White Paper

NetApp ONTAP reliability, availability, serviceability, and security

Balbeer Bhurjhee – Manager, Solution Engineering, NetApp
September 24, 2024 | WP-7354

Abstract

This white paper describes the capabilities of NetApp® ONTAP® software and NetApp All SAN Array (ASA), NetApp AFF, and NetApp FAS systems as they relate to reliability, availability, serviceability, and security (RASS).

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Executive summary

The NetApp® ONTAP® unified data platform is available as storage services, appliances, and software, including on-premises, hybrid multicloud, and wholly cloud-resident architectures. Unlike any other key primary storage offering, ONTAP is natively built into and offered directly by both AWS, Azure and Google Cloud. ONTAP is the number one data storage platform, with an unparalleled breadth of deployment models, and NetApp has invested heavily in reliability, accessibility, serviceability, and security (RASS).

Table 1) NetApp ONTAP services and products.

Storage services	Storage appliances	Storage software
• NetApp Keystone™ • Amazon FSx for NetApp ONTAP • Azure NetApp Files • Google Cloud NetApp Volumes	• NetApp ASA A-Series • NetApp ASA C-Series • NetApp AFF A-Series • NetApp AFF C-Series • NetApp FAS	• NetApp Cloud Volumes ONTAP • NetApp ONTAP Select

ONTAP provides partitioned multitenant security of data both at-rest and in-flight to applications using a wide range of network fabrics. All of these capabilities are available from a single unified scale-out data platform that is dynamic, from resource allocation across the cluster, increasing operational simplicity and operational and TCO management. Data is efficiently stored and transported by ONTAP across the hybrid cloud for multiple use cases. Performance can be managed with quality of service (QoS) policies that include maximum and minimum limits and data can be secured with National Security Agency validated dual-layer encryption Data availalbility is enhanced by a no-single-point-of-failure architecture.

Thanks to the dynamic and flexible nature of the platform, the ONTAP architecture supports a mixture of controller types (small, medium, large); data storage media (NL-SAS, SAS, Flash SSD including TLC and QLC, NVMe SSD, etc.); network fabrics (64/32/16Gb FC and 200/100/40/25/10/1G Ethernet); and protocols (NVMe/FC, NVMe/TCP, NFSv4/RDMA, FC, FCoE, NFS v3, NFSv4.1, NFSv4.2, pNFS, CIFS/SMB, and S3) in a single unified scale-out platform. This support offers genuinely unified storage that provides simultaneous block, file, and object protocol access using the same physical controllers and drives. NetApp All SAN Array (ASA) is available for customers who prefer block-only storage.

The flexible nature of ONTAP as a platform enables NetApp customers to adapt and exploit its rich and unique capabilities, with benefits in performance, capacity, access protocols, and costs. In short, ONTAP does not restrict or limit the imagination when it comes to building and powering enterprise applications. That’s true whether it’s running on engineered platforms or as software-defined storage in the data center and across multiple public clouds. ONTAP provides and enables one experience for any cloud.

Storage clusters can scale to include up to 24 storage controllers (for example, nodes) and up to 5,760 drives managed as a single logical pool. Scaling options include the ability of ONTAP storage to scale out horizontally (by adding new storage controller nodes) and scale up vertically (by upgrading the storage controller and increasing storage capacity). These options effectively create a two-dimensional framework for adapting performance and capacity to meet the needs of all storage workloads.

Introduction

Some terminology, such as SAN, is shared industrywide, but meanings can vary due to context and other factors. This section describes what NetApp means by some terms that are used in this paper.

Definitions

Reliability

NetApp defines reliability as the ability of a system to operate without failures. Reliability is usually reported using metrics that include the mean time between failure (MTBF), average failure rate (AFR), and average return rate (ARR). Reliance on MTBF metrics alone can result in misleading expectations because the failure probability of an individual component (that is, a single drive) is less predictive of system reliability than the AFR of a large population of components.

Availability

NetApp defines availability as the ability of a system to remain operational without interruption. Availability is usually reported using metrics that include the percentage of uptime (for example, 99.9999%) and the amount of downtime per period (for example, 32 seconds per year). Uptime percentages are sometimes described as “nines of availability,” with 6 nines equal to 99.9999% and 5 nines equal to 99.999%.

Serviceability

NetApp defines serviceability as the ability of a system to be maintained. As a practical matter, serviceability can include monitoring, diagnostics, repair, and upgrade factors. Serviceability is usually reported using metrics that indicate a nondisruptive or disruptive effect and involve customer or vendor action. Related terms include “hot swap,” “removable,” “replaceable,” and “in-chassis upgrades” (for example, AFF A700 to A900). Also, NetApp is committed to making its products accessible by using the accessibility best practices and standards defined in Section 508 of the U.S. Rehabilitation Act for guidance. And NetApp conforms to the Voluntary Product Accessibility Template (VPAT), which lists the requirements for a product to meet applicable accessibility standards.

Security

NetApp defines security as the ability of a system to mitigate unauthorized access. As a practical matter, security can include theft, damage, and sabotage to physical and logical assets. Security is usually reported using metrics and certifications that include the presence of certain features, such as passwords and locks, and compliance with relevant standards, such as NSA CSfC, ISO/IEC Common Criteria, and US FIPS. Key components of a datacentric security strategy are Zero Trust architecture, ransomware protection, platform security, encryption, replication, and certification.

Hybrid multicloud

NetApp defines hybrid multicloud as the ability of a system to include private and public cloud infrastructure (hybrid) supporting more than one cloud provider (multicloud). An example of NetApp hybrid multicloud includes AFF clusters and systems supporting private clouds and an instance of ONTAP running either as a first-party cloud data storage service - e.g., Amazon FSx for NetApp ONTAP, Azure NetApp File, or Google Cloud NetApp Volumes; or as a marketplace offering known as Cloud Volumes ONTAP running on AWS, Azure, and Google Cloud public cloud infrastructure. An essential characteristic is the support of the three primary hyperscaler clouds as both 1st-party and marketplace offerings simultaneously.

Unified storage

NetApp defines unified storage as the ability of a single operating system (not two operating systems with the same brand name) to offer block, file, and object storage access by using multiple networks and protocols. For NetApp AFF and FAS clusters and systems, supported networks include Ethernet and Fibre Channel. Supported protocols include NVMe, iSCSI, and Fibre Channel for block; NFS/pNFS and SMB/CIFS for file; and S3 for object storage. An essential characteristic is native support of multiple and different storage types, networks, and protocols from the same cluster or system.

Architecture

The flexibility of the NetApp ONTAP platform for hybrid multicloud storage results in support for many architectures. This white paper focuses on unified SAN (block) and NAS (file and object) storage using NetApp AFF and FAS storage clusters and systems. NetApp also offers an All SAN Array (ASA), a SAN-only appliance. Unified SAN and NAS, as well as SAN-only architectures, are described in the next subsection.

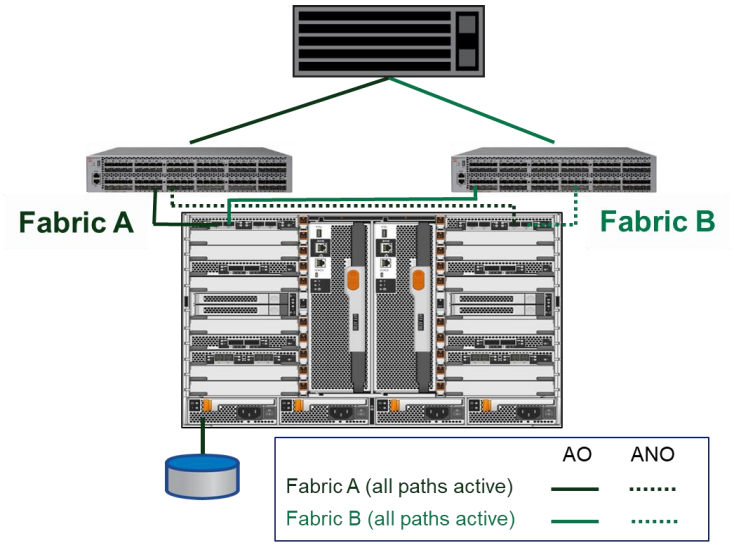
ONTAP® Unified Storage Operating System

NetApp ONTAP powers various storage products, including NetApp AFA, ASA, FAS, and Cloud Volumes ONTAP, across hybrid multicloud environments. It delivers enterprise-grade data center functionality and supports data access using popular block (iSCSI, FCP, and NVMe), file (NFS and SMB), and object (S3) protocols.

Unified SAN and NAS Storage Systems and Clusters

NetApp AFF and FAS clusters use an active-active controller architecture to deliver unified SAN and NAS storage by using multiple protocols and Fibre Channel and Ethernet fabrics. This architecture advertises routes directly to the controller that hosts the LUN as active-optimized (AO) paths, with all other paths (indirect paths) advertised as active-nonoptimized (ANO) paths. Active-nonoptimized paths are not used unless no active-optimized paths exist. This architecture was chosen to allow the performance capabilities of both controllers in the HA pair to contribute to the overall day-to-day performance of the system. Other vendors' active-active controller architectures relegate the second controller to a more passive status and thereby restrict the overall storage array performance for 99% of daily operation. Figure 1 illustrates the NetApp optimized/nonoptimized active-active controller pathing.

Figure 1) NetApp AFF and FAS unified storage architecture.



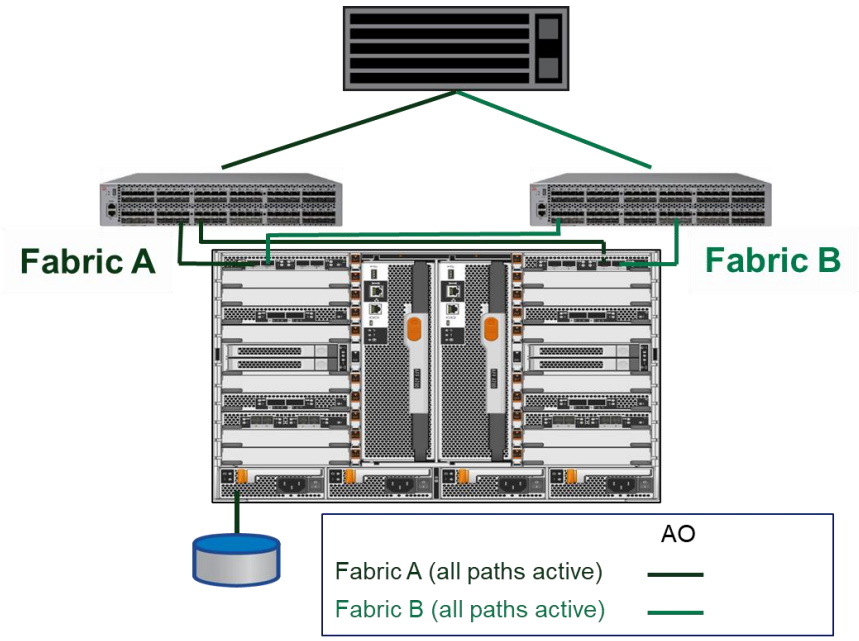
NetApp AFF and FAS are ideal for almost every environment. In case of a controller failure, either single controller can access all of the data on the array, and failover is executed in a few seconds.

Learn more about NetApp ONTAP, AFF, and FAS unified SAN and NAS.

SAN-only Storage Systems and Clusters

NetApp ASA clusters and systems deliver SAN-only block storage using FC SAN, NVMe/FC, NVMe/TCP, and iSCSI protocols. Also, they use symmetric active-active pathing designed to meet service level objectives geared toward reducing failover times to an absolute minimum by enabling virtually instantaneous and nondisruptive failovers. One way this is achieved is by advertising all paths as active-optimized so there are always active paths to all LUNs even if a storage failover (also called a takeover or giveback) occurs. Recoveries occur as fast as possible during a storage failover failure because hosts don't need to switch paths. They merely cease using any path that becomes unavailable. Figure 2 illustrates these paths.

Figure 2) NetApp ASA SAN-only architecture.



Also, the ASA symmetric active-active architecture reduces the impact of planned and unplanned storage failovers or other component failures. In particular, because of the symmetric access that ASA provides to all LUNs, even with a path, fabric, network, or other failures, a well-designed and managed ASA still provides continuous, consistent, low-latency data access. Consult the NetApp Technical Report 4968. For details about how the architecture of NetApp ASA systems differs from AFF systems.

Learn more about the NetApp ASA SAN-only storage with symmetric active-active architecture.

Data protection

Data protection is a complex subject. At NetApp, data protection includes the essential capabilities of business continuity (BC), disaster recovery (DR), high availability (HA), and backup and recovery (BR). NetApp ASA, AFF and FAS systems and clusters natively include all of these data protection capabilities,

as well as many other advanced capabilities for storage and data management supporting on-premises, hybrid multicloud, and wholly cloud-resident environments. This section describes these essential NetApp data protection capabilities.

Business continuity

In today's constantly connected global business environment, organizations need a rapid recovery of business-critical application data with zero data loss following a disruption such as a cyberattack, power outage, equipment failure, or natural disaster. Financial organizations especially have zero tolerance for data loss or application unavailability. Additionally, many enterprises must adhere to the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other regulatory mandates.

Organizations can devise an effective business continuity and disaster recovery plan with the following requirements as priorities:

- Zero recovery point objective (RPO) to achieve zero data loss enabled by synchronous replication.
- Zero recovery time objective (RTO) through Transparent Application Failover (TAF), to prevent disruption of business-critical applications in case of disaster*.

NetApp offers two solutions for business continuity:

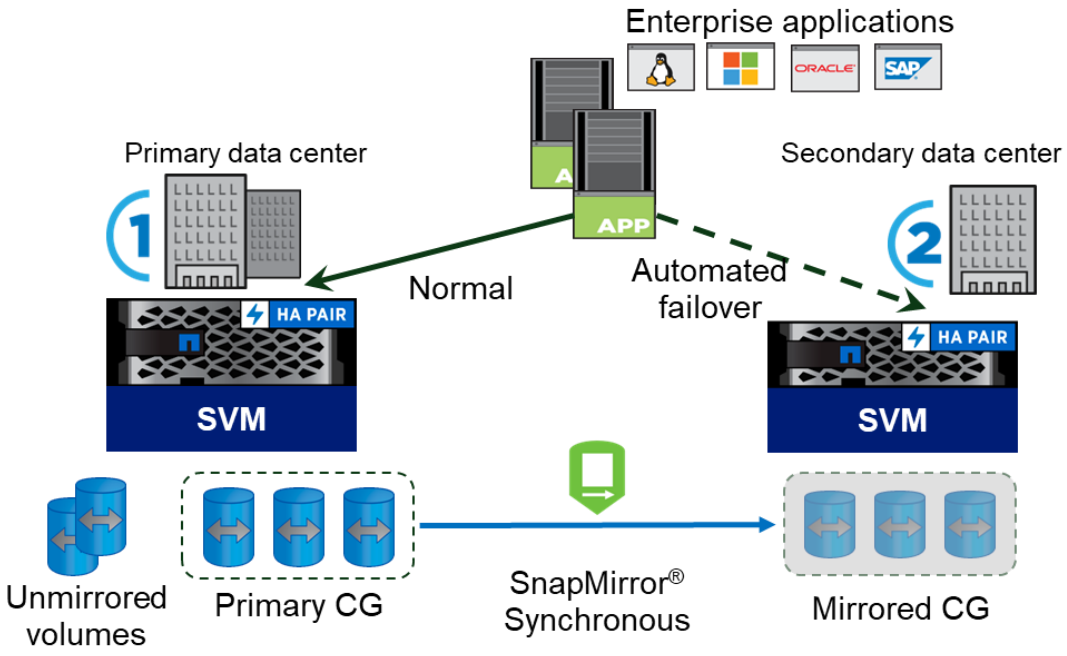
- SnapMirror® active sync (formerly SnapMirror® Business Continuity or SM-BC) delivers built-in business continuity and disaster recovery for nonstop data availability with zero RPO and RTO for continuous business operations.
- MetroCluster delivers continuous availability for all SAN and NAS applications by consolidating workloads on a dedicated solution that delivers bullet-proof reliability and performance at scale.

SnapMirror® active sync offers zero RPO and RTO using proven SnapMirror® active sync replication over IP networks to mirror NetApp clusters and systems from one data center to another over LAN or WAN across clusters or systems. End-to-end encryption encrypts back end traffic, such as NVlog and storage replication data, between the sites in a MetroCluster IP configuration.

MetroCluster offers zero RPO and what the industry refers to as zero RTO using FC or IP networks to distribute clusters across two locations. Both enable automatic failover for business-critical applications in virtual and physical environments without manual intervention. The primary difference is granularity. SnapMirror® active sync is based on specific datasets, which allows specific applications, servers, or other workloads to be failed over on an individual basis. In contrast, MetroCluster provides mirroring at the array layer, which delivers mirroring and failover for entire arrays as a single unit. This enables simple whole-infrastucture DR and BC protection.

** Strictly speaking, RTO=0 is impossible because an IO requires a nonzero amount of time to complete. The result is a disaster cannot be detected until at least a few seconds has elapsed. Furthermore, in many cases the host OS will wait through a timeout of up to 30 seconds before retrying a lost IO on the network, which effectively increases the RTO based on return to fully operational status. In general, RTO=0 is interpreted to mean nondisruptive to operations.*

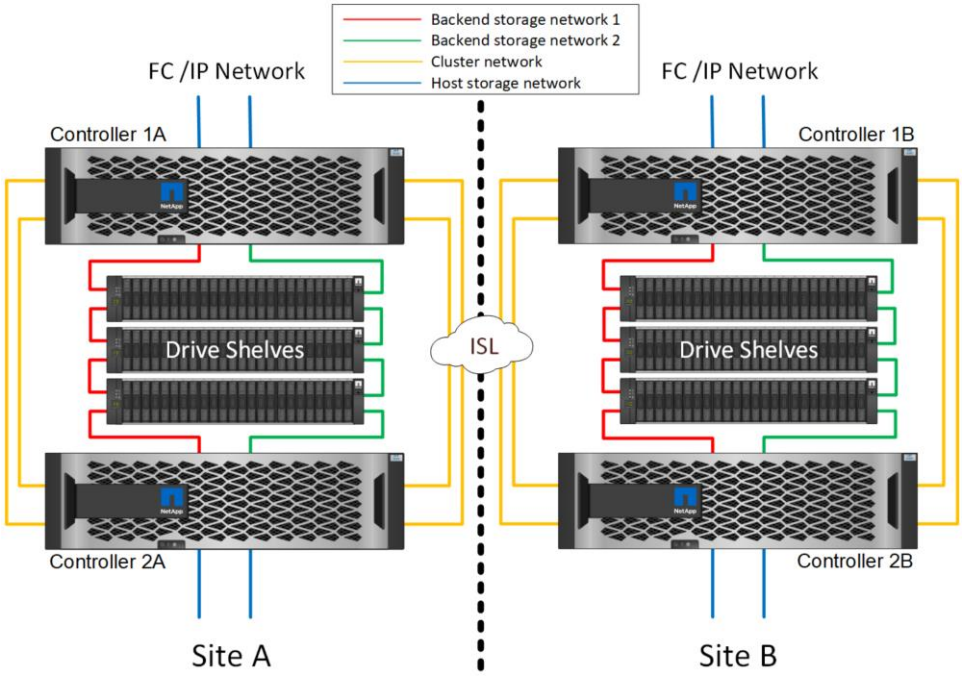
Figure 3) NetApp SnapMirror® active sync solution for business continuity.



SnapMirror® active sync is powered by a symmetric active-active architecture and proven synchronous replication technology that delivers cutting-edge resilience and performance for multisite protection with application-level granularity supporting zero RTP and RPO. With SnapMirror active sync, you get the peace of mind that comes with continuous data availability, delivered through a deployment that's easy to manage and cost-effective. Better yet, it's built in with NetApp ONTAP®-based storage systems as part of the ONTAP One software package, without the need for another software license.

SnapMirror® active sync enables mission-critical business services to continue operating even through a complete site failure with TAF to the secondary copy. No manual intervention or additional scripting is required to trigger this failover. TAF makes storage outages on-site completely agnostic to application and does not require any reconfiguration after a site disaster or storage outage. In other words, host access to storage is nondisruptive in the event of a site disaster or storage outage. For SAN, this requires the host MPIO to make a storage failover transparent to an application.

Figure 4) NetApp MetroCluster IP solution for business continuity.



In the event of a failure, MetroCluster manages the switchover process of providing access to NAS- and SAN-provisioned data at the other site within the protocol timeout periods or sooner, resulting in a zero RPO with applications continuing to access data without incurring failures. When MetroCluster is combined with similar application availability products, the complete solution provides a highly resilient architecture that can continue operating even in the event of a site-wide disaster. One example is using MetroCluster IP to provide storage availability and VMware vSphere Metro Storage Cluster (VMSC) to provide compute availability to continue operating even in the event of a complete site outage.

Learn more about NetApp business continuity with SnapMirror® active sync and MetroCluster.

Disaster recovery

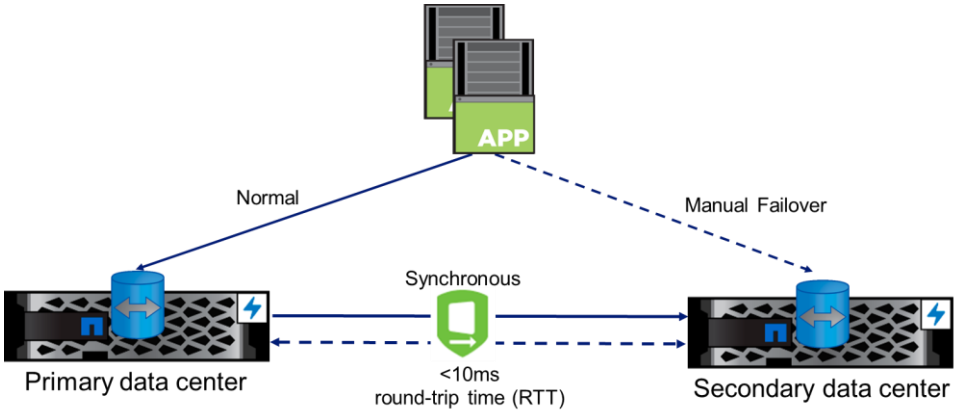
Businesses must be able to protect data from damaging natural or human-made events and recover it quickly when necessary. At the same time, they must maximize their investments to get the most out of their IT infrastructure. An effective data protection strategy is vital to prevent operations from stalling, which could result in lost productivity and revenue, and damage to company reputation. The most efficient data protection strategies even provide for the reuse of secondary data facilities for business intelligence or development and testing. In these scenarios, disaster recovery solutions can become business accelerators.

While MetroCluster and SnapMirror® active sync are business continuity solutions, not all customers require a complete BC solution. In such cases, SnapMirror® and SnapMirror® active sync are cost-effective, easy-to-use disaster recovery (DR) solutions that replicate data at high speeds over a local area network or metro area network. They provide high data availability and fast disaster recovery for business-critical applications such as Microsoft Exchange Server, Microsoft SQL Server, and Oracle, in both virtual and traditional environments.

- SnapMirror uses asynchronous mirroring across remote distances to support a low RPO and RTO.
- The companion data service, SnapMirror® Synchronous, uses synchronous mirroring across local distances to support a zero RPO and near-zero RTO.

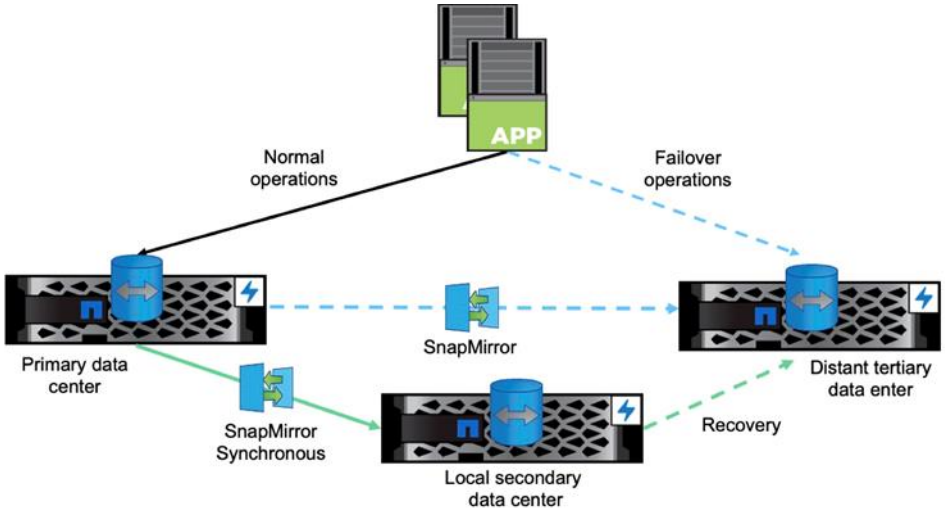
SnapMirror® and SnapMirror® active sync give businesses the flexibility to protect a subset of volumes in the cluster with replication between ONTAP storage systems of different models, capacities, and performance levels. As shown in Figure , a typical use case includes two data centers for disaster recovery of volumes from a primary data center to a secondary data center. If the primary site fails, the databases and applications can access the secondary data center for access to mirrored data and disaster recovery of databases and applications. The supported distances between data centers vary, with SnapMirror® active sync supporting a network connection with up to 10 milliseconds round trip time (RTT) and SnapMirror® supporting a network connection of any distance.

Figure 5) NetApp solution for disaster recovery using two data centers.



As shown in Figure , a second typical use case for SnapMirror® active sync and SnapMirror® includes three data centers for disaster recovery of volumes from a primary data center to a local secondary and remote tertiary data center. This involves SnapMirror® active sync mirroring of latency-sensitive data (such as logs) from the primary to the second data center and SnapMirror® asynchronous mirroring of other data (such as files) from the primary to the tertiary data center. If the primary data center fails, the databases and applications can access the secondary and tertiary data centers for access to mirrored data and disaster recovery of databases and applications.

Figure 6) NetApp solution for disaster recovery using three data centers.



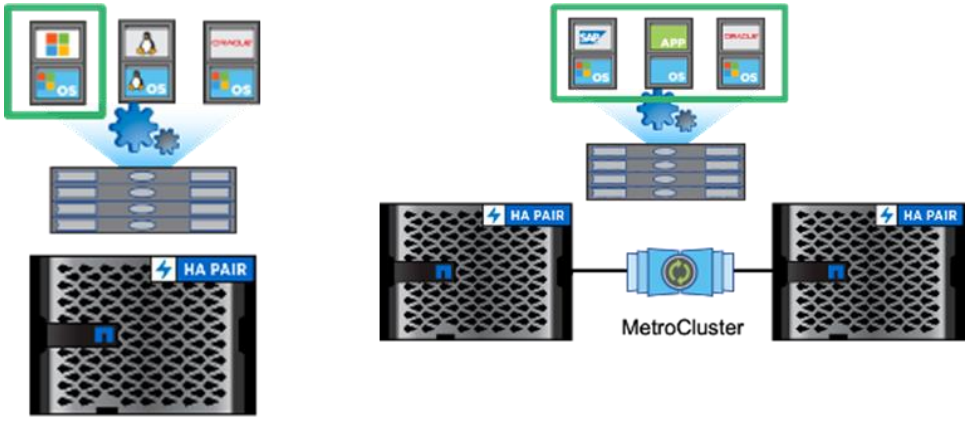
When using a three data center configuration, SnapMirror active sync and SnapMirror asynchronous support the automated and transparent failover and failback of applications between the primary to secondary data center as well as the automated failover and failback of asynchronous replica targets.

Learn more about NetApp disaster recovery with SnapMirror.

High availability

Businesses expect their databases and applications to be accessible always, even during storage component or data center site failures. As shown in Figure , NetApp offers two solutions for high availability (HA): high availability controller pairs for use within a data center and MetroCluster for use across two locations or data centers.

Figure 7) NetApp solutions for high availability.



NetApp storage clusters and systems use interconnected controller nodes configured as active-active HA pairs. If a node fails, or if a node is brought down for routine maintenance, its partner can take over its storage media access and continue to serve data until the offline node is brought back online. This continuity provides high availability through fault tolerance that supports nondisruptive operations during hardware and software upgrades, relocation of aggregate ownership, and hardware maintenance.

MetroCluster uses synchronous mirroring between two storage systems clustered together to achieve more robust high availability than HA pairs. This synchronous mirroring provides HA protection during more types of interruptions, including prolonged power outages or natural disasters, because MetroCluster supports rapid failover to a storage system with a copy of all data during catastrophic events. Cluster-level recovery with unplanned automatic switchover (failover) is supported when using the ONTAP Mediator service.

IDC reviewed NetApp ONTAP system availability statistics for the period from June to December 2019 (“Evolving Availability Requirements Demand More Than Just a Resilient Storage Infrastructure”). The report found that the data indicates a minimum of 99.99993% (6 nines) availability across the tens of thousands of controller pairs running ONTAP 9 software. This population includes NetApp AFF and FAS clusters and systems. IDC also found that although the latest NetApp systems deliver 100% data availability, not all workloads require that level. The flexibility of ONTAP gives customers the option to cost-effectively configure systems to meet the differing levels of availability that each workload requires within a single system.

Learn more about NetApp ONTAP high availability.

Non-disruptive firmware upgrades

The firmware of ONTAP system and cluster components can be upgraded without causing disruptions to clients. For example, firmware upgrades to solid-state drives and hard disk drives occur while they remain online.

ONTAP upgrades to controllers also occur non-disruptively to clients, with their systems and clusters remaining online, using an automated non-disruptive upgrade (ANDU) process. ANDU takes advantage of ONTAP's high-availability (HA) failover technology to ensure that clusters continue to serve data without interruption during the upgrade.

Learn more about firmware upgrades.

Automatic isolation of failed components

ONTAP storage systems and clusters offer robust automated isolation of failed components, including controllers and their components (e.g., IO cards, cables, etc.), shelves and their components (e.g., fans, power supplies, etc.), drives (i.e., solid-state drives and hard disk drives), and cluster network switches. High-availability pairs of nodes (HA pairs) can operate as a storage system and multiple HA pairs can operate as a storage cluster.

ONTAP clusters use quorum and epsilon to measure cluster health and function that together indicate how clusters address potential communications and connectivity challenges. In general, assuming reliable connectivity among the nodes of the cluster, a larger cluster is more stable than a smaller cluster.

Each node in the cluster participates in a voting protocol that elects one node master; each remaining node is a secondary. The master node is responsible for synchronizing information across the cluster. When quorum is formed, it is maintained by continual voting. If the master node goes offline and the cluster is still in quorum, a new master is elected by the nodes that remain online.

Because there is the possibility of a tie in a cluster that has an even number of nodes, one node has an extra fractional voting weight called epsilon. If the connectivity between two equal portions of a large cluster fails, the group of nodes containing epsilon maintains quorum, assuming that all of the nodes are healthy. Epsilon is automatically assigned to the first node when the cluster is created. If the node that holds epsilon becomes unhealthy, takes over its high-availability partner, or is taken over by its high-availability partner, then epsilon is automatically reassigned to a healthy node in a different HA pair.

When using MetroCluster, refer to ONTAP documentation for additional relevant information.

Dynamic cache memory read & write utilization

The cache (DRAM) of ONTAP storage systems operates globally within a controller and is available as a single unit across all IO ports. Its dynamic nature allows overall simplicity in management regardless of read and write access patterns. Also, ONTAP offers quality of service (QoS) capabilities that further support dynamic read and write optimization across three dimensions: 1) IOPS only, 2) throughput only, or 3) a combination of IOPS and throughput. ONTAP QoS supports customer-determined minimum and maximum limits, as well as patented adaptive QoS using system-determined dynamic limits that adapt to the system's configuration and workloads. Customer and system limits can be applied to a group of LUNs, a single LUN, or a virtual machine.

Backup and recovery

ONTAP storage includes built-in backup and restore capabilities that are accessed using NetApp BlueXP™, NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments. Although NetApp Backup and Recovery service is central to backup and recovery, it is enhanced when used with other NetApp products and services, including NetApp Classification and

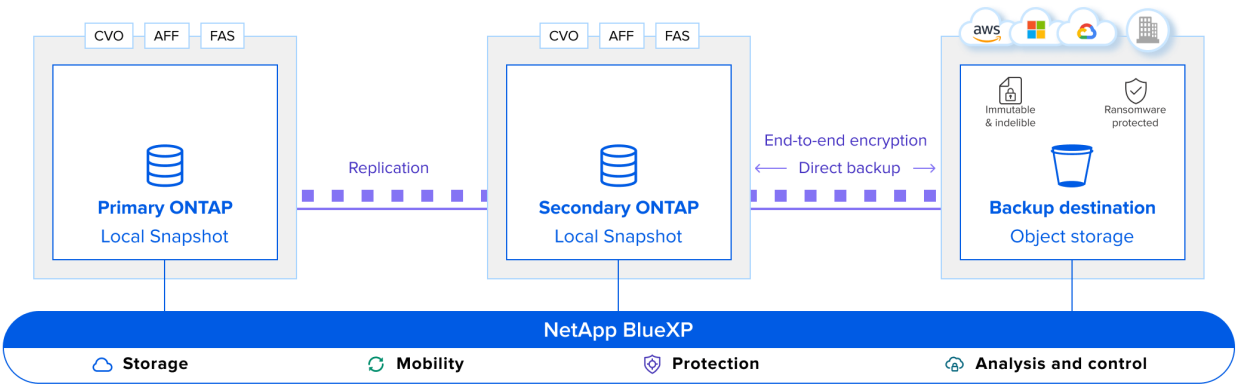
NetApp SnapCenter®. Of course, ONTAP storage is supported by third-party backup and recovery partners and software, including Commvault, Rubrik, and Veeam.

NetApp backup and recovery products and services include:

- NetApp Cloud Backup, a NetApp BlueXP™ cloud service that delivers simple, efficient, and secure backup and restore capabilities for the protection and long-term archiving of data from ONTAP storage to object storage provided by NetApp StorageGRID® object-based storage solution, AWS S3, Microsoft Azure Blob, and Google Cloud Storage.
- NetApp Classification (previously Cloud Data Sense), a NetApp BlueXP™ cloud service that uses artificial intelligence (AI) technology to classify, map, identify, and report on structured and unstructured data to improve visibility, gain insight, and support backup and recovery policy decision-making.
- NetApp SnapCenter, an ONTAP software component that enables database- and application-aware Snapshot™ copies and clones to shorten backup and recovery times for Microsoft SQL, Microsoft Exchange, Microsoft Windows, Oracle Database, SAP HANA Database, and VMware vSphere environments, as well as MySQL, DB2, MongoDB, Sybase, and PostgreSQL databases.

With the proven replication technology and complete automation and orchestration of the Backup and Recovery service, data is easily and efficiently backed up through secured and optimized transfers to an inexpensive, encrypted, and highly durable object store on-premises or in your public cloud accounts. By preserving storage efficiencies and performing block-level incremental updates forever, minimal data footprint is maintained end to end, further optimizing the costs. The impact on production is also reduced, resulting in optimized performance while meeting SLAs. Because it is independent of the backup source, data can be easily restored anytime and anywhere. With just a few simple operations, backup schedules and retention are all set, with streamlined architecture in place. Businesses gain more flexibility at a lower cost without requiring backup experts or needing to integrate third-party tools.

Figure 8) NetApp BlueXP™ solution for native backup and recovery for ONTAP workloads.



Learn more about NetApp backup and recovery.

Security and privacy

NetApp is committed to security certification to meet organizations' confidentiality, integrity, and data availability needs.

As the #1 provider of data storage and management to the U.S. Federal government, NetApp understands the importance of security. NetApp's history reflects an ongoing commitment to security certification and to the confidentiality, integrity, and availability needs of customers and partners.

Table 2) Major security and privacy certifications that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
NSA Commercial Solutions for Classified (CSfC)		X		X
DoD Approved Product List (DoDIN APL)		X		X
Common Criteria Certification (CISA)		X		X
NIST FIPS 140-2 Level 1 & 2		X		X
TLS v1.3 support		X		X

NetApp ONTAP is the first enterprise storage and data management platform to achieve Commercial Solutions for Classified (CSfC) validation – a cybersecurity program led by the U.S. National Security Agency – for data at rest. CSfC validates commercial IT products that have met the highest level of strict encryption standards and rigorous security requirements for both hardware and software solutions. With this validation, organizations around the globe can benefit from the robust security capabilities of ONTAP to protect information on-premises and in remote locations from foreign actors, ransomware attacks, and other data loss threats.

NetApp was the first enterprise storage and data management platform provider to:

- Achieve Commercial Solutions for Classified (CSfC) validation for data at rest
- Achieve Common Criteria (ISO/IEC 15408) certification
- Be certified and listed on the Unified Capabilities (UC) Approved Products List (APL), created by the United States Department of Defense

NetApp follows a security lifecycle model to ensure solution integrity. The ONTAP kernel and NetApp architecture provide reliability and security in the following ways:

- **Confidentiality.** Preventing unauthorized access to customer data
- **Integrity.** Preventing unauthorized changes to customer data
- **Availability.** Ensuring that customer data is available (resisting denial-of-service attacks)

NetApp products are equipped with strict role-based access control (RBAC) measures to control administrative access, as well as secure protocols, audit logging, and industry-standard encryption. Together, these features help to ensure secure products and solutions for our customers.

NetApp follows the ARC strategy (Accounts are assigned Roles and Roles are assigned Capabilities). This strategy enables the definition of sets of capabilities that are assigned to any user. Users are assigned to roles based on their job function, and each role is granted rule sets required to perform those functions.

Using this methodology, the only configuration an individual administrator must make is to ensure proper role assignment of the user or group. The user then inherits all the aligned capabilities and parameters assigned to those roles.

Using RBAC in NetApp's management console/dashboard leads to enhanced data protection through the concept of segregation of duties, also known as separation of duties. This concept prevents a single user

from affecting access to data or other objects, such as logical interfaces, by limiting access using the principle of least privilege.

The principle of least privilege states that a user or process should have the level of access required to perform his or her legitimate functions and no more. The principles of segregation of duties and least privilege are applied mostly in large IT departments with distributed responsibilities, but smaller environments can also take advantage of these features, particularly with system accounts and the processes and functions they perform. These principles prevent a security incident on one system from spreading to others.

NetApp provides comprehensive support for Transport Layer Security (TLS) and Lightweight Directory Access Protocol (LDAP). More ONTAP software and products are using TLS version 1.3 in place of TLS v1.2 to strengthen the privacy and security of data and communications moved across private and public networks, including the Internet. Examples of TLS v1.3 usage include NFS over TLS, Cluster Peering Encryption (CPE) with TLS, and ActiveIQ Transport using SMTP with TLS. Similarly, ONTAP currently uses LDAP version 2.5.16 to prevent incorrect vulnerability notifications and allow NetApp to provide a more streamlined deployment of security vulnerability fixes.

Learn more about NetApp product security and security certifications.

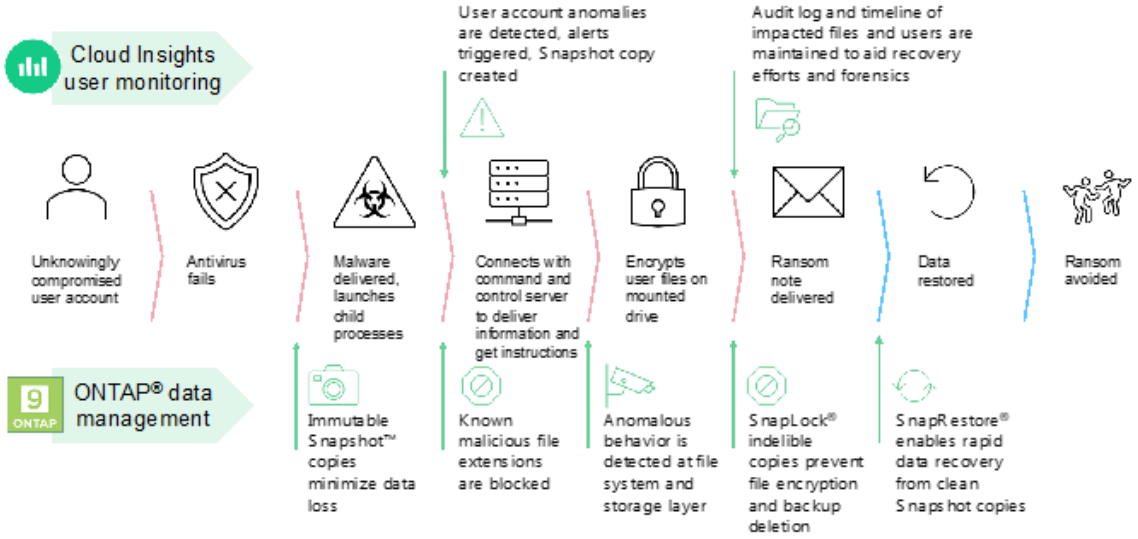
Ransomware protection

The evolution of today's threat landscape continues to present organizations with unique challenges for protecting their most valuable data and information. Ransomware is malware that prevents or limits the use of systems or resources until a ransom is paid. Ransomware attacks are one of the top cybersecurity threats an organization can face. The potential damage is not just the direct associated recovery cost, but also the effect on the company’s reputation and brand. Notably, the nature of the threat vectors is always changing and growing more widespread, and dormant malware can infect the environment weeks or months before it is activated.

Ransomware attacks can be generally placed into two categories:

- **Denial of service** ransomware uses a strategy where the attacker gets someone to inadvertently download a program (ransomware) that encrypts all accessible files on the corporate network. The attacker demands a ransom payment to provide the decryption key to regain access to data.
- **Data exfiltration** ransomware uses a strategy where the attacker gains access to a company’s IT systems, moving sensitive data to an unknown location outside of the company. The attacker threatens to publicly release that data unless a ransom is paid.

Figure 9) Anatomy and prevention of a ransomware attack.



Ransomware detection needs to occur as early as possible to prevent its spread and avoid costly downtime. However, an effective ransomware detection strategy should include more than a single layer of protection. A good analogy for this is the crash safety features of a vehicle. Drivers don't want to rely on a single feature, such as a seatbelt, for protection in an accident. Airbags, antilock brakes, and forward-collision warnings are additional safety features that can result in a much better outcome. Ransomware protection should be viewed in the same way.

Table 3) Major ransomware capabilities that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Identify		X		X
Protect		X		X
Detect		X		X
Respond		X		X
Recover		X		X

For example, NetApp FPolicy in combination with NetApp Cloud Insights, or similar capabilities from our partners, does an excellent job of detecting ransomware through user behavioral analytics (UBA). The software looks for potential ransomware attacks from the aspect of an individual user's behavior. Hijacking a single user account is just one avenue a hacker might take when launching a ransomware attack; malicious actors are constantly evolving their attack techniques.

NetApp Active IQ® also provides additional layers of detection for ransomware. Active IQ® checks NetApp ONTAP systems for adherence to NetApp configuration best practices, such as enabling FPolicy. Active IQ® Unified Manager generates alerts for abnormal growth of NetApp Snapshot copies or storage efficiency loss, which can indicate potential ransomware attacks.

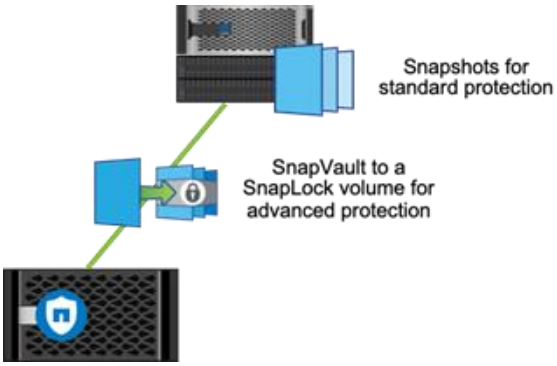
This is where the anti-ransomware feature in ONTAP 9.10.1 and later comes into play. It leverages built-in on-box machine learning that looks at volume workload activity plus data entropy to automatically

detect ransomware. It monitors activity that is different from UBA, so that it can detect attacks that UBA does not.

Visibility and detection are crucial for ransomware protection. If malware is moving through storage and encrypting files, rates of data change increase, storage efficiencies such as deduplication and compression decrease, and Snapshot sizes increase. Such changes are key indicators of malware activity, so NetApp provides monitoring tools that can help to identify these patterns. And in recent ONTAP releases, autonomous ransomware protection ensures that a Snapshot copy is automatically initiated when behavioral anomalies are detected using UBA.

Remediation of ransomware involves restoring Snapshot copies or backups that are known to be uninfected. NetApp immutable Snapshot copies make it possible to rapidly and efficiently recover (rollback) while databases and applications are running. NetApp SnapRestore® data recovery software can recover a single file or entire data volumes and enables the automation of data recovery. The SnapRestore data recovery process is nearly instantaneous and is independent of the storage capacity or the number of files restored. Snapshot technology is the foundation for SnapRestore, SnapLock®, SnapVault®, SnapMirror, and SnapManager®, all of which provide different capabilities to the Snapshot technology portfolio.

Figure 10) NetApp solution for ransomware protection.



Given the threat of ransomware and its ability to infiltrate or infect files, it's important to understand the immutability of NetApp Snapshot copies. In addition to being read-only, the NetApp SnapLock solution can be leveraged to add Snapshot copies on a specified cadence and automatically discard the copies that have aged out. This ensures that the copies cannot be changed, renamed, or deleted until they are aged out, based on the administrator's configured policy. This solution effectively adds an additional layer of immunity to threats such as ransomware.

Learn more about NetApp cyber-resiliency and ransomware protection and the NetApp Ransomware Recovery Guarantee.

Hardware

NetApp ASA and AFF clusters and systems use NVMe end to end. The newest ones also use PCIe Generation 4 (such as AFF A900), and generally consist of active-active, high-availability controller pairs, drive shelves, drives, fabric switches (for clusters only), and cabling installed in system cabinets (rack cabinets). NetApp systems are configured for SAN-only (ASA) or unified SAN and NAS (AFF) operations to match customer requirements and support the same controllers, drive shelves, and drives. NetApp FAS uses different controllers, drive shelves, and drives than AFF and ASA. In general, all ONTAP clusters support the same fabric switches and system cabinets.

Table 4) Controller, drive shelf, and fabric switch hardware.

	NetApp ASA A-Series	NetApp ASA C-Series	NetApp AFF A-Series	NetApp AFF C-Series	NetApp FAS
Controllers	A1K, A90, A70, A900, A800, A400, A250, A150	C800, C400, C250	A1K, A90, A70, A900, A800, A400, A250, A150	C800, C400, C250	FAS90, FAS70, FAS500f, FAS9000, FAS8700, FAS8300, FAS2750, FAS2720
Drive shelves	NS224				DS224C, DS212C, DS460C
Fabric switches	Broadcom BES-53248, Cisco Nexus 9336C-FX2, NVIDIA SN2100				

Learn more about NetApp NVMe and AFF solutions.

Active-active controllers

The controllers used by NetApp AFF, ASA, and FAS clusters and systems include many field-replaceable units (FRUs), which contributes to improved availability and serviceability. Except for the controller chassis, all FRUs are generally redundant and hot-swappable to protect availability and serviceability. For chassis fault tolerance, MetroCluster can be used, which also provides geographic separation. However, the NetApp AFF, ASA, and FAS clusters and systems support non-disruptive controller hardware upgrades that allow controller chassis field replacement without interrupting data access.

Table 5) Major controller components that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Redundant hot-swap controller modules	X	X	X	
Redundant hot-swap internal drives	X	X	X	
Redundant hot-swap power supplies	X	X	X	
Redundant hot-swap fan modules	X	X	X	
Redundant hot-swap SAN cables	X	X	X	
Redundant hot-swap NAS cables	X	X	X	
Redundant hot-swap interconnect cables	X	X	X	
Redundant hot-swap power cables	X	X	X	

	Reliability	Availability	Serviceability	Security
Replaceable controller chassis	X	X (with MetroCluster)	X	

Serviceability is increased because the following items on redundant hot-swap controller modules are FRUs (see Table). Availability is increased because these items can be non-disruptively replaced without affecting cluster or system availability when controllers are configured to best practices as HA pairs.

Table 6) Field replaceable units on controller modules.

System DIMM	NVDIMM battery	PCIe cards
Caching module	RTC battery	Mezzanine cards
NV battery module	Boot media (drive)	LED USB modules
NVDIMM/NVMEM/NVRAM	I/O modules	Fastening hardware

Nondisruptive controller software updates

NetApp AFF, ASA, and FAS clusters support using BlueXP™ for nondisruptive updates of controller ONTAP software and system firmware to improve reliability, availability, serviceability, and security. A cluster or individual nodes can be updated in high-availability (HA) pairs to a version of ONTAP software without disrupting access to client data. An automated rolling update is performed for clusters with fewer than 8 nodes, and an automated batch update is performed for clusters with more than 8 nodes.

Nondisruptive controller hardware upgrades

The controller hardware can be nondisruptively upgraded on a pair of nodes running ONTAP by migrating nonroot aggregates from the original nodes to the new nodes in the same cluster. The data hosted on the nodes that are being upgraded is accessible during the upgrade. This procedure uses a method called aggregate relocation, which takes advantage of the HA configuration to enable moving ownership of nonroot aggregates from one node to another if they share storage within the same cluster.

In general, the automated process involves six stages:

- Stage 1: Upgrade the node pair.
- Stage 2: Relocate and retire node1.
- Stage 3: Install and boot node3.
- Stage 4: Relocate and retire node2.
- Stage 5: Install and boot node4.
- Stage 6: Complete the upgrade.

NVMe drive shelf

NetApp AFF and ASA systems and clusters support end-to-end NVMe when used with model NS224 NVMe drive shelves and supported NVMe drives. NS224 drive shelves allow nondisruptive addition or removal from supported clusters and HA systems. Each drive shelf occupies two units of rack space and supports up to twenty-four 2.5-inch small form factor NVMe SSDs. Using self-encrypting drives (SEDs) or FIPS 140-2 compliant drives contributes to data security.

Table 7) Major NVMe drive shelf components that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Redundant hot-swap drives	X	X	X	X (with SEDs)
Redundant hot-swap power supplies	X	X	X	
Redundant hot-swap fan modules	X	X	X	
Hot-swap shelf DIMM	X	X	X	
Hot-swap RTC battery	X	X	X	
Hot-swap boot media	X	X	X	
Hot-swap NSM module	X	X	X	
Replaceable drive chassis	X		X	

Nondisruptive NVMe drive shelf addition and removal

When additional NVMe storage is needed, an NS224 drive shelf can be hot added after the HA pair meets certain requirements, and after the preparation tasks applicable to the HA pair are completed.

To add an NVMe drive shelf, the shelf is installed into a rack or cabinet, the two redundant power cords are connected (which automatically powers on the shelf), and the shelf ID is set to a unique value. Then each NVMe drive shelf is cabled by hot adding so that each shelf has two redundant connections to each controller module in the HA pair. Finally, drive ownership is assigned automatically or manually.

To move or replace one or more disk shelves, a disk shelf is hot removed (nondisruptively removed from a system that is powered on and serving data with I/O in progress).

Nondisruptive NVMe drive addition and removal

NVMe drives support hot swapping, which allows them to be nondisruptively added and removed, including live drive ownership reassignment.

To add an NVMe drive, locate an unused drive slot in an NVMe drive shelf, move the drive cam handle to the open position, and use both hands to guide and insert the drive into the shelf until it stops. Then close the cam handle to secure the drive in the shelf. Finally, drive ownership can be automatically or manually assigned.

To remove an NVMe drive, locate the drive in its drive shelf, press the release button on the drive face, and open the cam handle. Then slide the drive out of the shelf using the cam handle, while physically supporting the drive.

SAS drive shelf

NetApp FAS systems and clusters deliver balanced performance and capacity by using hybrid storage technology when used with model DS224C, DS212C, and DS460C SAS drive shelves. SAS drive shelves configured with IOM12 modules allow nondisruptive addition or removal from supported clusters and HA systems. Using self-encrypting drives (SEDs) or FIPS 140-2 compliant drives contributes to data security.

Table 8) Major SAS drive shelf components that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Redundant hot-swap internal drives	X	X	X	X (with NSE)
Redundant hot-swap power supply	X	X	X	
Redundant hot-swap fan module	X	X	X	
Redundant hot-swap IOM12 module	X	X	X	
Replaceable drive drawer	X		X	
Replaceable drive chassis	X		X	

Nondisruptive SAS drive shelf addition and removal

When additional SAS storage is needed, a DS224C, DS212C, or DS460C drive shelf can be hot added.

To add a SAS drive shelf, the shelf is installed into a rack or cabinet, Drive ownership is assigned automatically or manually.

To move or replace one or more disk shelves, a disk shelf is hot removed (nondisruptively removed from a system that is powered on and serving data with I/O in progress).

Nondisruptive SAS drive addition and removal

SAS drives support hot-swapping, which allows them to be nondisruptively added and removed, including live drive ownership reassignment.

Fabric switches

NetApp AFF, ASA, and FAS are configured as multimode clusters (2- to 24-node switched clusters) or HA pairs (2-node switchless clusters). Switched clusters require a cluster network consisting of a redundant pair of supported fabric switches and redundant cables. System- and cluster-level reliability, availability, serviceability, and security are similar for switchless and switched clusters. Redundant fabric switches support availability and serviceability by using redundant hot-swap power supplies and fan modules plus replaceable switch enclosures.

Table 9) Major fabric switch major components that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Broadcom BES-53248 fabric switch				
Redundant hot-swap power supplies	X	X	X	
Redundant hot-swap fan modules	X	X	X	
Replaceable switch enclosure	X		X	
Cisco Nexus 9336C-FX2 fabric switch				
Redundant hot-swap power supplies	X	X	X	
Redundant hot-swap fan modules	X	X	X	
Replaceable switch enclosure	X		X	
NVIDIA SN2100 fabric switch				
Redundant power supplies	X	X		
Redundant fan modules	X	X		

System cabinets

Designed to ensure that controllers, drive shelves, and fabric switches have the environment they need for proper operation, system cabinets provide equipment support, redundant power, cooling ventilation, and physical security for NetApp systems and clusters. Each cabinet typically includes front and rear doors, side panels, power distribution units (PDUs), and optional cabinet interconnect and bolt-down kits.

Table 10) Major system cabinet components that are relevant to RASS.

	Reliability	Availability	Serviceability	Security
Redundant power distribution units	X	X	X	
Perforated and lockable front door	X		X	X
Perforated and lockable rear door	X		X	X
Lockable left and right side panels	X		X	X
Passive blanking air control panels	X		X	
Cabinet interconnect and bolt-down kits	X			X

Redundant power distribution units

When the power distribution units installed in system cabinets are configured to best practices as one or two matched pairs, the resulting redundancy allows a PDU to fail without causing system downtime, and the PDU can be nondisruptively serviced or replaced. NetApp offers a variety of (PDUs to support different global data center power sources and system cabinet installed-equipment power requirements. Depending on these requirements, each system cabinet includes two or four PDUs to support the availability and serviceability of system cabinets and installed equipment. Each PDU offers multiple outlets to support dedicated connections to installed equipment.

Perforated and locking system cabinet front door

System cabinet front doors are perforated to support equipment cooling for increased reliability, and they include physical keyed locks to prevent unauthorized access for increased physical security. Each system cabinet uses a common key that authorized people must have in their possession and use to open a locked system cabinet front door. The system cabinet's common key is unique to each cabinet, and opens all doors and side panels. This key management and control further increase security.

Perforated and locking system cabinet rear door

The rear doors of system cabinets are vertically split into two parts to improve serviceability, and they are perforated to support equipment cooling, which increases reliability. They include physical keyed locks to prevent unauthorized access for increased physical security. Each system cabinet uses a common key that authorized people must have in their possession and use to open a locked system cabinet rear door. The system cabinet's common key is unique to each cabinet and opens all doors and side panels. This key management and control further increase security.

Locking system cabinet side panels

The side panels of system cabinets are removable to improve serviceability, and they include physical keyed locks to prevent unauthorized access for increased physical security. Each system cabinet uses a common key that authorized people must have in their possession and use to open a locked system cabinet side panel. The system cabinet's common key is unique to each cabinet and opens all doors and side panels. This key management and control further increase security.

Blanking panels

System cabinet blanking panels control air circulation and flow to increase the reliability of installed equipment. They are temporarily removable to improve serviceability by facilitating physical access to the system cabinet components and installed equipment. They contain no active parts that could lower availability by failing or lower serviceability by requiring replacement. Best practices involve installing a blanking panel in system cabinet locations without an installed controller, drive shelf, fabric switch, or other equipment.

Cabinet interconnect and bolt-down kits

The size (about 80 inches high, 50 inches deep, and 24 inches wide) and weight (about 400 pounds empty and up to 2,700 pounds with equipment) of system cabinets are significant. Bolt-down kits attach system cabinets to the floor to improve physical security by preventing unauthorized movement and safety by preventing unintended movement. Cabinet interconnect kits attach adjacent system cabinets together to similarly improve physical security and safety. These kits contain no active parts that could lower availability by failing or lower serviceability by requiring replacement.

Software

As the industry-leading enterprise data management software, NetApp ONTAP software seamlessly manages data as it flows to and from wherever it's needed, including the edge, core, and cloud. This flow helps to create a smart, powerful, and trusted data fabric that reduces costs, accelerates critical workloads, protects data, and secures it across the hybrid cloud on-premises and in multiple public clouds, including AWS, Microsoft Azure, and Google Cloud.

ONTAP software

NetApp ONTAP data management software offers unified storage for applications that read and write data using block, file, or object protocols, in storage configurations that range from high-speed flash to lower-priced spinning disk to cloud-based object storage. ONTAP implementations run on NetApp engineered appliances (AFF, ASA, or FAS); on commodity hardware (ONTAP Select); in private, public, and hybrid clouds (NetApp Private Storage or Cloud Volumes ONTAP); and as native data services within AWS and Azure. Specialized implementations offer best-in-class converged infrastructure (FlexPod® Express or FlexPod Datacenter) and access to third-party storage arrays (NetApp FlexArray® storage virtualization software). Together these implementations form the basic framework of a data fabric, with a common software-defined approach to data management and fast, efficient replication across platforms.

With ONTAP, storage can be flexibly deployed while enterprise data management is unified across all of the deployments. This flexibility allows the design of storage environments across the widest range of architectures to match the approach that's right for evolving business needs:

- On NetApp all-flash AFF ASA clusters and systems for performance-demanding workloads
- On NetApp hybrid FAS clusters and systems for a balance of performance and capacity
- Within a converged infrastructure as a FlexPod solution from NetApp and Cisco
- As software-defined storage on commodity servers as NetApp ONTAP Select
- Across multiple public clouds as NetApp Cloud Volumes ONTAP
- Natively within hyperscalers as AWS FSx for NetApp ONTAP, Azure NetApp Files and Google Cloud NetApp Volumes

Table 11) ONTAP software services that are relevant to RASS.

FabricPool	SnapCenter®	SnapMirror® Cloud
FlexCache®	SnapLock®	SnapRestore®
FlexClone®	Volume encryption	Snapshot™
FlexGroup	SnapMirror® (asynchronous)	Storage encryption
FlexVol®	SnapMirror® Synchronous	
MetroCluster™	SnapMirror® active sync	

Learn more about NetApp topologies with multiple data centers.

FabricPool

Reliability	Availability	Serviceability
Preserves drive service life by lowering workloads	Lowers storage cost without changing data protection	Allows moving unused data offsite during service

FabricPool is an ONTAP feature that automatically tiers data between a high-performance tier and a lower-cost tier based on access patterns. Tiering frees up higher-performance storage for hot data while keeping cold data readily available from lower-cost object storage. FabricPool constantly monitors data access and moves data between tiers to optimize performance and cost. It works at the storage block level, so it works with both file and LUN data. Also, databases and applications using the data are not affected by the tiering, so no changes to databases or applications are needed. Tiering is fully automatic, so no ongoing administration is needed. Using FabricPool to tier cold data to the cloud is one of the easiest ways to gain cloud efficiency and create a hybrid cloud configuration.

Learn more about NetApp FabricPool.

FlexCache

Reliability	Availability
Preserves drive service life by lowering workloads	Improves storage performance without changing protection

FlexCache software accelerates read performance for hot datasets by increasing data throughput within a cluster. It also improves the speed and productivity of collaboration across multiple locations by caching actively read datasets within a cluster and at remote sites. FlexCache works by creating sparsely populated NFS and SMB file volumes (FlexCache volumes) that directly serve read requests if the FlexCache volume contains the data requested, while write requests are directly served by origin volumes. FlexCache volumes help improve performance, especially when clients need to access the same data repeatedly because the data can be served directly without having to access the origin volume. Also, FlexCache volumes cache a directory listing for "file not found" errors to reduce origin volume calls for files that no longer exist.

Learn more about NetApp FlexCache.

FlexClone

Reliability	Availability	Serviceability	Security
Preserves drive service life by lowering workloads	Increases utilization using space-efficient LUN and file copies	Supports system maintenance using temporary copies	Protects data using fully independent volumes copies

FlexClone works with FlexVol to create two types of FlexClone volumes: read-write point-in-time copies of a parent volume that can increase storage utilization for better availability; and point-in-time copies of data protection volumes that can increase redundancy for better serviceability. Whenever a FlexClone volume is created, each cloned volume gains a unique encryption key that is independent of the FlexVol (host) encryption key. A FlexClone volume can be split from its parent volume to create a fully independent FlexVol volume with its own disk space, instead of sharing disk space with its parent. Also, FlexClone can be used to create FlexClone files and FlexClone LUNs that are writable and space-efficient clones of parent files and parent LUNs to improve the efficient utilization of the physical aggregate space.

Learn more about NetApp FlexClone.

FlexGroup

Availability	Serviceability
Automates cluster load distribution to improve scalability	Unifies namespaces to simplify cluster management

FlexGroup volumes enable a single NAS volume of virtually unlimited size to be presented using a single namespace that spans multiple in-use controllers across a cluster. Each FlexGroup volume is a scale-out NAS container that includes several constituents transparently sharing traffic to provide high capacity and high performance along with automatic load distribution and scalability. A FlexGroup volume can be provisioned automatically because ONTAP creates and configures a FlexGroup volume by automatically selecting the aggregates based on the best practices for optimum performance, which further improves availability and serviceability. Alternatively, a FlexGroup volume can be created by manually selecting the aggregates on which the FlexGroup volume must be created, and then specifying the number of constituents on each aggregate.

Learn more about NetApp FlexGroup.

FlexVol

Reliability	Availability	Serviceability	Security
Perform tasks on individual FlexVol volumes rather than entire file systems	Optimize services like Snapshot copies for individual FlexVol volumes	Take individual FlexVol volumes offline to perform administrative tasks	Save time by backing up and restoring individual FlexVol volumes

FlexVol volumes enable the management of the logical layer of the file system independently of the physical layer of storage. Multiple FlexVol volumes can exist within a single separate, physically defined aggregate structure of disks and RAID groups. FlexVol volumes contained by the same aggregate share the physical storage resources, RAID configuration, and plex structure of that aggregate.

Learn more about NetApp FlexVol.

MetroCluster

Reliability	Availability	Serviceability
Protects against local and remote data center failures	Administrators can recover from data center disasters	Synchronous data mirroring supports data center servicing

The MetroCluster robust infrastructure combines array-based clustering with synchronous mirroring to deliver continuous availability and zero data loss for SAN and NAS workloads running on nodes that are separated by distances up to 700km. This helps to maintain storage business continuity for critical enterprise databases, applications, and workloads if a data center disaster occurs. MetroCluster uses physically separated and synchronously mirrored clusters of ONTAP storage to protect data on local and cluster levels. Each cluster synchronously mirrors the data and storage virtual machine (SVM) configuration of the other. When a disaster occurs at one site, an administrator can activate the mirrored SVM and begin serving the mirrored data from the surviving site. Additionally, the nodes in each cluster are configured as an HA pair, providing a level of local failover.

Learn more about NetApp MetroCluster.

NetApp Storage Encryption

Security
Protects data with FIPS 140-2 level 2 hardware encryption

NetApp Storage Encryption (NSE) delivers full-disk AES 256-bit encryption for data at rest with no operational impact. NSE uses self-encrypting drives (SEDs) that are FIPS 140-2 level 2 certified for hardware-based transparent disk encryption. In addition, NetApp Storage Encryption combines with NetApp Volume Encryption (NVE) software-based AES 256-bit encryption, providing two-layer hardware and software encryption for data at rest. NSE is one component of NetApp's unique approach to data-at-rest encryption that is compliant with FIPS 140-2 Level 2 requirements and has achieved NSA CSfC validation.

Learn more about NetApp Storage Encryption.

NetApp Volume Encryption

Security
Protects data with 2-layer AES 256-bit software encryption

NetApp Volume Encryption (NVE) is a software-based, data-at-rest AES 256-bit encryption feature that allows ONTAP to encrypt data and to have that data stored on disk without requiring self-encrypting drives. Similarly, NetApp Aggregate Encryption (NAE) is an enhancement of NVE that allows ONTAP to encrypt data for each volume with the keys shared for the aggregate. Customers can use any existing disk with NVE and NAE, including NetApp Storage Encryption (NSE) drives with hardware-based encryption for double or layered encryption. NVE is one component of NetApp's unique approach to data-at-rest encryption that is compliant with FIPS 140-2 Level 2 requirements and has achieved NSA CSfC validation.

Learn more about NetApp Volume Encryption and Aggregate Encryption.

Snapshot

Availability	Serviceability	Security
Creates instant point-in-time copies of data	Helps protect data during servicing	Recovers data instantly from immutable copies

Snapshot copies are read-only, point-in-time images of a volume. Snapshot copies consume minimal storage space and incur negligible performance overhead because they record only changes since the last copy was made. Snapshot copies owe their efficiency to NetApp WAFL®, the ONTAP' core storage virtualization technology. Like a database, WAFL uses metadata to point to actual data blocks on disk. But unlike a database, WAFL does not overwrite existing blocks; rather, it writes updated data to a new block and changes the metadata. Snapshot copies are so efficient because ONTAP references metadata when it creates the copy, rather than copying data blocks. Doing so eliminates the seek time that other systems incur in locating the blocks to copy, as well as the cost of making the copy itself. Snapshot copies can be used to recover individual files or LUNs, or to restore the entire contents of a volume. That's because ONTAP compares pointer information in the Snapshot copy with data on disks to reconstruct the missing or damaged object, without downtime or a significant performance cost. A Snapshot policy defines how the system creates copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, how to name them, and how to label them for replication.

Learn more about NetApp Snapshot copies.

SnapRestore

Availability	Serviceability	Security
Instantly recovers data from point-in-time Snapshot copies	Helps protect data during servicing	Restores data to a specific point-in-time to "undo" changes

SnapRestore data recovery software instantly restores single files, directories, or entire LUNs and volumes to a point in time preserved by an available Snapshot copy. Files can be restored from an NFS or CIFS client as well as from the storage system. Users on an NFS or CIFS client can use SnapRestore to restore a file directly from a Snapshot copy without the intervention of a storage system administrator. Users can restore the file to a different location in the parent read-write volume to avoid replacing an existing file.

Learn more about NetApp SnapRestore.

ONTAP features

There are too many ONTAP features to individually describe in this paper. This section describes a few of the many features that are relevant to RASS.

Data protection against simultaneous drive failures with RAID-TEC and RAID DP

Reliability	Availability	Serviceability
Prevents cluster and system errors during multidrive failures	Data remains accessible during failure and recovery	Allows simultaneous replacement of multiple drives

ONTAP protects against the risk of data loss due to drive failure by using specialized RAID protection options. NetApp RAID-TEC™ uses triple parity, which allows ONTAP to use up to three spare disks to replace and reconstruct the data from up to three simultaneously failed disks within the RAID group. NetApp RAID DP® uses double-parity, which allows ONTAP to use up to two spare disks to replace and

reconstruct the data from up to two simultaneously failed disks within the RAID group. The use of RAID-TEC and RAID DP is verified by industry-standard benchmark data to have a negligible performance impact, so users can convert from RAID DP to RAID-TEC and from RAID-TEC to RAID DP when data protections requirements change.

ONTAP storage clusters and systems automatically select either RAID-TEC or RAID DP for aggregates (that is, a collection of disks or partitions arranged into one or more RAID groups), depending on factors including drive capacity. This results in aggregates that contain larger disks and therefore have a higher possibility of concurrent disk failures when using RAID-TEC.

Learn more about NetApp RAID-TEC and RAID DP.

Workload performance protection with adaptive QoS

Reliability	Availability
Prevents performance-related DB and app errors	Ensures specific performance for storage workloads

Adaptive quality of service (AQoS) uses throughput floor and ceiling (minimum and maximum) policies to set throttle limits for individual workloads. A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS or MBps. A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MBps. AqoS automatically scales the policy group value to workload size, maintaining the ratio of IOPS to TBs/GBs as the size of the workload changes, which provides a significant advantage when managing hundreds or thousands of workloads in a large deployment.

AqoS ensures that the performance of critical workloads is not degraded by competing workloads by setting a throughput ceiling on a competing workload to limit its impact on system resources. Also, AqoS can ensure that a critical workload meets minimum throughput targets regardless of demand by competing workloads by setting a throughput floor. A ceiling and floor can even be set for the same workload.

Learn more about NetApp adaptive QoS.

Autonomous Ransomware Protection with AI detection engine

Availability	Serviceability	Security
Minimizes interruption to data access by ransomware attacks	Enables rapid recovery from ransomware	Automates ransomware attack detection and reponse

Autonomous Ransomware Protection (ARP) uses NAS (NFS and SMB) workload analysis and an artificial intelligence (AI) detection engine to proactively detect and warn about abnormal activity that might indicate a ransomware attack with 99% precision (accurate alerts) and 99% recall (99% accurate detection). ARP automatically determines the optimal learning period interval and automates the switch, usually within 30 days. ARP is designed to protect against denial-of-service attacks where the attacker withholds data until a ransom is paid (i.e., ransomware attacks). ARP can detect the spread of most ransomware attacks after only a small number of files are encrypted, take action automatically to protect data, and alert you that a suspected attack is happening.

Learn more about Autonomous Ransomware Protection.

Dynamic Authorization to increase the security of remote access

Availability	Serviceability	Security
Provides user access from trusted devices depending on trust scores	Supports a visibility mode to test configurations	Configurable options support customization of defaults

Administrators can configure and enable Dynamic Authorization to increase the security of remote access to ONTAP while also mitigating potential damage that could be caused by a malicious actor. ONTAP Dynamic Authorization provides an initial framework for assigning a security score to users and, if their activity looks suspicious, challenging them with additional authorization checks or denying an operation completely. Administrators can create rules, assign trust scores, and restrict commands to determine when certain activity is allowed or denied for a user. Administrators can enable Dynamic Authorization cluster-wide or for individual storage VMs.

Learn more about Dynamic Authorization.

Multi-Admin Verification defends against internal threats

Availability	Serviceability	Security
Prevents malicious actors from compromising data access	Ensures service actions are approved by multiple admins	Prevents a single administrator from damaging or deleting data

Multi-Admin verification (MAV) helps to prevent data loss by defending against insider threats (rogue administrators) and compromised credentials by requiring multiple administrators to approve commands that can potentially destroy data, including volume and snapshot deletion. The MAV framework is extensible and regularly updated to offer additional protection from malicious insiders. Recent enhancements prevent cluster-level, storage, system-level, snapshot creation, and other commands from executing without approval from multiple administrators.

Learn more about Multi-admin Verification.

SnapCenter

Availability	Serviceability	Security
Instant data protection that is DB- and app-aware	Instant cloning of live databases and applications	Instant recovery of DB- and app-aware backups

SnapCenter is software for the database- and application-aware data protection of ONTAP storage. It supports Snapshot copy locking (also known as tamperproof snapshots) to prevent modifications to protected data and boost data security and compliance with SnapLock features to keep your data even safer. It simplifies data protection lifecycles by offloading Snapshot, backup, restore, and clone tasks to application owners without sacrificing the ability to oversee and regulate activity on the storage systems.

SnapCenter enables increased storage performance and data availability, as well as reduced database and application testing and development times, by leveraging ONTAP data management. Supported enterprise environments include DB2, Microsoft Exchange Server, Microsoft SQL Server, Microsoft Windows Server, MySQL, MongoDB, Oracle Database, PostgreSQL, SAP HANA, Sybase, and VMware.

SnapCenter 5.0 offers the unified management and automation capabilities of SnapCenter to extend your protection beyond Cloud Volumes ONTAP® hosted in AWS (Amazon Web Services) and Azure, into first-party services from AWS (Amazon FSx for ONTAP) and Microsoft (Azure NetApp Files).

Learn more about NetApp SnapCenter.

SnapLock

Availability	Serviceability	Security
Preserves data accessibility based on unalterable policy	Eliminates malicious destruction and mistaken deletion	Data is immutable and protected from cyber threats

SnapLock software delivers high-performance, disk-based, data permanence (WORM file-level locking) for ONTAP storage to help provide data integrity and retention that enables electronic records to be both unalterable (immutable) and rapidly accessible (online). SnapLock offers two retention features that prevent deletion before a specified expiration date. SnapLock Compliance prevents deletion before a specified expiration date and is certified to meet strict records-retention requirements, such as SEC Rule 17a-4, FINRA, HIPAA, and CFTC, and national requirements, such as DACH and GDPR. SnapLock Enterprise offers similar certifications but allows a trusted administrator to delete SnapLock Enterprise volumes or files.

Learn more about NetApp SnapLock.

SnapMirror® Active Sync

Availability	Serviceability
Continuous availability with RTO 0 and transparent application failover	Synchronous data replication with RPO 0 prevents data loss during servicing

SnapMirror® active sync, also called Business Continuity (SM-BC), combines flexible array-based clustering with more granular synchronous mirroring that preserves storage efficiency savings (data reductions) during and after the data transfer. It creates a continuously available storage solution with application-level granularity for NetApp AFF and ASA storage clusters and systems to meet the needs of the most critical business applications. SnapMirror® active sync supports a symmetric active/active capability, enabling read and write I/O operations from both copies of a protected LUN with bidirectional synchronous replication, enabling both LUN copies to serve I/O operations locally.

If a data center disaster occurs, SnapMirror® active sync maintains business continuity by delivering zero RPO and zero RTO for SAN workloads. It supports native IP-based data replication between ONTAP storage systems over existing WAN infrastructure without using host-based technology or data converters.

Learn more about NetApp SnapMirror® active sync.

SnapMirror® active sync

Availability	Serviceability
High availability with RTO near 0 and rapid failover and failback (resync)	Synchronous data replication with RPO 0 prevents data loss during servicing

SnapMirror® active sync delivers incremental, volume-granular, real-time data replication that achieves zero RPO while preserving storage efficiency savings (data reductions) during and after the data transfer. It provides high data availability and fast disaster recovery for business-critical applications such as Microsoft Exchange Server, Microsoft SQL Server, and Oracle, in both virtual and traditional environments. SnapMirror® active sync uses IP networks to replicate data at high speeds over LAN or WAN, to achieve high data availability and fast data replication for business-critical applications such as Oracle, Microsoft SQL Server, and so on, in both virtual and physical environments. SnapMirror® active sync offers the flexibility to protect a subset of volumes in the cluster, and replication can occur between ONTAP storage systems of different models. SnapMirror® active sync supports native IP-based data

replication between ONTAP storage systems over existing WAN infrastructure without using host-based technology or data converters.

Learn more about NetApp SnapMirror® Synchronous.

SnapMirror® (asynchronous)

Availability	Serviceability	Security
Maintains backup copies that can be rapidly recovered	Move data to create more nondisruptive servicing options	Delivers data replication protection with rapid recovery

SnapMirror® asynchronous replicates data at high speeds asynchronously over LAN or WAN for fast data replication of business-critical databases and applications, including Microsoft Exchange, Microsoft SQL Server, and Oracle in virtual and traditional environments. Its asynchronous data replication supports disaster recovery and data protection while preserving storage efficiency (data reductions using data from one ONTAP storage system to continually update another in near real-time and without requiring external replication servers). Also, SnapMirror® asynchronous supports three-site protection using SnapMirror® active sync replication between sites 1 and 2 and SnapMirror® asynchronous replication between sites 2 and 3. SnapMirror® supports native IP-based data replication between ONTAP storage systems over existing WAN infrastructure without using host-based technology or data converters.

Learn more about NetApp SnapMirror® (asynchronous).

Secure multitenancy infrastructure sharing with storage virtual machines

Availability	Serviceability	Security
Helps clusters to operate continuously during upgrades	Supports addition and removal of storage nodes	Isolates data, user, and administrator domains

Storage virtual machines (SVMs) provide data access to clients regardless of the physical storage or controller. Each SVM appears to the clients as a single independent server, which enables multiple SVMs to coexist in a cluster while ensuring that no data flows among them. SVMs deliver secure multitenancy to users by isolating shared and virtualized data storage and network infrastructure. SVMs deliver secure multitenancy to administrators by providing a separate administrator authentication domain that can be managed independently by its administrator. Also, SVMs help clusters to operate continuously during software and hardware upgrades, addition and removal of nodes, and all administrative operations.

Learn more about NetApp Storage Virtual Machines.

Data efficiency with data reduction beyond basic compression and deduplication

Reliability	Availability
Prevents capacity-related database and app errors	Ensures specific capacity for storage workloads

NetApp delivers high data efficiency for workloads that are enabled by continuous innovation and periodic enhancements to ONTAP with features that help get more usable capacity from a given amount of raw physical storage. ONTAP is well known for the space and performance efficiency of its Snapshot technology, which alone improves data reduction ratios by a factor of 10. NetApp knows that efficient storage requires more than basic deduplication and compression, so ONTAP provides many storage efficiency features, including:

- Inline zero pattern detection
- Inline data compaction

- Inline adaptive compression
- Inline cross-volume deduplication
- Inline aggregate deduplication
- Background volume deduplication
- Background aggregate deduplication

Learn more about NetApp storage efficiency and the NetApp Efficiency Guarantee.

Add storage workloads without overusing available performance capacity

Reliability	Availability
Helps to avoid mistakes leading to performance-related workload errors	Helps to ensure that workloads have access to expected performance

ONTAP offers a powerful set of tools for managing workloads by determining how much performance is available for use by storage workloads. ONTAP collects and reports available performance statistics for storage resources, including the percentage of used performance, the percentage of free performance, and the available IOPS that can be added to the resource before reaching the maximum performance available. Knowing these performance metrics helps to plan, provision, monitor, and balance workloads, eliminating potential mistakes that could cause workload errors due to a lack of expected storage performance and enabling maximum usage of storage resources without introducing performance issues.

Learn more about NetApp ONTAP performance metrics.

Cloud-native storage and data services

Cloud Volumes ONTAP

Cloud Volumes ONTAP is an enterprise software-defined storage (SDS) offering that delivers advanced data management for file (NFS and SMB) and block (iSCSI) workloads. Cloud Volumes ONTAP can make cloud storage infrastructure more affordable, intelligent, compliant, and secure by optimizing cloud storage costs and increasing application performance while enhancing data protection, security, and compliance. It can be used to protect on-premises or cloud ONTAP storage with highly efficient data replication, built-in storage efficiencies, and nondisruptive DR validation. Also, it allows users to replicate data quickly and easily across zones, regions, and clouds for portability; benefit from built-in data security that the user controls for security; and leverage always-on, AI-driven privacy compliance controls for privacy.

Learn more about NetApp Cloud Volumes ONTAP.

BlueXP™

NetApp storage management software empowers unprecedented data flexibility on-premises and across multiple private, public, and hybrid cloud environments. NetApp offers a portfolio of storage management software that includes BlueXP. Together, they help to improve and ensure the reliability, availability, serviceability, and security of ONTAP storage like ASA, AFF, and FAS clusters and systems.

Reliability	Availability	Serviceability	Security
Helps to manage, monitor, and automate data	Orchestrates data across the entire hybrid multicloud	Enables storage self-service for internal teams	Controls security capabilities to improve cyber resiliency

BlueXP™ delivers a unified experience for storage and data services across on-premises and cloud environments. It enables operational simplicity through the power of AIOps, with the flexible consumption parameters and integrated protection required for today's cloud-led world. BlueXP™ data services for replication, backup and recovery, and disaster recovery help to further improve NetApp reliability, availability, serviceability, and security.

BlueXP™ unifies all of NetApp's storage and data services into a single tool that lets you build, protect, and govern your hybrid multicloud data estate. Your data estate is your organization's combined storage infrastructure with the data stored in it. It's like your IT stack, but for data. BlueXP™ is designed to make these data estate operations simpler and more robust.

Learn more about NetApp BlueXP.

Cloud Sync

Reliability	Availability	Serviceability	Security
Synchronizes changes and maintains local copies of remote files	Synchronizes data as frequently as every minute	Temporarily moves data to facilitate servicing	Persistent server-side and data-in-flight encryption

Cloud Sync is an easy-to-use cloud-native service that copies, synchronizes, and moves file and object data across private, public, and hybrid cloud locations and transfers files between NFS and CIFS file shares or Amazon S3 object format, Azure Blob, IBM Cloud Object Storage, and StorageGRID.

Learn more about NetApp Cloud Sync.

Cloud Tiering

Reliability	Availability	Serviceability	Security
Off-loads inactive data to object storage, freeing resources for hot data	Tiered data is continuously accessible	Temporarily moves data off storage under service	Preserves data security options of hot and cold tiers

Cloud Tiering uses FabricPool technology to effortlessly scale data by extending ONTAP clusters and systems to include low-cost object storage like StorageGRID, AWS, Microsoft Azure, and Google Cloud. It efficiently manages storage pools by placing data at the right tier at the right time by using policy-based tiering of inactive (cold) data without compromising on storage manageability and performance. Also, policies can support long-term data retention by moving cold data to highly durable and inexpensive object storage.

Learn more about NetApp Cloud Tiering.

Cloud Backup

Reliability	Availability	Serviceability	Security
Supports data protection, disaster recovery, and data archiving strategy	Facilitates disaster recovery and minimizes data loss	Can be used to move data to clouds during service	TLS 1.3 in-flight and AES-256-bit at-rest encryption

Cloud Backup is an add-on service for NetApp storage systems and NetApp Cloud Volumes ONTAP that delivers backup and restore capabilities to support disaster recovery, data protection, and data archiving. Backups are read-only, immutable, and stored on secondary cloud object storage separated from primary storage to satisfy 3-2-1 backup strategies, protect against cyberattacks, and meet data protection

requirements. Recovery options include the original primary storage and Cloud Volumes ONTAP storage in the same public cloud and region as the backup data.

Learn more about NetApp Cloud Backup.

Disaster Recovery

Reliability	Availability	Serviceability	Security
Automates and simplifies otherwise complex DR operations	Facilitates disaster recovery for VMware workloads	Non-disruptive DR failover and failback testing	TLS 1.3 in-flight and AES-256-bit at-rest encryption

Disaster Recovery offers simple, low-cost disaster protection for VMware workloads, from on-premises to on-premises NetApp ONTAP environments or to VMware Cloud and Amazon FSx for NetApp ONTAP. This SaaS-based disaster recovery (DRaaS) solution can significantly lower your costs and reduce complexity since there's no need to acquire and deploy expensive alternative infrastructure. With Disaster Recovery, you can create a templatized disaster recovery plan for vSphere apps that use NFS data stores in ONTAP, replicate vSphere apps and data to a VMware Cloud disaster recovery site in AWS, test the failover process without disrupting your production workloads, and perform failback operations post-recovery to the primary site and resume business as usual.

Learn more about NetApp Disaster Recovery.

Replication

Reliability	Availability	Serviceability	Security
Maintains copies of data on seperate storage for data protection	Creates and maintains secondary copies of ONTAP data	Establishes a redundant copy of ONTAP volumes or SVMs	TLS 1.3 in-flight and AES-256-bit at-rest encryption

Replication offers high speed enterprise-grade replication for your ONTAP data, both on-premises and in the cloud. It utilizes NetApp SnapMirror technology to replicate data between ONTAP-based storage, so you can replicate data to and from ONTAP on-premises, Cloud Volumes ONTAP, Amazon FSx for NetApp ONTAP, Azure NetApp Files, and Google Cloud NetApp Volumes. With Replication, you can create and maintain secondary copies of ONTAP data to support advanced data protection strategy in hybrid and multicloud environments.

Learn more about NetApp Replication.

Ransomware Protection

Reliability	Availability	Serviceability	Security
Automates and simplifies otherwise complex ransomware protection	Safeguards data from potential interuptions caused by ransomware	Automatically creates indelible Snapshots to limit attack damage	AI-driven detection and response to threats, with recovery in minutes.

Ransomware Protection makes defending and recovering your workloads easier, faster, and more effective. It merges the powerful cyber-resilience features of ONTAP and BlueXP into a single control plane and adds tailored recommendations and one-click orchestrated actions. Comprehensive, workload-centric defenses include identifying critical workloads (apps, VMs, file shares) in your primary ONTAP storage and applying protection policies with a single click, accurately detecting potential attacks and automatically responding with immutable and indelible Snapshot copies to limit damage, and recovering entire workloads, with application consistency, within minutes to minimize costly downtime. Recent

enhancements include new prioritized workload protection, user & behavior analytics, and more SIEM integrations.

Learn more about NetApp Ransomware Protection.

Observability

Reliability	Availability	Serviceability	Security
Monitors & troubleshoots technology resources acresss hybrid clouds	Machine learning insights prevents issues before thay happen	Provides full stack visibility into applications and infrastructure	TLS 1.3 in-flight and AES-256-bit at-rest encryption

Observability, also known as Cloud Insights, brings complete full-stack visibility into your infrastructure and applications, so you can monitor, troubleshoot, and optimize your resources across the hybrid multicloud. It supports NetApp storage, plus some third-party storage, and many of the world's most popular container and hypervisor platforms, operating systems, databases, and applications. Observability helps to optimize resource utilization, visualize complex status information using customizable dashboards, and discover the health of your ONTAP storage operations.

Learn more about NetApp Observability.

Classification

Reliability	Availability	Serviceability	Security
Finds and identifies data to prevent gaps in data protection	Identifies and moves data to correct storage policies	Suppports data governance during maintenance operations	Archives or deletes inactive or obsolete data for protection

Classification automatically discovers, maps, and classifies data, wherever it's located across a hybrid multicloud. It can use granular data parameters and AI-driven contextual language identification to automatically label and act on information stored in files and database entries, and delete, archive, or protect data according to enterprise policies and global regulations. Classification analyzes a wide and growing range of data sources, including structured and unstructured data, on NetApp ONTAP (or third-party) storage that exists in the cloud or on-premises.

Learn more about NetApp Classification.

AIOps and Storage Health

Reliability	Availability	Serviceability	Security
Recommends actions that optimize storage health	Proactively suggests improvements to configurations	Offers automated actions to support maintenance	Helps to find potential security issues and proposes fixes

AIOps and Storage Health, also known as Active IQ, helps to optimize storage health, resiliency, and economics by uncovering and addressing otherwise hidden risk factors, finding opportunities to improve system availability, security, and performance, and handling storage data growth challenges efficiently. It offers integrated AIOps and storage health tools to simplify proactive care NetApp storage optimization. Tools enable visibility into storage health and provide prescriptive guidance to address misconfigurations, security vulnerabilities, outdated firmware, rapid growth, and best practice gaps. A digital advisor provides you with the visibility and insights required to maintain storage health, reduce time spent on storage operations, lower storage costs, and improve efficiency

Learn more about NetApp AIOps and Storage Health.

Conclusion

NetApp ONTAP storage combines hardware, software, and services to create enterprise storage that offers industry-leading reliability, availability, serviceability, and security. This section summarizes some of the numerous capabilities and features that support RASS.

Reliability

Table 12) Examples of items that contribute to increased reliability.

Specialized system cabinets	Specialized controllers	Specialized drive shelves
Specialized fabric switches	FabricPool	FlexCache
FlexClone	FlexVol	MetroCluster
RAID-TEC	RAID DP	Adaptive QoS
Data efficiency	Performance capacity	AIOps and Storage Health
Cloud Volumes ONTAP	BlueXP™	Cloud Sync
Cloud Tiering	Cloud Backup	Disaster Recovery
Replication	Ransomware Protection	Observability
Classification		

Availability

Table 13) Examples of items that contribute to increased availability.

Redundant controllers	Redundant drive shelves	Redundant fabric switches
Nondisruptive controller software updates	Nondisruptive controller hardware updates	Nondisruptive NVMe drive shelf addition and removal
Nondisruptive SAS drive shelf addition and removal	FabricPool	FlexCache
FlexClone	FlexGroup	FlexVol
MetroCluster	SnapCenter	SnapLock
SnapMirror® active sync	SnapMirror® Synchronous	SnapMirror® asynchronous
Classification	Snapshot	SnapRestore
RAID-TEC and RAID DP	Adaptive QoS	Storage virtual machines
Data efficiency	Performance capacity	Active IQ®
Cloud Volumes ONTAP	BlueXP™	Cloud Sync
Cloud Data Sense	Cloud Tiering	Cloud Backup

Disaster Recovery	Replication	Ransomware Protection
Dynamic Authorization	Multi-Admin Verification	Observability

Serviceability

Table 14) Examples of items that contribute to increased serviceability.

Hot-swap controllers	Hot-add and hot-removal of drive shelves	Hot-swap drives
Hot-swap fabric switches	Controller FRUs	Drive shelf FRUs
Fabric switch FRUs	System cabinet FRUs	FabricPool
FlexClone	FlexGroup	FlexVol
MetroCluster	SnapCenter	SnapLock
SnapMirror® active sync	SnapMirror® Synchronous	SnapMirror® (asynchronous)
Replication	Snapshot	SnapRestore
RAID-TEC	RAID DP	Storage virtual machines
AIOps and Storage Health	Astra Control	Cloud Manager
Cloud Sync	Cloud Tiering	Cloud Backup
Disaster Recovery	Observability	Ransomware Protection
Dynamic Authorization	Multi-Admin Verification	Classification

Security

Table 15) Examples of items that contribute to increased security.

SnapManager	AIOps and Storage Health	FPolicy
SnapCenter	SnapLock	Security certifications
SnapMirror® (asynchronous)	BlueXP	FIPS 140-2 level 2
Disaster Recovery	Cloud Manager	Two-layer encryption
Snapshot	NetApp Cloud Insights with Cloud Secure	Multifactor authentication (MFA)
SnapRestore	Cloud Sync	Role-based access control (RBAC)
SnapVault	Observability	Accounts, roles, and capabilities (ARC) strategy
Secure multitenancy with storage virtual machines	Cloud Tiering	Security development lifecycle

NetApp Volume Encryption	NSA CSfC validation	Segregation of duties
NetApp Storage Encryption (NSE)	Cloud Backup	Principle of least privilege
FlexClone	Ransomware Protection	Cabinet locking doors and side panels
FlexVol	Ransomware protection	Cabinet interconnect and bolt-down kits
Autonomous Ransomware Protection	Dynamic Authorization	Multi-Admin Verification
Cloud Backup	Replication	Classification

Where to find additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

NetApp products and services

- NetApp ONTAP software
  https://www.netapp.com/data-management/ontap-data-management-software
- NetApp ASA clusters and systems
  https://www.netapp.com/data-storage/all-flash-san-storage-array
- NetApp AFF A-Series clusters and systems
  https://www.netapp.com/data-storage/aff-a-series
- NetApp AFF C-Series clusters and systems
  https://www.netapp.com/data-storage/aff-c-series
- NetApp FAS clusters and systems
  https://www.netapp.com/data-storage/fas
- NetApp BlueXP™ cloud services
  https://bluexp.netapp.com

Reliability, availability, serviceability, and security

- NetApp product security
  https://security.netapp.com
- NetApp ONTAP security
  https://www.netapp.com/cyber-resilience/data-protection/ontap-security
- WP-7365: Introduction to the NetApp AI Security Framework
  https://www.netapp.com/media/107739-wp-7365-ai-security-framework.pdf
- WP-7366: Data-centric Zero Trust - An evolution in cyberdefense
  https://www.netapp.com/media/107740-wp-7366-data-centric-zero-trust.pdf
- TR-4569: Security hardening guide for NetApp ONTAP 9
  https://www.netapp.com/media/10674-tr4569.pdf
- Ransomware: Prevention is better than cure
  https://www.netapp.com/blog/ransomware-prevention-is-better-than-cure
- TR-4572: The NetApp solution for ransomware
  https://www.netapp.com/media/7334-tr4572.pdf

- TR-4829: NetApp and Zero Trust
  https://www.netapp.com/media/19756-tr-4829.pdf
- TR-4678: NetApp ONTAP FlexGroup volumes
  https://www.netapp.com/media/17064-tr4678.pdf
- TR-4968: NetApp All-SAN Array data availability and integrity
  https://www.netapp.com/media/85671-tr-4968.pdf
- TR-4080: Best practices for modern SAN in ONTAP
  https://www.netapp.com/media/10680-tr4080.pdf
- TR-4684: Implementing and configuring modern SANs with NVMe-oF
  https://www.netapp.com/media/10681-tr4684.pdf
- TR-4067: NFS in NetApp ONTAP
  https://www.netapp.com/media/10720-tr-4067.pdf
- TR-4814: S3 in ONTAP best practices
  https://www.netapp.com/media/17219-tr4814.pdf

Version history

Version	Date	Document version history
Version 1.0	February 2022	Initial release.
Version 1.1	September 2023	Updated NetApp ASA and NetApp AFF. Added NetApp AFF C-Series, Google Cloud NetApp Volumes, and BlueXP. Removed Astra Control, ONTAP System Manager, SnapMirror® Cloud, OnCommand.
Version 1.2	September 2024	Added AFF A1K, A90, and A70 models. Added ASA A1K, A90, and A70 models. Added FAS90 and FAS70 models. Added NVIDIA SN2100 fabric switch. Added Cluster Peering Encryption (CPE) TLS 1.3 support. Added ActiveIQ Transport using SMTP with TLS. Added Dynamic Authorization. Added Autonomous Ransomware Protection (ARP) AI Detection Engin. Added Multi-admin verification (MAV) enhancements. Added MetroCluster (MCC) Encrypted NVLOG Mirroring. Added NetApp Volume Encryption (NVE) Key for Flex Clone volumes. Added LDAP Version upgrade to 2.5.16. Added link to Data-Centric Zero Trust white paper (Alignment to the DoD ZT Pillars). Added link to Introduction to the NetApp AI Security Framework (NAISF) white paper. Updated BlueXP Ransomware Protection to include new prioritized workload protection, new user & entity behaviour analytics, and new SIEM integrations. Added links to additional NetApp Technical Report (TR) documents. Changed SnapMirror® Business Continuance to SnapMirror® active sync.

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

WP-7354-0222

NetApp