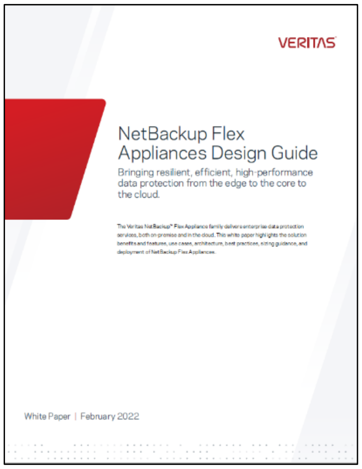

VERITAS

NetBackup Flex Appliances Design Guide

Bringing resilient, efficient, high-performance data protection from the edge to the core to the cloud.

The Veritas NetBackup™ Flex Appliance family delivers enterprise data protection services, both on-premise and in the cloud. This white paper highlights the solution benefits and features, use cases, architecture, best practices, sizing guidance, and deployment of NetBackup Flex Appliances.

White Paper | February 2022

NetBackup Flex Appliances Design Guide

Bringing resilient, efficient, high-performance data protection from the edge to the core to the cloud.

Thank you for downloading this Veritas White Paper. Carahsoft is the public sector distributer for Veritas solutions available via the GSA Schedule 70, Quilt, and NJSBA contract vehicles.

To learn how to take the next step toward acquiring Veritas' solutions, please check out the following resources and information:

For additional resources:
carah.io/VeritasResources

For upcoming events:
carah.io/VeritasEvents

For additional Veritas solutions:
carah.io/VeritasSolutions

For additional Veritas NetBackup solutions:
carah.io/VeritasNetBackup

To set up a meeting:
Veritas@carahsoft.com
(888)-662-2724

To purchase, check out the contract vehicles available for procurement:
carah.io/VeritasContracts

For more information, contact Carahsoft or our reseller partners:
Veritas@carahsoft.com | (888)-662-2724

VERITAS

NetBackup Flex Appliances Design Guide

Bringing resilient, efficient, high-performance data protection from the edge to the core to the cloud.

The Veritas NetBackup™ Flex Appliance family delivers enterprise data protection services, both on-premise and in the cloud. This white paper highlights the solution benefits and features, use cases, architecture, best practices, sizing guidance, and deployment of NetBackup Flex Appliances.

White Paper | February 2022

Contents

Contents

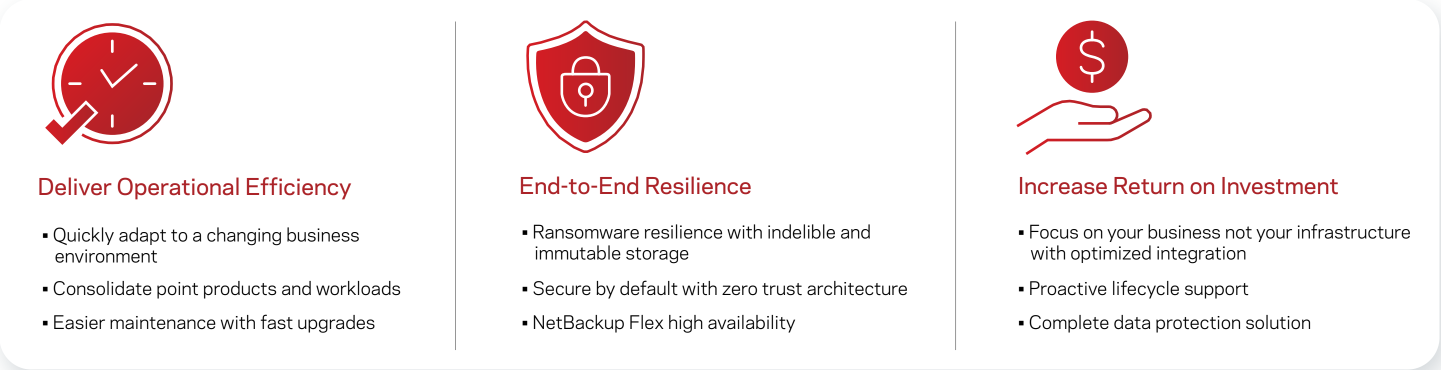
Contents

Introduction

Executive Summary

Today, the IT organization is more than the core data center. It spans from the edge to the core and to the cloud, including virtual environments and hybrid clouds along with traditional data protection deployments. One appliance model cannot meet the needs of all these different use cases. Organizations must quickly adapt their data protection infrastructure to rapidly changing business environments. IT organizations are also under increasing pressure to consolidate data protection solutions and to reduce costs.

The Veritas NetBackup Flex Appliance family delivers seamless deployments, workload consolidation, enterprise resilience, and agile performance. With robust systems and hardware integrations, you can get started with your NetBackup data protection in minutes with integrated system automations that reduce common infrastructure complexities. NetBackup Flex Appliances allow you to manage various deployments with a single, unified interface to reduce your data center footprint, simply IT management, and optimize storage performance with artificial intelligence/machine learning (AI/ML) testing. With NetBackup Flex Appliances, you get built-in ransomware recovery of business-critical data—at any scale—with near-zero recovery point objectives (RPOs) and recovery time objectives (RTOs). A Zero Trust architecture ensures ransomware prevention and protection with immutable storage and lets you retrieve stolen data with cryptographic-based security (FIPS 140-2 Standard), meet compliance needs with Cohasset Associates–approved governance, and perform policy-based retention blocks. NetBackup Flex Appliances software is the best one-stop solution, allowing you to store data from over 800 different data sources and over 60 cloud storage targets with a single platform. NetBackup Media Server Deduplication Pool Cloud Tier (MSDP-C) enables you to back up and restore data from cloud storage as a service (STaaS) vendors. NetBackup Flex Appliances increase return on investment (ROI) by integrating with Veritas NetInsights and Appliance management systems.
(See Figure 1.)



Deliver Operational Efficiency

- Quickly adapt to a changing business environment
- Consolidate point products and workloads
- Easier maintenance with fast upgrades

End-to-End Resilience

- Ransomware resilience with indelible and immutable storage
- Secure by default with zero trust architecture
- NetBackup Flex high availability

Increase Return on Investment

- Focus on your business not your infrastructure with optimized integration
- Proactive lifecycle support
- Complete data protection solution

Figure 1. An overview of the benefits of NetBackup Flex Appliances.

Scope

The purpose of this document is to provide technical details to assist in understanding NetBackup Flex Appliances. This white paper describes the solution benefits and features, use cases, architecture, and deployment of NetBackup Flex Appliances. There are additional resources available for NetBackup Flex Appliances:

- For best practices and sizing: NetBackup Flex Appliance Best Practices
- For more detail on ransomware resilience and Flex Appliances security: NetBackup Flex Appliance Security Guide
- For integration and API guide: NetBackup Flex API Guide
- For installation, configuration, and administration of each of the products discussed in this white paper: see the appropriate Veritas product documentation

Target Audience

This document is for customers, partners, and Veritas field personnel interested in learning more about NetBackup Flex Appliances. It provides a technical overview, architecture, guidance in sizing, and highlights some best practices.

Key Values and Features

Rather than relying on complex and costly data protection environments consisting of many converged or single-function backup, data deduplication, cloud tiering, and storage silos spread across the enterprise, NetBackup Flex Appliances provide operation efficiency, end-to-end resiliency, and optimized integration to deliver enterprise-wide data protection services on demand. Table 1 provides a summary of NetBackup Flex Appliance benefits and features.

Table 1. NetBackup Flex Appliance Benefits and Features

Benefit	Feature Description
Deliver Operational efficiency	▪ Consolidate NetBackup server deployment by hosting multiple NetBackup domains and multiple NetBackup servers on a single appliance ▪ MSDP container provides deduplication ▪ Simplify protection of remote or branch offices ▪ Easier maintenance with fast upgrades ▪ Universal Share significantly improves the dump-and-sweep process ▪ Instant Access for virtual machines (VMs) and files
High availability	▪ Container isolation prevents a container application failure from impacting other applications ▪ Deep monitoring of the Primary server's critical operation services and remedial actions during the failure
Security and compliance	▪ Provide WORM capability, retention locks, and platform hardening against ransomware and malware threats ▪ Use Security Enhanced SELinux to provide an intrusion detection and prevention system ▪ IPv6 support on the operating system (OS) ▪ FIPS 140-2 and STIG compliance ▪ Syslog and audit logs forwarding to syslog server or Splunk ▪ Secure Active Directory support ▪ Support for customizable login banner ▪ Ability to use external certificates
Secure and isolate tenant backup information for multi-domain	▪ Configure NetBackup application instance infrastructure into logical groups known as tenants ▪ Secure and isolate tenant backup data and network traffic with the Veritas Optimized Operating System (VxOS) security profiles to control container access
Manageability efficiency	▪ Manage multiple Flex Appliances with the Appliance Management Server (AMS) ▪ Update firmware from the web UI ▪ EEB package management for NetBackup instances

Monitoring, reporting, and insights	▪ Alert settings in the web UI ▪ SNMP v2/v3 ▪ Call Home with secure proxy ▪ Enable third-party monitoring tools like Grafana ▪ Monitor Flex Appliances in the NetInsights console
Long-term retention on-prem and in the public cloud	▪ Efficiently tiers to the cloud with NetBackup MSDP-C ▪ Connect with the Veritas Access Appliance, a software-defined storage appliance for long-term data retention with multi-cloud capability
API and integration	▪ Access to public APIs for integration and automation ▪ Integrated with Grafana to query appliance metrics ▪ API metrics and support access token

High-Level Architecture

NetBackup Flex Appliances tightly integrate with NetBackup and simplify your environment by providing a common platform for NetBackup applications. The NetBackup Flex Appliances let you deploy data protection services and change them on demand simply by selecting and configuring the NetBackup application container as needed. Once you've selected the container image and configured an instance, NetBackup applications are deployed into production across the business—in minutes. You can consolidate multiple NetBackup deployments (domains) on a single NetBackup Flex Appliance, substantially reducing data center costs and complexity.

The Docker container software runs directly on VxOS, which is a Linux-based operating system (OS). VxOS provides the NetBackup Flex Appliance kernel, runtime library, and container engine. The Flex Appliance uses the container isolation and security technology to ensure users are kept separate from one another when using different instances of NetBackup on a single appliance. Between the kernel features built into VxOS and the network and data segregation, users of NetBackup services are effectively firewalled from one another. This multi-tenant architecture simplifies your NetBackup environment by allowing multiple NetBackup domains to run on this common platform. (See Figure 2.)

MSDP-C can support both local storage and multiple cloud storage targets. After you configure the MSDP storage server, you can add a cloud storage target to that storage server, and then the MSDP-C can store data directly in the cloud target. The deduplication engine in the NetBackup MSDP stores the data in a storage optimized and portable format and is designed to transport to any compatible target on any infrastructure. It also features storage efficiency technologies such as deduplication and compression to reduce egress and ingress costs to and from the cloud.

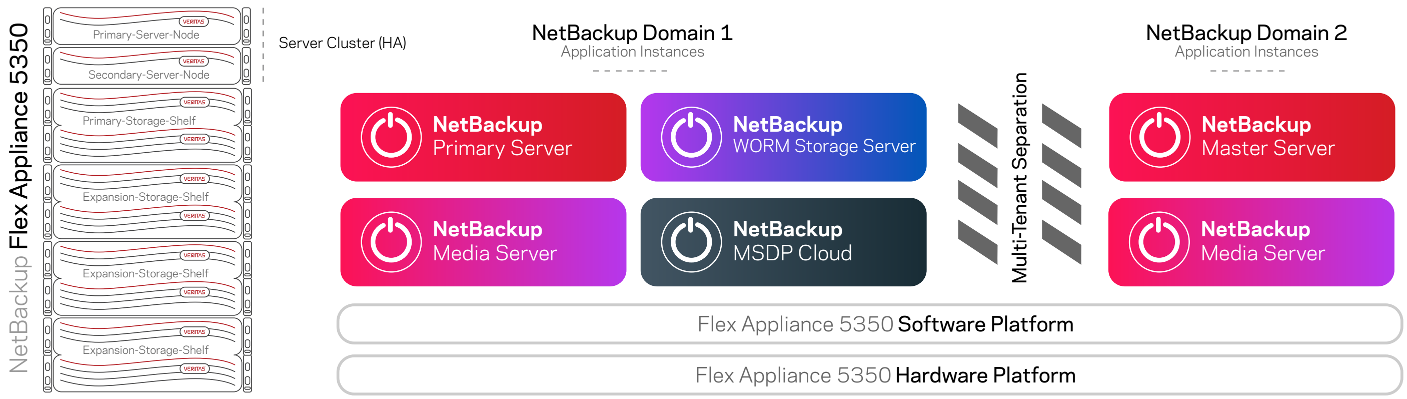


Figure 2. An overview of the NetBackup Flex Appliance's multi-tenant architecture.

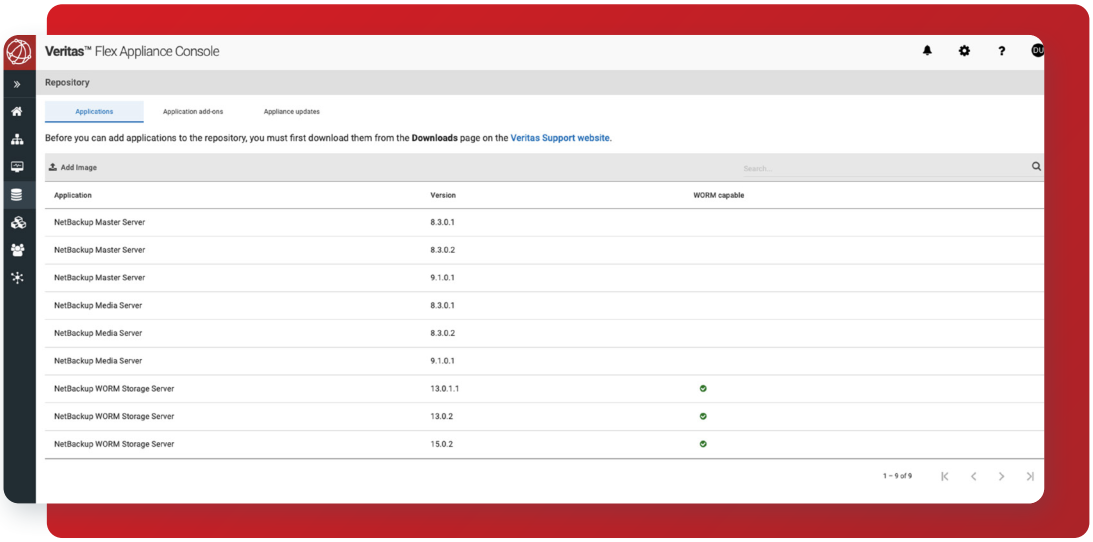
NetBackup Flex Appliances can now deliver enterprise-wide on-premises and cloud data protection on demand and rapidly adapted to meet the changing requirements of the business.

Application Container Image and Instance

Before you can create an application container instance, install an application add-on or upgrade, or update the appliance software, you must first add the applicable image files to the repository.

Container Images

Application container images are static and immutable. Adding support for multiple versions of NetBackup is easy with a NetBackup Flex Appliance (see Figure 3). You can download the NetBackup Container Images from the Veritas support website independently of the NetBackup Flex Appliance software.



Before you can add applications to the repository, you must first download them from the **Downloads** page on the Veritas Support website.

Application	Version	WORM capable
NetBackup Master Server	8.3.0.1	
NetBackup Master Server	8.3.0.2	
NetBackup Master Server	9.1.0.1	
NetBackup Media Server	8.3.0.1	
NetBackup Media Server	8.3.0.2	
NetBackup Media Server	9.1.0.1	
NetBackup WORM Storage Server	13.0.1.1	✓
NetBackup WORM Storage Server	13.0.2	✓
NetBackup WORM Storage Server	15.0.2	✓

1 – 9 of 9

Figure 3. An overview of the NetBackup Flex Appliance Console showing support for NetBackup by version.

There are different types of container images, as shown in Table 2.

Table 2. Container Image Types by Use Case

	Use Case	Content
Application	Instantiate and run a container	An application and changes required to make the application run and work
Add-On	Provide add-on components to application containers	Add-on libraries and binaries

Container Instance

Application container instances are built from static container images. One container has a single instance per role. Supported roles include NetBackup primary server, media server (including MSDP and Advanced Disk), deduplication (MSDP), and NetBackup Immutable MSDP Storage Server. You can create an instance with the NetBackup Flex Appliance's web UI.

An application container instance has persistent data and non-persistent data to simplify the application instance upgrade process. (See Figure 4.)

- The persistent data includes the primary service catalog, backup images, and configuration settings
- The non-persistent data includes base NetBackup software components, services, and binaries

Below are the processes during upgrades and maintenance:

- The original container instance is shut down
- A new instance based on the new container image is started
- Persisted data is mounted to the upgraded container instance
- NetBackup is available to do backups at the new version

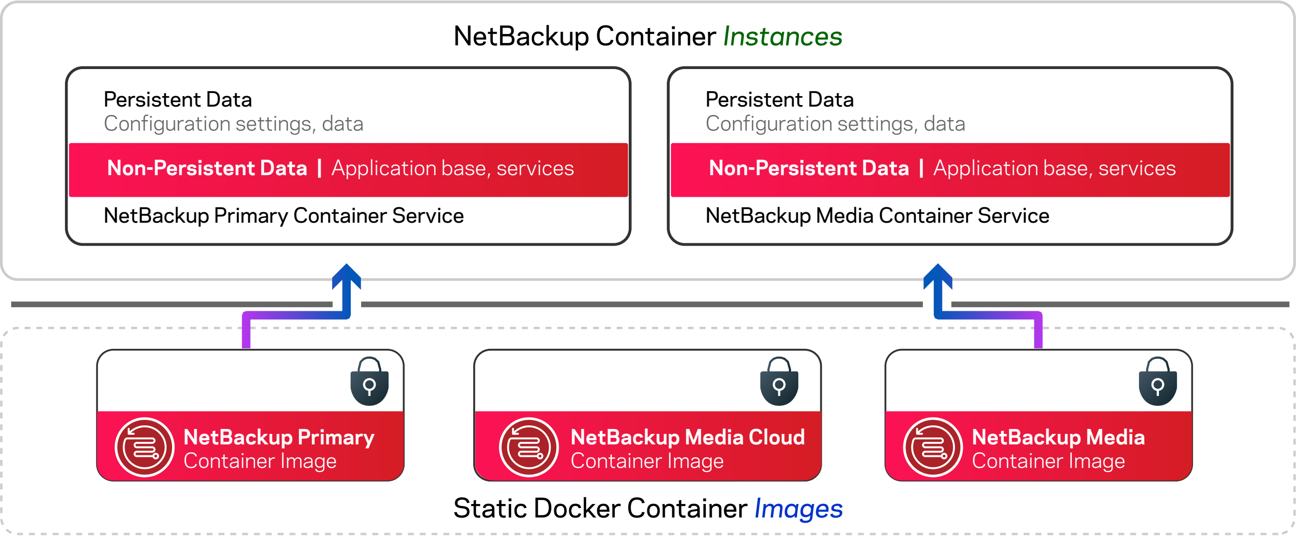

NetBackup Container Instances
Persistent Data
Configuration settings, data
Non-Persistent Data | Application base, services
NetBackup Primary Container Service
Persistent Data
Configuration settings, data
Non-Persistent Data | Application base, services
NetBackup Media Container Service
NetBackup Primary Container Image
NetBackup Media Cloud Container Image
NetBackup Media Container Image
Static Docker Container Images

Figure 4. An overview of the container instance upgrade process.

Architecture Deep Dive: Platform as a Service Components

The NetBackup Flex Appliance architecture's objective is to build a next-generation, multi-tenant appliance platform with high availability (HA), security, agility, and integration with Veritas applications. The platform owns the resources to provision applications, storage, network, and compute on demand. The service components have a management plane, a control plane, and a resource plane. (See Figure 5.)

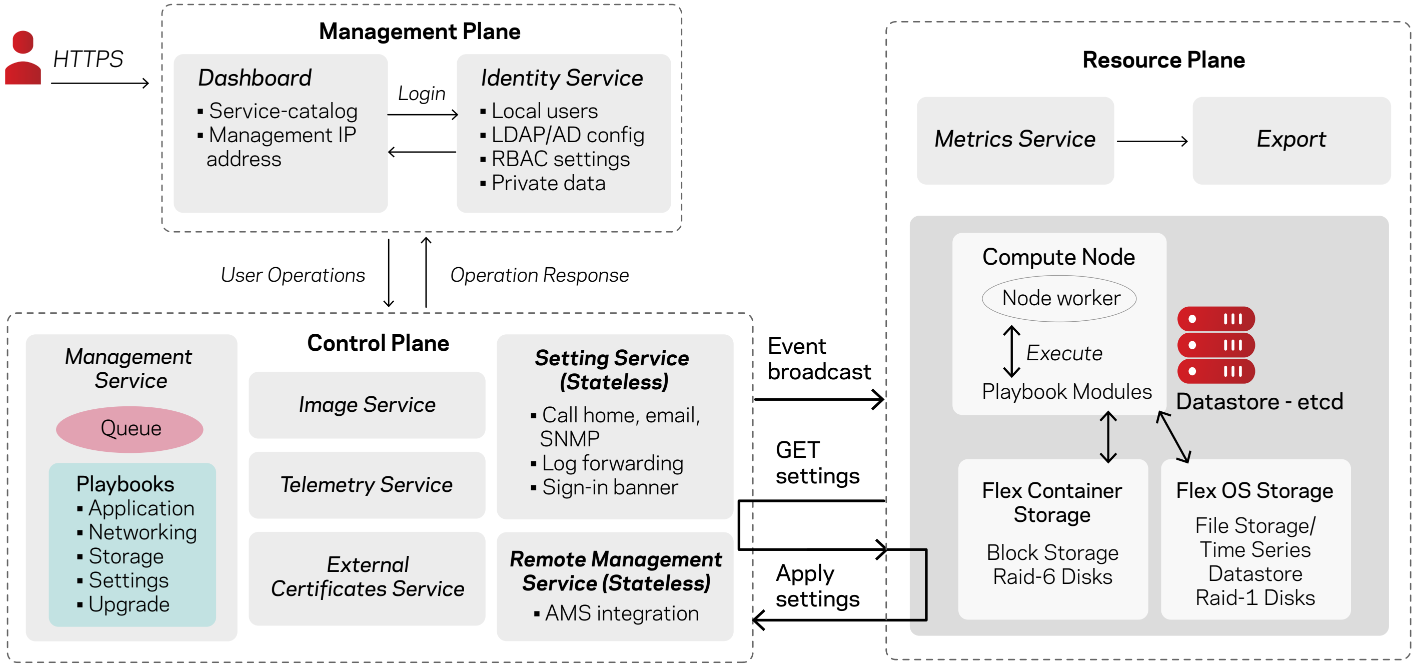


Figure 5. An overview of the NetBackup Flex Appliance architecture's service components.

Management Plane

The management plane provides a dashboard and identity service. The dashboard passes user login information to the identity service. After verification, the identity service returns an access token with the objects and roles the user has back to the dashboard.

Dashboard

The dashboard is a UI that lets users interact with the appliance to perform duties within their designated roles. The dashboard provides functionalities such as appliance- or node-specific changes, applications and instances, monitoring the various components, and resource usage. Users are prompted for their credentials to access the dashboard.

Identity Service

The dashboard forwards user credentials to the identity service to validate users and understand their roles. The identity service allows the super administrator to configure local users or Active Directory as an identity provider.

Control Plane

The control plane manages the infrastructure services. Upon a successful user login, the dashboard contacts the management service when a user performs actions. Before taking any action on user operations, the service contacts the identity service to validate the user and related capabilities using the access token sent by the dashboard.

Management Service

The management service executes the operations on applications, networking, storage, settings, and upgrades. The playbook modules include the specific instructions for each node with a set of variables/constraints to complete the action. The management service has various modules for different system capabilities such as storage and tenants that may require special processing. For example, adding a tenant and setting its properties requires only saving the information in the persistent store. The information can be used by all tenant operations to enforce constraints.

A management service instance can be hosted on one of the appliance nodes or externally as long as it can communicate with the appliance. This setup also makes the service capable of managing multiple appliances to provide a central management console.

For all write operations, the service records the change in a persistent store for a desired system state. This information can be used later to synchronize a node or re-create the system.

Persistent Service

The persistent service provides a stand-alone and technology-agnostic persistent store. The responsibilities of the service are to save and return requested information in the persistent store that it owns.

Registry Service

The registry service maintains and centrally serves Docker container images delivered by application images. The service is contacted by the orchestration layer when an application instance is provisioned and started.

Setting Service

The setting service provides supportability like Call Home, email, and SNMP and security like log forwarding and sign-in banner.

Remote Management Service

The remote management service does the integration with the AMS and NetInsights.

Resource Plane

The management service uses the playbook corresponding to the API along with user input and any other constraints to a random or set of target nodes, as appropriate, by calling the async task REST API exposed by the host agent in the resource plane. The service checks the state of the task periodically to keep the user apprised of progress.

Built-in Security Architecture

NetBackup Flex Appliances are built with a security mindset. The internal infrastructure services are running on Docker bridge, with firewall policies around the services to prevent direct access by a localhost user and outside hosts. These services can be accessed only via the API gateway service. Each service has a separate access token for the REST API connection with the least access permissions required to make the service functional. Each infrastructure and application container has unique SELinux MCS categories to isolate process, mount, and storage.

The remote management services are running on a different Docker bridge and cannot connect to other infrastructure services. The data or database holding sensitive information, like passwords, is encrypted with a one-way hash. Application containers have a seccomp policy that adds another security layer to manage system calls.

Deliver Operational Efficiency

NetBackup Flex Appliances quickly adapt to a changing business environment, consolidate point products and workloads, and provide easier maintenance with fast upgrades.

Container Technology

With containerization, the NetBackup application container provides the following benefits (see Table 3):

- Operational reliability when moved between nodes in the cluster
- Increased modularity
- Simplicity
- Application/process isolation
- Improved security
- Faster startup and shutdown

Table 3: Comparison of Containerization and Virtualization

	Containerization	Virtualization
Size	10s MBs	Several GBs
Boot time	Almost instantly	Several minutes
Modularity	Can split applications into modules for easy management and enhanced security	Not available

Universal Share

NetBackup Flex Appliance software release 2.0.1 supports the Universal Share. The Universal Share feature provides data ingest into a NetBackup Flex Appliance using an NFS or a CIFS (SMB) share. Space efficiency is achieved by storing this data directly into an existing NetBackup-based deduplication pool. Any data that is stored in a Universal Share is automatically placed in MSDP storage where it is deduplicated automatically. This data is then deduplicated against all other data that was previously ingested into the media server's MSDP. Because a typical MSDP storage server stores data across a broad scope of data types, the Universal Share offers significant deduplication efficiency. (See Table 4.)

Table 4. Advantages of Universal Shares

Benefit	Feature Description
Data protection	▪ Offers all the data protection and management capabilities that are provided by NetBackup ▪ Client software is not required for Universal Share backups or restores. Universal Shares work with any POSIX-compliant OS that supports NFS or CIFS
Space-saving	▪ Provides a space-saving (deduplicated) dump location along with direct integration with NetBackup technologies, including data retention, replication, and direct integration with cloud technologies
Cost-saving	▪ Eliminates the need to purchase and maintain third-party intermediary storage, which typically doubles the required I/O throughput because the data must be moved twice. Universal Shares also cuts the time it takes to protect valuable application or database data in half.
Protection Point	▪ Offers a fast point-in-time copy of all data that exists in the share ▪ Advanced NetBackup data management facilities such as Auto Image Replication (AIR), Storage Lifecycle Policies (SLPs), optimized duplication, cloud, and tape are all available with any data in the Universal Share ▪ You can provision a read/write copy of any Protection Point or make it available through a NAS/ (CIFS/NFS)-based share via powerful copy data management tools

Instant Access

With increasing threats like ransomware and other downtime incidents, organizations need a data protection strategy that will always help them improve RPOs and RTOs.

NetBackup Flex Appliance software release 2.0.1 along with NetBackup software provides the following benefits:

- Instant access to critical VMs and applications
- Agentless backup and recovery, for less management overhead
- Set-and-forget automated protection for new VMs

You can create an instant access VM from a NetBackup backup image. The VM is available almost instantaneously, achieving a near-zero RTO. NetBackup mounts the VM's snapshot directly on the backup storage device to allow your ESXi host or cluster to treat the snapshot as a normal VM.

You can use the mounted VM snapshot for a variety of purposes, including:

- Recovering files from the VM or copying a VMDK file
- Running tests on the VM, such as testing a patch
- Troubleshooting or disaster recovery (DR)

Provide Multi-Tenancy with Network and Storage Segregation

All application containers running on NetBackup Flex Appliances need to share the hardware resources of the node such as CPU, memory, disk I/O, and network. NetBackup Flex Appliances use network and data segregation and the VxOS security features to provide multi-tenancy.

Network Segregation

NetBackup Flex Appliances use the Macvlan network driver to assign a MAC address to each container's virtual network interface; each MAC address is bound directly to a physical network interface. This approach provides external connectivity to and from the containers as well as network isolation between them. Macvlan provides the best network isolation for containers and allows NetBackup Appliance containers to use an actual IP address. NetBackup instances on a NetBackup Flex Appliance support multiple interfaces, including physical interfaces and bonded interfaces. The support for multiple networks enables NetBackup media server instances to span multiple networks.

VxOS Security Features for Containers

The VxOS kernel provides namespaces, control groups, and secure computing mode to control processes and resources at the OS level. NetBackup Flex Appliances use these features to control access and manage resources.

Namespaces

The concept of namespaces is a feature of the VxOS kernel that provides fundamental support for containers in VxOS. Namespaces ensure a group of processes only sees its own set of assigned resources and another group of processes only has access to its own, discrete services. The processes cannot see the resources assigned to the other group.

Control Groups

Control groups (cgroups) provide resources management for the CPU, memory, disk I/O, and networking. Using cgroups protects an appliance from being taken down by one container consuming all available resources on the physical system. Cgroups can help defend against denial-of-service (DoS) attacks on NetBackup Flex Appliances.

Secure Computing Mode

The VxOS kernel secure computing mode (seccomp) feature limits the number of system calls a process can make through secure, one-way transactions. NetBackup Flex Appliances use seccomp to control the security of the NetBackup containers with a seccomp profile. Each profile represents a list of privileged system calls that are blocked within the container.

End-to-End Resilience and High Availability

NetBackup Flex Appliances provide resilience and high availability (HA) to your NetBackup environment with container isolation.

Container Isolation

Container isolation prevents a container application failure from impacting other applications. Containerized application architecture segregates network connectivity and eliminates inter-service interference. Backup administrators often test new software versions prior to deploying them in service. NetBackup Flex Appliances streamline this process and enable backup admins to rapidly bring new versions of NetBackup online for testing. After testing, you can simply replace a containerized application with the new version or run multiple versions simultaneously.

NetBackup Flex 5350 Appliance with High Availability

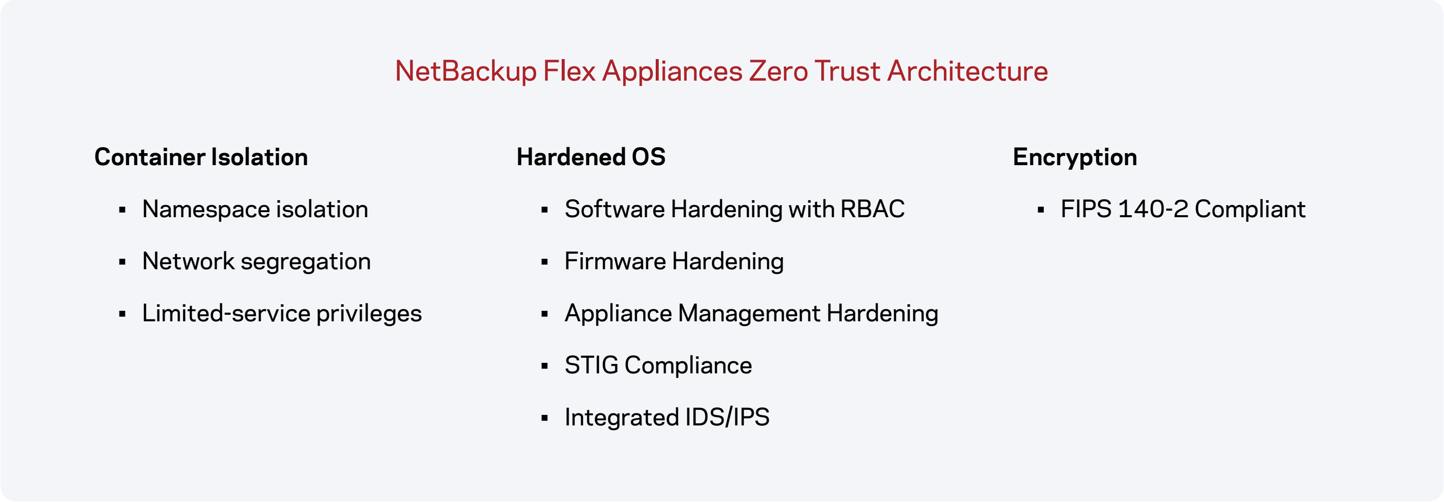
The NetBackup Flex 5350 Appliance includes InfoScale™ Availability components, enabling HA support. When configured with HA, the Flex 5350 includes two server nodes in a cluster configuration. The server nodes communicate through redundant, direct, or cross-over 1-GbE connections. In an HA configuration, services and applications on the NetBackup Flex Appliance, NetBackup services like the primary server, media server, and storage server, as well as the system services are resilient.

Deep Monitoring of the Primary Server on NetBackup Flex Appliances

From NetBackup Flex software release 2.0, the NetBackup Flex Appliance monitors the primary server's critical services. Remedial actions, like restarting a service or failing over the primary server to the other node in the cluster, will take place when a failure is detected.

Zero Trust Architecture

With the combination of a hardened OS, container isolation, and a Zero Trust security model, NetBackup Flex Appliances provide the multi-layered infrastructure immutability and indelibility necessary for ransomware protection (see Figure 6).



NetBackup Flex Appliances Zero Trust Architecture

Container Isolation

- Namespace isolation
- Network segregation
- Limited-service privileges

Hardened OS

- Software Hardening with RBAC
- Firmware Hardening
- Appliance Management Hardening
- STIG Compliance
- Integrated IDS/IPS

Encryption

- FIPS 140-2 Compliant

Figure 6. An overview of the NetBackup Flex Appliance's Zero Trust architecture.

Immutable Storage

NetBackup and the NetBackup Flex Appliances provide immutable and indelible storage that reduces the risk of malware or ransomware encrypting or deleting backup data, thereby making it unusable. Within the NetBackup Flex Appliance, the NetBackup WORM storage server offers a secure, container-based MSDP solution. NetBackup Flex Appliances offer Enterprise and Compliance lock-down modes, so you can choose the right immutability strength (see Figure 8). NetBackup and the NetBackup Flex Appliance solution have completed a third-party immutability assessment from Cohasset Associates, an industry-recognized assessor of immutability controls, specifically SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles of the Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1 .31(c)-(d).

The NetBackup Flex Appliance comes with a wide variety of security features (see the NetBackup Flex Security document for details) that include:

- OS security hardening, including Security-Enhanced Linux (SELinux)
- Intrusion Detection System (IDS)/Intrusion Protection System (IPS)
- Robust, role-based authentication
- Locked-down storage array

The NetBackup primary server communicates with the storage unit to determine the immutability and indelibility capability and WORM retention period (min/max) settings. Then the primary server sets up immutability controls on the storage unit and applies the WORM retention policy. NetBackup software provides backup image management with visual representation of the immutable lock, image deletion after the WORM retention period (via the command line interface [CLI]), and honors legal hold on the catalog. The NetBackup Flex Appliance runs the immutable storage server to provide WORM capability, retention locks, and platform hardening against ransomware and malware threats. The Compliance Clock is used for ensuring the retention period and is independent from OS time. The NetBackup Flex Appliance has two lock-down immutability modes—Enterprise and Compliance. You can enable the appliance lock-down state at any time. You can choose a Compliance mode or Enterprise mode MSDP storage container, but you cannot mix the modes.

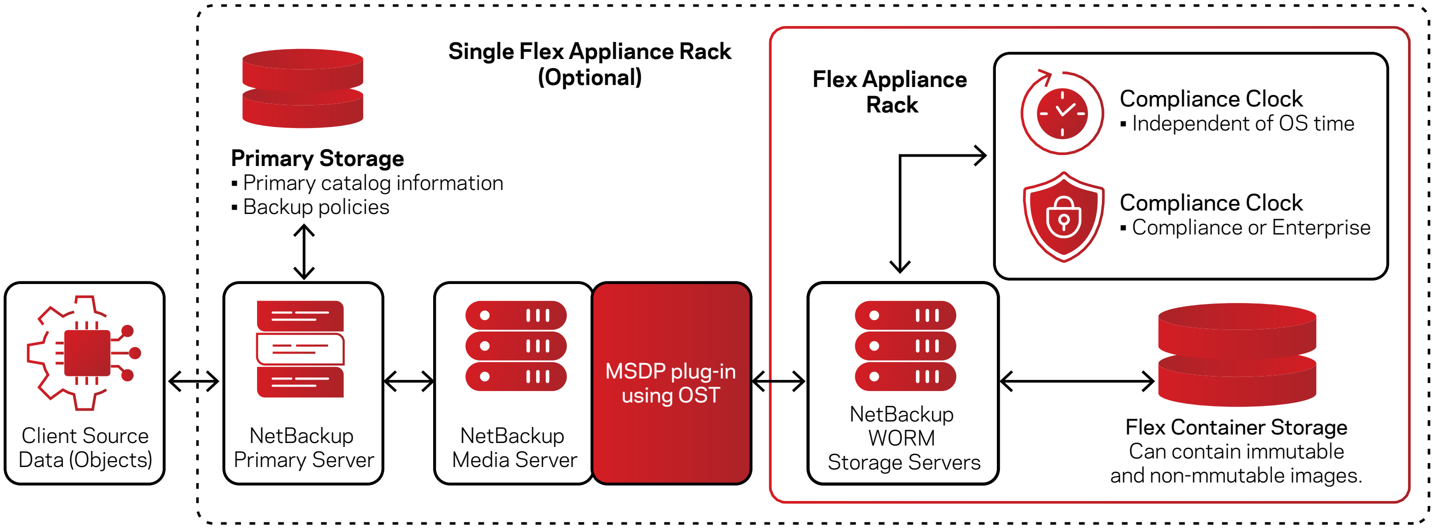


Figure 7: An overview of the Flex Appliance Immutable Storage Architecture.

Data Encryption

NetBackup Flex Appliances meet Federal Information Processing Standards (FIPS) 140-2 standards to protect customers' data via encryption in transit and at rest. This certification ensures government organizations, financial, and healthcare institutions' data handled by third-party organizations is stored and encrypted securely and with the proper levels of confidentiality, integrity, and authenticity. (See Figure 8.)

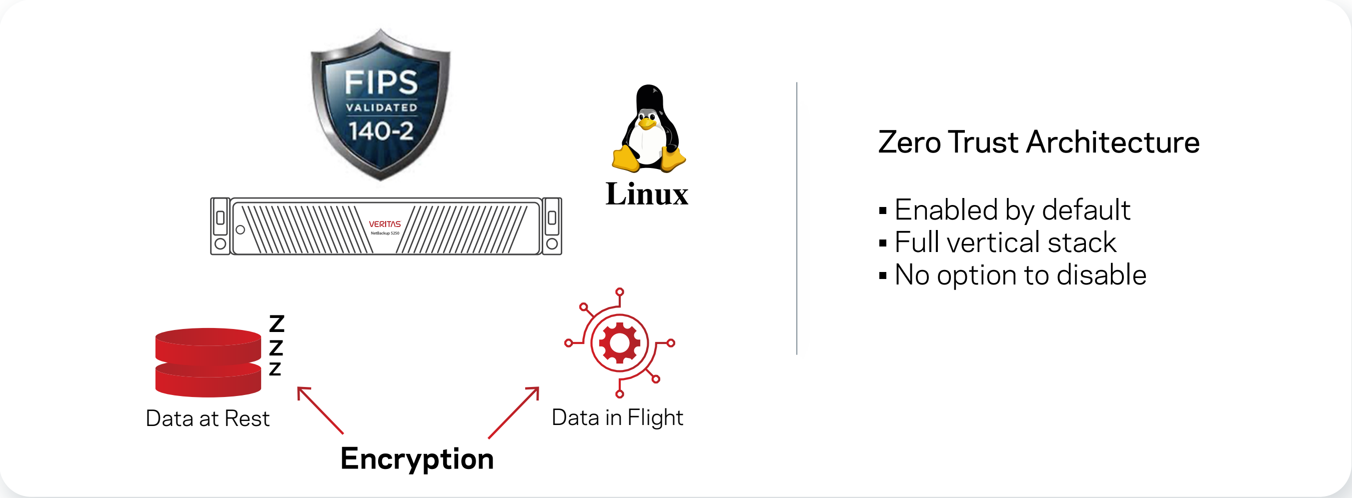


Figure 8: An overview of the FIPS 140-2 standard with which Flex Appliances comply.

FIPS is enabled on a Flex Appliance's host and infrastructure instances. SSH and sshd settings are updated to support FIPS-compliant ciphers and MAC ciphers. FIPS is enabled during the Flex Appliance installation process.

Security Technical Implementation Guide

NetBackup Flex Appliances provide organizations with peace of mind on governance and compliance issues affecting their data centers. NetBackup Flex Appliances include organic built-in layers of security. The operating system is hardened based on Security Technical Information Guide (STIG)–compliant rules established by the U.S. Defense Information Systems Agency. Flex Appliances also include IDS and IPS security software that adds additional layers of security and protects against nefarious exploits. NetBackup Flex Appliance 2.1 has STIG OS checklist, STIG OS Cat I, STIG OS Cat II/III, STIG ASD checklist and STIG-compliant disk partitioning. (See Figure 9.)

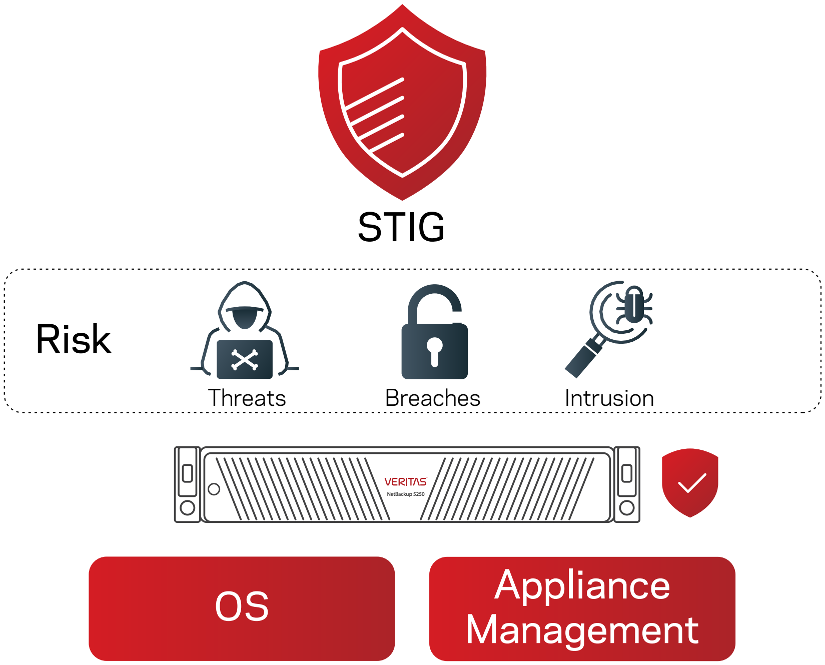
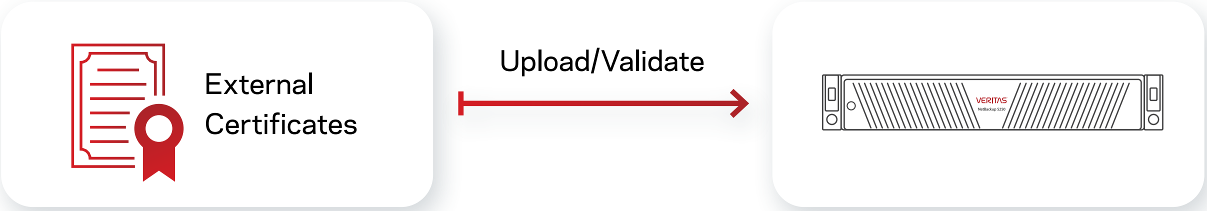


Figure 9: An overview of the STIG rules with which Flex Appliances comply.

For details, refer to the NetBackup Security and Implementation Guide and Flex Security documents to support secure deployment.

External Certificate Authorization

NetBackup Flex Appliances provide the flexibility to use certificates from an external certificate authority (ECA). You can upload and validate the ECA using the Flex web UI. Without an EC, the Flex Appliance will use the default self-signed certificates.



To use an external certificate, you must have the following:

- **Host certificate**—An X.509 certificate for the appliance, in PEM format. This certificate is different from the certificate for your NetBackup primary and media servers
- **Private key**—The RSA private key of the host certificate
- **Passphrase**—The passphrase of the private key if the key is encrypted

Log Forwarding

Log forwarding provides many benefits, including compliance, redundancy, running analytics, centralized monitoring, and reviewing threat behaviours and long-term patterns. To enhance security monitoring, analysis, and auditing, NetBackup Flex Appliances provide the capability of log forwarding to a syslog server or Splunk, expanding support for external log management platforms, and offering the flexibility for organizations to leverage their current investment areas. You can choose UDP or TCP protocols. To enhance security, you can also use TLS log transmission, a cryptographic protocol that provides end-to-end security of data sent between applications over the network (see Figure 10). You need a CA certificate and the client private key to configure TLS log transmission.

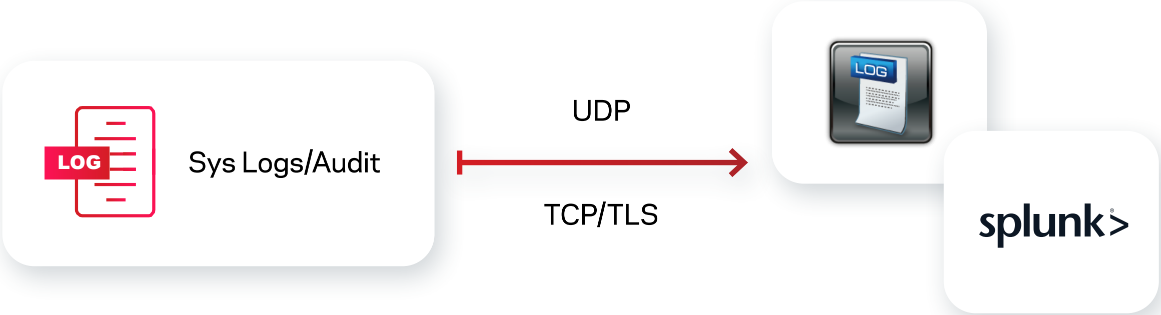


Figure 10: An overview of the log forwarding process used by Flex Appliances.

Customizable Login Banner

You can set a text banner that appears before a user signs in to the NetBackup Flex Appliance web UI, shell, and console. The typical use cases for login banners are legal notices, warning messages, and company policy information. The security banner can provide legal protection if an unauthorized user violates any access restrictions, such as Terms of Use, and accesses the system anyway.

Manageability

The Veritas Appliance Management Console is a centralized management interface for multiple appliances. It enables a single administrator to manage many appliances simultaneously. You can use the Appliance Management Console for some of your appliance and application instances management tasks.

Appliance Management Server Integration

Flex Appliances are supported on the Appliance Management Server (AMS) version 2.0 or later. AMS 2.0 or later is now available in a container form factor, which you can deploy in your container environment. You can register your Flex Appliance on the AMS server and the Flex Appliance hostname will be visible on the AMS server. You can install EEBs (add-ons) on NetBackup instances, upgrade NetBackup instances.

To enhance security, Flex Appliance and the remote management service API on AMS are enabled for HTTP2 to TLS-based communication.

AMS minimum requirements:

- Physical/virtual machine with 4 CPUs / 16 GB RAM / 200 GB disk space
- RHEL 7.9 / Ubuntu 18.04
- Docker 1.13 and above (Docker CE/EE are supported)

To install the AMS, enter the following command:

```
docker run --name ams-container -h fully.qualified.hostname.com -v </data/directory>:/data -p
443:443 appliancemgmt:2.0.0
```

Update Firmware from the web UI

You need to update the Flex Appliance firmware after you install any new hardware. As a prerequisite, all instances need to be offline . Firmware update does a version check before trying to install the Flex firmware update package. You can install only the compatible and higher version of the firmware package. You can monitor the firmware update progress through IPMI. The Flex Appliance will reboot after the firmware installation (see Figure 11).

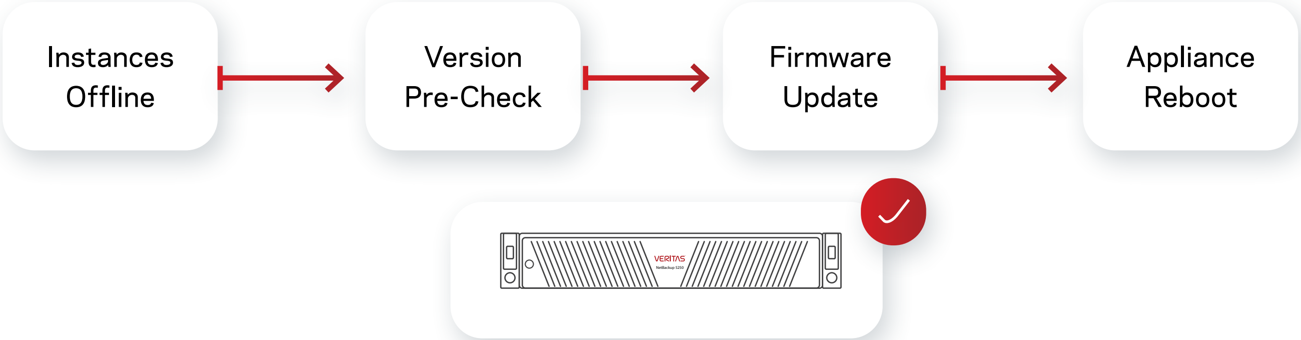


Figure 11: An overview of the Flex Appliance firmware update process.

EEB Package Management for NetBackup Instances

NetBackup Flex Appliances provide the capability to bundle multiple EEBs (add-ons) and upload them at once. To do so, follow this process:

- Identify and report the payload conflicts for the selected add-ons being applied to an instance
- Identify and report obsolete EEBs from the selected add-ons that will automatically be removed when applying add-ons to an instance
- Provide a mechanism for the user to choose between the conflicting EEBs before installing the add-ons for the instance

Optimized Workload

Manage Fibre Channel Ports

Flex Appliances support the following types of backups over Fibre Channel (see Figure 12):

- VMware SAN transport (initiator)
- Tape out (initiator)
- SAN Client (Fibre Transport Target) – supported on NetBackup 9.1.0.1 and later instances

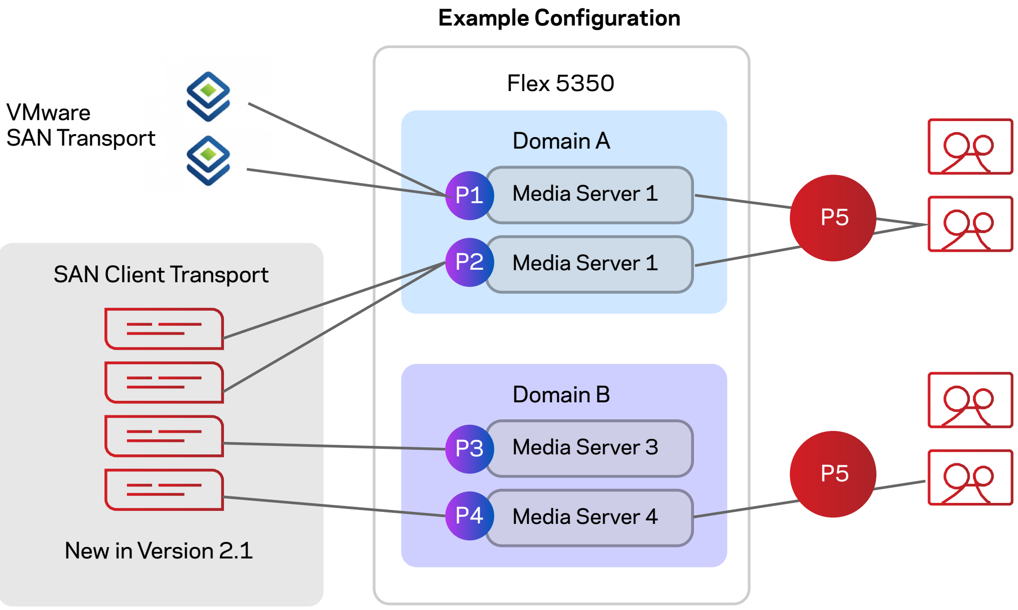


Figure 12: An overview of how Flex Appliances use Fibre Channel for backups.

VMware SAN Transport

VMware SAN transport mode only works with VMware Virtual Machine File System (VMFS) datastores version 6.0 or later. Other devices such as the raw device-mapping (RDM) format are not supported. Ensure only VMFS devices are zoned to the appliance to avoid backup failures. Refer to the NetBackup Software Compatibility List to confirm the supported VDDK versions.

For VMware backup, hypervisor-level snapshots are taken for VMs and the VM data is streamed directly from storage to backup server over Fibre Channel.

You can assign the same port to multiple instances if the instances belong to the same tenant. You can also use the same port for both VMware and tape out backups. If multiple ports are connected to the same devices, you can assign those ports to a single application instance in case one of the paths fails. You cannot assign the ports to different application instances.

SAN Client

Fibre Transport is the name of the NetBackup high-speed data transport method that is part of the SAN Client feature.

The Fibre Transport Media Server (FTMS) provides high-speed backups and restores of NetBackup clients. You can back up large amounts of data rapidly with the FTMS.

You can connect the target port to multiple SAN Clients; target ports are exclusive and cannot be shared among instances, and you can only connect one media server to one target port.

Monitoring and Reporting

AutoSupport

Veritas AutoSupport is a set of infrastructures, processes, and systems that enhance the support experience through proactive monitoring of Veritas Appliance hardware and software. AutoSupport also provides automated error reporting and support case creation. AutoSupport correlates the Call Home data with other site configuration data held by Veritas for technical support and error analysis. With AutoSupport, Veritas greatly improves the customer support experience.

Call Home

Call Home provides information regarding appliance component state and status. AutoSupport correlates the Call Home data with other site configuration data held by Veritas for technical support and error analysis. Security admins can configure Call Home events through the Flex Appliance UI. Support tickets can be created automatically in the event of hardware alerts. You can also use a proxy server for Call Home.

SNMP Alert

The Simple Network Management Protocol (SNMP) enables you to monitor appliance performance. Once an alarm is trigger, Flex Appliances can send an email alert via the SMTP server. You can also create an email template for the alerts.

Third-Party Monitoring Tools

The Flex Appliance public APIs allow organizations and developers to integrate customized codes into Veritas products and applications. Grafana is an open-source analytics and monitoring solution that lets you query, visualize, alert, and understand your metrics. You can use Flex Appliance APIs with Grafana to create, explore, and share usage and performance dashboards.

To install Grafana, see the official Grafana documentation.

To check Grafana metrics, you can look at these examples:

- Node exporter
- Prometheus

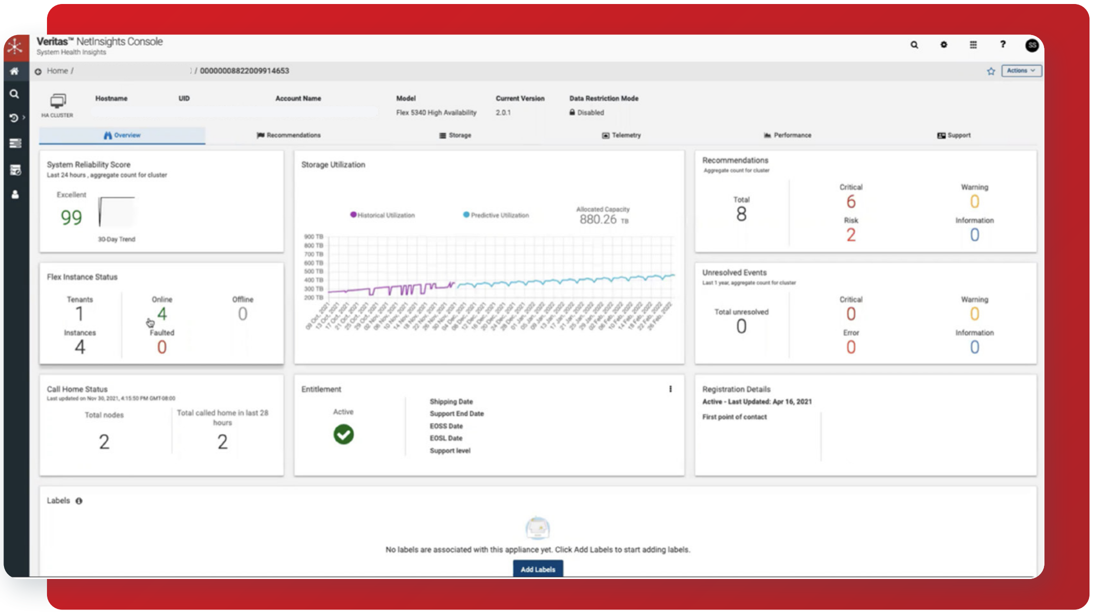
NetBackup Flex APIs are available with the Veritas™ Services and Operations Readiness Tools (SORT). APIs promote innovation, provide an additional channel for customer insights, and enhance the user experience by enabling collaboration.

You can automate a variety of management tasks and enhance performance monitoring with Flex APIs, including:

- Instance deployment
- Accessing appliance and instance performance data
    - CPU, memory, disk read and write, and network
    - "Joint" or "correlated" API to correlate what work the instance is doing in the NetBackup context to what is happening on the physical layer of the system

NetInsights Console Integration

The Veritas NetInsights Console lets you leverage accurate reporting to uncover the total amount of backup data involved and develop proactive budget decisions. By integrating Flex Appliances with the NetInsights Console, you can determine key risks and improve operational efficiency, reduce unplanned maintenance and downtime, and increase ROI with global insights and monitoring (see Figure 13).



Veritas™ NetInsights Console
System Health Insights

Home / / 00000008822009914653

Actions

HA CLUSTER

Hostname	UID	Account Name	Model	Current Version	Data Restriction Mode
			Flex 5340 High Availability	2.0.1	Disabled

System Reliability Score
Last 24 hours , aggregate count for cluster
Excellent
99
30-Day Trend

Storage Utilization
Historical Utilization
Predictive Utilization
Allocated Capacity
880.26 TB

Recommendations
Aggregate count for cluster
Total 8
Critical 6
Risk 2
Warning 0
Information 0

Flex Instance Status
Tenants 1
Instances 4
Online 4
Faulted 0
Offline 0

Unresolved Events
Last 1 year, aggregate count for cluster
Total unresolved 0
Critical 0
Error 0
Warning 0
Information 0

Call Home Status
Last updated on Nov 30, 2021, 4:15:50 PM GMT-08:00
Total nodes 2
Total called home in last 28 hours 2

Entitlement
Active ✓
Shipping Date
Support End Date
EOSS Date
EOSL Date
Support level

Registration Details
Active - Last Updated: Apr 16, 2021
First point of contact

Labels

No labels are associated with this appliance yet. Click Add Labels to start adding labels.

Add Labels

Figure 13: The NetInsights Console provides insight into system performance.

Integration with the Cloud

Data is an organization's most valuable digital resource. Because enterprises have many data types laid out across various data centers and the cloud, figuring out how to protect data silos in different locations, infrastructures, and management systems can be challenging.

NetBackup Flex Appliances are the best one-stop solution, allowing you to store data from over 800 different data sources and over 60 cloud storage targets with a single platform. NetBackup Media Server Deduplication Pool Cloud Tier (MSDP-C) enables you to back up and restore data from cloud storage as a service (STaaS) vendors.

Storage Efficiency

The most challenging factor organizations consider when choosing a long-term retention storage platform solution is storage cost.

The deduplication engine in the NetBackup MSDP stores data in a storage-optimized and portable format and is designed to transport it to any compatible target on any infrastructure. It also features storage efficiency technologies such as deduplication and compression to reduce egress and ingress costs to and from the cloud. Using MSDP, organizations have seen space savings of up to 95 percent, which means a lower storage bill at the end of the month. NetBackup can write this deduplicated data directly to local storage as well as, or in addition to, writing it to the cloud, resulting in significant cost savings for both local and cloud storage. NetBackup uses SHA-2 (SHA256) for the hash algorithm. The chunk segment size unit used to compute fingerprints is a fixed length of 128 KB by default or configurable to a variable-length size based on the chunk boundary. You have an option to encrypt deduplicated data. Both compression and encryption (if enabled) are performed after the fingerprint is calculated and prior to sending data to the target storage. NetBackup 9.1 adds support for Immutable Object storage to ensure backup data cannot be tampered with.

Security

NetBackup security and encryption provide protection for all parts of NetBackup operations on NetBackup primary servers, media servers, storage servers, and attached clients. The backup data is protected through encryption processes and vaulting. NetBackup data that is sent over the network is protected by dedicated and secure network ports. To ensure optimal security, NetBackup includes encryption features for data at rest and in motion. You can encrypt your data before you send it to the cloud. NetBackup uses the Key Management Service (KMS) to manage the keys for data encryption for cloud disk storage. KMS is a NetBackup primary server–based symmetric key management service. The service runs on the NetBackup primary server.

Simplicity

MSDP-C can support both local storage and multiple cloud storage targets. Based on the workloads, you can run the NetBackup Flex Appliances storage server, media server, or primary server containers on the same physical server. After you configure the MSDP storage server, you can add a cloud storage target to that storage server, and then the MSDP-C can store data directly in the cloud target. No matter where your data is, Veritas Appliances can help you protect and control valuable digital assets.

NetBackup Flex Appliances are designed for simplicity. It is very easy to set up cloud storage. Simply follow these steps to configure an appliance for MSDP cloud applications:

1. Create an MSDP storage server on the Flex Appliances.
2. Log in to the NetBackup web UI and configure the MSDP cloud storage:
   - Create a disk pool
   - Create a storage unit

It is clear that enterprises want to simplify data management and reduce IT complexity. The NetBackup MSDP-C server cloud tier provides protection for your data regardless of whether it is in the data center or the cloud. NetBackup Appliances and NetBackup Flex Appliances include NetBackup, the industry leader in data protection software, providing an efficient, secure, and simple solution.

Flex Appliance Models and Use Cases

The NetBackup Flex Appliance portfolio includes the NetBackup Flex 5150, 5250, and 5350 Appliances for edge/remote and core data centers.

Flex 5150 Appliance

The Flex 5150 is a purpose-built, cloud-connected NetBackup data protection solution in a self-contained, compact, easy-to-use appliance. The Flex 5150 expands the NetBackup family of appliances to the edge of the enterprise network and to departmental organizations within the enterprise. Flex 5150 use cases include:

- An enterprise backup team remotely managing edge solutions
- A standardize backup platform across all locations
- Multiple remote locations with a small number of clients and a limited amount of data to protect; data must be protected locally and backups replicated to a data center or the cloud for disaster recovery (DR)

The Flex 5150 is a 1U server system with no external storage shelf component designed for remote offices with smaller workload requirements. This design offers a simplified appliance that is reliable and cost-effective. You can run the protection job at the remote office on a nightly basis and replicate the backup data to a central office or data center. You can manage the Flex 5150 remotely without on-site technical support.

Flex 5250 Appliance

The Flex 5250 provides dynamic expandable storage capacity of up to 429 TiB, making it ideal for remote locations as well as enterprise data centers. The Flex 5250 also serves as a gateway unit for sending optimized backups to the cloud.

Flex 5350 Appliance

The Flex 5350 includes an enterprise-grade, resilient, HA hardware platform, plus a powerful Flex software platform with integrated Docker technology. Organizations can use the Flex 5350 to quickly provision multiple NetBackup servers in almost any configuration, including multiple NetBackup domains.

Flex 5350 use cases include:

- Running multiple NetBackup instances on a single Flex 5350
- Possible NetBackup instances that include a primary server, media server, and MSDP-C
- Each server instance runs in an isolated container, independent from any others
- Running multiple domains on a single appliance with full segregation

NetBackup servers are organized into logical constructs known as tenants, which can be configured to run as separate, isolated server groups with distinct storage and networking attributes. This capability allows organizations and partners to leverage the Flex 5350 as the foundation for offering backup functions as a service to end users while maintaining multi-tenant separation and security.

All Flex Appliances provide a complete, cloud-connected NetBackup data protection solution in a self-contained, compact, and easy-to-use appliance. Table 5 provides the Flex 5150, 5250, and 5350 positioning and hardware configurations.

Table 5: NetBackup Flex 5150, 5250, and 5350 Positioning and Technical Details

	Flex 5150	Flex 5250	Flex 5350
Use cases	Streamlined protection for remote, branch, and edge locations	Branch, remote office, and small to mid-size enterprises	Predictable highest- performance data protection with converged, highly availableHA, and operationally resilient solution for medium midsize and large-scale enterprises
Usable storage capacity	13.23 TiB	429 TiB maximum storage	240 TiB – 1,920 TiB Shelf: 240/480TB 1–4 Shelves
CPU	1X 1x Intel Xeon 3106 CPU	2x Intel Xeon 4214 CPUs @ 2.4 GHz	2x Xeon 6230R CPUs @ 2.1 GHz (26 cores each)
DDR4 memory @ 2933 MHz	64 GB	64 GB- 512 of DDR4 RAM	768 GB or 1.5 TB
Ethernet Pports	up to 2	1 GbE NIC - 4x 25/10 GbE NIC - up to 6x	1 GbE NIC - 4x 25/10 GbE NIC - up to 8x
Dimensions H x W x D cm (inches)	4.32 x 48.26 x 79.38 (1.7 x 19 x 31.25)	8.9x48.26x76.9 (3.5x19x30.25)	8.9 x 48.3 x 76.9 (3.5 x 19.0 x 30.5)
Maximum weight with disk drives (pounds/ kilograms)	36/16.4 appliance 6/2.7 optional mounting rails	53/42.1	43/19.5
Maximum power consumption	160 watts	500 watts	600 watts
Operating temperature (oF/oC)	50-95/10-35	50-95/10-35	50-95/10-35
AC voltage range	100–127 volts / 200–240 volts	100–127 volts / 200–240 volts	90–140 volts/ 180–264 volts

For more information on Flex Appliance models, refer to the following:

- Flex 5150 data sheet
- Flex 5250 data sheet
- Flex 5350 data sheet

Best Practices

Flex Appliances use container technology to enable multiple workloads and applications to run on a single Flex Appliance. Each application runs within an independent container, but all applications share the same underlying hardware resources—CPU, memory, disk I/O, and network. It is a best practice for organizations to plan the applications that run on the Flex Appliance and properly size, configure, and tune the Flex Appliance. Refer to the NetBackup Flex Appliances Best Practices for sizing and best practices.

Conclusion

NetBackup Flex Appliances bring the agility, efficiency, and security of container technology to NetBackup data protection. You can run multiple NetBackup deployments on a single NetBackup Flex Appliance and create new deployments and upgrade in minutes. NetBackup Flex Appliances efficiently tier to the cloud with NetBackup MSDP Cloud Tier. NetBackup Flex Appliances' ease of use lets you quickly respond in a rapidly changing business environment.

References

- NetBackup Flex Appliance Product Documents
- NetBackup Product Documents

Versions

Flex Version	Date	Author	Key Updates
1.4	May 2020	Rachel Zhu	Original document
2.0	Sep 2020	Rachel Zhu	▪ Immutable storage server ▪ Application service monitoring and failover ▪ Fibre Channel ▪ Supportability – Easy access and log download
2.0.1	May 2021	Rachel Zhu	▪ Instant Recovery and Universal Share ▪ MSDP-C ▪ New hardware: 5350 and 5250
2.1	Nov 2021	Rachel Zhu	▪ AMS integration, API token, reporting and log, security enhancements

About Veritas

Veritas Technologies is a global leader in data protection and availability. Over 80,000 customers—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at @veritastechllc.

VERITAS™

2625 Augustine Drive
Santa Clara, CA 95054
+1 (866) 837 4827
veritas.com

For global contact
information visit:
veritas.com/company/contact