Sicurezza

ONTAP Technical Reports

NetApp
January 23, 2026

Sommario

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 resilienti 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 (xattrs) 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.

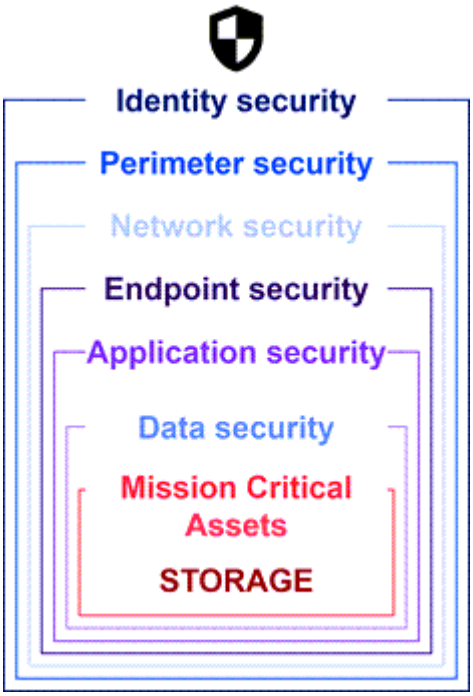
Le organizzazioni devono guardare nell'intera posizione di sicurezza da perimetro, rete, identità, applicazioni e dove si trovano i dati a livello di storage e mettere al sicuro questi layer. L'adozione di un approccio incentrato sui dati alla cyber Protection nel layer di storage è fondamentale nel 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 NetAppFornisce 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.

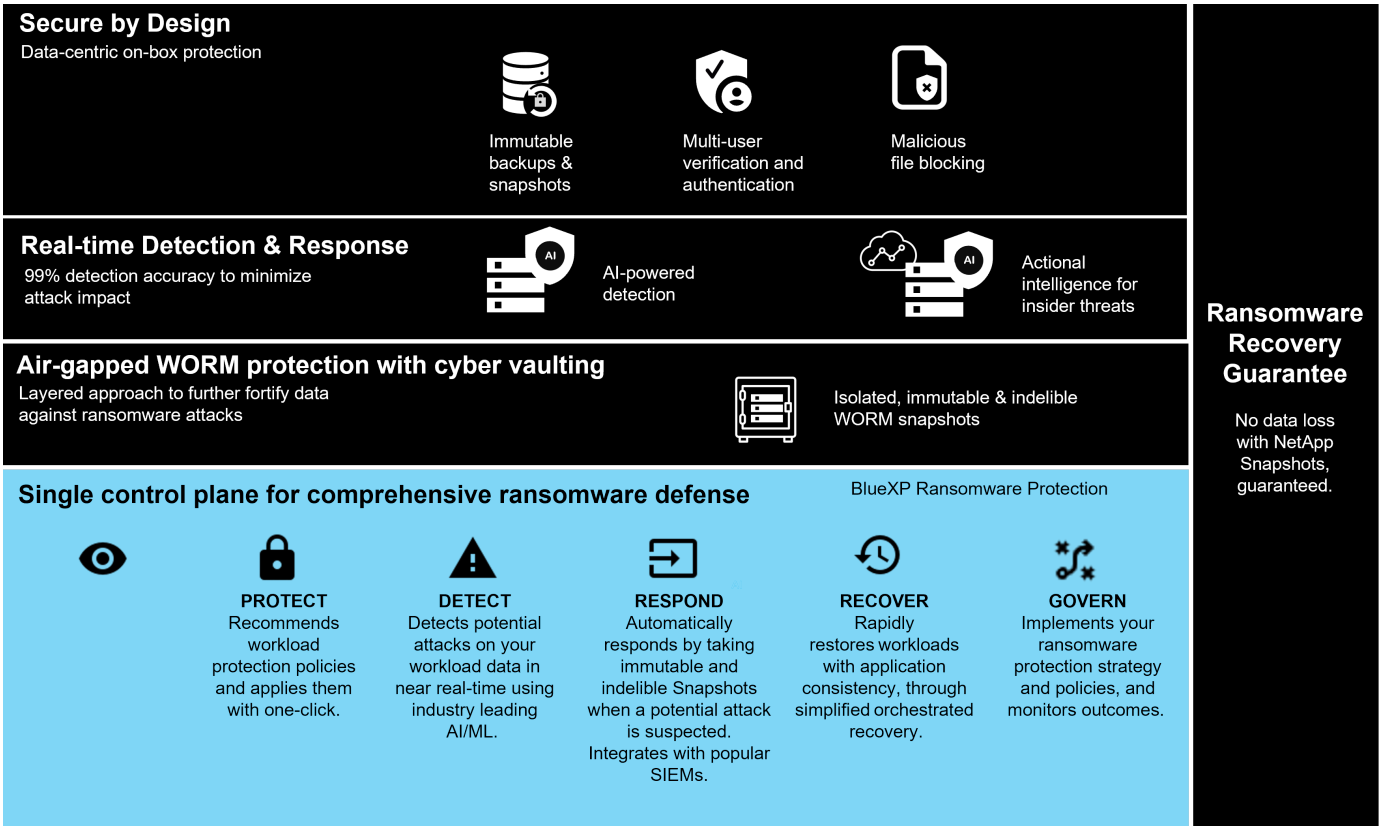
Protezione dal ransomware ai layer di dati

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 proteggerti 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.

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"

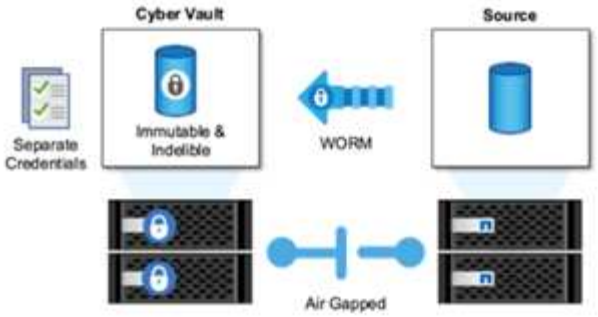
Protezione DA WORM a mappatura D'aria con cyber vaulting in ONTAP

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 Snapshot 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.

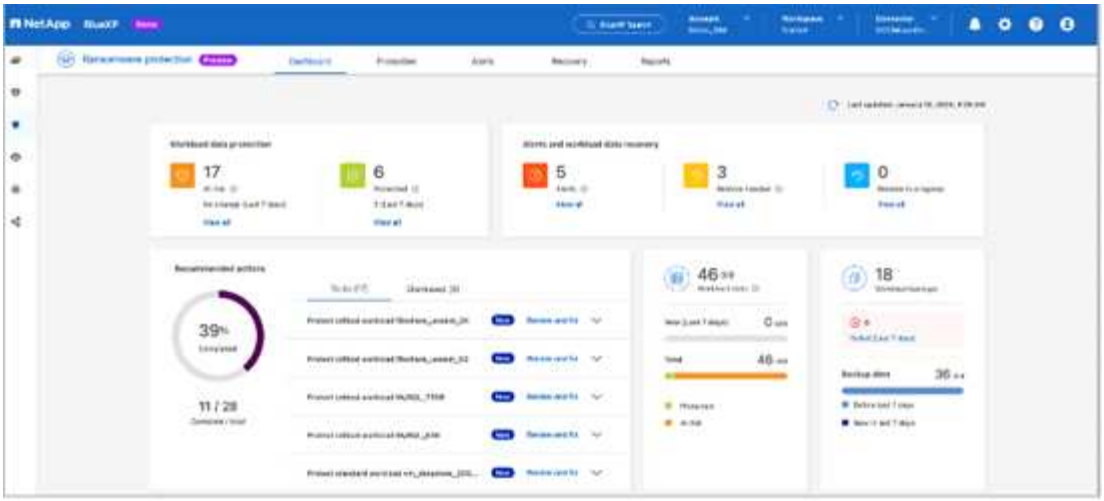
Per vedere la protezione dal ransomware in azione, consulta "Consulente digitale".

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.

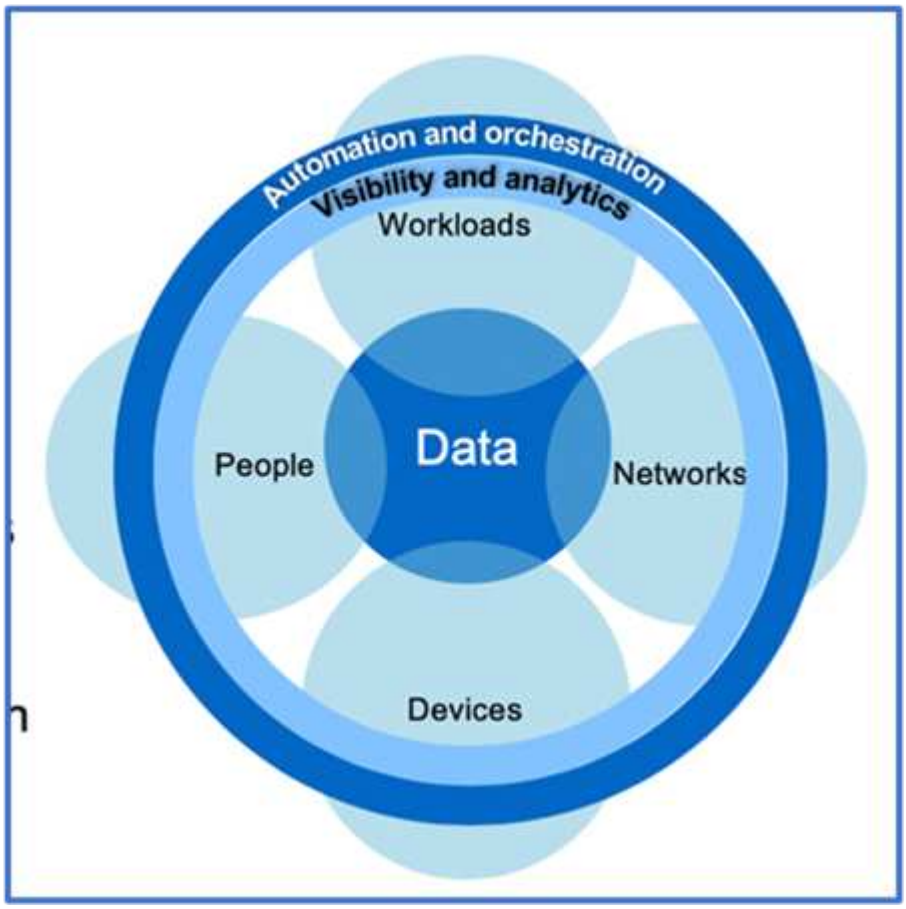
Risorse di sicurezza

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.

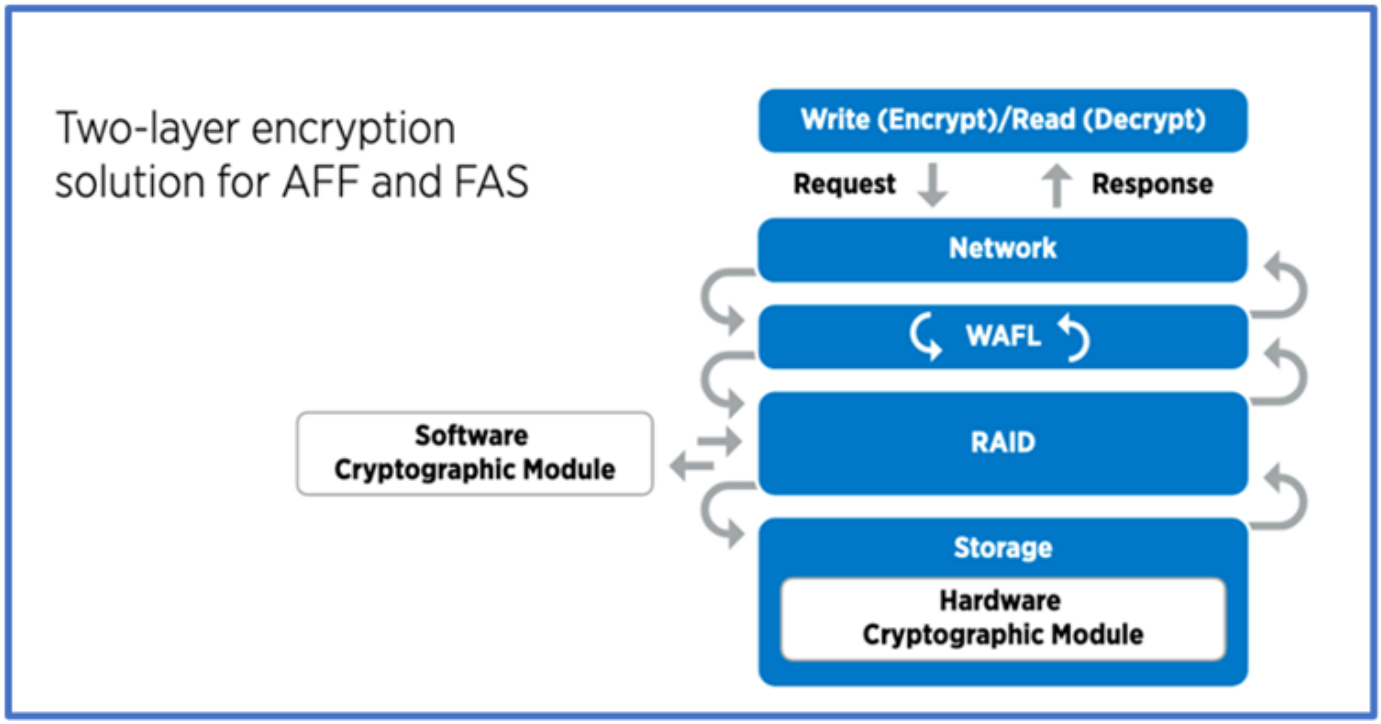
Utilizza la crittografia per i dati a riposo e in uso

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 amp;#44; crittografia dei volumi NetApp (NVE) e amp;#44; 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.



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.

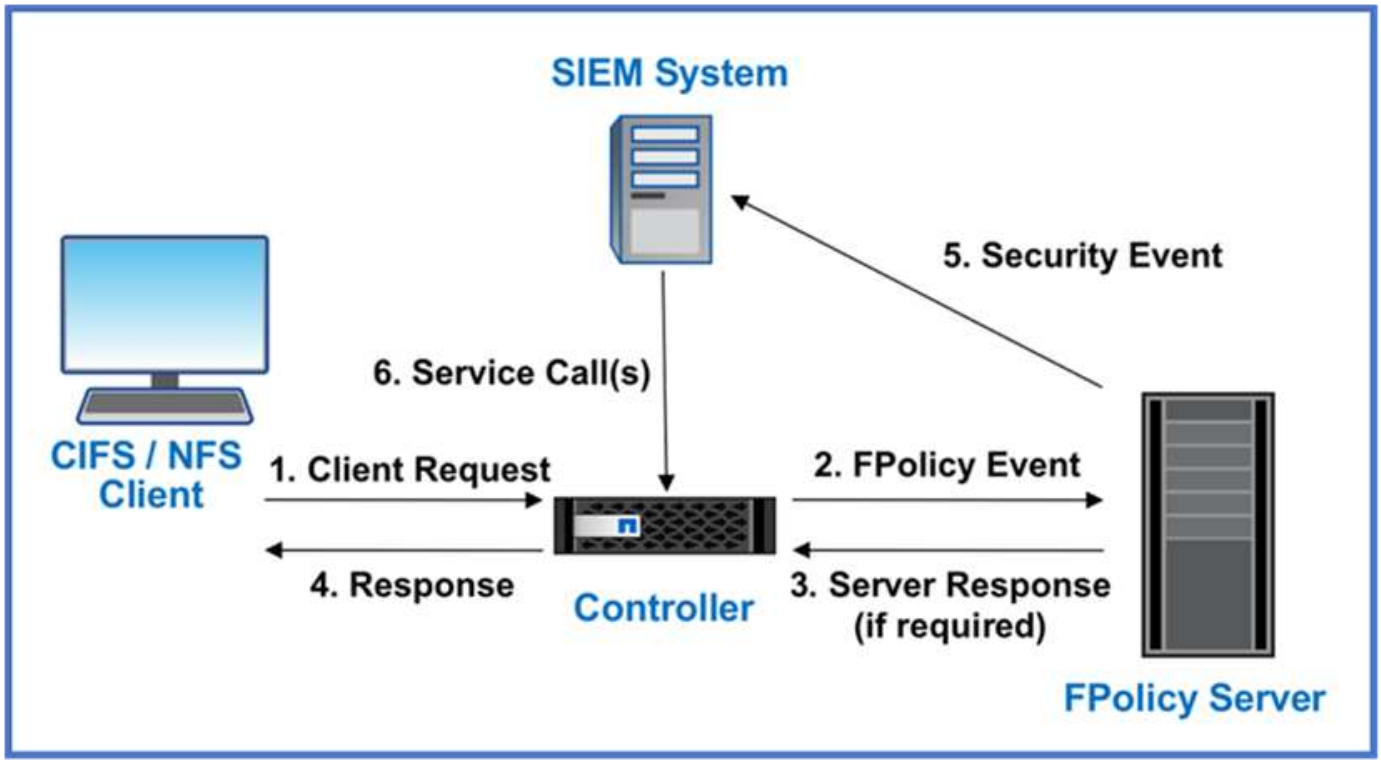
Crittografia dei dati in-flight

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 (xattrs) 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 xattrs è conforme agli standard NIST per le soluzioni ABAC, come indicato nella Pubblicazione speciale

NIST 800-162.

È possibile utilizzare le etichette di sicurezza e gli xattrs 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 (xattrs) 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`	`sysadm_r`	`sysadm_t`	`t:s0`
`jrsmith`	`user_r`	`user_t`	`t:s1 - t:s4`

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
`entitySecurityMark`	`t:s01 = UNCLASSIFIED`

Attributi estesi (xattrs)

A partire da ONTAP 9.12.1, ONTAP supporta xattrs. Xattrs 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 xattrs, è possibile utilizzare e `getfattr` le `setfattr` 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 xattrs 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 xattrs in ONTAP:

- Red Hat Enterprise Linux versione 8,4 o successiva
- Ubuntu 22.04 o versione successiva
- Ogni file può avere fino a 128 xattrs
- 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 xattrs
- Per impostare e recuperare xattrs, `w` o i bit di modalità di scrittura devono essere abilitati per l'utente e il gruppo

Gli Xattrs 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 xattrs

- `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. Xattrs, 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.

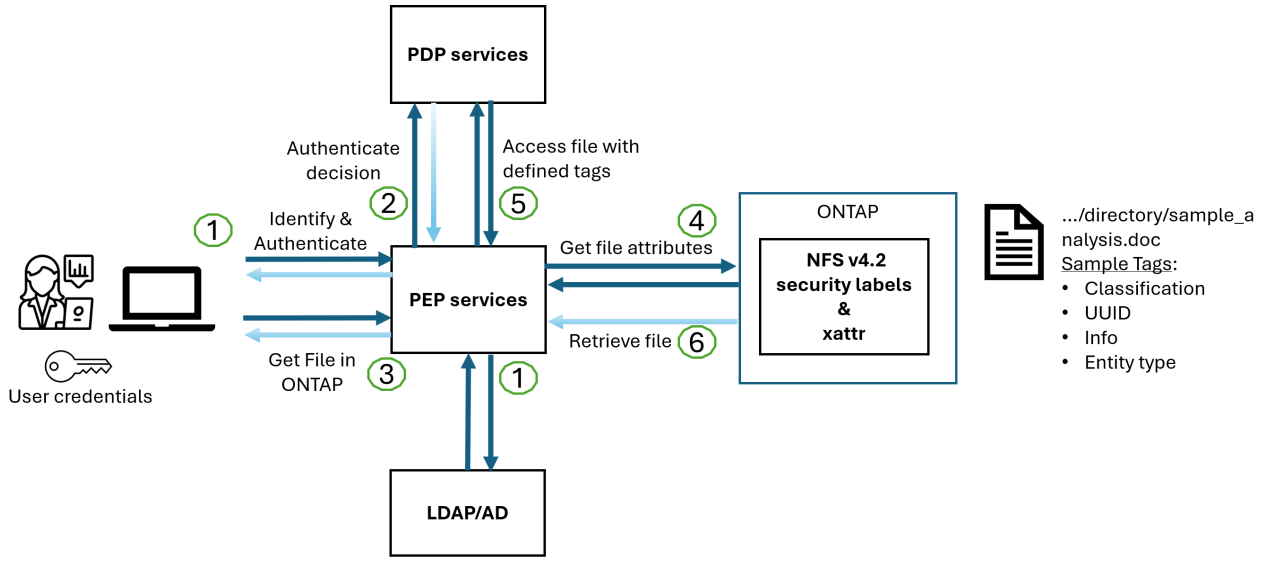
2. Il PDP valuta quindi questa richiesta in base ai criteri ABAC stabiliti.

   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	{
	"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"
	}
	}

specifiche	"DoD"
uuid	b4111349-7875-4115-ad30-0928565f2e15

AdminOrganization	{
	"value": "DoD"
	}

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	{
	"classification": "UNCLASSIFIED",
	"value": "cn=smith john r jrsmith, ou=dod, o=u.s. government, c=us"
	}

DissemTos	{
	"value": "DoD"
	}

DutyOrganization	{
	"value": "DoD"
	}

EntityType	{
	"value": "GOV"
	}

FineAccessControls	[
	{
	"value": "SI"
	},
	{
	"value": "TK"
	},
	{
	"value": "NSYS"
	}
	]

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	{
	"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"
	},

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"

Informazioni sul copyright

Informazioni sul marchio commerciale