Account degli amministratori dello storage locali

ONTAP 9

NetApp
July 19, 2024

Sommario

Account degli amministratori dello storage locali

Ruoli, applicazioni e autenticazione

ONTAP fornisce alle aziende attente alla sicurezza la capacità di fornire accesso granulare a diversi amministratori tramite diverse applicazioni e metodi di accesso. In questo modo, i clienti possono creare un modello zero-trust incentrato sui dati.

Questi sono i ruoli disponibili per gli amministratori di Storage Virtual Machine e Amministratore. Vengono specificati i metodi dell'applicazione di accesso e di autenticazione dell'accesso.

Ruoli

Con il role-based access control (RBAC), gli utenti possono accedere solo ai sistemi e alle opzioni necessari per le loro mansioni e funzioni. La soluzione RBAC in ONTAP limita l'accesso amministrativo degli utenti al livello concesso per il ruolo definito, consentendo agli amministratori di gestire gli utenti in base al ruolo assegnato. ONTAP fornisce diversi ruoli predefiniti. Gli operatori e gli amministratori possono creare, modificare o eliminare ruoli di controllo dell'accesso personalizzati e specificare restrizioni account per ruoli specifici.

Ruoli predefiniti per gli amministratori del cluster

Questo ruolo…	Dispone di questo livello di accesso…	Alle seguenti directory di comandi o comandi
`admin`	Tutto	Tutte le directory dei comandi (`DEFAULT`)
`admin-no-fsa` (Disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	• Tutte le directory dei comandi (`DEFAULT`) • `security login rest-role` • `security login role`

Di sola lettura	• `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`	Nessuno
`volume file show-disk-usage`	`autosupport`	Tutto
• `set` • `system node autosupport`	Nessuno	Tutte le altre directory di comando (`DEFAULT`)
`backup`	Tutto	`vserver services ndmp`
Di sola lettura	`volume`	Nessuno
Tutte le altre directory di comando (`DEFAULT`)	`readonly`	Tutto

• `security login password` Solo per la gestione della password locale del proprio account utente e delle informazioni sulle chiavi • `set`	Nessuno	`security`
Di sola lettura	Tutte le altre directory di comando (`DEFAULT`)	`none`

Il `autosupport` il ruolo viene assegnato al predefinito `autosupport` Account, utilizzato da AutoSupport OnDemand. ONTAP impedisce di modificare o eliminare `autosupport` account. ONTAP impedisce inoltre l'assegnazione di `autosupport` ruolo per altri account utente.

Ruoli predefiniti per gli amministratori delle Storage Virtual Machine (SVM)

Nome del ruolo	Funzionalità
`vsadmin`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestisci i volumi, tranne che per gli spostamenti dei volumi • Gestire quote, qtree, copie Snapshot e file • Gestire le LUN • Eseguire operazioni SnapLock, ad eccezione dell'eliminazione con privilegi • Configurare i protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurare i servizi: DNS, LDAP e NIS • Monitorare i lavori • Monitorare le connessioni di rete e l'interfaccia di rete • Monitorare lo stato di salute della SVM

`vsadmin-volume`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestire i volumi, inclusi gli spostamenti di volumi • Gestire quote, qtree, copie Snapshot e file • Gestire le LUN • Configurare i protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurare i servizi: DNS, LDAP e NIS • Monitorare l'interfaccia di rete • Monitorare lo stato di salute della SVM
`vsadmin-protocol`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Configurare i protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurare i servizi: DNS, LDAP e NIS • Gestire le LUN • Monitorare l'interfaccia di rete • Monitorare lo stato di salute della SVM
`vsadmin-backup`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestire le operazioni NDMP • Eseguire la lettura/scrittura di un volume ripristinato • Gestisci le relazioni di SnapMirror e le copie Snapshot • Visualizzare volumi e informazioni sulla rete
`vsadmin-snaplock`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestisci i volumi, tranne che per gli spostamenti dei volumi • Gestire quote, qtree, copie Snapshot e file • Eseguire operazioni SnapLock, compresa l'eliminazione con privilegi • Configurare i protocolli: NFS e SMB • Configurare i servizi: DNS, LDAP e NIS • Monitorare i lavori • Monitorare le connessioni di rete e l'interfaccia di rete

`vsadmin-readonly`	• Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Monitorare lo stato di salute della SVM • Monitorare l'interfaccia di rete • Visualizza volumi e LUN • Visualizzare servizi e protocolli

Metodi di applicazione

Il metodo dell'applicazione specifica il tipo di accesso del metodo di accesso. I valori possibili comprendono `console`, `http`, `ontapi`, `rsh`, `snmp`, `service-processor`, `ssh`, e `telnet`.

L'impostazione di questo parametro per `service-processor` consente all'utente di accedere al Service Processor. Quando questo parametro è impostato su `service-processor`, il `-authentication-method` parametro deve essere impostato su `password` perché Service Processor supporta solo l'autenticazione tramite password. Gli account utente SVM non possono accedere al Service Processor. Pertanto, gli operatori e gli amministratori non possono utilizzare il `-vserver` parametro quando questo parametro è impostato su `service-processor`.

Per limitare ulteriormente l'accesso a `service-processor` utilizzare il comando `system service-processor ssh add-allowed-addresses`. Il comando `system service-processor api-service` può essere utilizzato per aggiornare le configurazioni e i certificati.

Per motivi di sicurezza, Telnet e Remote Shell (RSH) sono disattivati per impostazione predefinita perché NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro. Se esiste un requisito o un'esigenza unica per Telnet o RSH, è necessario attivarli.

Il `security protocol modify` comando modifica la configurazione esistente a livello di cluster di RSH e Telnet. Attivare RSH e Telnet nel cluster impostando il campo abilitato su `true`.

Metodi di autenticazione

Il parametro metodo di autenticazione specifica il metodo di autenticazione utilizzato per gli accessi.

Metodo di autenticazione	Descrizione
`cert`	Autenticazione del certificato SSL
`community`	Stringhe di comunità SNMP
`domain`	Autenticazione Active Directory
`nsswitch`	Autenticazione LDAP o NIS
`password`	Password
`publickey`	Autenticazione a chiave pubblica
`usm`	Modello di protezione utente SNMP

L'uso di NIS non è raccomandato a causa di punti deboli della sicurezza del protocollo.

A partire da ONTAP 9,3, l'autenticazione a due fattori concatenata è disponibile per gli account SSH locali `admin` utilizzando `publickey` e password come due metodi di autenticazione. Oltre al `-authentication-method` campo nel `security login` comando, è stato aggiunto un nuovo campo denominato `-second-authentication-method` . È possibile specificare la chiave pubblica o la password come `-authentication-method` o `-second-authentication-method`. Tuttavia, durante l'autenticazione SSH, l'ordine è sempre chiave pubblica con autenticazione parziale, seguita dal prompt della password per l'autenticazione completa.

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

A partire da ONTAP 9,4, `nsswitch` può essere utilizzato come secondo metodo di autenticazione con `publickey`.

A partire da ONTAP 9.12.1, FIDO2 può essere utilizzato anche per l'autenticazione SSH utilizzando un dispositivo di autenticazione hardware YubiKey o altri dispositivi compatibili con FIDO2.

A partire da ONTAP 9.13.1:

- `domain` gli account possono essere utilizzati come secondo metodo di autenticazione con `publickey`.
- Time-based one-time password (`totp`) è un codice di accesso temporaneo generato da un algoritmo che utilizza l'ora corrente come uno dei suoi fattori di autenticazione per il secondo metodo di autenticazione.
- La revoca della chiave pubblica è supportata con chiavi pubbliche SSH e certificati che verranno controllati per la scadenza/revoca durante SSH.

Per ulteriori informazioni sull'autenticazione a più fattori (MFA) per ONTAP System Manager, Active IQ Unified Manager e SSH, vedere "TR-4647: Autenticazione multifattore in ONTAP 9".

Account amministrativi predefiniti

L'account admin deve essere limitato perché al ruolo di amministratore è consentito l'accesso utilizzando tutte le applicazioni. L'account diag consente l'accesso alla shell del sistema e deve essere riservato solo al supporto tecnico per eseguire le attività di risoluzione dei problemi.

Esistono due account amministrativi predefiniti: `admin` E `diag`.

Gli account orfani sono un importante vettore di sicurezza che spesso porta a vulnerabilità, inclusa l'escalation dei privilegi. Si tratta di account non necessari e inutilizzati che rimangono nell'archivio degli account utente. Si tratta principalmente di account predefiniti che non sono mai stati utilizzati o per i quali le password non sono mai state aggiornate o modificate. Per risolvere questo problema, ONTAP supporta la rimozione e la ridenominazione degli account.

ONTAP non può rimuovere o rinominare gli account incorporati. Tuttavia, NetApp consiglia di bloccare gli account incorporati non necessari con il comando LOCK.

Sebbene gli account orfani siano un problema di protezione significativo, NetApp consiglia vivamente di

verificare l'effetto della rimozione degli account dall'archivio degli account locali.

Elenca account locali

Per elencare gli account locali, eseguire il `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.
```

Rimuovere l'account admin predefinito

L' `admin` account ha il ruolo di amministratore e può accedere utilizzando tutte le applicazioni.

Fasi

1. Creare un altro account a livello di amministratore.

   Per rimuovere completamente l'account predefinito `admin` , è necessario prima creare un altro account a livello di amministratore che utilizzi l' `console` applicazione di accesso.

   > Queste modifiche possono causare alcuni effetti indesiderati. Verificare sempre prima le nuove impostazioni che potrebbero influire sullo stato di sicurezza della soluzione in un cluster non di produzione.

   Esempio:

   ```
   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. Dopo aver creato il nuovo account admin, verificare l'accesso con l'account `NewAdmin` . Con l' `NewAdmin` accesso, configurare l'account in modo che disponga delle stesse applicazioni di accesso dell'account admin predefinito o precedente (ad esempio, `http`, , `ontapi` `service-processor`o `ssh`). Questa operazione garantisce il mantenimento del controllo dell'accesso.

   Esempio:

```
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. Dopo aver verificato tutte le funzioni, è possibile disattivare l'account admin per tutte le applicazioni prima di rimuoverlo da ONTAP. Questo passaggio serve come test finale per confermare che non vi siano funzioni persistenti che si basano sull'account admin precedente.

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

4. Per rimuovere l'account admin predefinito e tutte le voci, eseguire il seguente 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.
```

Impostare la password dell'account diagnostico (diag)

Con il sistema di archiviazione viene fornito un account diagnostico denominato `diag` . È possibile utilizzare l' `diag` account per eseguire operazioni di risoluzione dei problemi in `systemshell`. L' `diag` account è l'unico account che può essere utilizzato per accedere alla shell di sistema tramite il `diag` comando privilegiato `systemshell`.

> La shell di sistema e l'account associato `diag` sono destinati a scopi diagnostici di basso livello. Il loro accesso richiede il livello di privilegio diagnostico ed è riservato solo per essere utilizzato con la guida del supporto tecnico per eseguire le attività di risoluzione dei problemi. Né il `diag` conto né il `systemshell` sono destinati a fini amministrativi generali.

Prima di iniziare

Prima di accedere a `systemshell`, è necessario impostare la `diag` password dell'account utilizzando il `security login password` comando . È necessario utilizzare i principi della password complessa e modificarla `diag` a intervalli regolari.

Fasi

1. Per impostare la `diag` password dell'utente dell'account:

```
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%
```

Verifica multi-admin

A partire da ONTAP 9.11.1, è possibile utilizzare la verifica multi-admin (MAV) per consentire l'esecuzione di determinate operazioni, come l'eliminazione di volumi o copie Snapshot, solo dopo le approvazioni da parte degli amministratori designati. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati.

La configurazione di MAV è composta dai seguenti elementi:

- "Creazione di uno o più gruppi di approvazione dell'amministratore."
- "Abilitazione della funzionalità di verifica multi-admin."
- "Aggiunta o modifica di regole."

Dopo la configurazione iniziale, solo gli amministratori di un gruppo di approvazione MAV (amministratori MAV) possono modificare questi elementi.

Quando MAV è abilitato, il completamento di ogni operazione protetta richiede tre fasi:

1. Quando un utente avvia l'operazione, a. "la richiesta viene generata."
2. Prima di poter essere eseguito, il numero richiesto di "Gli amministratori MAV devono approvare."
3. Dopo l'approvazione, l'utente completa l'operazione.

MAV non è destinato all'uso con volumi o flussi di lavoro che implicano un'automazione intensiva, poiché ogni attività automatizzata richiede l'approvazione prima che l'operazione possa essere completata. Se si desidera utilizzare insieme automazione e MAV, NetApp consiglia di utilizzare query per operazioni MAV specifiche. Ad esempio, è possibile applicare `volume delete` le regole MAV solo ai volumi in cui l'automazione non è coinvolta ed è possibile designare tali volumi con un particolare schema di denominazione.

Per informazioni più dettagliate su MAV, vedere "Documentazione di verifica multi-admin ONTAP".

Blocco della copia snapshot

Il blocco delle copie Snapshot è una funzionalità di SnapLock in cui le copie Snapshot vengono rese indelebili manualmente o automaticamente, con un periodo di conservazione nella policy delle Snapshot dei volumi. Lo scopo del blocco delle copie Snapshot è impedire agli amministratori fuori controllo o non attendibili di eliminare le Snapshot su un sistema ONTAP primario o secondario.

Il blocco della copia snapshot è stato introdotto in ONTAP 9.12.1. Il blocco delle copie snapshot è anche noto come blocco delle snapshot a prova di manomissione. Sebbene richieda la licenza SnapLock e l'inizializzazione del clock di conformità, il blocco della copia Snapshot non è correlato alla conformità SnapLock o a SnapLock Enterprise. Non esiste un amministratore dello storage fidato, come con SnapLock Enterprise e non protegge l'infrastruttura di storage fisico sottostante, come con la conformità di SnapLock. Si tratta di un miglioramento rispetto all'esecuzione di copie Snapshot su un sistema secondario. È possibile ottenere un rapido recovery di Snapshot bloccati sui sistemi primari per ripristinare i volumi corrotti dal ransomware.

Per ulteriori informazioni sul blocco della copia istantanea, vedere "Documentazione ONTAP".

Impostare l'accesso API basato su certificati

Invece dell'autenticazione tramite ID utente e password per l'accesso API REST o API SDK di gestione NetApp a ONTAP, è necessario utilizzare l'autenticazione basata su certificati.

> In alternativa all'autenticazione basata su certificati per le API REST, utilizzare "Autenticazione basata su token OAuth 2,0".)

È possibile generare e installare un certificato autofirmato su ONTAP come descritto in questi passaggi.

Fasi

1. Utilizzando OpenSSL, generare un certificato eseguendo il seguente 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'
```

   Questo comando genera un certificato pubblico denominato e una chiave privata denominata `test.pem key.out`. Il nome comune, CN, corrisponde all'ID utente ONTAP.

2. Installare il contenuto del certificato pubblico in formato PEM (Privacy Enhanced Mail) in ONTAP eseguendo il comando seguente e incollando il contenuto del certificato quando richiesto:

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

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

3. Abilitare ONTAP per consentire l'accesso client tramite SSL e definire l'ID utente per l'accesso 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
```

Nell'esempio seguente, l'ID utente `cert_user` è ora abilitato per utilizzare l'accesso API autenticato con certificato. Un semplice script Python SDK di gestione che utilizza `cert_user` per visualizzare la versione ONTAP appare come segue:

```
#!/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)
```

L'output dello script visualizza la versione di ONTAP.

```
./version.py

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

4. Per eseguire l'autenticazione basata su certificati con l'API REST ONTAP, attenersi alla seguente procedura:
   a. In ONTAP, definire l'ID utente per l'accesso http:

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

b. Sul client Linux, eseguire il seguente comando che produce la versione di ONTAP come output:

```
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"
        }
    }
}
```

Ulteriori informazioni

- "Autenticazione basata su certificati con NetApp Manageability SDK per ONTAP".

Autenticazione basata su token ONTAP OAuth 2,0 per API REST

In alternativa all'autenticazione basata su certificati, è possibile utilizzare l'autenticazione basata su token OAuth 2,0 per l'API REST.

A partire da ONTAP 9.14.1, puoi controllare l'accesso ai tuoi cluster ONTAP utilizzando il framework Open Authorization (OAuth 2,0). Puoi configurare questa funzionalità utilizzando qualsiasi interfaccia amministrativa di ONTAP, inclusi l'interfaccia a riga di comando di ONTAP, System Manager e l'API REST. Tuttavia, le decisioni relative all'autorizzazione e al controllo dell'accesso OAuth 2,0 possono essere applicate solo quando un client accede a ONTAP utilizzando l'API REST.

I token OAuth 2,0 sostituiscono le password per l'autenticazione dell'account utente.

Per ulteriori informazioni sull'utilizzo di OAuth 2,0, vedere "Documentazione ONTAP sull'autenticazione e l'autorizzazione utilizzando OAuth 2,0".

Parametri di accesso e password

Una posizione di sicurezza efficace rispetta le policy, le linee guida e qualsiasi governance o standard dell'organizzazione stabiliti. Esempi di questi requisiti includono la durata del nome utente, i requisiti di lunghezza della password, i requisiti dei caratteri e la memorizzazione di tali account. La soluzione ONTAP fornisce funzionalità e caratteristiche per affrontare questi costrutti di protezione.

Nuove funzioni dell'account locale

Per supportare i criteri, le linee guida o gli standard degli account utente di un'organizzazione, inclusa la governance, in ONTAP sono supportate le seguenti funzionalità:

- Configurazione dei criteri delle password per applicare un numero minimo di cifre, caratteri minuscoli o caratteri maiuscoli
- Richiede un ritardo dopo un tentativo di accesso non riuscito
- Definizione del limite di inattività dell'account
- Scadenza di un account utente
- Visualizzazione di un messaggio di avviso di scadenza della password
- Notifica di un accesso non valido

Le impostazioni configurabili vengono gestite utilizzando il comando di modifica della configurazione del ruolo di accesso di sicurezza.

Supporto SHA-512

Per migliorare la sicurezza delle password, ONTAP 9 supporta la funzione hash password SHA-2 e imposta il valore predefinito per l'utilizzo di SHA-512 per l'hashing di password appena create o modificate. Gli operatori e gli amministratori possono anche scadere o bloccare gli account in base alle necessità.

Gli account utente ONTAP 9 preesistenti con password non modificate continuano a utilizzare la funzione hash MD5 dopo l'aggiornamento a ONTAP 9,0 o versione successiva. Tuttavia, NetApp consiglia vivamente che questi account utente migrino alla soluzione SHA-512 più sicura, facendo in modo che gli utenti modifichino le proprie password.

La funzionalità hash password consente di eseguire le seguenti operazioni:

- Visualizza gli account utente che corrispondono alla funzione hash specificata:

```
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
```

- Scade gli account che utilizzano una funzione hash specificata (ad esempio, MD5), che obbliga gli utenti a modificare le proprie password al successivo accesso:

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

- Bloccare gli account con password che utilizzano la funzione hash specificata.

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

La funzione hash password non è nota per l'utente interno `autosupport` nella SVM amministrativa del cluster. Questo problema è superficiale. La funzione hash è sconosciuta perché l'utente interno non dispone di una password configurata per impostazione predefinita.

  - Per visualizzare la funzione hash password per l' `autosupport` utente, eseguire i seguenti comandi:

```
::> 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
```

  - Per impostare la funzione hash password (default: SHA512), eseguire il seguente comando:

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

Non importa a quale password è impostata.

```
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
```

Parametri password

La soluzione ONTAP supporta i parametri delle password che soddisfano e supportano i requisiti e le linee guida dei criteri organizzativi.

Attributo	Descrizione	Predefinito	Raggio d'azione
`username-minlength`	Lunghezza minima del nome utente richiesta	3	3-16
`username-alphanum`	Nome utente alfanumerico	disattivato	Attivato/disattivato
`passwd-minlength`	Lunghezza minima della password richiesta	8	3-64
`passwd-alphanum`	Password alfanumerica	attivato	Attivato/disattivato
`passwd-min-special-chars`	Numero minimo di caratteri speciali richiesti nella password	0	0-64
`passwd-expiry-time`	Ora di scadenza della password (in giorni)	Illimitato, il che significa che le password non scadono mai	0-illimitato 0 == scade ora
`require-initial-passwd-update`	Richiedi l'aggiornamento iniziale della password al primo accesso	Disattivato	Attivato/disattivato Modifiche consentite tramite console o SSH
`max-failed-login-attempts`	Numero massimo di tentativi non riusciti	0, non bloccare l'account	-
`lockout-duration`	Periodo di blocco massimo (in giorni)	L'impostazione predefinita è 0, ovvero l'account è bloccato per un giorno	-

Attributo	Descrizione	Predefinito	Raggio d'azione
`disallowed-reuse`	Non consentire le ultime N password	6	Il valore minimo è 6
`change-delay`	Ritardo tra le modifiche della password (in giorni)	0	-
`delay-after-failed-login`	Ritardo dopo ogni tentativo di accesso non riuscito (in secondi)	4	-
`passwd-min-lowercase-chars`	Numero minimo di caratteri alfabetici minuscoli richiesti nella password	0, che non richiede caratteri minuscoli	0-64
`passwd-min-uppercase-chars`	È richiesto un numero minimo di caratteri alfabetici maiuscoli	0, che non richiede caratteri maiuscoli	0-64
`passwd-min-digits`	Numero minimo di cifre richiesto nella password	0, che non richiede cifre	0-64
`passwd-expiry-warn-time`	Visualizza messaggio di avviso prima della scadenza della password (in giorni)	Illimitato, il che significa non avvisare mai della scadenza della password	0, che significa avvisare l'utente circa la scadenza della password ad ogni accesso riuscito
`account-expiry-time`	L'account scade tra N giorni	Illimitato, il che significa che i conti non scadono mai	Il tempo di scadenza dell'account deve essere maggiore del limite di inattività dell'account
`account-inactive-limit`	Durata massima di inattività prima della scadenza dell'account (in giorni)	Illimitato, il che significa che gli account inattivi non scadono mai	Il limite di inattività dell'account deve essere inferiore al tempo di scadenza dell'account

Esempio

```
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 partire dal 9.14.1, le password sono caratterizzate da una maggiore complessità e da regole di blocco. Questo vale solo per le nuove installazioni di ONTAP.

Informazioni sul copyright

Informazioni sul marchio commerciale