Get started

NetApp virtualization solutions

NetApp
August 25, 2025

Table of Contents

Get started

Core concepts

Learn about ONTAP for VMware vSphere

NetApp ONTAP is a leading storage solution for VMware vSphere, offering nearly two decades of reliable performance for datastore and guest-connected storage use cases. ONTAP supports SAN and NAS protocols, allows for independent scaling of storage and compute resources, and offloads storage tasks from hosts. Benefits include strong data protection, high availability, and advanced business continuity features such as SnapMirror and MetroCluster.

Introduction

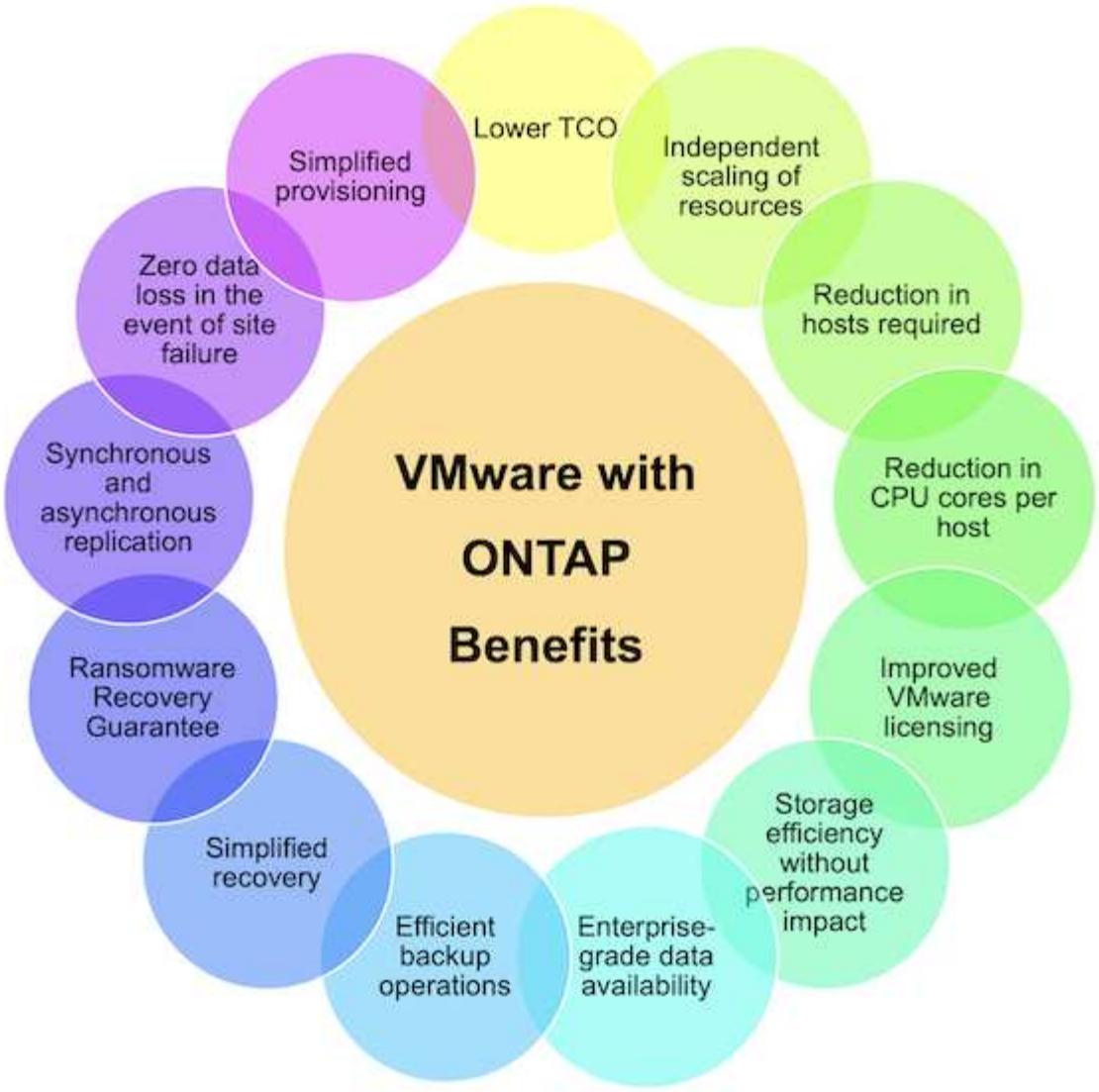
NetApp continues to add innovative capabilities to simplify storage management while reducing costs and increasing confidence in a consolidated, VMware-based virtual infrastructure that is cloud-ready. This collection of solutions introduces ONTAP offerings for VMware vSphere Foundation and VMware Cloud Foundation, including the latest product information and best practices, to streamline deployment, reduce risk, and simplify management.

For more information on using ONTAP with VMware vSphere, refer to VMware vSphere with ONTAP.

Why ONTAP for VMware

There are many reasons why tens of thousands of customers have selected ONTAP as their storage solution for vSphere, such as a unified storage system supporting both SAN and NAS protocols, robust data protection capabilities using space-efficient snapshots and a wealth of tools to help you manage application data. Using a storage system separate from the hypervisor allows you to offload many functions and maximize your investment in vSphere host systems. This approach not only makes sure your host resources are focused on application workloads, but it also avoids random performance effects on applications from storage operations.

Using ONTAP together with vSphere is a great combination that lets you reduce host hardware and VMware software expenses. You can also protect your data at lower cost with consistent high performance. Because virtualized workloads are mobile, you can explore different approaches using Storage vMotion to move VMs across VMFS, NFS, or vVols datastores, all on the same storage system.



Here are key benefits for NetApp and VMware customers:

- **Flexibility on day 1 and as you scale.** The need to grow can arise for a variety of reasons with any architecture. Whether performance or capacity needs evolve, or as new host are added and network or fabric considerations arise, it is critical to choose a storage platform that allows for independent scaling of resources.

  With ONTAP, you can start with the capacity required, grow as needed and take advantage of tiering all without having to add additional compute hosts. Additionally, a single ONTAP cluster can be used with multiple workload domains and avoids the creation of storage islands. These benefits yield significant cost savings for organization.

- **Offload storage tasks to ONTAP.** With typical HCI environments, the host platform is responsible for compute tasks, storage operations and any network optimization on the client side. For example, CPU overhead needs to be considered when determining the hardware requirements of the compute nodes. Often difficult to preemptively scope, this overhead is commonly accepted as 10-15% and is dependent on the I/O profile of the workloads. Additionally, it is important to consider memory consumption. Memory overhead is mandatory and shouldn't be compromised to maintain performance. Hosts can offset this by taking advantage of RDMA-capable NICs, improving network transfer efficiency, at additional costs. Finally, with an HCI platform, storage functions such as storage efficiency, RAID and failure tolerances, and

encryption are handled by the hosts.

Customers can mitigate any of these detrimental impacts on host CPU resources by leveraging ONTAP. This strategy enables hosts to focus on compute tasks while allowing ONTAP to manage the CPU-intensive storage operations. This strategy enhances overall performance by optimizing storage efficiency, encryption, snapshots, and more, all while reducing the total cost of ownership. By not only boosting host performance and decreasing the number of hosts needed to deliver the same workload, it also reduces the number of cores required per host, leading to further cost savings. These savings further extend to energy efficiency savings, reduced cooling requirements, optimized license costs and more; all by offloading CPU-intensive storge tasks to ONTAP and relying less on hosts to handle everything.

- **Storage Efficiency** Although NetApp was the first to deliver deduplication for production workloads, this innovation wasn't the first or last one in this area. It started with snapshots, a space-efficient data protection mechanism with no performance effect, along with FlexClone technology to instantly make read/write copies of VMs for production and backup use. NetApp went on to deliver inline capabilities, including deduplication, compression, and zero-block deduplication, to squeeze out the most storage from expensive SSDs. Most recently, ONTAP added the ability to pack smaller I/O operations and files into a disk block using compaction. The combination of these capabilities has resulted in customers seeing savings of up to 5:1 for VSI and up to 30:1 for VDI.
- **Enterprise-grade data availability.** The protection of data is paramount for any IT organization. Planning for workload fault tolerances requires careful consideration to ensure an adequate number of nodes are available when hosts are responsible for storage operations. As the number of faults tolerated increases, as does the need for additional hosts and the amount of storage provisioned to accommodate the required VM storage capacity.

  ONTAP's comprehensive availability features ensure that data is always accessible, secure, and resilient, making it a reliable choice for VMware deployments of all sizes. Leveraging shared storage in VMware environments facilitates the deployment of smaller vSphere clusters, streamlining the setup process and enabling storage sharing across clusters with enhanced fault tolerance.

  Key ONTAP availability features include:

  - High Availability (HA) Architecture: ONTAP supports a high-availability architecture that includes a clustered deployment model.
  - Automatic Failover and Failback: In the event of hardware or software failures, ONTAP allows for automatic failover to a standby storage node. Once the issue is resolved, failback can be performed to restore the original configuration, minimizing downtime.
  - Built in data protection: ONTAP includes built-in data protection features such as RAID-DP and RAID-TEC, which provide enhanced protection against disk failures and ensure data integrity and availability.
- **Efficient backup and recovery operations.** In addition to protecting data in the event of various faults, we must plan to backup VMs and workloads as part of regular IT operations. Snapshots capture the state of a VM at a specific point in time, including the VM's disk, memory, and settings. This allows an administrator to revert the VM to a previous state if something goes wrong, such as a failed update, configuration change or falling victim to a ransomware or virus attack. The storage consumed by snapshots should be taken into account when designing a balanced solution for VMware environments.

  While snapshots are an important tool, an overreliance on VMware based snapshots raises concerns with respect to frequency and retention policies. Additionally, having too many VMware based snapshots can downgrade performance. It is important to consider alternative such as NetApp snapshot copies and SnapCenter Plug-in for VMware vSphere. SnapCenter leverages snapshot copies, which are read-only, point-in-time images of a volume that initially share disk blocks with the active file system, requiring no additional space and minimal storage. These snapshots have negligible performance overhead, capturing only changes since the last snapshot. The SnapCenter Plug-in for VMware vSphere (SCV) utilizes these

snapshots to deliver efficient, crash-consistent backups and restores for VMs, Datastores, and VMDKs. These operations are integrated seamlessly and without performance impact within a vCenter environment. Additionally, ONTAP enables the offloading of snapshots to object storage for long-term retention.

- **Wholistic business continuity capabilities.** Beyond standard fault tolerance, backup and recovery, an organization must plan for various scenarios such as disasters, ransomware attacks, and data center site migrations. With host-based storage, addressing these challenges typically involves relying on a range of third-party solutions to effectively mitigate disasters and ensure business continuity. Furthermore, for scenarios that are network intensive, insufficiently sizing the networking and storage devices can lead to significant performance impacts.

  Building on its availability features and backup and recovery capabilities, ONTAP is an integral component of a comprehensive business continuity strategy for VMware environments. Organizations need VMs and workloads to be seamlessly available during both normal and maintenance operations, safeguarded with robust protection and recovery capabilities, and capable of leveraging space-efficient and cost-effective disaster recovery solutions.

  Key ONTAP business continuity features include:

  - Data Replication with SnapMirror: Taking advantage of snapshot copies, SnapMirror enables asynchronous and synchronous replication of data to remote sites or cloud environments for disaster recovery
  - MetroCluster: ONTAP's MetroCluster technology provides synchronous replication between geographically separated sites, ensuring zero data loss and rapid recovery in the event of a site failure.
  - Cloud Tiering: Cloud Tiering automatically identifies cold data (data that is infrequently accessed) on primary storage and moves it to lower-cost object storage, either in the cloud or on-premises.
  - BlueXP DRaaS: NetApp BlueXP Disaster Recovery as a Service (DRaaS) is a comprehensive solution designed to provide robust disaster recovery capabilities for businesses, ensuring data protection, rapid recovery, and business continuity in the event of a disaster.

Learn about NetApp platforms for VMware

NetApp offers platforms tailored for VMware environments, including FAS for cost-effective storage, AFF for high-performance workloads, ASA for dedicated SAN deployments, and cloud solutions for hybrid and multicloud architectures. Powered by ONTAP, these platforms support VMware Cloud Foundation and VMware vSphere.

Introduction

These offerings enhance performance, scalability, and data management for the VMware administrator. Additionally, ONTAP is utilized across these platforms, delivering a unified, scalable, and efficient data management solution that supports various storage protocols, enhances data protection, and optimizes performance for diverse workloads.

Common Benefits Across NetApp Platforms

- **VMware Integration:** All NetApp platforms offer deep integrations with VMware, enhancing the efficiency of the storage environment. On-premise solutions can leverage plugins, APIs, VAAI, and VASA to improve overall data management while improving versatility of the infrastructure.
- **Cost Optimization and storage efficiencies:** Leveraging NetApp storage takes advantage of native efficiency technologies such as deduplication, compression, and thin provisioning, significantly reduce

storage consumption and costs while maximizing capacity utilization and performance. Additionally these storage savings result in a reduced burden on compute resources.

- **Unified Data Management:** ONTAP provides a single management interface for both on-premises and cloud-based storage, simplifying administration and reducing complexity. This allows for seamless data movement and management across on-premises and cloud environments, providing flexibility and scalability for VMware workloads.
- **Multi-protocol support:** ONTAP supports a wide range of storage protocols including NFS, CIFS/SMB, iSCSI, FC and NVMe, allowing organizations to consolidate workloads on a single platform or take advantage of purpose-built SAN offerings without creating data silos.
- **Automation and Orchestration:** Support for automation tools like VMware Cloud Foundation Automation (formerly VMware Aria Automation) and integration with Ansible and other automation frameworks streamline operations and reduce administrative overhead.
- **Security:** Robust security features, including encryption at rest and in transit, secure multi-tenancy, and role-based access control, ensure that VMware environments remain secure.
- **ONTAP Tools for VMware:** NetApp ONTAP tools for VMware provides seamless integration and management capabilities, enabling efficient storage provisioning, data protection, and enhanced performance for VMware environments through a unified and intuitive interface.
- **SnapCenter for VMware vSphere:** NetApp SnapCenter for VMware vSphere simplifies and centralizes data protection, backup, and recovery operations for VMware environments, ensuring reliable and efficient management of virtual machine data.
- **High Availability and Resilience:** Features like RAID-TEC and RAID-DP provide robust data protection and high availability, critical for VMware environments.
- **Quality of Service (QoS):** Allows administrators to set performance guarantees for different VMs, ensuring that critical workloads receive the necessary resources.

Note: NetApp cloud solutions may have features limited by the cloud provider, yet they remain very robust for guest connect and support of native NFS datastores.

NetApp ASA (All SAN Array) Benefits

- **Optimized for SAN:** Designed specifically for SAN workloads, providing high performance and low latency for VMware environments that rely on block storage.
- **Enhanced High Availability:** Features like active-active controllers and synchronous replication ensure continuous availability and data protection.

The ASA lineup is comprised of both A-Series and C-Series models.

The NetApp A-Series all-NVMe flash arrays are designed for high-performance workloads, offering ultra-low latency and high resiliency, making them suitable for mission-critical applications.

C-Series QLC flash arrays are aimed at higher-capacity use cases, delivering the speed of flash with the economy of hybrid flash.

Storage Protocol Support

The ASA supports all standard SAN protocols including, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), and NVME over fabrics.

iSCSI - NetApp ASA provides robust support for iSCSI, allowing block-level access to storage devices over IP networks. It offers seamless integration with iSCSI initiators, enabling efficient provisioning and management of iSCSI LUNs. ONTAP's advanced features, such as multi-pathing, CHAP authentication, and ALUA support.

For design guidance on iSCSI configurations refer to the SAN Configuration reference documentation.

Fibre Channel - NetApp ASA offers comprehensive support for Fibre Channel (FC), a high-speed network technology commonly used in storage area networks (SANs). ONTAP seamlessly integrates with FC infrastructure, providing reliable and efficient block-level access to storage devices. It offers features like zoning, multi-pathing, and fabric login (FLOGI) to optimize performance, enhance security, and ensure seamless connectivity in FC environments.

For design guidance on Fibre Channel configurations refer to the SAN Configuration reference documentation.

NVMe over Fabrics - NetApp ONTAP and ASA support NVMe over fabrics. NVMe/FC enables the use of NVMe storage devices over Fibre Channel infrastructure, and NVMe/TCP over storage IP networks.

For design guidance on NVMe refer to NVMe configuration, support and limitations

Active-active technology

NetApp All-Flash SAN Arrays allows for active-active paths through both controllers, eliminating the need for the host operating system to wait for an active path to fail before activating the alternative path. This means that the host can utilize all available paths on all controllers, ensuring active paths are always present regardless of whether the system is in a steady state or undergoing a controller failover operation.

Furthermore, the NetApp ASA offers a distinctive feature that greatly enhances the speed of SAN failover. Each controller continuously replicates essential LUN metadata to its partner. As a result, each controller is prepared to take over data serving responsibilities in the event of a sudden failure of its partner. This readiness is possible because the controller already possesses the necessary information to start utilizing the drives that were previously managed by the failed controller.

With active-active pathing, both planned and unplanned takeovers have IO resumption times of 2-3 seconds.

For more information see TR-4968, NetApp All-SAS Array – Data Availability and Integrity with the NetApp ASA.

For detailed information see the NetApp ASA landing page.

NetApp AFF (All Flash FAS) Benefits

- **Extreme Performance:** Utilizes all-flash storage to deliver sub-millisecond latency and high IOPS, ideal for performance-sensitive VMware workloads.
- **Consistent Low Latency:** Ensures predictable performance for critical applications and VMs, crucial for maintaining SLAs.

For more information on NetApp AFF A-Series storage arrays see the NetApp AFF A-Series landing page.

For more information on NetApp C-Series storage arrays see the NetApp AFF C-Series landing page.

NetApp FAS (Fabric-Attached Storage) Benefits

- **Unified Storage Architecture:** Supports both SAN (block-level) and NAS (file-level) protocols, making it versatile for various VMware workloads.
- **Cost-Effective:** Ideal for environments that require a balance between performance and cost, offering a combination of HDDs and SSDs.

Cloud Solutions Benefits

- **Cloud-Native Data Management:** Utilizes cloud-native offerings to enhance data mobility, backup, and disaster recovery for VMware workloads. Support for native NFS datastore support for VMware cloud workloads is as follows:
  - VMware Cloud on AWS with Amazon FSx for NetApp ONTAP
  - Azure VMware Service with Azure NetApp Files
  - Google Cloud VMware Engine with Google Cloud NetApp Volume -
- **Hybrid Cloud Flexibility:** Seamless integration between on-premises and cloud environments, providing flexibility for VMware workloads that span multiple locations.

Summary

In summary, ONTAP and NetApp platforms offer a comprehensive set of benefits for VMware workloads, enhancing performance, scalability, and data management. While common features provide a solid foundation, each platform offers differentiated benefits tailored to specific needs, whether it's cost-effective storage with FAS, high performance with AFF, optimized SAN performance with ASA, or hybrid cloud flexibility with NetApp cloud offerings.

Learn about hybrid multicloud environments with NetApp and VMware

Discover how NetApp and VMware streamline hybrid multicloud setups by integrating on-premises infrastructure with public cloud services, enabling workload migration, resource optimization, and consistent operations across environments.

Introduction

This approach enables businesses to easily migrate workloads, optimize resource usage, and maintain consistent operations across both environments.

For more information on hybrid cloud scenarios with VMware and NetApp, see Overview of NetApp Hybrid Multicloud with VMware.

VMware Deployment Scenarios with NetApp

This section describes various deployment options for VMware environments across on-premises and public clouds. Each of the cloud providers support a VMware Software Defined Data Center (SDDC) and/or VMware Cloud Foundation (VCF) stack within their respective public cloud offerings.

- **VMware on-premises**

Using VMware with NetApp storage on-premises provides a robust, scalable and flexible virtualization environment. By pairing NetApp's advanced data management features like deduplication, compression, and efficient snapshots with the appropriate storage system powered by ONTAP, customers can choose the platform that works for them. This combination ensures high performance, reliability, and simplified management for virtualized workloads, enhancing overall data center efficiency.

- **Azure VMware Solution**

Azure VMware Solution is a hybrid cloud service that allows for fully functioning VMware SDDCs within the Microsoft Azure public cloud. Azure VMware Solution is a first-party solution fully managed and supported by Microsoft, verified by VMware leveraging Azure infrastructure. This means that when Azure VMware Solution is deployed, customer's get VMware's ESXi for compute virtualization, vSAN for hyper-converged storage, and NSX for networking and security, all while taking advantage of Microsoft Azure's global presence, class-leading data center facilities and proximity to the rich ecosystem of native Azure services and solutions.

- **VMware Cloud on AWS**

VMware Cloud on AWS brings VMware's enterprise-class SDDC software to the AWS Cloud with optimized access to native AWS services. Powered by VMware Cloud Foundation, VMware Cloud on AWS integrates VMware's compute, storage, and network virtualization products (VMware vSphere, VMware vSAN, and VMware NSX) along with VMware vCenter Server management, optimized to run on dedicated, elastic, bare-metal AWS infrastructure.

- **Google Cloud VMware Engine**

Google Cloud VMware Engine is an infrastructure-as-a-service (IaaS) offering built on Google Cloud's highly performant scalable infrastructure and VMware Cloud Foundation stack – VMware vSphere, vCenter, vSAN, and NSX-T. This service enables a fast path to the cloud, seamlessly migrating or extending existing VMware workloads from on-premises environments to Google Cloud Platform without the cost, effort ,or risk of rearchitecting applications or retooling operations. It is a service sold and supported by Google, working closely with VMware.

Management tools and solutions

Learn about managing virtual machines using ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere streamlines lifecycle management for VMs using NetApp storage. Administrators can manage storage directly from the vCenter Server, simplifying operations and enhancing scalability. Key components like the Virtual Storage Console (VSC), VASA Provider, and Storage Replication Adapter (SRA) optimize provisioning, performance monitoring, and disaster recovery.

Introduction

It enables administrators to manage the storage within the vCenter Server directly and simplify the storage and data management for VMware environments. The VMware vSphere Client plug-in tool is designed to integrate plug-in functionality into the vSphere Client without the need to run inside vCenter Server. This provides plug-in isolation and enables scale-out of plug-ins that operate in large vSphere environments.

ONTAP Tools Components

- **Virtual Storage Console (VSC)** The VSC includes the interface integrated with the vSphere client where you can add storage controllers, provision datastores, monitor performance of datastores, and view and update ESXi host settings.
- **VASA Provider** The VMware vSphere APIs for Storage Awareness (VASA) Provider for ONTAP send information about storage used by VMware vSphere to the vCenter Server, enabling provisioning of VMware Virtual Volumes (vVols) datastores, creation and use of storage capability profiles, compliance verification, and performance monitoring.
- **Storage Replication Adapter (SRA)** When enabled and used with VMware Site Recovery Manager (SRM), SRA facilitates the recovery of vCenter Server datastores and virtual machines in the event of a failure, allowing configuration of protected sites and recovery sites for disaster recovery.

For more information on NetApp ONTAP tools for VMware see ONTAP tools for VMware vSphere Documentation.

Learn about using ONTAP and VMware APIs for administration

ONTAP and VMware offer APIs for seamless integration and automation between storage and virtualization platforms. This enables streamlined provisioning, monitoring, and data protection to improve workflow consistency.

Introduction

VMware provides a range of APIs that allow administrators to interact programmatically with various VMware products and services, enhancing efficiency and consistency in operations. Additionally, NetApp ONTAP APIs

provide a robust set of tools that enable administrators to automate, integrate, and optimize the management of storage environments, particularly in conjunction with VMware workloads. These APIs facilitate seamless interaction between ONTAP storage systems and VMware, enhancing efficiency, performance, and data protection.

VMware-based APIs

- **VMware vSphere API:** The vSphere API is a comprehensive API that allows administrators to manage and automate VMware vSphere environments. It provides access to a wide range of vSphere features, including virtual machine provisioning, configuration, monitoring, and lifecycle management.
- **VMware vCenter Server REST API:** The vCenter Server REST API provides a modern, RESTful interface for managing vCenter Server and its associated components. It simplifies automation and integration with other systems and tools.
- **VMware Cloud Foundation API:** The VMware Software-Defined Data Center (SDDC) APIs provide programmatic access to the various components and services within a VMware SDDC environment. These APIs enable administrators and developers to automate, manage, and integrate the different aspects of the data center, including compute, storage, networking, and management services.
- **VMware vSphere Storage APIs - Storage Awareness:** VASA is a set of APIs providing integration of the storage arrays with vCenter for management and administration. The architecture is based on several components including the VASA Provider which handles communication between VMware vSphere and the storage systems. With ONTAP, the provider is implemented as part of ONTAP tools for VMware vSphere.
- **VMware vSphere Storage APIs - Array Integration:** VAAI is a set of APIs that enable communication between VMware vSphere ESXi hosts and the storage devices. The API includes a set of primitive operations used by the hosts to offload storage operations to the array. VAAI can provide significant performance improvements for storage-intensive tasks.

ONTAP-based APIs

- **NetApp ONTAP REST API:** The ONTAP REST API provides a modern, RESTful interface for managing ONTAP storage systems. It simplifies the automation of storage tasks such as provisioning, monitoring, and configuration. It allows for easy integration with VMware vSphere and other VMware management tools, enabling automated storage operations directly from VMware environments. It supports a wide range of operations, from basic storage management to advanced data protection and replication tasks, allowing for scalable and flexible storage management.
- **ONTAP Tools for VMware vSphere:** ONTAP tools for VMware vSphere is a set of tools for integrating ONTAP and vSphere. It implements the provider functionality of the VASA API framework. ONTAP tools also includes the vCenter plug-in, a storage replication adapter (SRA) for VMware Site Recovery Manager, and a REST API server you can use to build automation applications.

Summary

In summary, with ONTAP APIs, administrators can script the creation and configuration of datastores in VMware environments, ensuring quick and consistent storage provisioning. Additionally, they can automate the creation, scheduling, and deletion of snapshots for VMware virtual machines, providing efficient data protection and recovery options. SnapMirror APIs facilitate the automation of replication relationship setup and management, ensuring robust disaster recovery solutions for VMware workloads.
Administrators can also implement scripts to monitor storage performance metrics and trigger alerts or automated actions when performance thresholds are breached, ensuring optimal storage performance for VMware workloads. By integrating ONTAP APIs with VMware APIs, such as those provided by vSphere and vRealize, administrators can achieve a seamless and highly automated management experience, enhancing the overall efficiency and reliability of their virtualized infrastructure.

Learn about monitoring a complete infrastructure using NetApp Data Infrastructure Insights

NetApp Data Infrastructure Insights (formerly Cloud Insights) monitors on-premises and cloud systems, offering visibility into your complete IT environment, including VMware vSphere and ONTAP storage systems. It enables capabilities such as performance tracking, issue detection, and resource optimization across your public and private environments.

Introduction

With Data Infrastructure Insights, you can monitor, troubleshoot and optimize all your resources including your public clouds and your private data centers.

For more information on Data Infrastructure Insights, see Data Infrastructure Insights Documentation.

Data Infrastructure Insights Capabilities

- Data Infrastructure Insights provides hybrid multicloud monitoring, giving you full-stack observability of infrastructure and workloads.
- Data collectors for heterogeneous infrastructure and workloads, including Kubernetes
- Open Telegraf collector and open APIs for easy integration
- Comprehensive alerting and notifications
- Machine learning for intelligent insights
- Optimize resource utilization
- Built-in or customizable dashboards with advanced filters to minimize display noise to answer questions
- Discover the health of your ONTAP storage operations
- Protect your most valuable business asset – data - from ransomware or data destruction attack

Learn about VMs from VMware vSphere to ONTAP datastores

VMware vSphere administrators can enhance their infrastructure by migrating workloads to NetApp ONTAP datastores. ONTAP delivers VM-aware snapshots, storage-efficient clones, and seamless vMotion operations while supporting Storage Policy-Based Management (SPBM). Whether migrating from vSAN, legacy storage, or implementing hybrid cloud deployments, ONTAP provides improved performance and simplified storage operations for VMware environments.

This migration enables seamless integration, improved data protection, and greater flexibility in managing virtualized environments, ensuring a smooth transition with minimal downtime.

Use cases

There are many options with migration in terms of the source and destination when considering moving to ONTAP backed datastores.

- Migration from third party storage systems (including vSAN) to ONTAP datastores.

- Migration of VMs in the same vSphere cluster
- Migration of VMs across multiple vSphere clusters
- Migration of VMs across vCenter servers in same SSO domain
- Migration of VMs across vCenter servers in different SSO domains
- Migration of VMs across datacenter locations
- Migration from third party storage systems (including vSAN) to ONTAP datastores.
- Migration of VMs in a hybrid cloud environment

For more information on migrating VMware workloads to ONTAP backed datastores, see the Migrate VMs to ONTAP datastores.

Data protection solutions

Learn about protecting VMware environments with MetroCluster and SnapMirror active sync

Advanced business continuity is essential to safeguard VMware environments from domain-wide outages. NetApp and VMware offer solutions like NetApp MetroCluster, SnapMirror active sync, and VMware vSphere Metro Storage Cluster (vMSC) to enhance workload protection and ensure high availability.

Introduction

In addition to availabilities built into the products, VMware and NetApp offer advanced configurations that further protect workloads that are spread across failure domains such as racks, building, campuses or even cities.

NetApp MetroCluster

NetApp MetroCluster uses NetApp's high-availability (HA) capability to protect against controller failures. MetroCluster also includes SyncMirror technology, cluster failover on demand (CFOD), hardware redundancy, and geographical separation for high availability. SyncMirror synchronously mirrors data across two plexes: the local plex actively serving data and the remote plex as a standby. All MetroCluster components, such as controllers, storage, cables, switches, and adapters, have hardware redundancy.

NetApp SnapMirror active sync

NetApp SnapMirror active sync provides datastore-granular protection with FCP and iSCSI SAN protocols, selectively protecting high-priority workloads topology. It offers active-active access to both local and remote sites, unlike the active-standby MetroCluster. Starting with ONTAP 9.15.1, SnapMirror active sync supports symmetric active/active capability, allowing read and write I/O operations from both copies of a protected LUN with bidirectional synchronous replication.

VMware vSphere Metro Storage Cluster

VMware vSphere Metro Storage Cluster (vMSC) enhances VMware HA with active-active stretched storage. This certified configuration protects VMs and containers against failures. This is accomplished by using stretched storage concepts along with clusters of vSphere hosts. These hosts are distributed across different failure domains. The NetApp MetroCluster and SnapMirror active sync storage technologies are used to provide protection and supported storage offerings. By leveraging vMSC, with a NetApp certified solution

provides robust and resilient IT operations across failure domains.

For detailed information see the vSphere Metro Storage Cluster with ONTAP.

Learn about mitigating security and ransomware risks for VMware workloads

ONTAP enhances security and ransomware protection in VMware environments through encryption, snapshots, and advanced access controls, complementing VMware's security features to safeguard data.

Introduction

By leveraging the advanced capabilities of NetApp ONTAP within VMware environments, organizations can ensure the integrity, availability, and security of their data.

See below for how these technologies work together to deliver **security** and **backup benefits** in greater detail.

Security and Ransomware

Security is a paramount concern in virtualized environments, and NetApp ONTAP provides robust features to enhance security within VMware infrastructures. ONTAP offers encryption for data at rest and in transit, ensuring that sensitive information is protected from unauthorized access. Encryption keys are managed securely, and ONTAP supports both software-based and hardware-based encryption solutions. By integrating with VMware's security tools, such as vSphere's built-in security features and third-party security solutions, ONTAP helps create a secure and compliant environment.

Ransomware Defense

Ransomware attacks pose a significant threat to organizations, and the combination of VMware and ONTAP provides a strong defense mechanism. ONTAP's Snapshot technology allows for the creation of immutable snapshots that cannot be altered or deleted by ransomware. In the event of an attack, these snapshots can be used to quickly restore affected VMs and datastores to their pre-attack state, minimizing downtime and data loss. Additionally, ONTAP's integration with security information and event management (SIEM) systems enables proactive monitoring and alerting of suspicious activities. ONTAP also supports multi-factor authentication (MFA) and role-based access control (RBAC) to further enhance security.

Ransomware Recovery Guarantee

The NetApp Ransomware Guarantee provides organizations with a robust and reliable solution for protecting against ransomware attacks. By leveraging the advanced capabilities of NetApp ONTAP, organizations can ensure the security and availability of their data. The guarantee offers peace of mind, knowing that in the event of a ransomware attack, data can be quickly and effectively restored, minimizing downtime, data loss, and financial impact. This commitment to data security and resilience makes NetApp an ideal partner for organizations looking to safeguard their critical assets against evolving cyber threats.

Advanced Security Features

ONTAP includes advanced security features such as secure multi-tenancy, which isolates data and resources in multi-tenant environments, and compliance auditing, which tracks and logs access to sensitive data. These features ensure that data remains secure and that organizations can demonstrate compliance with industry regulations and standards.

Summary

The integration of ONTAP's security features—such as encryption, immutable snapshots, and advanced access controls—with VMware's tools provides robust defense against cyber threats, including ransomware. ONTAP's support for secure multi-tenancy and compliance auditing ensures data protection and regulatory compliance.

Together, NetApp ONTAP and VMware offer a comprehensive solution for securing virtualized environments, enabling organizations to protect data, minimize downtime, and maintain business continuity. Implementing these technologies helps businesses address modern IT challenges and safeguard critical assets against evolving security threats.

Autonomous Ransomware Protection for NFS and VMFS

Discover how NetApp ONTAP's Autonomous Ransomware Protection (ARP) uses machine learning to secure NFS and VMFS datastores in VMware environments, providing early threat detection, tamper-proof snapshots, and rapid recovery to strengthen data resilience across virtualized and cloud workloads.

Overview

Ransomware threats are evolving quickly, becoming more sophisticated and disruptive. Traditional security measures often fail to protect critical data assets. NetApp ONTAP storage provides built-in security features that proactively safeguard data. If a security breach occurs, ONTAP delivers real-time alerts and rapid recovery options to reduce downtime and limit data loss. ONTAP enables customers to protect, recover, and move their data and applications, strengthening ransomware resilience.

Use case – Protect VMware VMs and its files

Early detection of ransomware in VMware environments is critical to stopping its spread and minimizing downtime. An effective strategy uses multiple layers of protection across ESXi hosts and guest virtual machines. While many security controls help build a strong defense, NetApp ONTAP adds essential storage-level safeguards that further strengthen protection.

Key ONTAP features include Snapshot technology for point-in-time recovery, Autonomous Ransomware Protection (ARP) powered by built-in machine learning, multi-admin verify and tamperproof snapshots that preserve data integrity. These capabilities work together to enhance ransomware resilience and enable rapid recovery when needed.

Securing vSphere environments and guest virtual machines requires a comprehensive approach. Key measures include network segmentation, deploying EDR/XDR/SIEM solutions for endpoint monitoring, applying timely security updates, and following established hardening guidelines. Each VM typically runs a standard operating system, making it critical to install and regularly update enterprise-grade anti-malware solutions as part of a multi-layered ransomware defense strategy.

How ONTAP helps

ONTAP strengthens data protection with multiple layers of defense. Key features include Snapshots, Autonomous Ransomware Protection (ARP), tamper-proof snapshots, multi-admin verification, and more. This document focuses on the enhancements to ARP introduced in version 9.17.1.

You can enable ARP on NAS or SAN volumes that support VMware datastores. ARP uses ONTAP's built-in machine learning to monitor workload patterns and data entropy, automatically detect signs of ransomware activity, and provide an intelligent, proactive layer of security. Configure ARP per volume using ONTAP's CLI or

System Manager interface.

ARP feature evolution

Starting with ONTAP version 9.10.1, ARP is available for an existing volume or a new volume. In ONTAP version 9.16.1, you can enable ARP using System Manager or the CLI. ARP/AI protection becomes active immediately, with no learning period required. In version 9.17.1, ARP supports SAN volumes. When you enable ARP on a SAN volume, ARP/AI continuously monitors data during an evaluation period to determine workload suitability and set the optimal encryption threshold for detection.

ARP is built into ONTAP, providing integrated control and coordination with other ONTAP features. ARP works in real time, processing data as it is written or read, and quickly detects and responds to potential ransomware attacks. It creates locked snapshots at regular intervals alongside scheduled ones, and intelligently manages snapshot retention by recycling them when no anomalies are detected. If ARP detects suspicious activity, it preserves a snapshot taken before the attack for an extended period to ensure a reliable recovery point.

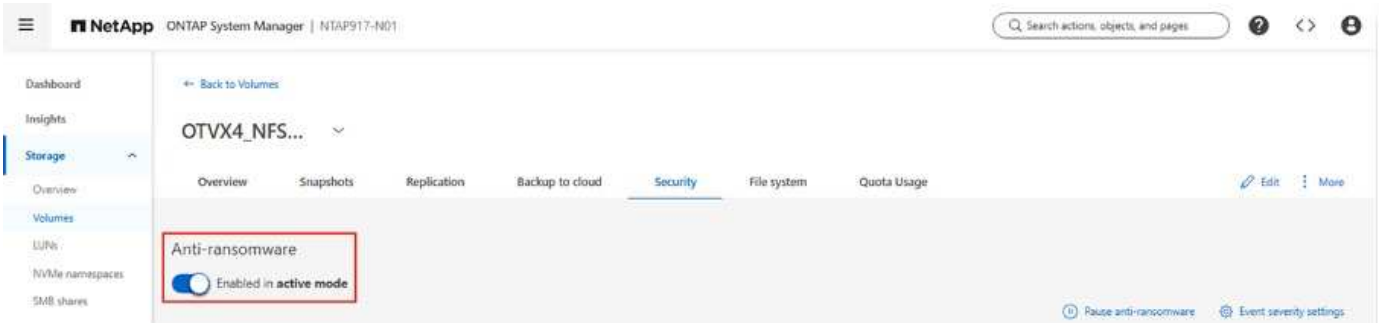
For more details, see What ARP detects.

ARP support is included with the ONTAP ONE license.

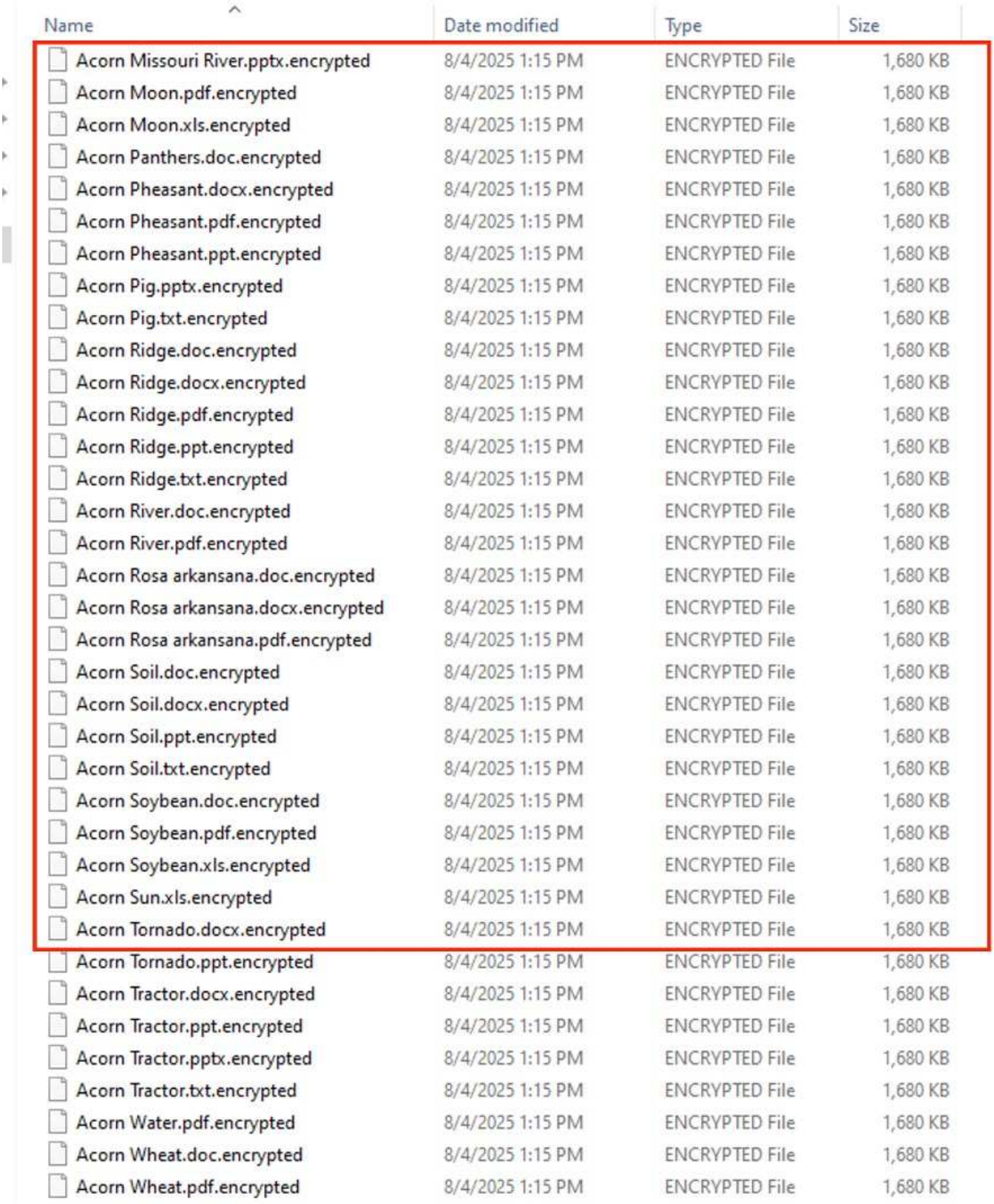
Configure ARP on NAS volumes and simulating an attack on a VM

Learn how to enable NetApp ONTAP Autonomous Ransomware Protection (ARP) on NAS and SAN volumes used for VMware datastores, and simulate ransomware attacks to see how ARP detects threats and facilitates rapid recovery.

When ARP is enabled on a NAS volume using System Manager or the CLI, ARP/AI protection is enabled and active immediately. No learning period is required.

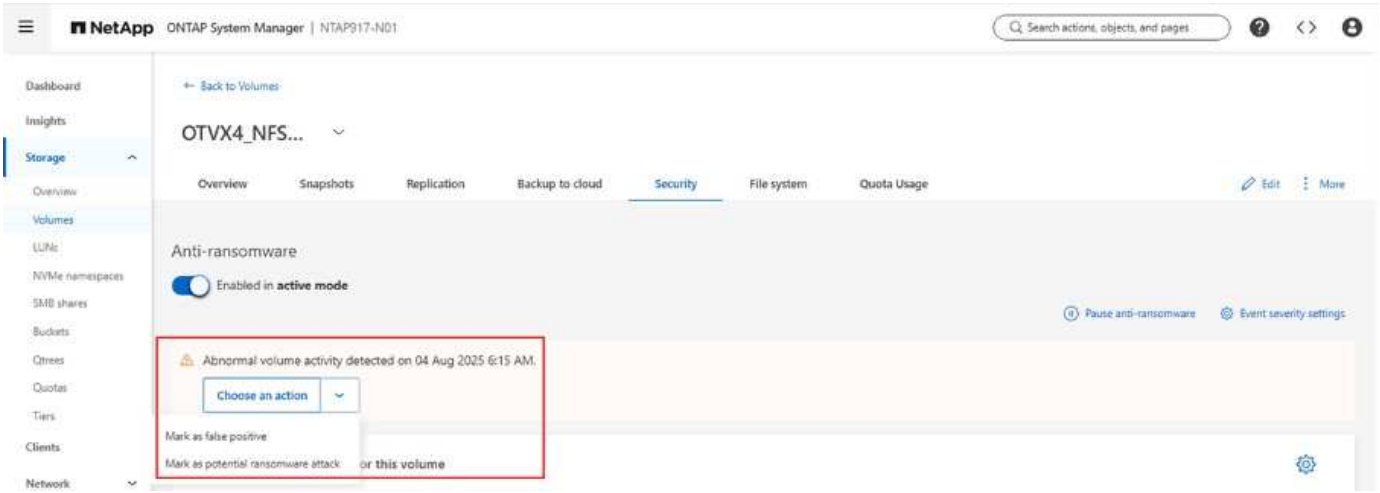


In this example, simulation is triggered using a script to modify the files or by modifying the file extension to simulate an attack within a VM residing on the NFS volume that is attached as datastore to vCenter.



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

As shown below, ARP detected the abnormal activity.

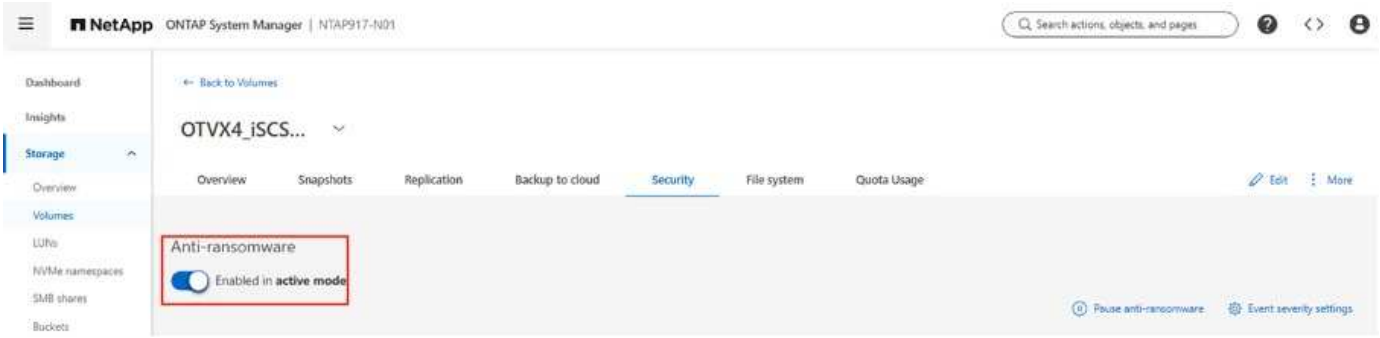


ARP detects the attack early and enables data recovery from snapshots taken close to the attack time. To rollback, use ARP periodic snapshot that was generated before the incident was triggered. And the screenshot below shows the snapshots created:

For detailed guidance to enable ARP on NFS volumes that serve as datastores and recover in the event of an attack, refer ARP for NFS storage.

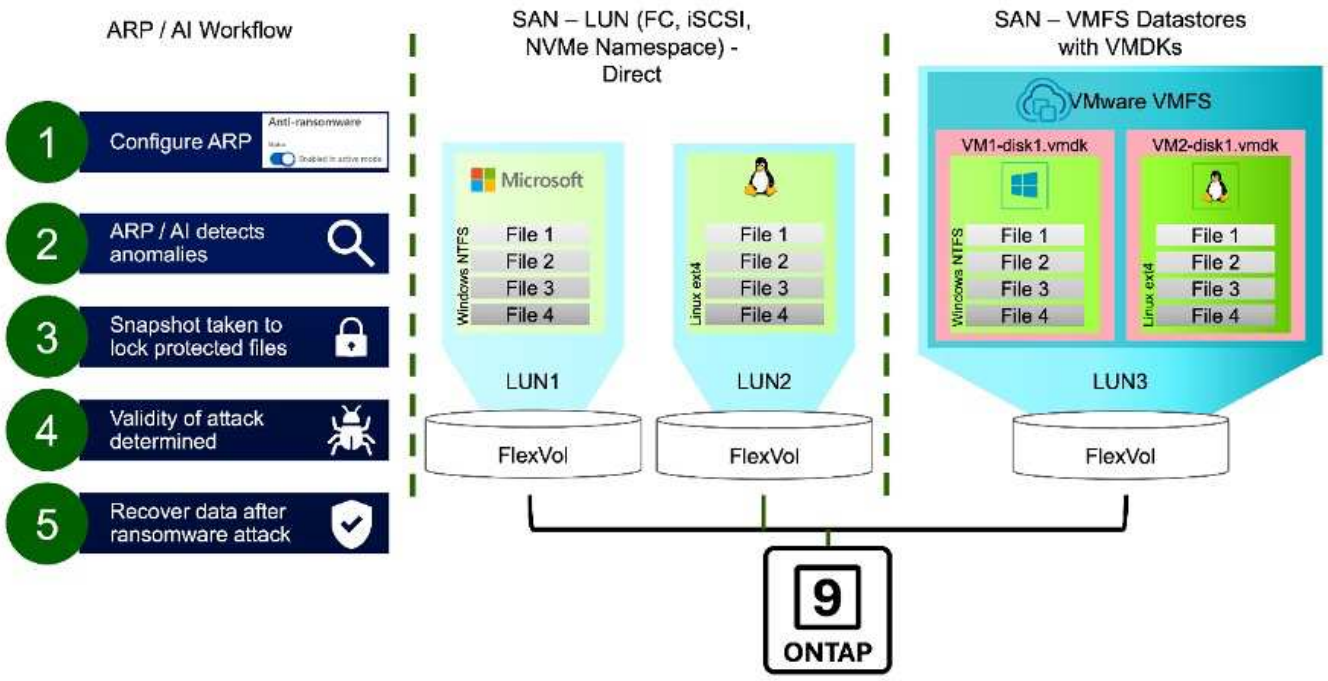
Configure ARP on SAN volumes and simulating an attack on a VM

When ARP is enabled on a SAN volume, it begins with an evaluation phase, similar to the learning mode used in NAS environments before automatically transitioning into active detection.



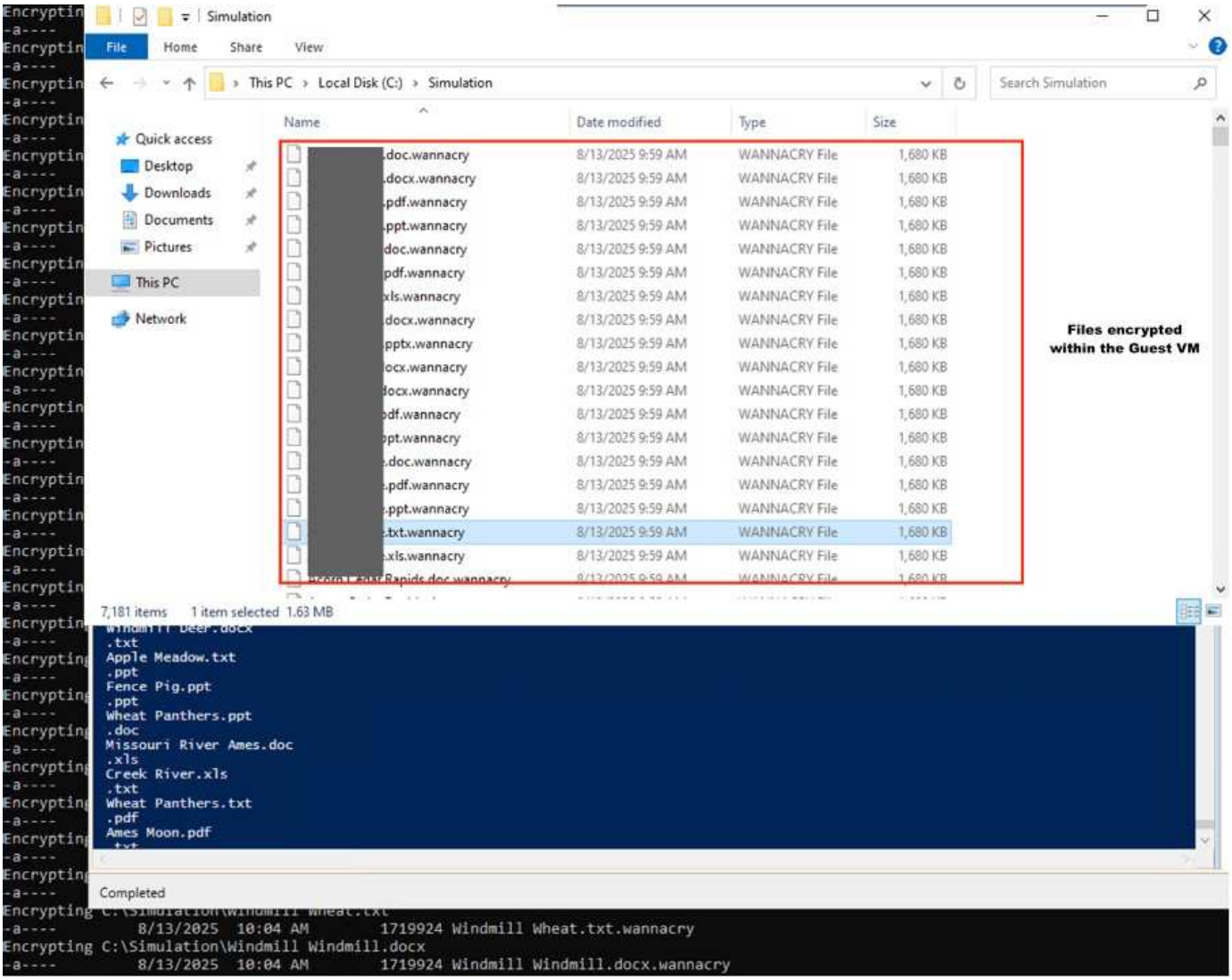
ARP initiates a two to four week evaluation period with a threshold of 75% to establish a baseline for encryption behaviour. Progress during this phase can be monitored using the `security anti-ransomware volume show` command by checking the **Block device detection status**. After the evaluation completes, a status of **Active_suitable_workload** confirms that the observed entropy levels are suitable for ongoing monitoring. Based on the data collected, ARP automatically adjusts its adaptive threshold to ensure accurate and responsive threat detection. Depending on the requirement, the snap creation interval can be changed from the default 4h to 1h. Exercise this modification with caution.

Beginning with ONTAP 9.17.1, ARP snapshots are generated at regular intervals for both NAS and SAN volumes.

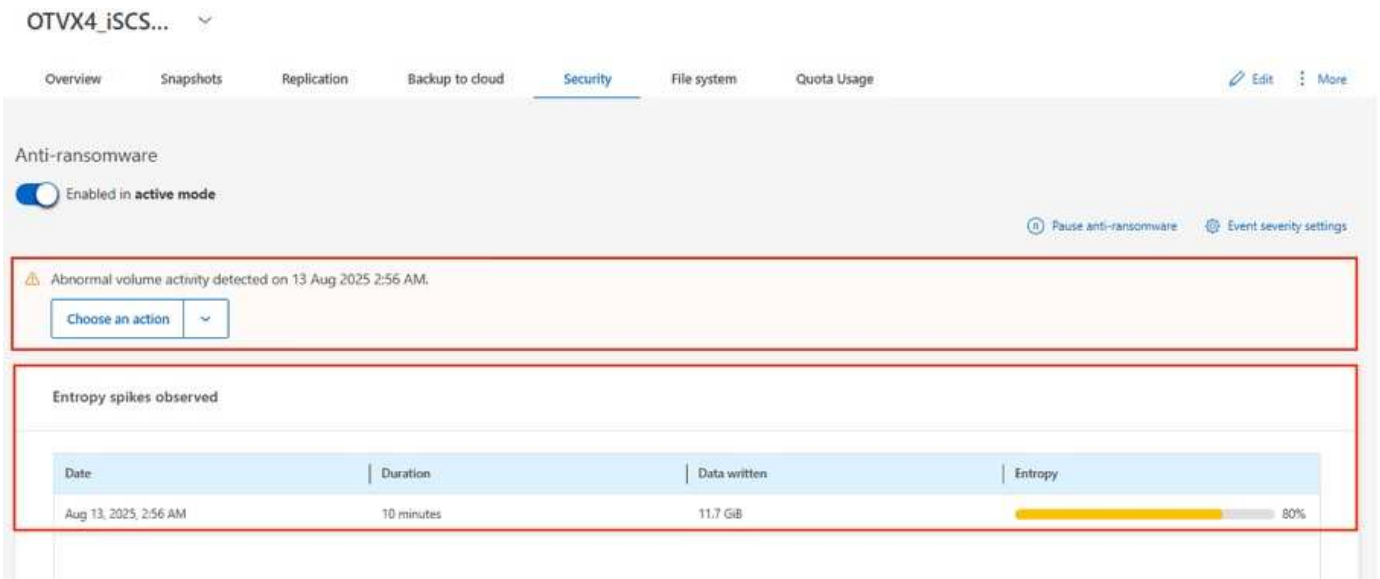


For detailed information, refer SAN environments and mode types

It’s time to simulate an attack. For demonstration purposes, files are encrypted within a virtual machine running on ISCSI based datastore. Nearly 7000 files are generated which is unfortunately affected by ransomware attack.

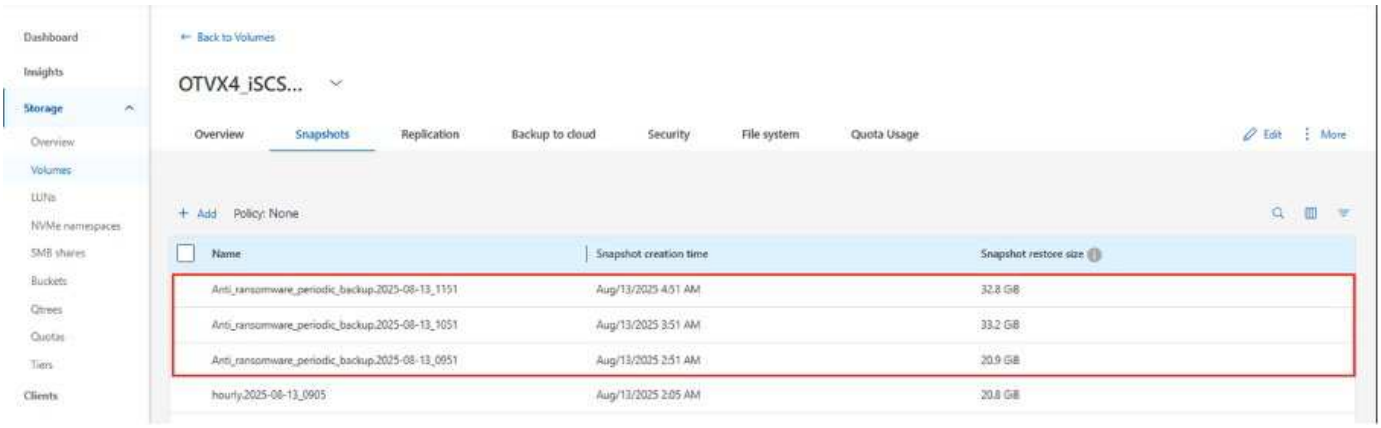


Within 10 mins, abnormal activity was detected on the volume based on the high entropy data and ARP generates a threat alert as it detected an entropy anomaly inside the VM.

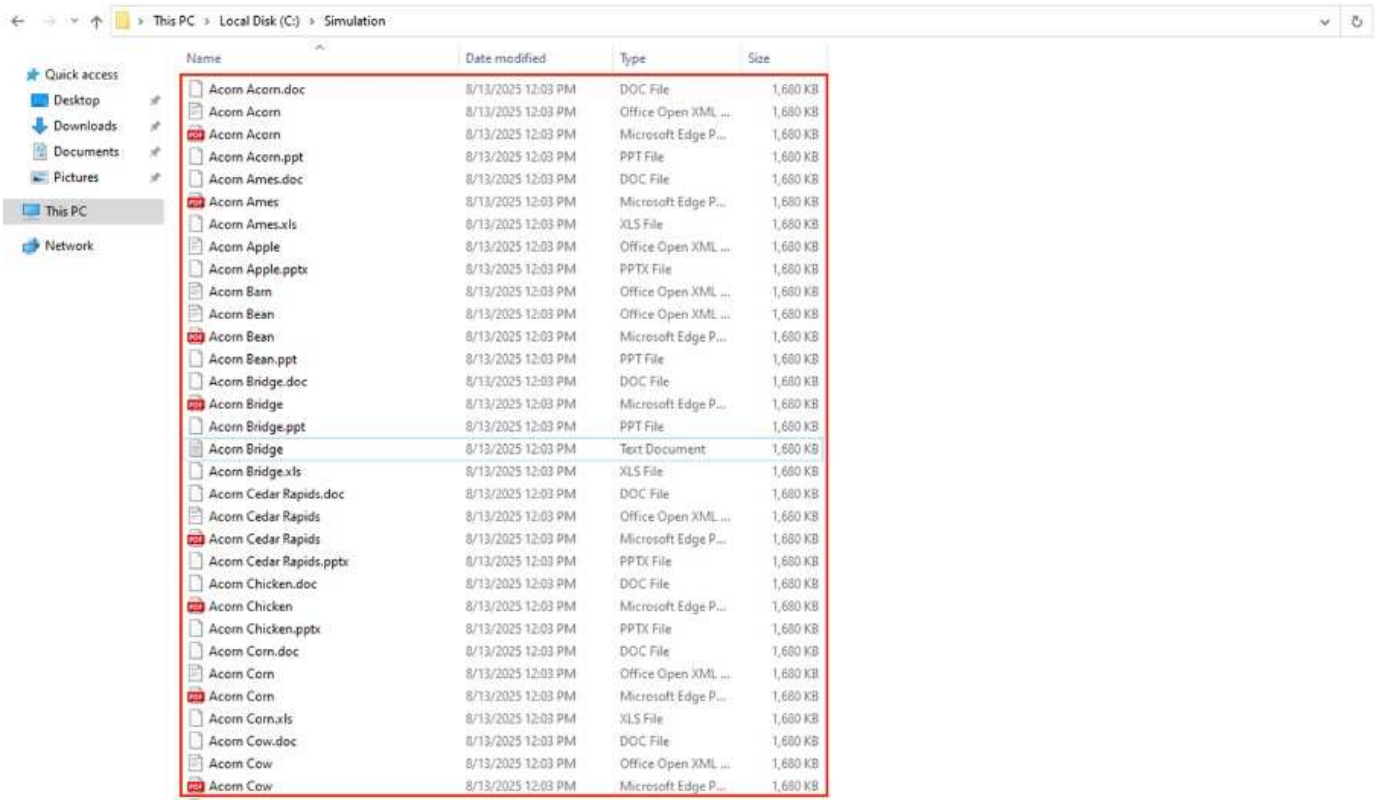


Recover VM and its data after a ransomware attack

Once the attack is confirmed based on the steps covered above, use one of the ARP snapshots or another snapshot of the volume to restore the data.



Once restored, the files are all recovered.



For detailed guidance, see Restore data from ARP snapshot after a ransomware attack

ONTAP as a defense layer for VMware and beyond

With just a few clicks, businesses can seamlessly enhance their data protection strategy. Powered by advanced machine learning-based detection mechanisms, ONTAP introduces a powerful layer of defense in VMware environments. This intelligent protection not only identifies threats early but also helps mitigate potential damage before it escalates.

This use case applies to more than just VMware. You can extend the same principles to any NAS or SAN-based application to build a multi-layered security architecture. Attackers are forced to navigate through

several fortified layers, significantly reducing the risk of successful breaches.

ONTAP doesn't just protect data—it empowers organizations to stay resilient in the face of evolving threats.

Backup and disaster recovery solutions

Learn about backup and restore of virtual machines using SnapCenter plug-in for VMware vSphere

The SnapCenter Plug-in for VMware vSphere enables fast, VM-consistent backup and restore operations for VMs, datastores, and VMDK files. This VMware plug-in integrates with SnapCenter Server to support application-based backup and restore for SnapCenter application-specific plug-ins.

Documentation resources

Refer to the following documentation resources for detailed information.

- SnapCenter Plug-in for VMware vSphere documentation

Solution resources

Refer to the following 3-2-1 backup solution featuring SnapCenter Plug-in for VMware vSphere and BlueXP backup and recovery for VMs.

Technical Report: 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs

Tech ONTAP Blog: 3-2-1 Data Protection for VMware with SnapCenter Plug-in and BlueXP backup and recovery for VMs

Video resources

SnapCenter Plug-in for VMware vSphere - Solution Pre-Requisites

SnapCenter Plug-in for VMware vSphere - Deployment

SnapCenter Plug-in for VMware vSphere - Backup Workflow

SnapCenter Plug-in for VMware vSphere - Restore Workflow

SnapCenter - SQL Restore Workflow

Learn about disaster recovery of virtual machines using BlueXP disaster recovery

BlueXP disaster recovery automates the replication and recovery of VMware virtual machines using ONTAP storage. It supports recovery from on-premises setup to VMware Cloud on AWS with Amazon FSx for NetApp ONTAP or another on-premises VMware environment.

Introduction

Having a successful plan and combination of technologies ensures the protection of critical data, applications and VMs. The challenge with DR is determining the appropriate level of protection and associated costs.

ONTAP arrays offer built-in replication to transfer volume data, and therefore the virtual machines residing on the designated datastore LUNs, from one site to another. BlueXP DRaaS integrates with vSphere and automates the entire workflow for seamless failover and failback in the event of disaster.

For more information on BlueXP DRaaS, see Overview of BlueXP DRaaS.

Considerations

The most time-consuming parts of a DR failover in a VMware vSphere environment is the execution of the steps necessary to inventory, register, reconfigure, and power up VMs at the DR site. An ideal solution has both a low RPO (as measured in minutes) and a low RTO (measured in minutes to hours). One factor that is often overlooked in a DR solution is the ability to test the DR solution efficiently on a periodic interval.

To architect a DR solution, keep the following factors in mind:

- The recovery time objective (RTO). The RTO is how quickly a business can recover from a disaster, or, more specifically, how long it takes to execute the recovery process to make business services available again.
- The recovery point objective (RPO). The RPO is how old the recovered data is after it has been made available, relative to the time that the disaster occurred.
- Scalability and adaptability. This factor includes the ability to grow storage resources incrementally as demand increases.

For more technical information on the available solutions, please see:

- DR using BlueXP DRaaS for NFS Datastores
- DR using BlueXP DRaaS for VMFS Datastores

Copyright information

Trademark information