Iniziare

NetApp virtualization solutions

NetApp
August 24, 2025

This PDF was generated from https://docs.netapp.com/it-it/netapp-solutions-virtualization/vmware/vmw-getting-started-overview.html on August 24, 2025. Always check docs.netapp.com for the latest.

Sommario

Iniziare . . . 1
- Concetti fondamentali . . . 1
  - Scopri di più su ONTAP per VMware vSphere . . . 1
  - Scopri di più sulle piattaforme NetApp per VMware . . . 4
  - Scopri di più sugli ambienti multicloud ibridi con NetApp e VMware . . . 8
- Strumenti e soluzioni di gestione . . . 9
  - Scopri come gestire le macchine virtuali utilizzando gli ONTAP tools for VMware vSphere . . . 9
  - Scopri come utilizzare ONTAP e le API VMware per l'amministrazione . . . 10
  - Scopri come monitorare un'infrastruttura completa utilizzando NetApp Data Infrastructure Insights . . . 11
  - Scopri di più sulle VM da VMware vSphere ai datastore ONTAP . . . 11
- Soluzioni per la protezione dei dati . . . 12
  - Scopri come proteggere gli ambienti VMware con MetroCluster e SnapMirror ActiveSync . . . 12
  - Scopri come mitigare i rischi di sicurezza e ransomware per i carichi di lavoro VMware . . . 13
  - Protezione autonoma contro i ransomware per NFS e VMFS . . . 14
- Soluzioni di backup e disaster recovery . . . 22
  - Scopri di più sul backup e il ripristino delle macchine virtuali utilizzando il plug-in SnapCenter per VMware vSphere . . . 22
  - Scopri di più sul disaster recovery delle macchine virtuali utilizzando BlueXP disaster recovery . . . 22

Iniziare

Concetti fondamentali

Scopri di più su ONTAP per VMware vSphere

NetApp ONTAP è una soluzione di storage leader per VMware vSphere, che offre quasi due decenni di prestazioni affidabili per i casi d'uso di datastore e storage connesso agli ospiti. ONTAP supporta i protocolli SAN e NAS, consente il ridimensionamento indipendente delle risorse di archiviazione e di elaborazione e scarica le attività di archiviazione dagli host. I vantaggi includono una solida protezione dei dati, elevata disponibilità e funzionalità avanzate di continuità aziendale come SnapMirror e MetroCluster.

Introduzione

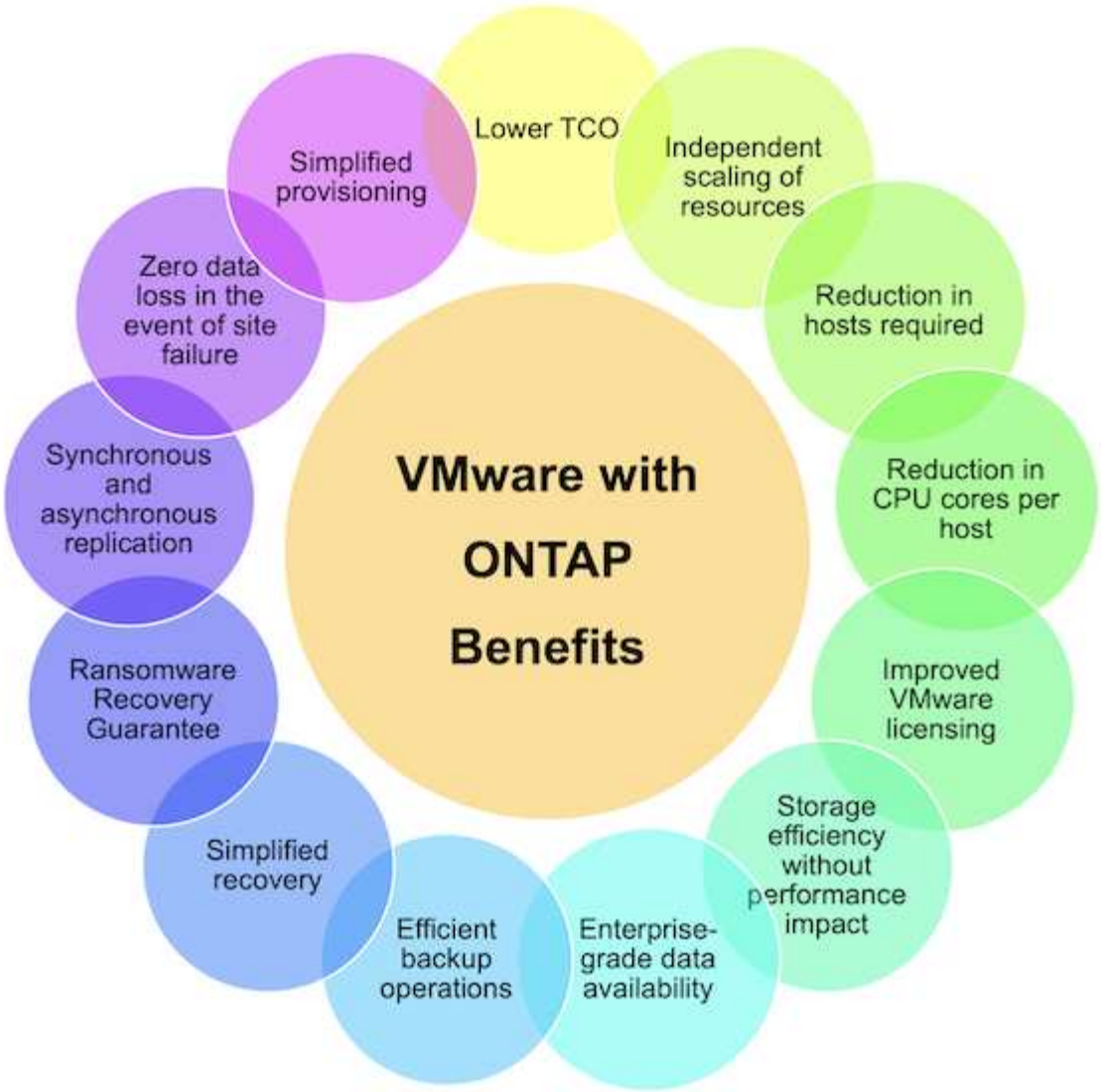
NetApp continua ad aggiungere funzionalità innovative per semplificare la gestione dello storage, riducendo al contempo i costi e aumentando la fiducia in un'infrastruttura virtuale consolidata, basata su VMware e pronta per il cloud. Questa raccolta di soluzioni presenta le offerte ONTAP per VMware vSphere Foundation e VMware Cloud Foundation, comprese le informazioni più recenti sui prodotti e le best practice, per semplificare la distribuzione, ridurre i rischi e semplificare la gestione.

Per ulteriori informazioni sull'utilizzo di ONTAP con VMware vSphere, fare riferimento a "VMware vSphere con ONTAP" .

Perché ONTAP per VMware

Sono molteplici i motivi per cui decine di migliaia di clienti hanno scelto ONTAP come soluzione di storage per vSphere, ad esempio un sistema di storage unificato che supporta sia i protocolli SAN che NAS, solide funzionalità di protezione dei dati mediante snapshot efficienti in termini di spazio e una vasta gamma di strumenti per aiutarti a gestire i dati delle applicazioni. Utilizzando un sistema di storage separato dall'hypervisor è possibile delegare numerose funzioni e massimizzare l'investimento nei sistemi host vSphere. Questo approccio non solo garantisce che le risorse host siano concentrate sui carichi di lavoro delle applicazioni, ma evita anche effetti casuali sulle prestazioni delle applicazioni derivanti dalle operazioni di archiviazione.

L'utilizzo di ONTAP insieme a vSphere è un'ottima combinazione che consente di ridurre le spese per l'hardware host e il software VMware. Puoi anche proteggere i tuoi dati a costi inferiori mantenendo prestazioni elevate e costanti. Poiché i carichi di lavoro virtualizzati sono mobili, è possibile esplorare diversi approcci utilizzando Storage vMotion per spostare le VM tra datastore VMFS, NFS o vVols , tutti sullo stesso sistema di storage.



Ecco i principali vantaggi per i clienti NetApp e VMware:

- **Flessibilità fin dal primo giorno e man mano che si aumenta la produttività.** In qualsiasi architettura, la necessità di crescere può sorgere per diverse ragioni. Indipendentemente dall'evoluzione delle esigenze in termini di prestazioni o capacità, dall'aggiunta di nuovi host e dall'emergere di considerazioni relative alla rete o al fabric, è fondamentale scegliere una piattaforma di storage che consenta il ridimensionamento indipendente delle risorse.

  Con ONTAP puoi iniziare con la capacità richiesta, crescere in base alle necessità e sfruttare i vantaggi della suddivisione in livelli, il tutto senza dover aggiungere ulteriori host di elaborazione. Inoltre, un singolo cluster ONTAP può essere utilizzato con più domini di carico di lavoro ed evita la creazione di isole di archiviazione. Questi vantaggi comportano notevoli risparmi sui costi per l'organizzazione.

- **Scaricare le attività di archiviazione su ONTAP.** Nei tipici ambienti HCI, la piattaforma host è responsabile delle attività di elaborazione, delle operazioni di archiviazione e di qualsiasi ottimizzazione di rete sul lato client. Ad esempio, quando si determinano i requisiti hardware dei nodi di elaborazione, è necessario considerare il sovraccarico della CPU. Spesso difficile da definire preventivamente, questo overhead è comunemente accettato pari al 10-15% e dipende dal profilo I/O dei carichi di lavoro. Inoltre, è importante considerare il consumo di memoria. L'overhead di memoria è obbligatorio e non dovrebbe essere compromesso per mantenere le prestazioni. Gli host possono compensare questo inconveniente

sfruttando le schede di rete compatibili con RDMA, migliorando l'efficienza del trasferimento di rete, a costi aggiuntivi. Infine, con una piattaforma HCI, le funzioni di archiviazione quali efficienza di archiviazione, RAID e tolleranza ai guasti, nonché crittografia, sono gestite dagli host.

I clienti possono mitigare qualsiasi di questi impatti negativi sulle risorse della CPU host sfruttando ONTAP. Questa strategia consente agli host di concentrarsi sulle attività di elaborazione, consentendo al contempo a ONTAP di gestire le operazioni di archiviazione ad alta intensità di CPU. Questa strategia migliora le prestazioni complessive ottimizzando l'efficienza di archiviazione, la crittografia, gli snapshot e altro ancora, riducendo al contempo il costo totale di proprietà. Non solo migliorando le prestazioni dell'host e riducendo il numero di host necessari per erogare lo stesso carico di lavoro, riduce anche il numero di core richiesti per host, con conseguente ulteriore risparmio sui costi. Questi risparmi si estendono ulteriormente al risparmio energetico, alla riduzione dei requisiti di raffreddamento, all'ottimizzazione dei costi di licenza e altro ancora; il tutto delegando le attività di archiviazione ad alta intensità di CPU a ONTAP e facendo meno affidamento sugli host per gestire tutto.

- **Efficienza di archiviazione** Sebbene NetApp sia stata la prima a offrire la deduplicazione per i carichi di lavoro di produzione, questa innovazione non è stata né la prima né l'ultima in questo settore. Tutto è iniziato con gli snapshot, un meccanismo di protezione dei dati efficiente in termini di spazio e senza effetti sulle prestazioni, insieme alla tecnologia FlexClone per creare istantaneamente copie di lettura/scrittura delle VM per uso in produzione e backup. NetApp ha continuato a fornire funzionalità inline, tra cui deduplicazione, compressione e deduplicazione a blocchi zero, per ottenere il massimo spazio di archiviazione dai costosi SSD. Più di recente, ONTAP ha aggiunto la possibilità di impacchettare operazioni di I/O e file più piccoli in un blocco di disco utilizzando la compattazione. La combinazione di queste funzionalità ha consentito ai clienti di ottenere risparmi fino a 5:1 per VSI e fino a 30:1 per VDI.
- **Disponibilità dei dati di livello aziendale.** La protezione dei dati è fondamentale per qualsiasi organizzazione IT. La pianificazione delle tolleranze di errore del carico di lavoro richiede un'attenta valutazione per garantire che sia disponibile un numero adeguato di nodi quando gli host sono responsabili delle operazioni di archiviazione. Con l'aumentare del numero di guasti tollerati, aumenta anche la necessità di host aggiuntivi e la quantità di storage fornita per soddisfare la capacità di storage della VM richiesta.

  Le funzionalità complete di disponibilità di ONTAP garantiscono che i dati siano sempre accessibili, sicuri e resilienti, rendendolo una scelta affidabile per le distribuzioni VMware di tutte le dimensioni. L'utilizzo dello storage condiviso negli ambienti VMware semplifica l'implementazione di cluster vSphere più piccoli, semplificando il processo di configurazione e consentendo la condivisione dello storage tra cluster con una maggiore tolleranza agli errori.

  Le principali caratteristiche di disponibilità ONTAP includono:

  - Architettura ad alta disponibilità (HA): ONTAP supporta un'architettura ad alta disponibilità che include un modello di distribuzione in cluster.
  - Failover e failback automatici: in caso di guasti hardware o software, ONTAP consente il failover automatico su un nodo di archiviazione in standby. Una volta risolto il problema, è possibile eseguire il failback per ripristinare la configurazione originale, riducendo al minimo i tempi di inattività.
  - Protezione dati integrata: ONTAP include funzionalità di protezione dati integrate, come RAID-DP e RAID-TEC, che forniscono una protezione avanzata contro i guasti del disco e garantiscono l'integrità e la disponibilità dei dati.
- **Operazioni di backup e ripristino efficienti.** Oltre a proteggere i dati in caso di guasti di vario tipo, dobbiamo pianificare il backup delle VM e dei carichi di lavoro come parte delle normali operazioni IT. Gli snapshot catturano lo stato di una VM in un momento specifico, inclusi il disco, la memoria e le impostazioni della VM. Ciò consente a un amministratore di ripristinare la macchina virtuale a uno stato precedente se qualcosa va storto, ad esempio un aggiornamento non riuscito, una modifica della configurazione o se si cade vittima di un attacco ransomware o di un virus. Quando si progetta una

soluzione bilanciata per gli ambienti VMware, è necessario tenere in considerazione lo spazio di archiviazione utilizzato dagli snapshot.

Sebbene gli snapshot siano uno strumento importante, un eccessivo affidamento sugli snapshot basati su VMware solleva preoccupazioni in merito alla frequenza e ai criteri di conservazione. Inoltre, avere troppi snapshot basati su VMware può ridurre le prestazioni. È importante prendere in considerazione alternative come le copie snapshot NetApp e il SnapCenter Plug-in for VMware vSphere. SnapCenter sfrutta le copie snapshot, ovvero immagini di un volume in un dato momento e di sola lettura che inizialmente condividono blocchi del disco con il file system attivo, senza richiedere spazio aggiuntivo e con una capacità di archiviazione minima. Questi snapshot hanno un sovraccarico di prestazioni trascurabile, poiché catturano solo le modifiche apportate dall'ultimo snapshot. Il SnapCenter Plug-in for VMware vSphere (SCV) utilizza questi snapshot per fornire backup e ripristini efficienti e coerenti con gli arresti anomali per VM, datastore e VMDK. Queste operazioni sono integrate in modo fluido e senza impatto sulle prestazioni all'interno di un ambiente vCenter. Inoltre, ONTAP consente di scaricare gli snapshot su un archivio di oggetti per la conservazione a lungo termine.

- **Capacità di continuità aziendale olistica.** Oltre alla tolleranza agli errori standard, al backup e al ripristino, un'organizzazione deve pianificare vari scenari, come disastri, attacchi ransomware e migrazioni di siti di data center. Con l'archiviazione basata su host, per affrontare queste sfide in genere è necessario affidarsi a una serie di soluzioni di terze parti per mitigare efficacemente i disastri e garantire la continuità aziendale. Inoltre, negli scenari che prevedono un utilizzo intensivo della rete, un dimensionamento insufficiente dei dispositivi di rete e di archiviazione può avere un impatto significativo sulle prestazioni.

  Grazie alle sue funzionalità di disponibilità e alle capacità di backup e ripristino, ONTAP è parte integrante di una strategia completa di continuità aziendale per gli ambienti VMware. Le organizzazioni hanno bisogno che le VM e i carichi di lavoro siano disponibili senza interruzioni durante le normali operazioni e quelle di manutenzione, protetti da solide capacità di protezione e ripristino e in grado di sfruttare soluzioni di disaster recovery convenienti e con un utilizzo efficiente dello spazio.

  Le principali caratteristiche di continuità aziendale ONTAP includono:

  - Replica dei dati con SnapMirror: sfruttando le copie snapshot, SnapMirror consente la replica asincrona e sincrona dei dati su siti remoti o ambienti cloud per il ripristino di emergenza
  - MetroCluster: la tecnologia MetroCluster di ONTAP fornisce una replica sincrona tra siti geograficamente separati, garantendo una perdita di dati pari a zero e un rapido ripristino in caso di guasto del sito.
  - Cloud Tiering: Cloud Tiering identifica automaticamente i dati inattivi (dati a cui si accede raramente) sullo storage primario e li sposta su uno storage di oggetti a costi inferiori, nel cloud o in locale.
  - BlueXP DRaaS: NetApp BlueXP Disaster Recovery as a Service (DRaaS) è una soluzione completa progettata per fornire solide funzionalità di disaster recovery alle aziende, garantendo protezione dei dati, ripristino rapido e continuità aziendale in caso di disastro.

Scopri di più sulle piattaforme NetApp per VMware

NetApp offre piattaforme su misura per gli ambienti VMware, tra cui FAS per uno storage conveniente, AFF per carichi di lavoro ad alte prestazioni, ASA per distribuzioni SAN dedicate e soluzioni cloud per architetture ibride e multicloud. Grazie alla ONTAP, queste piattaforme supportano VMware Cloud Foundation e VMware vSphere.

Introduzione

Queste offerte migliorano le prestazioni, la scalabilità e la gestione dei dati per l'amministratore VMware.

Inoltre, ONTAP viene utilizzato su queste piattaforme, offrendo una soluzione di gestione dei dati unificata, scalabile ed efficiente che supporta vari protocolli di archiviazione, migliora la protezione dei dati e ottimizza le prestazioni per diversi carichi di lavoro.

Vantaggi comuni tra le piattaforme NetApp

- **Integrazione VMware:** tutte le piattaforme NetApp offrono una profonda integrazione con VMware, migliorando l'efficienza dell'ambiente di storage. Le soluzioni on-premise possono sfruttare plugin, API, VAAI e VASA per migliorare la gestione complessiva dei dati, aumentando al contempo la versatilità dell'infrastruttura.
- **Ottimizzazione dei costi ed efficienza di storage:** sfruttando lo storage NetApp si sfruttano tecnologie di efficienza native quali deduplicazione, compressione e thin provisioning, riducendo significativamente il consumo e i costi di storage, massimizzando al contempo l'utilizzo della capacità e le prestazioni. Inoltre, questi risparmi di spazio di archiviazione si traducono in un carico ridotto sulle risorse di elaborazione.
- **Gestione unificata dei dati:** ONTAP fornisce un'unica interfaccia di gestione sia per l'archiviazione in sede che per quella basata su cloud, semplificando l'amministrazione e riducendo la complessità. Ciò consente lo spostamento e la gestione fluidi dei dati negli ambienti on-premise e cloud, garantendo flessibilità e scalabilità per i carichi di lavoro VMware.
- **Supporto multiprotocollo:** ONTAP supporta un'ampia gamma di protocolli di archiviazione, tra cui NFS, CIFS/SMB, iSCSI, FC e NVMe, consentendo alle organizzazioni di consolidare i carichi di lavoro su un'unica piattaforma o di sfruttare le offerte SAN appositamente progettate senza creare silos di dati.
- **Automazione e orchestrazione:** il supporto per strumenti di automazione come VMware Cloud Foundation Automation (in precedenza VMware Aria Automation) e l'integrazione con Ansible e altri framework di automazione semplificano le operazioni e riducono i costi amministrativi.
- **Sicurezza:** solide funzionalità di sicurezza, tra cui crittografia a riposo e in transito, multi-tenancy sicura e controllo degli accessi basato sui ruoli, garantiscono la sicurezza degli ambienti VMware.
- * Strumenti ONTAP per VMware:* gli strumenti NetApp ONTAP per VMware offrono funzionalità di integrazione e gestione senza interruzioni, consentendo un provisioning efficiente dello storage, protezione dei dati e prestazioni migliorate per gli ambienti VMware tramite un'interfaccia unificata e intuitiva.
- * SnapCenter per VMware vSphere:* NetApp SnapCenter per VMware vSphere semplifica e centralizza le operazioni di protezione, backup e ripristino dei dati per gli ambienti VMware, garantendo una gestione affidabile ed efficiente dei dati delle macchine virtuali.
- **Alta disponibilità e resilienza:** funzionalità come RAID-TEC e RAID-DP garantiscono una solida protezione dei dati e un'elevata disponibilità, fondamentali per gli ambienti VMware.
- **Qualità del servizio (QoS):** consente agli amministratori di impostare garanzie di prestazioni per diverse VM, assicurando che i carichi di lavoro critici ricevano le risorse necessarie.

Nota: le soluzioni cloud NetApp potrebbero avere funzionalità limitate dal provider cloud, ma restano comunque molto affidabili per la connessione guest e il supporto di datastore NFS nativi.

Vantaggi di NetApp ASA (All SAN Array)

- **Ottimizzato per SAN:** progettato specificamente per carichi di lavoro SAN, garantisce prestazioni elevate e bassa latenza per gli ambienti VMware che si basano sullo storage a blocchi.
- **Alta disponibilità migliorata:** funzionalità come i controller attivi-attivi e la replica sincrona garantiscono disponibilità continua e protezione dei dati.

La gamma ASA è composta dai modelli della serie A e della serie C.

Gli array flash NetApp A-Series all-NVMe sono progettati per carichi di lavoro ad alte prestazioni, offrendo

latenza estremamente bassa ed elevata resilienza, rendendoli adatti per applicazioni mission-critical.

Gli array flash QLC della serie C sono pensati per casi d'uso ad alta capacità, offrendo la velocità del flash con i costi contenuti del flash ibrido.

Supporto del protocollo di archiviazione

ASA supporta tutti i protocolli SAN standard, tra cui iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) e NVME over fabric.

iSCSI - NetApp ASA fornisce un solido supporto per iSCSI, consentendo l'accesso a livello di blocco ai dispositivi di archiviazione tramite reti IP. Offre un'integrazione perfetta con gli iniziatori iSCSI, consentendo un provisioning e una gestione efficienti delle LUN iSCSI. Funzionalità avanzate di ONTAP, come il multi-pathing, l'autenticazione CHAP e il supporto ALUA.

Per indicazioni di progettazione sulle configurazioni iSCSI fare riferimento a "Documentazione di riferimento sulla configurazione SAN" .

Fibre Channel - NetApp ASA offre un supporto completo per Fibre Channel (FC), una tecnologia di rete ad alta velocità comunemente utilizzata nelle reti di archiviazione (SAN). ONTAP si integra perfettamente con l'infrastruttura FC, garantendo un accesso affidabile ed efficiente a livello di blocco ai dispositivi di archiviazione. Offre funzionalità quali zoning, multi-pathing e fabric login (FLOGI) per ottimizzare le prestazioni, migliorare la sicurezza e garantire una connettività senza interruzioni negli ambienti FC.

Per indicazioni di progettazione sulle configurazioni Fibre Channel fare riferimento a "Documentazione di riferimento sulla configurazione SAN" .

NVMe su Fabric - NetApp ONTAP e ASA supportano NVMe su Fabric. NVMe/FC consente l'utilizzo di dispositivi di archiviazione NVMe su infrastrutture Fibre Channel e NVMe/TCP su reti di archiviazione IP.

Per indicazioni di progettazione su NVMe fare riferimento a "Configurazione, supporto e limitazioni NVMe"

Tecnologia attiva-attiva

Gli array SAN All-Flash NetApp consentono percorsi attivi-attivi attraverso entrambi i controller, eliminando la necessità per il sistema operativo host di attendere il fallimento di un percorso attivo prima di attivare il percorso alternativo. Ciò significa che l'host può utilizzare tutti i percorsi disponibili su tutti i controller, garantendo che i percorsi attivi siano sempre presenti indipendentemente dal fatto che il sistema sia in uno stato stabile o che stia subendo un'operazione di failover del controller.

Inoltre, NetApp ASA offre una caratteristica distintiva che aumenta notevolmente la velocità del failover SAN. Ogni controller replica continuamente i metadati LUN essenziali al proprio partner. Di conseguenza, ogni titolare del trattamento è pronto ad assumersi la responsabilità della gestione dei dati in caso di un guasto improvviso del proprio partner. Questa prontezza è possibile perché il controller possiede già le informazioni necessarie per iniziare a utilizzare le unità che erano precedentemente gestite dal controller guasto.

Con il percorso attivo-attivo, sia le acquisizioni pianificate che quelle non pianificate hanno tempi di ripresa IO di 2-3 secondi.

Per maggiori informazioni vedere "TR-4968, NetApp All-SAS Array: disponibilità e integrità dei dati con NetApp ASA" .

Per informazioni dettagliate vedere il "Pagina di destinazione di NetApp ASA" .

Vantaggi di NetApp AFF (All Flash FAS)

- **Prestazioni estreme:** utilizza l'archiviazione all-flash per garantire latenza inferiore al millisecondo e IOPS elevati, ideali per carichi di lavoro VMware sensibili alle prestazioni.
- **Bassa latenza costante:** garantisce prestazioni prevedibili per applicazioni e VM critiche, essenziali per il mantenimento degli SLA.

Per ulteriori informazioni sugli array di storage NetApp AFF A-Series, vedere"NetApp AFF serie A" pagina di destinazione.

Per ulteriori informazioni sugli array di storage NetApp C-Series, vedere"NetApp AFF serie C" pagina di destinazione.

Vantaggi NetApp FAS (Fabric-Attached Storage)

- **Architettura di archiviazione unificata:** supporta sia i protocolli SAN (a livello di blocco) sia NAS (a livello di file), rendendola versatile per vari carichi di lavoro VMware.
- **Conveniente:** ideale per ambienti che richiedono un equilibrio tra prestazioni e costi, offrendo una combinazione di HDD e SSD.

Vantaggi delle soluzioni cloud

- **Gestione dei dati cloud-native:** utilizza offerte cloud-native per migliorare la mobilità dei dati, il backup e il disaster recovery per i carichi di lavoro VMware. Il supporto per il datastore NFS nativo per i carichi di lavoro cloud VMware è il seguente:
  - VMware Cloud su AWS con Amazon FSx for NetApp ONTAP
  - Servizio Azure VMware con Azure NetApp Files
  - Google Cloud VMware Engine con Google Cloud NetApp Volume -

- **Flessibilità del cloud ibrido:** integrazione perfetta tra ambienti on-premise e cloud, che garantisce flessibilità per i carichi di lavoro VMware che si estendono su più sedi.

Riepilogo

In sintesi, le piattaforme ONTAP e NetApp offrono una serie completa di vantaggi per i carichi di lavoro VMware, migliorando le prestazioni, la scalabilità e la gestione dei dati. Sebbene le funzionalità comuni forniscano una solida base, ogni piattaforma offre vantaggi differenziati, personalizzati in base alle esigenze specifiche, che si tratti di storage conveniente con FAS, elevate prestazioni con AFF, prestazioni SAN ottimizzate con ASA o flessibilità del cloud ibrido con le offerte cloud NetApp .

Scopri di più sugli ambienti multicloud ibridi con NetApp e VMware

Scopri come NetApp e VMware semplificano le configurazioni multicloud ibride integrando l'infrastruttura on-premise con i servizi di cloud pubblico, consentendo la migrazione dei carichi di lavoro, l'ottimizzazione delle risorse e operazioni coerenti in tutti gli ambienti.

Introduzione

Questo approccio consente alle aziende di migrare facilmente i carichi di lavoro, ottimizzare l'utilizzo delle risorse e mantenere operazioni coerenti in entrambi gli ambienti.

Per ulteriori informazioni sugli scenari di cloud ibrido con VMware e NetApp, vedere"Panoramica di NetApp Hybrid Multicloud con VMware" .

Scenari di distribuzione VMware con NetApp

Questa sezione descrive le varie opzioni di distribuzione per gli ambienti VMware su cloud pubblici e locali. Ciascuno dei provider cloud supporta uno stack VMware Software Defined Data Center (SDDC) e/o VMware Cloud Foundation (VCF) all'interno delle rispettive offerte di cloud pubblico.

- **VMware in sede**

L'utilizzo di VMware con storage NetApp in sede fornisce un ambiente di virtualizzazione robusto, scalabile e flessibile. Abbinando le funzionalità avanzate di gestione dei dati di NetApp, come deduplicazione, compressione e snapshot efficienti, al sistema di storage più adatto basato su ONTAP, i clienti possono scegliere la piattaforma più adatta alle loro esigenze. Questa combinazione garantisce elevate prestazioni, affidabilità e gestione semplificata per i carichi di lavoro virtualizzati, migliorando l'efficienza complessiva del data center.

- **Soluzione Azure VMware**

Azure VMware Solution è un servizio cloud ibrido che consente di avere VMware SDDC completamente funzionanti all'interno del cloud pubblico Microsoft Azure. Azure VMware Solution è una soluzione proprietaria completamente gestita e supportata da Microsoft, verificata da VMware, che sfrutta l'infrastruttura di Azure. Ciò significa che quando viene distribuita la soluzione Azure VMware, i clienti ottengono ESXi di VMware per la virtualizzazione del calcolo, vSAN per l'archiviazione iperconvergente e NSX per la rete e la sicurezza, il tutto sfruttando la presenza globale di Microsoft Azure, le strutture dei data center leader del settore e la vicinanza al ricco ecosistema di servizi e soluzioni Azure nativi.

- **VMware Cloud su AWS**

VMware Cloud on AWS porta il software SDDC di classe enterprise di VMware su AWS Cloud con accesso

ottimizzato ai servizi AWS nativi. Basato su VMware Cloud Foundation, VMware Cloud on AWS integra i prodotti di virtualizzazione di rete, storage ed elaborazione di VMware (VMware vSphere, VMware vSAN e VMware NSX) insieme alla gestione di VMware vCenter Server, ottimizzati per l'esecuzione su infrastrutture AWS dedicate, elastiche e bare-metal.

- **Google Cloud VMware Engine**

Google Cloud VMware Engine è un'offerta Infrastructure-as-a-Service (IaaS) basata sull'infrastruttura scalabile ad alte prestazioni di Google Cloud e sullo stack VMware Cloud Foundation: VMware vSphere, vCenter, vSAN e NSX-T. Questo servizio consente un rapido accesso al cloud, migrando o estendendo senza problemi i carichi di lavoro VMware esistenti dagli ambienti on-premise a Google Cloud Platform, senza i costi, gli sforzi o i rischi di riprogettare le applicazioni o riorganizzare le operazioni. Si tratta di un servizio venduto e supportato da Google, in stretta collaborazione con VMware.

Strumenti e soluzioni di gestione

Scopri come gestire le macchine virtuali utilizzando gli ONTAP tools for VMware vSphere

Gli ONTAP tools for VMware vSphere semplificano la gestione del ciclo di vita delle VM che utilizzano lo storage NetApp . Gli amministratori possono gestire lo storage direttamente dal vCenter Server, semplificando le operazioni e migliorando la scalabilità. Componenti chiave come Virtual Storage Console (VSC), VASA Provider e Storage Replication Adapter (SRA) ottimizzano il provisioning, il monitoraggio delle prestazioni e il disaster recovery.

Introduzione

Consente agli amministratori di gestire direttamente lo storage all'interno di vCenter Server e di semplificare la gestione dello storage e dei dati per gli ambienti VMware. Lo strumento plug-in VMware vSphere Client è progettato per integrare la funzionalità plug-in in vSphere Client senza la necessità di eseguirlo all'interno di vCenter Server. Ciò garantisce l'isolamento dei plug-in e consente la scalabilità orizzontale dei plug-in che operano in ambienti vSphere di grandi dimensioni.

Componenti degli strumenti ONTAP

- **Virtual Storage Console (VSC)** La VSC include l'interfaccia integrata con il client vSphere, dove è possibile aggiungere controller di storage, eseguire il provisioning di datastore, monitorare le prestazioni dei datastore e visualizzare e aggiornare le impostazioni dell'host ESXi.
- **VASA Provider** Il provider VMware vSphere APIs for Storage Awareness (VASA) per ONTAP invia informazioni sullo storage utilizzato da VMware vSphere al vCenter Server, consentendo il provisioning dei datastore VMware Virtual Volumes (vVols), la creazione e l'utilizzo di profili di capacità di storage, la verifica della conformità e il monitoraggio delle prestazioni.
- **Storage Replication Adapter (SRA)** Se abilitato e utilizzato con VMware Site Recovery Manager (SRM), SRA facilita il ripristino dei datastore e delle macchine virtuali di vCenter Server in caso di guasto, consentendo la configurazione di siti protetti e siti di ripristino per il disaster recovery.

Per ulteriori informazioni sugli strumenti NetApp ONTAP per VMware, vedere "Documentazione sugli ONTAP tools for VMware vSphere" .

Scopri come utilizzare ONTAP e le API VMware per l'amministrazione

ONTAP e VMware offrono API per un'integrazione e un'automazione fluide tra piattaforme di storage e virtualizzazione. Ciò consente un provisioning, un monitoraggio e una protezione dei dati semplificati per migliorare la coerenza del flusso di lavoro.

Introduzione

VMware fornisce una gamma di API che consentono agli amministratori di interagire a livello di programmazione con vari prodotti e servizi VMware, migliorando l'efficienza e la coerenza delle operazioni. Inoltre, le API NetApp ONTAP forniscono un solido set di strumenti che consentono agli amministratori di automatizzare, integrare e ottimizzare la gestione degli ambienti di storage, in particolare in combinazione con i carichi di lavoro VMware. Queste API facilitano l'interazione senza soluzione di continuità tra i sistemi di storage ONTAP e VMware, migliorando l'efficienza, le prestazioni e la protezione dei dati.

API basate su VMware

- **VMware vSphere API:** vSphere API è un'API completa che consente agli amministratori di gestire e automatizzare gli ambienti VMware vSphere. Fornisce accesso a un'ampia gamma di funzionalità vSphere, tra cui provisioning, configurazione, monitoraggio e gestione del ciclo di vita delle macchine virtuali.
- **API REST di VMware vCenter Server:** l'API REST di vCenter Server fornisce un'interfaccia RESTful moderna per la gestione di vCenter Server e dei componenti associati. Semplifica l'automazione e l'integrazione con altri sistemi e strumenti.
- **API VMware Cloud Foundation:** le API VMware Software-Defined Data Center (SDDC) forniscono accesso programmatico ai vari componenti e servizi all'interno di un ambiente VMware SDDC. Queste API consentono ad amministratori e sviluppatori di automatizzare, gestire e integrare i diversi aspetti del data center, tra cui servizi di elaborazione, archiviazione, networking e gestione.
- **API di storage VMware vSphere - Storage Awareness:** VASA è un set di API che fornisce l'integrazione degli array di storage con vCenter per la gestione e l'amministrazione. L'architettura si basa su diversi componenti, tra cui il provider VASA che gestisce la comunicazione tra VMware vSphere e i sistemi di storage. Con ONTAP, il provider viene implementato come parte degli ONTAP tools for VMware vSphere.
- **API di storage VMware vSphere - Integrazione array:** VAAI è un set di API che consentono la comunicazione tra gli host VMware vSphere ESXi e i dispositivi di storage. L'API include un set di operazioni primitive utilizzate dagli host per scaricare le operazioni di archiviazione sull'array. VAAI può apportare significativi miglioramenti delle prestazioni per le attività che richiedono un uso intensivo di spazio di archiviazione.

API basate su ONTAP

- * API REST ONTAP NetApp :* l'API REST ONTAP fornisce un'interfaccia RESTful moderna per la gestione dei sistemi di storage ONTAP . Semplifica l'automazione delle attività di archiviazione quali provisioning, monitoraggio e configurazione. Consente una facile integrazione con VMware vSphere e altri strumenti di gestione VMware, consentendo operazioni di archiviazione automatizzate direttamente dagli ambienti VMware. Supporta un'ampia gamma di operazioni, dalla gestione di base dell'archiviazione alle attività avanzate di protezione e replicazione dei dati, consentendo una gestione dell'archiviazione scalabile e flessibile.
- * Strumenti ONTAP per VMware vSphere:* ONTAP tools for VMware vSphere è un set di strumenti per l'integrazione ONTAP e vSphere. Implementa la funzionalità provider del framework API VASA. Gli strumenti ONTAP includono anche il plug-in vCenter, uno storage replication adapter (SRA) per VMware Site Recovery Manager e un server REST API che puoi utilizzare per creare applicazioni di automazione.

Riepilogo

In sintesi, con le API ONTAP , gli amministratori possono creare e configurare tramite script i datastore negli ambienti VMware, garantendo un provisioning dello storage rapido e coerente. Inoltre, possono automatizzare la creazione, la pianificazione e l'eliminazione di snapshot per macchine virtuali VMware, offrendo opzioni efficienti di protezione e ripristino dei dati. Le API SnapMirror facilitano l'automazione della configurazione e della gestione delle relazioni di replica, garantendo soluzioni di disaster recovery affidabili per i carichi di lavoro VMware. Gli amministratori possono anche implementare script per monitorare le metriche delle prestazioni di storage e attivare avvisi o azioni automatizzate quando vengono superate le soglie di prestazioni, garantendo prestazioni di storage ottimali per i carichi di lavoro VMware. Integrando le API ONTAP con le API VMware, come quelle fornite da vSphere e vRealize, gli amministratori possono ottenere un'esperienza di gestione fluida e altamente automatizzata, migliorando l'efficienza e l'affidabilità complessive della loro infrastruttura virtualizzata.

Scopri come monitorare un'infrastruttura completa utilizzando NetApp Data Infrastructure Insights

NetApp Data Infrastructure Insights (in precedenza Cloud Insights) monitora i sistemi on-premise e cloud, offrendo visibilità sull'intero ambiente IT, inclusi i sistemi di storage VMware vSphere e ONTAP . Abilita funzionalità quali il monitoraggio delle prestazioni, il rilevamento dei problemi e l'ottimizzazione delle risorse negli ambienti pubblici e privati.

Introduzione

Con Data Infrastructure Insights puoi monitorare, risolvere i problemi e ottimizzare tutte le tue risorse, inclusi i tuoi cloud pubblici e i tuoi data center privati.

Per ulteriori informazioni su Data Infrastructure Insights, vedere"Documentazione Data Infrastructure Insights" .

Capacità Data Infrastructure Insights

- Data Infrastructure Insights fornisce un monitoraggio multicloud ibrido, garantendo l'osservabilità completa dell'infrastruttura e dei carichi di lavoro.
- Raccoglitori di dati per infrastrutture e carichi di lavoro eterogenei, incluso Kubernetes
- Collettore Telegraf aperto e API aperte per una facile integrazione
- Avvisi e notifiche completi
- Apprendimento automatico per informazioni intelligenti
- Ottimizzare l'utilizzo delle risorse
- Dashboard integrate o personalizzabili con filtri avanzati per ridurre al minimo il rumore di visualizzazione per rispondere alle domande
- Scopri lo stato di salute delle tue operazioni di archiviazione ONTAP
- Proteggi il tuo bene aziendale più prezioso, i dati, da attacchi ransomware o di distruzione dei dati

Scopri di più sulle VM da VMware vSphere ai datastore ONTAP

Gli amministratori di VMware vSphere possono migliorare la propria infrastruttura migrando i carichi di lavoro verso i datastore NetApp ONTAP . ONTAP fornisce snapshot VM-aware, cloni efficienti in termini di storage e operazioni vMotion senza interruzioni, supportando al contempo la gestione basata su policy di storage (SPBM). Che si tratti di

migrazione da vSAN, storage legacy o implementazione di distribuzioni cloud ibride, ONTAP garantisce prestazioni migliorate e operazioni di storage semplificate per gli ambienti VMware.

Questa migrazione consente un'integrazione fluida, una migliore protezione dei dati e una maggiore flessibilità nella gestione degli ambienti virtualizzati, garantendo una transizione fluida con tempi di inattività minimi.

Casi d'uso

Quando si valuta il passaggio a datastore supportati ONTAP , sono disponibili numerose opzioni di migrazione in termini di origine e destinazione.

- Migrazione da sistemi di archiviazione di terze parti (incluso vSAN) a datastore ONTAP .
- Migrazione di VM nello stesso cluster vSphere
- Migrazione di VM su più cluster vSphere
- Migrazione di VM tra server vCenter nello stesso dominio SSO
- Migrazione di VM tra server vCenter in diversi domini SSO
- Migrazione di VM tra le sedi dei data center
- Migrazione da sistemi di archiviazione di terze parti (incluso vSAN) a datastore ONTAP .
- Migrazione di VM in un ambiente cloud ibrido

Per ulteriori informazioni sulla migrazione dei carichi di lavoro VMware verso datastore supportati da ONTAP , vedere"Migrare le VM nei datastore ONTAP" .

Soluzioni per la protezione dei dati

Scopri come proteggere gli ambienti VMware con MetroCluster e SnapMirror ActiveSync

La continuità aziendale avanzata è essenziale per proteggere gli ambienti VMware da interruzioni a livello di dominio. NetApp e VMware offrono soluzioni come NetApp MetroCluster, SnapMirror Active Sync e VMware vSphere Metro Storage Cluster (vMSC) per migliorare la protezione del carico di lavoro e garantire un'elevata disponibilità.

Introduzione

Oltre alle disponibilità integrate nei prodotti, VMware e NetApp offrono configurazioni avanzate che proteggono ulteriormente i carichi di lavoro distribuiti su domini di errore quali rack, edifici, campus o persino città.

NetApp MetroCluster

NetApp MetroCluster sfrutta la funzionalità di alta disponibilità (HA) di NetApp per proteggere dai guasti del controller. MetroCluster include anche la tecnologia SyncMirror , il failover on demand del cluster (CFOD), la ridondanza hardware e la separazione geografica per un'elevata disponibilità. SyncMirror esegue il mirroring sincrono dei dati su due plex: il plex locale che gestisce attivamente i dati e il plex remoto che funge da standby. Tutti i componenti MetroCluster , come controller, storage, cavi, switch e adattatori, sono dotati di ridondanza hardware.

Sincronizzazione attiva NetApp SnapMirror

NetApp SnapMirror Active Sync offre una protezione granulare a livello di datastore con protocolli FCP e iSCSI SAN, proteggendo in modo selettivo la topologia dei carichi di lavoro ad alta priorità. Offre un accesso attivo-attivo sia ai siti locali che a quelli remoti, a differenza di MetroCluster attivo-standby. A partire da ONTAP 9.15.1, SnapMirror ActiveSync supporta la funzionalità attivo/attivo simmetrica, consentendo operazioni di I/O in lettura e scrittura da entrambe le copie di una LUN protetta con replica sincrona bidirezionale.

Cluster di archiviazione VMware vSphere Metro

VMware vSphere Metro Storage Cluster (vMSC) potenzia VMware HA con storage esteso attivo-attivo. Questa configurazione certificata protegge le VM e i container dai guasti. Ciò si ottiene utilizzando concetti di storage esteso insieme a cluster di host vSphere. Questi host sono distribuiti su diversi domini di errore. Per fornire protezione e offerte di storage supportate vengono utilizzate le tecnologie di storage ActiveSync NetApp MetroCluster e SnapMirror . Sfruttando vMSC, una soluzione certificata NetApp garantisce operazioni IT solide e resilienti in tutti i domini di errore.

Per informazioni dettagliate vedere il "Cluster di storage vSphere Metro con ONTAP" .

Scopri come mitigare i rischi di sicurezza e ransomware per i carichi di lavoro VMware

ONTAP migliora la sicurezza e la protezione da ransomware negli ambienti VMware tramite crittografia, snapshot e controlli di accesso avanzati, integrando le funzionalità di sicurezza di VMware per salvaguardare i dati.

Introduzione

Sfruttando le funzionalità avanzate di NetApp ONTAP negli ambienti VMware, le organizzazioni possono garantire l'integrità, la disponibilità e la sicurezza dei propri dati.

Di seguito è riportato in dettaglio come queste tecnologie interagiscono per offrire **sicurezza** e **vantaggi di backup**.

Sicurezza e ransomware

La sicurezza è una preoccupazione fondamentale negli ambienti virtualizzati e NetApp ONTAP offre funzionalità affidabili per migliorare la sicurezza nelle infrastrutture VMware. ONTAP offre la crittografia per i dati inattivi e in transito, garantendo la protezione delle informazioni sensibili da accessi non autorizzati. Le chiavi di crittografia sono gestite in modo sicuro e ONTAP supporta soluzioni di crittografia sia basate su software che su hardware. Integrandosi con gli strumenti di sicurezza di VMware, come le funzionalità di sicurezza integrate di vSphere e le soluzioni di sicurezza di terze parti, ONTAP contribuisce a creare un ambiente sicuro e conforme.

Difesa dal ransomware

Gli attacchi ransomware rappresentano una minaccia significativa per le organizzazioni e la combinazione di VMware e ONTAP fornisce un solido meccanismo di difesa. La tecnologia Snapshot di ONTAP consente la creazione di snapshot immutabili che non possono essere alterati o eliminati dal ransomware. In caso di attacco, questi snapshot possono essere utilizzati per ripristinare rapidamente le VM e i datastore interessati allo stato precedente all'attacco, riducendo al minimo i tempi di inattività e la perdita di dati. Inoltre, l'integrazione di ONTAP con i sistemi di gestione degli eventi e delle informazioni di sicurezza (SIEM) consente il monitoraggio proattivo e l'invio di avvisi in caso di attività sospette. ONTAP supporta inoltre l'autenticazione a più fattori (MFA) e il controllo degli accessi basato sui ruoli (RBAC) per migliorare ulteriormente la sicurezza.

Garanzia di recupero dal ransomware

La garanzia NetApp Ransomware offre alle aziende una soluzione solida e affidabile per proteggersi dagli attacchi ransomware. Sfruttando le funzionalità avanzate di NetApp ONTAP, le organizzazioni possono garantire la sicurezza e la disponibilità dei propri dati. La garanzia offre tranquillità, sapendo che in caso di attacco ransomware i dati possono essere ripristinati in modo rapido ed efficace, riducendo al minimo i tempi di inattività, la perdita di dati e l'impatto finanziario. Questo impegno verso la sicurezza e la resilienza dei dati rende NetApp un partner ideale per le organizzazioni che desiderano proteggere le proprie risorse critiche dalle minacce informatiche in continua evoluzione.

Funzionalità di sicurezza avanzate

ONTAP include funzionalità di sicurezza avanzate come il multi-tenancy sicuro, che isola dati e risorse in ambienti multi-tenant, e il controllo di conformità, che tiene traccia e registra l'accesso ai dati sensibili. Queste funzionalità garantiscono la sicurezza dei dati e consentono alle organizzazioni di dimostrare la conformità alle normative e agli standard del settore.

Riepilogo

L'integrazione delle funzionalità di sicurezza di ONTAP, come crittografia, snapshot immutabili e controlli di accesso avanzati, con gli strumenti VMware garantisce una solida difesa contro le minacce informatiche, tra cui il ransomware. Il supporto di ONTAP per il multi-tenancy sicuro e l'audit di conformità garantisce la protezione dei dati e la conformità normativa.

Insieme, NetApp ONTAP e VMware offrono una soluzione completa per la protezione degli ambienti virtualizzati, consentendo alle organizzazioni di proteggere i dati, ridurre al minimo i tempi di inattività e mantenere la continuità aziendale. L'implementazione di queste tecnologie aiuta le aziende ad affrontare le moderne sfide IT e a salvaguardare le risorse critiche dalle minacce alla sicurezza in continua evoluzione.

Protezione autonoma contro i ransomware per NFS e VMFS

Scopri come la protezione autonoma dai ransomware (ARP) di NetApp ONTAP utilizza l'apprendimento automatico per proteggere i datastore NFS e VMFS negli ambienti VMware, garantendo il rilevamento precoce delle minacce, snapshot a prova di manomissione e un ripristino rapido per rafforzare la resilienza dei dati nei carichi di lavoro virtualizzati e cloud.

Panoramica

Le minacce ransomware si evolvono rapidamente, diventando sempre più sofisticate e destabilizzanti. Le misure di sicurezza tradizionali spesso non riescono a proteggere le risorse di dati critiche. Lo storage NetApp ONTAP offre funzionalità di sicurezza integrate che proteggono proattivamente i dati. In caso di violazione della sicurezza, ONTAP invia avvisi in tempo reale e opzioni di ripristino rapido per ridurre i tempi di inattività e limitare la perdita di dati. ONTAP consente ai clienti di proteggere, recuperare e spostare i propri dati e applicazioni, rafforzando la resilienza al ransomware.

Caso d'uso: proteggere le VM VMware e i relativi file

Il rilevamento precoce del ransomware negli ambienti VMware è fondamentale per fermarne la diffusione e ridurre al minimo i tempi di inattività. Una strategia efficace utilizza più livelli di protezione sugli host ESXi e sulle macchine virtuali guest. Sebbene molti controlli di sicurezza contribuiscano a creare una difesa efficace, NetApp ONTAP aggiunge misure di sicurezza essenziali a livello di storage che rafforzano ulteriormente la protezione.

Le principali funzionalità ONTAP includono la tecnologia Snapshot per il ripristino puntuale, la protezione autonoma dai ransomware (ARP) basata sull'apprendimento automatico integrato, la verifica multi-amministratore e gli snapshot a prova di manomissione che preservano l'integrità dei dati. Queste funzionalità lavorano insieme per migliorare la resilienza al ransomware e consentire un rapido ripristino quando necessario.

Per proteggere gli ambienti vSphere e le macchine virtuali guest è necessario un approccio completo. Le misure chiave includono la segmentazione della rete, l'implementazione di soluzioni EDR/XDR/SIEM per il monitoraggio degli endpoint, l'applicazione di aggiornamenti di sicurezza tempestivi e il rispetto delle linee guida di rafforzamento stabilite. In genere, ogni macchina virtuale esegue un sistema operativo standard, il che rende fondamentale installare e aggiornare regolarmente soluzioni antimalware di livello aziendale come parte di una strategia di difesa anti-ransomware multilivello.

Come aiuta ONTAP

ONTAP rafforza la protezione dei dati con più livelli di difesa. Le funzionalità principali includono snapshot, protezione autonoma dai ransomware (ARP), snapshot a prova di manomissione, verifica multi-amministratore e molto altro. Questo documento si concentra sui miglioramenti apportati ad ARP nella versione 9.17.1.

È possibile abilitare ARP su volumi NAS o SAN che supportano i datastore VMware. ARP utilizza l'apprendimento automatico integrato di ONTAP per monitorare i modelli di carico di lavoro e l'entropia dei dati, rilevare automaticamente i segnali di attività ransomware e fornire un livello di sicurezza intelligente e proattivo. Configurare ARP per volume utilizzando l'interfaccia CLI o System Manager di ONTAP.

Evoluzione delle funzionalità ARP

A partire dalla versione 9.10.1 ONTAP , ARP è disponibile per un volume esistente o per un nuovo volume. Nella versione 9.16.1 ONTAP , è possibile abilitare ARP tramite System Manager o la CLI. La protezione ARP/AI diventa attiva immediatamente, senza alcun periodo di apprendimento. Nella versione 9.17.1, ARP supporta i volumi SAN. Quando si abilita ARP su un volume SAN, ARP/AI monitora costantemente i dati durante un periodo di valutazione per determinare l'idoneità del carico di lavoro e impostare la soglia di crittografia ottimale per il rilevamento.

ARP è integrato in ONTAP e fornisce controllo e coordinamento integrati con altre funzionalità ONTAP . ARP funziona in tempo reale, elaborando i dati mentre vengono scritti o letti e rilevando e rispondendo rapidamente a potenziali attacchi ransomware. Crea snapshot bloccati a intervalli regolari insieme a quelli programmati e gestisce in modo intelligente la conservazione degli snapshot riciclandoli quando non vengono rilevate anomalie. Se ARP rileva un'attività sospetta, conserva per un periodo prolungato uno snapshot acquisito prima dell'attacco, per garantire un punto di ripristino affidabile.

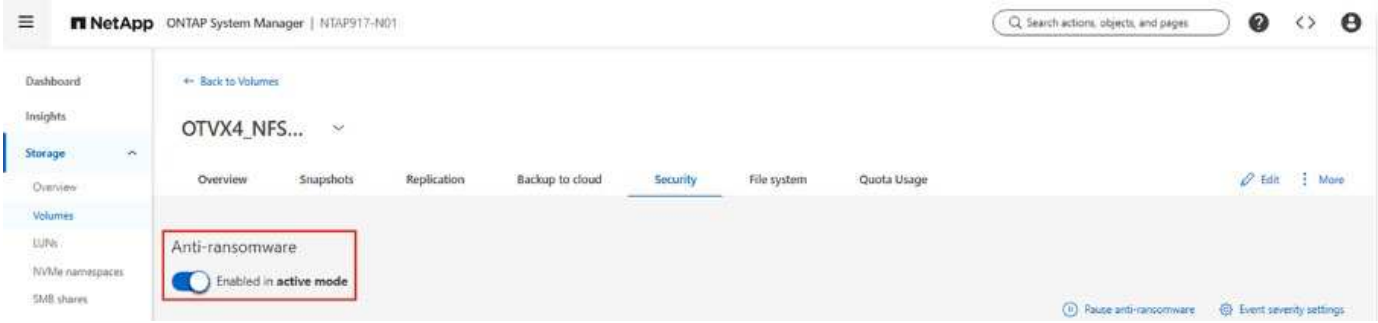
Per maggiori dettagli, vedere"Cosa rileva ARP" .

> Il supporto ARP è incluso nella licenza ONTAP ONE.

Configurare ARP su volumi NAS e simulare un attacco su una VM

Scopri come abilitare NetApp ONTAP Autonomous Ransomware Protection (ARP) sui volumi NAS e SAN utilizzati per i datastore VMware e simulare attacchi ransomware per vedere come ARP rileva le minacce e facilita un rapido ripristino.

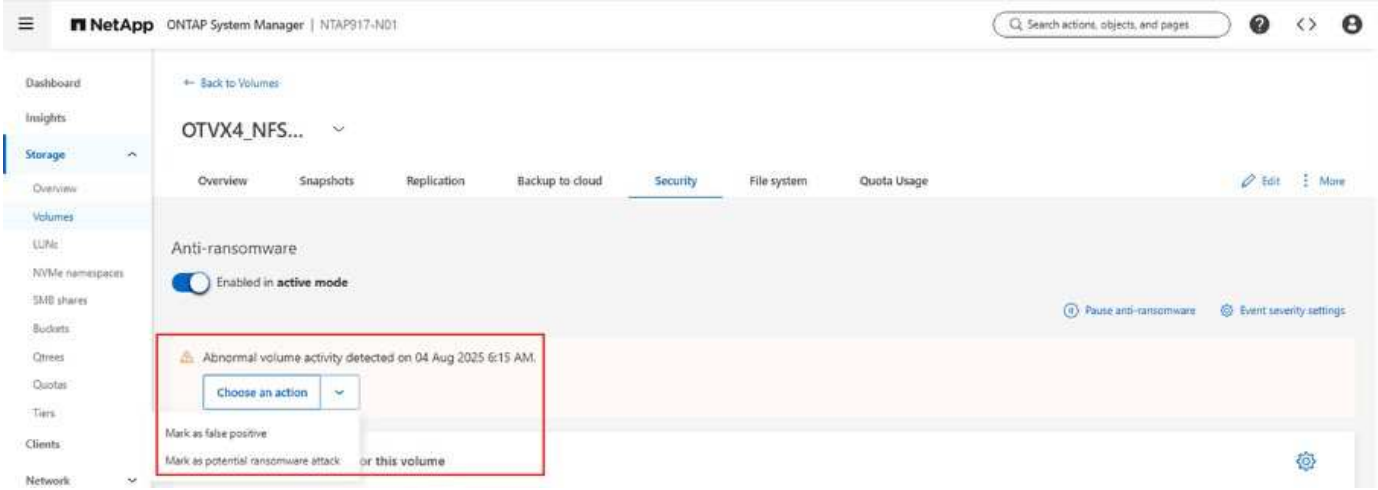
Quando ARP è abilitato su un volume NAS tramite System Manager o CLI, la protezione ARP/AI è abilitata e attiva immediatamente. Non è richiesto alcun periodo di apprendimento.



In questo esempio, la simulazione viene attivata utilizzando uno script per modificare i file o modificando l'estensione del file per simulare un attacco all'interno di una VM residente sul volume NFS collegato come datastore a vCenter.

Name	Date modified	Type	Size
Acorn Missouri River.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Moon.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Moon.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Panthers.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pheasant.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pig.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Pig.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Ridge.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn River.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn River.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Rosa arkansana.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soil.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Soybean.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Sun.xls.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tornado.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tornado.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.docx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.ppt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.pptx.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Tractor.txt.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Water.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Wheat.doc.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB
Acorn Wheat.pdf.encrypted	8/4/2025 1:15 PM	ENCRYPTED File	1,680 KB

Come mostrato di seguito, ARP ha rilevato l’attività anomala.

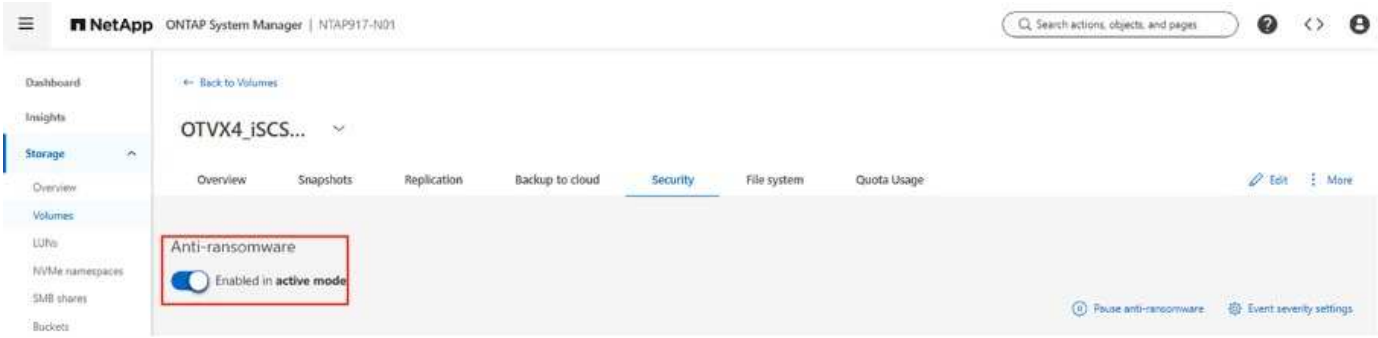


ARP rileva l'attacco in anticipo e consente il recupero dei dati da snapshot acquisiti in prossimità dell'attacco. Per eseguire il rollback, utilizzare lo snapshot periodico ARP generato prima che si verificasse l'incidente. E lo screenshot qui sotto mostra gli snapshot creati:

Per una guida dettagliata su come abilitare ARP sui volumi NFS che fungono da datastore e da ripristino in caso di attacco, fare riferimento"ARP per l'archiviazione NFS" .

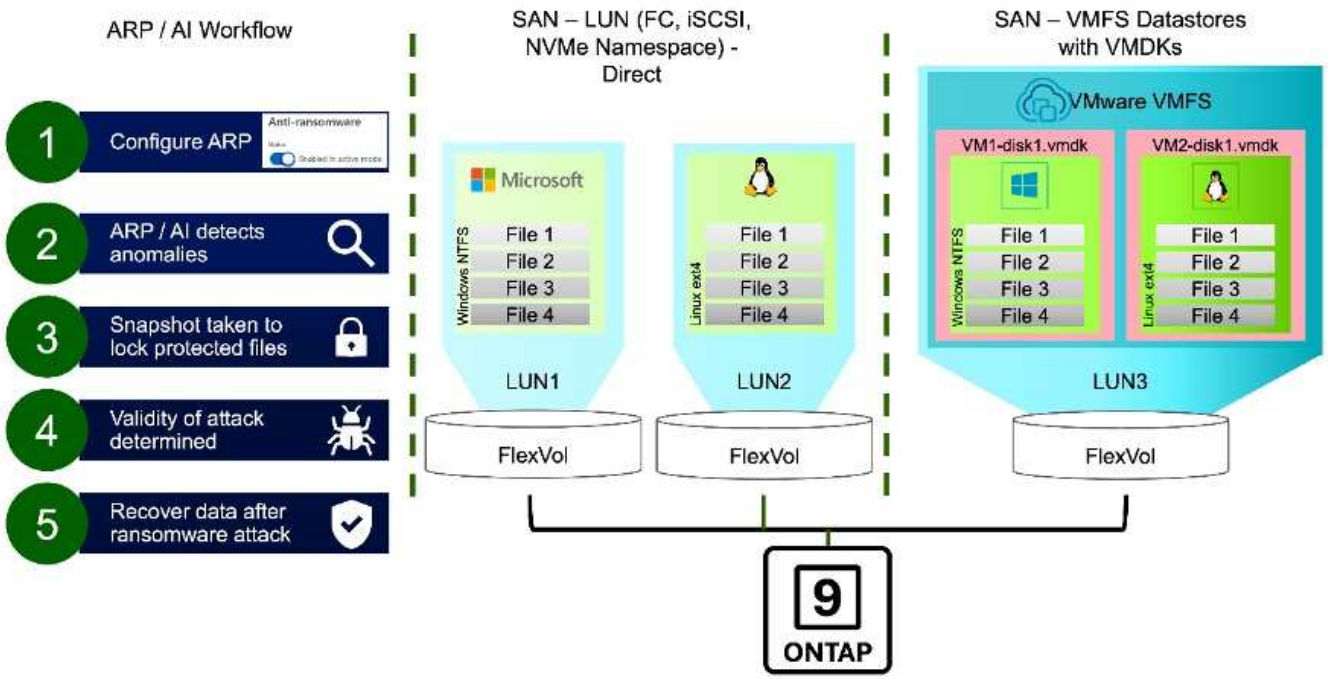
Configurare ARP su volumi SAN e simulare un attacco su una VM

Quando ARP è abilitato su un volume SAN, inizia con una fase di valutazione, simile alla modalità di apprendimento utilizzata negli ambienti NAS, prima di passare automaticamente al rilevamento attivo.



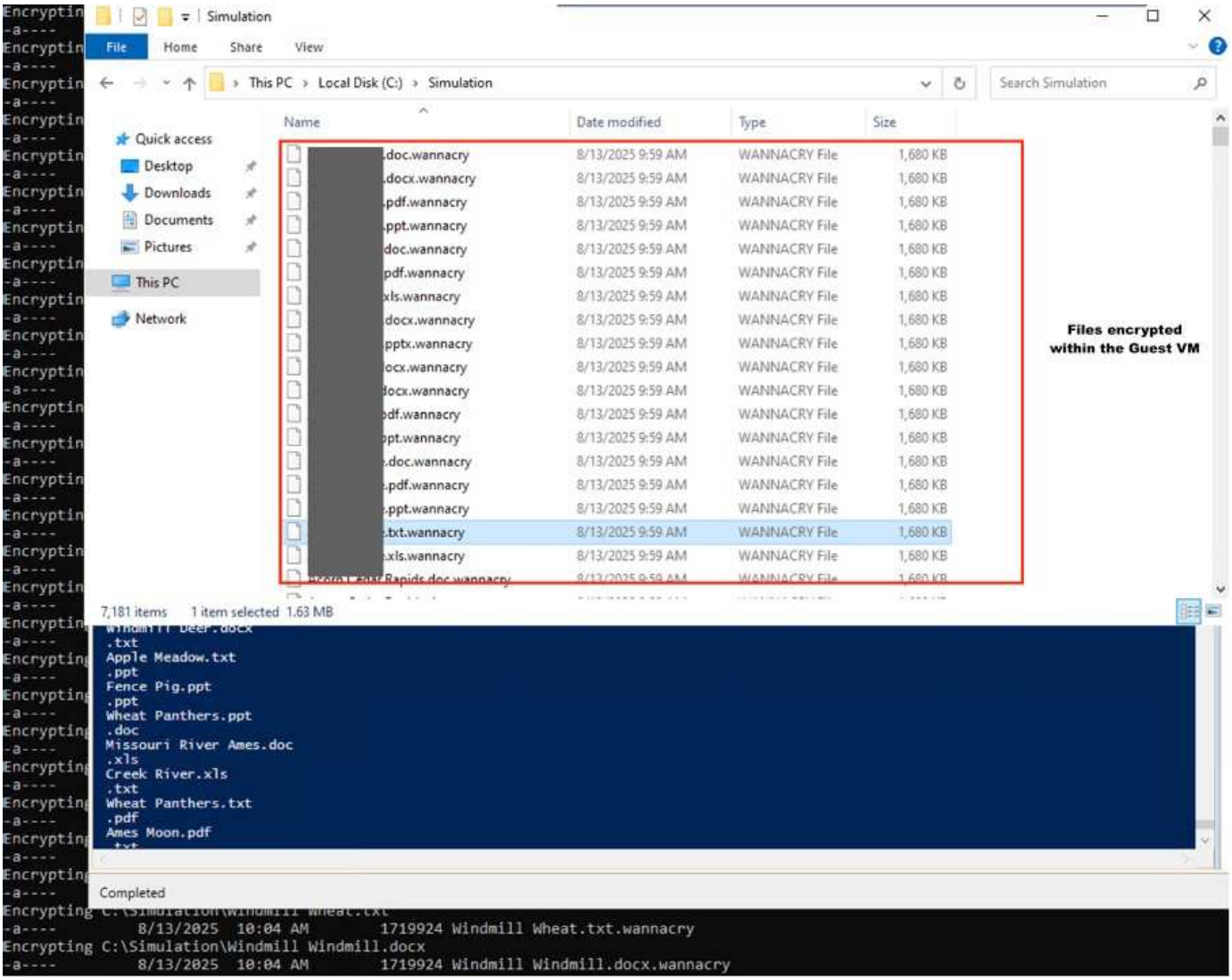
ARP avvia un periodo di valutazione da due a quattro settimane con una soglia del 75% per stabilire una base di riferimento per il comportamento della crittografia. I progressi durante questa fase possono essere monitorati utilizzando il `security anti-ransomware volume show` comando controllando lo **Stato di rilevamento del dispositivo di blocco**. Una volta completata la valutazione, lo stato **Active_suitable_workload** conferma che i livelli di entropia osservati sono adatti al monitoraggio continuo. Sulla base dei dati raccolti, ARP regola automaticamente la propria soglia adattiva per garantire un rilevamento delle minacce accurato e reattivo. A seconda delle esigenze, l'intervallo di creazione degli snap può essere modificato dal valore predefinito di 4 ore a 1 ora. Eseguire questa modifica con cautela.

A partire da ONTAP 9.17.1, gli snapshot ARP vengono generati a intervalli regolari sia per i volumi NAS che SAN.

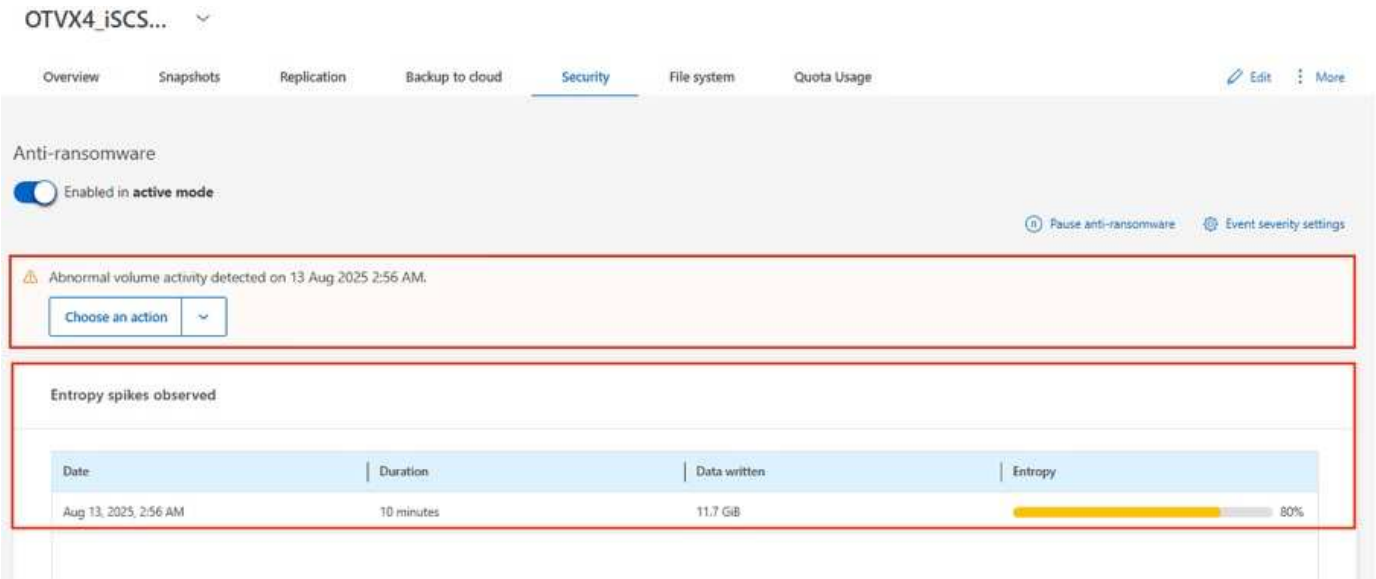


Per informazioni dettagliate, fare riferimento"Ambienti SAN e tipi di modalità"

È il momento di simulare un attacco. A scopo dimostrativo, i file vengono crittografati all'interno di una macchina virtuale in esecuzione su un datastore basato su ISCSI. Vengono generati circa 7000 file che purtroppo sono stati colpiti da attacchi ransomware.

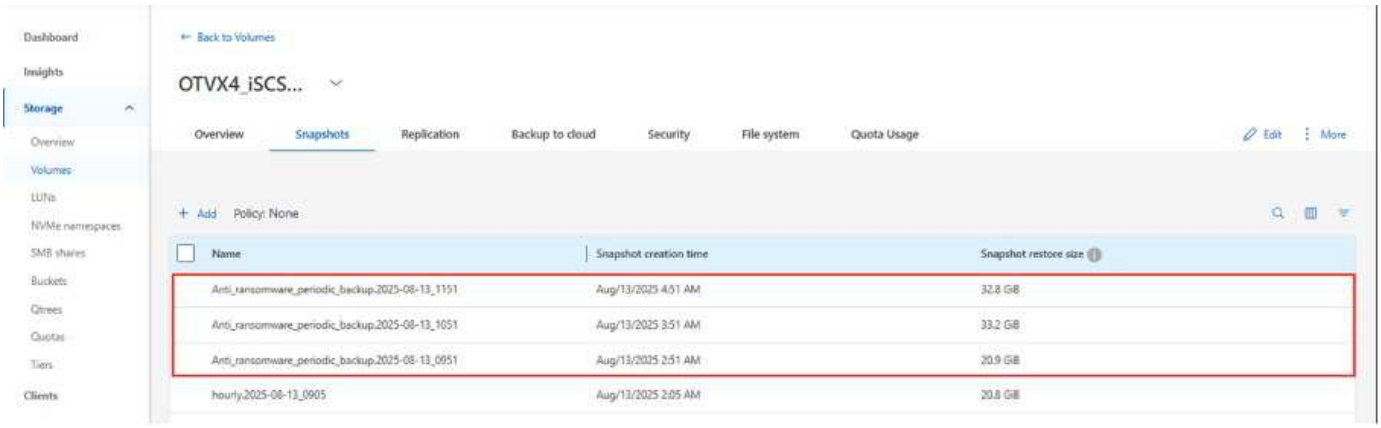


Entro 10 minuti, è stata rilevata un'attività anomala sul volume in base ai dati ad alta entropia e ARP ha generato un avviso di minaccia poiché ha rilevato un'anomalia di entropia all'interno della VM.

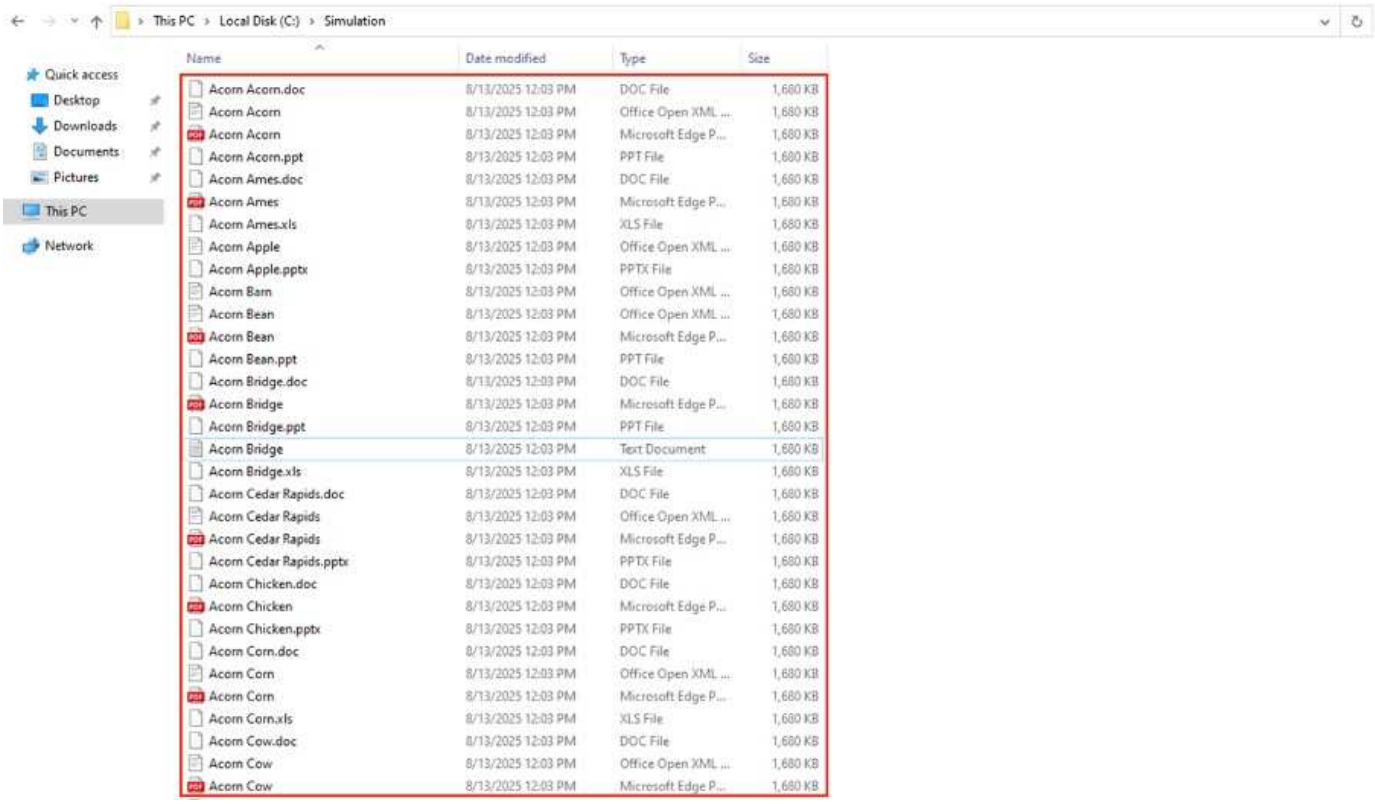


Recupera la VM e i suoi dati dopo un attacco ransomware

Una volta confermato l'attacco in base ai passaggi descritti sopra, utilizzare uno degli snapshot ARP o un altro snapshot del volume per ripristinare i dati.



Una volta ripristinati, tutti i file sono recuperati.



Per una guida dettagliata, vedere"Ripristina i dati dallo snapshot ARP dopo un attacco ransomware"

ONTAP come livello di difesa per VMware e oltre

Con pochi clic, le aziende possono migliorare senza problemi la propria strategia di protezione dei dati. Grazie a meccanismi di rilevamento avanzati basati sull'apprendimento automatico, ONTAP introduce un potente livello di difesa negli ambienti VMware. Questa protezione intelligente non solo identifica le minacce in anticipo, ma aiuta anche a mitigare i potenziali danni prima che degenerino.

Questo caso d'uso non si applica solo a VMware. È possibile estendere gli stessi principi a qualsiasi applicazione basata su NAS o SAN per creare un'architettura di sicurezza multilivello. Gli aggressori sono

costretti a muoversi attraverso diversi livelli fortificati, riducendo significativamente il rischio di violazioni riuscite.

ONTAP non si limita a proteggere i dati: consente alle organizzazioni di rimanere resilienti di fronte alle minacce in continua evoluzione.

Soluzioni di backup e disaster recovery

Scopri di più sul backup e il ripristino delle macchine virtuali utilizzando il plug-in SnapCenter per VMware vSphere

Il SnapCenter Plug-in for VMware vSphere consente operazioni di backup e ripristino rapide e coerenti con le VM per VM, datastore e file VMDK. Questo plug-in VMware si integra con SnapCenter Server per supportare il backup e il ripristino basati sulle applicazioni per i plug-in specifici delle applicazioni SnapCenter .

Risorse di documentazione

Per informazioni dettagliate, fare riferimento alle seguenti risorse di documentazione.

- "Documentazione SnapCenter Plug-in for VMware vSphere"

Risorse della soluzione

Fare riferimento alla seguente soluzione di backup 3-2-1 con SnapCenter Plug-in for VMware vSphere e BlueXP backup and recovery per VM.

Rapporto tecnico:"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM"

Blog Tech ONTAP :"Protezione dei dati 3-2-1 per VMware con plug-in SnapCenter e BlueXP backup and recovery per VM"

Risorse video

SnapCenter Plug-in for VMware vSphere - Prerequisiti della soluzione

SnapCenter Plug-in for VMware vSphere - Distribuzione

SnapCenter Plug-in for VMware vSphere - Flusso di lavoro di backup

SnapCenter Plug-in for VMware vSphere - Ripristino del flusso di lavoro

SnapCenter - Flusso di lavoro di ripristino SQL

Scopri di più sul disaster recovery delle macchine virtuali utilizzando BlueXP disaster recovery

Il BlueXP disaster recovery automatizza la replica e il ripristino delle macchine virtuali VMware utilizzando l’archiviazione ONTAP . Supporta il ripristino dalla configurazione on-premise a VMware Cloud on AWS con Amazon FSx for NetApp ONTAP o un altro ambiente VMware on-premise.

Introduzione

Avere un piano efficace e una combinazione di tecnologie garantisce la protezione di dati, applicazioni e VM critici. La sfida della DR è determinare il livello di protezione appropriato e i costi associati.

Gli array ONTAP offrono una replica integrata per trasferire i dati del volume e, di conseguenza, le macchine virtuali residenti sui LUN del datastore designati, da un sito all'altro. BlueXP DRaaS si integra con vSphere e automatizza l'intero flusso di lavoro per un failover e un failback senza interruzioni in caso di disastro.

Per ulteriori informazioni su BlueXP DRaaS, vedere"Panoramica di BlueXP DRaaS" .

Considerazioni

La parte più dispendiosa in termini di tempo di un failover DR in un ambiente VMware vSphere è l'esecuzione dei passaggi necessari per inventariare, registrare, riconfigurare e accendere le VM nel sito DR. Una soluzione ideale ha sia un basso RPO (misurato in minuti) sia un basso RTO (misurato in minuti o ore). Un fattore che spesso viene trascurato in una soluzione DR è la capacità di testare la soluzione DR in modo efficiente a intervalli periodici.

Per progettare una soluzione DR, è necessario tenere a mente i seguenti fattori:

- L'obiettivo del tempo di recupero (RTO). L'RTO indica la rapidità con cui un'azienda può riprendersi da un disastro o, più specificamente, il tempo necessario per eseguire il processo di ripristino e rendere nuovamente disponibili i servizi aziendali.
- L'obiettivo del punto di ripristino (RPO). L'RPO indica l'età dei dati recuperati dopo essere stati resi disponibili, in relazione al momento in cui si è verificato il disastro.
- Scalabilità e adattabilità. Questo fattore include la possibilità di aumentare gradualmente le risorse di archiviazione man mano che aumenta la domanda.

Per maggiori informazioni tecniche sulle soluzioni disponibili, consultare:

- "DR tramite BlueXP DRaaS per datastore NFS"
- "DR tramite BlueXP DRaaS per datastore VMFS"

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.