



Contas de administrador de armazenamento local

ONTAP Technical Reports

NetApp
January 23, 2026

Índice

Contas de administrador de armazenamento local	1
Funções, aplicativos e autenticação do ONTAP	1
Funções	1
Métodos de aplicação	5
Métodos de autenticação	5
Contas administrativas padrão	6
Listar contas locais	7
Definir a palavra-passe da conta de diagnóstico (diag)	7
Verificação multi-admin	8
Bloqueio instantâneo	9
Configure o acesso à API baseado em certificado	9
Autenticação baseada em token ONTAP OAuth 2,0 para API REST	12
Parâmetros de login e senha	12
Novos recursos de conta local	13
Suporte SHA-512	13
Parâmetros da palavra-passe	15

Contas de administrador de armazenamento local

Funções, aplicativos e autenticação do ONTAP

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 do 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
vsadmin	<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, snapshots 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, exceto movimentos de volume • Gerencie cotas, qtrees, snapshots 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 • Gerenciar relacionamentos e snapshots do SnapMirror • 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, snapshots 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
```

- 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 ative 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`o .
- 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.



Não é possível remover ou renomear contas incorporadas. Se um administrador remover a conta, após reiniciar, a conta incorporada será recriada. **NetApp recomenda** bloquear quaisquer contas incorporadas desnecessárias com o comando lock.

Embora contas órfãs representem um problema de segurança significativo, **NetApp recomenda fortemente** testar o efeito da remoção de contas do repositório local.

Listar contas locais

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

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

vserver: cluster1
          Authentication          Acct  Is-Nsswitch
User/Group Name Application Method  Role Name  Locked  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, você pode usar a verificação multiadministrador (MAV) para permitir que determinadas operações, como a exclusão de volumes ou snapshots, 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 usuário inicia a operação, um ["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 instantâneo

O bloqueio de snapshot é um recurso do SnapLock no qual os snapshots são tornados indeléveis manual ou automaticamente com um período de retenção na política de snapshot de volume. O objetivo do bloqueio de snapshot é impedir que administradores desonestos ou não confiáveis excluam snapshots no sistema ONTAP primário ou secundário.

O bloqueio instantâneo foi introduzido no ONTAP 9.12.1. O bloqueio de snapshot também é conhecido como bloqueio de snapshot à prova de violação. Embora exija a licença SnapLock e a inicialização do relógio de conformidade, o bloqueio de instantâneos 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. Essa é uma melhoria em relação aos snapshots 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, consulte "["documentação de bloqueio de instantâneos"](#)".

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 carateres 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.

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

Todas as senhas devem ser distintas do nome de usuário.

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

Atributo	Descrição	Padrão	Alcance
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	-
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 carateres alfabéticos minúsculos necessário na senha	0, que não requer carateres minúsculos	0-64
passwd-min-uppercase-chars	Número mínimo de carateres alfabéticos maiúsculos necessário	0, que não requer carateres 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
```

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 SOBRESSAENTES; 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.