256-etm
- hmac-sha2-512-etm
- hmac-md5-etm
- hmac-md5-96-etm
- hmac-ripemd160-etm
- umac-64-etm
- umac-128-etm



A configuração de gerenciamento SSH se aplica ao ONTAP e à plataforma BMC.

NetApp AutoSupport

O recurso AutoSupport do ONTAP permite que você monitore proativamente a integridade do sistema e envie mensagens e detalhes automaticamente para o suporte técnico da NetApp, para a equipe de suporte interna da organização ou para um parceiro de suporte. Por padrão, as mensagens AutoSupport para o suporte técnico do NetApp são ativadas quando o sistema de armazenamento é configurado pela primeira vez. Além disso, o AutoSupport começa a enviar mensagens para o suporte técnico da NetApp 24 horas depois de ativado. Este período de 24 horas é configurável. Para aproveitar a comunicação com a equipe de suporte interno de uma organização, a configuração do host de e-mail deve ser concluída.

Somente o administrador do cluster pode executar o gerenciamento de AutoSupport (configuração). O administrador do SVM não tem acesso ao AutoSupport. O recurso AutoSupport pode ser desativado. No entanto, a NetApp recomenda habilitá-la porque o AutoSupport ajuda a acelerar a identificação e a resolução de problemas caso ocorra algum problema no sistema de storage. Por padrão, o sistema coleta informações do AutoSupport e as armazena localmente, mesmo que você desative o AutoSupport.

Para obter mais detalhes sobre mensagens AutoSupport, incluindo o que está contido nas várias mensagens e onde diferentes tipos de mensagens são enviadas, consulte "[Consultor digital da NetApp](#)"a documentação.

As mensagens do AutoSupport contêm dados confidenciais, incluindo, entre outros, os seguintes itens:

- Ficheiros de registo
- Dados sensíveis ao contexto relativos a subsistemas específicos
- Dados de configuração e status
- Dados de performance

O AutoSupport suporta HTTPS, HTTP e SMTP para protocolos de transporte. Devido à natureza sensível das mensagens AutoSupport, a NetApp recomenda fortemente o uso de HTTPS como o protocolo de transporte padrão para enviar mensagens AutoSupport para o suporte ao NetApp.

Além disso, você deve utilizar o `system node autosupport modify` comando para especificar os destinos dos dados do AutoSupport (por exemplo, suporte técnico da NetApp, operações internas de uma organização ou parceiros). Esse comando também permite especificar quais detalhes específicos do AutoSupport enviar (por exemplo, dados de desempenho, arquivos de log, etc.).

Para desativar completamente o AutoSupport, use o `system node autosupport modify -state disable` comando.

Protocolo de hora de rede

Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com pelo menos três servidores NTP externos.

Podem ocorrer problemas quando o tempo do cluster é impreciso. Embora o ONTAP permita que você defina manualmente o fuso horário, a data e a hora no cluster, você deve configurar os servidores NTP (Network Time Protocol) para sincronizar a hora do cluster com servidores NTP externos.

A partir do ONTAP 9.5, você pode configurar seu servidor NTP com autenticação simétrica.

Você pode associar um máximo de 10 servidores NTP externos usando o `cluster time-service ntp server create` comando. Para redundância e qualidade do serviço de tempo, você deve associar pelo menos três servidores NTP externos ao cluster.

Para obter detalhes sobre a configuração do NTP no ONTAP, "[Gerenciamento do tempo do cluster \(somente administradores de cluster\)](#)" consulte .

Contas locais do sistema de arquivos nas (grupo de trabalho CIFS)

A autenticação de cliente de grupo de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Use o `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

A partir do ONTAP 9, você pode configurar um servidor CIFS em um grupo de trabalho com clientes CIFS que se autenticam no servidor usando usuários e grupos definidos localmente. A autenticação de cliente de grupo de trabalho fornece uma camada extra de segurança para a solução ONTAP que é consistente com uma postura tradicional de autenticação de domínio. Para configurar o servidor CIFS, use o `vserver cifs create` comando. Depois que o servidor CIFS é criado, você pode associá-lo a um domínio CIFS ou associá-lo a um grupo de trabalho. Para ingressar em um grupo de trabalho, use o `-workgroup` parâmetro. Aqui está um exemplo de configuração:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSEVER1  
-workgroup Sales
```



Um servidor CIFS no modo de grupo de trabalho suporta apenas a autenticação do Windows NT LAN Manager (NTLM) e não suporta autenticação Kerberos.

A NetApp recomenda a utilização da função de autenticação NTLM com grupos de trabalho CIFS para manter a postura de segurança da sua organização. Para validar a postura de segurança do CIFS, o NetApp recomenda o uso do `vserver cifs session show` comando para exibir vários detalhes relacionados à postura, incluindo informações de IP, mecanismo de autenticação, versão do protocolo e tipo de autenticação.

Auditoria do sistema de arquivos nas

Os sistemas de arquivos nas ocupam um espaço maior no cenário de ameaças atuais. As funções de auditoria são essenciais para oferecer suporte à visibilidade.

A segurança requer validação. O ONTAP 9 fornece maiores eventos de auditoria e detalhes em toda a solução. Como os sistemas de arquivos nas ocupam um espaço físico maior no cenário de ameaças atuais, as funções de auditoria são essenciais para oferecer suporte à visibilidade. Devido à capacidade de auditoria aprimorada no ONTAP 9, os detalhes de auditoria do CIFS são mais abundantes do que nunca. Os principais detalhes, incluindo os seguintes, são registrados com eventos criados:

- Acesso a arquivos, pastas e compartilhamentos
- Arquivos criados, modificados ou excluídos
- Acesso de leitura de ficheiros bem-sucedido
- Tentativas falhadas de ler ou gravar ficheiros
- Alterações de permissão de pasta

Crie uma configuração de auditoria

É necessário habilitar a auditoria CIFS para gerar eventos de auditoria. Use o `vserver audit create` comando para criar uma configuração de auditoria. Por padrão, o log de auditoria usa um método de rotação baseado no tamanho. Você pode usar uma opção de rotação baseada no tempo, se especificado no campo `Rotation Parameters` (parâmetros de rotação). Os detalhes adicionais da configuração de rotação de auditoria de log incluem o cronograma de rotação, os limites de rotação, os dias de rotação da semana e o tamanho da rotação. O texto a seguir fornece um exemplo de configuração que descreve uma configuração de auditoria usando uma rotação mensal baseada em tempo agendada para todos os dias da semana às 12:30.

```
cluster1:~> vserver audit create -vserver vs1 -destination /audit_log
-rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule
-hour 12 -rotate-schedule-minute 30
```

Eventos de auditoria CIFS

Os eventos de auditoria CIFS são os seguintes:

- **Compartilhamento de arquivos:** Gera um evento de auditoria quando um compartilhamento de rede CIFS é adicionado, modificado ou excluído usando os comandos relacionados `vserver cifs share`.
- **Alteração da política de auditoria:** Gera um evento de auditoria quando a política de auditoria é desativada, ativada ou modificada usando os comandos relacionados `vserver audit`.
- **Conta de usuário:** Gera um evento de auditoria quando um usuário local CIFS ou UNIX é criado ou excluído; uma conta de usuário local é ativada, desativada ou modificada; ou uma senha é redefinida ou alterada. Este evento usa o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-user`.
- **Security group:** Gera um evento de auditoria quando um grupo de segurança local CIFS ou UNIX é criado ou excluído usando o `vserver cifs users-and-groups local-group` comando ou o comando relacionado `vserver services name-service unix-group`.
- **Alteração da política de autorização:** Gera um evento de auditoria quando os direitos são concedidos ou revogados para um usuário CIFS ou um grupo CIFS usando o `vserver cifs users-and-groups privilege` comando.



Esta funcionalidade é baseada na função de auditoria do sistema, que permite que um administrador analise o que o sistema está permitindo e executando a partir da perspectiva de um usuário de dados.

Efeito de APIS REST na auditoria nas

O ONTAP inclui a capacidade de contas de administrador acessarem e manipularem arquivos SMB/CIFS ou NFS usando APIs REST. Embora as APIs REST só possam ser executadas por administradores do ONTAP, os comandos da API REST ignoram o log de auditoria nas do sistema. Além disso, as permissões de arquivo também podem ser ignoradas pelos administradores do ONTAP ao usar APIs REST. No entanto, as ações do administrador com APIs REST em arquivos são capturadas no log do histórico de comandos do sistema.

Criar função de API REST sem acesso

É possível impedir que os administradores do ONTAP usem APIs REST para acesso a arquivos ao criar uma função de API REST que não tenha acesso a volumes do ONTAP por meio DE REST. Para provisionar essa

função, execute as etapas a seguir.

Passos

1. Crie uma nova função REST que não tenha acesso a volumes de storage, além de ter todos os outros acessos à API REST.

```
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api/storage/volumes" -access none
cluster1::> security login rest-role create nofiles -vserver cluster1
"/api" -access all
```

2. Atribua a conta de administrador à nova função API REST que você criou na etapa anterior.

```
cluster1::> security login modify -user-or-group-name user1 -application
http -authentication-method password -vserver cluster1 -role nofile
```



Se você quiser impedir que a conta de administrador de cluster do ONTAP integrada use APIs REST para acesso a arquivos, primeiro será necessário ["crie uma nova conta de administrador e desative ou exclua a conta interna"](#).

Configure e ative a assinatura e a vedação CIFS SMB

Você pode configurar e ativar a assinatura SMB que protege a segurança do Data Fabric. Isso garante que o tráfego entre sistemas de storage e clientes não seja comprometido com replay ou ataques man-in-the-middle. A assinatura SMB protege verificando se as mensagens SMB têm assinaturas válidas.

Sobre esta tarefa

Um vetor de ameaça comum para sistemas de arquivos e arquiteturas está no protocolo SMB. Para lidar com esse vetor, a solução ONTAP 9 usa assinatura e vedação padrão do setor SMB. A assinatura de SMB protege a segurança do Data Fabric ao garantir que o tráfego entre sistemas de storage e clientes não seja comprometido com replays ou ataques diretos. Ele faz isso verificando se as mensagens SMB têm assinaturas válidas.

Embora a assinatura SMB esteja desativada por padrão no interesse do desempenho, a NetApp recomenda fortemente que você a ative. Além disso, a solução ONTAP oferece suporte à criptografia SMB, que também é conhecida como vedação. Esta abordagem permite o transporte seguro de dados numa base de partilha por partilha. Por predefinição, a encriptação SMB está desativada. No entanto, a NetApp recomenda que você ative a criptografia SMB.

Agora, a assinatura e a vedação LDAP são suportadas no SMB 2,0 e posterior. A assinatura (proteção contra adulteração) e a vedação (criptografia) permitem a comunicação segura entre SVMs e servidores do ativo Directory. A criptografia AES acelerada (Intel AES NI) agora é suportada no SMB 3,0 e posterior. O Intel AES NI melhora o algoritmo AES e acelera a criptografia de dados com famílias de processadores suportadas.

Passos

1. Para configurar e ativar a assinatura SMB, use o `vserver cifs security modify` comando e

verifique se o `-is-signing-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock
-skew 3 -kerberos-ticket-age 8 -is-signing-required true
```

2. Para configurar e ativar a selagem e a criptografia SMB, use o `vserver cifs security modify` comando e verifique se o `-is-smb-encryption-required` parâmetro está definido como `true`. Veja o seguinte exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-----  -----
vs1      true
```

Proteção do NFS

As regras de exportação são os elementos funcionais de uma política de exportação. As regras de exportação correspondem às solicitações de acesso do cliente para um volume em relação aos parâmetros específicos que você configura para determinar como lidar com as solicitações de acesso do cliente. Uma política de exportação deve conter pelo menos uma regra de exportação para permitir o acesso aos clientes. Se uma política de exportação contiver mais de uma regra, as regras serão processadas na ordem em que aparecem na política de exportação.

O controle de acesso é fundamental para manter uma postura segura. Portanto, o ONTAP usa o recurso de política de exportação para limitar o acesso de volume NFS a clientes que correspondem a parâmetros específicos. As políticas de exportação contêm uma ou mais regras de exportação que processam cada solicitação de acesso de cliente. Uma política de exportação está associada a cada volume para configurar o acesso do cliente ao volume. O resultado deste processo determina se o cliente é concedido ou negado (com uma mensagem de permissão negada) o acesso ao volume. Este processo também determina que nível de acesso é fornecido ao volume.



Uma política de exportação com regras de exportação deve existir em um SVM para que os clientes acessem os dados. Um SVM pode conter várias políticas de exportação.

A ordem da regra é ditada pelo número do índice da regra. Se uma regra corresponder a um cliente, as permissões dessa regra serão usadas e nenhuma outra regra será processada. Se nenhuma regra corresponder, o cliente é negado o acesso.

As regras de exportação determinam as permissões de acesso do cliente aplicando os seguintes critérios:

- O protocolo de acesso ao arquivo usado pelo cliente que envia a solicitação (por exemplo, NFSv4 ou SMB)
- Um identificador de cliente (por exemplo, nome de host ou endereço IP)
- O tipo de segurança usado pelo cliente para autenticar (por exemplo, Kerberos v5, NTLM ou AUTH_SYS)

Se uma regra especificar vários critérios e o cliente não corresponder a um ou mais deles, a regra não se aplica.

Um exemplo de política de exportação contém uma regra de exportação com os seguintes parâmetros:

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

O tipo de segurança determina o nível de acesso que um cliente recebe. Os três níveis de acesso são somente leitura, leitura-gravação e superusuário (para clientes com ID de usuário 0). Como o nível de acesso determinado pelo tipo de segurança é avaliado nesta ordem, você deve observar as regras listadas:

Regras para parâmetros de nível de acesso em regras de exportação

Para que um cliente obtenha os seguintes níveis de acesso	Esses parâmetros de acesso devem corresponder ao tipo de segurança do cliente
Apenas de leitura normal do utilizador	Somente leitura (<code>-rorule</code>)
Leitura-escrita normal do utilizador	Somente leitura (<code>-rorule</code>) e leitura-gravação (<code>-rwrule</code>)
Somente leitura do superusuário	Apenas leitura (<code>-rorule</code>) e <code>-superuser</code>
Leitura-gravação do superusuário	Somente leitura (<code>-rorule</code>) e leitura-gravação (<code>-rwrule</code>) e <code>-superuser</code>


Os seguintes são tipos de segurança válidos para cada um destes três parâmetros de acesso:

- Qualquer
- Nenhum
- Nunca

Esses tipos de segurança não são válidos para uso com o `-superuser` parâmetro:

- `krb5`
- `ntlm`
- `sistema`

Regras para resultados de parâmetros de acesso

Se o tipo de segurança do cliente ...	Então ...
Corresponde a um tipo de segurança especificado no parâmetro de acesso.	O cliente recebe acesso para esse nível com seu próprio ID de usuário.
Não corresponde a um tipo de segurança especificado, mas o parâmetro Access inclui a opção none.	O cliente recebe acesso para esse nível e recebe o usuário anônimo com o ID de usuário especificado pelo -anon parâmetro.
Não corresponde a um tipo de segurança especificado e o parâmetro Access não inclui a opção none.	O cliente não recebe nenhum acesso para esse nível.  Esta restrição não se aplica ao -superuser parâmetro porque este parâmetro sempre inclui nenhum, mesmo quando não especificado.

Kerberos 5 e Krb5p

A partir do ONTAP 9, a autenticação Kerberos 5 com serviço de privacidade (krb5p) é suportada. O modo de autenticação krbp5 é seguro e protege contra adulteração e espionagem de dados usando checksums para criptografar todo o tráfego entre cliente e servidor. A solução ONTAP suporta criptografia AES de 128 bits e 256 bits para Kerberos. O serviço de privacidade inclui verificar a integridade dos dados recebidos, autenticar usuários e criptografar dados antes da transmissão.

A opção krb5p está mais presente no recurso de política de exportação, onde é definida como uma opção de criptografia. O método de autenticação krb5p.1X pode ser usado como um parâmetro de autenticação, como mostrado no exemplo a seguir:

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
10.22.32.42 -volume flex_vol -authentication-method krb5p -protocol nfs3
-access- type read
```

Ative a assinatura e a vedação do protocolo Lightweight Directory Access

Assinatura e selagem são suportados para habilitar a segurança da sessão em consultas a um servidor LDAP. Essa abordagem fornece uma alternativa à segurança de sessão LDAP-over-TLS.

A assinatura confirma a integridade dos dados de carga útil LDAP usando tecnologia de chave secreta. A vedação criptografa os dados de carga útil LDAP para evitar a transmissão de informações confidenciais em texto não criptografado. As configurações de segurança de sessão em um SVM correspondem às disponíveis no servidor LDAP. Por padrão, a assinatura e a vedação LDAP são desativadas.

Passos

1. Para ativar esta função, execute o `vserver cifs security modify` comando com o `session-security-for-ad-ldap` parâmetro.

Opções para funções de segurança LDAP:

- **Nenhum:** Padrão, sem assinatura ou vedação
- **Sign:** Assine o tráfego LDAP
- **Seal:** Assine e criptografe o tráfego LDAP



Os parâmetros de sinal e selo são cumulativos, o que significa que, se a opção de sinal for usada, o resultado será LDAP com assinatura. No entanto, se a opção de vedação for usada, o resultado será sinal e selo. Além disso, se um parâmetro não for especificado para esse comando, o padrão será nenhum.

O seguinte é um exemplo de configuração:

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock  
-skew 3 -kerberos-ticket-age 8 -session-security-for-ad-ldap seal
```

Crie e use um FPolicy do NetApp

Você pode criar e usar um FPolicy, um componente de infraestrutura da solução ONTAP, que permite que aplicativos parceiros monitorem e definam permissões de acesso a arquivos. Uma das aplicações mais avançadas é a Segurança de workload de storage, uma aplicação SaaS da NetApp que oferece visibilidade e controle centralizados de todos os acessos a dados corporativos em ambientes de nuvem híbrida para garantir que as metas de segurança e conformidade sejam atingidas.

O controle de acesso é um conceito chave de segurança. A visibilidade e a capacidade de responder a acesso aos arquivos e operações de arquivos são essenciais para manter sua postura de segurança. Para fornecer visibilidade e controle de acesso para arquivos, a solução ONTAP usa o recurso NetApp FPolicy.

As políticas de arquivo podem ser definidas com base no tipo de arquivo. O FPolicy determina como o sistema de armazenamento processa solicitações de sistemas clientes individuais para operações como criar, abrir, renomear e excluir. A partir do ONTAP 9, a estrutura de notificação de acesso a arquivos FPolicy é aprimorada com controles de filtragem e resiliência contra interrupções de rede curtas.

Passos

1. Para aproveitar o recurso FPolicy, primeiro você deve criar a política FPolicy com o `vserver fpolicy policy create` comando.



Além disso, use o `-events` parâmetro se você usar o FPolicy para visibilidade e a coleção de eventos. A granularidade adicional fornecida pelo ONTAP permite filtrar e acessar o nível de controle do nome de usuário. Para controlar o Privileges e o acesso com nomes de usuário, especifique o `-privilege-user-name` parâmetro.

O texto a seguir fornece um exemplo de criação de FPolicy:

```
cluster1::> vservers fpolicy policy create -vservers vs1.example.com
-policy-name vs1_pol -events cserver_evt,vle1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Depois de criar a política FPolicy, você deve ativá-la com o `vservers fpolicy enable` comando. Este comando também define a prioridade ou a sequência da entrada FPolicy.



A sequência FPolicy é importante porque, se várias políticas se inscreveram no mesmo evento de acesso ao arquivo, a sequência dita a ordem em que o acesso é concedido ou negado.

O texto a seguir fornece uma configuração de exemplo para ativar a política FPolicy e validar a configuração com o `vservers fpolicy show` comando:

```
cluster1::> vservers fpolicy enable -vservers vs2.example.com -policy-name
vs2_pol -sequence-number 5

cluster1::> vservers fpolicy show
Vserver                Policy Name                Sequence  Status
Engine
-----
vs1.example.com        vs1_pol
vs2.example.com        vs2_pol
external
2 entries were displayed.
```

Melhorias de FPolicy

O ONTAP 9 inclui os aprimoramentos de FPolicy descritos nas seções a seguir.

Controles de filtragem

Novos filtros estão disponíveis para `SetAttr` e para remover notificações sobre atividades de diretório.

Resiliência assíncrona

Se um servidor FPolicy que opera no modo assíncrono sofrer uma interrupção na rede, as notificações FPolicy geradas durante a interrupção serão armazenadas no nó de storage. Quando o servidor FPolicy volta online, ele é alertado das notificações armazenadas e pode buscá-las a partir do nó de armazenamento. O período de tempo em que as notificações podem ser armazenadas durante uma interrupção é configurável até 10 minutos.

Segurança LIF

Um LIF é um endereço IP ou nome de porta mundial (WWPN) com características associadas, como uma função, uma porta inicial, um nó inicial, uma lista de portas para failover e uma política de firewall. Você pode configurar LIFs em portas pelas quais o cluster envia e recebe comunicações pela rede. É fundamental entender as características de segurança de cada função de LIF.

Funções do LIF

As funções de LIF podem ser as seguintes:

- **Data LIF:** Um LIF associado a um SVM e usado para comunicação com clientes.
- **Cluster LIF:** Um LIF usado para transportar tráfego entre nós em um cluster.
- **LIF de gerenciamento de nós:** Um LIF que fornece um endereço IP dedicado para gerenciar um nó específico em um cluster.
- **Cluster Management LIF:** Um LIF que fornece uma única interface de gerenciamento para todo o cluster.
- **Intercluster LIF:** Um LIF usado para comunicação entre clusters, backup e replicação.

Caraterísticas de segurança de cada função de LIF

	LIF de dados	LIF de cluster	LIF de gerenciamento de nós	LIF de gerenciamento de clusters	LIF entre clusters
Requer sub-rede IP privada?	Não	Sim	Não	Não	Não
Requer rede segura?	Não	Sim	Não	Não	Sim
Política de firewall predefinida	Muito restritivo	Completamente aberto	Média	Média	Muito restritivo
O firewall é personalizável?	Sim	Não	Sim	Sim	Sim



- Como o LIF do cluster está completamente aberto sem política de firewall configurável, ele deve estar em uma sub-rede IP privada em uma rede segura isolada.
- Sob nenhuma circunstância quaisquer papéis de LIF devem ser expostos à Internet.

Saiba mais sobre como proteger LIFs, consulte "[Configurar políticas de firewall para LIFs](#)".

Segurança de protocolo e porta

Além de executar operações e funções de segurança on-box, o endurecimento de uma solução também deve incluir mecanismos de segurança off-box. Aproveitar dispositivos de infraestrutura adicionais, como firewalls, sistemas de prevenção de intrusão (IPSs) e outros dispositivos de segurança, para filtrar e limitar o acesso ao ONTAP é uma maneira eficaz de estabelecer e manter uma postura de segurança rigorosa. Esta informação é

um componente chave para filtrar e limitar o acesso ao ambiente e aos seus recursos.

Protocolos e portas comumente usados

Serviço	Porta/protocolo	Descrição
SSH	22/TCP	Login SSH
telnet	23/TCP	Início de sessão remoto
Domain	53/TCP	Servidor de nomes de domínio
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Chamada de procedimento remoto
NTP	123/UDP	Protocolo de hora de rede
msrpc	135/UDP	Chamada de procedimento remoto da Microsoft
Netbios-name	137/TCP 137/UDP	Serviço de nomes NetBIOS
netbios-ssn	139/TCP	Sessão de serviço NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Link seguro:http
microsoft-ds	445/TCP	Serviços de diretório Microsoft
IPsec	500/UDP	Segurança do protocolo da Internet
mount	635/UDP	Montagem em NFS
named	953/UDP	Daemon de nomes
NFS	2049/UDP 2049/TCP	Daemon do servidor NFS
nrv	2050/TCP	Protocolo de volume remoto NetApp
iscsi	3260/TCP	Porta de destino iSCSI
Lockd	4045/TCP 4045/UDP	Daemon de bloqueio NFS
NFS	4046/TCP	Protocolo de montagem NFS
acp-proto	4046/UDP	Protocolo de contabilidade
rquotad	4049/UDP	Protocolo rquotad NFS
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Segurança do protocolo da Internet
acp	5125/UDP 5133/UDP 5144/TCP	Porta de controle alternativa para disco

Serviço	Porta/protocolo	Descrição
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS: Protocolo binário de escuta
TELNET	8023/TCP	Telnet com escopo de nó
HTTPS	8443/TCP	Ferramenta GUI 7MTT através do xref:./ontap-security-hardening/HTTPS
RSH	8514/TCP	RSH do nó-escopo
KMIP	9877/TCP	Porta de cliente KMIP (somente host local interno)
ndmp	10000/TCP	NDMP
cifs testemunha do porto	40001/TCP	Porta de testemunhas CIFS
TLS	50000/TCP	Segurança da camada de transporte
Iscsi	65200/TCP	Porta iSCSI
SSH	65502/TCP	Shell seguro
vsun	65503/TCP	vsun

Portas internas do NetApp

Porta/protocolo	Descrição
900	RPC de cluster NetApp
902	RPC de cluster NetApp
904	RPC de cluster NetApp
905	RPC de cluster NetApp
910	RPC de cluster NetApp
911	RPC de cluster NetApp
913	RPC de cluster NetApp
914	RPC de cluster NetApp
915	RPC de cluster NetApp
918	RPC de cluster NetApp
920	RPC de cluster NetApp
921	RPC de cluster NetApp
924	RPC de cluster NetApp
925	RPC de cluster NetApp
927	RPC de cluster NetApp
928	RPC de cluster NetApp
929	RPC de cluster NetApp

Porta/protocolo	Descrição
931	RPC de cluster NetApp
932	RPC de cluster NetApp
933	RPC de cluster NetApp
934	RPC de cluster NetApp
935	RPC de cluster NetApp
936	RPC de cluster NetApp
937	RPC de cluster NetApp
939	RPC de cluster NetApp
940	RPC de cluster NetApp
951	RPC de cluster NetApp
954	RPC de cluster NetApp
955	RPC de cluster NetApp
956	RPC de cluster NetApp
958	RPC de cluster NetApp
961	RPC de cluster NetApp
963	RPC de cluster NetApp
964	RPC de cluster NetApp
966	RPC de cluster NetApp
967	RPC de cluster NetApp
7810	RPC de cluster NetApp
7811	RPC de cluster NetApp
7812	RPC de cluster NetApp
7813	RPC de cluster NetApp
7814	RPC de cluster NetApp
7815	RPC de cluster NetApp
7816	RPC de cluster NetApp
7817	RPC de cluster NetApp
7818	RPC de cluster NetApp
7819	RPC de cluster NetApp
7820	RPC de cluster NetApp
7821	RPC de cluster NetApp
7822	RPC de cluster NetApp
7823	RPC de cluster NetApp

Porta/protocolo	Descrição
7824	RPC de cluster NetApp

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 SOFTWARES, 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.