



Segurança

ONTAP automation

NetApp
January 18, 2026

This PDF was generated from https://docs.netapp.com/pt-br/ontap-automation/workflows/wf_sec_list_accounts.html on January 18, 2026. Always check docs.netapp.com for the latest.

Índice

Segurança	1
Contas	1
Liste as contas usando a API REST do ONTAP	1
Certificados e chaves	3
Liste os certificados instalados usando a API REST do ONTAP	3
Instale um certificado usando a API REST do ONTAP	5
RBAC	6
Prepare-se para usar o RBAC usando a API REST do ONTAP	6
Crie funções	7
Crie um usuário com uma função usando a API REST do ONTAP	11

Segurança

Contas

Liste as contas usando a API REST do ONTAP

Você pode recuperar uma lista das contas. Você pode fazer isso para avaliar seu ambiente de segurança ou antes de criar uma nova conta.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/accounts

Tipo de processamento

Síncrono

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Exemplo de saída JSON

```
{  
    "records": [  
        {  
            "owner": {  
                "uuid": "642573a8-9d14-11ee-9330-005056aed3de",  
                "name": "vs0",  
                "_links": {  
                    "self": {  
                        "href": "/api/svm/svms/642573a8-9d14-11ee-9330-  
005056aed3de"  
                    }  
                }  
            },  
            "name": "vsadmin",  
            "_links": {  
                "self": {  
                    "href": "/api/security/accounts/642573a8-9d14-11ee-9330-  
005056aed3de/vsadmin"  
                }  
            }  
        },  
        {  
            "owner": {  
                "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",  
                "name": "sti214nscluster-1"  
            },  
            "name": "admin",  
            "_links": {  
                "self": {  
                    "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-  
005056aed3de/admin"  
                }  
            }  
        },  
        {  
            "owner": {  
                "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",  
                "name": "sti214nscluster-1"  
            },  
            "name": "autosupport",  
            "_links": {  
                "self": {  
                    "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-  
005056aed3de/autosupport"  
                }  
            }  
        }  
    ]  
}
```

```

        }
    }
},
"num_records": 3,
"_links": {
    "self": {
        "href": "/api/security/accounts"
    }
}
}

```

Certificados e chaves

Liste os certificados instalados usando a API REST do ONTAP

Pode listar os certificados instalados no cluster do ONTAP. Você pode fazer isso para ver se um certificado específico está disponível ou para obter a ID de um certificado específico.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/certificates

Parâmetros de entrada adicionais para exemplos curl

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados no exemplo curl nesta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
max_records	Consulta	Não	Especifique o número de Registros que você deseja retornar.

Curl exemplo: Retornar três certificados

```

curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"

```

Exemplo de saída JSON

```
{  
    "records": [  
        {  
            "uuid": "dad822c2-573c-11ee-a310-005056aecc29",  
            "name": "vs0_17866DB5C933E2EA",  
            "_links": {  
                "self": {  
                    "href": "/api/security/certificates/dad822c2-573c-11ee-a310-005056aecc29"  
                }  
            }  
        },  
        {  
            "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",  
            "name": "BuypassClass3RootCA",  
            "_links": {  
                "self": {  
                    "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-005056aecc29"  
                }  
            }  
        },  
        {  
            "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",  
            "name": "EntrustRootCertificationAuthority",  
            "_links": {  
                "self": {  
                    "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-005056aecc29"  
                }  
            }  
        }  
    ],  
    "num_records": 3,  
    "_links": {  
        "self": {  
            "href": "/api/security/certificates?max_records=3"  
        },  
        "next": {  
            "href": "/api/security/certificates?start.svm_id=sti214nscluster-1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"  
        }  
    }  
}
```

Instale um certificado usando a API REST do ONTAP

Você pode instalar um certificado X,509 assinado no cluster do ONTAP. Você pode fazer isso como parte da configuração de um recurso ou protocolo do ONTAP que requer autenticação forte.

Antes de começar

Tem de ter o certificado que pretende instalar. Você também deve certificar-se de que todos os certificados intermediários estão instalados conforme necessário.



Antes de usar os exemplos de entrada JSON incluídos abaixo, certifique-se de atualizar o `public_certificate` valor com o certificado para o seu ambiente.

Passo 1: Instale o certificado

Você pode emitir uma chamada de API para instalar o certificado.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/certificates

Exemplo de curl: Instale um certificado de CA raiz no nível do cluster

```
curl --request POST \
--location "https://$FQDN_IP/api/security/certificates" \
--include \
--header "Content-Type: application/json" \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{  
    "type": "server_ca",  
    "public_certificate":  
        "-----BEGIN CERTIFICATE-----  
MIID0TCCArkCFGYdznvTVvay1VZPNfy4yCCyPph6MA0GCSqGSIB3DQEBCwUAMIGk  
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDAAKBgNVBAcMA1JUUDEWMBQGA1UE  
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwT  
Ki5vbnRhcC1leGFtcGx1LmNvbTEvMC0GCSqGSIB3DQEJARYgZGF2aWQuGV0ZXJz  
b25Ab250YXAtZXhhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjQxMDA0MTUy  
OTE4WjCBpDELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQHDANSFAX  
FjAUBgNVBAoMDU9OVEFQIEV4YW1wbGUxEzARBgNVBAsMCK9OVEFQIDkuMTQxHDAa  
BgNVBAMMeYOUb250YXAtZXhhbXBsZS5jb20xLzAtBkgqhkiG9w0BCQEwigRhdmlk  
LnBldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAO  
AQ8AMIIBCgKCAQEAxQgy8mhblJhkf0D/MBodpzw0aSp2jGbWJ+Zv2G8BXkp1762  
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjh/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea  
tMTA/ZpQdZbQFZ5RKtdWz7dzzPYEl2x8Q1Jc8Kh7NxERNMtgpGWZZn7mfXKYr4O  
N/+vgahIhDibS8YK5rf1w6bfmrik9E2D+PEab9DX/1DL5RX4tz1H20kyN2UxoBR6  
Fq716n1Hi/5yR0Oi1xStN6s07EPoGak+KS1K41q+EciKRo0bP4mEQp8WMjJuiTkb  
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIB3DQEBCwUA  
A4IBAQABfBqOuROmYxdfrj93OyIiRoDcoMzvo8cHGNUsuhn1BDnL203qhWEs97s0  
mIy6zFMGnyNYa0t4i1cFsGDKP/JuljmYHjvv+21HWnxHjTo7AOQCnXmQH5swoDbf  
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUqlsbbM7w03tthBVMgo/h1  
E9I2jVOZsqMFujm2CYfMs4XKZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB  
WB/FE9n+P+FFJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvABC  
IpYuBcuKXLwAarhDEacXttVjC+Bq  
-----END CERTIFICATE-----"  
}
```

Passo 2: Confirme se o certificado foi instalado

Execute o fluxo de trabalho "[Liste os certificados instalados](#)" e confirme se o certificado está disponível.

RBAC

Prepare-se para usar o RBAC usando a API REST do ONTAP

Você pode usar a funcionalidade RBAC do ONTAP de várias maneiras diferentes, dependendo do seu ambiente. Alguns cenários comuns são apresentados como fluxos de trabalho nesta seção. Em cada caso, o foco está em um objetivo específico de segurança e administração.

Antes de criar quaisquer funções e atribuir uma função a uma conta de usuário do ONTAP, você deve se preparar revisando os principais requisitos e opções de segurança apresentados abaixo. Certifique-se também de rever os conceitos gerais do fluxo de trabalho em "[Prepare-se para usar os fluxos de trabalho](#)".

Qual versão do ONTAP você está usando?

A versão do ONTAP determina quais endpoints REST e recursos RBAC estão disponíveis.

Identificar os recursos e o escopo protegidos

Você precisa identificar os recursos ou comandos a serem protegidos e o escopo (cluster ou SVM).

Que acesso o usuário deve ter?

Depois de identificar os recursos e o escopo, você precisa determinar o nível de acesso a ser concedido.

Como os usuários acessarão o ONTAP?

O usuário pode acessar o ONTAP por meio da API REST ou CLI ou ambos.

Uma das funções incorporadas é suficiente ou é necessária uma função personalizada?

É mais conveniente usar uma função integrada existente, mas você pode criar uma nova função personalizada, se necessário.

Que tipo de papel é necessário?

Com base nos requisitos de segurança e no acesso à ONTAP, você precisa escolher se deseja criar uma FUNÇÃO REST ou tradicional.

Crie funções

Limitar o acesso a operações de volume do SVM com a API REST do ONTAP

É possível definir uma função para restringir a administração de volumes de storage em uma SVM.

Sobre este fluxo de trabalho

Uma função tradicional é criada pela primeira vez para permitir o acesso a todas as principais funções de administração de volume, exceto a clonagem. A função é definida com as seguintes características:

- Capaz de executar todas as operações de volume CRUD, incluindo obter, criar, modificar e excluir
- Não é possível criar um clone de volume

Você pode, então, opcionalmente, atualizar a função conforme necessário. Nesse fluxo de trabalho, a função é alterada na segunda etapa para permitir que o usuário crie um clone de volume.

Passo 1: Crie a função

Você pode emitir uma chamada de API para criar a função RBAC.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    { "path": "volume create", "access": "all" },
    { "path": "volume delete", "access": "all" }
  ]
}
```

Passo 2: Atualize a função

Você pode emitir uma chamada de API para atualizar a função existente.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Parâmetros de entrada adicionais para exemplos curl

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados no exemplo curl nesta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
SVM_ID	Caminho	Sim	Este é o UUID do SVM que contém a definição da função.
NOME_FUNÇÃO	Caminho	Sim	Esse é o nome da função na SVM a ser atualizada.

Curl exemplo

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{
  "path": "volume clone",
  "access": "all"
}
```

Ative a administração da proteção de dados usando a API REST do ONTAP

Você pode fornecer a um usuário recursos limitados de proteção de dados.

Sobre este fluxo de trabalho

O papel tradicional criado é definido com as seguintes características:

- Capaz de criar e excluir snapshots, bem como atualizar relacionamentos do SnapMirror
- Não é possível criar ou modificar objetos de nível superior, como volumes ou SVMs

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{  
    "name": "role1",  
    "owner": {  
        "name": "cluster-1",  
        "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
    },  
    "privileges": [  
        {"path": "volume snapshot create", "access": "all"},  
        {"path": "volume snapshot delete", "access": "all"},  
        {"path": "volume show", "access": "readonly"},  
        {"path": "vserver show", "access": "readonly"},  
        {"path": "snapmirror show", "access": "readonly"},  
        {"path": "snapmirror update", "access": "all"}  
    ]  
}
```

Permitir a geração de relatórios do ONTAP usando a API REST do ONTAP

Você pode criar uma FUNÇÃO REST para fornecer aos usuários a capacidade de gerar relatórios do ONTAP.

Sobre este fluxo de trabalho

A função criada é definida com as seguintes características:

- Capaz de recuperar todas as informações de objetos de storage relacionadas à capacidade e performance (como volume, qtree, LUN, agregados, nó e relacionamentos SnapMirror)
- Não é possível criar ou modificar objetos de nível superior (como volumes ou SVMs)

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

Exemplo de entrada JSON

```
{  
    "name": "rest_role1",  
    "owner": {  
        "name": "cluster-1",  
        "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
    },  
    "privileges": [  
        {"path": "/api/storage/volumes", "access": "readonly"},  
        {"path": "/api/storage/qtrees", "access": "readonly"},  
        {"path": "/api/storage/luns", "access": "readonly"},  
        {"path": "/api/storage/aggregates", "access": "readonly"},  
        {"path": "/api/cluster/nodes", "access": "readonly"},  
        {"path": "/api/snapmirror/relationships", "access": "readonly"},  
        {"path": "/api/svm/svms", "access": "readonly"}  
    ]  
}
```

Crie um usuário com uma função usando a API REST do ONTAP

Você pode usar esse fluxo de trabalho para criar um usuário com uma FUNÇÃO REST associada.

Sobre este fluxo de trabalho

Este fluxo de trabalho inclui as etapas típicas necessárias para criar uma FUNÇÃO REST personalizada e associá-la a uma nova conta de usuário. O usuário e a função têm um escopo do SVM e estão associados a um SVM de dados específico. Algumas das etapas podem ser opcionais ou precisam mudar dependendo do seu ambiente.

Etapa 1: Listar os SVMs de dados no cluster

Execute a seguinte chamada de API REST para listar os SVMs no cluster. O UUID e o nome de cada SVM são fornecidos na saída.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/svm/svms

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Depois de terminar

Selecione o SVM desejado na lista onde você criará o novo usuário e a função.

Etapa 2: Listar os usuários definidos para o SVM

Execute a seguinte chamada à API REST para listar os usuários definidos no SVM selecionado. Você pode identificar o SVM por meio do parâmetro proprietário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/accounts

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

Depois de terminar

Com base nos usuários já definidos no SVM, escolha um nome exclusivo para o novo usuário.

Etapa 3: Listar as funções REST definidas no SVM

Execute a seguinte chamada à API REST para listar as funções definidas no SVM selecionado. Você pode identificar o SVM por meio do parâmetro proprietário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
OBTER	/api/security/roles

Curl exemplo

```
curl --request GET \
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Depois de terminar

Com base nas funções já definidas no SVM, escolha um nome exclusivo para a nova função.

Passo 4: Crie uma FUNÇÃO REST personalizada

Execute a seguinte chamada de API REST para criar uma FUNÇÃO REST personalizada no SVM. A função inicialmente tem apenas um privilégio que estabelece um acesso padrão de **none** para que todo o acesso seja negado.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles

Curl exemplo

```
curl --request POST \
--location "https://$FQDN_IP/api/security/roles" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{
  "name": "dprole1",
  "owner": {
    "name": "dmp",
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api", "access": "none"},
  ]
}
```

Depois de terminar

Opcionalmente, execute a etapa 3 novamente para exibir a nova função. Você também pode exibir as funções na CLI do ONTAP.

Passo 5: Atualize a função adicionando mais Privileges

Execute a seguinte chamada de API REST para modificar a função adicionando Privileges conforme necessário.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/roles/"owner.randomUUID"/Privileges

Parâmetros de entrada adicionais para exemplos curl

Além dos parâmetros comuns com todas as chamadas de API REST, os seguintes parâmetros também são usados no exemplo curl nesta etapa.

Parâmetro	Tipo	Obrigatório	Descrição
SVM_ID	Caminho	Sim	UUID do SVM que contém a definição da função.
NOME_FUNÇÃO	Caminho	Sim	O nome da função no SVM a ser atualizado.

Curl exemplo

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

Depois de terminar

Opcionalmente, execute a etapa 3 novamente para exibir a nova função. Você também pode exibir as funções na CLI do ONTAP.

Passo 6: Crie um usuário

Execute a seguinte chamada de API REST para criar uma conta de usuário. A função **dprole1** criada acima está associada ao novo usuário.



Você pode criar o usuário sem uma função. Nesse caso, é atribuída ao usuário uma função padrão (`admin`ou `vsadmin`), dependendo se o usuário está definido com escopo de cluster ou SVM. Você precisará modificar o usuário para atribuir uma função diferente.

Método HTTP e endpoint

Essa chamada de API REST usa o método e o endpoint a seguir.

Método HTTP	Caminho
POST	/api/security/accounts

Curl exemplo

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

Exemplo de entrada JSON

```
{
  "owner": {"uuid":"daf84055-248f-11ed-a23d-005056ac4fe6"} ,
  "name": "david",
  "applications": [
    {"application":"ssh",
     "authentication_methods": ["password"] ,
     "second_authentication_method": "none" }
  ],
  "role": "dprole1",
  "password": "<password>"
}
```

Depois de terminar

Você pode fazer login na interface de gerenciamento do SVM usando as credenciais do novo usuário.

Informações sobre direitos autorais

Copyright © 2026 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 DESTE DOCUMENTO. 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 SOBRESSALENTES; 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 DESTE SOFTWARE, 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.