Erste Schritte

NetApp virtualization solutions

NetApp
August 24, 2025

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

Inhalt

Erste Schritte . . . 1
- Kernkonzepte . . . 1
  - Erfahren Sie mehr über ONTAP für VMware vSphere . . . 1
  - Erfahren Sie mehr über NetApp -Plattformen für VMware . . . 4
  - Erfahren Sie mehr über hybride Multicloud-Umgebungen mit NetApp und VMware . . . 8
- Verwaltungstools und -lösungen . . . 9
  - Erfahren Sie mehr über die Verwaltung virtueller Maschinen mit ONTAP tools for VMware vSphere . . . 9
  - Erfahren Sie mehr über die Verwendung von ONTAP und VMware APIs für die Verwaltung . . . 10
  - Erfahren Sie mehr über die Überwachung einer kompletten Infrastruktur mit NetApp Data Infrastructure Insights . . . 11
  - Erfahren Sie mehr über VMs von VMware vSphere bis hin zu ONTAP -Datenspeichern . . . 12
- Datenschutzlösungen . . . 13
  - Erfahren Sie mehr über den Schutz von VMware-Umgebungen mit MetroCluster und SnapMirror Active Sync . . . 13
  - Erfahren Sie mehr über die Minimierung von Sicherheits- und Ransomware-Risiken für VMware-Workloads . . . 14
  - Autonomer Ransomware-Schutz für NFS und VMFS . . . 15
- Backup- und Disaster-Recovery-Lösungen . . . 22
  - Erfahren Sie mehr über die Sicherung und Wiederherstellung virtueller Maschinen mit dem SnapCenter -Plug-in für VMware vSphere . . . 22
  - Erfahren Sie mehr über die Notfallwiederherstellung virtueller Maschinen mit BlueXP disaster recovery . . . 22

Erste Schritte

Kernkonzepte

Erfahren Sie mehr über ONTAP für VMware vSphere

NetApp ONTAP ist eine führende Speicherlösung für VMware vSphere und bietet fast zwei Jahrzehnte zuverlässige Leistung für Anwendungsfälle mit Datenspeichern und Gastverbindungen im Speicher. ONTAP unterstützt SAN- und NAS-Protokolle, ermöglicht eine unabhängige Skalierung von Speicher- und Rechenressourcen und entlastet Hosts von Speicheraufgaben. Zu den Vorteilen zählen starker Datenschutz, hohe Verfügbarkeit und erweiterte Geschäftskontinuitätsfunktionen wie SnapMirror und MetroCluster.

Einführung

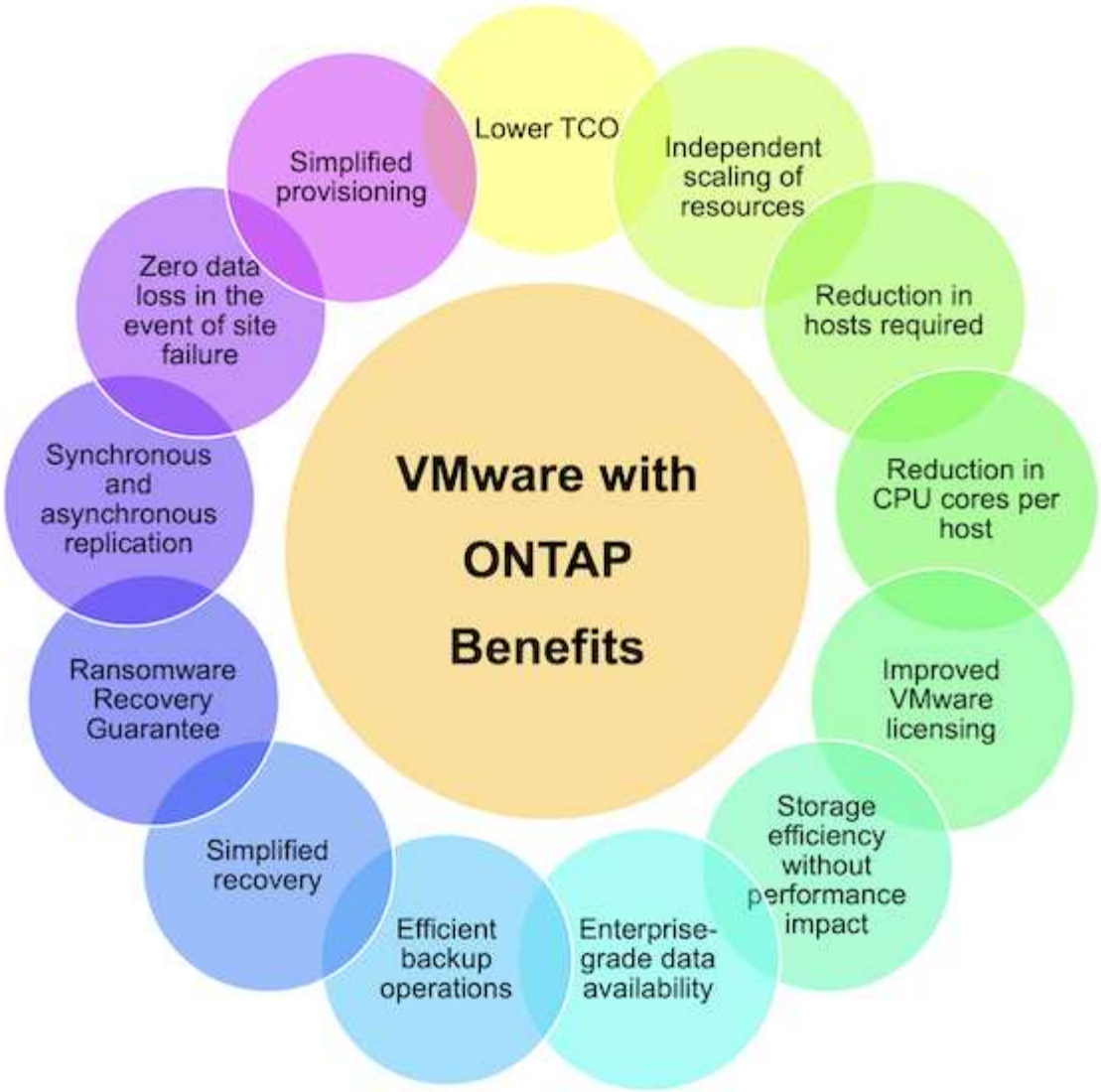
NetApp erweitert seine Kapazitäten kontinuierlich um innovative Funktionen, um die Speicherverwaltung zu vereinfachen, gleichzeitig die Kosten zu senken und das Vertrauen in eine konsolidierte, VMware-basierte virtuelle Infrastruktur zu stärken, die Cloud-fähig ist. Diese Lösungssammlung stellt ONTAP -Angebote für VMware vSphere Foundation und VMware Cloud Foundation vor, einschließlich der neuesten Produktinformationen und Best Practices, um die Bereitstellung zu optimieren, Risiken zu reduzieren und die Verwaltung zu vereinfachen.

Weitere Informationen zur Verwendung von ONTAP mit VMware vSphere finden Sie unter "VMware vSphere mit ONTAP" .

Warum ONTAP für VMware

Es gibt viele Gründe, warum sich Zehntausende von Kunden für ONTAP als Speicherlösung für vSphere entschieden haben. Dazu gehören beispielsweise ein einheitliches Speichersystem, das sowohl SAN- als auch NAS-Protokolle unterstützt, robuste Datenschutzfunktionen durch platzsparende Snapshots und eine Fülle von Tools, die Sie bei der Verwaltung von Anwendungsdaten unterstützen. Durch die Verwendung eines vom Hypervisor getrennten Speichersystems können Sie viele Funktionen auslagern und Ihre Investition in vSphere-Hostsysteme maximieren. Dieser Ansatz stellt nicht nur sicher, dass Ihre Hostressourcen auf Anwendungs-Workloads konzentriert sind, sondern vermeidet auch zufällige Leistungseinbußen bei Anwendungen durch Speichervorgänge.

Die Verwendung von ONTAP zusammen mit vSphere ist eine großartige Kombination, mit der Sie die Kosten für Host-Hardware und VMware-Software senken können. Darüber hinaus können Sie Ihre Daten zu geringeren Kosten bei gleichbleibend hoher Leistung schützen. Da virtualisierte Workloads mobil sind, können Sie mithilfe von Storage vMotion verschiedene Ansätze erkunden, um VMs zwischen VMFS-, NFS- oder vVols Datenspeichern zu verschieben, und zwar alle auf demselben Speichersystem.



Hier sind die wichtigsten Vorteile für NetApp und VMware-Kunden:

- **Flexibilität am ersten Tag und beim Skalieren.** Der Bedarf an Wachstum kann bei jeder Architektur aus den unterschiedlichsten Gründen entstehen. Unabhängig davon, ob sich die Leistungs- oder Kapazitätsanforderungen weiterentwickeln oder neue Hosts hinzugefügt werden und Netzwerk- oder Fabric-Überlegungen auftauchen, ist es wichtig, eine Speicherplattform auszuwählen, die eine unabhängige Skalierung der Ressourcen ermöglicht.

  Mit ONTAP können Sie mit der erforderlichen Kapazität beginnen, diese nach Bedarf erweitern und die Vorteile der Tiering-Funktion nutzen, ohne zusätzliche Compute-Hosts hinzufügen zu müssen. Darüber hinaus kann ein einzelner ONTAP Cluster mit mehreren Workload-Domänen verwendet werden und vermeidet die Erstellung von Speicherinseln. Diese Vorteile führen zu erheblichen Kosteneinsparungen für Unternehmen.

- **Lagern Sie Speicheraufgaben auf ONTAP aus.** In typischen HCI-Umgebungen ist die Hostplattform für Rechenaufgaben, Speichervorgänge und jegliche Netzwerkoptimierung auf der Clientseite verantwortlich. Beispielsweise muss der CPU-Overhead bei der Bestimmung der Hardwareanforderungen der Rechenknoten berücksichtigt werden. Dieser Overhead lässt sich oft nur schwer im Voraus abschätzen. Er wird allgemein mit 10–15 % angegeben und hängt vom E/A-Profil der Workloads ab. Darüber hinaus ist es wichtig, den Speicherverbrauch zu berücksichtigen. Der Speicher-Overhead ist obligatorisch und sollte

nicht beeinträchtigt werden, um die Leistung aufrechtzuerhalten. Hosts können dies ausgleichen, indem sie RDMA-fähige NICs nutzen und so die Effizienz der Netzwerkübertragung verbessern, allerdings gegen Aufpreis. Schließlich werden bei einer HCI-Plattform Speicherfunktionen wie Speichereffizienz, RAID- und Fehlertoleranzen sowie Verschlüsselung von den Hosts übernommen.

Kunden können diese nachteiligen Auswirkungen auf die CPU-Ressourcen des Hosts durch die Nutzung von ONTAP abmildern. Diese Strategie ermöglicht es Hosts, sich auf Rechenaufgaben zu konzentrieren, während ONTAP die CPU-intensiven Speichervorgänge verwaltet. Diese Strategie verbessert die Gesamtleistung durch Optimierung der Speichereffizienz, Verschlüsselung, Snapshots und mehr und senkt gleichzeitig die Gesamtbetriebskosten. Dadurch wird nicht nur die Host-Leistung gesteigert und die Anzahl der Hosts verringert, die zur Bereitstellung derselben Arbeitslast erforderlich sind. Auch die Anzahl der pro Host erforderlichen Kerne wird reduziert, was zu weiteren Kosteneinsparungen führt. Diese Einsparungen erstrecken sich außerdem auf Energieeinsparungen, einen geringeren Kühlbedarf, optimierte Lizenzkosten und mehr; und zwar durch die Auslagerung CPU-intensiver Speicheraufgaben an ONTAP und die geringere Abhängigkeit von Hosts bei der Abwicklung aller Aufgaben.

- **Speichereffizienz** Obwohl NetApp als erstes Unternehmen Deduplizierung für Produktions-Workloads bereitstellte, war diese Innovation weder die erste noch die letzte in diesem Bereich. Es begann mit Snapshots, einem platzsparenden Datenschutzmechanismus ohne Leistungseinbußen, zusammen mit der FlexClone -Technologie zum sofortigen Erstellen von Lese-/Schreibkopien von VMs für die Produktion und Sicherung. NetApp lieferte anschließend Inline-Funktionen, darunter Deduplizierung, Komprimierung und Zero-Block-Deduplizierung, um den größtmöglichen Speicherplatz aus teuren SSDs herauszuholen. Vor Kurzem wurde bei ONTAP die Möglichkeit hinzugefügt, kleinere E/A-Vorgänge und Dateien mittels Komprimierung in einen Festplattenblock zu packen. Durch die Kombination dieser Funktionen konnten Kunden Einsparungen von bis zu 5:1 bei VSI und bis zu 30:1 bei VDI erzielen.
- **Datenverfügbarkeit auf Unternehmensniveau.** Der Schutz von Daten hat für jede IT-Organisation höchste Priorität. Die Planung von Workload-Fehlertoleranzen erfordert sorgfältige Überlegungen, um sicherzustellen, dass eine ausreichende Anzahl von Knoten verfügbar ist, wenn Hosts für Speichervorgänge verantwortlich sind. Mit zunehmender Anzahl tolerierter Fehler steigt auch der Bedarf an zusätzlichen Hosts und der Umfang des bereitgestellten Speichers, um die erforderliche VM-Speicherkapazität bereitzustellen.

  Die umfassenden Verfügbarkeitsfunktionen von ONTAP stellen sicher, dass die Daten immer zugänglich, sicher und belastbar sind, und machen es zu einer zuverlässigen Wahl für VMware-Bereitstellungen jeder Größe. Die Nutzung von gemeinsam genutztem Speicher in VMware-Umgebungen erleichtert die Bereitstellung kleinerer vSphere-Cluster, rationalisiert den Einrichtungsprozess und ermöglicht die gemeinsame Nutzung von Speicher über Cluster hinweg mit verbesserter Fehlertoleranz.

  Zu den wichtigsten ONTAP Verfügbarkeitsfunktionen gehören:

  - Hochverfügbarkeitsarchitektur (HA): ONTAP unterstützt eine Hochverfügbarkeitsarchitektur, die ein Cluster-Bereitstellungsmodell umfasst.
  - Automatisches Failover und Failback: Im Falle von Hardware- oder Softwarefehlern ermöglicht ONTAP ein automatisches Failover auf einen Standby-Speicherknoten. Sobald das Problem behoben ist, kann ein Failback durchgeführt werden, um die ursprüngliche Konfiguration wiederherzustellen und so die Ausfallzeit zu minimieren.
  - Integrierter Datenschutz: ONTAP umfasst integrierte Datenschutzfunktionen wie RAID-DP und RAID-TEC, die einen verbesserten Schutz vor Festplattenausfällen bieten und die Datenintegrität und -verfügbarkeit gewährleisten.
- **Effiziente Sicherungs- und Wiederherstellungsvorgänge.** Neben der Sicherung der Daten im Falle verschiedener Störungen müssen wir im Rahmen des regulären IT-Betriebs auch die Sicherung von VMs und Workloads einplanen. Snapshots erfassen den Zustand einer VM zu einem bestimmten Zeitpunkt, einschließlich der Festplatte, des Speichers und der Einstellungen der VM. Auf diese Weise kann ein

Administrator die VM in einen früheren Zustand zurücksetzen, wenn etwas schief geht, beispielsweise ein fehlgeschlagenes Update, eine Konfigurationsänderung oder ein Angriff durch Ransomware oder Viren. Der von Snapshots verbrauchte Speicherplatz sollte beim Entwurf einer ausgewogenen Lösung für VMware-Umgebungen berücksichtigt werden.

Snapshots sind zwar ein wichtiges Tool, doch ein übermäßiges Vertrauen auf VMware-basierte Snapshots wirft Bedenken hinsichtlich der Häufigkeit und der Aufbewahrungsrichtlinien auf. Darüber hinaus kann die Leistung durch zu viele VMware-basierte Snapshots beeinträchtigt werden. Es ist wichtig, Alternativen wie NetApp Snapshot-Kopien und das SnapCenter Plug-in for VMware vSphere in Betracht zu ziehen. SnapCenter nutzt Snapshot-Kopien. Dabei handelt es sich um schreibgeschützte, zeitpunktbezogene Abbilder eines Datenträgers, die sich zunächst Datenträgerblöcke mit dem aktiven Dateisystem teilen und daher keinen zusätzlichen Speicherplatz und nur minimalen Speicherplatz benötigen. Diese Snapshots haben einen vernachlässigbaren Leistungsaufwand, da sie nur Änderungen seit dem letzten Snapshot erfassen. Das SnapCenter Plug-in for VMware vSphere (SCV) nutzt diese Snapshots, um effiziente, absturzkonsistente Backups und Wiederherstellungen für VMs, Datastores und VMDKs bereitzustellen. Diese Vorgänge werden nahtlos und ohne Leistungseinbußen in eine vCenter-Umgebung integriert. Darüber hinaus ermöglicht ONTAP das Auslagern von Snapshots in den Objektspeicher zur langfristigen Aufbewahrung.

- **Ganzheitliche Geschäftskontinuitätsfunktionen.** Über die standardmäßige Fehlertoleranz sowie Sicherung und Wiederherstellung hinaus muss ein Unternehmen verschiedene Szenarien wie Katastrophen, Ransomware-Angriffe und Standortmigrationen im Rechenzentrum planen. Um diese Herausforderungen bei hostbasiertem Speicher zu bewältigen, muss man sich in der Regel auf eine Reihe von Drittanbieterlösungen verlassen, um Katastrophen effektiv zu mildern und die Geschäftskontinuität sicherzustellen. Darüber hinaus kann eine unzureichende Dimensionierung der Netzwerk- und Speichergeräte bei netzwerkintensiven Szenarien zu erheblichen Leistungseinbußen führen.

  Aufbauend auf seinen Verfügbarkeitsfunktionen sowie seinen Backup- und Wiederherstellungsfunktionen ist ONTAP ein integraler Bestandteil einer umfassenden Business-Continuity-Strategie für VMware-Umgebungen. Organisationen benötigen VMs und Workloads, die sowohl während des Normalbetriebs als auch während der Wartungsarbeiten nahtlos verfügbar sind, über robuste Schutz- und Wiederherstellungsfunktionen verfügen und platzsparende und kostengünstige Disaster-Recovery-Lösungen nutzen können.

  Zu den wichtigsten Funktionen von ONTAP Business Continuity gehören:

  - Datenreplikation mit SnapMirror: SnapMirror nutzt Snapshot-Kopien und ermöglicht die asynchrone und synchrone Replikation von Daten an Remote-Standorte oder in Cloud-Umgebungen zur Notfallwiederherstellung.
  - MetroCluster: Die MetroCluster -Technologie von ONTAP ermöglicht eine synchrone Replikation zwischen geografisch getrennten Standorten und stellt so sicher, dass im Falle eines Standortausfalls kein Datenverlust auftritt und eine schnelle Wiederherstellung möglich ist.
  - Cloud-Tiering: Cloud-Tiering identifiziert automatisch kalte Daten (Daten, auf die selten zugegriffen wird) auf dem Primärspeicher und verschiebt sie in einen kostengünstigeren Objektspeicher, entweder in der Cloud oder vor Ort.
  - BlueXP DRaaS: NetApp BlueXP Disaster Recovery as a Service (DRaaS) ist eine umfassende Lösung, die Unternehmen robuste Disaster-Recovery-Funktionen bietet und im Katastrophenfall Datenschutz, schnelle Wiederherstellung und Geschäftskontinuität gewährleistet.

Erfahren Sie mehr über NetApp -Plattformen für VMware

NetApp bietet auf VMware-Umgebungen zugeschnittene Plattformen, darunter FAS für kostengünstigen Speicher, AFF für Hochleistungs-Workloads, ASA für dedizierte SAN-

Bereitstellungen und Cloud-Lösungen für Hybrid- und Multicloud-Architekturen. Diese Plattformen werden von ONTAP betrieben und unterstützen VMware Cloud Foundation und VMware vSphere.

Einführung

Diese Angebote verbessern die Leistung, Skalierbarkeit und Datenverwaltung für den VMware-Administrator. Darüber hinaus wird ONTAP auf diesen Plattformen eingesetzt und bietet eine einheitliche, skalierbare und effiziente Datenverwaltungslösung, die verschiedene Speicherprotokolle unterstützt, den Datenschutz verbessert und die Leistung für unterschiedliche Workloads optimiert.

Gemeinsame Vorteile aller NetApp Plattformen

- **VMware-Integration:** Alle NetApp -Plattformen bieten tiefe Integrationen mit VMware, wodurch die Effizienz der Speicherumgebung verbessert wird. Vor-Ort-Lösungen können Plug-Ins, APIs, VAAI und VASA nutzen, um das gesamte Datenmanagement zu verbessern und gleichzeitig die Vielseitigkeit der Infrastruktur zu steigern.
- **Kostenoptimierung und Speichereffizienz:** Durch die Nutzung von NetApp -Speicher profitieren Sie von nativen Effizienztechnologien wie Deduplizierung, Komprimierung und Thin Provisioning, wodurch Speicherverbrauch und -kosten erheblich gesenkt und gleichzeitig Kapazitätsauslastung und Leistung maximiert werden. Darüber hinaus führen diese Speichereinsparungen zu einer geringeren Belastung der Rechenressourcen.
- **Einheitliches Datenmanagement:** ONTAP bietet eine einzige Verwaltungsschnittstelle sowohl für lokale als auch für Cloud-basierte Speicherung, wodurch die Verwaltung vereinfacht und die Komplexität reduziert wird. Dies ermöglicht eine nahtlose Datenbewegung und -verwaltung zwischen lokalen und Cloud-Umgebungen und bietet Flexibilität und Skalierbarkeit für VMware-Workloads.
- **Multiprotokoll-Unterstützung:** ONTAP unterstützt eine breite Palette von Speicherprotokollen, darunter NFS, CIFS/SMB, iSCSI, FC und NVMe, sodass Unternehmen Workloads auf einer einzigen Plattform konsolidieren oder speziell entwickelte SAN-Angebote nutzen können, ohne Datensilos zu erstellen.
- **Automatisierung und Orchestrierung:** Unterstützung für Automatisierungstools wie VMware Cloud Foundation Automation (ehemals VMware Aria Automation) und Integration mit Ansible und anderen Automatisierungsframeworks rationalisieren den Betrieb und reduzieren den Verwaltungsaufwand.
- **Sicherheit:** Robuste Sicherheitsfunktionen, darunter Verschlüsselung im Ruhezustand und während der Übertragung, sichere Mandantenfähigkeit und rollenbasierte Zugriffskontrolle, gewährleisten die Sicherheit von VMware-Umgebungen.
- * ONTAP Tools für VMware:* NetApp ONTAP Tools für VMware bieten nahtlose Integrations- und Verwaltungsfunktionen und ermöglichen über eine einheitliche und intuitive Benutzeroberfläche eine effiziente Speicherbereitstellung, Datenschutz und verbesserte Leistung für VMware-Umgebungen.
- * SnapCenter für VMware vSphere:* NetApp SnapCenter für VMware vSphere vereinfacht und zentralisiert Datenschutz-, Sicherungs- und Wiederherstellungsvorgänge für VMware-Umgebungen und gewährleistet so eine zuverlässige und effiziente Verwaltung der Daten virtueller Maschinen.
- **Hohe Verfügbarkeit und Ausfallsicherheit:** Funktionen wie RAID-TEC und RAID-DP bieten robusten Datenschutz und hohe Verfügbarkeit, die für VMware-Umgebungen von entscheidender Bedeutung sind.
- **Quality of Service (QoS):** Ermöglicht Administratoren, Leistungsgarantien für verschiedene VMs festzulegen und so sicherzustellen, dass kritische Workloads die erforderlichen Ressourcen erhalten.

Hinweis: NetApp Cloud-Lösungen verfügen möglicherweise über durch den Cloud-Anbieter eingeschränkte Funktionen, sind jedoch dennoch sehr robust für die Gastverbindung und die Unterstützung nativer NFS-Datenspeicher.

Vorteile von NetApp ASA (All SAN Array)

- **Optimiert für SAN:** Speziell für SAN-Workloads entwickelt und bietet hohe Leistung und geringe Latenz für VMware-Umgebungen, die auf Blockspeicher basieren.
- **Verbesserte Hochverfügbarkeit:** Funktionen wie Active-Active-Controller und synchrone Replikation gewährleisten kontinuierliche Verfügbarkeit und Datenschutz.

Die ASA Produktreihe umfasst Modelle der A-Serie und der C-Serie.

Die All-NVMe-Flash-Arrays der NetApp A-Serie sind für Hochleistungs-Workloads konzipiert und bieten extrem niedrige Latenz und hohe Ausfallsicherheit, sodass sie sich für unternehmenskritische Anwendungen eignen.

QLC-Flash-Arrays der C-Serie sind auf Anwendungsfälle mit höherer Kapazität ausgerichtet und bieten die Geschwindigkeit von Flash mit der Wirtschaftlichkeit von Hybrid-Flash.

Unterstützung von Speicherprotokollen

Die ASA unterstützt alle Standard-SAN-Protokolle, einschließlich iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) und NVME over Fabrics.

iSCSI – NetApp ASA bietet robuste Unterstützung für iSCSI und ermöglicht so den Zugriff auf Speichergeräte auf Blockebene über IP-Netzwerke. Es bietet eine nahtlose Integration mit iSCSI-Initiatoren und ermöglicht so eine effiziente Bereitstellung und Verwaltung von iSCSI-LUNs. Erweiterte Funktionen von ONTAP, wie Multipathing, CHAP-Authentifizierung und ALUA-Unterstützung.

Designhinweise zu iSCSI-Konfigurationen finden Sie im "Referenzdokumentation zur SAN-Konfiguration" .

Fibre Channel – NetApp ASA bietet umfassende Unterstützung für Fibre Channel (FC), eine Hochgeschwindigkeits-Netzwerktechnologie, die häufig in Storage Area Networks (SANs) verwendet wird. ONTAP lässt sich nahtlos in die FC-Infrastruktur integrieren und bietet zuverlässigen und effizienten Zugriff auf

Speichergeräte auf Blockebene. Es bietet Funktionen wie Zoning, Multipathing und Fabric Login (FLOGI), um die Leistung zu optimieren, die Sicherheit zu verbessern und eine nahtlose Konnektivität in FC-Umgebungen sicherzustellen.

Hinweise zum Design von Fibre Channel-Konfigurationen finden Sie im "Referenzdokumentation zur SAN-Konfiguration" .

NVMe über Fabrics – NetApp ONTAP und ASA unterstützen NVMe über Fabrics. NVMe/FC ermöglicht die Verwendung von NVMe-Speichergeräten über Fibre-Channel-Infrastruktur und NVMe/TCP über Speicher-IP-Netzwerke.

Designrichtlinien für NVMe finden Sie unter "NVMe-Konfiguration, -Unterstützung und -Einschränkungen"

Aktiv-Aktiv-Technologie

NetApp All-Flash SAN-Arrays ermöglichen Active-Active-Pfade über beide Controller, sodass das Host-Betriebssystem nicht mehr warten muss, bis ein aktiver Pfad ausfällt, bevor der alternative Pfad aktiviert wird. Dies bedeutet, dass der Host alle verfügbaren Pfade auf allen Controllern nutzen kann. Dadurch wird sichergestellt, dass immer aktive Pfade vorhanden sind, unabhängig davon, ob sich das System in einem stabilen Zustand befindet oder ein Controller-Failover-Vorgang durchgeführt wird.

Darüber hinaus bietet NetApp ASA eine besondere Funktion, die die Geschwindigkeit des SAN-Failovers erheblich verbessert. Jeder Controller repliziert kontinuierlich wichtige LUN-Metadaten an seinen Partner. Dadurch ist jeder Controller darauf vorbereitet, im Falle eines plötzlichen Ausfalls seines Partners die Aufgaben der Datenbereitstellung zu übernehmen. Diese Bereitschaft ist möglich, weil der Controller bereits über die erforderlichen Informationen verfügt, um mit der Nutzung der Laufwerke zu beginnen, die zuvor vom ausgefallenen Controller verwaltet wurden.

Bei Active-Active-Pathing betragen die IO-Wiederaufnahmezeiten sowohl bei geplanten als auch bei ungeplanten Übernahmen 2–3 Sekunden.

Weitere Informationen finden Sie unter "TR-4968, NetApp All-SAS Array – Datenverfügbarkeit und -integrität mit dem NetApp ASA" .

Ausführliche Informationen finden Sie im "NetApp ASA -Landingpage" .

Vorteile von NetApp AFF (All Flash FAS)

- **Extreme Leistung:** Nutzt All-Flash-Speicher, um Latenzen von unter einer Millisekunde und hohe IOPS zu liefern, ideal für leistungssensible VMware-Workloads.
- **Konstant niedrige Latenz:** Gewährleistet eine vorhersehbare Leistung für kritische Anwendungen und VMs, die für die Einhaltung von SLAs von entscheidender Bedeutung ist.

Weitere Informationen zu NetApp AFF A-Series Storage Arrays finden Sie im"NetApp AFF A-Serie" Zielseite.

Weitere Informationen zu NetApp C-Series Storage Arrays finden Sie im"NetApp AFF C-Serie" Zielseite.

Vorteile von NetApp FAS (Fabric-Attached Storage)

- **Unified Storage Architecture:** Unterstützt sowohl SAN- (Blockebene) als auch NAS-Protokolle (Dateiebene) und ist daher vielseitig für verschiedene VMware-Workloads geeignet.
- **Kostengünstig:** Ideal für Umgebungen, die ein Gleichgewicht zwischen Leistung und Kosten erfordern,

bietet eine Kombination aus HDDs und SSDs.

Vorteile von Cloud-Lösungen

- **Cloud-natives Datenmanagement:** Nutzt Cloud-native Angebote, um die Datenmobilität, Sicherung und Notfallwiederherstellung für VMware-Workloads zu verbessern. Die Unterstützung für native NFS-Datenspeicherunterstützung für VMware-Cloud-Workloads ist wie folgt:
  - VMware Cloud auf AWS mit Amazon FSx for NetApp ONTAP
  - Azure VMware Service mit Azure NetApp Files
  - Google Cloud VMware Engine mit Google Cloud NetApp Volume –
- **Hybrid Cloud-Flexibilität:** Nahtlose Integration zwischen lokalen und Cloud-Umgebungen, die Flexibilität für VMware-Workloads bietet, die sich über mehrere Standorte erstrecken.

Zusammenfassung

Zusammenfassend lässt sich sagen, ONTAP und NetApp -Plattformen eine umfassende Reihe von Vorteilen für VMware-Workloads bieten und Leistung, Skalierbarkeit und Datenverwaltung verbessern. Während gemeinsame Funktionen eine solide Grundlage bilden, bietet jede Plattform differenzierte, auf spezielle Anforderungen zugeschnittene Vorteile, sei es kostengünstiger Speicher mit FAS, hohe Leistung mit AFF, optimierte SAN-Leistung mit ASA oder Hybrid-Cloud-Flexibilität mit NetApp -Cloud-Angeboten.

Erfahren Sie mehr über hybride Multicloud-Umgebungen mit NetApp und VMware

Entdecken Sie, wie NetApp und VMware hybride Multicloud-Setups optimieren, indem sie lokale Infrastruktur mit öffentlichen Cloud-Diensten integrieren und so Workload-Migration, Ressourcenoptimierung und konsistente Vorgänge in allen Umgebungen ermöglichen.

Einführung

Dieser Ansatz ermöglicht es Unternehmen, Workloads problemlos zu migrieren, die Ressourcennutzung zu optimieren und konsistente Vorgänge in beiden Umgebungen aufrechtzuerhalten.

Weitere Informationen zu Hybrid-Cloud-Szenarien mit VMware und NetApp finden Sie unter"Übersicht über NetApp Hybrid Multicloud mit VMware" .

VMware-Bereitstellungsszenarien mit NetApp

In diesem Abschnitt werden verschiedene Bereitstellungsoptionen für VMware-Umgebungen in lokalen und öffentlichen Clouds beschrieben. Jeder der Cloud-Anbieter unterstützt einen VMware Software Defined Data Center (SDDC)- und/oder VMware Cloud Foundation (VCF)-Stack innerhalb seiner jeweiligen öffentlichen Cloud-Angebote.

- **VMware vor Ort**

Die Verwendung von VMware mit NetApp -Speicher vor Ort bietet eine robuste, skalierbare und flexible Virtualisierungsumgebung. Durch die Kombination der erweiterten Datenverwaltungsfunktionen von NetApp wie Deduplizierung, Komprimierung und effiziente Snapshots mit dem entsprechenden Speichersystem auf Basis von ONTAP können Kunden die für sie geeignete Plattform auswählen. Diese Kombination gewährleistet hohe Leistung, Zuverlässigkeit und vereinfachte Verwaltung für virtualisierte Workloads und verbessert so die Gesamteffizienz des Rechenzentrums.

- **Azure VMware-Lösung**

Azure VMware Solution ist ein Hybrid-Cloud-Dienst, der voll funktionsfähige VMware SDDCs innerhalb der öffentlichen Microsoft Azure-Cloud ermöglicht. Azure VMware Solution ist eine Erstanbieterlösung, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware unter Nutzung der Azure-Infrastruktur verifiziert wurde. Dies bedeutet, dass Kunden bei der Bereitstellung der Azure VMware Solution VMware ESXi für die Computervirtualisierung, vSAN für hyperkonvergenten Speicher und NSX für Netzwerk und Sicherheit erhalten und gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Rechenzentrumseinrichtungen und der Nähe zum umfangreichen Ökosystem nativer Azure-Dienste und -Lösungen profitieren.

- **VMware Cloud auf AWS**

VMware Cloud auf AWS bringt die SDDC-Software der Enterprise-Klasse von VMware in die AWS Cloud mit optimiertem Zugriff auf native AWS-Dienste. VMware Cloud on AWS basiert auf VMware Cloud Foundation und integriert die Computing-, Speicher- und Netzwerkvirtualisierungsprodukte von VMware (VMware vSphere, VMware vSAN und VMware NSX) zusammen mit der VMware vCenter Server-Verwaltung, die für die Ausführung auf einer dedizierten, elastischen Bare-Metal-AWS-Infrastruktur optimiert ist.

- **Google Cloud VMware Engine**

Google Cloud VMware Engine ist ein Infrastructure-as-a-Service (IaaS)-Angebot, das auf der leistungsstarken, skalierbaren Infrastruktur und dem VMware Cloud Foundation Stack von Google Cloud basiert – VMware vSphere, vCenter, vSAN und NSX-T. Dieser Dienst ermöglicht einen schnellen Weg in die Cloud und ermöglicht die nahtlose Migration oder Erweiterung bestehender VMware-Workloads von lokalen Umgebungen zur Google Cloud Platform, ohne die Kosten, den Aufwand oder das Risiko einer Neustrukturierung von Anwendungen oder Umrüstungen. Es handelt sich um einen von Google verkauften und unterstützten Dienst in enger Zusammenarbeit mit VMware.

Verwaltungstools und -lösungen

Erfahren Sie mehr über die Verwaltung virtueller Maschinen mit ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere optimieren das Lebenszyklusmanagement für VMs mit NetApp -Speicher. Administratoren können den Speicher direkt vom vCenter Server aus verwalten, was den Betrieb vereinfacht und die Skalierbarkeit verbessert. Schlüsselkomponenten wie die Virtual Storage Console (VSC), der VASA Provider und der Storage Replication Adapter (SRA) optimieren die Bereitstellung, Leistungsüberwachung und Notfallwiederherstellung.

Einführung

Es ermöglicht Administratoren, den Speicher innerhalb des vCenter Servers direkt zu verwalten und die Speicher- und Datenverwaltung für VMware-Umgebungen zu vereinfachen. Das Plug-In-Tool für den VMware vSphere-Client ist darauf ausgelegt, Plug-In-Funktionen in den vSphere-Client zu integrieren, ohne dass eine Ausführung innerhalb von vCenter Server erforderlich ist. Dies bietet Plug-In-Isolierung und ermöglicht die Skalierung von Plug-Ins, die in großen vSphere-Umgebungen ausgeführt werden.

ONTAP Tools-Komponenten

- **Virtual Storage Console (VSC)** Die VSC umfasst die in den vSphere-Client integrierte Schnittstelle, über

die Sie Speichercontroller hinzufügen, Datenspeicher bereitstellen, die Leistung von Datenspeichern überwachen und ESXi-Hosteinstellungen anzeigen und aktualisieren können.

- **VASA-Anbieter** Die VMware vSphere APIs for Storage Awareness (VASA)-Anbieter für ONTAP senden Informationen über den von VMware vSphere verwendeten Speicher an den vCenter Server und ermöglichen so die Bereitstellung von VMware Virtual Volumes (vVols)-Datenspeichern, die Erstellung und Verwendung von Speicherkapazitätsprofilen, die Konformitätsprüfung und die Leistungsüberwachung.
- **Storage Replication Adapter (SRA)** Wenn SRA aktiviert ist und mit VMware Site Recovery Manager (SRM) verwendet wird, erleichtert es die Wiederherstellung von vCenter Server-Datenspeichern und virtuellen Maschinen im Falle eines Fehlers und ermöglicht die Konfiguration geschützter Sites und Wiederherstellungssites für die Notfallwiederherstellung.

Weitere Informationen zu NetApp ONTAP -Tools für VMware finden Sie unter "ONTAP tools for VMware vSphere Dokumentation" .

Erfahren Sie mehr über die Verwendung von ONTAP und VMware APIs für die Verwaltung

ONTAP und VMware bieten APIs für die nahtlose Integration und Automatisierung zwischen Speicher- und Virtualisierungsplattformen. Dies ermöglicht eine optimierte Bereitstellung, Überwachung und Datensicherung, um die Workflow-Konsistenz zu verbessern.

Einführung

VMware bietet eine Reihe von APIs, die Administratoren die programmgesteuerte Interaktion mit verschiedenen VMware-Produkten und -Diensten ermöglichen und so die Effizienz und Konsistenz im Betrieb verbessern. Darüber hinaus bieten NetApp ONTAP APIs einen robusten Satz von Tools, mit denen Administratoren die Verwaltung von Speicherumgebungen automatisieren, integrieren und optimieren können, insbesondere in Verbindung mit VMware-Workloads. Diese APIs ermöglichen eine nahtlose Interaktion zwischen ONTAP Speichersystemen und VMware und verbessern so Effizienz, Leistung und Datenschutz.

VMware-basierte APIs

- **VMware vSphere API:** Die vSphere API ist eine umfassende API, die es Administratoren ermöglicht, VMware vSphere-Umgebungen zu verwalten und zu automatisieren. Es bietet Zugriff auf eine breite Palette von vSphere-Funktionen, einschließlich Bereitstellung, Konfiguration, Überwachung und Lebenszyklusverwaltung virtueller Maschinen.
- **VMware vCenter Server REST API:** Die vCenter Server REST API bietet eine moderne, RESTful-Schnittstelle zur Verwaltung von vCenter Server und den zugehörigen Komponenten. Es vereinfacht die Automatisierung und Integration mit anderen Systemen und Tools.
- **VMware Cloud Foundation API:** Die VMware Software-Defined Data Center (SDDC)-APIs bieten programmgesteuerten Zugriff auf die verschiedenen Komponenten und Dienste innerhalb einer VMware SDDC-Umgebung. Diese APIs ermöglichen Administratoren und Entwicklern die Automatisierung, Verwaltung und Integration der verschiedenen Aspekte des Rechenzentrums, einschließlich Rechen-, Speicher-, Netzwerk- und Verwaltungsdienste.
- **VMware vSphere Storage APIs – Storage Awareness:** VASA ist ein Satz von APIs, der die Integration der Speicher-Arrays mit vCenter für Management und Administration ermöglicht. Die Architektur basiert auf mehreren Komponenten, einschließlich des VASA-Providers, der die Kommunikation zwischen VMware vSphere und den Speichersystemen übernimmt. Bei ONTAP wird der Provider als Teil der ONTAP tools for VMware vSphere implementiert.

- **VMware vSphere Storage APIs – Array-Integration:** VAAI ist ein Satz von APIs, die die Kommunikation zwischen VMware vSphere ESXi-Hosts und den Speichergeräten ermöglichen. Die API umfasst eine Reihe primitiver Operationen, die von den Hosts verwendet werden, um Speicheroperationen auf das Array auszulagern. VAAI kann bei speicherintensiven Aufgaben erhebliche Leistungsverbesserungen bieten.

ONTAP-basierte APIs

- * NetApp ONTAP REST API:* Die ONTAP REST API bietet eine moderne, RESTful-Schnittstelle für die Verwaltung von ONTAP Speichersystemen. Es vereinfacht die Automatisierung von Speicheraufgaben wie Bereitstellung, Überwachung und Konfiguration. Es ermöglicht eine einfache Integration mit VMware vSphere und anderen VMware-Verwaltungstools und ermöglicht automatisierte Speichervorgänge direkt aus VMware-Umgebungen. Es unterstützt eine breite Palette von Vorgängen, von der grundlegenden Speicherverwaltung bis hin zu erweiterten Datenschutz- und Replikationsaufgaben, und ermöglicht so eine skalierbare und flexible Speicherverwaltung.
- * ONTAP -Tools für VMware vSphere:* ONTAP tools for VMware vSphere sind ein Satz von Tools zur Integration von ONTAP und vSphere. Es implementiert die Providerfunktionalität des VASA-API-Frameworks. Zu den ONTAP -Tools gehören außerdem das vCenter-Plug-in, ein Storage Replication Adapter (SRA) für VMware Site Recovery Manager und ein REST-API-Server, mit dem Sie Automatisierungsanwendungen erstellen können.

Zusammenfassung

Zusammenfassend lässt sich sagen, dass Administratoren mit ONTAP APIs die Erstellung und Konfiguration von Datenspeichern in VMware-Umgebungen per Skript durchführen können und so eine schnelle und konsistente Speicherbereitstellung gewährleisten. Darüber hinaus können sie die Erstellung, Planung und Löschung von Snapshots für virtuelle VMware-Maschinen automatisieren und so effiziente Optionen für Datenschutz und Wiederherstellung bieten. SnapMirror -APIs erleichtern die Automatisierung der Einrichtung und Verwaltung von Replikationsbeziehungen und gewährleisten robuste Disaster-Recovery-Lösungen für VMware-Workloads. Administratoren können außerdem Skripte implementieren, um die Speicherleistungsmetriken zu überwachen und beim Überschreiten von Leistungsschwellenwerten Warnmeldungen oder automatisierte Aktionen auszulösen. So wird eine optimale Speicherleistung für VMware-Workloads sichergestellt. Durch die Integration von ONTAP -APIs mit VMware-APIs, wie sie beispielsweise von vSphere und vRealize bereitgestellt werden, können Administratoren eine nahtlose und hochautomatisierte Verwaltungserfahrung erzielen und so die Gesamteffizienz und Zuverlässigkeit ihrer virtualisierten Infrastruktur verbessern.

Erfahren Sie mehr über die Überwachung einer kompletten Infrastruktur mit NetApp Data Infrastructure Insights

NetApp Data Infrastructure Insights (ehemals Cloud Insights) überwacht lokale und Cloud-Systeme und bietet Einblick in Ihre komplette IT-Umgebung, einschließlich VMware vSphere- und ONTAP -Speichersystemen. Es ermöglicht Funktionen wie Leistungsverfolgung, Problemerkennung und Ressourcenoptimierung in Ihren öffentlichen und privaten Umgebungen.

Einführung

Mit Data Infrastructure Insights können Sie alle Ihre Ressourcen, einschließlich Ihrer öffentlichen Clouds und Ihrer privaten Rechenzentren, überwachen, Fehler beheben und optimieren.

Weitere Informationen zu Data Infrastructure Insights finden Sie unter"Dokumentation zu Data Infrastructure

Insights" .

Funktionen zur Data Infrastructure Insights

- Data Infrastructure Insights bietet hybrides Multicloud-Monitoring und verschafft Ihnen so vollständige Transparenz über Infrastruktur und Workloads.
- Datensammler für heterogene Infrastrukturen und Workloads, einschließlich Kubernetes
- Offener Telegraf-Collector und offene APIs für einfache Integration
- Umfassende Alarmierung und Benachrichtigungen
- Maschinelles Lernen für intelligente Erkenntnisse
- Optimieren Sie die Ressourcennutzung
- Integrierte oder anpassbare Dashboards mit erweiterten Filtern zur Minimierung von Anzeigestörungen bei der Beantwortung von Fragen
- Ermitteln Sie den Zustand Ihrer ONTAP Speichervorgänge
- Schützen Sie Ihr wertvollstes Geschäftsgut – Ihre Daten – vor Ransomware oder Datenzerstörungsangriffen

Erfahren Sie mehr über VMs von VMware vSphere bis hin zu ONTAP -Datenspeichern

VMware vSphere-Administratoren können ihre Infrastruktur verbessern, indem sie Workloads auf NetApp ONTAP -Datenspeicher migrieren. ONTAP bietet VM-fähige Snapshots, speichereffiziente Klone und nahtlose vMotion-Vorgänge und unterstützt gleichzeitig Storage Policy-Based Management (SPBM). Ganz gleich, ob Sie von vSAN oder Legacy-Speicher migrieren oder Hybrid-Cloud-Bereitstellungen implementieren: ONTAP bietet verbesserte Leistung und vereinfachte Speichervorgänge für VMware-Umgebungen.

Diese Migration ermöglicht eine nahtlose Integration, verbesserten Datenschutz und größere Flexibilität bei der Verwaltung virtualisierter Umgebungen und gewährleistet einen reibungslosen Übergang mit minimalen Ausfallzeiten.

Anwendungsfälle

Wenn Sie eine Migration auf ONTAP gestützte Datenspeicher in Erwägung ziehen, stehen Ihnen hinsichtlich Quelle und Ziel zahlreiche Migrationsoptionen zur Verfügung.

- Migration von Speichersystemen von Drittanbietern (einschließlich vSAN) zu ONTAP -Datenspeichern.
- Migration von VMs im selben vSphere-Cluster
- Migration von VMs über mehrere vSphere-Cluster
- Migration von VMs über vCenter-Server in derselben SSO-Domäne
- Migration von VMs über vCenter-Server in verschiedenen SSO-Domänen
- Migration von VMs zwischen Rechenzentrumsstandorten
- Migration von Speichersystemen von Drittanbietern (einschließlich vSAN) zu ONTAP -Datenspeichern.
- Migration von VMs in einer Hybrid-Cloud-Umgebung

Weitere Informationen zur Migration von VMware-Workloads zu ONTAP gestützten Datenspeichern finden Sie im"Migrieren Sie VMs zu ONTAP -Datenspeichern" .

Datenschutzlösungen

Erfahren Sie mehr über den Schutz von VMware-Umgebungen mit MetroCluster und SnapMirror Active Sync

Um VMware-Umgebungen vor domänenweiten Ausfällen zu schützen, ist eine erweiterte Geschäftskontinuität unerlässlich. NetApp und VMware bieten Lösungen wie NetApp MetroCluster, SnapMirror Active Sync und VMware vSphere Metro Storage Cluster (vMSC) an, um den Workload-Schutz zu verbessern und eine hohe Verfügbarkeit sicherzustellen.

Einführung

Zusätzlich zu den in die Produkte integrierten Verfügbarkeiten bieten VMware und NetApp erweiterte Konfigurationen, die Workloads, die über Fehlerdomänen wie Racks, Gebäude, Campusgelände oder sogar Städte verteilt sind, zusätzlich schützen.

NetApp MetroCluster

NetApp MetroCluster nutzt die Hochverfügbarkeitsfunktion (HA) von NetApp zum Schutz vor Controller-Ausfällen. MetroCluster umfasst außerdem SyncMirror -Technologie, Cluster Failover on Demand (CFOD), Hardwareredundanz und geografische Trennung für hohe Verfügbarkeit. SyncMirror spiegelt Daten synchron über zwei Plexi: den lokalen Plex, der aktiv Daten bereitstellt, und den Remote-Plex als Standby. Alle MetroCluster -Komponenten wie Controller, Speicher, Kabel, Switches und Adapter verfügen über Hardwareredundanz.

NetApp SnapMirror aktive Synchronisierung

NetApp SnapMirror Active Sync bietet datenspeichergranularen Schutz mit FCP- und iSCSI-SAN-Protokollen und schützt selektiv die Topologie der Workloads mit hoher Priorität. Im Gegensatz zum Active-Standby-MetroCluster bietet es Active-Active-Zugriff auf lokale und Remote-Sites. Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync die symmetrische Aktiv/Aktiv-Funktion und ermöglicht Lese- und Schreib-E/A-Vorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replikation.

VMware vSphere Metro Storage Cluster

VMware vSphere Metro Storage Cluster (vMSC) erweitert VMware HA mit Active-Active-Stretched Storage. Diese zertifizierte Konfiguration schützt VMs und Container vor Ausfällen. Dies wird durch die Verwendung von Stretched-Storage-Konzepten zusammen mit Clustern von vSphere-Hosts erreicht. Diese Hosts sind auf verschiedene Fehlerdomänen verteilt. Die Active-Sync-Speichertechnologien NetApp MetroCluster und SnapMirror werden verwendet, um Schutz und unterstützte Speicherangebote bereitzustellen. Durch die Nutzung von vMSC mit einer zertifizierten NetApp -Lösung werden robuste und belastbare IT-Vorgänge über Fehlerdomänen hinweg gewährleistet.

Ausführliche Informationen finden Sie im "vSphere Metro Storage Cluster mit ONTAP" .

Erfahren Sie mehr über die Minimierung von Sicherheits- und Ransomware-Risiken für VMware-Workloads

ONTAP verbessert die Sicherheit und den Ransomware-Schutz in VMware-Umgebungen durch Verschlüsselung, Snapshots und erweiterte Zugriffskontrollen und ergänzt die Sicherheitsfunktionen von VMware zum Schutz von Daten.

Einführung

Durch die Nutzung der erweiterten Funktionen von NetApp ONTAP in VMware-Umgebungen können Unternehmen die Integrität, Verfügbarkeit und Sicherheit ihrer Daten gewährleisten.

Nachfolgend erfahren Sie ausführlicher, wie diese Technologien zusammenarbeiten, um **Sicherheits-** und **Backup-Vorteile** zu bieten.

Sicherheit und Ransomware

Sicherheit ist in virtualisierten Umgebungen ein vorrangiges Anliegen und NetApp ONTAP bietet robuste Funktionen zur Verbesserung der Sicherheit innerhalb von VMware-Infrastrukturen. ONTAP bietet Verschlüsselung für gespeicherte und übertragene Daten und stellt so sicher, dass vertrauliche Informationen vor unbefugtem Zugriff geschützt sind. Verschlüsselungsschlüssel werden sicher verwaltet und ONTAP unterstützt sowohl software- als auch hardwarebasierte Verschlüsselungslösungen. Durch die Integration mit den Sicherheitstools von VMware, wie den integrierten Sicherheitsfunktionen von vSphere und Sicherheitslösungen von Drittanbietern, trägt ONTAP zur Schaffung einer sicheren und konformen Umgebung bei.

Ransomware-Abwehr

Ransomware-Angriffe stellen eine erhebliche Bedrohung für Unternehmen dar und die Kombination aus VMware und ONTAP bietet einen starken Abwehrmechanismus. Die Snapshot-Technologie von ONTAP ermöglicht die Erstellung unveränderlicher Snapshots, die von Ransomware nicht verändert oder gelöscht werden können. Im Falle eines Angriffs können diese Snapshots verwendet werden, um betroffene VMs und Datenspeicher schnell in den Zustand vor dem Angriff zurückzusetzen und so Ausfallzeiten und Datenverluste zu minimieren. Darüber hinaus ermöglicht die Integration von ONTAP mit SIEM-Systemen (Security Information and Event Management) eine proaktive Überwachung und Warnung vor verdächtigen Aktivitäten. ONTAP unterstützt außerdem die Multi-Faktor-Authentifizierung (MFA) und die rollenbasierte Zugriffskontrolle (RBAC), um die Sicherheit weiter zu verbessern.

Ransomware-Wiederherstellungsgarantie

Die NetApp Ransomware-Garantie bietet Unternehmen eine robuste und zuverlässige Lösung zum Schutz vor Ransomware-Angriffen. Durch die Nutzung der erweiterten Funktionen von NetApp ONTAP können Unternehmen die Sicherheit und Verfügbarkeit ihrer Daten gewährleisten. Die Garantie bietet die Gewissheit, dass im Falle eines Ransomware-Angriffs die Daten schnell und effektiv wiederhergestellt werden können, wodurch Ausfallzeiten, Datenverlust und finanzielle Auswirkungen minimiert werden. Dieses Engagement für Datensicherheit und Ausfallsicherheit macht NetApp zum idealen Partner für Unternehmen, die ihre kritischen Vermögenswerte vor sich entwickelnden Cyber-Bedrohungen schützen möchten.

Erweiterte Sicherheitsfunktionen

ONTAP umfasst erweiterte Sicherheitsfunktionen wie sichere Mandantenfähigkeit, die Daten und Ressourcen in Umgebungen mit mehreren Mandanten isoliert, und Compliance-Auditing, das den Zugriff auf vertrauliche Daten verfolgt und protokolliert. Diese Funktionen gewährleisten die Sicherheit der Daten und ermöglichen es Unternehmen, die Einhaltung branchenspezifischer Vorschriften und Standards nachzuweisen.

Zusammenfassung

Die Integration der Sicherheitsfunktionen von ONTAP – wie Verschlüsselung, unveränderliche Snapshots und erweiterte Zugriffskontrollen – mit den Tools von VMware bietet einen robusten Schutz vor Cyberbedrohungen, einschließlich Ransomware. Die Unterstützung von ONTAP für sichere Mandantenfähigkeit und Compliance-Audits gewährleistet Datenschutz und Einhaltung gesetzlicher Vorschriften.

Gemeinsam bieten NetApp ONTAP und VMware eine umfassende Lösung zur Sicherung virtualisierter Umgebungen, die es Unternehmen ermöglicht, Daten zu schützen, Ausfallzeiten zu minimieren und die Geschäftskontinuität aufrechtzuerhalten. Durch die Implementierung dieser Technologien können Unternehmen moderne IT-Herausforderungen bewältigen und kritische Ressourcen vor neuen Sicherheitsbedrohungen schützen.

Autonomer Ransomware-Schutz für NFS und VMFS

Entdecken Sie, wie Autonomous Ransomware Protection (ARP) von NetApp ONTAP maschinelles Lernen nutzt, um NFS- und VMFS-Datenspeicher in VMware-Umgebungen zu sichern. Es bietet eine frühzeitige Bedrohungserkennung, manipulationssichere Snapshots und eine schnelle Wiederherstellung, um die Datenausfallsicherheit bei virtualisierten und Cloud-Workloads zu stärken.

Überblick

Ransomware-Bedrohungen entwickeln sich schnell weiter und werden immer ausgefeilter und störender. Herkömmliche Sicherheitsmaßnahmen können kritische Datenbestände oft nicht schützen. NetApp ONTAP -Speicher bietet integrierte Sicherheitsfunktionen, die Daten proaktiv schützen. Wenn eine Sicherheitsverletzung auftritt, liefert ONTAP Echtzeitwarnungen und schnelle Wiederherstellungsoptionen, um Ausfallzeiten zu reduzieren und Datenverluste zu begrenzen. ONTAP ermöglicht es Kunden, ihre Daten und Anwendungen zu schützen, wiederherzustellen und zu verschieben und so die Widerstandsfähigkeit gegen Ransomware zu stärken.

Anwendungsfall – Schützen Sie VMware-VMs und deren Dateien

Die frühzeitige Erkennung von Ransomware in VMware-Umgebungen ist entscheidend, um ihre Verbreitung zu stoppen und Ausfallzeiten zu minimieren. Eine effektive Strategie nutzt mehrere Schutzebenen für ESXi-Hosts und virtuelle Gastmaschinen. Während viele Sicherheitskontrollen zum Aufbau einer starken Verteidigung beitragen, fügt NetApp ONTAP wichtige Sicherheitsvorkehrungen auf Speicherebene hinzu, die den Schutz weiter verstärken.

Zu den wichtigsten ONTAP -Funktionen gehören die Snapshot-Technologie für zeitpunktbezogene Wiederherstellung, Autonomous Ransomware Protection (ARP) auf Basis von integriertem maschinellem Lernen, Multi-Admin-Verifizierung und manipulationssichere Snapshots, die die Datenintegrität bewahren. Diese Funktionen arbeiten zusammen, um die Widerstandsfähigkeit gegen Ransomware zu verbessern und bei Bedarf eine schnelle Wiederherstellung zu ermöglichen.

Die Sicherung von vSphere-Umgebungen und virtuellen Gastmaschinen erfordert einen umfassenden Ansatz. Zu den wichtigsten Maßnahmen zählen die Netzwerksegmentierung, der Einsatz von EDR/XDR/SIEM-Lösungen zur Endpunktüberwachung, die zeitnahe Anwendung von Sicherheitsupdates und die Einhaltung etablierter Härtungsrichtlinien. Auf jeder VM läuft normalerweise ein Standardbetriebssystem. Daher ist es wichtig, im Rahmen einer mehrschichtigen Ransomware-Abwehrstrategie Anti-Malware-Lösungen auf Unternehmensniveau zu installieren und regelmäßig zu aktualisieren.

So hilft ONTAP

ONTAP stärkt den Datenschutz mit mehreren Verteidigungsebenen. Zu den wichtigsten Funktionen gehören Snapshots, Autonomous Ransomware Protection (ARP), manipulationssichere Snapshots, Multi-Admin-Verifizierung und mehr. Dieses Dokument konzentriert sich auf die Verbesserungen an ARP, die in Version 9.17.1 eingeführt wurden.

Sie können ARP auf NAS- oder SAN-Volumes aktivieren, die VMware-Datenspeicher unterstützen. ARP nutzt das integrierte maschinelle Lernen von ONTAP, um Arbeitslastmuster und Datenentropie zu überwachen, Anzeichen von Ransomware-Aktivitäten automatisch zu erkennen und eine intelligente, proaktive Sicherheitsebene bereitzustellen. Konfigurieren Sie ARP pro Volume mithilfe der CLI oder der System Manager-Schnittstelle von ONTAP.

Entwicklung der ARP-Funktionen

Ab ONTAP Version 9.10.1 ist ARP für ein vorhandenes oder ein neues Volume verfügbar. In ONTAP Version 9.16.1 können Sie ARP mithilfe von System Manager oder der CLI aktivieren. Der ARP/AI-Schutz wird sofort aktiv, ohne dass eine Lernphase erforderlich ist. In Version 9.17.1 unterstützt ARP SAN-Volumes. Wenn Sie ARP auf einem SAN-Volume aktivieren, überwacht ARP/AI während eines Evaluierungszeitraums kontinuierlich die Daten, um die Eignung der Arbeitslast zu ermitteln und den optimalen Verschlüsselungsschwellenwert für die Erkennung festzulegen.

ARP ist in ONTAP integriert und bietet integrierte Steuerung und Koordination mit anderen ONTAP Funktionen. ARP arbeitet in Echtzeit, verarbeitet Daten beim Schreiben oder Lesen und erkennt und reagiert schnell auf potenzielle Ransomware-Angriffe. Es erstellt in regelmäßigen Abständen neben geplanten Snapshots auch gesperrte Snapshots und verwaltet die Snapshot-Aufbewahrung intelligent, indem es sie wiederverwendet, wenn keine Anomalien erkannt werden. Wenn ARP verdächtige Aktivitäten erkennt, speichert es einen vor dem Angriff erstellten Snapshot für einen längeren Zeitraum, um einen zuverlässigen Wiederherstellungspunkt zu gewährleisten.

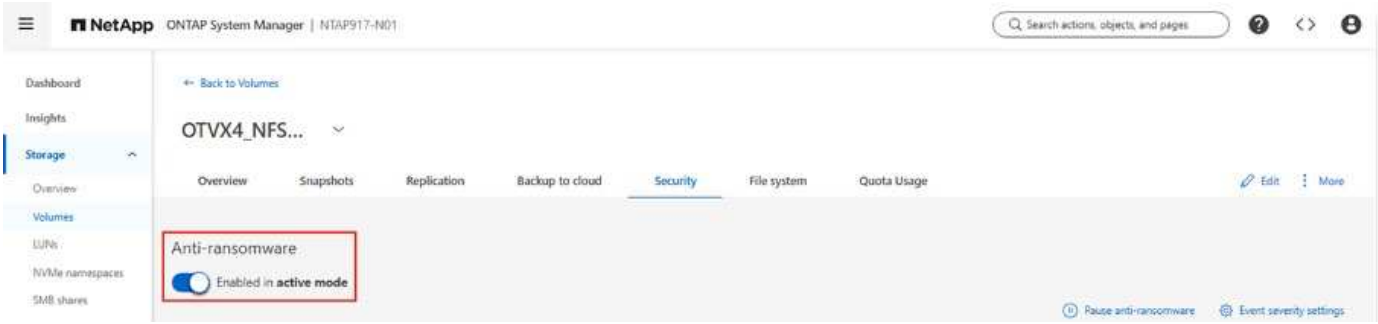
Weitere Einzelheiten finden Sie unter"Was ARP erkennt" .

ARP-Support ist in der ONTAP ONE-Lizenz enthalten.

Konfigurieren Sie ARP auf NAS-Volumes und simulieren Sie einen Angriff auf eine VM

Erfahren Sie, wie Sie NetApp ONTAP Autonomous Ransomware Protection (ARP) auf NAS- und SAN-Volumes aktivieren, die für VMware-Datenspeicher verwendet werden, und simulieren Sie Ransomware-Angriffe, um zu sehen, wie ARP Bedrohungen erkennt und eine schnelle Wiederherstellung ermöglicht.

Wenn ARP auf einem NAS-Volume mithilfe von System Manager oder der CLI aktiviert wird, ist der ARP/AI-Schutz sofort aktiviert und aktiv. ist keine Einarbeitungszeit erforderlich.

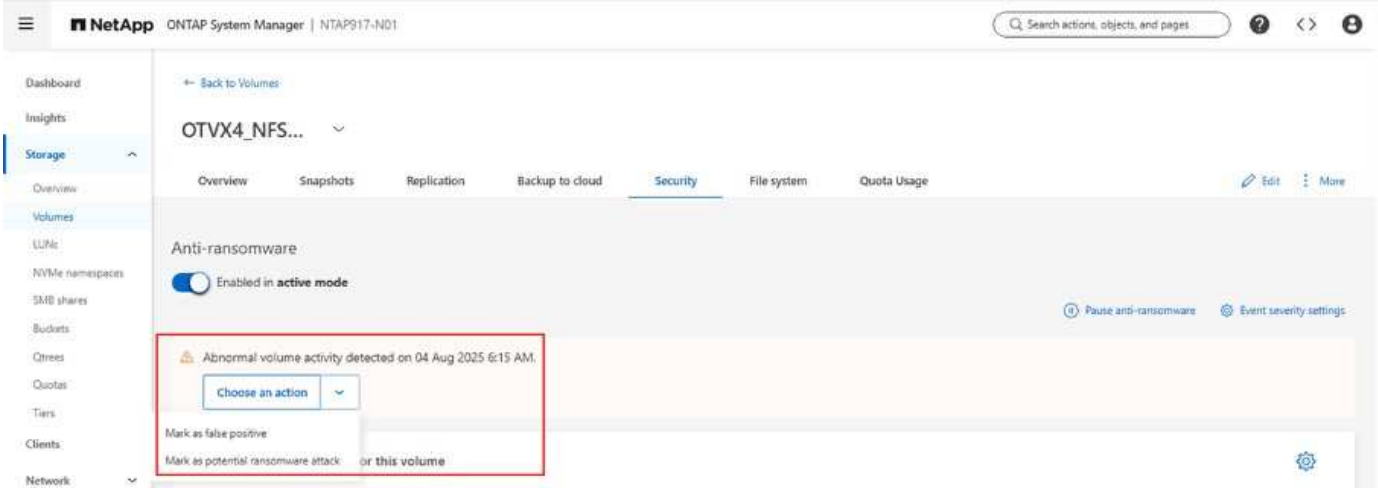


In diesem Beispiel wird die Simulation mithilfe eines Skripts zum Ändern der Dateien oder durch Ändern der

Dateierweiterung ausgelöst, um einen Angriff innerhalb einer VM zu simulieren, die sich auf dem NFS-Volume befindet, das als Datenspeicher an vCenter angeschlossen ist.

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

Wie unten gezeigt, hat ARP die abnormale Aktivität erkannt.

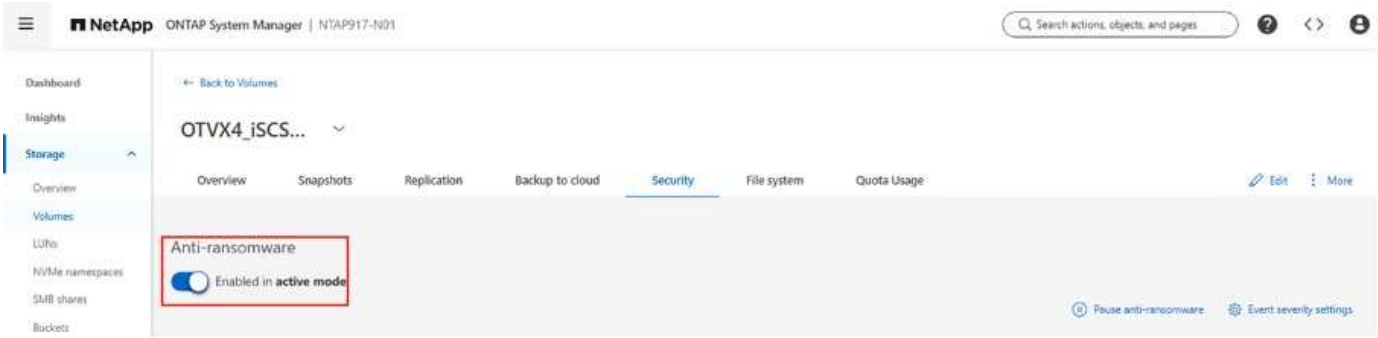


ARP erkennt den Angriff frühzeitig und ermöglicht die Datenwiederherstellung aus Snapshots, die kurz vor dem Angriffszeitpunkt erstellt wurden. Verwenden Sie zum Rollback den periodischen ARP-Snapshot, der vor dem Auslösen des Vorfalls generiert wurde. Und der Screenshot unten zeigt die erstellten Snapshots:

Ausführliche Anleitungen zum Aktivieren von ARP auf NFS-Volumes, die als Datenspeicher dienen und im Falle eines Angriffs wiederhergestellt werden, finden Sie unter"ARP für NFS-Speicher" .

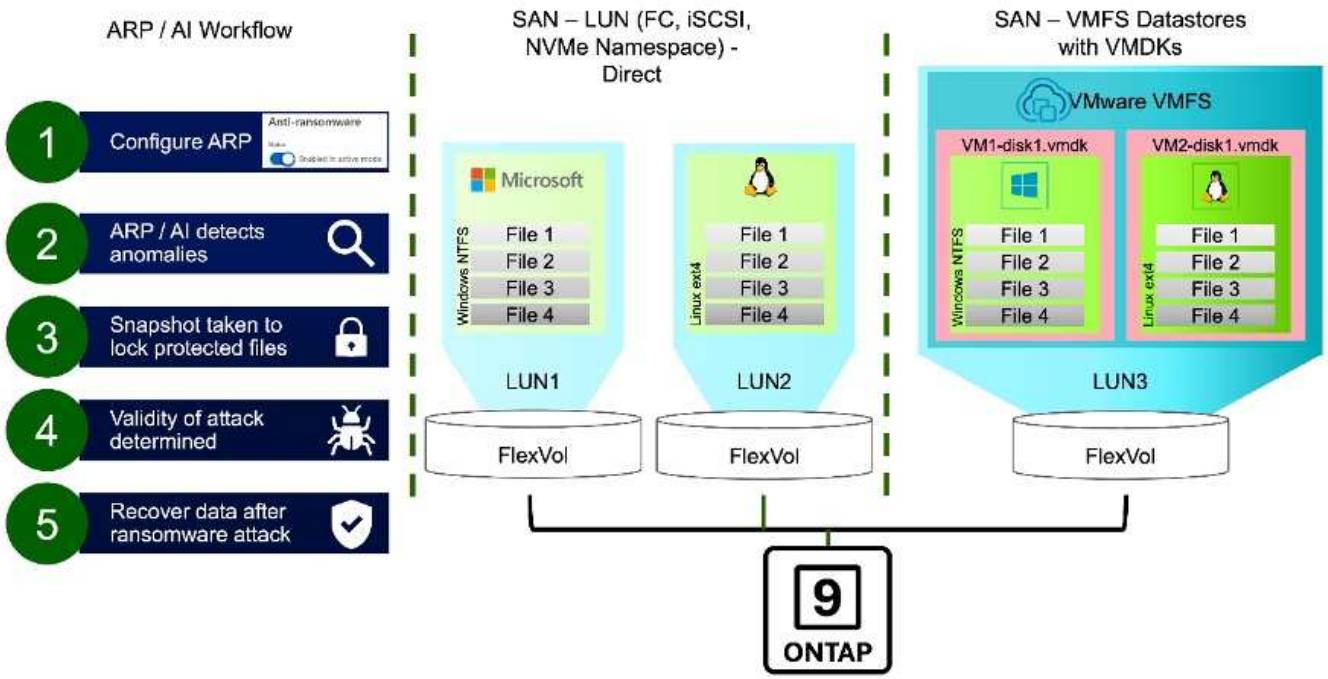
Konfigurieren Sie ARP auf SAN-Volumes und simulieren Sie einen Angriff auf eine VM

Wenn ARP auf einem SAN-Volume aktiviert ist, beginnt es mit einer Evaluierungsphase, ähnlich dem Lernmodus, der in NAS-Umgebungen verwendet wird, bevor automatisch in die aktive Erkennung übergegangen wird.



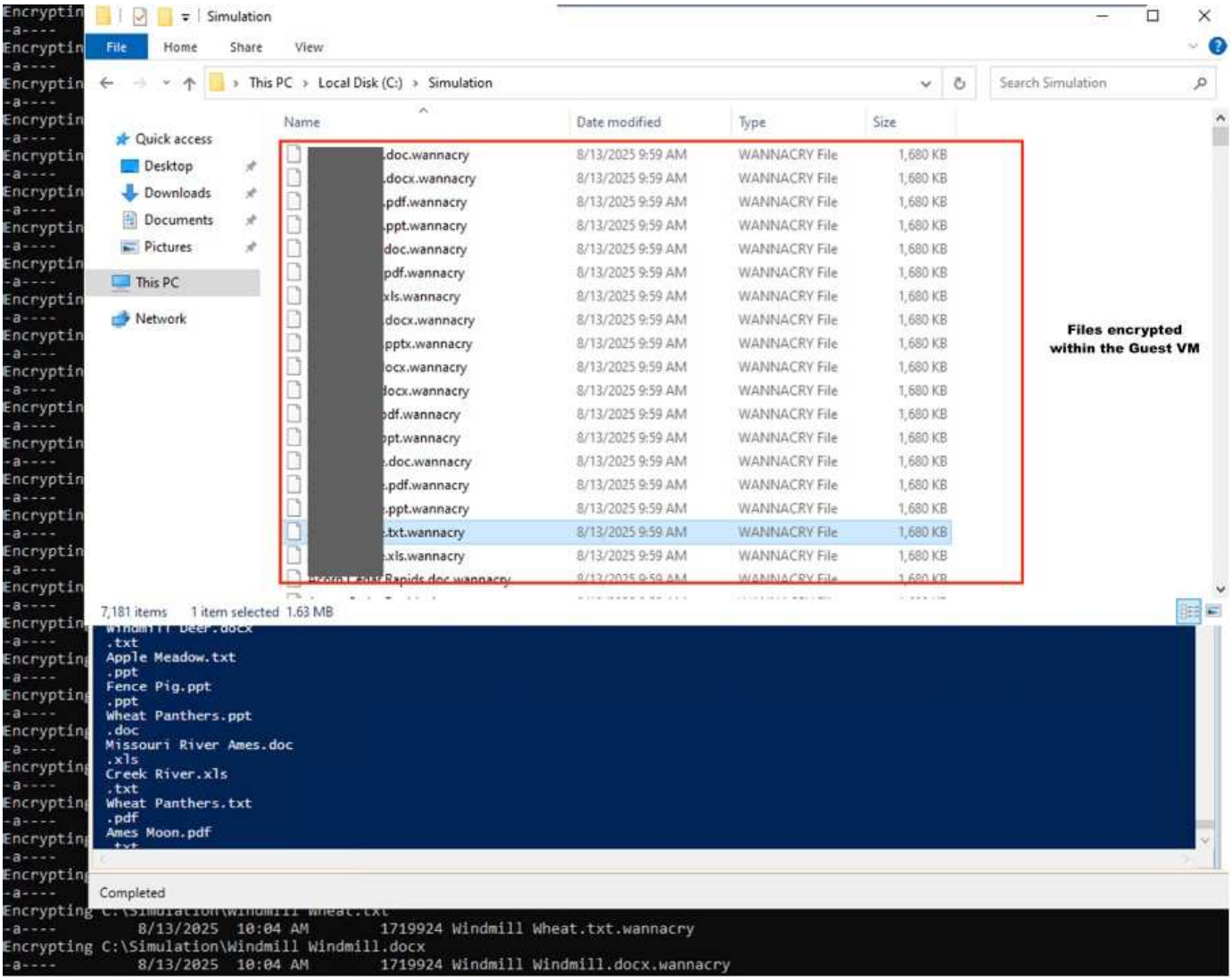
ARP leitet eine zwei- bis vierwöchige Evaluierungsphase mit einem Schwellenwert von 75 % ein, um eine Basislinie für das Verschlüsselungsverhalten festzulegen. Der Fortschritt dieser Phase kann überwacht werden mit dem `security anti-ransomware volume show` Befehl, indem Sie den **Blockgeräterkennungsstatus** überprüfen. Nach Abschluss der Auswertung bestätigt der Status **Active_suitable_workload**, dass die beobachteten Entropieniveaus für eine laufende Überwachung geeignet sind. Basierend auf den gesammelten Daten passt ARP seinen adaptiven Schwellenwert automatisch an, um eine genaue und reaktionsschnelle Bedrohungserkennung zu gewährleisten. Je nach Bedarf kann das Snap-Erstellungsintervall vom Standardwert 4h auf 1h geändert werden. Führen Sie diese Änderung mit Vorsicht durch.

Ab ONTAP 9.17.1 werden in regelmäßigen Abständen ARP-Snapshots für NAS- und SAN-Volumes generiert.

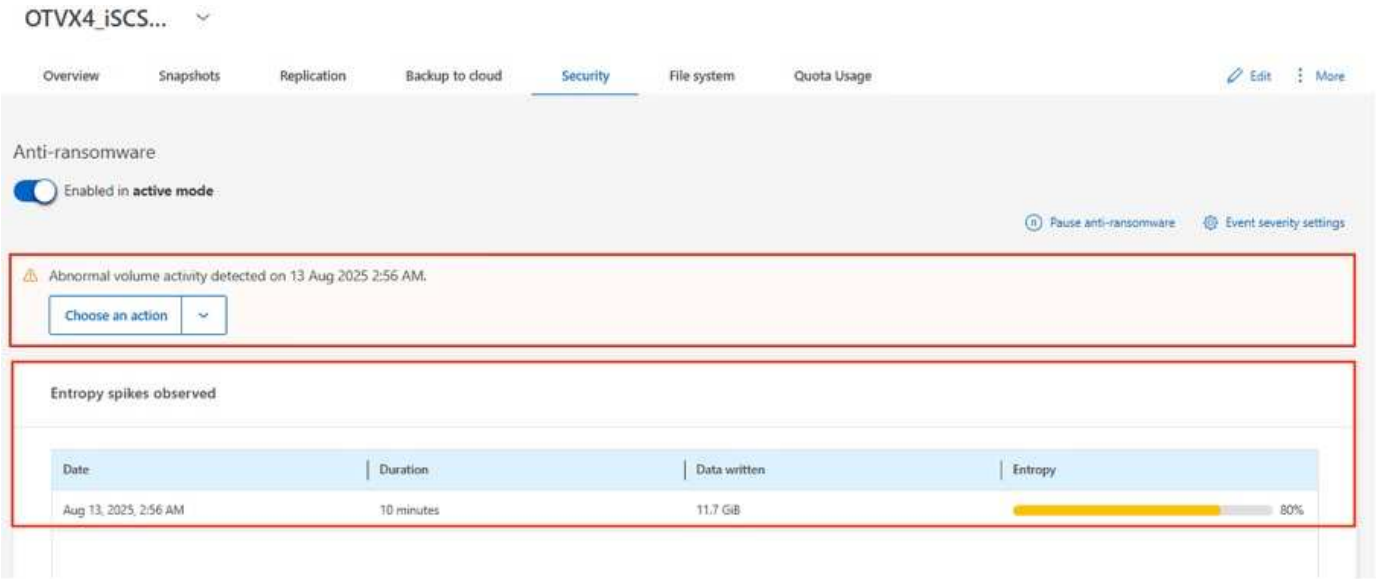


Ausführliche Informationen finden Sie unter"SAN-Umgebungen und Modustypen"

Es ist Zeit, einen Angriff zu simulieren. Zu Demonstrationszwecken werden Dateien innerhalb einer virtuellen Maschine verschlüsselt, die auf einem ISCSI-basierten Datenspeicher läuft. Es werden fast 7.000 Dateien generiert, die leider von Ransomware-Angriffen betroffen sind.

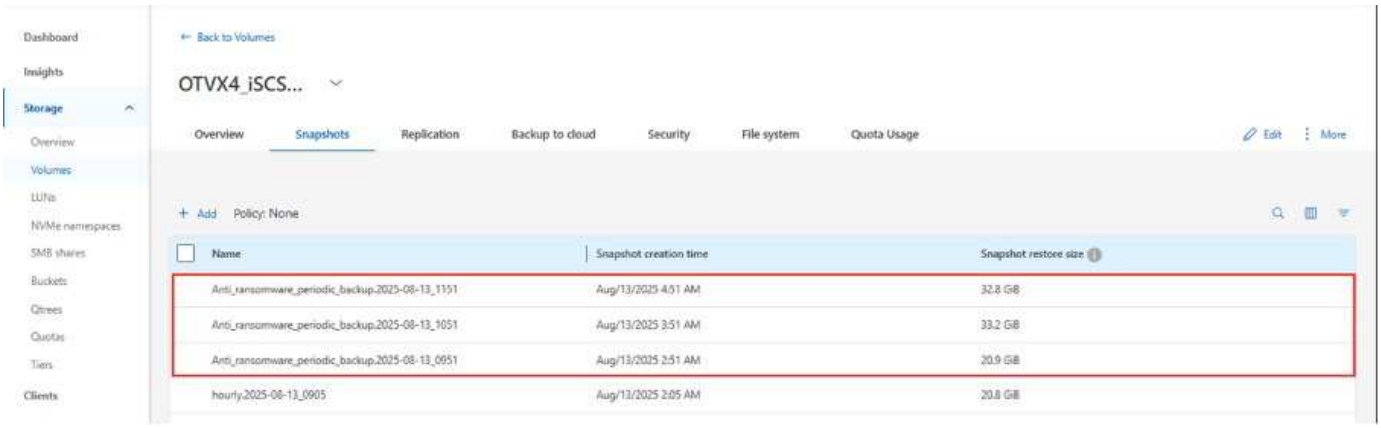


Innerhalb von 10 Minuten wurde auf dem Datenträger aufgrund der hohen Entropiedaten eine anormale Aktivität erkannt und ARP generiert eine Bedrohungswarnung, da es eine Entropieanomalie innerhalb der VM erkannt hat.

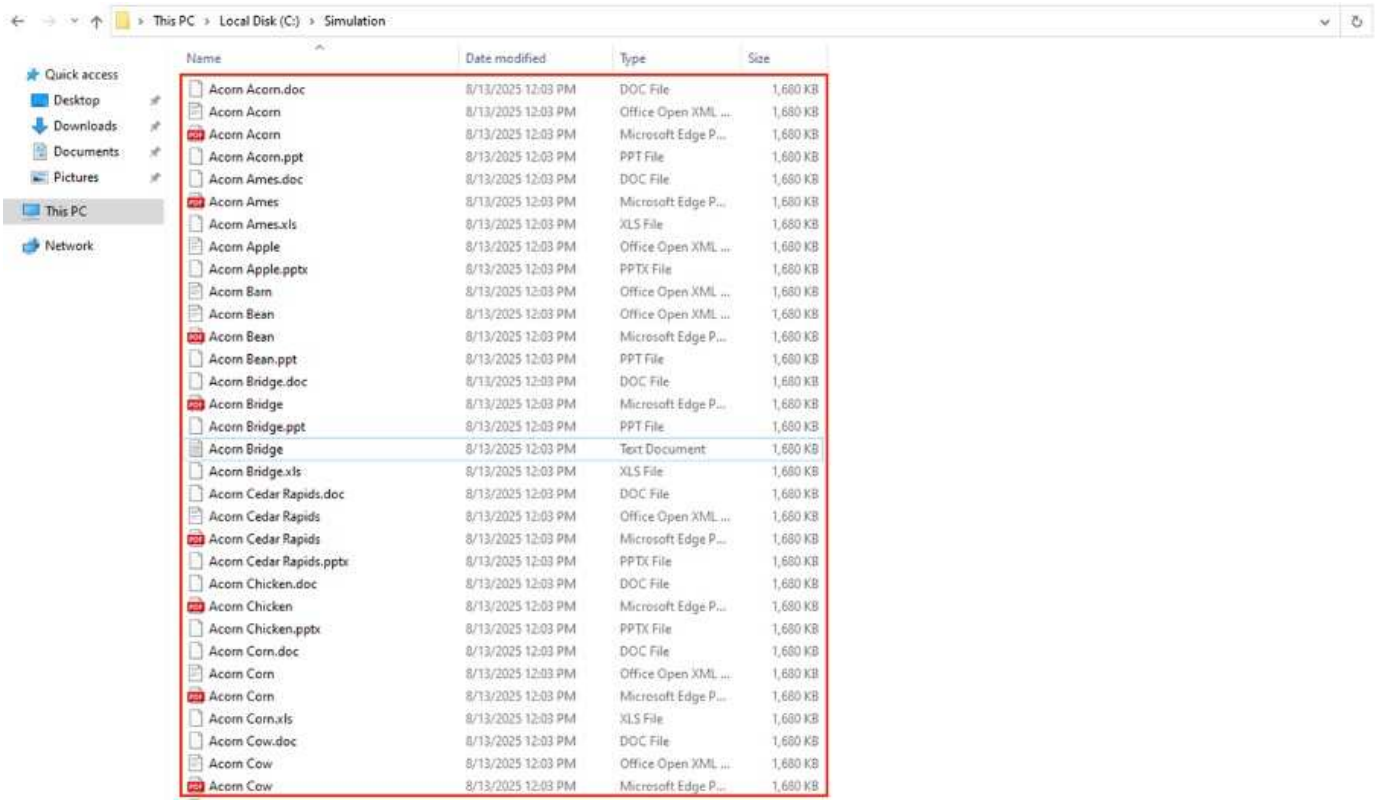


Wiederherstellen der VM und ihrer Daten nach einem Ransomware-Angriff

Sobald der Angriff anhand der oben beschriebenen Schritte bestätigt wurde, verwenden Sie einen der ARP-Snapshots oder einen anderen Snapshot des Volumes, um die Daten wiederherzustellen.



Nach der Wiederherstellung sind alle Dateien wiederhergestellt.



Ausführliche Anleitungen finden Sie unter"Wiederherstellen von Daten aus einem ARP-Snapshot nach einem Ransomware-Angriff"

ONTAP als Verteidigungsschicht für VMware und darüber hinaus

Mit nur wenigen Klicks können Unternehmen ihre Datenschutzstrategie nahtlos verbessern. ONTAP basiert auf fortschrittlichen, auf maschinellem Lernen basierenden Erkennungsmechanismen und führt eine leistungsstarke Verteidigungsebene in VMware-Umgebungen ein. Dieser intelligente Schutz erkennt nicht nur Bedrohungen frühzeitig, sondern hilft auch, potenzielle Schäden zu mindern, bevor sie eskalieren.

Dieser Anwendungsfall gilt nicht nur für VMware. Sie können dieselben Prinzipien auf jede NAS- oder SAN-

basierte Anwendung erweitern, um eine mehrschichtige Sicherheitsarchitektur aufzubauen. Angreifer sind gezwungen, sich durch mehrere befestigte Ebenen zu navigieren, wodurch das Risiko erfolgreicher Einbrüche erheblich reduziert wird.

ONTAP schützt nicht nur Daten – es versetzt Unternehmen auch in die Lage, angesichts sich entwickelnder Bedrohungen widerstandsfähig zu bleiben.

Backup- und Disaster-Recovery-Lösungen

Erfahren Sie mehr über die Sicherung und Wiederherstellung virtueller Maschinen mit dem SnapCenter -Plug-in für VMware vSphere

Das SnapCenter Plug-in for VMware vSphere ermöglicht schnelle, VM-konsistente Sicherungs- und Wiederherstellungsvorgänge für VMs, Datenspeicher und VMDK-Dateien. Dieses VMware-Plug-in lässt sich in SnapCenter Server integrieren, um anwendungsbasierte Sicherung und Wiederherstellung für anwendungsspezifische Plug-ins von SnapCenter zu unterstützen.

Dokumentationsressourcen

Ausführliche Informationen finden Sie in den folgenden Dokumentationsressourcen.

- "SnapCenter Plug-in for VMware vSphere Dokumentation"

Lösungsressourcen

Beachten Sie die folgende 3-2-1-Backup-Lösung mit SnapCenter Plug-in for VMware vSphere und BlueXP backup and recovery für VMs.

Technischer Bericht:"3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs"

Tech ONTAP Blog:"3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs"

Videoressourcen

SnapCenter Plug-in for VMware vSphere – Lösungsvoraussetzungen

SnapCenter Plug-in for VMware vSphere – Bereitstellung

SnapCenter Plug-in for VMware vSphere – Sicherungsworkflow

SnapCenter Plug-in for VMware vSphere – Wiederherstellungs-Workflow

SnapCenter – SQL-Wiederherstellungs-Workflow

Erfahren Sie mehr über die Notfallwiederherstellung virtueller Maschinen mit BlueXP disaster recovery

BlueXP disaster recovery automatisiert die Replikation und Wiederherstellung virtueller VMware-Maschinen mithilfe von ONTAP Speicher. Es unterstützt die Wiederherstellung

von der lokalen Einrichtung zu VMware Cloud auf AWS mit Amazon FSx for NetApp ONTAP oder einer anderen lokalen VMware-Umgebung.

Einführung

Ein erfolgreicher Plan und eine Kombination von Technologien gewährleisten den Schutz kritischer Daten, Anwendungen und VMs. Die Herausforderung bei DR besteht darin, das angemessene Schutzniveau und die damit verbundenen Kosten zu bestimmen.

ONTAP -Arrays bieten integrierte Replikation zum Übertragen von Volume-Daten und damit der virtuellen Maschinen, die sich auf den angegebenen Datastore-LUNs befinden, von einem Standort zum anderen. BlueXP DRaaS lässt sich in vSphere integrieren und automatisiert den gesamten Workflow für nahtloses Failover und Failback im Katastrophenfall.

Weitere Informationen zu BlueXP DRaaS finden Sie unter"Übersicht über BlueXP DRaaS" .

Überlegungen

Der zeitaufwändigste Teil eines DR-Failovers in einer VMware vSphere-Umgebung ist die Ausführung der Schritte, die zum Inventarisieren, Registrieren, Neukonfigurieren und Einschalten der VMs am DR-Standort erforderlich sind. Eine ideale Lösung hat sowohl einen niedrigen RPO (gemessen in Minuten) als auch einen niedrigen RTO (gemessen in Minuten bis Stunden). Ein Faktor, der bei einer DR-Lösung oft übersehen wird, ist die Möglichkeit, die DR-Lösung in regelmäßigen Abständen effizient zu testen.

Berücksichtigen Sie beim Entwerfen einer DR-Lösung die folgenden Faktoren:

- Das Wiederherstellungszeitziel (RTO). Die RTO gibt an, wie schnell sich ein Unternehmen von einem Desaster erholen kann, oder genauer gesagt, wie lange es dauert, den Wiederherstellungsprozess auszuführen, um die Geschäftsdienste wieder verfügbar zu machen.
- Das Wiederherstellungspunktziel (RPO). Das RPO gibt an, wie alt die wiederhergestellten Daten nach ihrer Bereitstellung im Verhältnis zum Zeitpunkt des Katastrophenfalls sind.
- Skalierbarkeit und Anpassungsfähigkeit. Zu diesem Faktor gehört die Möglichkeit, die Speicherressourcen bei steigender Nachfrage schrittweise zu erweitern.

Weitere technische Informationen zu den verfügbaren Lösungen finden Sie unter:

- "DR mit BlueXP DRaaS für NFS-Datenspeicher"
- "DR mit BlueXP DRaaS für VMFS-Datenspeicher"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.