



Report tecnici di ONTAP

ONTAP Technical Reports

NetApp

January 23, 2026

This PDF was generated from <https://docs.netapp.com/it-it/ontap-technical-reports/index.html> on January 23, 2026. Always check docs.netapp.com for the latest.

Sommario

Report tecnici di ONTAP	1
Report tecnici su ONTAP e applicazioni e database	2
Microsoft SQL Server	2
MySQL	2
Oracle	2
PostgreSQL	4
SAP HANA	4
EPIC	4
Report tecnici sulla business continuity	5
SnapMirror Active Sync (in precedenza SM-BC)	5
MetroCluster	5
Report tecnici su disaster recovery e data Protection di ONTAP	6
SnapMirror	6
Applicazione e infrastruttura con SnapMirror	6
Cyber vault di ONTAP	6
Report tecnici su volumi ONTAP FlexCache e FlexGroup	8
FlexCache	8
Write-back di FlexCache	8
Volumi FlexGroup	8
Report tecnici su NAS di ONTAP	9
NFS	9
PMI	9
Multiprotocollo	9
ONTAP S3	9
Servizi di nome	9
Sicurezza NAS	10
Report tecnici sulle reti di ONTAP	11
Report tecnici SAN di ONTAP	12
Sicurezza	13
Report tecnici sulla sicurezza di ONTAP	13
Cyber vault di ONTAP	13
Ransomware	13
Zero Trust	13
Autenticazione a più fattori	13
Multi-tenancy	14
Standard	14
Controllo degli accessi basato su attributi	14
Soluzione NetApp per i ransomware	14
Il portfolio di protezione di NetApp e ransomware	14
SnapLock e snapshot a prova di manomissione per la protezione dal ransomware	17
Blocco dei file FPolicy	18
Data Infrastructure Insights, sicurezza del carico di lavoro e dello storage	19
Rilevazione e risposta NetApp ONTAP integrate on-box basata su ai	20

Protezione DA WORM a mappatura D'aria con cyber vaulting in ONTAP	21
Protezione dal ransomware di Digital Advisor	22
Resilienza completa con la protezione ransomware NetApp	23
NetApp e zero trust	24
NetApp e zero trust	24
Progetta un approccio incentrato sui dati a Zero Trust con ONTAP	26
Controlli di orchestrazione e automazione della sicurezza NetApp esterni a ONTAP	30
Implementazioni di cloud ibrido e zero trust	31
Controllo degli accessi basato su attributi	31
Controllo degli accessi basato su attributi con ONTAP	31
Approcci al controllo di accesso basato sugli attributi (ABAC) in ONTAP	32
Protezione avanzata	45
Guide alla protezione avanzata di ONTAP	45
Guide per la protezione avanzata	45
Linee guida per la protezione avanzata di ONTAP	45
Panoramica sulla protezione avanzata di ONTAP	45
Convalida dell'immagine ONTAP	46
Account degli amministratori dello storage locali	46
Metodi di amministrazione del sistema	62
Protezione autonoma dal ransomware di ONTAP	68
Controllo del sistema amministrativo di storage	68
Crittografia dello storage in ONTAP	70
Crittografia replica dei dati	72
Crittografia dati in-flight IPSec	73
Modalità FIPS e gestione TLS e SSL in ONTAP	74
Creare un certificato digitale con firma CA	76
Protocollo di stato del certificato in linea	77
Gestione SSHv2	77
NetApp AutoSupport	78
Network Time Protocol	79
Account locali del file system NAS (gruppo di lavoro CIFS)	79
Auditing del file system NAS	80
Configurazione e attivazione della firma e della sigillatura SMB CIFS	82
Sicurezza NFS	83
Abilitare la firma e la sigillatura del protocollo Lightweight Directory Access Protocol	85
Creare e utilizzare un NetApp FPolicy	86
Caratteristiche di sicurezza dei ruoli LIF in ONTAP	87
Sicurezza del protocollo e delle porte	88
Report tecnici di ONTAP SnapCenter	92
SnapCenter per Oracle	92
SnapCenter per Microsoft SQL Server	92
SnapCenter per server Microsoft Exchange	92
SnapCenter per SAP HANA	92
Guida alla protezione avanzata di SnapCenter	93
Report tecnici sul tiering ONTAP	94

Report tecnici sulla virtualizzazione di ONTAP	95
Note legali	97
Copyright	97
Marchi	97
Brevetti	97
Direttiva sulla privacy	97
Open source	97
ONTAP	97
ONTAP Mediator per configurazioni IP MetroCluster	97

Report tecnici di ONTAP

Report tecnici su ONTAP e applicazioni e database

ONTAP è la base per la gestione dei dati e la protezione dei dati per molte applicazioni aziendali e tecnologie di database. I seguenti report tecnici forniscono indicazioni sulle procedure di implementazione e sulle procedure consigliate da NetApp per Microsoft SQL Server, MySQL, Oracle, PostgreSQL, SAP HANA ed Epic.

Microsoft SQL Server

SQL Server è la base della piattaforma dati di Microsoft, che offre prestazioni mission-critical con tecnologie in memoria e informazioni più rapide su qualsiasi dato, sia in sede che nel cloud.

["Best practice per Microsoft SQL Server con ONTAP"](#) Scopri come gli amministratori dello storage e dei database possono implementare con successo Microsoft SQL Server sullo storage ONTAP.



Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4590: Best practice guide for Microsoft SQL Server with ONTAP*.

["TR-4976: Performance virtualizzate di Microsoft SQL Server su sistemi NetApp AFF A-Series e C-Series"](#)

Scopri le caratteristiche delle performance di Microsoft SQL Server utilizzando i sistemi NetApp AFF A-Series e C-Series e ottieni indicazioni su come scegliere il sistema giusto in base al carico di lavoro.

["TR-4714: Best practice per Microsoft SQL Server con SnapCenter"](#)

Scopri ora come implementare con successo Microsoft SQL Server sullo storage ONTAP utilizzando la tecnologia SnapCenter per la protezione dei dati.

MySQL

Questo documento descrive i requisiti di configurazione e fornisce istruzioni sull'ottimizzazione e la configurazione dello storage per l'implementazione di MySQL su ONTAP.

["Database MySQL su Best practice NetApp ONTAP"](#) MySQL e le sue varianti, tra cui MariaDB e Percona, sono ampiamente utilizzati per molte applicazioni aziendali. Queste applicazioni spaziano dai siti di social networking globali ai sistemi di e-commerce di grandi dimensioni ai sistemi di hosting per PMI contenenti migliaia di istanze di database. Scopri i requisiti di configurazione e le indicazioni per l'ottimizzazione e la configurazione dello storage per l'implementazione di MySQL su ONTAP.



Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4722: Database MySQL sulle Best practice NetApp ONTAP*.

Oracle

ONTAP è progettato per i database Oracle. Per decenni, ONTAP è stato ottimizzato per le esigenze uniche di i/o dei database relazionali e sono state create più funzionalità di ONTAP appositamente per soddisfare le esigenze dei database Oracle e persino su richiesta della stessa Oracle Inc.

["Database Oracle su ONTAP"](#) Scopri le procedure consigliate che consentono agli amministratori dello storage e dei database di implementare con successo lo storage Oracle su ONTAP.

["Data Protection di Oracle con ONTAP"](#) Scopri le procedure consigliate che consentono agli amministratori dello storage e dei database di eseguire correttamente il backup, il ripristino, la replica e il disaster recovery su Oracle su storage ONTAP.

["Disaster recovery di Oracle con ONTAP"](#) Informazioni sulle procedure consigliate, sulle procedure di test e sulle altre considerazioni per il funzionamento dei database Oracle su un ambiente MetroCluster e SnapMirror Business Continuity.

["Migrazione dei database Oracle sui sistemi di storage ONTAP"](#) Scopri le considerazioni generali per la pianificazione di una strategia di migrazione, i tre diversi livelli di spostamento dei dati e consulta in dettaglio alcune delle varie procedure disponibili.



La documentazione sopra riportata sostituisce i report tecnici precedentemente pubblicati *TR-3633: Database Oracle su ONTAP*; *TR-4591: Data Protection Oracle: Backup, recovery, replica*; *TR-4592: Oracle su MetroCluster*; e *TR-4534: Migrazione dei database Oracle sui sistemi di storage NetApp*

["TR-4969: Performance dei database Oracle su AFF A-Series e C-Series"](#)

ONTAP è una potente piattaforma per la gestione dei dati con funzionalità native che includono compressione inline, aggiornamenti hardware senza interruzioni e la possibilità di importare un LUN da uno storage array esterno. È possibile eseguire il clustering di un massimo di 24 nodi, fornendo contemporaneamente i dati attraverso i protocolli NFS (Network file System), SMB (Server message Block), iSCSI, Fibre Channel (FC) e NVMe (Nonvolatile Memory Express). Inoltre, la tecnologia Snapshot è la base per la creazione di decine di migliaia di backup online e cloni di database completamente operativi. Oltre al ricco set di funzionalità di ONTAP, esistono una vasta gamma di requisiti per gli utenti, tra cui dimensioni del database, requisiti di performance e esigenze di protezione dei dati. Scopri le performance dei database bare metal utilizzando i sistemi storage AFF, inclusi I Sistemi A-Series e C-Series, e copre sia i massimi che la differenza pratica tra le due opzioni AFF.

["TR-4971: Performance del database Oracle virtualizzato su AFF A-Series e C-Series"](#)

ONTAP è una potente piattaforma per la gestione dei dati con funzionalità native che includono compressione inline, aggiornamenti hardware senza interruzioni e la possibilità di importare un LUN da uno storage array esterno. È possibile eseguire il clustering di un massimo di 24 nodi, fornendo contemporaneamente i dati attraverso i protocolli NFS (Network file System), SMB (Server message Block), iSCSI, Fibre Channel (FC) e NVMe (Nonvolatile Memory Express). Inoltre, la tecnologia Snapshot è la base per la creazione di decine di migliaia di backup online e cloni di database completamente operativi. Oltre al ricco set di funzionalità di ONTAP, esistono una vasta gamma di requisiti per gli utenti, tra cui dimensioni del database, requisiti di performance e esigenze di protezione dei dati. Scopri le performance dei database virtualizzati che utilizzano i sistemi storage AFF, inclusi I Sistemi A-Series e C-Series, e copre sia i massimi che la differenza pratica tra le due opzioni AFF.

["TR-4695: Tiering dello storage del database con FabricPool"](#)

Scopri i vantaggi e le opzioni di configurazione di FabricPool con diversi database, incluso il sistema di gestione dei database relazionali Oracle (RDBMS).

["TR-4899: Failover applicativo trasparente per i database Oracle con sincronizzazione attiva SnapMirror"](#)

SnapMirror Active Sync (in precedenza SM-BC) e Oracle Real Application Cluster (RAC) offrono failover dell'applicazione trasparente (TAF) e continuità in caso di black-out e disastri reali. Scopri la guida alla configurazione e le procedure consigliate di uno storage array AFF con SnapMirror Active Sync come componente di storage di Oracle RAC.

["TR-4876: Best practice per la soluzione e l'implementazione della multitenancy Oracle con ONTAP"](#)

Scopri le procedure consigliate per il provisioning, la gestione e la protezione dei database multi-tenant Oracle utilizzando lo storage ONTAP per massimizzare i vantaggi dei database multi-tenant Oracle e delle funzionalità

del software ONTAP.

PostgreSQL

PostgreSQL viene fornito con varianti che includono PostgreSQL, PostgreSQL Plus ed EDB Postgres Advanced Server (ECAS). PostgreSQL viene in genere distribuito come database back-end per applicazioni multi-Tier. NetApp ONTAP è una scelta eccellente per l'esecuzione di database PostgreSQL per la sua affidabilità, prestazioni elevate ed efficienza di gestione dei dati.

"Database PostgreSQL sulle Best practice di ONTAP" PostgreSQL viene fornito con varianti che includono PostgreSQL, PostgreSQL Plus e EDB Postgres Advanced Server (EPAS). PostgreSQL viene in genere implementato come database back-end per applicazioni multi-Tier. È supportato da pacchetti middleware comuni (come PHP, Java, Python, Tcl/TK, ODBC, E JDBC) ed è stata storicamente una scelta popolare per i sistemi di gestione di database open-source. Scopri i requisiti di configurazione e le istruzioni per l'ottimizzazione e la configurazione dello storage per l'implementazione di PostgreSQL su ONTAP.



Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-4770: Database PostgreSQL sulle Best practice ONTAP*.

SAP HANA

"Soluzioni per i database SAP HANA su ONTAP" Le Best practice per la configurazione, la gestione e l'automazione delle soluzioni SAP sono disponibili nella pagina soluzioni SAP di NetApp.

EPIC

"Best practice di EPIC su ONTAP" Una guida per comprendere le Best practice per implementare Epic on-premise e nel cloud, rispettando al contempo gli standard di configurazione per una corretta implementazione su ONTAP.



Questa documentazione sostituisce il report tecnico precedentemente pubblicato *TR-3923: Best practice NetApp per Epic*.

Report tecnici sulla business continuity

NetApp offre un'ampia gamma di soluzioni che razionalizzano la posizione in cui risiedono applicazioni e dati per migliorare le performance in modo conveniente. Data Protection, replica e disponibilità continua: La gestione dei dati di ONTAP può semplificare la data Protection con una gestione delle policy set-it-and-forget-it, offrendo business continuity con MetroCluster e SnapMirror Active Sync.



Questi report tecnici si espandono nella "[Sincronizzazione attiva di ONTAP SnapMirror](#)" documentazione di e "[ONTAP MetroCluster](#)" del prodotto.

SnapMirror Active Sync (in precedenza SM-BC)

["TR-4878: Sincronizzazione attiva SnapMirror"](#) SnapMirror Active Sync è una soluzione storage continuamente disponibile con granularità a livello dell'applicazione, disponibile per ONTAP sui sistemi storage AFF o All SAN Array (ASA), per soddisfare le esigenze RPO 0 e RTO 0 delle applicazioni business più critiche.

MetroCluster

["TR-4705: Architettura e progettazione della soluzione NetApp MetroCluster"](#)

Questo documento descrive l'architettura di alto livello e i concetti di progettazione per le funzionalità di MetroCluster in ONTAP.

MetroCluster IP (IP WAN)

["TR-4689: IP NetApp MetroCluster"](#) MetroCluster è una soluzione storage sempre disponibile per ONTAP eseguito su sistemi FAS e AFF. MetroCluster IP è l'ultima evoluzione che utilizza un fabric di storage back-end basato su Ethernet. MetroCluster IP offre una configurazione altamente ridondante per soddisfare le esigenze delle applicazioni aziendali più critiche. MetroCluster IP è incluso in ONTAP e fornisce connettività NAS e SAN per client e server che utilizzano lo storage ONTAP.

FC MetroCluster

["TR-4375: FC NetApp MetroCluster"](#) MetroCluster offre una disponibilità dei dati continua in data center separati geograficamente per applicazioni mission-critical. Scopri le procedure consigliate da MetroCluster FC, le decisioni di progettazione e le configurazioni supportate.

Report tecnici su disaster recovery e data Protection di ONTAP

SnapMirror è una soluzione di replica unificata conveniente e facile da utilizzare per tutto il data fabric. Replica i dati ad alta velocità su LAN o WAN. Ottieni un'elevata disponibilità dei dati e una rapida replica dei dati per le tue applicazioni business-critical, come Microsoft Exchange, Microsoft SQL Server e Oracle, in ambienti virtuali e tradizionali. Quando si replicano i dati su uno o più sistemi storage ONTAP e si aggiornano continuamente i dati secondari, i dati vengono mantenuti aggiornati e disponibili ogni volta che ne hai bisogno. Non sono richiesti server di replica esterni.



Questi report tecnici si espandono nella "ONTAP protezione dei dati e disaster recovery" documentazione del prodotto.

SnapMirror

Connessione asincrona SnapMirror

"[TR-4015: Configurazione asincrona e Best practice di SnapMirror](#)" Scopri le procedure consigliate per la configurazione della replica asincrona di volumi, gruppi di coerenza e Storage Virtual Machine (disaster recovery delle SVM) con SnapMirror.

"[TR-4678: Protezione dei dati e backup dei volumi ONTAP FlexGroup](#)"

Scopri la protezione dei dati e il backup consigliati per i volumi FlexGroup. Gli argomenti includono copie Snapshot, SnapMirror e altre soluzioni di backup e protezione dei dati.

SnapMirror sincrono

"[TR-4733: Configurazione sincrona e Best practice di SnapMirror](#)" Scopri le procedure consigliate per la configurazione della replica sincrona di SnapMirror (SM-S).

Dr dei tre data center SnapMirror

"[TR-4832: Disaster recovery per tre data center con SnapMirror di NetApp per ONTAP 9.7](#)" Scopri una configurazione di disaster recovery di tre data center che utilizza la tecnologia ONTAP SnapMirror per la replica.

Applicazione e infrastruttura con SnapMirror

"[TR-4900: VMware Site Recovery Manager con ONTAP](#)" ONTAP è una soluzione storage leader per gli ambienti VMware vSphere fin dall'introduzione nel moderno data center nel 2002 e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo i costi. Informazioni sulla soluzione ONTAP consigliata per VMware Site Recovery Manager (SRM), il software di disaster recovery (DR) leader del settore di VMware, incluse le informazioni più recenti sui prodotti e le procedure consigliate per semplificare la distribuzione, ridurre i rischi e semplificare la gestione continua.

Cyber vault di ONTAP

"[Cyber vault di ONTAP](#)" Il cyber vault di NetApp basato su ONTAP fornisce alle organizzazioni una soluzione completa e flessibile per proteggere le loro risorse dati più critiche. Sfruttando l'air-gapping logico con solide metodologie di potenziamento, ONTAP ti consente di creare ambienti storage sicuri e isolati in grado di

resistere alle minacce informatiche in evoluzione. Con ONTAP, puoi garantire la riservatezza, l'integrità e la disponibilità dei tuoi dati mantenendo al contempo l'agilità e l'efficienza della tua infrastruttura storage.

Report tecnici su volumi ONTAP FlexCache e FlexGroup

Le soluzioni NAS di NetApp semplificano la gestione dei dati e ti aiutano a tenere il passo con la crescita, ottimizzando al contempo i costi. Le soluzioni NAS di ONTAP offrono operazioni senza interruzioni, efficienza comprovata e scalabilità perfetta all'interno di un'architettura unificata. Basato su ONTAP, il NAS scale-out sfrutta l'enorme ecosistema ONTAP, con un significativo vantaggio in termini di innovazione e una visione per un'innovazione futura aggressiva.



Questi report tecnici si espandono nella "["Volume ONTAP FlexCache"](#)" documentazione di e "["Volume ONTAP FlexGroup"](#)" del prodotto.

FlexCache

["TR-4743: FlexCache in ONTAP"](#)

FlexCache è una tecnologia di caching che crea repliche di volumi sparse e scrivibili sullo stesso cluster ONTAP o su cluster diversi. Consente di avvicinare dati e file all'utente per un throughput più rapido con un ingombro ridotto. Scopri come utilizzare FlexCache, le procedure consigliate, i limiti e le considerazioni per la progettazione e l'implementazione.

Write-back di FlexCache

["Write-back di FlexCache"](#) Introdotto in ONTAP 9.15.1, FlexCache write-back è una modalità operativa alternativa per la scrittura in una cache. La funzione write-back consente il commit della scrittura nello storage stabile nella cache e il riconoscimento al client senza attendere che i dati giungano all'origine. I dati vengono sottoposti nuovamente all'origine in modo asincrono. Il risultato è un file system distribuito a livello globale che consente alle scritture di operare a velocità quasi locali per carichi di lavoro e ambienti specifici, offrendo benefici di performance significativi.

Volumi FlexGroup

["TR-4571a: Le dieci Best practice di FlexGroup"](#)

Questo report tecnico è una versione condensata di TR-4571: Best practice e guida all'implementazione di NetApp ONTAP FlexGroup Volumes per un consumo rapido.

["TR-4557: NetApp ONTAP FlexGroup Volumes - Panoramica tecnica"](#)

Scopri FlexGroup Volumes, un container NAS scale-out di ONTAP, che unisce capacità quasi infinita con performance prevedibili e a bassa latenza in carichi di lavoro con elevati carichi di metadati.

["TR-4571: Best practice e guida all'implementazione di NetApp ONTAP FlexGroup Volumes"](#)

Scopri i volumi FlexGroup, le procedure consigliate e i suggerimenti per l'implementazione. I volumi FlexGroup sono un'evoluzione dei container NAS scale-out di ONTAP, che combina capacità quasi infinita con performance prevedibili e a bassa latenza in carichi di lavoro con carichi di lavoro elevati di metadati.

["TR-4678: Protezione dei dati e backup dei volumi FlexGroup"](#)

Scopri di più sulla protezione dei dati e sul backup per i volumi FlexGroup, tra cui copie Snapshot, SnapMirror e altre soluzioni di backup e protezione dei dati.

Report tecnici su NAS di ONTAP

Le soluzioni NAS di NetApp semplificano la gestione dei dati e ti aiutano a tenere il passo con la crescita, ottimizzando al contempo i costi. Le soluzioni NAS di ONTAP offrono operazioni senza interruzioni, efficienza e scalabilità perfetta all'interno di un'architettura unificata. Basato su NetApp ONTAP, il NAS scale-out sfrutta l'enorme ecosistema ONTAP, con un significativo vantaggio in termini di innovazione e una visione per un'innovazione futura aggressiva.



Questi report tecnici si espandono nella "["Gestione dello storage NAS ONTAP"](#)" documentazione di e "["Gestione dello storage ONTAP S3"](#)" del prodotto.

NFS

["TR-4067: Best practice e guida all'implementazione di NFS in ONTAP"](#)

Scopri i concetti di base, le informazioni di supporto, i suggerimenti per la configurazione e le procedure consigliate per NFS in ONTAP.

["TR-4962: Attributi estesi NFSv4.2"](#)

Scopri come abilitare e utilizzare gli attributi estesi NFSv4.2 in ONTAP 9.12.1 e versioni successive.

PMI

["TR-4740: SMB 3.0 multicanale"](#)

Microsoft ha introdotto multicannel protocollo SMB 3.0 con l'obiettivo di migliorare il protocollo SMB3 affrontando le limitazioni di performance e affidabilità di SMB1 e SMB2. Scopri la funzionalità multicanale di ONTAP, incluse le funzionalità, le procedure consigliate e i risultati dei test delle performance.

Multiprotocollo

["TR-4887: Panoramica e Best practice del NAS multiprotocollo in ONTAP"](#)

Scopri come funziona l'accesso NAS multiprotocollo in ONTAP e le procedure consigliate per gli ambienti multiprotocollo.

ONTAP S3

["TR-4814: Best practice S3 in ONTAP"](#) Scopri le pratiche consigliate per l'utilizzo di Amazon Simple Storage Service (S3) con il software ONTAP oltre a funzionalità e configurazioni per l'utilizzo di ONTAP come archivio di oggetti con applicazioni S3 native o come destinazione di tiering per FabricPool.

Servizi di nome

["TR-4523: Bilanciamento del carico DNS in ONTAP"](#)

Scopri come configurare ONTAP per l'utilizzo con metodologie di bilanciamento del carico DNS, tra cui DNS in ONTAP, vari metodi di configurazione e procedure consigliate.

["TR-4668: Guida alle Best practice per i name service"](#)

Scopri le procedure, i limiti e le considerazioni consigliate per l'implementazione di soluzioni NAS (Network-

Attached Storage) come CIFS/SMB e NFS in ONTAP.

[**"TR-4835: Come configurare LDAP nella gestione delle identità NAS multiprotocollo di ONTAP"**](#)

Scopri come configurare la gestione delle identità LDAP (Lightweight Directory Access Protocol) in ONTAP per NAS multiprotocollo.

Sicurezza NAS

[**"TR-4616: NFS Kerberos in ONTAP"**](#)

Scopri di più su NFS Kerberos in ONTAP, incluse le fasi di configurazione con Active Directory e i client Red Hat Enterprise Linux (RHEL).

Report tecnici sulle reti di ONTAP

ONTAP offre diverse funzionalità e configurazioni di rete per soddisfare le applicazioni scale-out più esigenti. Utilizzando le funzionalità e le funzionalità di rete, le aziende possono creare un accesso affidabile e sicuro ai propri dati.



Questi report tecnici si espandono nella "[Gestione della rete ONTAP](#)" documentazione del prodotto.

["TR-4949: BGP/VIP con ONTAP nel data center"](#)

Scopri come implementare rapidamente una configurazione BGP di base in ONTAP.

Report tecnici SAN di ONTAP

Lo storage SAN ONTAP offre un'esperienza SAN semplificata che fornisce alta disponibilità per i database mission-critical della tua organizzazione e altri workload SAN. Grazie all'integrazione dei servizi dati Best-in-class con database Oracle, SAP e Microsoft SQL Server, oltre a VMware e altri hypervisor leader del settore, ONTAP SAN offre un time-to-value accelerato per le applicazioni di database aziendali.



Questi report tecnici si espandono nella "[Gestione dello storage SAN ONTAP](#)" documentazione del prodotto.

["TR-4080: Best practice per LE SAN moderne in ONTAP"](#)

Scopri i protocolli a blocchi in ONTAP e le procedure consigliate.

["TR-4684: Implementazione e configurazione di SAN moderne con NVMe over Fabrics \(NVMe-of\)"](#)

Scopri come implementare e configurare NVMe sui trasporti di fabric (NVMe su Fibre Channel e NVMe su TCP). Gli argomenti trattati includono le linee guida di progettazione, implementazione, configurazione, gestione e le procedure consigliate per creare soluzioni SAN moderne ad alta disponibilità e performance utilizzando i protocolli e i trasporti NVMe.

["TR-4968: Integrità e disponibilità dei dati dell'array all-SAN NetApp"](#)

Scopri in che modo le varie funzionalità di protezione dei dati e integrità dei dati di un array all SAN funzionano per ottenere il massimo uptime delle applicazioni e le procedure consigliate per la progettazione, l'implementazione e la gestione di una rete SAN.

["Moderna soluzione flash SAN connessa al cloud"](#)

Questa architettura verificata da NetApp è stata progettata e verificata congiuntamente da NetApp, VMware e Broadcom. Utilizza le più recenti soluzioni tecnologiche Brocade, Emulex e VMware vSphere insieme allo storage all-flash NetApp, che definisce un nuovo standard per lo storage SAN aziendale e la protezione dei dati che favorirà un valore di business superiore.

Sicurezza

Report tecnici sulla sicurezza di ONTAP

ONTAP continua a evolversi, con la sicurezza come parte integrante della soluzione. Le ultime versioni di ONTAP contengono molte nuove funzionalità di sicurezza che sono preziose per la tua organizzazione per proteggere i propri dati nel cloud ibrido, prevenire gli attacchi ransomware e rispettare le pratiche consigliate dal settore. Queste nuove funzionalità supportano anche il passaggio dell'organizzazione verso un modello Zero Trust.



Questi report tecnici si espandono nella "["Sicurezza ONTAP e crittografia dei dati"](#) documentazione del prodotto.

Cyber vault di ONTAP

"Cyber vault di ONTAP" Il cyber vault di NetApp basato su ONTAP fornisce alle organizzazioni una soluzione completa e flessibile per proteggere le loro risorse dati più critiche. Sfruttando l'air-gapping logico con solide metodologie di potenziamento, ONTAP ti consente di creare ambienti storage sicuri e isolati in grado di resistere alle minacce informatiche in evoluzione. Con ONTAP, puoi garantire la riservatezza, l'integrità e la disponibilità dei tuoi dati mantenendo al contempo l'agilità e l'efficienza della tua infrastruttura storage.

Ransomware

"TR-4572: La soluzione NetApp per ransomware" Scopri come si è evoluto il ransomware e come identificare gli attacchi, prevenire la diffusione e ripristinare il più rapidamente possibile utilizzando la soluzione NetApp per i ransomware. Le linee guida e le soluzioni fornite in questo documento sono progettate per aiutare le organizzazioni a disporre di soluzioni resistenti dal punto di vista informatico, rispettando al contempo gli obiettivi di sicurezza prescritti in termini di riservatezza, integrità e disponibilità dei sistemi informatici.

"TR-4526: Storage WORM conforme con NetApp SnapLock"

Molte aziende si affidano allo storage dei dati WORM (write once, Read Many) per soddisfare i requisiti di conformità alle normative o semplicemente per aggiungere un altro livello alla propria strategia di protezione dei dati. Scopri come integrare SnapLock, la soluzione WORM di ONTAP, in ambienti che richiedono lo storage dei dati WORM.

Zero Trust

"NetApp e zero trust" Zero Trust è tradizionalmente un approccio incentrato sulla rete per la progettazione di micro core e perimetro (MCAP) per la protezione di dati, servizi, applicazioni o asset con controlli noti come gateway di segmentazione. ONTAP adotta un approccio incentrato sui dati a Zero Trust, in cui il sistema di gestione dello storage diventa il gateway di segmentazione per proteggere e monitorare l'accesso ai dati del cliente. In particolare, il motore FPolicy Zero Trust e l'ecosistema di partner FPolicy diventano un centro di controllo per acquisire una comprensione dettagliata dei modelli di accesso ai dati normali e aberranti e identificare le minacce interne.

Autenticazione a più fattori

["TR-4647: Guida all'implementazione e Best practice per l'autenticazione multifattore in ONTAP"](#)

Scopri la funzionalità di autenticazione multifattore di ONTAP per l'accesso amministrativo utilizzando Gestione

di sistema, Active IQ Unified Manager e l'autenticazione CLI di ONTAP Secure shell (SSH).

["TR-4717: Autenticazione SSH ONTAP con una scheda di accesso comune"](#)

Scopri come configurare e testare client SSH di terze parti, insieme al software ActivClient, per autenticare un amministratore dello storage ONTAP tramite la chiave pubblica memorizzata su una CAC (Common Access Card) quando è configurato in ONTAP.

Multi-tenancy

["TR-4160: Multi-tenancy sicura in ONTAP"](#)

Scopri come implementare la multi-tenancy sicura utilizzando le VM di storage in ONTAP, incluse considerazioni di progettazione e procedure consigliate.

Standard

["TR-4401: PCI-DSS 4.0 e ONTAP"](#)

Scopri come convalidare un sistema in base allo standard PCI DSS 4.0 e soddisfare i requisiti dei controlli applicati a un sistema NetApp ONTAP.

Controllo degli accessi basato su attributi

["Controllo degli accessi basato su attributi con ONTAP"](#) Scopri come configurare le etichette di sicurezza NFSv4,2 e gli attributi estesi (xattr) per supportare il role-based access control (RBAC) e il controllo degli accessi basato sugli attributi (ABAC), una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi di utenti, risorse e ambiente.

Soluzione NetApp per i ransomware

Il portfolio di protezione di NetApp e ransomware

Il ransomware resta una delle minacce più significative che causano l'interruzione del business per le organizzazioni nel 2024. Secondo il ["Sophos state of ransomware 2024"](#), gli attacchi ransomware hanno colpito il 72% dei partecipanti intervistati. Gli attacchi ransomware si sono evoluti per diventare più sofisticati e mirati, con i soggetti delle minacce che utilizzano tecniche avanzate come l'intelligenza artificiale per massimizzare il loro impatto e i loro profitti.

Le organizzazioni devono guardare nell'intera posizione di sicurezza da perimetro, rete, identità, applicazioni e dove si trovano i dati a livello di storage e mettere al sicuro questi layer. L'adozione di un approccio incentrato sui dati alla cyber Protection nel layer di storage è fondamentale nel panorama odierno delle minacce. Anche se non esiste una singola soluzione in grado di bloccare tutti gli attacchi, l'uso di un portfolio di soluzioni, inclusi partnership e terze parti, offre una difesa a più layer.

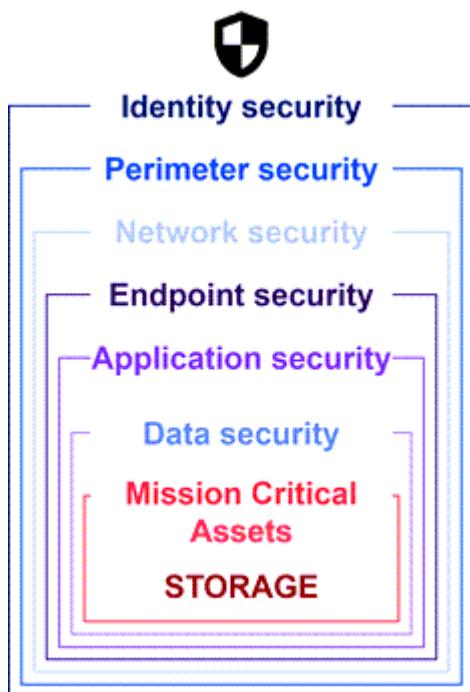
Portfolio di prodotti NetApp Fornisce vari strumenti efficaci per visibilità, rilevamento e correzione, in modo da rilevare tempestivamente il ransomware, prevenire la diffusione e ripristinare rapidamente, se necessario, per evitare costosi downtime. Le soluzioni di difesa tradizionali a layer rimangono le più diffuse, così come quelle di partner e terze parti per la visibilità e il rilevamento. Una correzione efficace rimane una parte fondamentale della risposta a qualsiasi minaccia. L'esclusivo approccio di settore che sfrutta la tecnologia Snapshot NetApp immutabile e la soluzione con interfaccia logica SnapLock è un fattore di differenziazione nel settore e una Best practice nel settore per le funzionalità di correzione dal ransomware.



A partire da luglio 2024, i contenuti del report tecnico *TR-4572: NetApp ransomware Protection*, precedentemente pubblicato come PDF, sono disponibili su docs.netapp.com.

I dati sono la destinazione primaria

I criminali informatici si rivolgono sempre più direttamente ai dati, riconoscendo il loro valore. Sebbene la sicurezza perimetrale, di rete e delle applicazioni siano importanti, è possibile ignorarle. La focalizzazione sulla protezione dei dati all'origine, il layer di storage, fornisce un'ultima linea critica di difesa. L'obiettivo degli attacchi ransomware è ottenere l'accesso ai dati di produzione, crittografarli o renderli inaccessibili. Per raggiungere questo obiettivo, gli autori degli attacchi devono aver già forato le difese esistenti implementate dalle organizzazioni oggi, dal perimetro alla sicurezza delle applicazioni.



Purtroppo, molte organizzazioni non sfruttano le funzionalità di sicurezza a livello di dati. È qui che entra in gioco il portfolio di protezione ransomware di NetApp, con la protezione che trovi all'ultima linea di difesa.

Il costo reale del ransomware

Il pagamento del riscatto in sé non costituisce l'effetto monetario più grande per un'azienda. Anche se il pagamento non è insignificante, sale in confronto al costo dei downtime dovuti alla sofferenza di un incidente ransomware.

I pagamenti dei riscatti sono solo un elemento dei costi di recovery legati agli eventi ransomware. Escludendo qualsiasi riscatto pagato, nel 2024 le organizzazioni hanno riferito un costo medio per il recovery da un attacco ransomware di 2,73M milioni di dollari, un aumento di quasi 1M milioni di dollari rispetto ai 1,82M milioni di dollari registrati nel 2023, secondo il "["2024 Sophos state of ransomware"](#)" report. Per le organizzazioni che dipendono fortemente dalla disponibilità IT, come l'e-commerce, il trading di azioni e l'assistenza sanitaria, i costi possono essere 10 volte superiori o più.

Anche i costi dell'assicurazione informatica continuano ad aumentare, considerata la verosimile probabilità che si verifichi un attacco ransomware sulle aziende assicurate.

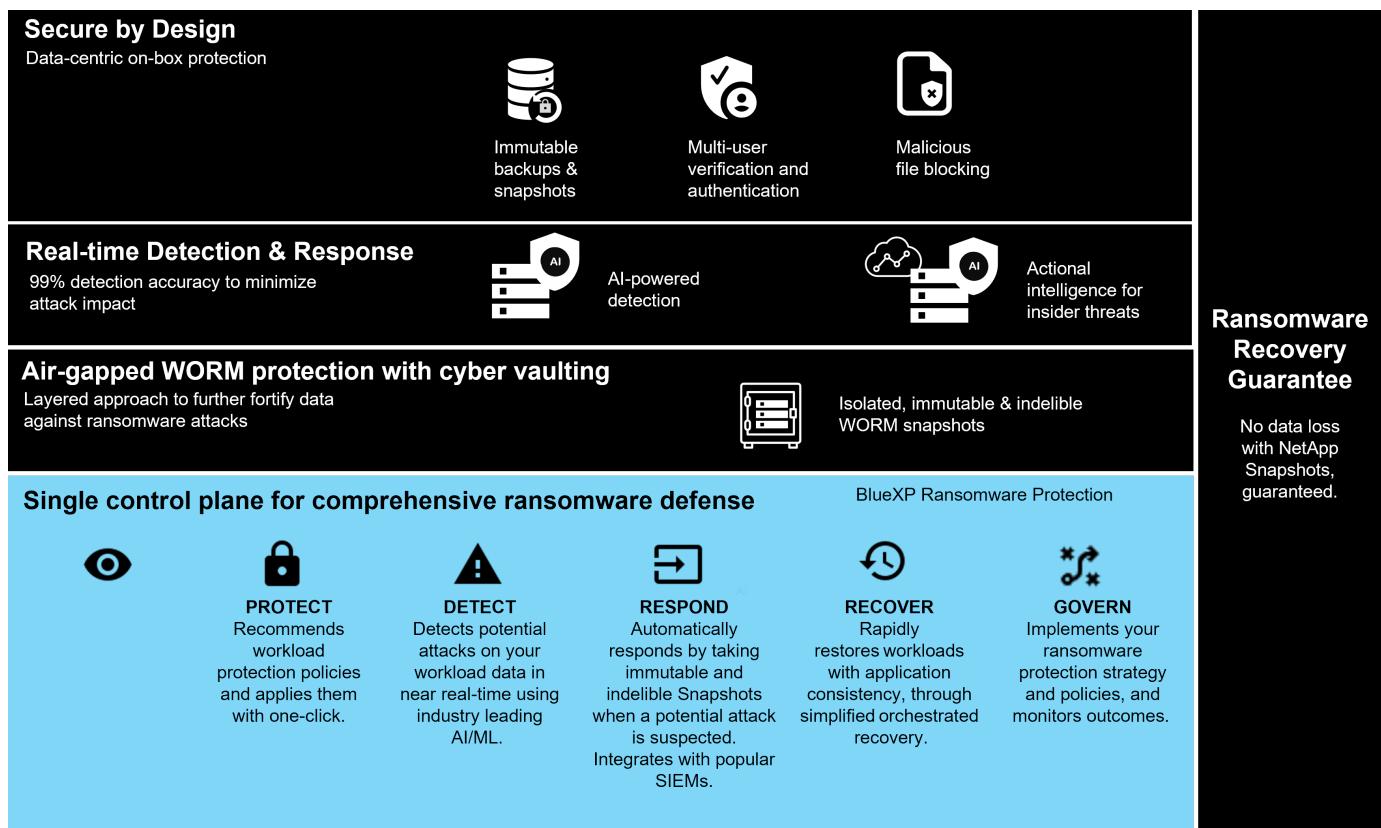
Protezione dal ransomware ai layer di dati

NetApp comprende che il tuo livello di sicurezza è ampio e profondo in tutta l'organizzazione, dal perimetro alla posizione in cui risiedono i dati nel layer di storage. Lo stack di sicurezza è complesso e dovrebbe fornire sicurezza a ogni livello dello stack tecnologico.

La protezione in real-time a livello di dati è ancora più importante e ha requisiti specifici. Per essere efficaci, le soluzioni di questo livello devono offrire questi attributi critici:

- **Sicurezza per progettazione** per ridurre al minimo la possibilità di un attacco riuscito
- **Rilevamento e risposta in tempo reale** per ridurre al minimo l'impatto di un attacco riuscito
- **Protezione WORM a mappatura D'aria** per isolare i backup dei dati critici
- **Un singolo piano di controllo** per una difesa ransomware completa

NetApp è in grado di offrire tutto questo e molto altro.



Il portfolio di protezione dal ransomware di NetApp

NetApp "protezione dal ransomware integrata" offre una difesa real-time, solida e sfaccettata per i tuoi dati critici. Al centro, gli algoritmi di rilevamento avanzati basati sull'AI monitorano costantemente i modelli di dati, identificando rapidamente le potenziali minacce ransomware con una precisione del 99%. La rapida reazione agli attacchi consente al nostro storage di creare rapidamente un snapshot dei dati e di proteggere le copie, garantendo un rapido recovery.

Per rafforzare ulteriormente i dati, "replica informatica" la capacità di NetApp isola i dati con un'air gap logica. Salvaguardando i dati critici, garantiamo una rapida business continuity.

NetApp "Protezione ransomware NetApp" riduce gli oneri operativi con un singolo piano di controllo per coordinare ed eseguire in modo intelligente una difesa ransomware end-to-end incentrata sul carico di lavoro,

in modo da poter identificare e proteggere i dati critici del carico di lavoro a rischio con un solo clic, rilevare e rispondere in modo accurato e automatico per limitare l'impatto di un potenziale attacco e ripristinare i carichi di lavoro in pochi minuti, non in giorni, salvaguardando i preziosi dati del carico di lavoro e riducendo al minimo le costose interruzioni.

In qualità di soluzione ONTAP integrata e nativa per la protezione degli accessi non autorizzati ai dati, "["Verifica multi-admin \(MAV\)"](#)" dispone di un solido set di funzionalità che garantiscono l'esecuzione di operazioni quali l'eliminazione di volumi, la creazione di ulteriori utenti amministrativi o l'eliminazione di snapshot solo dopo le approvazioni di almeno un secondo amministratore designato. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati. È possibile configurare tutti i responsabili dell'approvazione dell'amministratore designati che si desidera prima di eliminare uno snapshot.



NetApp ONTAP soddisfa i requisiti per l' "["Autenticazione a più fattori \(MFA\)"](#)" autenticazione CLI basata su web in System Manager e SSH.

La protezione dal ransomware di NetApp offre tranquillità in un panorama di minacce in continua evoluzione. Il suo approccio completo non solo si difende dalle attuali varianti di ransomware, ma si adatta anche alle minacce emergenti, garantendo sicurezza a lungo termine per la tua infrastruttura dati.

Ulteriori informazioni sulle altre opzioni di protezione

- "["Protezione dal ransomware di Digital Advisor"](#)"
- "["Data Infrastructure Insights, sicurezza del carico di lavoro e dello storage"](#)"
- "["FPolicy"](#)"
- "["SnapLock e snapshot a prova di manomissione"](#)"

Garanzia di recovery dal ransomware

NetApp offre una garanzia di ripristino dei dati Snapshot in caso di attacco ransomware. La nostra garanzia: Se non possiamo aiutarvi a ripristinare i vostri dati snapshot, noi lo faremo. La garanzia è disponibile sui nuovi acquisti dei sistemi AFF A-Series, AFF C-Series, ASA e FAS.

Scopri di più

- "["Descrizione del servizio di garanzia di recupero"](#)"
- "["Blog sulla garanzia di recovery dal ransomware"](#)".

Informazioni correlate

- "["Pagina delle risorse del sito di supporto NetApp"](#)"
- "["Sicurezza dei prodotti NetApp"](#)"

SnapLock e snapshot a prova di manomissione per la protezione dal ransomware

Un'arma vitale nell'arsenale Snap di NetApp è SnapLock, che si è dimostrato altamente efficace nel proteggere dalle minacce ransomware. Prevenendo la cancellazione non autorizzata dei dati, SnapLock fornisce un ulteriore livello di sicurezza, garantendo che i dati critici rimangano intatti e accessibili anche in caso di attacchi dannosi.

Conformità SnapLock

SnapLock Compliance (SLC) fornisce una protezione indelebile dei tuoi dati. SLC impedisce l'eliminazione dei

dati anche quando un amministratore tenta di reinizializzare l'array. A differenza di altri prodotti della concorrenza, SnapLock Compliance non è vulnerabile agli attacchi di social engineering attraverso i team di supporto di questi prodotti. I dati protetti da SnapLock Compliance Volumes sono ripristinabili fino a quando tali dati non hanno raggiunto la data di scadenza.

Per abilitare SnapLock, "[ONTAP uno](#)" è necessaria una licenza.

Scopri di più

- ["Documentazione SnapLock"](#)

Snapshot a prova di manomissione

Le copie Snapshot a prova di manomissione (TPS) offrono un modo rapido e pratico per proteggere i dati da atti dannosi. A differenza di SnapLock Compliance, il TPS viene in genere utilizzato sui sistemi primari in cui l'utente può proteggere i dati per un determinato periodo di tempo e lasciato localmente per ripristini rapidi o in cui i dati non devono essere replicati dal sistema primario. TPS utilizza le tecnologie SnapLock per impedire l'eliminazione dello snapshot primario anche da parte di un amministratore ONTAP che utilizza lo stesso periodo di scadenza della conservazione SnapLock. L'eliminazione degli Snapshot viene evitata anche se il volume non è abilitato per SnapLock, sebbene gli snapshot non abbiano la stessa natura indelebile dei volumi SnapLock Compliance.

Per rendere gli snapshot a prova di manomissione, è necessaria una "[ONTAP uno](#)" licenza.

Scopri di più

- ["Bloccare una snapshot per la protezione dagli attacchi ransomware"](#).

Blocco dei file FPolicy

FPolicy blocca la memorizzazione dei file indesiderati nell'appliance di storage Enterprise. FPolicy ti offre inoltre un modo per bloccare le estensioni di file ransomware note. Un utente dispone ancora delle autorizzazioni di accesso completo alla cartella principale, ma FPolicy non consente a un utente di memorizzare i file contrassegnati dall'amministratore come bloccati. Non importa se quei file sono file MP3 o estensioni note di file ransomware.

Blocco dei file dannosi con la modalità nativa di FPolicy

La modalità nativa di NetApp FPolicy (un'evoluzione del nome, file Policy) è un framework di blocco delle estensioni di file che consente di impedire che estensioni di file indesiderate entrino nell'ambiente. Fa parte di ONTAP da oltre dieci anni ed è incredibilmente utile per aiutarti a protegerti dai ransomware. Questo motore Zero Trust è utile perché offre ulteriori misure di sicurezza oltre i permessi dell'elenco di controllo degli accessi (ACL).

In ONTAP System Manager e nella NetApp Console è disponibile un elenco di oltre 3000 estensioni di file come riferimento.



Alcune estensioni potrebbero essere legittime nell'ambiente e il loro blocco può causare problemi imprevisti. Prima di configurare FPolicy nativo, creare un elenco personalizzato appropriato per l'ambiente in uso.

La modalità nativa FPolicy è inclusa in tutte le licenze ONTAP.

Scopri di più

- ["Blog: Combattere il ransomware: Parte tre — ONTAP FPolicy, un altro potente tool nativo \(anche noto come gratuito\)"](#)

Abilitare l'analisi del comportamento di utenti ed entità (UEBA) con la modalità esterna FPolicy

La modalità esterna FPolicy è un framework di controllo e notifica delle attività dei file che fornisce visibilità delle attività degli utenti e dei file. Queste notifiche possono essere utilizzate da una soluzione esterna per eseguire analytics basati su ai per rilevare comportamenti dannosi.

La modalità esterna FPolicy può anche essere configurata in modo da attendere l'approvazione dal server FPolicy prima di consentire l'esecuzione di attività specifiche. In un cluster è possibile configurare più policy di questo tipo, per una maggiore flessibilità.



I server FPolicy devono rispondere alle richieste FPolicy se configurati per fornire l'approvazione; altrimenti, le performance del sistema storage potrebbero avere un impatto negativo.

La modalità esterna FPolicy è inclusa in ["Tutte le licenze ONTAP"](#).

Scopri di più

- ["Blog: Combattere il ransomware: Parte quarta — UBA e ONTAP con modalità esterna FPolicy."](#)

Data Infrastructure Insights, sicurezza del carico di lavoro e dello storage

Storage Workload Security (SWS) è una funzionalità di NetApp Data Infrastructure Insights che migliora notevolmente la sicurezza, la recuperabilità e la responsabilità di un ambiente ONTAP . SWS adotta un approccio incentrato sull'utente, monitorando tutte le attività sui file di ogni utente autenticato nell'ambiente. Utilizza analisi avanzate per stabilire modelli di accesso normali e stagionali per ogni utente. Questi modelli vengono utilizzati per identificare rapidamente comportamenti sospetti senza bisogno di firme ransomware.

Quando SWS rileva un potenziale ransomware o l'eliminazione di dati, può intraprendere azioni automatiche come:

- Creare un'istantanea del volume interessato.
- Bloccare l'account utente e l'indirizzo IP sospettati di attività dannose.
- Inviare un avviso agli amministratori.

Poiché può intraprendere azioni automatizzate per fermare rapidamente una minaccia interna e tenere traccia di ogni attività dei file, SWS rende il recovery da un evento ransomware molto più semplice e veloce. Con gli strumenti avanzati di audit e analisi forense integrati, gli utenti possono vedere immediatamente quali volumi e file sono stati influenzati da un attacco, da quale account utente proviene l'attacco e da quale azione dannosa è stata eseguita. Gli snapshot automatici riducono i danni e accelerano il ripristino dei file.

Total Attack Results



1,488 Files have been copied, deleted, and potentially encrypted by **1 user account**.

This is potentially a sign of Ransomware Attack.

The extension ".wanna" was added to each file.

Gli avvisi della protezione autonoma da ransomware (ARP) di ONTAP sono visibili anche in SWS, che fornisce una singola interfaccia per i clienti che utilizzano sia ARP che SWS per proteggersi dagli attacchi ransomware.

Scopri di più

- ["Data Infrastructure Insights NetApp"](#)

Rilevazione e risposta NetApp ONTAP integrate on-box basata su ai

Mentre le minacce ransomware diventano sempre più sofisticate, i tuoi meccanismi di difesa dovrebbero farlo. La protezione autonoma da ransomware (ARP) di NetApp si basa sull'ai con rilevamento intelligente delle anomalie integrato in ONTAP. Attiva questa funzione per aggiungere un altro livello di difesa alla tua resilienza informatica.

ARP e ARP/ai sono configurabili tramite l'interfaccia di gestione integrata di ONTAP, System Manager, e abilitati in base al volume.

Protezione ransomware autonoma (ARP)

Protezione autonoma dal ransomware (ARP), un'altra soluzione nativa integrata nel ONTAP dal 9.10.1, analizza l'attività dei file di workload del volume di storage NAS e l'entropia dei dati per rilevare automaticamente il potenziale ransomware. ARP offre agli amministratori un rilevamento in tempo reale, informazioni approfondite e un punto di ripristino dei dati per un potenziale rilevamento ransomware on-box senza precedenti.

Per ONTAP 9.15.1 e le versioni precedenti che supportano ARP, ARP inizia in modalità di apprendimento per apprendere le attività tipiche dei dati del carico di lavoro. Questa operazione può richiedere sette giorni per la maggior parte degli ambienti. Una volta completata la modalità di apprendimento, ARP passerà automaticamente alla modalità attiva e inizierà a cercare attività anomale sui carichi di lavoro che potrebbero essere potenzialmente ransomware.

Se viene rilevata un'attività anomala, viene immediatamente acquisito uno snapshot automatico, che fornisce un punto di ripristino il più vicino possibile al momento dell'attacco con un numero minimo di dati infetti. Allo stesso tempo, viene generato un avviso automatico (configurabile) che consente agli amministratori di visualizzare le attività anomale dei file in modo che possano determinare se l'attività è effettivamente dannosa e intraprendere le azioni appropriate.

Se l'attività è un carico di lavoro previsto, gli amministratori possono facilmente contrassegnarla come un falso positivo. ARP apprende questo cambiamento come attività normale del carico di lavoro e non lo contrassegna più come un potenziale attacco in futuro.

Per attivare ARP, "[ONTAP uno](#)" è necessaria una licenza.

Scopri di più

- "["Protezione ransomware autonoma"](#)

Protezione autonoma da ransomware/ai (ARP/ai)

Introdotto come anteprima tecnica in ONTAP 9.15.1, ARP/ai porta il rilevamento in tempo reale on-box dei sistemi storage NAS a un livello superiore. La nuova tecnologia di rilevamento basata sull'ai è preparata su oltre un milione di file e vari attacchi ransomware noti. Oltre ai segnali utilizzati in ARP, ARP/ai rileva anche la cifratura dell'intestazione. La potenza ai e i segnali aggiuntivi consentono ad ARP/ai di fornire una precisione di rilevamento superiore al 99%. Questo è stato convalidato da se Labs, un laboratorio di test indipendente che ha assegnato ad ARP/ai la più alta classificazione AAA.

Poiché l'addestramento dei modelli avviene continuamente nel cloud, ARP/ai non richiede una modalità di apprendimento. È attivo nel momento in cui viene acceso. Il training continuo significa anche che l'ARP/ai è sempre validata a fronte di nuovi tipi di attacchi ransomware man mano che si presentano. ARP/ai include anche funzionalità di aggiornamento automatico che forniscono nuovi parametri a tutti i clienti per mantenere aggiornato il rilevamento del ransomware. Tutte le altre funzionalità di rilevazione, Insight e punto di recupero dati di ARP sono mantenute per ARP/ai.

Per abilitare ARP/ai, "[ONTAP uno](#)" è necessaria una licenza.

Scopri di più

- "["Blog: La soluzione di rilevamento ransomware in tempo reale basata su ai di NetApp ottiene una classificazione AAA"](#)

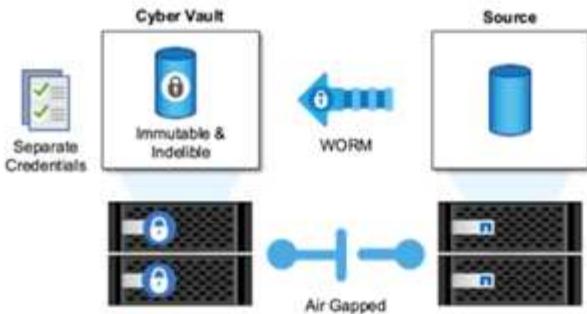
Protezione DA WORM a mappatura D'aria con cyber vaulting in ONTAP

L'approccio di NetApp a un cyber-vault è un'architettura di riferimento appositamente creata per un cyber-vault logicamente a mappatura d'aria. Questo approccio sfrutta le tecnologie di protezione avanzata e conformità, come SnapLock, per consentire snapshot immutabili e indelebili.

Il vaulting dei computer informatici con SnapLock Compliance e un'air gap logico

Un trend in crescita è quello di distruggere le copie di backup e, in alcuni casi, persino crittografarle. Questo è il motivo per cui molti nel settore della sicurezza informatica consigliano di utilizzare i backup air gap come parte di una strategia globale di resilienza informatica.

Il problema è che i tradizionali gap aerei (nastro e supporti offline) possono aumentare significativamente i tempi di ripristino, aumentando così i tempi di inattività e i costi complessivi associati. Anche un approccio più moderno a una soluzione per il gap aereo può rivelarsi problematico. Ad esempio, se il vault di backup viene temporaneamente aperto per ricevere nuove copie di backup e quindi disconnette e chiude la connessione di rete ai dati primari per essere nuovamente "sottoposto a air gap", un utente malintenzionato potrebbe sfruttare l'apertura temporanea. Nel momento in cui la connessione è in linea, un utente malintenzionato potrebbe colpire per compromettere o distruggere i dati. Questo tipo di configurazione, inoltre, in genere aggiunge complessità indesiderata. Un air gap logico è un eccellente sostituto di un air gap tradizionale o moderno, perché ha gli stessi principi di protezione della sicurezza mantenendo il backup online. Con NetApp, è possibile risolvere la complessità del nastro o dell'air gapping del disco con l'air gapping logico, che può essere ottenuto con istantanee immutabili e NetApp SnapLock Compliance.



NetApp ha rilasciato la funzione SnapLock più di 10 anni fa per soddisfare i requisiti di conformità dei dati, come la legge HIPAA (Health Insurance Portability and Accountability Act), Sarbanes-Oxley e altre regole normative in materia di dati. È anche possibile archiviare gli snapshot primari nei volumi SnapLock in modo che le copie possano essere assegnate al WORM, impedendo l'eliminazione. Esistono due versioni di licenza SnapLock: SnapLock Compliance e SnapLock Enterprise. Per la protezione dal ransomware, NetApp consiglia SnapLock Compliance, perché puoi impostare un periodo di conservazione specifico durante il quale gli snapshot sono bloccati e non possono essere eliminati, anche dagli amministratori di ONTAP o dal supporto NetApp.

Scopri di più

- ["Blog: Panoramica sul cyber vault di ONTAP"](#)

Snapshot a prova di manomissione

Sfruttando SnapLock Compliance come air gap logico, è garantita la massima protezione per impedire agli hacker di eliminare le copie di backup, è necessario spostare le snapshot tramite SnapVault in un volume secondario abilitato per SnapLock. Di conseguenza, molti clienti implementano questa configurazione su storage secondario in tutta la rete. Ciò consente tempi di ripristino più lunghi rispetto al ripristino di un volume primario sullo storage primario.

A partire da ONTAP 9.12.1, le snapshot a prova di manomissione offrono protezione a livello quasi SnapLock Compliance per le snapshot su storage primario e nei volumi primari. Non è necessario archiviare lo snapshot utilizzando SnapVault in un volume SnapLocked secondario. Gli snapshot a prova di manomissione utilizzano la tecnologia SnapLock per impedire l'eliminazione dello snapshot primario, anche da parte di un amministratore ONTAP completo che utilizza lo stesso periodo di scadenza della conservazione SnapLock. In questo modo è possibile ottenere tempi di ripristino più rapidi e backup di un volume FlexClone da uno snapshot protetto e antimanomissione, cosa che non è possibile fare con uno snapshot vault SnapLock Compliance tradizionale.

La differenza principale tra gli snapshot SnapLock Compliance e antimanomissione consiste nel fatto che SnapLock Compliance non consente l'inizializzazione e il cancellazione dell'array ONTAP se i volumi SnapLock Compliance esistono con snapshot nel vault che non hanno ancora raggiunto la data di scadenza. Per rendere gli snapshot a prova di manomissione, è necessaria una licenza SnapLock Compliance.

Scopri di più

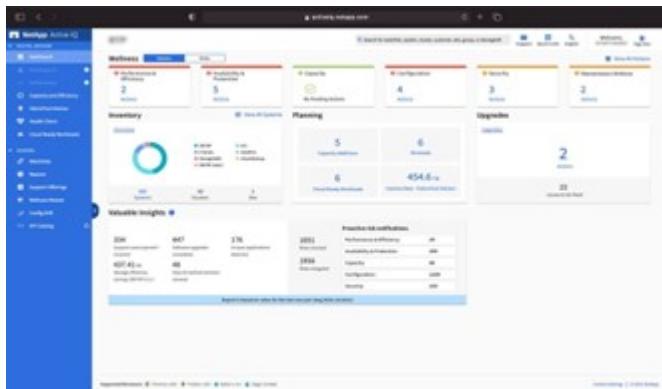
- ["Bloccare una snapshot per la protezione dagli attacchi ransomware"](#)

Protezione dal ransomware di Digital Advisor

Digital Advisor powered by Active IQ semplifica la cura proattiva e l'ottimizzazione dello storage NetApp con informazioni fruibili per una gestione ottimale dei dati. Alimentato dai dati di telemetria provenienti dalla nostra base installata altamente diversificata, utilizza

tecniche avanzate di AI e ML per individuare opportunità di riduzione dei rischi e miglioramento delle prestazioni e dell'efficienza del vostro ambiente di storage.

Non solo può "[Consulente digitale NetApp](#)" aiutare "[eliminare le vulnerabilità di sicurezza](#)", ma fornisce anche informazioni e linee guida specifiche per la protezione dai ransomware. Una wellness card dedicata mostra le azioni necessarie e i rischi affrontati, in modo da essere sicuri che i sistemi soddisfino le raccomandazioni sulle Best practice.



I rischi e le azioni tracciati nella pagina benessere della difesa dal ransomware includono quanto segue (e molto altro ancora):

- Il numero di snapshot dei volumi è basso, riducendo il potenziale di protezione ransomware.
- FPolicy non è abilitato per tutte le Storage Virtual Machine (SVM) configurate per i protocolli NAS.

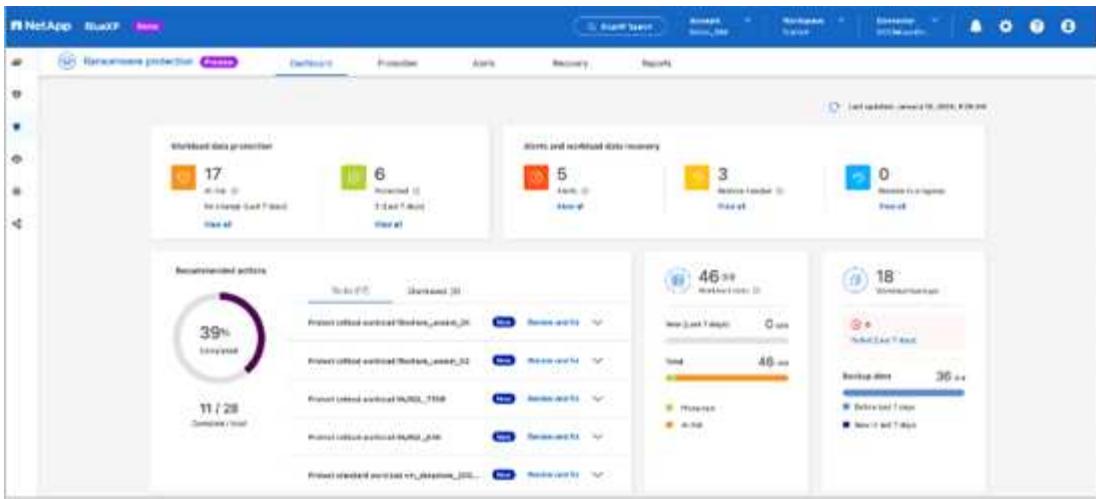
Per vedere la protezione dal ransomware in azione, consulta "["Consulente digitale"](#)".

Resilienza completa con la protezione ransomware NetApp

È importante che il rilevamento del ransomware avvenga il prima possibile, in modo da prevenirne la diffusione ed evitare costosi tempi di inattività. Tuttavia, una strategia efficace per rilevare i ransomware dovrebbe includere più di un singolo livello di protezione. La protezione ransomware di NetApp adotta un approccio completo che include funzionalità integrate in tempo reale che si estendono ai servizi dati tramite NetApp Console e una soluzione isolata e stratificata per il cyber vaulting.

Protezione ransomware NetApp

NetApp Console è un unico piano di controllo per orchestrare in modo intelligente una difesa anti-ransomware completa e incentrata sul carico di lavoro. La protezione ransomware NetApp unisce le potenti funzionalità di resilienza informatica di ONTAP, come ARP, FPolicy e snapshot antimanomissione, e i servizi dati di NetApp, come NetApp Backup and Recovery. Aggiunge inoltre raccomandazioni e indicazioni con flussi di lavoro automatizzati per fornire una difesa end-to-end tramite un'unica interfaccia utente. Opera a livello di carico di lavoro per garantire che le applicazioni che gestiscono la tua attività siano protette e possano essere ripristinate il più rapidamente possibile in caso di attacco.



Vantaggi per il cliente:

- La predisposizione al ransomware assistita riduce l'overhead operativo e migliora l'efficacia
- Il rilevamento delle anomalie basato su ai/ML offre una maggiore precisione e una risposta più rapida per contenere i rischi
- Il ripristino guidato, coerente con l'applicazione, ti consente di ripristinare i workload più facilmente e in pochi minuti

"Protezione ransomware NetApp" rende più facile realizzare queste funzioni NIST:

- Automaticamente **rilevamento** e assegnazione di priorità ai dati nello storage NetApp **con particolare attenzione ai workload basati sulle applicazioni**.
- **Protezione con un solo clic** del backup dei dati del carico di lavoro principale, configurazione immutabile e sicura, blocco di file dannosi e dominio di sicurezza diverso.
- **Rileva con precisione** il ransomware nel modo **rapido** possibile utilizzando **il rilevamento delle anomalie basato su ai di prossima generazione**.
- Risposta e flussi di lavoro automatizzati e integrazione con le principali soluzioni **SIEM e XDR**.
- Ripristina rapidamente i dati utilizzando un "recovery orchestrato" semplificato per accelerare l'uptime dell'applicazione.
- Implementa la tua protezione dal ransomware **strategia e policy**, e **monitora i risultati**.

NetApp e zero trust

NetApp e zero trust

Zero Trust è tradizionalmente un approccio incentrato sulla rete che prevede l'architettura di micro core e perimetro (MCAP) per proteggere dati, servizi, applicazioni o risorse con controlli noti come gateway di segmentazione. NetApp ONTAP sta adottando un approccio incentrato sui dati in Zero Trust, in cui il sistema di gestione dello storage diventa il gateway di segmentazione per proteggere e monitorare l'accesso ai dati dei clienti. In particolare, il motore FPolicy Zero Trust e l'ecosistema di partner FPolicy diventano un centro di controllo per acquisire una comprensione dettagliata dei modelli di accesso ai dati normali e aberranti e identificare le minacce interne.



A partire da luglio 2024, il contenuto del report tecnico *TR-4829: NetApp and Zero Trust: Enabling a data-centric Zero Trust model*, precedentemente pubblicato come PDF, è disponibile all'indirizzo docs.netapp.com.

I dati sono le risorse più importanti della tua organizzazione. Secondo il 2022, le minacce interne sono la causa del 18% delle violazioni dei dati "[Rapporto Verizon Data Breach Investigations](#)". Le organizzazioni possono rafforzare la propria vigilanza implementando controlli Zero Trust leader di settore intorno ai dati con il software per la gestione dei dati NetApp ONTAP.

Che cos'è Zero Trust?

Il modello Zero Trust è stato sviluppato per la prima volta da John Kindervag in Forrester Research. Prevede la sicurezza della rete dall'interno verso l'esterno e non dall'esterno. L'approccio Inside-out Zero Trust identifica un microcore e un perimetro (MCAP). La certificazione MCAP è una definizione interna di dati, servizi, applicazioni e risorse da proteggere con un set completo di controlli. Il concetto di perimetro esterno sicuro è obsoleto. Le entità attendibili e autorizzate ad eseguire correttamente l'autenticazione attraverso il perimetro possono rendere l'organizzazione vulnerabile agli attacchi. Gli addetti interni, per definizione, sono già all'interno del perimetro sicuro. Dipendenti, appaltatori e partner sono inclusi e devono essere abilitati a operare con controlli appropriati per l'esecuzione dei loro ruoli all'interno dell'infrastruttura dell'organizzazione.

Zero Trust è stata menzionata come una tecnologia che offre promesse al DoD nel settembre 2019 "[FY19-23 DoD strategia di modernizzazione digitale](#)". Definisce Zero Trust come "Una strategia di sicurezza informatica che incorpora la sicurezza in tutta l'architettura allo scopo di fermare le violazioni dei dati. Questo modello di protezione incentrato sui dati elimina l'idea di reti, dispositivi, figure o processi attendibili o non attendibili e passa a livelli di confidenza basati su più attributi che consentono l'autenticazione e l'autorizzazione dei criteri in base al concetto di accesso con privilegi minimi. L'implementazione di zero trust richiede un ripensamento del modo in cui utilizziamo l'infrastruttura esistente per implementare la sicurezza in base alla progettazione in modo più semplice ed efficiente, consentendo allo stesso tempo operazioni senza ostacoli."

Nell'agosto del 2020, il NIST ha pubblicato "[Speciale Pub 800-207 architettura Zero Trust](#)" (ZTA). ZTA si concentra sulla protezione delle risorse, non dei segmenti di rete, perché la posizione della rete non è più considerata come il componente principale della posizione di sicurezza della risorsa. Le risorse sono dati e calcolo. Le strategie ZTA sono destinate agli architetti di reti aziendali. ZTA introduce una nuova terminologia dai concetti originali di Forrester. I meccanismi di protezione denominati PDP (Policy Decision Point) e PEP (Policy Enforcement Point) sono analoghi a un gateway di segmentazione Forrester. ZTA introduce quattro modelli di distribuzione:

- Implementazione basata su gateway o agente dispositivo
- Implementazione basata su Enclave (in qualche modo analoga alla certificazione Forrester MCAP)
- Implementazione basata su portale di risorse
- Sandboxing dell'applicazione del dispositivo

Ai fini di questa documentazione, utilizziamo concetti e terminologia di Forrester Research piuttosto che NIST ZTA.

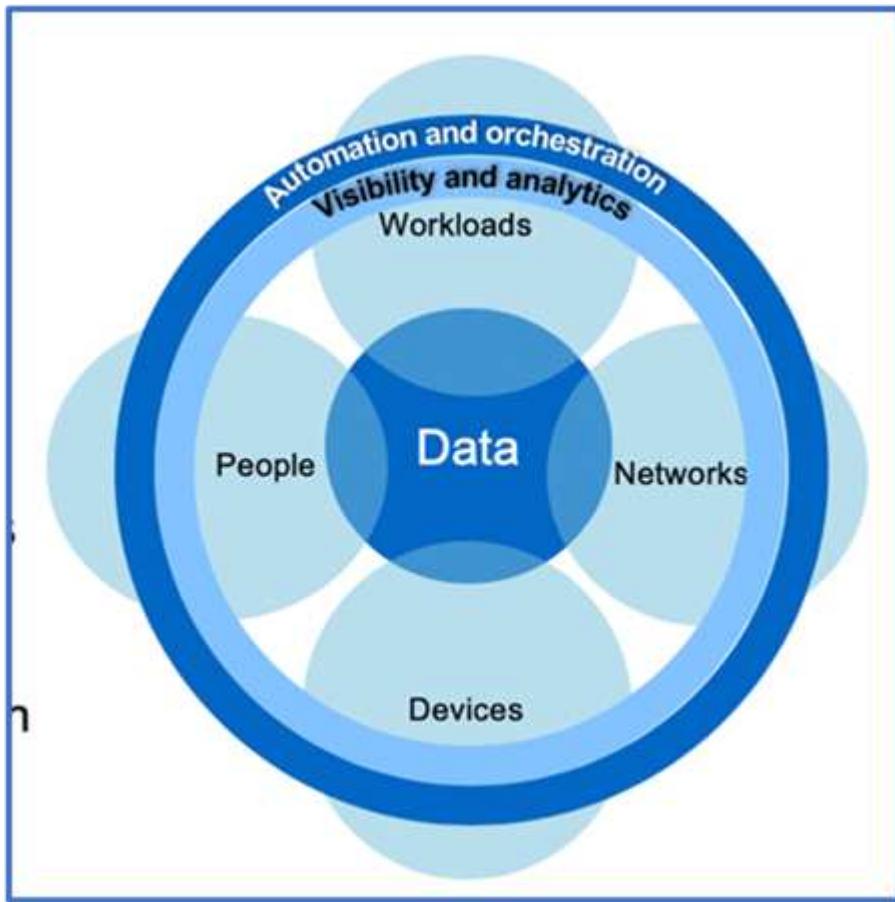
Risorse di sicurezza

Per informazioni sulla segnalazione di vulnerabilità e incidenti, risposte di sicurezza NetApp e riservatezza dei clienti, vedere "[Portale NetApp sulla sicurezza](#)".

Progetta un approccio incentrato sui dati a Zero Trust con ONTAP

Una rete Zero Trust viene definita da un approccio incentrato sui dati, in cui i controlli di sicurezza devono trovarsi il più vicino possibile ai dati. Le funzionalità di ONTAP, insieme all'ecosistema partner di NetApp FPolicy, possono fornire i controlli necessari per il modello Zero Trust incentrato sui dati.

ONTAP è un software NetApp per la gestione dei dati con sicurezza robusta e il motore Zero Trust di FPolicy è una funzione ONTAP leader di settore che offre un'interfaccia di notifica di eventi granulare e basata su file. I partner NetApp FPolicy possono utilizzare questa interfaccia per ottenere maggiore visibilità sull'accesso ai dati all'interno di ONTAP.



Crea un MCAP basato sui dati Zero Trust

Per progettare una certificazione MCAP Zero Trust incentrata sui dati, attenersi alla seguente procedura:

1. Identificare l'ubicazione di tutti i dati dell'organizzazione.
2. Classificazione dei dati.
3. Smaltire in modo sicuro i dati non più necessari.
4. Comprendere quali ruoli devono avere accesso alle classificazioni dei dati.
5. Applicare il principio del privilegio minimo per applicare i controlli di accesso.
6. Utilizza la Multifactor Authentication per l'accesso amministrativo e l'accesso ai dati.
7. Utilizza la crittografia per i dati a riposo e in uso.

8. Monitorare e registrare tutti gli accessi.
9. Avvisa di accessi o comportamenti sospetti.

Identificare l'ubicazione di tutti i dati dell'organizzazione

La funzionalità FPolicy di ONTAP, insieme all'ecosistema di partner NetApp Alliance, ti consente di identificare dove sono presenti i dati della tua organizzazione e chi ne ha accesso. Ciò avviene con l'analisi dei comportamenti degli utenti, che identifica se gli schemi di accesso ai dati sono validi. Ulteriori dettagli sull'analisi del comportamento degli utenti sono discussi in Monitor e registrano tutti gli accessi. Se non si capisce dove si trovano i dati e chi vi ha accesso, l'analisi comportamentale degli utenti può fornire una base per creare classificazione e policy a partire da osservazioni empiriche.

Classificazione dei dati

Nella terminologia del modello Zero Trust, la classificazione dei dati implica l'identificazione dei dati tossici. I dati tossici sono dati sensibili che non sono destinati a essere divulgati all'esterno di un'organizzazione. La divulgazione di dati tossici potrebbe violare la conformità normativa e danneggiare la reputazione di un'organizzazione. In termini di conformità normativa, i dati tossici includono i dati del titolare della carta per "[Payment Card Industry Data Security Standard \(PCI-DSS\)](#)" , dati personali per l'UE "[Regolamento generale sulla protezione dei dati \(GDPR\)](#)" , o dati sanitari per il "[Health Insurance Portability and Accountability Act \(HIPAA\)](#)" . Puoi usare NetApp "[NetApp Data Classification](#)" (precedentemente noto come Cloud Data Sense), un toolkit basato sull'intelligenza artificiale per analizzare, scansionare e categorizzare automaticamente i tuoi dati.

Smaltire in modo sicuro i dati non più necessari

Dopo aver classificato i dati della tua organizzazione, potresti scoprire che alcuni di essi non sono più necessari o rilevanti per la funzione della tua organizzazione. La conservazione di dati non necessari è una responsabilità e tali dati devono essere cancellati. Per un meccanismo avanzato che consente di cancellare crittograficamente i dati, vedere la descrizione dell'eliminazione sicura nella crittografia dei dati inattivi.

Comprendere quali ruoli devono avere accesso alle classificazioni dei dati e applicare il principio del minimo privilegio per applicare i controlli di accesso

La mappatura dell'accesso ai dati sensibili e l'applicazione del principio del privilegio minimo consentono agli utenti dell'organizzazione di accedere solo ai dati necessari per svolgere il proprio lavoro. Questo processo comporta il controllo dell'accesso basato sui ruoli ("[RBAC](#)"), che si applica all'accesso ai dati e all'accesso amministrativo.

Con ONTAP, è possibile utilizzare una Storage Virtual Machine (SVM) per segmentare l'accesso ai dati organizzativi da parte dei tenant all'interno di un cluster ONTAP. RBAC può essere applicato all'accesso ai dati e all'accesso amministrativo alla SVM. RBAC può anche essere applicato a livello amministrativo del cluster.

Oltre ai role-based access control, è possibile utilizzare ONTAP "[Verifica con amministratori multipli](#)" (MAV) per richiedere a uno o più amministratori di approvare comandi come `volume delete` o `volume snapshot delete`. Una volta attivato MAV, la modifica o la disattivazione di MAV richiede l'approvazione dell'amministratore MAV.

Un altro modo per proteggere gli snapshot è con ONTAP "[blocco delle istantanee](#)". Il blocco degli snapshot è una funzionalità SnapLock in cui gli snapshot vengono resi indelebili manualmente o automaticamente, con un periodo di conservazione nel criterio dello snapshot del volume. Il blocco delle istantanee viene anche definito blocco delle istantanee a prova di manomissione. Lo scopo del blocco delle snapshot è impedire agli amministratori non autorizzati o non attendibili di eliminare snapshot sui sistemi ONTAP primari e secondari. È possibile ottenere un rapido recovery degli snapshot bloccati sui sistemi primari per ripristinare volumi corrotti dal ransomware.

Utilizza la Multifactor Authentication per l'accesso amministrativo e l'accesso ai dati

Oltre al RBAC amministrativo del cluster, "[Autenticazione multifattore \(MFA\)](#)" può essere implementato per l'accesso amministrativo web di ONTAP e l'accesso Secure Shell (SSH) a riga di comando. MFA per l'accesso amministrativo è un requisito per le organizzazioni del settore pubblico statunitense o per quelle che devono seguire il PCI-DSS. MFA rende impossibile per un utente malintenzionato compromettere un account utilizzando solo un nome utente e una password. L'autenticazione MFA richiede due o più fattori indipendenti. Un esempio di autenticazione a due fattori è qualcosa che un utente possiede, come una chiave privata, e qualcosa che un utente conosce, come una password. L'accesso web amministrativo al ONTAP System Manager o ActiveIQ Unified Manager è abilitato dal Security Assertion Markup Language (SAML) 2.0. L'accesso a riga di comando SSH utilizza un'autenticazione a due fattori concatenata con una chiave pubblica e una password.

È possibile controllare l'accesso di utenti e macchine tramite API con le funzionalità di gestione delle identità e degli accessi di ONTAP:

- Utente:
 - **Autenticazione e autorizzazione.** Attraverso le funzionalità dei protocolli NAS per SMB e NFS.
 - **Audit.** Syslog di accesso ed eventi. Logging dettagliato dell'audit del protocollo CIFS per testare le policy di autenticazione e autorizzazione. Controllo FPolicy granulare e fine dell'accesso NAS dettagliato a livello di file.
- Dispositivo:
 - **Autenticazione.** Autenticazione basata su certificati per l'accesso API.
 - **Autorizzazione.** Controllo degli accessi (RBAC) predefinito o personalizzato in base al ruolo.
 - **Audit.** Syslog di tutte le azioni eseguite.

Utilizza la crittografia per i dati a riposo e in uso

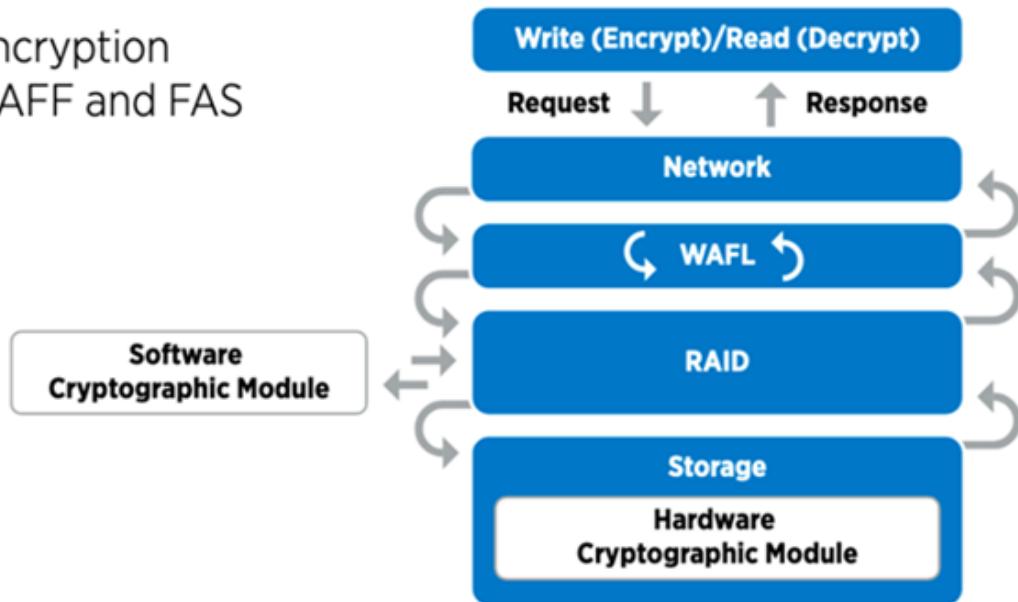
Crittografia dei dati inattivi

Ogni giorno esistono nuovi requisiti per ridurre i rischi del sistema storage e il gap dell'infrastruttura quando un'organizzazione riutilizza i dischi, restituisce i dischi difettosi o effettua gli upgrade a dischi più grandi vendendoli o tramite permuta. Come amministratori e operatori dei dati, i tecnici dello storage sono tenuti a gestire e mantenere i dati in modo sicuro per tutto il loro ciclo di vita. "[Crittografia dello storage NetApp \(NSE\)](#) e [crittografia dei volumi NetApp \(NVE\)](#) e [crittografia aggregata di NetApp](#)" aiuta a crittografare costantemente tutti i dati a riposo, che siano tossici e non influiscano sulle operazioni quotidiane. "[NSE](#)" È una soluzione hardware ONTAP "[dati a riposo](#)" che utilizza dischi con crittografia automatica convalidati FIPS 140-2 livello 2. "[NVE e NAE](#)" Sono una soluzione software ONTAP "[dati a riposo](#)" che utilizza "[Modulo crittografico NetApp validato FIPS 140-2 livello 1](#)". Con NVE e NAE, è possibile utilizzare i dischi rigidi o i dischi a stato solido per la crittografia dei dati a riposo. Inoltre, i dischi NSE possono essere utilizzati per fornire una soluzione per la crittografia nativa e su più layer che garantisca ridondanza della crittografia e sicurezza aggiuntiva. Se un livello viene violato, il secondo livello protegge comunque i dati. Queste funzionalità rendono ONTAP ben posizionato per "[crittografia quantum-ready](#)".

NVE fornisce anche una funzionalità chiamata "[spurgo sicuro](#)" che rimuove crittograficamente i dati tossici da perdite di dati quando i file sensibili vengono scritti in un volume non classificato.

È possibile utilizzare il "[Onboard Key Manager \(OKM\)](#)", che è il gestore delle chiavi integrato in ONTAP, o "[approvato](#)" terze parti "[responsabili esterni delle chiavi](#)" con NSE e NVE per memorizzare in modo sicuro il materiale di codifica.

Two-layer encryption solution for AFF and FAS



Come illustrato nella figura precedente, è possibile combinare la crittografia basata su hardware e software. Questa funzionalità ha portato a "[Convalida di ONTAP nelle soluzioni commerciali della NSA per il programma classificato](#)" che consente la memorizzazione di dati top secret.

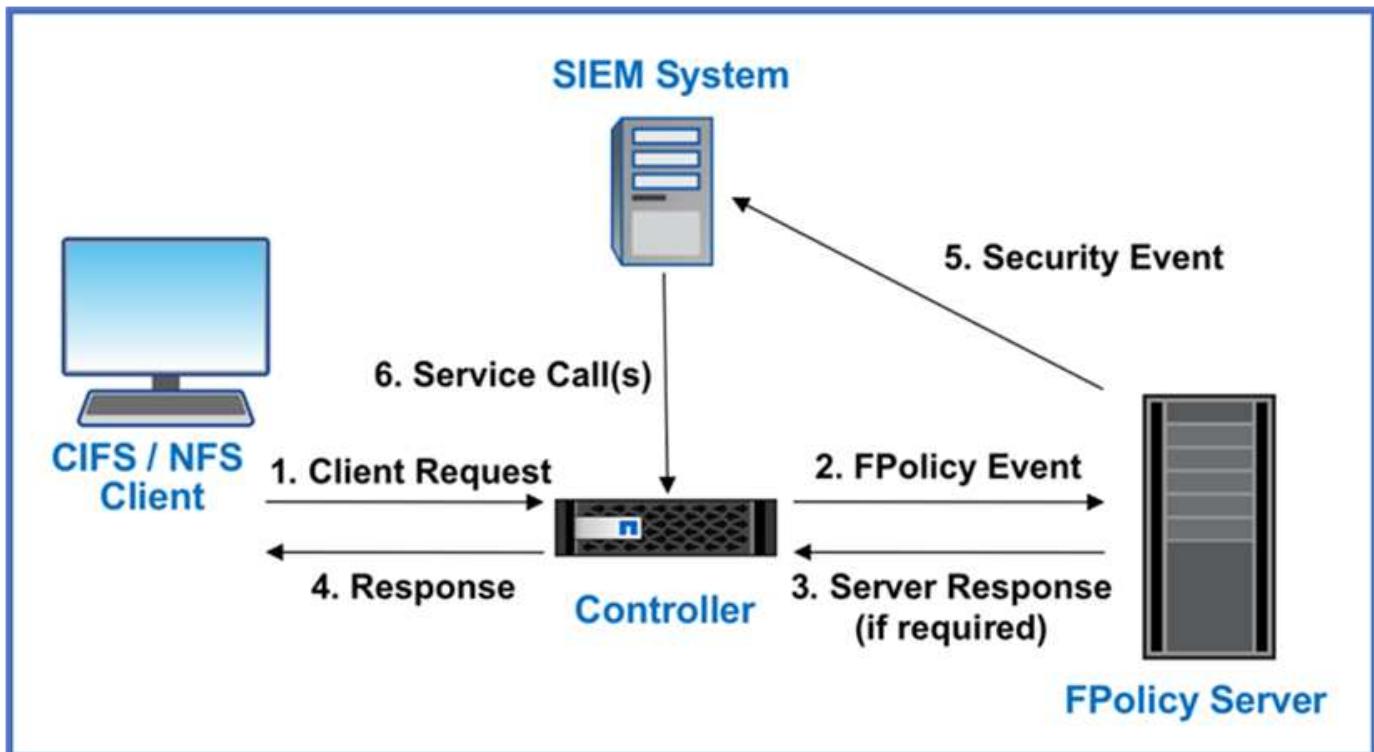
Crittografia dei dati in-flight

La crittografia dei dati in-flight di ONTAP protegge l'accesso ai dati degli utenti e l'accesso da un piano di controllo. L'accesso ai dati degli utenti può essere crittografato con la crittografia SMB 3,0 per l'accesso alla condivisione CIFS di Microsoft o con krb5P per NFS Kerberos 5. L'accesso ai dati dell'utente può anche essere crittografato con "[IPSec](#)" per CIFS, NFS e iSCSI. L'accesso al piano di controllo è crittografato con Transport Layer Security (TLS). ONTAP fornisce la "[FIPS](#)" modalità di conformità per l'accesso al piano di controllo, che attiva algoritmi approvati FIPS e disattiva algoritmi non approvati FIPS. La replica dei dati viene crittografata con "[crittografia di peering dei cluster](#)". In questo modo viene fornita la crittografia per le tecnologie ONTAP SnapVault e SnapMirror.

Monitorare e registrare tutti gli accessi

Una volta messe in atto le policy RBAC, devi implementare monitoring, audit e avvisi attivi. Il motore Zero Trust FPolicy di NetApp ONTAP, insieme a "[Ecosistema di partner NetApp FPolicy](#)", fornisce i controlli necessari per il modello Zero Trust incentrato sui dati. NetApp ONTAP è un software per la gestione dei dati ricco di sicurezza e "[FPolicy](#)" una funzionalità ONTAP leader di settore che offre un'interfaccia di notifica degli eventi granulare basata su file. I partner NetApp FPolicy possono utilizzare questa interfaccia per ottenere maggiore visibilità sull'accesso ai dati all'interno di ONTAP. La funzionalità FPolicy di ONTAP, insieme all'ecosistema di partner NetApp Alliance di FPolicy, ti consente di identificare dove sono presenti i dati della tua organizzazione e chi ne ha accesso. Ciò avviene con l'analisi dei comportamenti degli utenti, che identifica se gli schemi di accesso ai dati sono validi. L'analisi del comportamento degli utenti può essere utilizzata per avvisare in caso di accesso ai dati sospetto o aberrante che non rientra nel normale modello e, se necessario, per intraprendere azioni volte a negare l'accesso.

I partner FPolicy stanno andando oltre gli analytics comportamentali degli utenti verso il machine learning (ML) e l'intelligenza artificiale (ai), per una maggiore fedeltà agli eventi e meno falsi positivi, se presenti. Tutti gli eventi devono essere registrati su un server syslog o su un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) in grado di utilizzare ML e ai.



NetApp "Sicurezza del carico di lavoro di archiviazione DII" sfrutta l'interfaccia FPolicy e l'analisi comportamentale degli utenti sui sistemi di archiviazione ONTAP sia cloud che on-premise per fornire avvisi in tempo reale sui comportamenti dannosi degli utenti. Storage Workload Security protegge i dati aziendali dall'uso improprio da parte di utenti malintenzionati o compromessi tramite apprendimento automatico avanzato e rilevamento delle anomalie. Storage Workload Security è in grado di identificare attacchi ransomware o altri comportamenti illeciti, richiamare snapshot e mettere in quarantena gli utenti malintenzionati. Storage Workload Security è dotato anche di una capacità forense per visualizzare in dettaglio le attività degli utenti e delle entità. Storage Workload Security è una parte di NetApp Data Infrastructure Insights.

Oltre alla sicurezza del workload di storage, ONTAP dispone di una funzionalità di rilevamento del ransomware integrata nota come "[Protezione ransomware autonoma](#)" (ARP). ARP usa l'apprendimento automatico per determinare se un'attività anomala dei file indica che è in corso un attacco ransomware e richiama una snapshot e avvisa gli amministratori. Storage workload Security si integra con ONTAP per ricevere eventi ARP e fornisce un livello aggiuntivo di analisi e risposte automatiche.

Per ulteriori informazioni sui comandi descritti in questa procedura, consultare la "[Riferimento comando ONTAP](#)".

Controlli di orchestrazione e automazione della sicurezza NetApp esterni a ONTAP

L'automazione consente di eseguire un processo o una procedura con un'assistenza minima da parte dell'operatore. L'automazione consente alle organizzazioni di scalare le implementazioni di tipo Zero Trust ben oltre le procedure manuali, in modo da difendersi da attività miscibili e automatizzate.

Ansible è un tool di provisioning software open-source, gestione della configurazione e implementazione dell'applicazione. Funziona su molti sistemi Unix-like, e può configurare sia sistemi Unix-like che Microsoft Windows. Include il proprio linguaggio dichiarativo per descrivere la configurazione del sistema. Ansible è stato scritto da Michael DeHaan e acquisito da Red Hat nel 2015. Ansible si connette temporaneamente e senza

agenti tramite SSH o Windows Remote Management (consentendo l'esecuzione remota di PowerShell) per eseguire i task. NetApp ha sviluppato molto di più di "[150 moduli Ansible per il software ONTAP](#)", consentendo un'ulteriore integrazione con il framework di automazione Ansible. I moduli Ansible per NetApp forniscono una serie di istruzioni su come definire lo stato desiderato e trasferirlo all'ambiente NetApp di destinazione. I moduli sono realizzati per supportare task come l'impostazione del licensing, la creazione di aggregati e di Storage Virtual Machine, la creazione di volumi e il ripristino di snapshot per citarne alcuni. Un ruolo Ansible è stato ["Pubblicato su GitHub"](#) specifico per la NetApp DoD Unified Capabilities (UC) Deployment Guide.

Utilizzando la libreria di moduli disponibili, gli utenti possono facilmente sviluppare i playbook Ansible e personalizzarli in base alle proprie applicazioni e esigenze aziendali per automatizzare i task ordinari. Una volta scritto un playbook, puoi eseguirlo per eseguire il task specificato, risparmiando tempo e migliorando la produttività. NetApp ha creato e condiviso playbook di esempio che possono essere utilizzati direttamente o personalizzati per le tue esigenze.

Data Infrastructure Insights è uno strumento di monitoraggio dell'infrastruttura che ti offre visibilità sull'intera infrastruttura. Con Data Infrastructure Insights puoi monitorare, risolvere i problemi e ottimizzare tutte le tue risorse, comprese le istanze del cloud pubblico e i data center privati. Data Infrastructure Insights può ridurre il tempo medio di risoluzione del 90% e impedire che l'80% dei problemi del cloud interessino gli utenti finali. Può inoltre ridurre in media del 33% i costi dell'infrastruttura cloud e ridurre l'esposizione alle minacce interne proteggendo i dati con informazioni fruibili. La funzionalità Storage Workload Security di Data Infrastructure Insights consente l'analisi comportamentale degli utenti con intelligenza artificiale e apprendimento automatico per avvisare quando si verificano comportamenti anomali degli utenti dovuti a una minaccia interna. Per ONTAP, Storage Workload Security utilizza il motore Zero Trust FPolicy.

Implementazioni di cloud ibrido e zero trust

NetApp è l'autorità in materia di dati per il cloud ibrido. NetApp offre diverse opzioni per estendere i sistemi di gestione dei dati on-premise al cloud ibrido con Amazon Web Services (AWS), Microsoft Azure, Google Cloud e altri importanti provider cloud. Le soluzioni cloud ibride NetApp supportano gli stessi controlli di sicurezza Zero Trust disponibili con i sistemi ONTAP on-premise e lo storage software-defined ONTAP Select .

È possibile espandere facilmente la capacità nei cloud pubblici senza i tipici vincoli CAPEX utilizzando servizi file cloud-native di livello enterprise per AWS (FSxN), Google Cloud (GCNV) e Azure NetApp Files per Microsoft Azure. Ideali per carichi di lavoro ad alta intensità di dati, come analisi e DevOps, questi servizi di dati cloud combinano l'archiviazione elastica e on-demand come servizio di NetApp con la gestione dei dati ONTAP in un'offerta completamente gestita.

ONTAP consente lo spostamento dei dati tra i sistemi ONTAP locali e l'ambiente di archiviazione AWS, Google Cloud o Azure con il software di replicazione dei dati NetApp SnapMirror .

Controllo degli accessi basato su attributi

Controllo degli accessi basato su attributi con ONTAP

A partire dalla versione 9.12.1, è possibile configurare ONTAP con etichette di sicurezza NFSv4,2 e attributi estesi (xattr) per supportare il role-based access control (RBAC) con attributi e il controllo degli accessi basato sugli attributi (ABAC).

ABAC è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi degli utenti, agli attributi delle risorse e alle condizioni ambientali. L'integrazione di ONTAP con le etichette di sicurezza NFS v4,2 e xattr è conforme agli standard NIST per le soluzioni ABAC, come indicato nella Pubblicazione speciale

È possibile utilizzare le etichette di sicurezza e gli xattr NFS v4,2 per assegnare ai file attributi ed etichette definiti dall'utente. ONTAP può integrarsi con il software di gestione degli accessi e delle identità basato su ABAC per applicare policy di controllo degli accessi granulari a file e cartelle basate su questi attributi ed etichette.

Informazioni correlate

- ["Approcci ad ABAC con ONTAP"](#)
- ["NFS in NetApp ONTAP: Best practice e guida all'implementazione"](#)

Approcci al controllo di accesso basato sugli attributi (ABAC) in ONTAP

ONTAP fornisce diversi approcci che è possibile utilizzare per ottenere il controllo dell'accesso basato sugli attributi a livello di file (ABAC), incluse le etichette di sicurezza NFS v4,2 e gli attributi estesi (xattr) utilizzando NFS.

Etichette di sicurezza NFS v4,2

A partire da ONTAP 9,9.1, è supportata la funzione NFS v4,2 denominata NFS.

Le etichette di sicurezza NFS v4,2 consentono di gestire l'accesso granulare a file e cartelle utilizzando le etichette SELinux e il controllo di accesso obbligatorio (MAC). Queste etichette MAC sono memorizzate con file e cartelle e funzionano in combinazione con autorizzazioni UNIX e ACL NFS v4.x.

Il supporto per le etichette di sicurezza NFS v4,2 significa che ONTAP ora riconosce e comprende le impostazioni delle etichette SELinux del client NFS. Le etichette di sicurezza NFS v4,2 sono coperte dal documento RFC-7204.

I casi di utilizzo delle etichette di sicurezza di NFS v4,2 includono quanto segue:

- Etichettatura MAC delle immagini della macchina virtuale (VM)
- Classificazione di sicurezza dei dati per il settore pubblico (segreto, top secret e altre classificazioni)
- Conformità alla sicurezza
- Linux senza disco

Abilitare le etichette di sicurezza NFS v4.2

È possibile attivare o disattivare le etichette di sicurezza NFS v4,2 con il seguente comando (è richiesto il privilegio avanzato):

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel <disabled|enabled>
```

Ulteriori informazioni su `vserver nfs modify` nella ["Riferimento comando ONTAP"](#).

Modalità di applicazione per le etichette di sicurezza NFS v4,2

A partire da ONTAP 9,9.1, ONTAP supporta le seguenti modalità di applicazione:

- **Modalità server limitata:** ONTAP non può applicare le etichette ma può memorizzarle e trasmetterle.



La possibilità di modificare le etichette MAC dipende dal client da applicare.

- **Modalità ospite:** Se il client non è etichettato NFS-aware (v4,1 o inferiore), le etichette MAC non vengono trasmesse.



ONTAP attualmente non supporta la modalità completa (memorizzazione e applicazione delle etichette MAC).

Esempi di etichette di sicurezza NFS v4,2

Nell'esempio di configurazione riportato di seguito vengono illustrati i concetti che utilizzano Red Hat Enterprise Linux release 9,3 (Plow).

L'utente `jrsmith`, creato in base alle credenziali di John R. Smith, dispone del seguente account Privileges:

- Nome utente = `jrsmith`
- Privileges = `uid=1112(jrsmith) gid=1112(jrsmith) groups=1112(jrsmith)`
`context=user_u:user_r:user_t:s0`

Esistono due ruoli: L'account admin che è un utente e un utente con privilegi `jrsmith`, come descritto nella seguente tabella MLS Privileges:

Utenti	Ruolo	Tipo	Livelli
admins	<code>sysadm_r</code>	<code>sysadm_t</code>	<code>t:s0</code>
<code>jrsmith</code>	<code>user_r</code>	<code>user_t</code>	<code>t:s1 - t:s4</code>

In questo ambiente di esempio, l'utente `jrsmith` ha accesso ai file ai s3 livelli di s0 . Possiamo migliorare le classificazioni di sicurezza esistenti, come descritto di seguito, per garantire che gli amministratori non abbiano accesso a dati specifici dell'utente.

- s0 = dati utente amministratore con privilegi
- s0 = dati non classificati
- s1 = riservato
- s2 = dati segreti
- s3 = dati top secret

Esempio di etichette di sicurezza NFS v4,2 con MCS

Oltre alla protezione multilivello (MLS), un'altra funzionalità denominata protezione multi-categoria (MCS) consente di definire categorie come i progetti.

Etichetta di sicurezza NFS	Valore
<code>entitySecurityM</code>	<code>t:s01 = UNCLASSIFIED</code>
<code>ark</code>	

Attributi estesi (xattrs)

A partire da ONTAP 9.12.1, ONTAP supporta xattr. Xattr consente l'associazione dei metadati a file e directory oltre a quanto fornito dal sistema, come gli elenchi di controllo di accesso (ACL) o gli attributi definiti dall'utente.

Per implementare xattr, è possibile utilizzare `setfattr` e `getfattr` le utilità della riga di comando in Linux. Questi strumenti forniscono un metodo efficace per gestire metadati aggiuntivi per file e directory. Devono essere utilizzati con cautela, poiché un uso improprio può causare comportamenti imprevisti o problemi di sicurezza. Per istruzioni dettagliate sull'uso, consultare sempre `setfattr` le pagine man e `getfattr` o altra documentazione affidabile.

Quando xattr è abilitato su un filesystem ONTAP, gli utenti possono impostare, modificare e recuperare attributi arbitrari sui file. Questi attributi possono essere utilizzati per memorizzare informazioni aggiuntive sul file che non vengono acquisite dal set standard di attributi del file, come le informazioni sul controllo dell'accesso.

Esistono diversi requisiti e limiti per l'utilizzo di xattr in ONTAP:

- Red Hat Enterprise Linux versione 8,4 o successiva
- Ubuntu 22.04 o versione successiva
- Ogni file può avere fino a 128 xattr
- Le chiavi xattr sono limitate a 255 byte
- La dimensione combinata della chiave o del valore è di 1.729 byte per xattr
- Directory e file possono avere xattr
- Per impostare e recuperare xattr, w o i bit di modalità di scrittura devono essere abilitati per l'utente e il gruppo

Gli Xattr sono utilizzati all'interno dello spazio dei nomi utente e non hanno alcun significato intrinseco per ONTAP stesso. Le loro applicazioni pratiche sono invece determinate e gestite esclusivamente dall'applicazione lato client che interagisce con il file system.

Esempi di casi di utilizzo di xattr:

- Registrazione del nome dell'applicazione responsabile della creazione di un file
- Mantenere un riferimento al messaggio e-mail da cui è stato ottenuto un file
- Definizione di un framework di categorizzazione per l'organizzazione degli oggetti file
- Etichettare i file con l'URL della fonte di download originale

Comandi per la gestione di xattr

- `setfattr` imposta un attributo esteso di un file o di una directory:

```
setfattr -n <attribute_name> -v <attribute_value> <file or directory name>
```

Esempio di comando:

```
setfattr -n user.comment -v test example.txt
```

- `getfattr` recupera il valore di un attributo esteso specifico o elenca tutti gli attributi estesi di un file o di una directory:

Attributo specifico:

```
getfattr -n <attribute_name> <file or directory name>
```

Tutti gli attributi:

```
getfattr <file or directory name>
```

Esempio di comando:

```
getfattr -n user.comment example.txt
```

Esempi di coppie di valori chiave xattr

La tabella seguente mostra due esempi di coppie di valori chiave xattr:

xattr	Valore
user.digitalIdentifier	CN=John Smith jrsmith, OU=Finance, OU=U.S.ACME, O=US, C=US
user.countryOfAffiliations	USA

Autorizzazioni utente con ACE per xattrs

Una voce di controllo di accesso (ACE) è un componente all'interno di un ACL che definisce i diritti di accesso o le autorizzazioni concesse a un singolo utente o a un gruppo di utenti per una risorsa specifica, ad esempio un file o una directory. Ogni ACE specifica il tipo di accesso consentito o negato ed è associato a un'identità di protezione particolare (identità utente o gruppo).

Per gli xattrs è richiesta la voce ACE (Access Control Entry)

- Recupera xattr: Autorizzazioni necessarie per la lettura degli attributi estesi di un file o di una directory da parte di un utente. La "R" indica che è necessario il permesso di lettura.
- Set xattrs: Le autorizzazioni necessarie per modificare o impostare gli attributi estesi. "A", "w" e "T" rappresentano diversi esempi di permessi, quali append, write e un permesso specifico relativo a xattrs.
- File: Gli utenti hanno bisogno di aggiungere, scrivere e potenzialmente di un'autorizzazione speciale relativa a xattrs per impostare gli attributi estesi.
- Directory: Per impostare gli attributi estesi è necessaria un'autorizzazione specifica "T".

Tipo di file	Recupera xattr	Set xattrs
File	R	A, w, T
Directory	R	T

Integrazione con il software ABAC Identity and Access Control

Per sfruttare appieno le funzionalità di ABAC, ONTAP può integrarsi con un software di gestione delle identità e degli accessi orientato all'ABAC.

In un sistema ABAC, il Policy Enforcement Point (PEP) e il Policy Decision Point (PDP) svolgono ruoli cruciali. Il PEP è responsabile dell'applicazione dei criteri di controllo degli accessi, mentre il PDP decide se concedere o negare l'accesso in base ai criteri.

In un ambiente pratico, un'organizzazione impiegherebbe una combinazione di etichette di sicurezza NFS e xattrs. Vengono utilizzati per rappresentare una varietà di metadati, tra cui classificazione, protezione, applicazione e contenuto, che sono tutti fondamentali per prendere decisioni ABAC. Xattr, ad esempio, può essere utilizzato per memorizzare gli attributi delle risorse che il PDP utilizza per il processo decisionale. È possibile definire un attributo per rappresentare il livello di classificazione di un file (ad esempio, "non classificato", "riservato", "segreto" o "Segreto principale"). Il PDP potrebbe quindi utilizzare questo attributo per applicare un criterio che limita l'accesso degli utenti solo ai file con un livello di classificazione uguale o inferiore al livello di verifica.



Questo contenuto presuppone che i servizi di identità, autenticazione e accesso del cliente includano almeno un PEP e un PDP che fungono da intermediari per l'accesso al file system.

Esempio di flusso di processo per ABAC

1. L'utente presenta le credenziali (ad esempio, PKI, OAuth, SAML) per l'accesso al sistema PEP e ottiene i risultati da PDP.

Il ruolo del PEP è quello di intercettare la richiesta di accesso dell'utente e inoltrarla al PDP.

2. Il PDP valuta quindi questa richiesta in base ai criteri ABAC stabiliti.

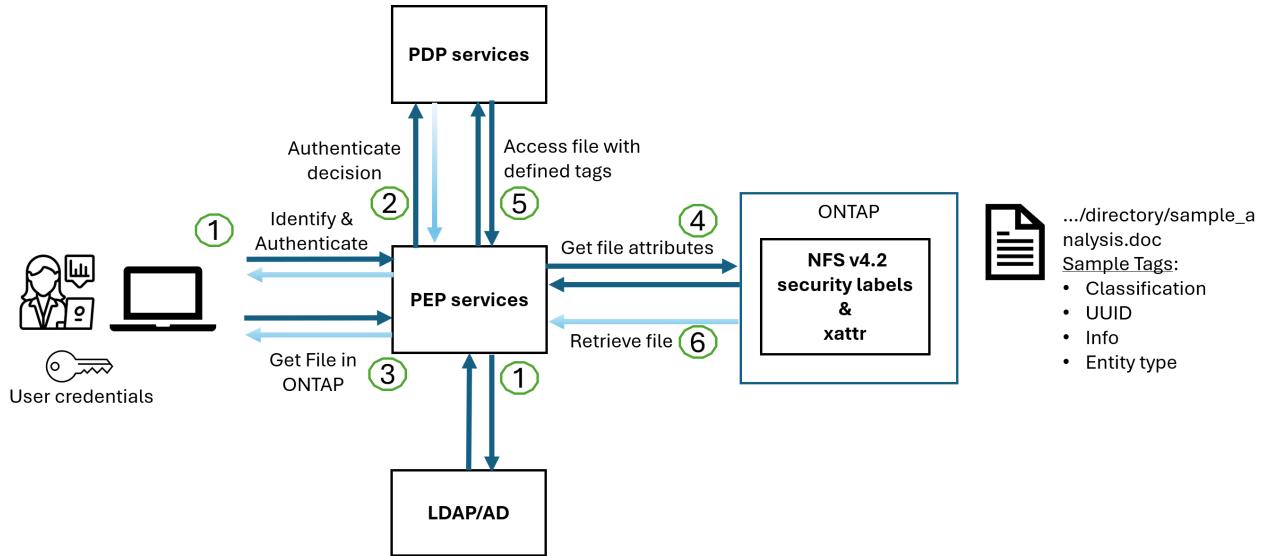
Questi criteri considerano diversi attributi correlati all'utente, alla risorsa in questione e all'ambiente circostante. Sulla base di questi criteri, il PDP prende una decisione di accesso per consentire o negare e quindi comunica questa decisione al PEP.

PDP fornisce criteri a PEP da applicare. Il PEP applica quindi questa decisione, concedendo o negando la richiesta di accesso dell'utente in base alla decisione del PDP.

3. Dopo una richiesta riuscita, l'utente richiede un file memorizzato in ONTAP (ad esempio, AFF, AFF-C).
4. Se la richiesta viene eseguita correttamente, PEP riceve dal documento i tag di controllo dell'accesso con precisione.
5. PEP richiede un criterio per l'utente in base ai certificati di quell'utente.
6. PEP prende una decisione in base a criteri e tag se l'utente ha accesso al file e consente all'utente di recuperare il file.



L'accesso effettivo può essere eseguito utilizzando i token.



Clonazione ONTAP e SnapMirror

Le tecnologie di clonazione e SnapMirror di ONTAP sono progettate per fornire funzionalità di replica e clonazione dei dati efficienti e affidabili, garantendo che tutti gli aspetti dei dati dei file, compresi xattrs, vengano preservati e trasferiti insieme al file. Le xattrs sono fondamentali per la memorizzazione di metadati aggiuntivi associati a un file, come etichette di sicurezza, informazioni di controllo degli accessi e dati definiti dall'utente, essenziali per mantenere il contesto e l'integrità del file.

Quando un volume viene clonato utilizzando la tecnologia FlexClone di ONTAP, viene creata una replica scrivibile esatta del volume. Questo processo di cloning è istantaneo, efficiente in termini di spazio e include tutti i dati e i metadati dei file per assicurare la replica completa delle xattrs. Allo stesso modo, SnapMirror garantisce che i dati vengano mirrorati su un sistema secondario, con piena fedeltà. Questo include xattrs, che sono fondamentali per le applicazioni che si basano su questi metadati per funzionare correttamente.

Includendo xattrs in operazioni di cloning e replica, NetApp ONTAP garantisce che il set di dati completo, con tutte le sue caratteristiche, sia disponibile e coerente nei sistemi di storage primario e secondario. Questo approccio completo alla gestione dei dati è fondamentale per le organizzazioni che richiedono una data Protection coerente, un recovery rapido e il rispetto degli standard normativi e di compliance. Inoltre, semplifica la gestione dei dati in diversi ambienti, sia on-premise che nel cloud, offrendo agli utenti la certezza che i loro dati saranno completi e inalterati durante i processi.



Le etichette di sicurezza NFS v4,2 hanno gli avvertimenti definiti in 2.

Controllo delle modifiche alle etichette

Il controllo delle modifiche alle etichette di sicurezza xattrs o NFS è un aspetto critico della gestione e della sicurezza del file system. Gli strumenti standard di audit del file system consentono il monitoraggio e la registrazione di tutte le modifiche apportate al file system, incluse le modifiche apportate agli xattrs e alle etichette di sicurezza.

Negli ambienti Linux, il `auditd` demone è comunemente usato per stabilire il controllo degli eventi del file system. Consente agli amministratori di configurare le regole per controllare chiamate di sistema specifiche correlate alle modifiche xattr, quali `setxattr`, `lsetxattr` e per impostare gli attributi e, `lremovexattr` e `fsetxattr` per la `fremovexattr` rimozione degli attributi `removexattr`.

ONTAP FPolicy estende queste funzionalità fornendo un solido framework per il monitoraggio e il controllo in tempo reale delle operazioni sui file. FPolicy può essere configurato per supportare vari eventi xattr, offrendo un controllo granulare sulle operazioni dei file e la capacità di applicare policy di gestione dei dati complete.

Per gli utenti che utilizzano xattrs, specialmente negli ambienti NFS v3 e NFS v4, sono supportate solo alcune combinazioni di operazioni e filtri per il monitoraggio. L'elenco delle combinazioni di operazioni e filtri supportate per il monitoraggio FPolicy degli eventi di accesso ai file NFS v3 e NFS v4 è descritto di seguito:

Operazioni di file supportate	Filtri supportati
setattr	offline-bit, setattr_with_owner_change, setattr_with_group_change, setattr_with_mode_change, setattr_with_modify_time_change, setattr_with_access_time_change, setattr_with_size_change, exclude_directory

Esempio di un frammento di registro auditd per un'operazione setattr:

```
type=SYSCALL msg=audit(1713451401.168:106964): arch=c000003e syscall=188
success=yes exit=0 a0=7fac252f0590 a1=7fac251d4750 a2=7fac252e50a0 a3=25
items=1 ppid=247417 pid=247563 auid=1112 uid=1112 gid=1112 euid=1112
suid=1112 fsuid=1112 egid=1112 sgid=1112 fsgid=1112 tty=pts0 ses=141
comm="python3" exe="/usr/bin/python3.9"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
key="*set-xattr*ARCH=x86_64 SYSCALL=**setxattr** AUID="jrsmith"
UID="jrsmith" GID="jrsmith" EUID="jrsmith" SUID="jrsmith"
FSUID="jrsmith" EGID="jrsmith" SGID="jrsmith" FSGID="jrsmith"
```

L'abilitazione "[FPolicy di ONTAP](#)" per gli utenti che lavorano con xattrs fornisce un livello di visibilità e controllo essenziale per mantenere l'integrità e la sicurezza del file system. Sfruttando le funzionalità di monitoraggio avanzate di FPolicy, le organizzazioni possono garantire che tutte le modifiche apportate agli xattrs vengano monitorate, controllate e allineate ai loro standard di sicurezza e conformità. Questo approccio proattivo alla gestione del file system è per questo motivo l'attivazione di ONTAP FPolicy è vivamente consigliata a tutte le organizzazioni che desiderano migliorare le proprie strategie di data governance e protezione.

Esempi di controllo dell'accesso ai dati

La seguente voce di esempio per i dati memorizzati nel cert PKI di John R. Smith mostra come l'approccio di NetApp può essere applicato a un file e fornire un controllo di accesso dettagliato.



Questi esempi sono a scopo illustrativo ed è responsabilità del cliente determinare i metadati associati alle etichette di sicurezza NFS v4,2 e agli xattrs. I dettagli sull'aggiornamento e sulla conservazione delle etichette vengono omessi per semplicità.

Esempio di valori cert PKI

Chiave	Valore
EntitySecurityMark	t:S01 = NON CLASSIFICATO
Info	<pre>{ "commonName": { "value": "Smith John R jrsmith" }, "emailAddresses": [{ "value": "jrsmith@dod.mil" }], "employeeId": { "value": "00000387835" }, "firstName": { "value": "John" }, "lastName": { "value": "Smith" }, "telephoneNumber": { "value": "938/260-9537" }, "uid": { "value": "jrsmith" } }</pre>
specifiche	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15
AdminOrganization	<pre>{ "value": "DoD" }</pre>

Chiave	Valore
briefing	[{ "value": "ABC1000" }, { "value": "DEF1001" }, { "value": "EFG2000" }]
CitizenshipStatus	{ "value": "US" }
giochi	[{ "value": "TS" }, { "value": "S" }, { "value": "C" }, { "value": "U" }]
CountryOfAffiliations	[{ "value": "USA" }]

Chiave	Valore
DigitalIdentifier	<pre>{ "classification": "UNCLASSIFIED", "value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us" }</pre>
DissemTos	<pre>{ "value": "DoD" }</pre>
DutyOrganization	<pre>{ "value": "DoD" }</pre>
EntityType	<pre>{ "value": "GOV" }</pre>
FineAccessControls	<pre>[{ "value": "SI" }, { "value": "TK" }, { "value": "NSYS" }]</pre>

Questi diritti PKI mostrano i dettagli di accesso di John R. Smith, incluso l'accesso per tipo di dati e attribuzione.

Negli scenari in cui i metadati IC-TDF vengono archiviati separatamente dal file, NetApp sostiene la necessità di un ulteriore livello di controllo degli accessi dettagliato. Ciò comporta l'archiviazione delle informazioni di controllo dell'accesso sia a livello di directory che in associazione con ciascun file. Ad esempio, considerare i seguenti tag collegati a un file:

- Etichette di sicurezza NFS v4.2: Utilizzate per prendere decisioni sulla sicurezza
- Xattrs: Fornire informazioni supplementari pertinenti al file e ai requisiti del programma organizzativo

Le seguenti coppie di valori chiave sono esempi di metadati che possono essere memorizzati come xattrs e offrono informazioni dettagliate sull'autore del file e sulle relative classificazioni di sicurezza. Tali metadati possono essere utilizzati dalle applicazioni client per prendere decisioni di accesso informate e organizzare i file in base a standard e requisiti organizzativi.

Esempio di coppie chiave-valore xattr

Chiave	Valore
user.uuid	"761d2e3c-e778-4ee4-997b-3bb9a6a1d3fa"
user.entitySecurityMark	"UNCLASSIFIED"
user.specification	"INFO"

Chiave	Valore
user.info	<pre>{ "commonName": { "value": "Smith John R jrsmith" }, "currentOrganization": { "value": "TUV33" }, "displayName": { "value": "John Smith" }, "emailAddresses": ["jrsmith@example.org"], "employeeId": { "value": "00000405732" }, "firstName": { "value": "John" }, "lastName": { "value": "Smith" }, "managers": [{ "value": "" }], "organizations": [{ "value": "TUV33" }, { "value": "WXY44" }], "personalTitle": { "value": "" }, "secureTelephoneNumber": { "value": "506-7718" }, "telephoneNumber": { "value": "264/160-7187" }, "title": { "value": "Software Engineer" }, }</pre>

Chiave	Valore
user.geo_point	[-78.7941, 35.7956]

}

Informazioni correlate

}

- ["NFS in NetApp ONTAP: Best practice e guida all'implementazione"](#)
- ["Riferimento comando ONTAP"](#)
- Richiesta di commenti (RFC)
 - ["RFC 7204: Requisiti per NFS etichettato"](#)
 - ["RFC 2203: Specifica del protocollo RPCSEC_GSS"](#)
 - ["RFC 3530: Protocollo NFS \(Network file System\) versione 4"](#)

Protezione avanzata

Guide alla protezione avanzata di ONTAP

Questi report tecnici forniscono indicazioni su come rafforzare NetApp ONTAP e altri prodotti NetApp.



Questi report tecnici si espandono nella "Sicurezza ONTAP e crittografia dei dati" documentazione del prodotto.

Guide per la protezione avanzata

"[TR-4569: Guida alla protezione avanzata per NetApp ONTAP](#)" Scoprite come configurare NetApp ONTAP per aiutare le organizzazioni a soddisfare gli obiettivi di protezione prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

"[Guida alla protezione avanzata per gli strumenti ONTAP per VMware vSphere](#)" Scopri come configurare gli strumenti ONTAP per VMware vSphere per aiutare le organizzazioni a soddisfare gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

"[TR-4957: Guida alla protezione avanzata per NetApp SnapCenter](#)"

Scopri come configurare il software NetApp SnapCenter per aiutare le organizzazioni a raggiungere gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

"[TR-4963: Guida al rafforzamento della sicurezza: NetApp Backup and Recovery for Applications](#)" Scopri come configurare NetApp Cloud Backup for Applications per aiutare le organizzazioni a soddisfare gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità dei sistemi informativi.

"[TR-4943: Guida alla protezione avanzata per NetApp Active IQ Unified Manager](#)"

Scopri come configurare NetApp Active IQ Unified Manager per aiutare le organizzazioni a raggiungere gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

"[TR-4945: Guida al rafforzamento della protezione per l'SDK per la gestibilità NetApp](#)"

Scopri come configurare l'SDK per la gestibilità NetApp (NMSDK) per aiutare le organizzazioni a raggiungere gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

"[Guida alla protezione avanzata per host e database MetroCluster Tiebreaker](#)" Scopri come configurare l'host e il database di NetApp MetroCluster Tiebreaker per aiutare le organizzazioni a soddisfare gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informatico.

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 del report tecnico *TR-4569: Security Hardening Guide for ONTAP*, precedentemente pubblicato in formato PDF, è disponibile su docs.netapp.com.

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

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 di comando (DEFAULT)
admin-no-fsa (Disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	<ul style="list-style-type: none"> • Tutte le directory di comando (DEFAULT) • security login rest-role • security login role
Di sola lettura	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	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** ruolo viene assegnato all'account predefinito **autosupport**, utilizzato da AutoSupport OnDemand. ONTAP non consente di modificare o eliminare l'**autosupport** account. ONTAP impedisce inoltre di assegnare il **autosupport** ruolo ad altri account utente.

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

Nome del ruolo	Funzionalità

vsadmin	<ul style="list-style-type: none"> • Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestisci i volumi, tranne che per gli spostamenti dei volumi • Gestisci quote, qtree, 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	<ul style="list-style-type: none"> • Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestisci i volumi, tranne che per gli spostamenti dei volumi • Gestisci quote, qtree, 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 relazioni e snapshot SnapMirror • Visualizzare volumi e informazioni sulla rete
vsadmin-snaplock	<ul style="list-style-type: none"> • Gestire la password locale del proprio account utente e le informazioni relative alla chiave • Gestisci i volumi, tranne che per gli spostamenti dei volumi • Gestisci quote, qtree, 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	<ul style="list-style-type: none"> • 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 password l'autenticazione. 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
<code>cert</code>	Autenticazione del certificato SSL
<code>community</code>	Stringhe di comunità SNMP
<code>domain</code>	Autenticazione Active Directory
<code>nsswitch</code>	Autenticazione LDAP o NIS
<code>password</code>	Password
<code>publickey</code>	Autenticazione a chiave pubblica
<code>usm</code>	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 o `password` come `-authentication-method` o `-second-authentication-method`. Tuttavia, durante l'autenticazione SSH, l'ordine è sempre `publickey` 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 ridefinizione degli account.



Non è possibile rimuovere o rinominare gli account predefiniti. Se un amministratore rimuove l'account, al riavvio l'account predefinito verrà ricreato. **NetApp consiglia** di bloccare tutti gli account predefiniti non necessari con il comando lock.

Sebbene gli account orfani rappresentino un problema di sicurezza significativo, **NetApp consiglia vivamente** di testare l'effetto della rimozione degli account dal repository 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.
```

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 snapshot, solo dopo l'approvazione 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".
- "Attivazione 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, un "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 delle istantanee

Il blocco degli snapshot è una funzionalità SnapLock in cui gli snapshot vengono resi indelebili manualmente o automaticamente, con un periodo di conservazione nel criterio dello snapshot del volume. Lo scopo del blocco delle snapshot è impedire agli amministratori non autorizzati o non attendibili di eliminare le snapshot su un sistema ONTAP primario o secondario.

Il blocco delle istantanee è stato introdotto in ONTAP 9.12.1. Il blocco delle istantanee viene anche definito blocco delle istantanee a prova di manomissione. Sebbene richieda la licenza SnapLock e l'inizializzazione del clock di conformità, il blocco delle snapshot non è correlato a SnapLock Compliance o 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 alle snapshot SnapVaulting su un sistema secondario. È possibile ottenere un rapido recovery degli snapshot bloccati sui sistemi primari per ripristinare i volumi corrotti dal ransomware.

Per ulteriori informazioni, vedere "[documentazione del blocco delle istantanee](#)".

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'utente interno autosupport, 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.

A partire dal 9.14.1, vi sono regole di blocco e complessità maggiori per le password che si applicano solo alle nuove installazioni di ONTAP.

Tutte le password devono essere distinte dal nome utente.

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	-

Attributo	Descrizione	Predefinito	Raggio d'azione
lockout-duration	Periodo di blocco massimo (in giorni)	L'impostazione predefinita è 0, ovvero l'account è bloccato per un giorno	-
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
```

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
vs0          aes256-ctr,    diffie-helman-group-
              aes192-ctr,    exchange-sha256,
              aes128-ctr,    ecdh-sha2-nistp384
vs1          aes128-gcm   curve25519-sha256
              aes256-ctr,    diffie-hellman-group-
              aes192-ctr,    exchange-sha256
              aes128-ctr,    ecdh-sha2-nistp384
              3des-cbc,     ecdh-sha2-nistp512
              aes128-gcm
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	<p>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 "-".</p> <p>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.</p> <p>I caratteri non ASCII devono utilizzare Unicode UTF-8.</p>
uri	`(ftp
http://(hostname	<p>IPv4`</p> <p>Utilizzare questo parametro per specificare l'URI da cui viene scaricato il banner di accesso.</p> <p>La lunghezza del messaggio non deve superare i 2048 byte. I caratteri non ASCII devono essere forniti come Unicode UTF-8.</p>

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	<p>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 <code>-vserver</code> 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:</p> <ul style="list-style-type: none"> • <code>\\\</code> - Un singolo carattere di gioco • <code>\b</code> - Nessun output (supportato solo per la compatibilità con Linux) • <code>\C</code> - Nome cluster • <code>\d</code> - La data corrente impostata sul nodo di accesso • <code>\t</code> - Ora corrente impostata sul nodo di accesso • <code>\I</code> - Indirizzo IP LIF in entrata (stampa la console per <code>console</code> l'accesso) • <code>\l</code> - Nome dispositivo di accesso (stampa la console per un <code>console login</code>) • <code>\L</code> - Ultimo accesso per l'utente su qualsiasi nodo nel cluster • <code>\m</code> - Architettura della macchina • <code>\n</code> - Nome SVM del nodo o dei dati • <code>\N</code> - Nome dell'utente che effettua l'accesso • <code>\o</code> - Uguale a <code>\O</code>. Fornito per la compatibilità con Linux. • <code>\O</code> - Nome dominio DNS del nodo. Si noti che l'output dipende dalla configurazione di rete e potrebbe essere vuoto. • <code>\r</code> - Numero di versione del software • <code>\s</code> - Nome del sistema operativo • <code>\u</code> - 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. • <code>\U</code> - Uguale a <code>\u</code>, ma ha <code>user</code> o <code>users</code> aggiunto • <code>\v</code> - Stringa della versione del cluster effettiva • <code>\w</code> - Sessioni attive nel cluster per l'accesso dell'utente (<code>who</code>)

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 le `http` applicazioni e `ontapi` l'aggiunta dell' `console` applicazione 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-security-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 dal 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 dal ransomware	La protezione autonoma da ransomware è supportata su diverse SVM, ma non ancora configurate.
FPolicy nativo non è configurato	FPolicy non è impostato per SVM NAS.
Abilita la modalità attiva della 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](#)".

Timeout sessione di System Manager

È possibile modificare il timeout di inattività della sessione di System Manager. Il timeout di inattività predefinito è 30 minuti. Un timeout è importante per evitare sessioni stalose e piggybacking di sessione.



Se SAML è configurato, il timeout di inattività è controllato dalle impostazioni sull'IdP.

Fasi

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. In **Impostazioni UI**, selezionare .
3. Nella casella **Timeout inattività**, digitare un valore compreso tra 2 e 180 o immettere "0" per disattivare il timeout.
4. Selezionare **Salva**.

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, crea una snapshot e informa l'amministratore quando si sospetta un attacco.

Oltre al rilevamento e alla prevenzione del ransomware mediante l'analisi comportamentale degli utenti (UBA) esterna di FPolicy con NetApp Data Infrastructure Insights Storage Workload Security e l'ecosistema di partner NetApp FPolicy, ONTAP 9.10.1 introduce una protezione autonoma dal ransomware. La protezione autonoma contro i ransomware ONTAP utilizza una funzionalità di apprendimento automatico (ML) integrata che analizza l'attività del carico di lavoro in volume e l'entropia dei dati per rilevare automaticamente i ransomware. Monitora le attività diverse da quelle di UBA, in modo da poter rilevare attacchi che UBA non rileva.

Per informazioni più dettagliate su questa funzionalità, vedere "["Soluzioni 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 di 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 in ONTAP

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 deduplicazione aggregata. I volumi NAE partecipano e traggono vantaggio dalla deduplicazione 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 comando `security key-manager setup` 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 preconddivisa (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 via cavo NFS richiedeva la configurazione e la configurazione di Kerberos per utilizzare 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).
```

Informazioni correlate

["Preparare l'utilizzo della protezione IP sulla rete ONTAP"](#)

Modalità FIPS e gestione TLS e SSL in ONTAP

Lo standard FIPS 140-2 specifica i requisiti di sicurezza per i moduli crittografici all'interno dei sistemi di sicurezza che proteggono le informazioni sensibili nei sistemi informatici e di telecomunicazione. Lo standard FIPS 140-2 si applica *specificamente* al modulo crittografico, piuttosto che al prodotto, all'architettura, ai dati o all'ecosistema. Il modulo crittografico è il componente specifico (hardware, software, firmware o una combinazione dei tre) che implementa le funzioni di sicurezza approvate da NIST.

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.

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.

Configurazione NetApp ONTAP in modalità FIPS

NetApp ONTAP dispone di una configurazione in modalità FIPS che crea un'istanza di un livello di protezione aggiuntivo per il piano di controllo:

- A partire da ONTAP 9.11.1 quando la modalità di conformità FIPS 140-2 è abilitata, TLSv1, TLSv1.1 e SSLv3 sono disabilitati e solo TSLv1.2 e TSLv1.3 rimangono abilitati. Riguarda altri sistemi e comunicazioni interni ed esterni a ONTAP 9. Se si attiva la modalità di conformità FIPS 140-2 e successivamente si disattiva, TLSv1, TLSv1.1 e SSLv3 rimangono disattivati. TLSv1.2 o TLSv1.3 resteranno abilitati a seconda della configurazione precedente.
- Per le versioni di ONTAP precedenti alla 9.11.1 quando la modalità di conformità FIPS 140-2 è abilitata, sia TLSv1 che SSLv3 sono disabilitati e solo TLSv1.1 e TLSv1.2 rimangono abilitati. ONTAP impedisce di abilitare sia TLSv1 che SSLv3 quando è attivata la modalità di conformità FIPS 140-2. Se si attiva la modalità di conformità FIPS 140-2 e successivamente la si disattiva, TLSv1 e SSLv3 rimangono disattivati, ma TLSv1.2 o TLSv1.1 e TLSv1.2 vengono attivati a seconda della configurazione precedente.
- "[Modulo di protezione crittografica NetApp \(NCSM\)](#)", Convalidato FIPS 140-2 livello 1, garantisce la conformità basata su software.

 NIST ha inviato uno standard FIPS-140-3 e NCSM disporrà di convalide FIPS-140-2 e FIPS-140-3. Tutte le convalide FIPS 140-2 passeranno allo stato storico il 21 settembre 2026, ovvero cinque anni dopo l'ultimo giorno per la presentazione dei nuovi certificati.

Attiva la modalità di conformità FIPS-140-2 e FIPS-140-3-2

A partire da ONTAP 9, puoi abilitare la modalità di conformità FIPS-140-2 e FIPS-140-3 per le interfacce planari di controllo a livello del cluster.

- "[Attiva FIPS](#)"
- "[Visualizza stato FIPS](#)"

Abilitazione e protocolli FIPS

Il security config modify comando consente di modificare la configurazione di sicurezza esistente a livello del cluster. Se si attiva 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 i protocolli TLSv1,3 (a partire da ONTAP 9.11.1) e TLSv1,2 sono attivati.
- Nelle precedenti versioni di ONTAP i seguenti protocolli TLS erano attivati per impostazione predefinita:
 - TLSv1,1 (disattivata per impostazione predefinita a partire da ONTAP 9.12.1)
 - TLSv1 (disattivata per impostazione predefinita a partire da ONTAP 9.8)
- Per la compatibilità con le versioni precedenti, ONTAP supporta l'aggiunta di SSLv3 all'elenco dei protocolli supportati quando la modalità FIPS è disattivata.

Abilitazione FIPS e cifrari

- Utilizzare il `-supported-cipher-suites` parametro per configurare solo AES (Advanced Encryption Standard) o AES e 3DES.
- È 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 attivate, ad eccezione di quelle che utilizzano algoritmi di crittografia a 64 o 56 bit senza autenticazione, senza crittografia, senza esportazione e suite di crittografia a bassa crittografia.

- 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 il "[pagina cifrari](#)" documento su OpenSSL (pubblicato 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.

Protezione avanzata della sicurezza SSH e TLS

L'amministrazione SSH di ONTAP 9 richiede 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.

Per rafforzare la protezione TLS, abilitare solo TLS 1,2 e utilizzare suite di crittografia in grado di garantire il Perfect Forward Secrecy (PFS). 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 decriptografare tutte le sessioni di rete tra un client e un server.

Attivare suite di crittografia compatibili con TLSv1,2 e PFS

Per attivare solo suite di crittografia compatibili con TLS 1,2 e PFS, utilizzare il `security config modify` comando dal livello di privilegi avanzato.

 Prima di modificare la configurazione dell'interfaccia SSL, assicurarsi che il client supporti i cifrari DHE ed ECDHE quando si effettua la connessione a ONTAP per mantenere la connettività con ONTAP.

Esempio

```
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](#)".

Informazioni correlate

["Pubblicazione Federal Information Processing Standard \(FIPS\) 140"](#)

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`, `kmp`, `ldap_ad`, `ldap_nis_namemap`, o `all`. 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	-

Cifrari	Scambio di chiavi
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](#)" 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 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 sicurezza richiede convalida. ONTAP fornisce un numero maggiore di eventi e dettagli di auditing in tutta la soluzione. Poiché i file system NAS occupano una posizione sempre maggiore nell'attuale panorama delle minacce, le funzioni di audit sono fondamentali per supportare la visibilità. Grazie alle funzionalità di audit migliorate in ONTAP, i dettagli di audit CIFS sono più numerosi 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 ai file creando un ruolo API REST che non ha accesso ai volumi ONTAP via REST. Per assegnare questo ruolo, completare i passaggi seguenti.

 L'API REST `/api/storage/volumes` viene utilizzata per scopi che vanno oltre il semplice accesso ai file. Viene utilizzata da System Manager e da altre interfacce GUI per creare, visualizzare e modificare volumi.

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 lettura-scrittura (-rwrule)
Superuser di sola lettura	Sola lettura (-rorule) e. -superuser
Lettura/scrittura superutente	Sola lettura (-rorule) e lettura-scrittura (-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 ...	Poi ...
Corrisponde a un tipo di protezione specificato nel parametro di accesso.	Il client riceve l'accesso per quel livello con il proprio ID utente.

Se il tipo di protezione del client ...	Poi ...
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.	<p>Il client non riceve alcun accesso per quel livello.</p> <p></p> <p>Questa restrizione non si applica al -superuser parametro perché questo parametro non include sempre nessuno, anche se non specificato.</p>

Kerberos 5 e Krb5p

A partire da ONTAP 9, è supportata l'autenticazione Kerberos 5 con servizio di privacy (krb5p). La modalità di autenticazione krb5p 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

- 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 ridefinizione 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.

Caratteristiche di sicurezza dei ruoli LIF in ONTAP

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 dei dati	LIF cluster	LIF di gestione dei nodi	LIF di gestione del cluster	Intercluster LIF
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.
 • I ruoli LIF non devono mai essere esposti a Internet.

Per saperne di più sulla protezione dei LIF, vedere "[Configurare le policy firewall per le LIF](#)". Questa pagina fornisce anche dettagli sulle policy del servizio LIF a partire da ONTAP 9.10.1.

Per saperne di più su come creare una nuova policy di servizio, vedere `network interface service-policy create` comando nel "[Riferimento ai comandi](#)".

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

Servizio	Porta/protocollo	Descrizione
telnet	23/TCP	Accesso remoto
Domain	53/TCP	Server dei nomi di dominio
HTTP	80/TCP	HTTP
	80/UDP	
rpcbind	111/TCP 111/UDP	Chiamata di procedura remota
NTP	123/UDP	Network Time Protocol
msrpc	135/TCP	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
Mdns	5353/UDP	DNS multicast
HTTPS	5986/UDP	Porta HTTPS: Protocollo binario in ascolto

Servizio	Porta/protocollo	Descrizione
TELNET	8023/TCP	Telnet con ambito di nodo
HTTPS	8443/TCP	7MTT strumento GUI tramite xref:./ontap-security-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
931	RPC cluster NetApp
932	RPC cluster NetApp

Porta/protocollo	Descrizione
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
7824	RPC cluster NetApp

Report tecnici di ONTAP SnapCenter

SnapCenter offre una piattaforma unificata per la protezione dei dati coerente con l'applicazione e la gestione dei cloni. SnapCenter semplifica il backup, il ripristino e la gestione del ciclo di vita dei cloni con flussi di lavoro integrati nell'applicazione. Sfruttando la gestione dei dati basata sullo storage, SnapCenter consente di aumentare le performance e la disponibilità e ridurre i tempi di test e sviluppo.



Questi report tecnici si espandono nella "["SnapCenter"](#) documentazione del prodotto.

SnapCenter per Oracle

["TR-4700: Plug-in SnapCenter per le Best practice del database Oracle"](#)

NetApp SnapCenter è una piattaforma unificata e scalabile per la protezione dei dati coerente con Oracle che automatizza operazioni complesse con controllo e supervisione centralizzati. Scopri le procedure consigliate per l'implementazione di database Oracle con SnapCenter.

["TR-4964: Backup, ripristino e clonazione di database Oracle con i servizi SnapCenter"](#) Scopri come configurare SnapCenter Services per il backup, il ripristino e la clonazione di database Oracle implementati in Amazon FSX per lo storage ONTAP e di istanze di calcolo EC2. Sebbene sia molto più semplice da configurare e utilizzare, i servizi SnapCenter offrono funzionalità chiave disponibili tramite l'interfaccia SnapCenter.

SnapCenter per Microsoft SQL Server

["TR-4714: Best practice per Microsoft SQL Server con NetApp SnapCenter"](#)

Scopri come implementare con successo Microsoft SQL Server sullo storage NetApp utilizzando SnapCenter per la protezione dei dati.

SnapCenter per server Microsoft Exchange

["TR-4681: Best practice per Microsoft Exchange Server con NetApp SnapCenter"](#)

Scopri come implementare con successo Microsoft Exchange Server sullo storage NetApp utilizzando SnapCenter per la protezione dei dati.

SnapCenter per SAP HANA

["TR-4614: Backup e recovery SAP HANA con SnapCenter"](#) SnapCenter è una piattaforma unificata e scalabile per la data Protection coerente con l'applicazione per SAP HANA e altri database. SnapCenter offre controllo e supervisione centralizzati, delegando al contempo la capacità degli utenti di gestire processi di backup, ripristino e clonazione specifici dell'applicazione. Con SnapCenter, gli amministratori di database e storage imparano a utilizzare un unico strumento per gestire le operazioni di backup, ripristino e clonazione per una vasta gamma di applicazioni e database.

["TR-4926: SAP HANA su Amazon FSX per NetApp ONTAP - Backup e recovery con SnapCenter"](#) Scopri le pratiche consigliate per la data Protection di SAP HANA in Amazon FSX per NetApp ONTAP e SnapCenter. Gli argomenti trattati includono i concetti di SnapCenter, i consigli di configurazione e i flussi di lavoro operativi, tra cui configurazione, operazioni di backup, e operazioni di ripristino e recovery.

["TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"](#) Il cloning dello storage SnapCenter e l'opzione di definire in maniera flessibile le operazioni di pre-cloning e post-cloning consentono agli amministratori di base SAP di accelerare e automatizzare le operazioni di refresh, cloning o copia del sistema SAP. Scopri ora la possibilità di scegliere qualsiasi backup Snapshot di SnapCenter in qualsiasi storage primario o secondario consente di affrontare i casi di utilizzo più importanti, tra cui corruzione logica, test di disaster recovery o il refresh di un sistema QA SAP.

["TR-4719: Backup e ripristino della replica del sistema SAP HANA con SnapCenter"](#)

Scopri come utilizzare la tecnologia SnapCenter e il plug-in SAP HANA per il backup e il ripristino in un ambiente di replica del sistema SAP HANA.

["TR-4667: Automazione delle operazioni di copia e clonazione del sistema SAP HANA con SnapCenter"](#) La possibilità di creare backup di Snapshot NetApp coerenti con l'applicazione nel layer di storage è la base per le operazioni di copia del sistema e cloning del sistema. I backup Snapshot basati sullo storage vengono creati utilizzando il plug-in NetApp SnapCenter per SAP HANA e le interfacce fornite dal database SAP HANA. SnapCenter registra i backup Snapshot nel catalogo di backup SAP HANA in modo che possano essere utilizzati per il ripristino e il ripristino, nonché per le operazioni di cloning.

Guida alla protezione avanzata di SnapCenter

["TR-4957: Guida alla protezione avanzata per NetApp SnapCenter"](#)

Scopri come configurare SnapCenter per aiutare le organizzazioni a raggiungere gli obiettivi di sicurezza prescritti per la riservatezza, l'integrità e la disponibilità del sistema informativo.

Report tecnici sul tiering ONTAP

Con la soluzione di tiering dei dati FabricPool, l'esperienza utente complessiva dei sistemi flash di un'azienda migliora, evitando al tempo stesso i problemi legati alla riprogettazione delle applicazioni per l'efficienza dello storage. FabricPool riduce l'impatto dello storage e i costi associati dell'ambiente di un sistema. I dati attivi rimangono su SSD dalle performance elevate. I dati inattivi vengono suddivisi in livelli per lo storage a oggetti a basso costo, preservando al contempo l'efficienza dello storage.



Questi report tecnici si espandono nella "[ONTAP FabricPool](#)" documentazione del prodotto.

["TR-4598: Best practice FabricPool"](#)

Scopri le funzionalità, i requisiti, l'implementazione e le procedure consigliate per FabricPool.

["TR-4826: Guida ai consigli di NetApp FabricPool con StorageGRID"](#)

Scopri le procedure consigliate per l'implementazione e il dimensionamento di StorageGRID come livello di capacità per il componente ONTAP FabricPool. Il presente documento illustra inoltre le funzionalità, i requisiti, l'implementazione e le procedure consigliate per l'utilizzo di StorageGRID.

["TR-4695: Tiering dello storage del database con NetApp FabricPool"](#)

Scopri i vantaggi e le opzioni di configurazione di FabricPool con diversi database, incluso il sistema di gestione dei database relazionali Oracle (RDBMS).

Report tecnici sulla virtualizzazione di ONTAP

Le soluzioni di virtualizzazione NetApp ti aiutano a offrire il massimo valore dai tuoi server. Grazie a un'infrastruttura server virtuale reattiva basata su sistemi flash ONTAP dalle performance elevate e all'avanguardia, potrai accedere ai dati molto più rapidamente. La tua infrastruttura virtuale granulare è scalabile senza interruzioni per diversi petabyte di dati, offrendo le performance necessarie per l'accesso condiviso a più carichi di lavoro. ONTAP aiuta a ottimizzare e ridurre la complessità dell'implementazione dell'infrastruttura server virtuale con partnership chiave, guida all'implementazione, integrazione applicativa e design di livello superiore. ONTAP offre numerose procedure e soluzioni consigliate per un ambiente di virtualizzazione solido, sia on-premise che nel cloud.

Questi report tecnici si espandono nella "[Strumenti ONTAP per VMware vSphere](#)" documentazione del prodotto.

"TR-4597: VMware vSphere per ONTAP" ONTAP è una soluzione storage leader per gli ambienti VMware vSphere da quasi vent'anni e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo i costi. Questo documento presenta la soluzione ONTAP per vSphere, incluse le informazioni più recenti sui prodotti e le procedure consigliate, per ottimizzare l'implementazione, ridurre i rischi e semplificare la gestione.

"TR-4400: Volumi virtuali VMware vSphere (vVol) con NetApp ONTAP" ONTAP è una soluzione storage leader per gli ambienti VMware vSphere da oltre vent'anni e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo i costi. Il presente documento illustra le funzionalità di ONTAP per i volumi virtuali VMware vSphere (vVol), incluse le informazioni più recenti sui prodotti e i casi di utilizzo, oltre a procedure consigliate e altre informazioni per semplificare l'implementazione e ridurre gli errori.

"TR-4900: VMware Site Recovery Manager con NetApp ONTAP" ONTAP è una soluzione storage leader per gli ambienti VMware vSphere fin dall'introduzione nel moderno data center nel 2002 e continua ad aggiungere funzionalità innovative per semplificare la gestione riducendo i costi. In questo documento viene presentata la soluzione ONTAP per VMware Site Recovery Manager (SRM), il software di disaster recovery (DR) leader del settore di VMware, che include le informazioni più recenti sui prodotti e le procedure consigliate per semplificare la distribuzione, ridurre i rischi e semplificare la gestione continua.

"Introduzione all'automazione per ONTAP e vSphere" L'automazione è parte integrante della gestione degli ambienti VMware sin dai primi giorni di VMware ESX. La capacità di implementare l'infrastruttura come codice ed estendere le pratiche alle operazioni del cloud privato aiuta ad alleviare i problemi legati a scalabilità, flessibilità, self-provisioning ed efficienza. Questo documento presenta la soluzione ONTAP per l'automazione dell'ambiente ONTAP e VMware vSphere.

"WP-7353: Strumenti ONTAP per VMware vSphere - sicurezza del prodotto" Questo documento descrive le tecniche e la tecnologia utilizzate per proteggere gli strumenti ONTAP per VMware vSphere 9.X dalle minacce esistenti ed emergenti negli ambienti di prodotto.

"WP-7355: Plug-in SnapCenter VMware vSphere - sicurezza del prodotto" Questo documento descrive le tecniche e la tecnologia utilizzate per proteggere il plug-in NetApp SnapCenter per VMware vSphere 4.X dalle minacce esistenti ed emergenti negli ambienti di prodotto.

"TR-4568: Linee guida per l'implementazione di NetApp e Best practice per lo storage per Windows Server" Microsoft Windows Server è un sistema operativo di classe Enterprise che copre networking, sicurezza, virtualizzazione, cloud, infrastruttura desktop virtuale, protezione degli accessi, protezione delle informazioni,

servizi Web, infrastruttura della piattaforma applicativa e molto altro. Il presente documento si concentra su Microsoft Windows, che si concentra in particolare sulla tecnologia di virtualizzazione Hyper-V, incluse le ultime informazioni sui prodotti e le pratiche consigliate, al fine di semplificare l'installazione, ridurre i rischi e semplificare la gestione.

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Direttiva sulla privacy

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

ONTAP

"Avviso per ONTAP 9.16.1" "Avviso per ONTAP 9.16.0" "Avviso per ONTAP 9.15.1" "Avviso per ONTAP 9.15.0" "Avviso per ONTAP 9.14.1" "Avviso per ONTAP 9.14.0" "Avviso per ONTAP 9.13.1" "Avviso per ONTAP 9.12.1" "Avviso per ONTAP 9.12.0" "Avviso per ONTAP 9.11.1" "Avviso per ONTAP 9.10.1" "Avviso per ONTAP 9.10.0" "Avviso per ONTAP 9.9.1" "Avviso per ONTAP 9.8" "Avviso per ONTAP 9,7" "Avviso per ONTAP 9,6" "Avviso per ONTAP 9,5" "Avviso per ONTAP 9,4" "Avviso per ONTAP 9,3" "Avviso per ONTAP 9,2" "Avviso per ONTAP 9,1"

ONTAP Mediator per configurazioni IP MetroCluster

"9,9,1 Avviso per ONTAP Mediator per le configurazioni IP di MetroCluster" "9,8 Avviso per ONTAP Mediator per le configurazioni IP di MetroCluster" "9,7 Avviso per ONTAP Mediator per le configurazioni IP di MetroCluster"

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.