Linee guida per la protezione avanzata di ONTAP

ONTAP 9

NetApp
July 19, 2024

Sommario

Linee guida per la protezione avanzata di ONTAP

Panoramica sulla protezione avanzata di ONTAP

ONTAP offre una serie di controlli che consentono di rafforzare il sistema operativo per lo storage ONTAP, il software per la gestione dei dati leader del settore. Utilizzare le linee guida e le impostazioni di configurazione di ONTAP per aiutare l'organizzazione a soddisfare gli obiettivi di protezione prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

L'evoluzione del panorama delle minacce attuali presenta un'organizzazione che si trova a dover affrontare sfide uniche per la protezione delle sue risorse più preziose: Dati e informazioni. Le minacce e le vulnerabilità avanzate e dinamiche che ci troviamo ad affrontare sono sempre più sofisticate. Oltre a un aumento dell'efficacia delle tecniche di offuscamento e ricognizione da parte di potenziali intrusi, i responsabili di sistema devono affrontare in modo proattivo la sicurezza dei dati e delle informazioni.

A partire da luglio 2024, il contenuto dei report tecnici precedentemente pubblicati come PDF è stato integrato nella documentazione del prodotto ONTAP. La documentazione sulla protezione di ONTAP contiene ora il contenuto di *TR-4569: Guida alla protezione avanzata per ONTAP*.

Convalida dell'immagine ONTAP

ONTAP fornisce meccanismi per garantire che l'immagine ONTAP sia valida al momento dell'aggiornamento e dell'avvio.

Convalida dell'immagine di aggiornamento

La firma del codice consente di verificare che le immagini ONTAP installate tramite aggiornamenti delle immagini senza interruzioni o aggiornamenti automatici delle immagini, CLI o API ONTAP siano prodotte in modo autentico da NetApp e non siano state manomesse. La convalida dell'immagine di aggiornamento è stata introdotta in ONTAP 9,3.

Questa funzione è un miglioramento della protezione senza tocco per l'aggiornamento o la riversione di ONTAP. Non ci si aspetta che l'utente faccia nulla di diverso, tranne che per la verifica opzionale della firma di livello superiore "image.tgz".

Convalida dell'immagine al momento dell'avvio

A partire da ONTAP 9,4, l'avvio protetto UEFI (Unified Extensible firmware Interface) è abilitato per i sistemi NetApp AFF A800, AFF A220, FAS2750 e FAS2720 e per i sistemi di nuova generazione successivi che utilizzano il BIOS UEFI.

Durante l'accensione, il bootloader convalida il database whitelist delle chiavi di avvio protette con la firma associata a ciascun modulo caricato. Dopo la convalida e il caricamento di ciascun modulo, il processo di avvio continua con l'inizializzazione di ONTAP. Se la convalida della firma non riesce per qualsiasi modulo, il sistema viene riavviato.

Questi elementi si applicano alle immagini ONTAP e al BIOS della piattaforma.

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.

Metodi di amministrazione del sistema

Questi sono parametri importanti per rafforzare l'amministrazione del sistema ONTAP.

Accesso a riga di comando

Stabilire un accesso sicuro ai sistemi è fondamentale per mantenere una soluzione sicura. Le opzioni di accesso alla riga di comando più comuni sono SSH, Telnet e RSH. Di questi, SSH è la Best practice più sicura e standard del settore per l'accesso remoto a riga di comando. NetApp consiglia vivamente di utilizzare SSH per l'accesso a riga di comando alla soluzione ONTAP.

Configurazioni SSH

Il `security ssh show` comando mostra le configurazioni degli algoritmi di scambio chiavi SSH, cifrari e algoritmi MAC per il cluster e le SVM. Il metodo di scambio della chiave utilizza questi algoritmi e cifrari per specificare il modo in cui le chiavi di sessione monouso vengono generate per la crittografia e l'autenticazione e come avviene l'autenticazione del server.

```
cluster1::> security ssh show

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

Banner di accesso

I banner di accesso consentono alle organizzazioni di presentare agli operatori, agli amministratori e persino ai malintenzionati i termini e le condizioni di corretto utilizzo, indicando chi ha il permesso di accedere al sistema. Questo approccio è utile per stabilire le aspettative per l'accesso e l'utilizzo del sistema. Il `security login banner modify` comando modifica il banner di accesso. Il banner di accesso viene visualizzato poco prima della fase di autenticazione durante il processo di login del dispositivo SSH e della console. Il testo del banner deve essere tra virgolette doppie (" "), come illustrato nell'esempio seguente.

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

Parametri banner di accesso

Parametro	Descrizione
`vserver`	Utilizzare questo parametro per specificare la SVM con il banner modificato. Utilizza il nome della SVM di amministrazione cluster per modificare il messaggio a livello di cluster. Il messaggio a livello di cluster è utilizzato come impostazione predefinita per le SVM di dati che non hanno definito un messaggio.

Parametro	Descrizione
`message`	Questo parametro opzionale può essere utilizzato per specificare un messaggio banner di accesso. Se il cluster ha un set di messaggi di login banner, anche il banner di login al cluster viene utilizzato da tutte le SVM di dati. L'impostazione del banner di accesso di una SVM dati ha la priorità sulla visualizzazione del banner di accesso al cluster. Per reimpostare il banner di accesso di una SVM dati e utilizzare il banner di accesso del cluster, utilizza questo parametro con il valore "-". Se si utilizza questo parametro, il banner di accesso non può contenere nuove righe (note anche come estremità delle righe [EOLS] o interruzioni di riga). Per immettere un messaggio banner di accesso con nuove righe, non specificare alcun parametro. Viene richiesto di immettere il messaggio in modo interattivo. I messaggi immessi in modo interattivo possono contenere nuove righe. I caratteri non ASCII devono utilizzare Unicode UTF-8.
`uri`	`(ftp
http):///(hostname	IPv4` Utilizzare questo parametro per specificare l'URI da cui viene scaricato il banner di accesso. La lunghezza del messaggio non deve superare i 2048 byte. I caratteri non ASCII devono essere forniti come Unicode UTF-8.

Messaggio del giorno

Il `security login motd modify` comando aggiorna il messaggio del giorno (MOTD).

Ci sono due categorie di MOTD: Il MOTD a livello di cluster e il MOTD a livello di SVM dati. Un utente che accede alla shell di un cluster di dati della SVM potrebbe visualizzare due messaggi: Il MOTD a livello di cluster seguito dal MOTD a livello di SVM per tale SVM.

L'amministratore del cluster può attivare o disattivare il MOTD a livello di cluster su ciascuna SVM singolarmente, se necessario. Se l'amministratore del cluster disabilita il MOTD a livello di cluster per una SVM, un utente che accede alla SVM non visualizza il messaggio a livello di cluster. Solo un amministratore del cluster può attivare o disattivare il messaggio a livello di cluster.

Parametro MOTD	Descrizione
Server virtuale	Utilizzare questo parametro per specificare la SVM per la quale viene modificato il MOTD. Utilizza il nome della SVM di amministrazione cluster per modificare il messaggio a livello di cluster.

Parametro MOTD	Descrizione
messaggio	Questo parametro opzionale può essere utilizzato per specificare un messaggio. Se si utilizza questo parametro, MOTD non può contenere nuove righe. Se non si specifica alcun parametro diverso dal `-vserver` parametro, viene richiesto di immettere il messaggio in modo interattivo. I messaggi immessi in modo interattivo possono contenere nuove righe. I caratteri non ASCII devono essere forniti come Unicode UTF-8. Il messaggio può contenere contenuti generati dinamicamente utilizzando le seguenti sequenze di escape: • `\\` - Un singolo carattere di gioco • `\b` - Nessun output (supportato solo per la compatibilità con Linux) • `\C` - Nome cluster • `\d` - La data corrente impostata sul nodo di accesso • `\t` - Ora corrente impostata sul nodo di accesso • `\I` - Indirizzo IP LIF in entrata (stampa la console per `console` l'accesso) • `\l` - Nome dispositivo di accesso (stampa la console per un `console` login) • `\L` - Ultimo accesso per l'utente su qualsiasi nodo nel cluster • `\m` - Architettura della macchina • `\n` - Nome SVM del nodo o dei dati • `\N` - Nome dell'utente che effettua l'accesso • `\o` - Uguale a \O. Fornito per la compatibilità con Linux. • `\O` - Nome dominio DNS del nodo. Si noti che l'output dipende dalla configurazione di rete e potrebbe essere vuoto. • `\r` - Numero di versione del software • `\s` - Nome del sistema operativo • `\u` - Numero di sessioni clustershell attive sul nodo locale. Per l'amministratore del cluster: Tutti gli utenti di clustershell. Per l'amministratore della SVM dei dati: Solo sessioni attive per la SVM dei dati. • `\U` - Uguale a `\u`, ma ha `user` o `users` aggiunto • `\v` - Stringa della versione del cluster effettiva • `\W` - Sessioni attive nel cluster per l'accesso dell'utente (`who`)

Per ulteriori informazioni sulla configurazione del messaggio del giorno in ONTAP, vedere "Documentazione ONTAP su messaggio del giorno".

Timeout sessione CLI

Il timeout predefinito della sessione CLI è di 30 minuti. Il timeout è importante per evitare sessioni stalose e piggybacking di sessione.

Utilizzare il `system timeout show` comando per visualizzare il timeout della sessione CLI corrente. Per

impostare il valore di timeout, utilizzare `system timeout modify -timeout <minutes>` il comando.

Accesso Web con Gestione di sistema di NetApp ONTAP

Se un amministratore di ONTAP preferisce utilizzare un'interfaccia grafica anziché l'interfaccia CLI per l'accesso e la gestione di un cluster, usa NetApp ONTAP System Manager. È incluso in ONTAP come servizio Web, attivato per impostazione predefinita e accessibile tramite un browser. Puntare il browser al nome host se si utilizza DNS o l'indirizzo IPv4 o IPv6 tramite `https://cluster-management-LIF`.

Se il cluster utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile confermare il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) sul cluster per l'autenticazione del server.

A partire da ONTAP 9,3, l'autenticazione SAML (Security Assertion Markup Language) è un'opzione per Gestione di sistema di ONTAP.

Autenticazione SAML per Gestione di sistema ONTAP

SAML 2,0 è uno standard di settore ampiamente adottato che consente a qualsiasi Identity provider (IdP) conforme a SAML di terze parti di eseguire MFA utilizzando meccanismi esclusivi dell'IdP dell'azienda e come origine del single sign-on (SSO).

Nella specifica SAML sono definiti tre ruoli: Principal, IdP e Service Provider. Nell'implementazione di ONTAP, un'entità è rappresentata dall'amministratore del cluster che accede a ONTAP tramite ONTAP System Manager o NetApp Active IQ Unified Manager. L'IdP è un software IdP di terze parti. A partire da ONTAP 9,3, Microsoft Active Directory Federated Services (ADFS) e l'IdP Shibboleth open-source sono IDP supportati. A partire da ONTAP 9.12.1, Cisco DUO è un IdP supportato. Il provider di servizi è la funzionalità SAML integrata in ONTAP utilizzata dal gestore di sistema di ONTAP o dall'applicazione Web di Active IQ Unified Manager.

A differenza del processo di configurazione a due fattori SSH, dopo l'attivazione dell'autenticazione SAML, l'accesso al Gestore di sistema ONTAP o al processore di servizio ONTAP richiede a tutti gli amministratori esistenti di eseguire l'autenticazione tramite l'IdP SAML. Non è necessario apportare modifiche agli account utente cluster. Quando l'autenticazione SAML è attivata, viene aggiunto un nuovo metodo di autenticazione di `saml` agli utenti esistenti con ruoli di amministratore per le `http` applicazioni e `ontapi` .

Dopo l'attivazione dell'autenticazione SAML, è necessario definire altri nuovi account che richiedono l'accesso IdP SAML in ONTAP con il ruolo di amministratore e il metodo di autenticazione saml per le `http` applicazioni e `ontapi` . Se a un certo punto l'autenticazione SAML è disabilitata, questi nuovi account richiedono che il `password` metodo di autenticazione sia definito con il ruolo di amministratore per `http` le applicazioni e `ontapi` l'aggiunta dell'applicazione console per l'autenticazione ONTAP locale a Gestione sistema ONTAP.

Dopo l'abilitazione dell'IdP SAML, l'IdP esegue l'autenticazione per l'accesso a ONTAP System Manager utilizzando metodi disponibili per l'IdP, come Lightweight Directory Access Protocol (LDAP), Active Directory (ad), Kerberos, password e così via. I metodi disponibili sono esclusivi dell'IdP. È importante che gli account configurati in ONTAP dispongano di ID utente associati ai metodi di autenticazione IdP.

Gli IDP convalidati da NetApp sono Microsoft ADFS, Cisco DUO e l'open-source Shibboleth IdP.

A partire da ONTAP 9.14.1, è possibile utilizzare Cisco DUO come secondo fattore di autenticazione per SSH.

Per ulteriori informazioni su MFA per Gestore di sistema ONTAP, Active IQ Unified Manager e SSH, vedere "TR-4647: Autenticazione multifattore in ONTAP 9".

Informazioni su System Manager di ONTAP

A partire da ONTAP 9.11.1, ONTAP System Manager fornisce informazioni utili agli amministratori dei cluster per ottimizzare i task di tutti i giorni. Le informazioni sulla sicurezza si basano sulle raccomandazioni contenute in questo report tecnico.

Informazioni sulla sicurezza	Determinazione
Telnet è attivato	NetApp consiglia Secure Shell (SSH) per un accesso remoto sicuro.
Remote Shell (RSH) è attivato	NetApp consiglia SSH per un accesso remoto sicuro.
AutoSupport sta utilizzando un protocollo non sicuro	AutoSupport non è configurato per l'invio tramite xref:./ontap-hardening/HTTPS.
Il banner di accesso non è configurato sul cluster a livello di cluster	Avvertenza se il banner di accesso non è configurato per il cluster.
SSH sta utilizzando cifrari non sicuri	Avvertimento se SSH utilizza cifrari non sicuri.
Sono stati configurati troppi server NTP	Avvertenza se il numero di server NTP configurati è inferiore a tre.
Utente amministratore predefinito non bloccato	Quando non si utilizzano account amministrativi predefiniti (admin o diag) per accedere a System Manager e questi account non sono bloccati, si consiglia di bloccarli.
Difesa da ransomware: I volumi non dispongono di policy Snapshot	Nessuna policy Snapshot adeguata è collegata a uno o più volumi.
Difesa dal ransomware — disattiva l'eliminazione automatica delle snapshot	L'eliminazione automatica dello snapshot è impostata per uno o più volumi.
I volumi non vengono monitorati alla ricerca di attacchi ransomware	La protezione autonoma da ransomware è supportata su diversi volumi, ma non ancora configurata.
Le SVM non sono configurate per la protezione autonoma da ransomware	La protezione autonoma da ransomware è supportata su diverse SVM, ma non ancora configurata.
FPolicy nativo non è configurato	FPolicy non è impostato per SVM NAS.
Attiva la modalità attiva di protezione autonoma dal ransomware	Diversi volumi hanno completato la modalità di apprendimento ed è possibile attivare la modalità attiva
La compliance FIPS globale 140-2 è disattivata	La conformità FIPS 140-2 globale non è abilitata.
Il cluster non è configurato per le notifiche	E-mail, webhook o traphost SNMP non sono configurati per ricevere notifiche.

Per ulteriori informazioni su Gestione di sistema di ONTAP, vedere "Documentazione di ONTAP System Manager".

Protezione autonoma dal ransomware di ONTAP

Per integrare gli analytics sul comportamento degli utenti per la sicurezza del workload di storage, la protezione autonoma da ransomware di ONTAP analizza i carichi di lavoro dei volumi e l'entropia per rilevare il ransomware ed effettua una Snapshot e informa

l'amministratore quando si sospetta un attacco.

Oltre al rilevamento e alla prevenzione del ransomware che utilizzano l'analisi comportamentale esterna degli utenti FPolicy (UBA) con NetApp Cloud Insights / Cloud Secure e l'ecosistema di partner NetApp FPolicy, ONTAP 9.10.1 introduce una protezione autonoma dal ransomware. La protezione autonoma dal ransomware ONTAP utilizza una funzionalità integrata di machine learning (ML) on-box che analizza l'attività del carico di lavoro dei volumi più l'entropia dei dati per rilevare automaticamente il ransomware. Esegue il monitoraggio di attività diverse da quelle di UBA, in modo da rilevare attacchi che UBA non ha.

Per informazioni più dettagliate su questa funzionalità, vedere "TR-4572: La soluzione NetApp per il ransomware" o "Documentazione sulla protezione autonoma dal ransomware di ONTAP".

Controllo del sistema amministrativo di storage

Garantire l'integrità del controllo degli eventi trasferendo gli eventi ONTAP in un server syslog remoto. Questo server può essere un sistema di gestione di eventi di informazioni sulla sicurezza come Splunk.

Inviare syslog

Le informazioni di log e di audit sono preziose per un'organizzazione dal punto di vista del supporto e della disponibilità. Inoltre, le informazioni e i dettagli contenuti nei log (syslog), nei report e nei risultati di revisione sono generalmente di natura sensibile. Per mantenere i controlli e la posizione di sicurezza, è fondamentale che le organizzazioni gestiscano i dati di log e di revisione in modo sicuro.

L'offload delle informazioni syslog è necessario per limitare l'ambito o l'impatto di una violazione a un singolo sistema o soluzione. Pertanto, NetApp consiglia di trasferire in modo sicuro le informazioni syslog in una posizione di storage o conservazione sicura.

Creare una destinazione di inoltro dei log

Utilizzare il `cluster log-forwarding create` comando per creare destinazioni di inoltro dei log per la registrazione remota.

Parametri

Utilizzare i seguenti parametri per configurare il `cluster log-forwarding create` comando:

- **Host di destinazione.** Questo nome è il nome host o l'indirizzo IPv4 o IPv6 del server a cui inoltrare i registri.

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

- **Porta di destinazione.** Questa è la porta sulla quale il server di destinazione ascolta.

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

- **Protocollo di inoltro log.** Questo protocollo viene utilizzato per inviare messaggi alla destinazione.

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

Il protocollo di inoltro dei log può utilizzare uno dei seguenti valori:

- `udp-unencrypted`. User Datagram Protocol senza protezione.
- `tcp-unencrypted`. TCP senza protezione.
- `tcp-encrypted`. TCP con TLS (Transport Layer Security).

- **Verificare l'identità del server di destinazione.** Quando questo parametro è impostato su true, l'identità della destinazione di inoltro dei log viene verificata convalidandone il certificato. Il valore può essere impostato su vero solo quando il `tcpencrypted` valore è selezionato nel campo protocollo.

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

- **Funzione Syslog.** Questo valore è la funzione syslog da utilizzare per i registri inoltrati.

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

- **Saltare il test di connettività.** In genere, il `cluster log-forwarding create` comando verifica che la destinazione sia raggiungibile inviando un ping ICMP (Internet Control message Protocol) e non riesce se non è raggiungibile. L'impostazione di questo valore `true` consente di ignorare il controllo ping in modo da poter configurare la destinazione quando non è raggiungibile.

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

NetApp consiglia di utilizzare il `cluster log-forwarding` comando per forzare la connessione su un `-tcp-encrypted` tipo.

Notifica degli eventi

Proteggere le informazioni e i dati che lasciano un sistema è fondamentale per mantenere e gestire la posizione di sicurezza del sistema. Gli eventi generati dalla soluzione ONTAP forniscono una vasta gamma di informazioni su ciò che la soluzione incontra, le informazioni elaborate e altro ancora. La vitalità di questi dati evidenzia la necessità di gestirli e migrarli in modo sicuro.

Il `event notification create` comando invia una nuova notifica di una serie di eventi definiti da un filtro eventi a una o più destinazioni di notifica. Gli esempi seguenti illustrano la configurazione della notifica degli eventi e il `event notification show` comando, che visualizza i filtri e le destinazioni di notifica degli eventi configurati.

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

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

Crittografia dello storage

Per proteggere i dati sensibili in caso di furto, restituzione o riutilizzo di un disco, utilizzare la crittografia storage NetApp basata su hardware o la crittografia dei volumi NetApp basata su software/crittografia aggregata NetApp. Entrambi i meccanismi sono validati FIPS-140-2 e quando si utilizzano meccanismi basati su hardware con meccanismi basati su software, la soluzione è idonea per il programma Commercial Solutions for Classified (CSFC). Consente una protezione di sicurezza avanzata per dati segreti e top-secret a riposo sia a livello hardware che software.

La crittografia dei dati inattivi è importante per proteggere i dati sensibili in caso di furto, restituzione o riordinamento di un disco.

ONTAP 9 dispone di tre soluzioni di crittografia dei dati a riposo conformi a Federal Information Processing Standard (FIPS) 140-2:

- Crittografia storage NetApp (NSE) è una soluzione hardware che utilizza dischi con crittografia automatica.
- NetApp Volume Encryption (NVE) è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco dove è abilitato con una chiave univoca per ciascun volume.
- Crittografia degli aggregati NetApp (NAE) è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco con chiavi univoche per ciascun aggregato.

NSe, NVE e NAE possono utilizzare la gestione delle chiavi esterna o il gestore delle chiavi integrato (OKM). L'utilizzo di NSE, NVE e NAE non influisce sulle funzionalità di efficienza dello storage di ONTAP. Tuttavia, i volumi NVE sono esclusi dalla deduplica aggregata. I volumi NAE partecipano e traggono vantaggio dalla deduplica aggregata.

OKM offre una soluzione per la crittografia autonoma dei dati a riposo con NSE, NVE o NAE.

NVE, NAE e OKM utilizzano ONTAP CryptoMod. CryptoMod è elencato nell'elenco dei moduli validati di CMVP FIPS 140-2. Vedere "FIPS 140-2 certificato n. 4144".

Per avviare la configurazione OKM, utilizzare il `security key-manager onboard enable` comando. Per configurare manager delle chiavi esterni KMIP (Key Management Interoperability Protocol), utilizza il `security key-manager external enable` comando. A partire da ONTAP 9,6, la multi-tenancy è supportata per i gestori delle chiavi esterne. Utilizza il `-vserver <vserver name>` parametro per abilitare la gestione esterna delle chiavi per una SVM specifica. Prima della versione 9,6, il `security key-manager setup` comando era stato utilizzato per configurare sia il gestore delle chiavi OKM che quello esterno. Per la gestione della chiave integrata, questa configurazione guida l'operatore o l'amministratore attraverso l'impostazione della passphrase e parametri aggiuntivi per la configurazione di OKM.

Una parte della configurazione viene fornita nel seguente esempio:

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

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

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

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

A partire da ONTAP 9,4, è possibile utilizzare `-enable-cc-mode` l'opzione true con `security key-manager setup` per richiedere agli utenti di immettere la passphrase dopo un riavvio. Per ONTAP 9,6 e versioni successive, la sintassi del comando è `security key-manager onboard enable -cc-mode -enabled yes`.

A partire da ONTAP 9,4, puoi utilizzare la `secure-purge` funzionalità con privilegio avanzato per "scrub" dei dati senza interruzioni su volumi abilitati per NVE. Lo scrubbing dei dati su un volume crittografato garantisce che non possano essere recuperati dal supporto fisico. Il seguente comando rimuove in modo sicuro i file eliminati su vol1 in SVM VS1:

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

A partire da ONTAP 9,7, NAE e NVE sono abilitate per impostazione predefinita se è in uso la licenza VE, sono configurati gestore delle chiavi OKM o esterni e NSE non viene utilizzato. I volumi NAE sono creati per impostazione predefinita sugli aggregati NAE e i volumi NVE sono creati per impostazione predefinita su aggregati non NAE. È possibile ignorare questo comando immettendo il seguente comando:

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

A partire da ONTAP 9,6, è possibile utilizzare un ambito SVM per configurare la gestione delle chiavi esterne per una SVM dati nel cluster. Si tratta della soluzione ottimale per gli ambienti multitenant in cui ogni tenant utilizza una SVM (o un set di SVM) differente per fornire i dati. Solo l'amministratore SVM di un determinato tenant ha accesso alle chiavi del tenant. Per ulteriori informazioni, consultare la "Attiva la gestione esterna delle chiavi in ONTAP 9,6 e versioni successive" documentazione di ONTAP.

A partire da ONTAP 9.11.1, puoi configurare la connettività ai server per la gestione delle chiavi esterne in cluster designando i server chiavi primari e secondari su una SVM. Per ulteriori informazioni, consultare la "configurare i server chiavi esterne in cluster" documentazione di ONTAP.

A partire da ONTAP 9.13.1, è possibile configurare i server di gestione chiavi esterni in Gestione di sistema. Per ulteriori informazioni, consultare la "Gestire i key manager esterni" documentazione di ONTAP.

Crittografia replica dei dati

Per integrare la crittografia dei dati inattivi, puoi crittografare il traffico di replica dei dati ONTAP tra i cluster utilizzando TLS 1,2 con una chiave pre-condivisa per SnapMirror, SnapVault o FlexCache.

Durante la replica dei dati per il disaster recovery, il caching o il backup, è necessario proteggerli durante il trasporto via cavo da un cluster ONTAP a un altro. In questo modo si previene un attacco malware man-in-the-middle contro i dati sensibili mentre sono in movimento.

A partire da ONTAP 9,6, la crittografia di peering dei cluster fornisce il supporto per la crittografia TLS 1,2 AES-256 GCM per funzioni di replica dei dati ONTAP come SnapMirror, SnapVault e FlexCache. La crittografia viene impostata tramite una chiave precondivisa (PSK) tra due peer del cluster.

I clienti che utilizzano tecnologie come NSE, NVE e NAE per proteggere i dati a riposo possono anche utilizzare la crittografia dei dati end-to-end effettuando l'aggiornamento a ONTAP 9,6 o versioni successive per utilizzare la crittografia di peering del cluster.

Il peering dei cluster crittografa tutti i dati tra peer cluster. Ad esempio, quando si utilizza SnapMirror, tutte le informazioni di peering e tutte le relazioni SnapMirror tra il peer del cluster di origine e di destinazione vengono crittografate. Non è possibile inviare dati non crittografati tra peer cluster con la crittografia di peering dei cluster abilitata.

A partire da ONTAP 9,6, la crittografia delle nuove relazioni cluster-peer è abilitata per impostazione predefinita. Per abilitare la crittografia delle relazioni di cluster peer create prima di ONTAP 9,6, è necessario aggiornare il cluster di origine e destinazione a 9,6. Inoltre, per utilizzare la crittografia di peering dei cluster, è necessario `cluster peer modify` utilizzare il comando per modificare i peer dei cluster di origine e di destinazione.

È possibile convertire una relazione peer esistente per utilizzare la crittografia di peering dei cluster in ONTAP 9,6, come illustrato nell'esempio seguente:

```
On the Destination Cluster Peer

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

When prompted enter a passphrase.

On the Source Cluster Peer

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

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

Crittografia dati in-flight IPSec

I clienti che utilizzano tecnologie di crittografia dei dati a riposo come crittografia dello storage NetApp (NSE) o crittografia dei volumi NetApp (NVE) e crittografia del peering del cluster (CPE) per il traffico di replica dei dati possono ora utilizzare la crittografia end-to-end tra client e storage nel data fabric multicloud ibrido effettuando l'aggiornamento a ONTAP 9,8 o versioni successive e utilizzando IPSec. IPSec offre un'alternativa alla crittografia NFS o SMB/CIFS ed è l'unica opzione di crittografia in-flight per il traffico iSCSI.

In alcune situazioni, potrebbe essere necessario proteggere tutti i dati dei client trasferiti via cavo (o in volo) all'SVM di ONTAP. In questo modo si previene il replay e gli attacchi malevoli di tipo "man-in-the-middle" contro i dati sensibili mentre sono in movimento.

A partire da ONTAP 9,8, Internet Protocol Security (IPSec) fornisce il supporto di crittografia end-to-end per tutto il traffico IP tra un client e una SVM ONTAP. La crittografia dei dati IPSec per tutto il traffico IP include i protocolli NFS, iSCSI e SMB/CIFS. IPSec fornisce l'unica opzione di crittografia in volo per il traffico iSCSI.

Fornire la crittografia NFS via cavo è uno dei principali casi di utilizzo di IPsec. Prima di ONTAP 9,8, la crittografia NFS over-the-wire richiedeva la configurazione e la configurazione di Kerberos per l'utilizzo di krb5p per crittografare i dati NFS in-flight. Ciò non è sempre semplice o facile da realizzare in ogni ambiente del cliente.

I clienti che utilizzano tecnologie di crittografia dei dati a riposo come crittografia dello storage NetApp (NSE) o crittografia dei volumi NetApp (NVE) e crittografia del peering del cluster (CPE) per il traffico di replica dei dati possono ora utilizzare la crittografia end-to-end tra client e storage nel data fabric multicloud ibrido effettuando l'aggiornamento a ONTAP 9,8 o versioni successive e utilizzando IPSec.

IPSec è uno standard IETF. ONTAP utilizza IPSec in modalità di trasporto. Utilizza inoltre il protocollo IKE (Internet Key Exchange) versione 2, che utilizza una chiave precondivisa (PSK) per la negoziazione del materiale chiave tra il client e ONTAP con IPv4 o IPv6. Per impostazione predefinita, IPSec utilizza la crittografia a 256 bit Suite-B AES-GCM. Sono supportati anche Suite-B AES-GMAC256 e AES-CBC256 con crittografia a 256 bit.

Sebbene sia necessario attivare la funzionalità IPsec nel cluster, essa si applica ai singoli indirizzi IP delle

SVM mediante l'uso di una voce SPD (Security Policy Database). La voce del criterio (SPD) contiene l'indirizzo IP del client (subnet IP remota), l'indirizzo IP della SVM (subnet IP locale), la suite di crittografia da utilizzare e la password precondivisa (PSK) necessaria per eseguire l'autenticazione tramite IKEv2 e stabilire la connessione IPsec. Oltre alla voce del criterio IPsec, il client deve essere configurato con le stesse informazioni (IP locale e remoto, PSK e suite di crittografia) prima che il traffico possa passare attraverso la connessione IPsec. A partire da ONTAP 9.10.1, viene aggiunto il supporto per l'autenticazione del certificato IPsec. In questo modo vengono rimossi i limiti dei criteri IPsec e viene attivato il supporto del sistema operativo Windows per IPsec.

Se tra il client e l'indirizzo IP della SVM è presente un firewall, è necessario consentire i protocolli ESP e UDP (porta 500 e 4500), sia in entrata (ingresso) che in uscita (uscita), affinché la negoziazione IKEv2 abbia successo e consenta quindi il traffico IPsec.

Per la crittografia del traffico di peering di NetApp SnapMirror e del cluster, si consiglia comunque la crittografia CPE (Cluster peering Encryption) su IPSec per un transito sicuro via cavo. Le prestazioni di CPE per questi carichi di lavoro sono migliori rispetto a IPsec. Non è necessaria una licenza per IPsec e non sono previste restrizioni per l'importazione o l'esportazione.

È possibile attivare IPSec nel cluster e creare una voce SPD per un singolo client e un singolo indirizzo IP SVM, come illustrato nell'esempio seguente:

```
On the Destination Cluster Peer

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

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

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

Gestione TLS e SSL

È possibile attivare la modalità di conformità FIPS 140-2/3 per le interfacce del piano di controllo impostando il `is-fips-enabled` parametro su true con il comando ONTAP `security config modify`.

A partire da ONTAP 9, è possibile attivare la modalità di conformità FIPS 140-2 per le interfacce del piano di controllo a livello di cluster. Per impostazione predefinita, la modalità solo FIPS 140-2 è disattivata. È possibile attivare la modalità di conformità FIPS 140-2 impostando il `is-fips-enabled` parametro su `true` per il `security config modify` comando. È quindi possibile utilizzare `security config show command` per confermare lo stato online.

Quando la conformità FIPS 140-2 è attivata, TLSv1 e SSLv3 sono disattivati e rimangono attivati solo TLSv1.1 e TLSv1.2. ONTAP impedisce di abilitare TLSv1 e SSLv3 quando la conformità FIPS 140-2 è attivata. Se si attiva FIPS 140-2 e successivamente lo si disattiva, TLSv1 e SSLv3 rimangono disabilitati, ma TLSv1,2 o entrambi TLSv1,1 e TLSv1,2 rimangono abilitati, a seconda della configurazione precedente.

Il `security config modify` comando modifica la configurazione di sicurezza esistente a livello del cluster. Se viene attivata la modalità conforme a FIPS, il cluster seleziona automaticamente solo i protocolli TLS. Utilizzare il `-supported-protocols` parametro per includere o escludere i protocolli TLS

indipendentemente dalla modalità FIPS. Per impostazione predefinita, la modalità FIPS è disattivata e ONTAP supporta i protocolli TLSv1,2, TLSv1,1 e TLSv1.

Per la compatibilità con le versioni precedenti, ONTAP supporta l'aggiunta di SSLv3 all' `supported-protocols` elenco quando la modalità FIPS è disattivata. Utilizzare il `-supported-cipher-suites` parametro per configurare solo AES (Advanced Encryption Standard) o AES e 3DES. È inoltre possibile disattivare le crittografie deboli, ad esempio RC4, specificando !RC4. Per impostazione predefinita, l'impostazione di cifratura supportata è `ALL:!LOW:!aNULL:!EXP:!eNULL`. Questa impostazione significa che tutte le suite di crittografia supportate per i protocolli sono abilitate, ad eccezione di quelle senza autenticazione, senza crittografia, senza esportazioni e suite di crittografia a bassa crittografia. Si tratta di suite che utilizzano algoritmi di crittografia a 64 o 56 bit.

Selezionare una suite di crittografia disponibile con il protocollo selezionato corrispondente. Una configurazione non valida potrebbe causare il mancato funzionamento di alcune funzionalità.

Per la sintassi corretta della stringa di cifratura, vedere la "cifrari" pagina su OpenSSL (pubblicata dalla base del software OpenSSL). A partire da ONTAP 9.9.1 e versioni successive, non è più necessario riavviare manualmente tutti i nodi dopo aver modificato la configurazione di protezione.

L'attivazione della conformità FIPS 140-2 ha effetti su altri sistemi e comunicazioni interne ed esterne a ONTAP 9. NetApp consiglia vivamente di verificare queste impostazioni su un sistema non di produzione che disponga dell'accesso alla console.

> Se SSH è usato per amministrare ONTAP 9, allora dovete usare un client OpenSSH 5,7 o successivo. I client SSH devono negoziare con l'algoritmo a chiave pubblica ECDSA (Elliptic Curve Digital Signature Algorithm) affinché la connessione abbia esito positivo.

La protezione TLS può essere ulteriormente rafforzata solo abilitando TLS 1,2 e utilizzando suite di crittografia PFS (Perfect Forward Secrecy). PFS è un metodo di scambio di chiavi che, se utilizzato in combinazione con protocolli di crittografia come TLS 1,2, consente di impedire a un utente malintenzionato di decrittografare tutte le sessioni di rete tra un client e un server. Per attivare solo le suite di crittografia compatibili con TLS 1,2 e PFS, utilizzare il `security config modify` comando dal livello di privilegi avanzato come illustrato nell'esempio seguente.

> Prima di modificare la configurazione dell'interfaccia SSL, è importante ricordare che il client deve supportare i cifrari menzionati (DHE, ECDHE) quando si effettua la connessione a ONTAP. In caso contrario, la connessione non è consentita.

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

Confermare `y` per ogni richiesta. Per ulteriori informazioni su PFS, vedere "Questo blog di NetApp".

A partire dal supporto di ONTAP 9.11.1 e TLS 1,3, puoi convalidare FIPS 140-3.

> La configurazione FIPS è valida per ONTAP e BMC.

Creare un certificato digitale con firma CA

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso Web a ONTAP non è conforme ai criteri di InfoSec. Nei sistemi di produzione, è NetApp consigliabile installare un certificato digitale firmato CA da utilizzare per l'autenticazione del cluster o della SVM come server SSL.

È possibile utilizzare il `security certificate generate-csr` comando per generare una richiesta di firma del certificato (CSR) e il `security certificate install` comando per installare il certificato ricevuto dalla CA.

Fasi

1. Per creare un certificato digitale firmato dalla CA dell'organizzazione, procedere come segue:
   a. Generare una CSR.
   b. Seguire la procedura dell'organizzazione per richiedere un certificato digitale utilizzando la CSR alla CA dell'organizzazione. Ad esempio, utilizzando l'interfaccia Web servizi certificati di Microsoft Active Directory, accedere a `<CA_server_name>/certsrv` e richiedere un certificato.
   c. Installare il certificato digitale in ONTAP.

Protocollo di stato del certificato in linea

Il protocollo OCSP (Online Certificate Status Protocol) consente alle applicazioni ONTAP che utilizzano le comunicazioni TLS, ad esempio LDAP o TLS, di ricevere lo stato di certificato digitale quando OCSP è attivato. L'applicazione riceve una risposta firmata che indica che il certificato richiesto è valido, revocato o sconosciuto.

OCSP consente di determinare lo stato corrente di un certificato digitale senza richiedere elenchi di revoche di certificati (CRL, Certificate Revocation List).

Per impostazione predefinita, il controllo dello stato del certificato OCSP è disattivato. Può essere attivato con il comando `security config ocsp enable -app name`, dove il nome dell'applicazione può essere `autosupport`, `audit_log`, `fabricpool`, , `ems` `kmip` `ldap_ad` `ldap_nis_namemap`, o tutti. Il comando richiede un livello di privilegi avanzato.

Gestione SSHv2

Il `security ssh modify` comando sostituisce le configurazioni esistenti degli algoritmi di scambio chiavi SSH, cifrari o algoritmi MAC per il cluster o una SVM con le impostazioni di configurazione specificate.

NetApp consiglia di:

- Utilizzare le password per le sessioni utente.
- Utilizzare una chiave pubblica per l'accesso alla macchina.

Cifrari supportati e scambi chiave

Cifrari	Scambio di chiavi
aes256-ctr	diffie-hellman-Group-Exchange-sha256 (SHA-2)
aes192-ctr	diffie-hellman-Group-Exchange-sha1 (SHA-1)
aes128-ctr	diffie-hellman-group14-sha1 (SHA-1)
aes256-cbc	diffie-hellman-group1-sha1 (SHA-1)
aes192-cbc	-
aes128-cbc	-
aes128-mtc	-
aes256-mtc	-
3des-cbc	-

Crittografia simmetrica AES e 3DES supportata

ONTAP supporta inoltre i seguenti tipi di crittografia simmetrica AES e 3DES (noti anche come cifrari):

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

La configurazione della gestione SSH si applica a ONTAP e alla piattaforma BMC.

NetApp AutoSupport

La funzione AutoSupport di ONTAP consente di monitorare in modo proattivo lo stato di salute del sistema e di inviare automaticamente messaggi e dettagli al supporto tecnico NetApp, al team di supporto interno dell'organizzazione o a un partner di supporto. Per impostazione predefinita, i messaggi AutoSupport inviati al supporto tecnico NetApp vengono abilitati quando il sistema di archiviazione viene configurato per la prima volta. Inoltre, AutoSupport inizia a inviare messaggi al supporto tecnico NetApp 24 ore dopo l'attivazione. Questo periodo di 24 ore è configurabile. Per sfruttare la comunicazione al team di supporto interno di un'organizzazione, è necessario completare la configurazione dell'host di posta.

Solo l'amministratore del cluster può eseguire la gestione (configurazione) di AutoSupport. L'amministratore della SVM non ha accesso a AutoSupport. La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitarla perché AutoSupport consente di velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema storage. Per impostazione predefinita, il sistema raccoglie le informazioni AutoSupport e le memorizza localmente anche se si disattiva AutoSupport.

Per ulteriori informazioni sui messaggi AutoSupport, inclusi i contenuti nei vari messaggi e le destinazioni in cui vengono inviati diversi tipi di messaggi, consultare la "Consulente digitale NetApp Active IQ" documentazione.

I messaggi AutoSupport contengono dati riservati, inclusi, a titolo esemplificativo, i seguenti elementi:

- File di log
- Dati sensibili al contesto relativi a sottosistemi specifici
- Dati di configurazione e stato
- Dati sulle performance

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. A causa della natura sensibile dei messaggi AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di messaggi AutoSupport al supporto NetApp.

Inoltre, è necessario utilizzare il `system node autosupport modify` comando per specificare gli obiettivi dei dati AutoSupport (ad esempio, il supporto tecnico di NetApp, le operazioni interne di un'organizzazione o i partner). Questo comando consente inoltre di specificare quali dettagli AutoSupport specifici inviare (ad esempio, dati sulle prestazioni, file di log e così via).

Per disattivare completamente AutoSupport, utilizzare il `system node autosupport modify -state disable` comando.

Network Time Protocol

Sebbene ONTAP consenta di impostare manualmente il fuso orario, la data e l'ora sul cluster, è necessario configurare i server NTP (Network Time Protocol) per sincronizzare l'ora del cluster con almeno tre server NTP esterni.

I problemi possono verificarsi quando il tempo del cluster non è preciso. Sebbene ONTAP consenta di impostare manualmente il fuso orario, la data e l'ora sul cluster, è necessario configurare i server NTP (Network Time Protocol) per sincronizzare l'ora del cluster con i server NTP esterni.

A partire da ONTAP 9.5, è possibile configurare il server NTP con autenticazione simmetrica.

È possibile associare un massimo di 10 server NTP esterni utilizzando il `cluster time-service ntp server create` comando. Per garantire la ridondanza e la qualità del servizio nel tempo, è necessario associare almeno tre server NTP esterni al cluster.

Per ulteriori informazioni sulla configurazione di NTP in ONTAP, vedere "Gestione del tempo del cluster (solo amministratori del cluster)".

Account locali del file system NAS (gruppo di lavoro CIFS)

L'autenticazione del client workgroup fornisce un livello di protezione aggiuntivo alla soluzione ONTAP, in linea con la tradizionale posizione di autenticazione del dominio. Utilizzare il `vserver cifs session show` comando per visualizzare numerosi dettagli relativi alla postura, tra cui le informazioni IP, il meccanismo di autenticazione, la versione del protocollo e il tipo di autenticazione.

A partire da ONTAP 9, è possibile configurare un server CIFS in un gruppo di lavoro con client CIFS che eseguono l'autenticazione sul server utilizzando utenti e gruppi definiti localmente. L'autenticazione del client workgroup fornisce un livello di protezione aggiuntivo alla soluzione ONTAP, in linea con la tradizionale posizione di autenticazione del dominio. Per configurare il server CIFS, utilizzare il `vserver cifs create` comando. Una volta creato il server CIFS, è possibile unirsi a un dominio CIFS o a un gruppo di lavoro. Per entrare in un gruppo di lavoro, utilizzare il `-workgroup` parametro. Ecco un esempio di configurazione:

```
cluster1::> vserver cifs create -vserver vs1 -cifs-server CIFSSERVER1
-workgroup Sales
```

Un server CIFS in modalità workgroup supporta solo l'autenticazione NTLM (Windows NT LAN Manager) e non supporta l'autenticazione Kerberos.

NetApp consiglia di utilizzare la funzione di autenticazione NTLM con i gruppi di lavoro CIFS per mantenere la sicurezza dell'organizzazione. Per validare la postura di sicurezza CIFS, NetApp consiglia di utilizzare il `vserver cifs session show` comando per visualizzare numerosi dettagli relativi alla postura, tra cui informazioni IP, il meccanismo di autenticazione, la versione del protocollo e il tipo di autenticazione.

Auditing del file system NAS

I file system NAS occupano un impatto sempre maggiore nel panorama delle minacce di oggi, le funzioni di audit sono critiche per supportare la visibilità.

La protezione richiede convalida. ONTAP 9 fornisce maggiori eventi di controllo e dettagli in tutta la soluzione. Poiché i file system NAS occupano un impatto sempre maggiore nel panorama delle minacce odierno, le funzioni di audit sono critiche per supportare la visibilità. Grazie alla migliore funzionalità di audit di ONTAP 9, i dettagli di audit CIFS sono più abbondanti che mai. I dettagli chiave, inclusi i seguenti, vengono registrati con gli eventi creati:

- Accesso a file, cartelle e condivisioni
- File creati, modificati o eliminati

- Accesso corretto ai file di lettura
- Tentativi di lettura o scrittura dei file non riusciti
- Modifiche ai permessi della cartella

Creare una configurazione di controllo

È necessario attivare il controllo CIFS per generare eventi di controllo. Utilizzare il `vserver audit create` comando per creare una configurazione di controllo. Per impostazione predefinita, il registro di controllo utilizza un metodo di rotazione basato sulle dimensioni. È possibile utilizzare un'opzione di rotazione basata sul tempo se specificata nel campo parametri di rotazione. I dettagli aggiuntivi della configurazione della rotazione del registro audit includono il programma di rotazione, i limiti di rotazione, i giorni di rotazione della settimana e le dimensioni della rotazione. Nel testo seguente viene fornita una configurazione di esempio che illustra una configurazione di controllo utilizzando una rotazione mensile basata sull'ora programmata per tutti i giorni della settimana alle 12:30.

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

Eventi di audit CIFS

Gli eventi di audit CIFS sono i seguenti:

- **Condivisione file**: Genera un evento di controllo quando una condivisione di rete CIFS viene aggiunta, modificata o eliminata utilizzando i comandi correlati `vserver cifs share` .
- **Modifica criterio di controllo**: Genera un evento di controllo quando il criterio di controllo viene disattivato, attivato o modificato utilizzando i comandi correlati `vserver audit` .
- **Account utente**: Genera un evento di controllo quando un utente CIFS o UNIX locale viene creato o eliminato; un account utente locale viene attivato, disattivato o modificato; oppure una password viene reimpostata o modificata. Questo evento utilizza il `vserver cifs users-and-groups local-group` comando o il comando correlato `vserver services name-service unix-user` .
- **Gruppo di protezione**: Genera un evento di controllo quando un gruppo di protezione CIFS o UNIX locale viene creato o eliminato utilizzando il `vserver cifs users-and-groups local-group` comando o il comando correlato `vserver services name-service unix-group` .
- **Modifica della policy di autorizzazione**: Genera un evento di controllo quando vengono concessi o revocati diritti per un utente CIFS o un gruppo CIFS utilizzando il `vserver cifs users-and-groups privilege` comando.

> Questa funzionalità si basa sulla funzione di audit del sistema, che consente a un amministratore di esaminare ciò che il sistema consente e le sue prestazioni dal punto di vista di un utente di dati.

Effetto delle API REST sull'audit NAS

ONTAP include la possibilità per gli account degli amministratori di accedere e manipolare i file SMB/CIFS o NFS utilizzando le API REST. Anche se le API REST possono essere eseguite solo dagli amministratori di ONTAP, i comandi delle API REST ignorano il log di audit del NAS del sistema. Inoltre, gli amministratori di

ONTAP possono ignorare le autorizzazioni dei file quando utilizzano le API REST. Tuttavia, le azioni dell'amministratore con le API REST sui file vengono acquisite nel registro della cronologia dei comandi di sistema.

Creare un ruolo API REST senza accesso

Puoi impedire agli amministratori di ONTAP di utilizzare le API REST per l'accesso al file creando un ruolo API REST che non ha accesso ai volumi ONTAP via REST. Per assegnare questo ruolo, completare i passaggi seguenti.

Fasi

1. Creare un nuovo ruolo REST che non abbia accesso ai volumi storage ma che disponga di tutti gli altri accesso ad API REST.

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

2. Assegnare l'account amministratore al nuovo ruolo API REST creato nel passaggio precedente.

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

Se si desidera impedire all'account amministratore del cluster ONTAP integrato di utilizzare le API REST per l'accesso ai file, è necessario prima "creare un nuovo account amministratore e disattivare o eliminare l'account incorporato".

Configurazione e attivazione della firma e della sigillatura SMB CIFS

Puoi configurare e abilitare la SMB signing che protegge la sicurezza del data fabric assicurandoti che il traffico tra sistemi storage e client non venga compromesso da attacchi replay o man-in-the-middle. La SMB signing protegge i messaggi SMB verificando che dispongano di firme valide.

A proposito di questa attività

Un comune vettore di minaccia per i file system e le architetture si trova nel protocollo SMB. Per risolvere questo problema, la soluzione ONTAP 9 utilizza la firma e la sigillatura SMB standard del settore. La SMB signing protegge la sicurezza del data fabric garantendo che il traffico tra i sistemi storage e i client non venga compromesso da attacchi replay o man-in-the-middle. Lo fa verificando che i messaggi SMB dispongano di firme valide.

Sebbene la firma SMB sia disattivata per impostazione predefinita nell'interesse delle prestazioni, NetApp consiglia vivamente di attivarla. Inoltre, la soluzione ONTAP supporta la SMB Encryption, nota anche come sealing. Questo approccio consente il trasporto sicuro dei dati su base condivisa. Per impostazione predefinita, la crittografia SMB è disattivata. Tuttavia, NetApp consiglia di attivare la crittografia SMB.

La firma e la sigillatura LDAP sono ora supportate in SMB 2,0 e versioni successive. La firma (protezione contro la manomissione) e la crittografia (crittografia) consentono comunicazioni sicure tra SVM e server Active Directory. La crittografia Accelerated AES New Instructions (Intel AES NI) è ora supportata in SMB 3,0 e versioni successive. Intel AES NI migliora l'algoritmo AES e accelera la crittografia dei dati con famiglie di processori supportati.

Fasi

1. Per configurare e abilitare la firma SMB, utilizzare il `vserver cifs security modify` comando e verificare che il `-is-signing-required` parametro sia impostato su `true`. Fare riferimento alla seguente configurazione di esempio:

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

2. Per configurare e attivare la crittografia e la sigillatura SMB, utilizzare il `vserver cifs security modify` comando e verificare che il `-is-smb-encryption-required` parametro sia impostato su `true`. Fare riferimento alla seguente configurazione di esempio:

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

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

Sicurezza NFS

Le regole di esportazione sono gli elementi funzionali di una policy di esportazione. Le regole di esportazione corrispondono alle richieste di accesso client per un volume rispetto a parametri specifici configurati per determinare come gestire le richieste di accesso client. Un criterio di esportazione deve contenere almeno una regola di esportazione per consentire l'accesso ai client. Se un criterio di esportazione contiene più di una regola, le regole vengono elaborate nell'ordine in cui appaiono nel criterio di esportazione.

Il controllo degli accessi è fondamentale per mantenere una posizione sicura. Pertanto, ONTAP utilizza la funzionalità di policy di esportazione per limitare l'accesso al volume NFS ai client che corrispondono a parametri specifici. I criteri di esportazione contengono una o più regole di esportazione che elaborano ogni richiesta di accesso client. A ciascun volume è associato un criterio di esportazione per configurare l'accesso del client al volume. Il risultato di questo processo determina se al client viene concesso o negato (con un messaggio di autorizzazione negata) l'accesso al volume. Questo processo determina inoltre il livello di accesso fornito al volume.

Per consentire ai client di accedere ai dati, deve esistere una policy di esportazione con regole di esportazione in una SVM. Una SVM può contenere diverse policy di esportazione.

L'ordine delle regole è determinato dal numero di indice delle regole. Se una regola corrisponde a un client, vengono utilizzate le autorizzazioni di tale regola e non vengono elaborate altre regole. Se nessuna regola corrisponde, al client viene negato l'accesso.

Le regole di esportazione determinano le autorizzazioni di accesso dei client applicando i seguenti criteri:

- Il protocollo di accesso ai file utilizzato dal client che invia la richiesta (ad esempio NFSv4 o SMB)
- Un identificatore client (ad esempio, il nome host o l'indirizzo IP)
- Il tipo di protezione utilizzato dal client per l'autenticazione (ad esempio, Kerberos v5, NTLM o AUTH_SYS)

Se una regola specifica più criteri e il client non corrisponde a uno o più criteri, la regola non viene applicata.

Un criterio di esportazione di esempio contiene una regola di esportazione con i seguenti parametri:

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

Il tipo di protezione determina il livello di accesso ricevuto da un client. I tre livelli di accesso sono di sola lettura, lettura-scrittura e superutente (per i client con ID utente `0`). Poiché il livello di accesso determinato dal tipo di protezione viene valutato in questo ordine, è necessario rispettare le regole elencate:

Regole per i parametri del livello di accesso nelle regole di esportazione

Per un client, ottenere i seguenti livelli di accesso	Questi parametri di accesso devono corrispondere al tipo di protezione del client
Utente normale di sola lettura	Sola lettura (`-rorule`)
Lettura/scrittura utente normale	Sola lettura (`-rorule`) e read-write (`-rwrule`)
Superuser di sola lettura	Sola lettura (`-rorule`) e. `-superuser`
Lettura/scrittura superutente	Sola lettura (`-rorule`) e read-write (`-rwrule`) e. `-superuser`

Di seguito sono riportati i tipi di protezione validi per ciascuno di questi tre parametri di accesso:

- Qualsiasi
- Nessuno
- Mai

Questi tipi di protezione non sono validi per l'uso con il `-superuser` parametro:

- krb5
- ntlm

- sis

Regole per i risultati dei parametri di accesso

Se il tipo di protezione del client…	Allora…
Corrisponde a un tipo di protezione specificato nel parametro di accesso.	Il client riceve l'accesso per quel livello con il proprio ID utente.
Non corrisponde a un tipo di protezione specificato, ma il parametro di accesso include l'opzione `none`.	Il client riceve l'accesso per quel livello e riceve l'utente anonimo con l'ID utente specificato dal `-anon` parametro.
Non corrisponde a un tipo di protezione specificato e il parametro di accesso non include l'opzione `none`.	Il client non riceve alcun accesso per quel livello. Questa restrizione non si applica al `-superuser` parametro perché questo parametro non include sempre nessuno, anche se non specificato.

Kerberos 5 e Krb5p

A partire da ONTAP 9, è supportata l'autenticazione Kerberos 5 con servizio di privacy (krb5p). La modalità di autenticazione krbp5 è sicura e protegge da possibili tentativi di manomissione e snooping dei dati utilizzando dei checksum per crittografare tutto il traffico tra client e server. La soluzione ONTAP supporta la crittografia AES a 128 e 256 bit per Kerberos. Il servizio di privacy include la verifica dell'integrità dei dati ricevuti, l'autenticazione degli utenti e la crittografia dei dati prima della trasmissione.

L'opzione krb5p è più presente nella funzione dei criteri di esportazione, dove è impostata come opzione di crittografia. Il metodo di autenticazione krb5p può essere utilizzato come parametro di autenticazione, come illustrato nell'esempio seguente:

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

Abilitare la firma e la sigillatura del protocollo Lightweight Directory Access Protocol

La firma e la sigillatura sono supportate per abilitare la protezione della sessione sulle query in un server LDAP. Questo approccio offre un'alternativa alla protezione delle sessioni LDAP-over-TLS.

La firma conferma l'integrità dei dati di payload LDAP utilizzando la tecnologia codifica-chiave. Il sealing crittografa i dati del payload LDAP per evitare la trasmissione di informazioni sensibili in testo non crittografato. Le impostazioni di protezione della sessione su una SVM corrispondono a quelle disponibili sul server LDAP. Per impostazione predefinita, la firma e la firma LDAP sono disattivate.

Fasi

1. Per attivare questa funzione, eseguire `vserver cifs security modify` il comando con il `session-security-for-ad-ldap` parametro .

   Opzioni per le funzioni di protezione LDAP:

   - **Nessuno**: Impostazione predefinita, nessuna firma o sigillatura
   - **Firma**: Firma il traffico LDAP
   - **Seal**: Firma e crittografa il traffico LDAP

   > I parametri segno e sigillo sono cumulativi, il che significa che se si utilizza l'opzione segno, il risultato è LDAP con firma. Tuttavia, se si utilizza l'opzione di tenuta, il risultato è sia segno che sigillo. Inoltre, se non viene specificato un parametro per questo comando, il valore predefinito è nessuno.

   Di seguito è riportato un esempio di configurazione:

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

Creare e utilizzare un NetApp FPolicy

È possibile creare e utilizzare un FPolicy, un componente dell'infrastruttura della soluzione ONTAP, che consente alle applicazioni partner di monitorare e impostare le autorizzazioni di accesso ai file. Una delle applicazioni più potenti è Storage workload Security, un'applicazione SaaS NetApp che fornisce visibilità e controllo centralizzati di tutti gli accessi ai dati aziendali negli ambienti di cloud ibrido per garantire che gli obiettivi di sicurezza e conformità siano soddisfatti.

Il controllo degli accessi è un concetto chiave di sicurezza. La visibilità e la capacità di rispondere alle operazioni di accesso e modifica dei file sono critiche per mantenere la posizione di sicurezza. Per fornire visibilità e controllo degli accessi ai file, la soluzione ONTAP utilizza la funzionalità NetApp FPolicy.

Le policy dei file possono essere impostate in base al tipo di file. FPolicy determina il modo in cui il sistema storage gestisce le richieste da singoli sistemi client per operazioni quali la creazione, l'apertura, la ridenominazione e l'eliminazione. A partire da ONTAP 9, il framework di notifica di accesso ai file FPolicy è stato migliorato con controlli di filtraggio e resilienza in caso di brevi interruzioni della rete.

Fasi

1. Per utilizzare la funzione FPolicy, è necessario creare prima il criterio FPolicy con il `vserver fpolicy policy create` comando.

   > Inoltre, utilizzare il `-events` parametro se si utilizza FPolicy per la visibilità e la raccolta di eventi. La granularità aggiuntiva fornita da ONTAP consente il filtraggio e l'accesso fino al livello di controllo del nome utente. Per controllare i privilegi e l'accesso con i nomi utente, specificare il `-privilege-user-name` parametro.

   Il testo seguente fornisce un esempio di creazione di FPolicy:

```
cluster1::> vserver fpolicy policy create -vserver vs1.example.com
-policy-name vs1_pol -events cserver_evt,v1e1 -engine native -is
-mandatory true -allow-privileged-access no -is-passthrough-read-enabled
false
```

2. Dopo aver creato il criterio FPolicy, è necessario attivarlo con il `vserver fpolicy enable` comando . Questo comando imposta inoltre la priorità o la sequenza della voce FPolicy.

   La sequenza FPolicy è importante perché, se più policy hanno sottoscritto lo stesso evento di accesso ai file, la sequenza determina l'ordine in cui l'accesso viene concesso o negato.

   Nel testo seguente viene fornita una configurazione di esempio per abilitare il criterio FPolicy e convalidare la configurazione con il `vserver fpolicy show` comando:

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

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

Miglioramenti di FPolicy

ONTAP 9 include i miglioramenti FPolicy descritti nelle sezioni seguenti.

Controlli di filtraggio

Sono disponibili nuovi filtri per `SetAttr` e per la rimozione delle notifiche sulle attività della directory.

Resilienza asincrona

Se un server FPolicy che opera in modalità asincrona subisce un'interruzione di rete, le notifiche FPolicy generate durante l'interruzione vengono memorizzate nel nodo di storage. Quando il server FPolicy torna in linea, viene avvisato delle notifiche memorizzate e può recuperarle dal nodo di storage. Il periodo di tempo in cui le notifiche possono essere memorizzate durante un'interruzione è configurabile fino a 10 minuti.

Sicurezza LIF

Una LIF è un indirizzo IP o nome di porta mondiale (WWPN) con caratteristiche associate, come un ruolo, una porta home, un nodo home, un elenco di porte su cui

eseguire il failover e una policy firewall. È possibile configurare le LIF sulle porte su cui il cluster invia e riceve le comunicazioni sulla rete. È fondamentale comprendere le caratteristiche di sicurezza di ogni ruolo LIF.

Ruoli di LIF

I ruoli LIF possono essere i seguenti:

- **Data LIF**: Un LIF associato a una SVM e utilizzato per la comunicazione con i client.
- **Cluster LIF**: Una LIF utilizzata per trasportare il traffico tra nodi in un cluster.
- **LIF di gestione nodi**: Una LIF che fornisce un indirizzo IP dedicato per la gestione di un nodo specifico in un cluster.
- **Cluster management LIF**: Una LIF che fornisce una singola interfaccia di gestione per l'intero cluster.
- **Intercluster LIF**: Una LIF utilizzata per la comunicazione, il backup e la replica tra cluster.

Caratteristiche di sicurezza di ogni ruolo LIF

	LIF dati	LIF del cluster	LIF di gestione dei nodi	LIF di gestione del cluster	LIF intercluster
Richiede subnet IP privata?	No	Sì	No	No	No
Richiede una rete protetta?	No	Sì	No	No	Sì
Policy firewall predefinita	Molto restrittivo	Aprire completamente	Medio	Medio	Molto restrittivo
Il firewall è personalizzabile?	Sì	No	Sì	Sì	Sì

- Dato che il cluster LIF è completamente aperto senza policy del firewall configurabili, deve trovarsi in una subnet IP privata in una rete isolata e sicura.
- In nessun caso i ruoli LIF devono essere esposti a Internet.

Per ulteriori informazioni sulla protezione delle LIF, consulta "Configurare le policy firewall per le LIF".

Sicurezza del protocollo e delle porte

Oltre all'esecuzione di operazioni e funzioni di protezione on-box, la protezione avanzata di una soluzione deve includere anche meccanismi di protezione off-box. L'utilizzo di dispositivi infrastrutturali aggiuntivi, come firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza, per il filtraggio e la limitazione dell'accesso a ONTAP è un modo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. Queste informazioni sono un componente chiave per filtrare e limitare l'accesso all'ambiente e alle sue risorse.

Protocolli e porte di uso comune

Servizio	Porta/protocollo	Descrizione
SSH	22/TCP	Login SSH
telnet	23/TCP	Accesso remoto
Domain	53/TCP	Server dei nomi di dominio
HTTP	80/TCP 80/UDP	HTTP
rpcbind	111/TCP 111/UDP	Chiamata di procedura remota
NTP	123/UDP	Network Time Protocol
msrpc	135/UDP	Chiamata di procedura remota Microsoft
Netbios-name	137/TCP 137/UDP	Servizio nomi NetBIOS
netbios-ssn	139/TCP	Sessione del servizio NetBIOS
SNMP	161/UDP	SNMP
HTTPS	443/TCP	Collegamento protetto:http
microsoft-ds	445/TCP	Servizi directory Microsoft
IPsec	500/UDP	Internet Protocol Security (sicurezza protocollo Internet)
mount	635/UDP	Montaggio NFS
named	953/UDP	Nome daemon
NFS	2049/UDP 2049/TCP	Daemon del server NFS
nrv	2050/TCP	Protocollo volume remoto NetApp
iscsi	3260/TCP	Porta di destinazione iSCSI
Lockd	4045/TCP 4045/UDP	Daemon di blocco NFS
NFS	4046/TCP	Protocollo NFS mountd
acp-proto	4046/UDP	Protocollo di contabilità
rquotad	4049/UDP	Protocollo NFS rquotad
krb524	4444/UDP	Kerberos 524
IPsec	4500/UDP	Internet Protocol Security (sicurezza protocollo Internet)
acp	5125/UDP 5133/UDP 5144/TCP	Porta di controllo alternativa per il disco

Servizio	Porta/protocollo	Descrizione
`Mdns`	5353/UDP	DNS multicast
`HTTPS`	5986/UDP	Porta HTTPS: Protocollo binario in ascolto
`TELNET`	8023/TCP	Telnet con ambito di nodo
`HTTPS`	8443/TCP	7MTT strumento GUI tramite xref:./ontap-hardening/HTTPS
`RSH`	8514/TCP	Ambito nodo RSH
`KMIP`	9877/TCP	Porta client KMIP (solo host locale interno)
`ndmp`	10000/TCP	NDMP
`cifs` porta testimone	40001/TCP	Porta di controllo CIFS
`TLS`	50000/TCP	Sicurezza del livello di trasporto
`Iscsi`	65200/TCP	Porta iSCSI
`SSH`	65502/TCP	Shell sicura
`vsun`	65503/TCP	vsun

Porte interne NetApp

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

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

Porta/protocollo	Descrizione
7824	RPC cluster NetApp

Risorse di sicurezza

Per ulteriori informazioni sulle informazioni descritte in questa documentazione sulla protezione di ONTAP, fare riferimento alle seguenti informazioni aggiuntive e ai concetti di protezione.

Per informazioni sulla segnalazione di vulnerabilità e incidenti, risposte di sicurezza NetApp e riservatezza dei clienti, vedere "Portale NetApp sulla sicurezza".

- "Note sulla versione di ONTAP 9"
- "Riferimenti dei comandi di ONTAP 9"
- "Amministrazione del sistema"
- "Autenticazione dell'amministratore e RBAC"
- "Crittografia NetApp"
- "TR-4647: Autenticazione multifattore in ONTAP 9,3"
- "Crittografie OPENSSL"
- "CryptoMod FIPS-140-2 livello 1"
- "Autenticazione basata su certificati con NetApp Manageability SDK per ONTAP"
- "Gestione della rete"

Informazioni sul copyright

Informazioni sul marchio commerciale