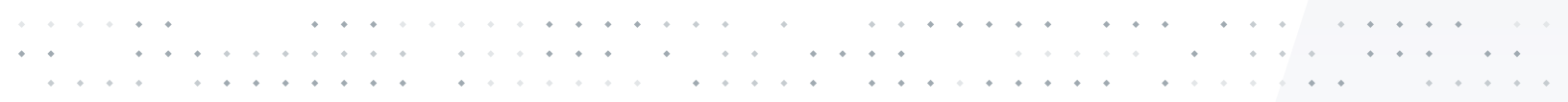


NetBackup Isolated Recovery Environment

Build a multi-layer fortress to protect your data.



Contents

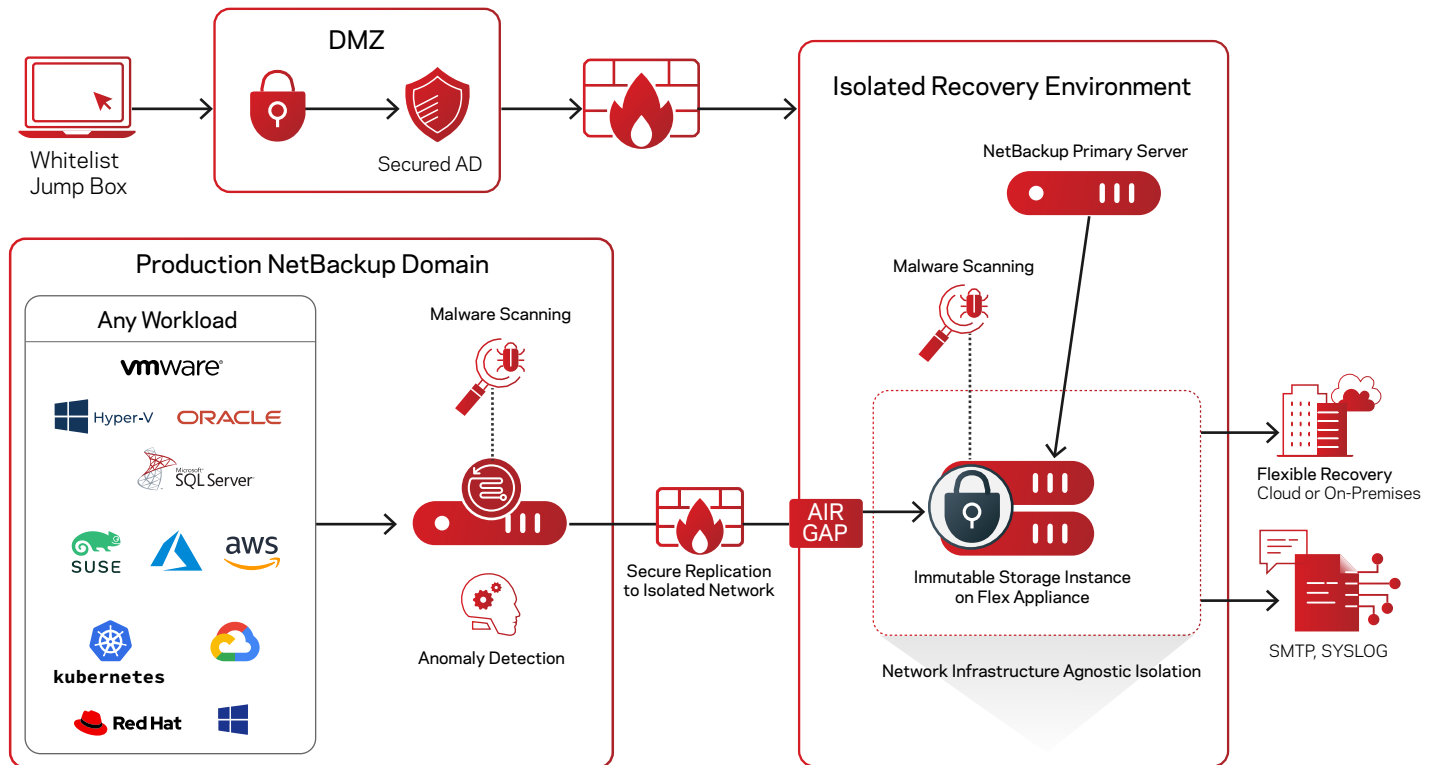
Overview	3
NetBackup Flex IRE Architecture	4
Protect	4
Detect	4
Recover	4
NetBackup Anomaly Detection and Malware Scanning	5
NetBackup Flex Appliance Enhanced Security.	5
Flex Appliance Zero Trust Architecture	5
NetBackup Flex Appliances Immutable Storage.	6
NetBackup Malware Scanning and Anomaly	6
Flex Air Gap Deployment	8
Configuring the Air Gap	9
Summary11
References.11
Versions.11

Overview

It's common for malware attacks to enter your primary environment and target your backup data. Customers have concerns about the reliability and speed of recovery from ransomware attacks. After posting record highs throughout 2021, SonicWall recorded a high of 78.4 million ransomware attacks in the month of June 2021 alone (that is over 30 attacks per second). SonicWall reported over 623.3 million attacks globally. This total marked a 105% increase over 2020 and more than triple the number seen in 2019.

For enhanced ransomware resiliency, it is important to not only secure your backup data on immutable storage but also to maintain an isolated copy of your backup data. This is often referred to as an air gapped copy. An Isolated Recovery Environment (IRE) enables air-gapped backup copies by disabling network connectivity to a secure copy of your critical data, providing administrators a clean set of files on demand to neutralize the impact from a ransomware attack. The NetBackup IRE solution:

- Stores an isolated copy of the data ensuring it stays unaltered until it's no longer needed
- Ensures data is immutable and indelible – minimizing threats from both ransomware and rogue users
- Detects ransomware infections within the protected data to prevent re-infection when restoring data
- Enables recovery operations at scale so business services can meet service level objectives
- Enables predictable recovery processes that can be rehearsed to on-premises or cloud infrastructure



Unlike traditional IRE solutions, the NetBackup IRE solution offers a unified, scalable solution with immutability and indelibility. In addition, the Veritas IRE is based on the Flex appliances' container-based multi-tenant WORM storage with hardening OS and a zero-trust architecture without additional license cost. NetBackup Anomaly and Malware Detection provides another line of defense against malware propagating in the environment. NetBackup IRE provides a simple means to determine Service Lifecycle Policy (SLP) windows and configure an Air-Gapped schedule for maximum protection with a simple streamlined approach.

Veritas' IRE solution provides a high performance NetBackup solution with zero-trust security without any extra license cost.



Performance

- High throughput, fast backup and restore
- Active/Active high availability support increases reliability and performance



Security

- Microservices implementation of NetBackup processes further lowers attack surface
- No successful malicious penetration or compromise of hardened appliance solutions on record



Cost

- Significant OpEx savings, container based to consolidate NetBackup deployments
- Supports all key enterprise deployment models increase data protection flexibility and choice



Simplicity

- No third-party add-ons required for Cyber Resiliency based on NetBackup
- Anomaly scanning is fully integrated into core NetBackup

NetBackup Flex IRE Architecture

The Veritas IRE solution focuses on 3 pillars: Protect, Detect, and Recover.



Protect

One copy of the backup images is stored on the primary site and a second is replicated to a WORM storage container on a Flex Appliance. The IRE provides another line of defense against malware propagating in the environment by isolating the second copy of the backup in a network isolated immutable storage. It works by disabling this WORM storage container's network access to the production network outside of the replication window. The Flex Appliance also includes multiple layers of security built-in including a hardened OS, zero trust architecture, immutable and indelible storage, and infrastructure to further protect your backup data.



Detect

The Veritas IRE solution includes anomaly detection and malware scanning. The AI driven anomaly detection can identify abnormalities in backup behaviors and can automatically initiate malware scanning. The malware scanning can detect infected files within backup images.



Recover

The IRE provides a secure copy of the critical backup data, providing administrators a clean set of files on demand for recovery. NBU detects impacted images, alerts the backup administrator and provides the capability of viewing the impacted files list, expiring all copies, The last-known-good image will be clearly visible in the recovery workflow and selecting an impacted image will present several warnings to the user.

To ensure quick recovery, Instant Access technology is available from the IRE site, allowing compute or application workloads to be launched directly from IRE backup storage.

NetBackup Anomaly Detection and Malware Scanning

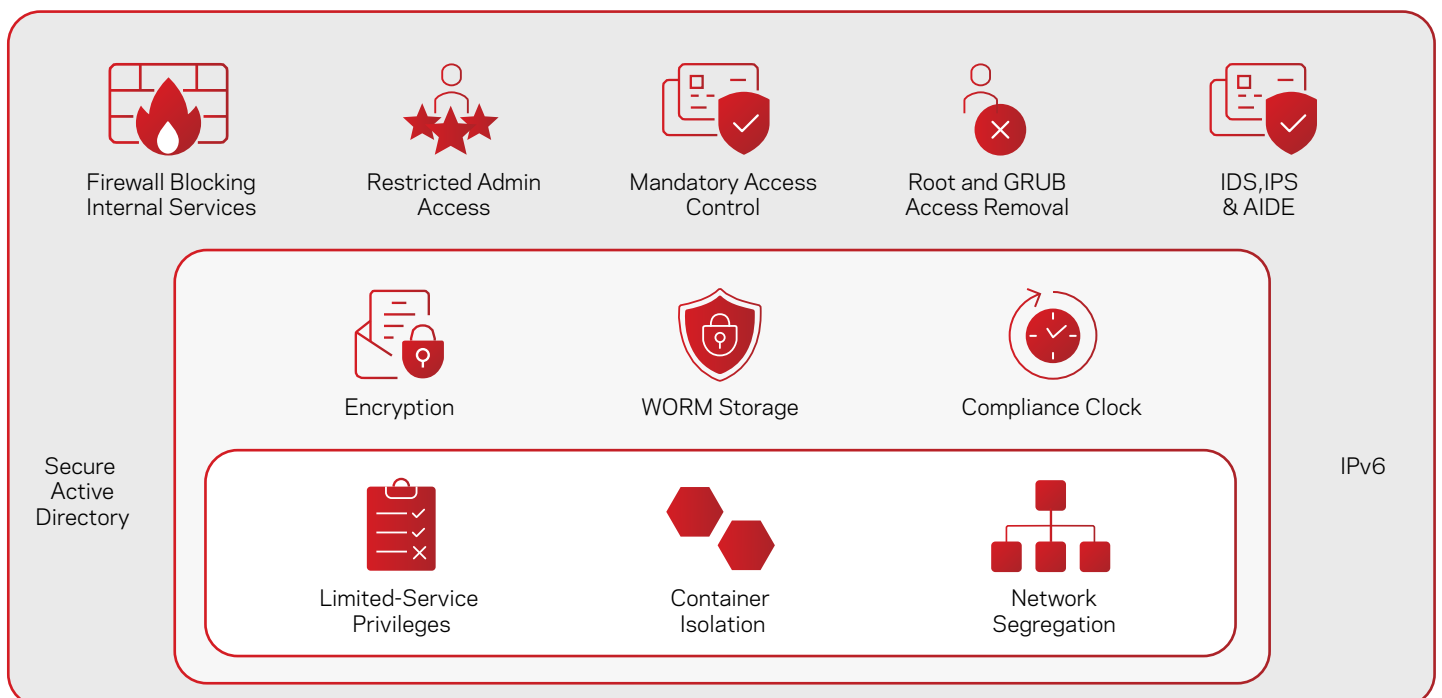
The AI driven anomaly detection can identify abnormalities in backup behaviors and can automatically initiate malware scanning. With the NetBackup Anomaly Detection engine and malware scanning running on the production side, anomalies in the backup process are automatically and continuously analyzed to avoid transferring malware to the IRE side. Data transfer to the IRE Air Gap site is done using NetBackup storage lifecycle policies. The immutable storage server at the recovery site provides a complete immutable storage solution to defend your backup data. The immutable and indelible data cannot be changed for a determined length of time to protect data against cybercriminal intrusion and internal threats. You can transfer data from multiple immutable storage servers in one or multiple NBU domain(s) to a single IRE domain. We suggest adding Malware Detection workflows on the IRE side. The last-known-good image will be clearly visible in the recovery workflow and selecting an impacted image will present several warnings to the user. If we find something infected in the immutable storage, the image cannot be expired before the minimum retention period, but in this situation, administrators will know there is infection and can plan accordingly. Also, you can scan the image before the recovery, NetBackup will give warnings on detection before the restore. Malware Detection offers a powerful point of insight into the backup images as a response to an alert or on-demand scan of a backup image.

NetBackup Flex Appliance Enhanced Security

Flex Appliance is designed with security at the forefront. With a zero-trust architecture, hardened OS and immutable storage it provides the easiest way to deploy a secure IRE environment.

Flex Appliance Zero Trust Architecture

Zero trust architecture is designed to use the least privileges needed to complete a particular task based on roles and permissions, combined with robust user authentication, authorization and policy-based data protection. With Zero trust architecture Veritas NetBackup Flex Appliances provides a unified, multi-layered platform approach to seamlessly integrate intelligent protection, comprehensive detection, and industry-leading backup and recovery. With a container-based architecture, Flex offers multi-domain isolation, network segregation and limited-service privileges. With WORM storage, STIG fully compliant OS hardening, FIPS140-2 compliant data encryption, and comprehensive security access controls, NetBackup Flex Appliances provide a complete immutable and indelible storage solution to ensure your system and data are recovered.



STIG (conforms to latest), DISA (RHEL 7 VERE profiles, CAT1 and CA2 compliant

FIPS 140-2 compliant

Veritas data protection appliances provide native ransomware recovery for business-critical data—at any scale—with near-zero RPO and RTO. Some key benefits include:

- Simplifying IT management with immutable storage
- A secure by default architecture
- Integrated highly available system configurations

NetBackup Flex Appliances Immutable Storage

Veritas NetBackup Flex Appliance provides a complete immutable storage solution to defend your backup data. Flex Appliance runs immutable storage server(s) to provide WORM capability with retention locks. With the combination of an immutable WORM storage, a hardened OS, container isolation and zero-trust security model, NetBackup Flex appliance provides the multi-layered infrastructure immutability and indelibility necessary for ransomware protection.

NetBackup and Flex Appliance immutability solutions meet the Cohasset Immutability assessment requirements (in compliance mode):

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f)
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c)
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d)

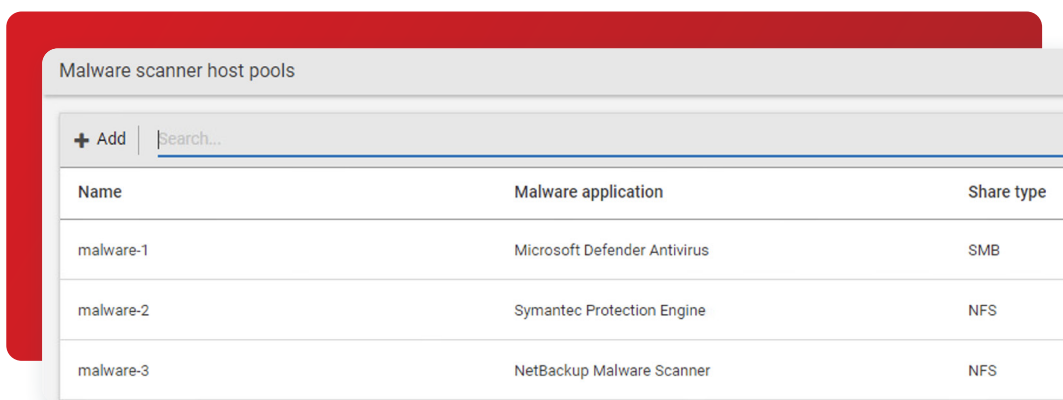
To see the full assessment, visit

<https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup>.

NetBackup Malware Scanning and Anomaly

NetBackup Malware Detection provides more control in the detection and recovery portions of the workflow. On-demand malware scans and malware scans triggered from high anomaly scores ensure confidence in the data integrity of the backup image. Storing the scan's status in the NetBackup catalog empowers you to restore confidently with visibility into the malware scan status. Add your malware scanning engine to NetBackup for added resistance to the growing cyber-terror threats.

The integrated NetBackup malware engine allows you to perform on-demand scans of backup images for latent threats. The NetBackup 10 release also includes integration with leading malware scanners such as Microsoft Defender, and Symantec Protection Engine.



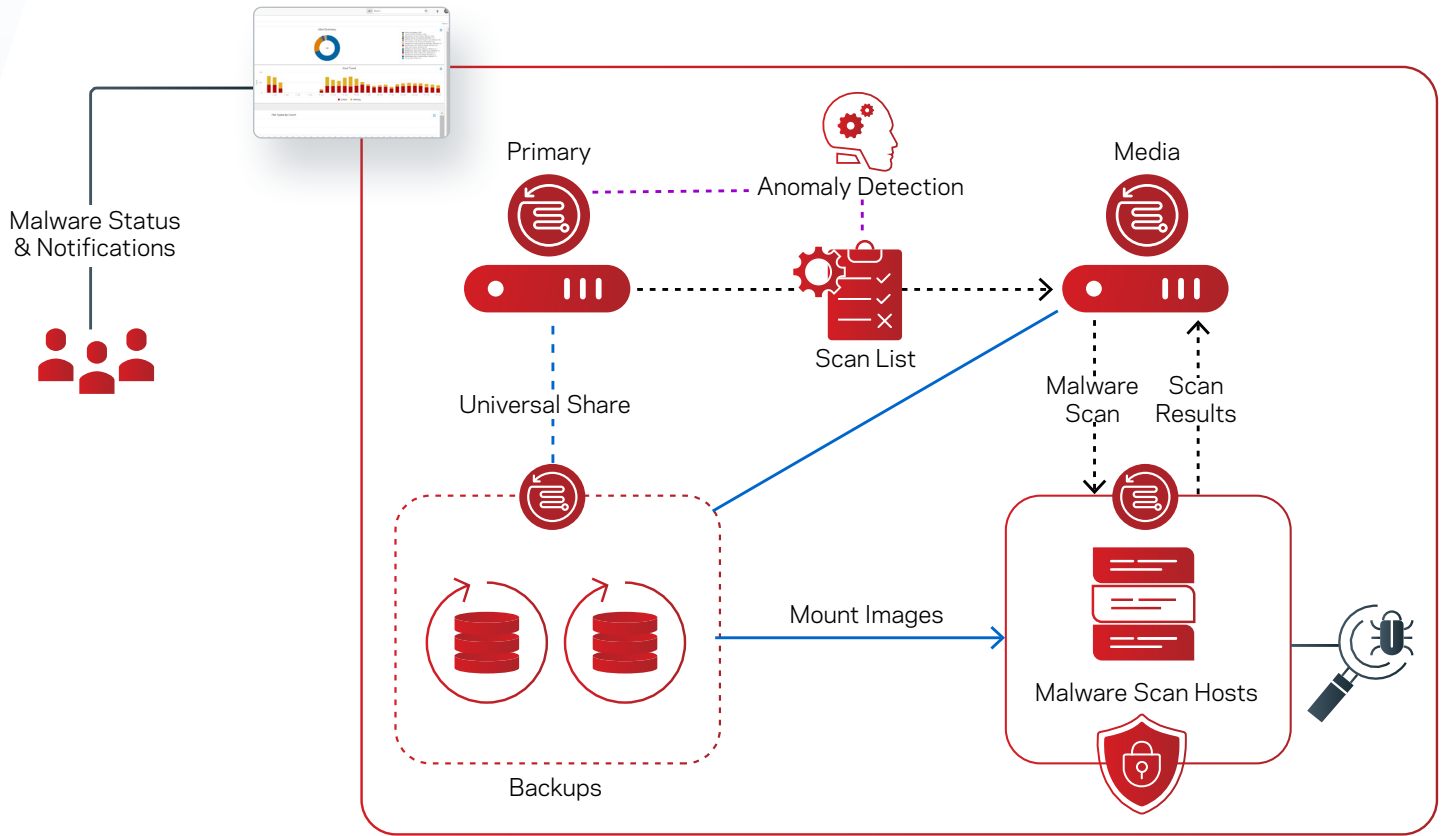
Name	Malware application	Share type
malware-1	Microsoft Defender Antivirus	SMB
malware-2	Symantec Protection Engine	NFS
malware-3	NetBackup Malware Scanner	NFS

Malware scanners can be deployed on one or more hosts, depending upon concurrent scanning requirements. These scan hosts are grouped together into a scan pool that is capable of inspecting unstructured data of either MS-Windows or Standard data types.

Malware scanning can be initiated using the WebUI or launched automatically when a high anomaly score is generated from Anomaly Detection activity. You can also create custom data protection workflows using our powerful APIs. Scan pools should be configured with a common malware application along with the desired protocol and you should not mix engines or protocols when adding additional scan hosts.

Malware Detection leverages Universal Shares so you don't need to configure a specific share for scanning. NetBackup Flex appliances have all the pre-requisites for Malware Detection and support SMB and NFS shares.

The MSDP host exposes the image to the scan host as a read-only share so there is no additional risk to read a potentially infected image. As an image passes through its Storage Lifecycle Policy (SLP), you can scan images once they reside on MSDP without interrupting the secondary SLP operations.



An on-demand scan model in the NetBackup WebUI is focused on periodic inspection of images, with the option of enabling automatic scanning for images with high Anomaly Detection scores. Focus your on-demand scans against the high-risk hosts—hosts interfacing with the public internet, Internet-of-Things (IoT) devices and other edge machines.

On-Demand scanning targets images within a specific range for a specific host, and each image will be scanned in a single job. The scan's output status is stored with the image and offers common remediation actions. This also triggers an alert in the top right of the WebUI.

Once an impacted image is detected, you can view the impacted files list, expire all copies, or leave the image in place where the scanning status tag will alert when the backup image is selected in a recovery workflow in the future. The last-known-good image will be clearly visible in the recovery workflow and selecting an impacted image will present several warnings to the user.

Client	Backup time	Scan result	Backup type	Date of scan ↑	Malware application	Number of files impacted
efaf3312306.virta	September 24, 2021 12:19 PM	Not impacted	Full	September 24, 2021 12:25 PM	Symantec Protection Engine	0
efaf3312306.virta	September 24, 2021 12:21 PM	Impacted	Full	September 24, 2021 12:25 PM	Symantec Protection Engine	1
efaf3312306.virta	September 24, 2021 12:19 PM	Not impacted	Full	September 24, 2021 2:09 PM	Symantec Protection Engine	0
efaf3312306.virta	September 24, 2021 12:21 PM	Impacted	Full	September 24, 2021 2:09 PM	Symantec Protection Engine	1

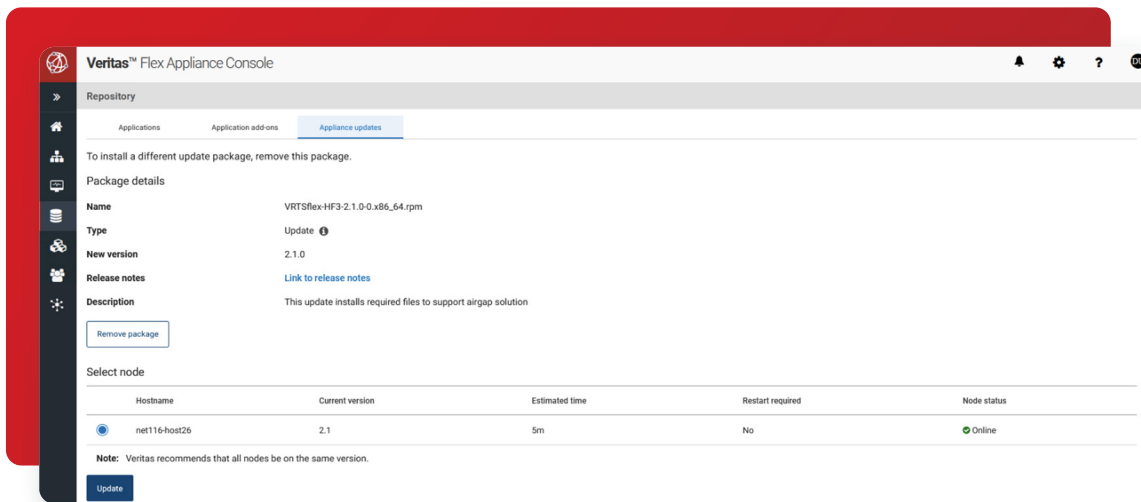
Flex Air Gap Deployment

The following versions have been tested and are supported for this solution:

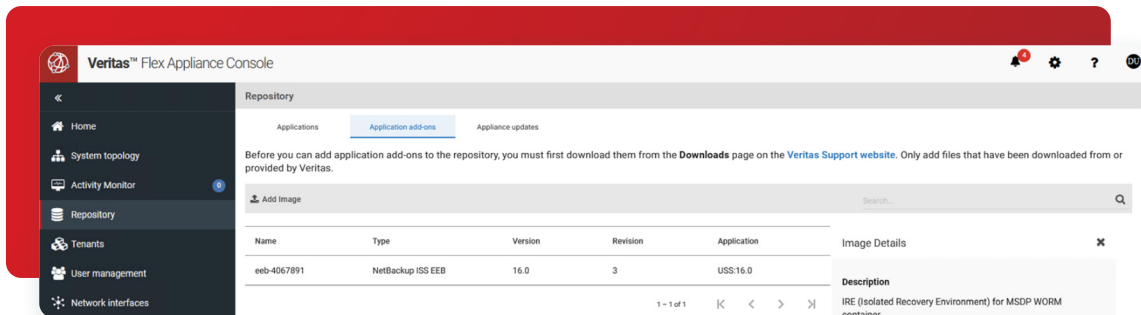
- NetBackup 10.0
- MSDP 16.0
- Flex 2.1

The production domain simply requires a NetBackup deployment, no additional steps are required. The IRE domain requires the a NetBackup Flex Appliance deployment as well as the additional steps listed below.

1. Upload the Veritas IRE hotfix VRTSflex-HF3-2.1.0-0.x86_64.rpm through the Flex Appliance console "Repository" -> "Appliance updates"-> "Add package", then apply the update.

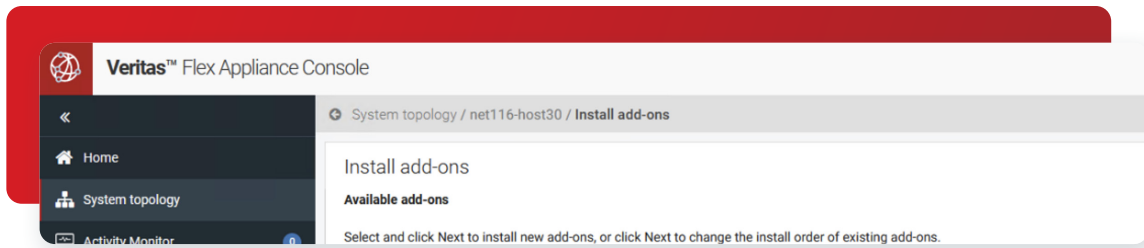


2. Upload the MSDP 16.0 Veritas IRE EEB through Flex Appliance console "Repository" -> "Appliance add-ons" -> "Add Image" to apply it.



3. Stop the MSDP WORM instance and then apply the Veritas IRE MSDP EEB through the Flex Appliance console:

- "System topology" -> MSDP WORM instance "Name" -> "Add-ons"
- Choose the EEB uploaded at step2 and apply it
- Start the WORM instance after applied the EEB

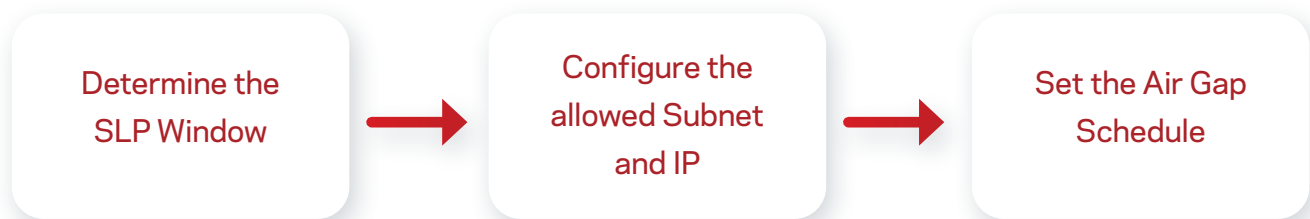


After NetBackup deployment is completed on both the Production and IRE domains, refer to the chapter “Configuring replication” in “Veritas NetBackup™ Administrator’s Guide, Volume I” for configuring Auto Image Replication from the Production domain to the IRE domain, and choose the MSDP WORM storage as the target storage unit.

Please note that the IRE network control schedule open windows should be configured as the same time windows used for the SLP replication window on the production domain.

Configuring the Air Gap

Configuring the Air Gap involves determining the period of time that the network is available for replication from the production site. Outside of this period of time all network access to the Flex appliance is disabled except for any specific IP addresses or subnets as defined by the IRE admin.



1. Determine the SLP Window

Before configuring the Air Gap, an understanding of the schedule required to perform normal replication from the production site to the IRE site is needed. This can be determined by running the `show-slp-windows` command on the IRE’s MSDP restricted shell. This command collects the information on all SLP windows to this MSDP server from the given primary server and generates a report.

Usage of the command is as follows:

```
[msdp-16.0] ire-msdp > setting ire_network_control show-slp-windows production_primary_server=<examplePrimary.domain.com> production_primary_server_username=<prodUsername> ire_primary_server=<exampleIREPrimary.domain.com> ire_primary_server_username=<ireUsername>
```

Where `<examplePrimary.domain.com>` is the fully qualified domain name (FQDN) of the primary server in your production environment, and `<exampleIREPrimary.domain.com>` is the FQDN of the primary server in the IRE. The `ire_primary_server` should match the Target primary server as configured in the SLPs in the production environment.

Where `<prodUsername>` is a user with permission to list SLPs and SLP Windows in the production environment and `<ireUsername>` is a user with permission to list SLPs and storage units in the IRE environment.

It is important to note that the start times in the output of this command are in the production primary server’s timezone. If the production and IRE environments are in different timezones, the start times will need to be adjusted before setting the air gap schedule.

2. Configuring Allowed IPs and Subnets

The allowed IPs and subnets are configured using the `ire_network_control` command on the IRE MSDP restricted shell.

For the VERITAS IRE to remain healthy, the IRE Primary Server, IRE Media Servers, and the DNS server for the IRE environment must be included in the allow list. If all these servers are in the same subnet, only the subnet is required to be in the allow list.

Example: Configuring specific IP's and subnets for the allow list.

The example below would add the IP address 70.80.120.208 and the 10.84.48.0/20 subnet to the allowed list:

```
[msdp-16.0] ire-msdp > setting ire-network-control allow-subnets subnets=10.80.120.208,10.84.48.0/20
```

```
[msdp-16.0] ire-msdp > setting ire-network-control show-allows
```

The following subnets are allowed to connect even when the external network is closed:

```
'10.80.120.208,10.84.48.0/20'.
```

3. Setting the Air Gap Schedule

Now that the SLP windows are understood and the allowed IPs and subnets are configured, the Air Gap schedule can be set. This is also performed with the `ire_network_control` command on the IRE MSDP restricted shell.

Refer to the previous section "Configuring Allowed IPs and Subnets" for the command usage.

For the IRE schedule, a simple daily schedule is required for the Flex 2.1 release. More complex scheduling will be available in a future release.

When setting the schedule, the timezone is assumed to be the timezone of the IRE WORM storage server.

Examples:

To list the current schedule:

```
[msdp-16.0] ire-msdp > setting ire-network-control show-schedule
```

```
Current time is Fri Feb 25 01:16:18 2022
```

```
No schedule is configured
```

To set a schedule with a specific start time and duration:

```
[msdp-16.0] ire-msdp > setting ire-network-control set-schedule start_time=16:00:00 duration=02:00:00
```

```
External network is configured to be open at 16:00:00 every day. The duration is 02:00:00
```

Summary

The combination of NetBackup's anomaly detection and malware scanning with Flex Appliances' multiple layers of security in an airgapped configuration provides the easiest and most secure way to protect your important backup data. Recover your applications quickly with Universal Share and have confidence that you are recovering from a known clean copy with the clean restore option.

References

- Flex Appliance Product: https://sort.veritas.com/documents/doc_details/FAPP/2.1/Veritas%205350/Documentation/
- NetBackup Product: https://sort.veritas.com/documents/doc_details/nbu/10.0/Windows%20and%20UNIX/Documentation/

Versions

Flex Version	Date	Author	Key Updates
2.1	Mar 2022	Rachel Zhu	Original document

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](https://twitter.com/veritastechllc).

VERITAS™

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

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