Cuentas de administrador de almacenamiento local

ONTAP 9

NetApp
July 19, 2024

Tabla de contenidos

Cuentas de administrador de almacenamiento local

Roles, aplicaciones y autenticación

ONTAP proporciona a la empresa condicionada por la seguridad la capacidad de brindar acceso granular a distintos administradores mediante diferentes métodos y aplicaciones de inicio de sesión. Esto ayuda a los clientes a crear un modelo de confianza cero centrado en los datos.

Estas son las funciones disponibles para los administradores de máquinas virtuales de almacenamiento y administradores. Se especifican los métodos de aplicación de inicio de sesión y los métodos de autenticación de inicio de sesión.

Funciones

Con el control de acceso basado en roles, los usuarios solo tienen acceso a los sistemas y las opciones requeridas para sus roles y funciones de trabajo. La solución RBAC de ONTAP limita el acceso administrativo de los usuarios al nivel permitido por el rol que tengan definido, lo que permite a los administradores gestionar usuarios según el rol asignado. ONTAP ofrece varios roles predefinidos. Los operadores y administradores pueden crear, modificar o suprimir roles de control de acceso personalizados, y pueden especificar restricciones de cuenta para roles específicos.

Roles predefinidos para administradores de clúster

Este rol…	Tiene este nivel de acceso…	A los siguientes comandos o directorios de comandos
`admin`	Todo	Todos los directorios de comandos (`DEFAULT`)
`admin-no-fsa` (Disponible a partir de ONTAP 9.12.1)	Lectura/Escritura	• Todos los directorios de comandos (`DEFAULT`) • `security login rest-role` • `security login role`

Solo lectura	• `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`	Ninguno
`volume file show-disk-usage`	`autosupport`	Todo
• `set` • `system node autosupport`	Ninguno	Todos los demás directorios de comandos (`DEFAULT`)
`backup`	Todo	`vserver services ndmp`
Solo lectura	`volume`	Ninguno
Todos los demás directorios de comandos (`DEFAULT`)	`readonly`	Todo

• `security login password` Sólo para gestionar la contraseña local y la información de claves de la cuenta de usuario propia • `set`	Ninguno	`security`
Solo lectura	Todos los demás directorios de comandos (`DEFAULT`)	`none`

> La `autosupport` el rol se asigna a los predefinidos `autosupport` Cuenta, que utiliza AutoSupport OnDemand. ONTAP le impide modificar o eliminar el `autosupport` cuenta. ONTAP también le impide asignar el `autosupport` función para otras cuentas de usuario.

Roles predefinidos para administradores de máquinas virtuales de almacenamiento (SVM)

Nombre del rol	Funcionalidades
`vsadmin`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Realice operaciones de SnapLock, excepto la supresión con privilegios • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red • Supervise el estado de la SVM

`vsadmin-volume`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestión de volúmenes, incluidos los movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Gestionar las LUN • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-protocol`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Configurar protocolos: NFS, SMB, iSCSI, FC, FCoE y NVMe/FC y NVMe/TCP • Configurar servicios: DNS, LDAP y NIS • Gestionar las LUN • Supervise la interfaz de red • Supervise el estado de la SVM
`vsadmin-backup`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestione las operaciones de NDMP • Haga que un volumen restaurado sea de lectura/escritura • Gestionar relaciones de SnapMirror y copias Snapshot • Ver información de volúmenes y redes

`vsadmin-snaplock`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Gestionar volúmenes, excepto movimientos de volúmenes • Gestione cuotas, qtrees, copias Snapshot y archivos • Realizar operaciones de SnapLock, incluida la supresión con privilegios • Configurar protocolos: NFS y SMB • Configurar servicios: DNS, LDAP y NIS • Supervisar trabajos • Supervise las conexiones de red y la interfaz de red
`vsadmin-readonly`	• Administrar la contraseña local y la información de clave de la cuenta de usuario propia • Supervise el estado de la SVM • Supervise la interfaz de red • Ver volúmenes y LUN • Ver servicios y protocolos

Métodos de aplicación

El método de aplicación especifica el tipo de acceso del método de inicio de sesión. Los valores posibles incluyen `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, y `telnet`.

Configurar este parámetro `service-processor` para otorgar al usuario acceso a Service Processor. Cuando este parámetro se define en `service-processor`, el `-authentication-method` parámetro se debe definir en `password` porque el procesador de servicios sólo admite la autenticación de contraseña. Las cuentas de usuario de SVM no pueden acceder a Service Processor. Por lo tanto, los operadores y administradores no pueden utilizar el `-vserver` parámetro cuando este parámetro se define en `service-processor`.

Para restringir aún más el acceso al `service-processor` comando, utilice el comando `system service-processor ssh add-allowed-addresses`. El comando `system service-processor api-service` se puede utilizar para actualizar las configuraciones y los certificados.

Por motivos de seguridad, Telnet y el Shell remoto (RSH) están deshabilitados de forma predeterminada porque NetApp recomienda el shell seguro (SSH) para el acceso remoto seguro. Si hay un requisito o una necesidad única de Telnet o RSH, deben estar activados.

El `security protocol modify` comando modifica la configuración existente en todo el cluster de RSH y Telnet. Active RSH y Telnet en el cluster definiendo el campo Activado en `true`.

Métodos de autenticación

El parámetro del método de autenticación especifica el método de autenticación utilizado para inicios de sesión.

Método de autenticación	Descripción
`cert`	Autenticación de certificado SSL
`community`	Cadenas de comunidad SNMP
`domain`	Autenticación de Active Directory
`nsswitch`	Autenticación LDAP o NIS
`password`	Contraseña
`publickey`	Autenticación de clave pública
`usm`	Modelo de seguridad de usuario SNMP

No se recomienda el uso de NIS debido a las debilidades de seguridad del protocolo.

A partir de ONTAP 9,3, la autenticación encadenada de dos factores está disponible para cuentas SSH locales `admin` que utilizan `publickey` y contraseña como los dos métodos de autenticación. Además del `-authentication-method` campo del `security login` comando, se ha agregado un nuevo campo denominado `-second-authentication-method` . La clave pública o la contraseña se pueden especificar como `-authentication-method` o la `-second-authentication-method`. Sin embargo, durante la autenticación SSH, el orden es siempre clave pública con autenticación parcial, seguido de la solicitud de contraseña para la autenticación completa.

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

A partir de ONTAP 9,4, `nsswitch` se puede utilizar como un segundo método de autenticación con `publickey`.

A partir de ONTAP 9.12.1, FIDO2 también se puede usar para la autenticación SSH usando un dispositivo de autenticación de hardware YubiKey u otros dispositivos compatibles con FIDO2.

A partir de ONTAP 9,13.1:

- `domain` las cuentas se pueden utilizar como un segundo método de autenticación con `publickey`.
- Contraseña de un solo uso basada en tiempo (`totp`) es un código de acceso temporal generado por un algoritmo que utiliza la hora actual del día como uno de sus factores de autenticación para el segundo método de autenticación.
- La revocación de claves públicas es compatible con claves públicas SSH, así como con certificados que se comprobarán para su caducidad/revocación durante SSH.

Para obtener más información sobre la autenticación multifactor (MFA) para el administrador del sistema de ONTAP, Active IQ Unified Manager y SSH, consulte "TR-4647: Autenticación multifactor en ONTAP 9".

Cuentas administrativas predeterminadas

Se debe restringir la cuenta de administrador porque se permite el acceso al rol de administrador mediante todas las aplicaciones. La cuenta de diagnóstico (diag) permite acceder al shell del sistema y se debe reservar solo para que el soporte técnico realice tareas de solución de problemas.

Hay dos cuentas administrativas predeterminadas `admin` : Y `diag`.

Las cuentas huérfanas son un vector de seguridad importante que a menudo conduce a vulnerabilidades, incluida la escalada de privilegios. Se trata de cuentas innecesarias y no utilizadas que permanecen en el repositorio de cuentas de usuario. Son principalmente cuentas predeterminadas que nunca se usaron o para las que las contraseñas nunca se actualizaron o cambiaron. Para solucionar este problema, ONTAP admite la eliminación y el cambio de nombre de las cuentas.

ONTAP no puede eliminar ni cambiar el nombre de las cuentas integradas. Sin embargo, NetApp recomienda bloquear cualquier cuenta incorporada innecesaria con el comando lock.

Aunque las cuentas huérfanas son un problema de seguridad importante, NetApp recomienda probar el efecto de eliminar cuentas del repositorio de cuentas local.

Enumerar las cuentas locales

Para mostrar las cuentas locales, ejecute `security login show` el 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.
```

Elimine la cuenta de administrador predeterminada

La `admin` cuenta tiene el rol de administrador y se le permite el acceso utilizando todas las aplicaciones.

Pasos

1. Cree otra cuenta de nivel de administrador.

   Para eliminar por completo la cuenta predeterminada `admin` , primero debe crear otra cuenta de nivel de administrador que utilice la `console` aplicación de inicio de sesión.

Hacer estos cambios puede causar algunos efectos no deseados. Pruebe siempre los nuevos ajustes que puedan afectar el estado de seguridad de la solución en un clúster que no sea de producción primero.

Ejemplo:

```
cluster1::*> security login create -user-or-group-name NewAdmin
-application console -authentication-method password -vserver cluster1
```

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

Vserver: cluster1
                             Authentication             Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name        Locked Group
---------------- ----------- --------- ---------------- ------
-----------
NewAdmin         console     password  admin            no     no
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
7 entries were displayed.
```

2. Después de crear la nueva cuenta de administrador, pruebe el acceso a esa cuenta con el `NewAdmin` inicio de sesión de la cuenta. Con la `NewAdmin` conexión, configure la cuenta para que tenga las mismas aplicaciones de conexión que la cuenta de administración predeterminada o anterior (por ejemplo, `http ontapi`, , `service-processor`o `ssh`). Este paso garantiza que se mantenga el control de acceso.

   Ejemplo:

```
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ssh -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application http -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application ontapi -authentication-method password
cluster1::*> security login create -vserver cluster1 -user-or-group-name
NewAdmin -application service-processor -authentication-method password
```

3. Después de probar todas las funciones, puede desactivar la cuenta de administrador para todas las aplicaciones antes de eliminarla de ONTAP. Este paso sirve como prueba final para confirmar que no hay

funciones persistentes que se basen en la cuenta de administrador anterior.

```
cluster1::*> security login lock -vserver cluster1 -user-or-group-name
admin -application *
```

4. Para eliminar la cuenta de administrador predeterminada y todas las entradas para ella, ejecute el siguiente comando:

```
cluster1::*> security login delete -vserver cluster1 -user-or-group-name
admin -application *
cluster1::*> security login show -vserver cluster1

Vserver: cluster1
                             Authentication              Acct   Is-
Nsswitch
User/Group Name  Application Method    Role Name         Locked Group
---------------- ----------- --------- ----------------- ------
-----------
NewAdmin         console     password  admin             no     no
NewAdmin         http        password  admin             no     no
NewAdmin         ontapi      password  admin             no     no
NewAdmin         service-processor password admin        no     no
NewAdmin         ssh         password  admin             no     no
autosupport      console     password  autosupport       no     no
7 entries were displayed.
```

Establezca la contraseña de la cuenta de diagnóstico (diag)

El sistema de almacenamiento se proporciona una cuenta de diagnóstico llamada `diag` . Puede utilizar `diag` la cuenta para realizar tareas de solución de problemas en la `systemshell`. La `diag` cuenta es la única cuenta que se puede utilizar para acceder al systemshell a través del `diag` comando con privilegios `systemshell`.

> El systemshell y la cuenta asociada `diag` están pensados para fines de diagnóstico de bajo nivel. Su acceso requiere el nivel de privilegio de diagnóstico y se reserva solo para utilizarse con orientación del soporte técnico para realizar tareas de solución de problemas. Ni la `diag` cuenta ni la `systemshell` está destinada a fines administrativos generales.

Antes de empezar

Antes de acceder a `systemshell`, debe definir `diag` la contraseña de la cuenta mediante el `security login password` comando. Debe utilizar principios de contraseña seguros y cambiar la `diag` contraseña a intervalos regulares.

Pasos

1. Establezca `diag` la contraseña de usuario de la cuenta:

```
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%
```

Verificación de varios administradores

A partir de ONTAP 9.11.1, puede usar la verificación multiadministrador (MAV) para permitir que ciertas operaciones, como la eliminación de volúmenes o copias de Snapshot, se ejecuten solo después de las aprobaciones de los administradores designados. De este modo, se evita que administradores comprometidos, malintencionados o inexpertos realicen cambios no deseados o eliminen datos.

La configuración de MAV consiste en lo siguiente:

- "Crear uno o varios grupos de aprobación de administrador."
- "Habilitar la funcionalidad de verificación multi-administrador."
- "Adición o modificación de reglas."

Después de la configuración inicial, solo los administradores de un grupo de aprobación MAV (administradores de MAV) pueden modificar estos elementos.

Cuando MAV está activado, la realización de todas las operaciones protegidas requiere tres pasos:

1. Cuando un usuario inicia la operación, a. "se genera la solicitud."
2. Antes de que se pueda ejecutar, el número necesario de "Los administradores de MAV deben aprobar."
3. Después de la aprobación, el usuario completa la operación.

MAV no se ha diseñado para su uso con volúmenes o flujos de trabajo que implican una gran automatización, ya que cada tarea automatizada requiere aprobación antes de que se pueda completar la operación. Si desea utilizar la automatización y MAV conjuntamente, NetApp recomienda que utilice consultas para operaciones de MAV específicas. Por ejemplo, puede aplicar `volume delete` reglas MAV solo a volúmenes en los que la automatización no esté involucrada, y puede designar esos volúmenes con un esquema de nomenclatura particular.

Para obtener información más detallada sobre MAV, consulte la "Documentación de verificación multiadministrador de ONTAP".

Bloqueo de copia de snapshot

El bloqueo de copia de Snapshot es una función de SnapLock en la que las copias de Snapshot se vuelven indelebles manual o automáticamente con un periodo de retención en la política de snapshots para volúmenes. El propósito del bloqueo de copias de Snapshot es impedir que los administradores malintencionados o que no sean de confianza eliminen snapshots en sistemas de ONTAP principales o secundarios.

Se introdujo el bloqueo de copias snapshot en ONTAP 9.12.1. El bloqueo de copia de SnapVault se conoce también como bloqueo de instantáneas a prueba de manipulaciones. Aunque requiere la licencia de SnapLock y la inicialización del reloj de cumplimiento de normativas, el bloqueo de copia de SnapShot no está relacionado con el cumplimiento de normativas de SnapLock ni con SnapLock Enterprise. No existe un administrador de almacenamiento de confianza, como sucede con SnapLock Enterprise y no protege la infraestructura de almacenamiento físico subyacente, como sucede con el cumplimiento de normativas de SnapLock. Esta es una mejora con respecto a la copia snapshot de SnapVault en un sistema secundario. Es posible lograr una rápida recuperación de copias Snapshot bloqueadas en sistemas principales para restaurar volúmenes dañados por el ransomware.

Si quiere más información sobre el bloqueo de copias snapshot, consulte "Documentación de ONTAP".

Configure el acceso de API basado en certificados

En lugar de utilizar la autenticación basada en certificado y el ID de usuario para la API de REST o el acceso de la API de SDK de capacidad de gestión de NetApp para ONTAP.

> Como alternativa a la autenticación basada en certificados para la API de REST, utilice "Autenticación basada en token OAuth 2,0".)

Puede generar e instalar un certificado autofirmado en ONTAP, tal y como se describe en estos pasos.

Pasos

1. Con OpenSSL, genere un certificado ejecutando el siguiente 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 genera un certificado público denominado `test.pem` y una clave privada denominada `key.out`. El nombre común, CN, corresponde al ID de usuario de ONTAP.

2. Instale el contenido del certificado público en formato de correo mejorado de privacidad (pem) en ONTAP ejecutando el siguiente comando y pegando el contenido del certificado cuando se le solicite:

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

Please enter Certificate: Press <Enter> when done
```

3. Active ONTAP para permitir el acceso del cliente a través de SSL y defina el ID de usuario para el acceso a la 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
```

En el siguiente ejemplo, el ID de usuario `cert_user` ahora está habilitado para utilizar acceso a API autenticado con certificado. Un script de Python de SDK de gestión simple que utiliza `cert_user` para mostrar la versión de ONTAP aparece de la siguiente manera:

```
#!/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)
```

El resultado del script muestra la versión de ONTAP.

```
./version.py

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

4. Para realizar una autenticación basada en certificados con la API REST DE ONTAP, complete los siguientes pasos:
   a. En ONTAP, defina el ID de usuario para el acceso http:

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

b. En su cliente Linux, ejecute el siguiente comando que genera la versión de ONTAP como resultado:

```
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"
        }
    }
}
```

Más información

- "Autenticación basada en certificados con el SDK de capacidad de gestión de NetApp para ONTAP".

Autenticación basada en token OAuth 2,0 de ONTAP para la API de REST

Como alternativa a la autenticación basada en certificados, puede utilizar la autenticación basada en tokens OAuth 2,0 para la API REST.

A partir de ONTAP 9.14.1, tiene la opción de controlar el acceso a sus clústeres de ONTAP mediante el marco de autorización abierta (OAuth 2,0). Es posible configurar esta función mediante cualquiera de las interfaces administrativas de ONTAP, incluida la interfaz de línea de comandos de ONTAP, System Manager y la API de REST. Sin embargo, las decisiones de autorización y control de acceso de OAuth 2,0 solo se pueden aplicar cuando un cliente accede a ONTAP mediante la API REST.

Los tokens OAuth 2,0 reemplazan las contraseñas para la autenticación de cuentas de usuario.

Para obtener más información sobre el uso de OAuth 2,0, consulte la "Documentación de ONTAP sobre autenticación y autorización mediante OAuth 2,0".

Parámetros de inicio de sesión y contraseña

Una postura de seguridad efectiva se adhiere a las políticas organizativas establecidas, directrices y cualquier gobierno o estándares que se apliquen a la organización. Algunos ejemplos de estos requisitos incluyen la vida útil del nombre de usuario, los requisitos de longitud de contraseña, los requisitos de caracteres y el almacenamiento de dichas cuentas. La solución ONTAP ofrece características y funciones para abordar estos problemas de seguridad.

Nuevas funciones de cuenta local

Para admitir las políticas, directrices o estándares de cuentas de usuario de una organización, incluida la gobernanza, ONTAP admite las siguientes funciones:

- Configuración de políticas de contraseñas para aplicar un número mínimo de dígitos, caracteres en minúsculas o caracteres en mayúsculas
- Se requiere un retraso después de un intento fallido de inicio de sesión
- Definición del límite inactivo de la cuenta
- Vencimiento de una cuenta de usuario
- Mostrando un mensaje de advertencia de caducidad de contraseña
- Notificación de una conexión no válida

Los ajustes configurables se gestionan mediante el comando security login role config modify.

Compatibilidad con SHA-512

Para mejorar la seguridad de las contraseñas, ONTAP 9 admite la función hash de contraseña SHA-2 y utiliza por defecto SHA-512 para hash de contraseñas recién creadas o modificadas. Los operadores y administradores también pueden caducar o bloquear cuentas según sea necesario.

Las cuentas de usuario de ONTAP 9 preexistentes con contraseñas sin modificar siguen utilizando la función hash MD5 después de la actualización a ONTAP 9,0 o posterior. Sin embargo, NetApp recomienda encarecidamente que estas cuentas de usuario migren a la solución SHA-512 más segura al hacer que los usuarios cambien sus contraseñas.

La funcionalidad hash de contraseña le permite realizar las siguientes tareas:

- Muestra las cuentas de usuario que coinciden con la función 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
```

- Las cuentas Expire que utilizan una función hash especificada (por ejemplo, MD5), que obliga a los usuarios a cambiar sus contraseñas en el siguiente inicio de sesión:

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

- Bloquear cuentas con contraseñas que utilizan la función hash especificada.

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

La función hash de contraseña es desconocida para el usuario interno `autosupport` de la SVM administrativa del clúster. Este problema es cosmético. La función hash es desconocida porque este usuario interno no tiene una contraseña configurada por defecto.

  - Para ver la función hash de contraseña del `autosupport` usuario, ejecute los siguientes 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 establecer la función hash de contraseña (valor por defecto: SHA512), ejecute el siguiente comando:

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

No importa en qué se establezca la contraseña.

```
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
```

Parámetros de contraseña

La solución de ONTAP admite parámetros de contraseña que abordan los requisitos y las directrices de las políticas de la organización y los respaldan.

Atributo	Descripción	Predeterminado	Rango
`username-minlength`	Longitud mínima de nombre de usuario requerida	3	3-16
`username-alphanum`	Nombre de usuario alfanumérico	deshabilitado	Activado/Desactivado
`passwd-minlength`	Longitud mínima requerida de contraseña	8	3-64
`passwd-alphanum`	Contraseña alfanumérica	activado	Activado/Desactivado
`passwd-min-special-chars`	Número mínimo de caracteres especiales requeridos en la contraseña	0	0-64
`passwd-expiry-time`	Tiempo de caducidad de la contraseña (en días)	Ilimitado, lo que significa que las contraseñas nunca caducan	0-ilimitado 0 == vence ahora
`require-initial-passwd-update`	Requerir la actualización inicial de la contraseña en el primer inicio de sesión	Deshabilitado	Activado/Desactivado Cambios permitidos a través de la consola o SSH
`max-failed-login-attempts`	Número máximo de intentos fallidos	0, no bloquee la cuenta	-

Atributo	Descripción	Predeterminado	Rango
`lockout-duration`	Período máximo de bloqueo (en días)	El valor predeterminado es 0, lo que significa que la cuenta está bloqueada durante un día	-
`disallowed-reuse`	No permitir las últimas N contraseñas	6	El mínimo es 6
`change-delay`	Retraso entre cambios de contraseña (en días)	0	-
`delay-after-failed-login`	Retraso tras cada intento de inicio de sesión fallido (en segundos)	4	-
`passwd-min-lowercase-chars`	Número mínimo de caracteres alfabéticos en minúscula necesarios en la contraseña	0, que no requiere caracteres en minúsculas	0-64
`passwd-min-uppercase-chars`	Núm. Mínimo de caracteres alfabéticos en mayúsculas necesario	0, que no requiere caracteres en mayúsculas	0-64
`passwd-min-digits`	Número mínimo de dígitos necesarios en la contraseña	0, que no requiere dígitos	0-64
`passwd-expiry-warn-time`	Mostrar mensaje de advertencia antes del vencimiento de la contraseña (en días)	Ilimitado, lo que significa que nunca advierta sobre la caducidad de la contraseña	0, lo que significa advertir al usuario sobre la caducidad de la contraseña cada vez que se inicia sesión correctamente
`account-expiry-time`	La cuenta caduca en N días	Ilimitado, lo que significa que las cuentas nunca caducan	La hora de vencimiento de la cuenta debe ser mayor que el límite inactivo de la cuenta
`account-inactive-limit`	Duración máxima de la inactividad antes del vencimiento de la cuenta (en días)	Ilimitado, lo que significa que las cuentas inactivas nunca caducan	El límite inactivo de la cuenta debe ser inferior al tiempo de vencimiento de la cuenta

Ejemplo

```
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, se aumenta la complejidad y las reglas de bloqueo de las contraseñas. Esto se aplica solo a las nuevas instalaciones de ONTAP.