Sicurezza

ONTAP 9

NetApp
January 08, 2026

Sommario

Sicurezza

Autenticazione e autorizzazione del client

ONTAP utilizza metodi standard per proteggere l'accesso client e amministratore allo storage e per proteggerlo dai virus. Sono disponibili tecnologie avanzate per la crittografia dei dati a riposo e per lo storage WORM.

ONTAP autentica un computer client e un utente verificando la propria identità con un'origine attendibile. ONTAP autorizza un utente ad accedere a un file o a una directory confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory.

Autenticazione

È possibile creare account utente locali o remoti:

- Un account locale è un account in cui le informazioni dell'account risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.

ONTAP utilizza i servizi dei nomi locali o esterni per cercare informazioni relative a nome host, utente, gruppo, netgroup e mappatura dei nomi. ONTAP supporta i seguenti servizi per i nomi:

- Utenti locali
- DNS
- Domini NIS esterni
- Domini LDAP esterni

Una *name service switch table* specifica le fonti per la ricerca delle informazioni di rete e l'ordine in cui ricercarle (fornendo la funzionalità equivalente del file /etc/nsswitch.conf sui sistemi UNIX). Quando un client NAS si connette a SVM, ONTAP verifica i servizi dei nomi specificati per ottenere le informazioni richieste.

supporto Kerberos Kerberos è un protocollo di autenticazione di rete che fornisce "sautenticazione trong" crittografando le password utente nelle implementazioni client-server. ONTAP supporta l'autenticazione Kerberos 5 con controllo dell'integrità (krb5i) e l'autenticazione Kerberos 5 con controllo della privacy (krb5p).

Autorizzazione

ONTAP valuta tre livelli di sicurezza per determinare se un'entità è autorizzata a eseguire un'azione richiesta su file e directory che risiedono su una SVM. L'accesso è determinato dalle autorizzazioni effettive dopo la valutazione dei livelli di sicurezza:

- Sicurezza di esportazione (NFS) e condivisione (SMB)

  La sicurezza di esportazione e condivisione si applica all'accesso client a una data esportazione NFS o condivisione SMB. Gli utenti con privilegi amministrativi possono gestire la sicurezza a livello di esportazione e condivisione dai client SMB e NFS.

- Protezione di file e directory di Access Guard a livello di storage

La sicurezza di Access Guard a livello di storage si applica all'accesso dei client SMB e NFS ai volumi SVM. Sono supportate solo le autorizzazioni di accesso NTFS. Affinché ONTAP esegua controlli di sicurezza sugli utenti UNIX per l'accesso ai dati sui volumi per i quali è stato applicato Storage-Level Access Guard, l'utente UNIX deve eseguire il mapping a un utente Windows sulla SVM proprietaria del volume.

- Sicurezza nativa a livello di file in NTFS, UNIX e NFSv4

  La protezione nativa a livello di file esiste nel file o nella directory che rappresenta l'oggetto di storage. È possibile impostare la sicurezza a livello di file da un client. Le autorizzazioni dei file sono efficaci indipendentemente dal fatto che SMB o NFS vengano utilizzati per accedere ai dati.

Autenticazione con SAML

ONTAP supporta il linguaggio SAML (Security Assertion Markup Language) per l'autenticazione degli utenti remoti. Sono supportati diversi provider di identità (IDP). Per ulteriori informazioni sugli IDP supportati e istruzioni per l'attivazione dell'autenticazione SAML, fare riferimento a. "Configurare l'autenticazione SAML".

OAuth 2,0 con client API REST ONTAP

Il supporto per il framework Open Authorization (OAuth 2,0) è disponibile a partire da ONTAP 9,14. È possibile utilizzare OAuth 2,0 solo per prendere decisioni di autorizzazione e controllo degli accessi quando il client utilizza l'API REST per accedere a ONTAP. Tuttavia, puoi configurare e abilitare la funzionalità con qualsiasi interfaccia amministrativa di ONTAP, inclusi CLI, System Manager e API REST.

Le funzionalità standard di OAuth 2,0 sono supportate insieme a diversi server di autorizzazione più diffusi. È possibile migliorare ulteriormente la protezione di ONTAP utilizzando token di accesso con vincoli di mittente basati su TLS comuni. Inoltre, è disponibile una vasta gamma di opzioni di autorizzazione, tra cui ambiti indipendenti, oltre all'integrazione con i ruoli REST di ONTAP e le definizioni degli utenti locali. Vedere "Panoramica dell'implementazione di ONTAP OAuth 2,0" per ulteriori informazioni.

Autenticazione amministratore e RBAC

Gli amministratori utilizzano account di accesso locali o remoti per autenticarsi al cluster e alla SVM. RBAC (Role-Based Access Control) determina i comandi a cui un amministratore ha accesso.

Autenticazione

È possibile creare account di amministratore SVM e cluster locali o remoti:

- Un account locale è un account in cui le informazioni sull'account, la chiave pubblica o il certificato di protezione risiedono nel sistema di storage.
- Un account remoto è un account in cui le informazioni sull'account vengono memorizzate in un controller di dominio Active Directory, in un server LDAP o in un server NIS.

Ad eccezione del DNS, ONTAP utilizza gli stessi servizi di nome per autenticare gli account amministratore utilizzati per autenticare i client.

RBAC

Il *ruolo* assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Scansione virus

È possibile utilizzare la funzionalità antivirus integrata nel sistema di storage per proteggere i dati da virus o altri codici dannosi. La scansione antivirus di ONTAP, denominata *Vscan*, combina il software antivirus di terze parti più all'avanguardia con le funzionalità di ONTAP che offrono la flessibilità necessaria per controllare quali file vengono sottoposti a scansione e quando.

I sistemi storage trasferiscono le operazioni di scansione a server esterni che ospitano software antivirus di terze parti. Il *connettore antivirus ONTAP*, fornito da NetApp e installato sul server esterno, gestisce le comunicazioni tra il sistema di storage e il software antivirus.

- È possibile utilizzare *on-access scanning* per verificare la presenza di virus quando i client aprono, leggono, rinominano o chiudono i file su SMB. L'operazione sul file viene sospesa fino a quando il server esterno non riporta lo stato di scansione del file. Se il file è già stato sottoposto a scansione, ONTAP consente l'operazione. In caso contrario, richiede una scansione dal server.

  La scansione all'accesso non è supportata per NFS.

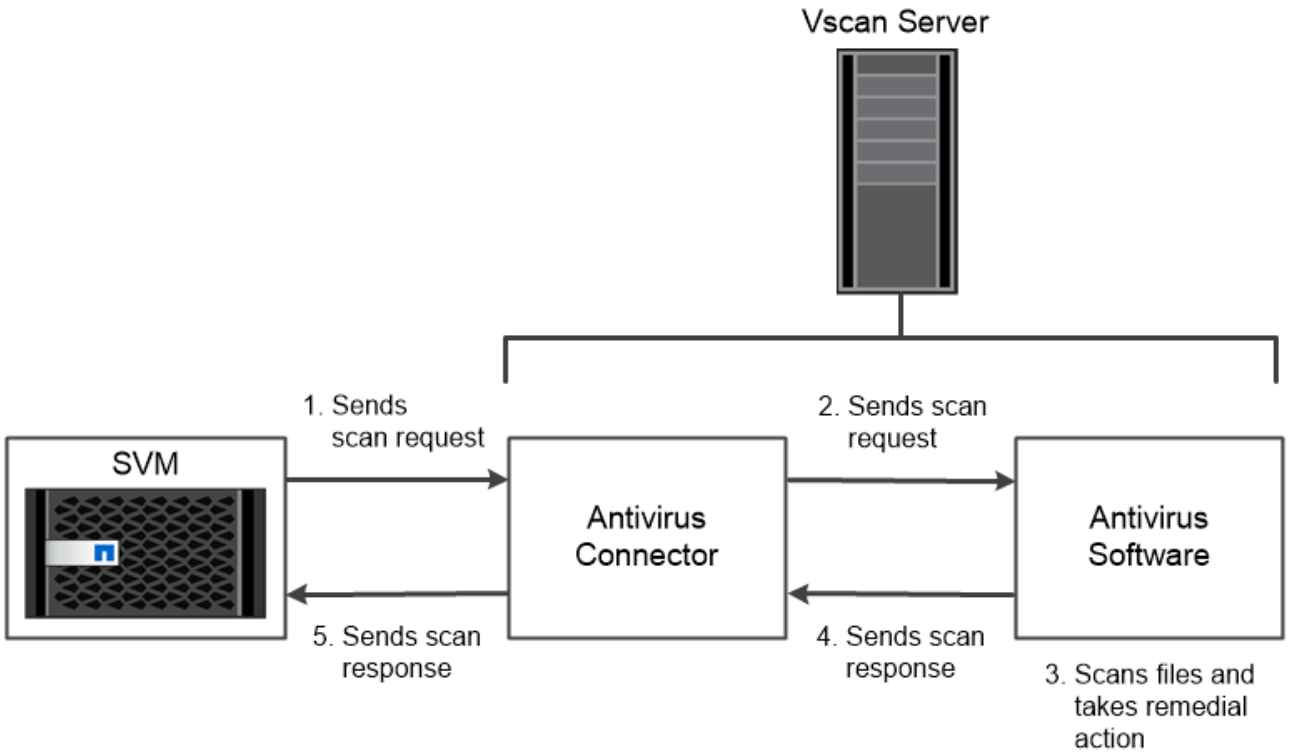
- È possibile utilizzare la *scansione on-demand* per controllare i file alla ricerca di virus immediatamente o in base a una pianificazione. Ad esempio, è possibile eseguire scansioni solo in ore non di punta. Il server esterno aggiorna lo stato di scansione dei file selezionati, in modo che la latenza di accesso ai file (presupponendo che non siano stati modificati) sia in genere ridotta al successivo accesso tramite SMB.

  È possibile utilizzare la scansione on-demand per qualsiasi percorso nello spazio dei nomi SVM, anche per i volumi esportati solo tramite NFS.

In genere, si abilitano entrambe le modalità di scansione su una SVM. In entrambe le modalità, il software antivirus esegue un'azione correttiva sui file infetti in base alle impostazioni del software.

scansione virus in disaster recovery e configurazioni MetroCluster

Per le configurazioni di disaster recovery e MetroCluster, è necessario configurare server Vscan separati per i cluster locali e partner.



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

Crittografia

ONTAP offre tecnologie di crittografia basate su software e hardware per garantire che i dati inattivi non possano essere letti in caso di riposizionamento, restituzione, smarrimento o furto del supporto di storage.

ONTAP è conforme agli standard federali sull'elaborazione delle informazioni (FIPS) 140-2 per tutte le connessioni SSL. È possibile utilizzare le seguenti soluzioni di crittografia:

- Soluzioni hardware:
  - NetApp Storage Encryption (NSE)

    NSE è una soluzione hardware che utilizza dischi con crittografia automatica (SED).

  - SED NVMe

    ONTAP offre la crittografia completa del disco per i SED NVMe che non dispongono della certificazione FIPS 140-2.
- Soluzioni software:
  - NetApp aggregate Encryption (NAE)

    NAE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con chiavi univoche per ciascun aggregato.

  - NetApp Volume Encryption (NVE)

NVE è una soluzione software che consente la crittografia di qualsiasi volume di dati su qualsiasi tipo di disco in cui è abilitato con una chiave univoca per ciascun volume.

Utilizzare soluzioni di crittografia sia software (NAE o NVE) che hardware (NSE o NVMe SED) per ottenere una doppia crittografia a riposo. L'efficienza dello storage non è influenzata dalla crittografia NAE o NVE.

Crittografia dello storage NetApp

NetApp Storage Encryption (NSE) supporta i SED che crittografano i dati durante la scrittura. I dati non possono essere letti senza una chiave di crittografia memorizzata sul disco. La chiave di crittografia, a sua volta, è accessibile solo a un nodo autenticato.

In caso di richiesta i/o, un nodo esegue l'autenticazione in un SED utilizzando una chiave di autenticazione recuperata da un server di gestione delle chiavi esterno o da Onboard Key Manager:

- Il server di gestione delle chiavi esterno è un sistema di terze parti nell'ambiente di storage che fornisce le chiavi di autenticazione ai nodi utilizzando il protocollo KMIP (Key Management Interoperability Protocol).
- Onboard Key Manager è uno strumento integrato che fornisce chiavi di autenticazione ai nodi dello stesso sistema storage dei dati.

NSE supporta HDD e SSD con crittografia automatica. È possibile utilizzare NetApp Volume Encryption con NSE per la doppia crittografia dei dati sui dischi NSE.

Se stai utilizzando NSE su un sistema con un modulo Flash cache, dovresti abilitare anche NVE o NAE. NSe non crittografa i dati che risiedono nel modulo Flash cache.

Dischi con crittografia automatica NVMe

NVMe SED non dispone della certificazione FIPS 140-2; tuttavia, questi dischi utilizzano la crittografia del disco trasparente AES a 256 bit per proteggere i dati a riposo.

Le operazioni di crittografia dei dati, come la generazione di una chiave di autenticazione, vengono eseguite internamente. La chiave di autenticazione viene generata la prima volta che il sistema di storage accede al disco. In seguito, i dischi proteggono i dati inattivi richiedendo l'autenticazione del sistema di storage ogni volta che vengono richieste operazioni sui dati.

Crittografia aggregata NetApp

NetApp aggregate Encryption (NAE) è una tecnologia software per la crittografia di tutti i dati su un aggregato. Un vantaggio di NAE è che i volumi sono inclusi nella deduplica a livello di aggregato, mentre i volumi NVE sono esclusi.

Con NAE attivato, i volumi all'interno dell'aggregato possono essere crittografati con chiavi aggregate.

A partire da ONTAP 9.7, gli aggregati e i volumi appena creati sono criptati per impostazione predefinita quando si dispone della "Licenza NVE"gestione delle chiavi integrata o esterna.

Crittografia dei volumi NetApp

NetApp Volume Encryption (NVE) è una tecnologia software per la crittografia dei dati inattivi di un volume alla volta. Una chiave di crittografia accessibile solo al sistema di storage garantisce che i dati del volume non possano essere letti se il dispositivo sottostante è separato dal sistema.

Entrambi i dati, inclusi snapshot e metadati sono crittografati. L'accesso ai dati viene fornito da una chiave XTS-AES-256 univoca, una per volume. Un Onboard Key Manager integrato protegge le chiavi dello stesso sistema con i dati.

È possibile utilizzare NVE su qualsiasi tipo di aggregato (HDD, SSD, ibrido, LUN array), con qualsiasi tipo di RAID e in qualsiasi implementazione ONTAP supportata, incluso ONTAP Select. È inoltre possibile utilizzare NVE con NetApp Storage Encryption (NSE) per eseguire la doppia crittografia dei dati sui dischi NSE.

quando utilizzare i server KMIP sebbene sia meno costoso e generalmente più conveniente utilizzare Onboard Key Manager, è necessario configurare i server KMIP se si verifica una delle seguenti condizioni:

- La soluzione di gestione delle chiavi di crittografia deve essere conforme agli standard FIPS (Federal Information Processing Standards) 140-2 o ALLO standard OASIS KMIP.
- Hai bisogno di una soluzione multi-cluster. I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

  I server KMIP supportano più cluster con gestione centralizzata delle chiavi di crittografia.

- La tua azienda richiede una maggiore sicurezza nell'archiviazione delle chiavi di autenticazione su un sistema o in una posizione diversa dai dati.

  I server KMIP memorizzano le chiavi di autenticazione separatamente dai dati.

Informazioni correlate

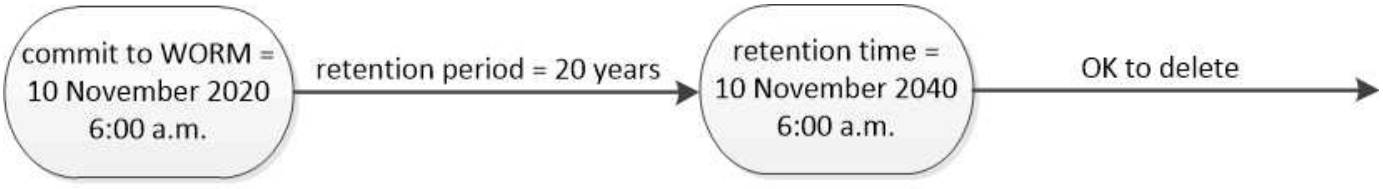
"FAQ - NetApp Volume Encryption e NetApp aggregate Encryption"

Storage WORM

SnapLock è una soluzione per la compliance dalle performance elevate per le organizzazioni che utilizzano lo storage *write once, Read Many (WORM)* per conservare i file critici in forma non modificata per scopi normativi e di governance.

Una singola licenza autorizza l'utilizzo di SnapLock in modalità rigorosa *conformità*, per soddisfare requisiti esterni come la norma SEC 17a-4(f) e una modalità più flessibile *Enterprise,* per rispettare le normative interne per la protezione delle risorse digitali. SnapLock utilizza un *ComplianceClock* a prova di manomissione per determinare quando è trascorso il periodo di conservazione di un file WORM.

È possibile utilizzare *SnapLock per SnapVault* per proteggere le snapshot su storage secondario mediante WORM. È possibile utilizzare SnapMirror per replicare i file WORM in un'altra posizione geografica per il disaster recovery e altri scopi.



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

Informazioni sul copyright

Informazioni sul marchio commerciale