VERITAS

NetBackup Isolated Recovery Environment

Build a multi-layer fortress to protect your data.

White Paper | September 2022

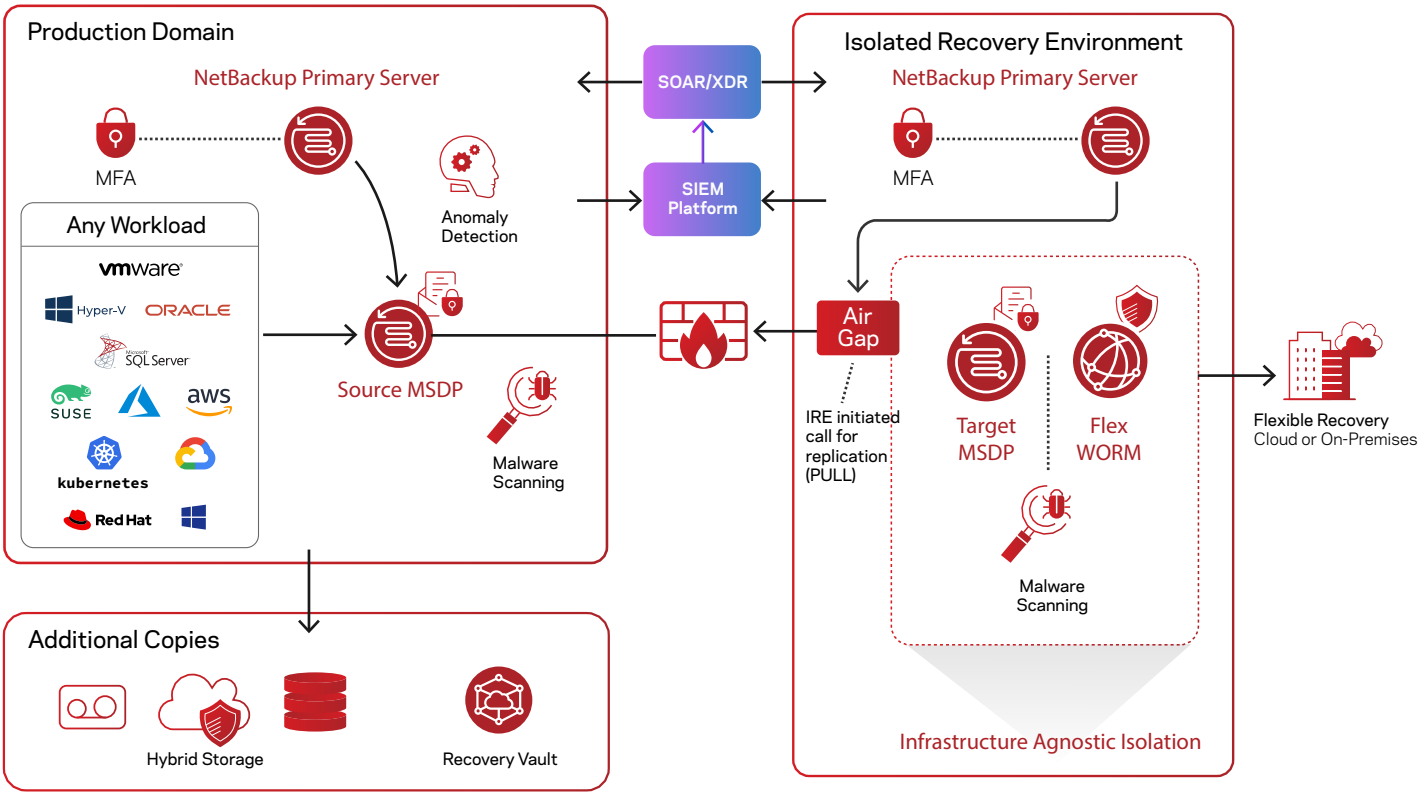
Contents

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 Isolated Recovery Environment solution:

- Ensures data is immutable and indelible – minimizing threats from both ransomware and rogue users
- Detects ransomware infections within the protected data to prevent reinfection 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. As of NetBackup 10.1, the air-gap restricts network access to the IRE all the time and works for Flex Appliances and BYO.

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

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. NetBackup 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.

Restricts Network Access to the IRE Environment all the Time With NetBackup

Traditional network isolation solutions physically or logically break connectivity between secure locations. Commonly referred to as the "pushing" of replication data from the source to the target, this traditional approach, limits the time available to replicate critical data into a secure environment.

In a Push model, the source domain is independently calculated and controlled when initiating a replication job to a target domain. By contrast, the Pull model "pulls" the replication request from the source through a specific window as defined in the IRE air gap schedule. By initiating a data transfer request from inside the IRE domain, you have better control over data flow to secure the environment further both logically and physically.

As of version 10.1, NetBackup's IRE solution optimizes data movement by offering a "Pull" replication model whereby the request to send data comes from the IRE side, the MSDP reverse connection.

You can deploy the tertiary copy of the backup images behind a firewall to an isolated environment without opening any inbound firewall ports to NetBackup. This keeps the environment secure, allowing a sandbox approach to perform malware scans or test recovery procedures before recovering at a larger scale. Customers can optionally add a physical air gap as an additional layer of protection. By empowering the destination environment to request the data from the source environment—by invitation only, we can support 24x7 data movement while isolating the stored data from any potential threats.

NetBackup Anomaly Detection

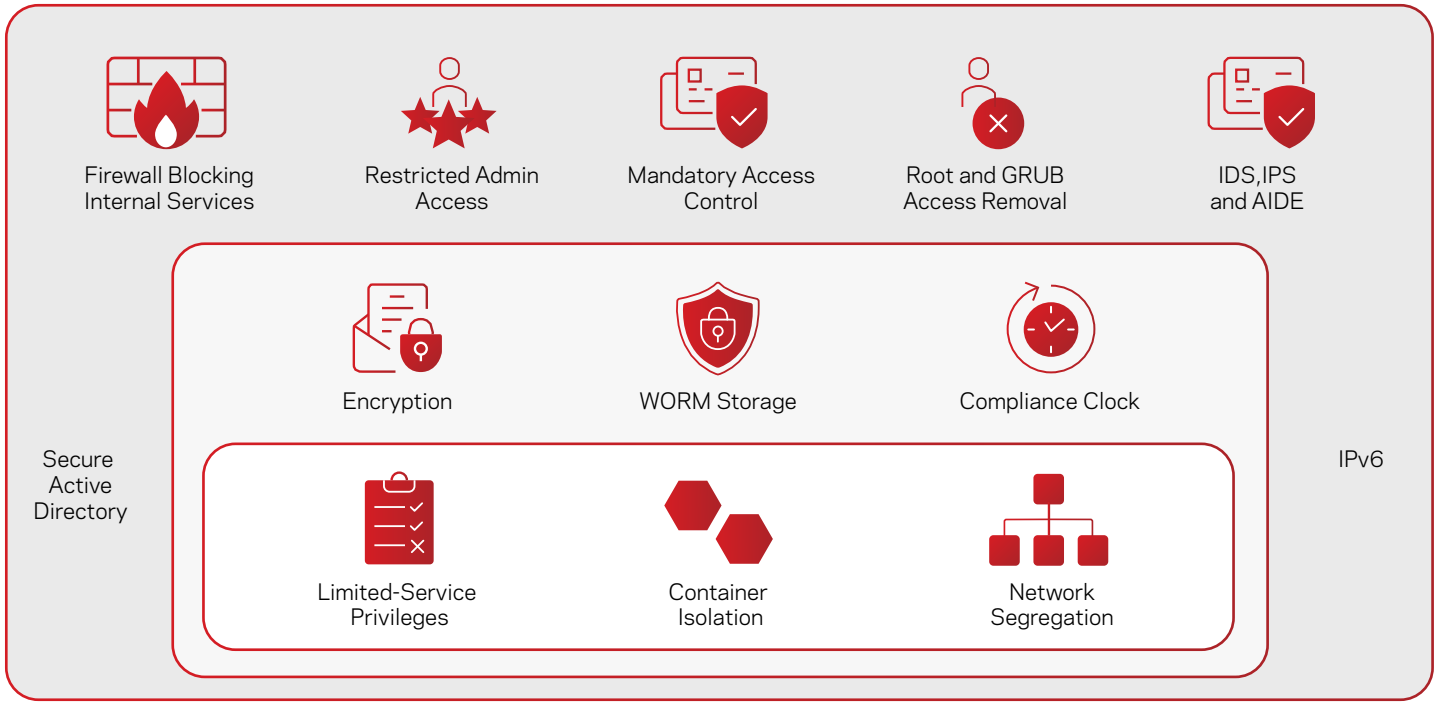
The machine learning (ML)-driven anomaly detection can identify backup behavior abnormalities and automatically initiate malware scanning. With the NetBackup Anomaly Detection engine and malware scanning running on the production side, anomalies in the backup process are automatically and continuously analyzed. Detecting anomalies in backup images provides the backup administrator with an important metric that plays a role in the organization's security posture and understanding trends and deviations in the data protection footprint. Anomaly Detection was previously only possible through rigorous manual analysis of the NetBackup Activity Monitor, but with the Anomaly Detection engine, this is now automated. Introduced in NetBackup 9.1, Anomaly Detection uses metadata already available to key in on likely indicators of issues. An anomaly is any significant change in backup image size, number of backup files, data that is transferred in KB, deduplication rate, or backup job completion time. NetBackup uses machine learning to detect anomalies using statistical data clustering analysis to form an anomaly's score. A higher score is more significant and reflects how different one set of data is compared to previous sets of data to form a baseline.

NetBackup Flex Appliance Enhanced Security

The NetBackup Flex Appliance is designed with security at the forefront and provides a complete immutable and indelible storage solution to ensure your system and data are recoverable.

Flex Appliance Zero Trust Architecture

A 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 authorization and policy-based data protection. NetBackup Flex Appliances' Zero-Trust architecture provides a unified, multi-layered platform approach to seamlessly integrate intelligent protection, comprehensive detection, and industry-leading backup and recovery. For container-based architecture, Flex offers multi-domain isolation, network segregation, and limited-service privileges. Additionally, with WORM storage, STIG fully compliant OS hardening, FIPS 140-2 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 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)

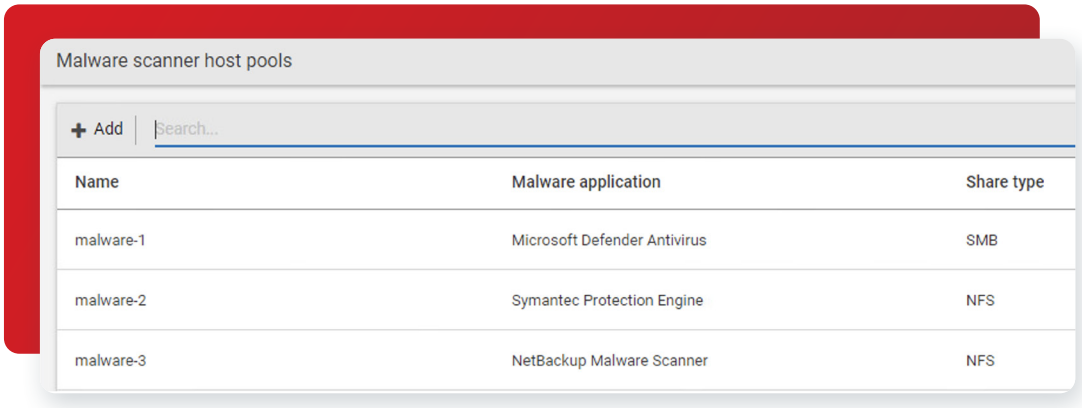
To see the full assessment, visit
https://www.veritas.com/form/whitepaper/cohasset-associates-immutability-assessment-for-netbackup.

NetBackup Malware Scanning

NetBackup Malware Detection provides greater control in the detection and recovery portions of the workflow. NetBackup offers two malware scanning methods to protect your data's integrity and the backup image: on-demand scans and scans automatically triggered by high anomaly scores.

We recommend 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 an 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.

The integrated NetBackup malware engine allows you to perform on-demand scans of backup images for latent threats. Additionally, integration with leading malware scanners such as Microsoft Defender and Symantec Protection Engine was made available in the NetBackup 10.0 release.

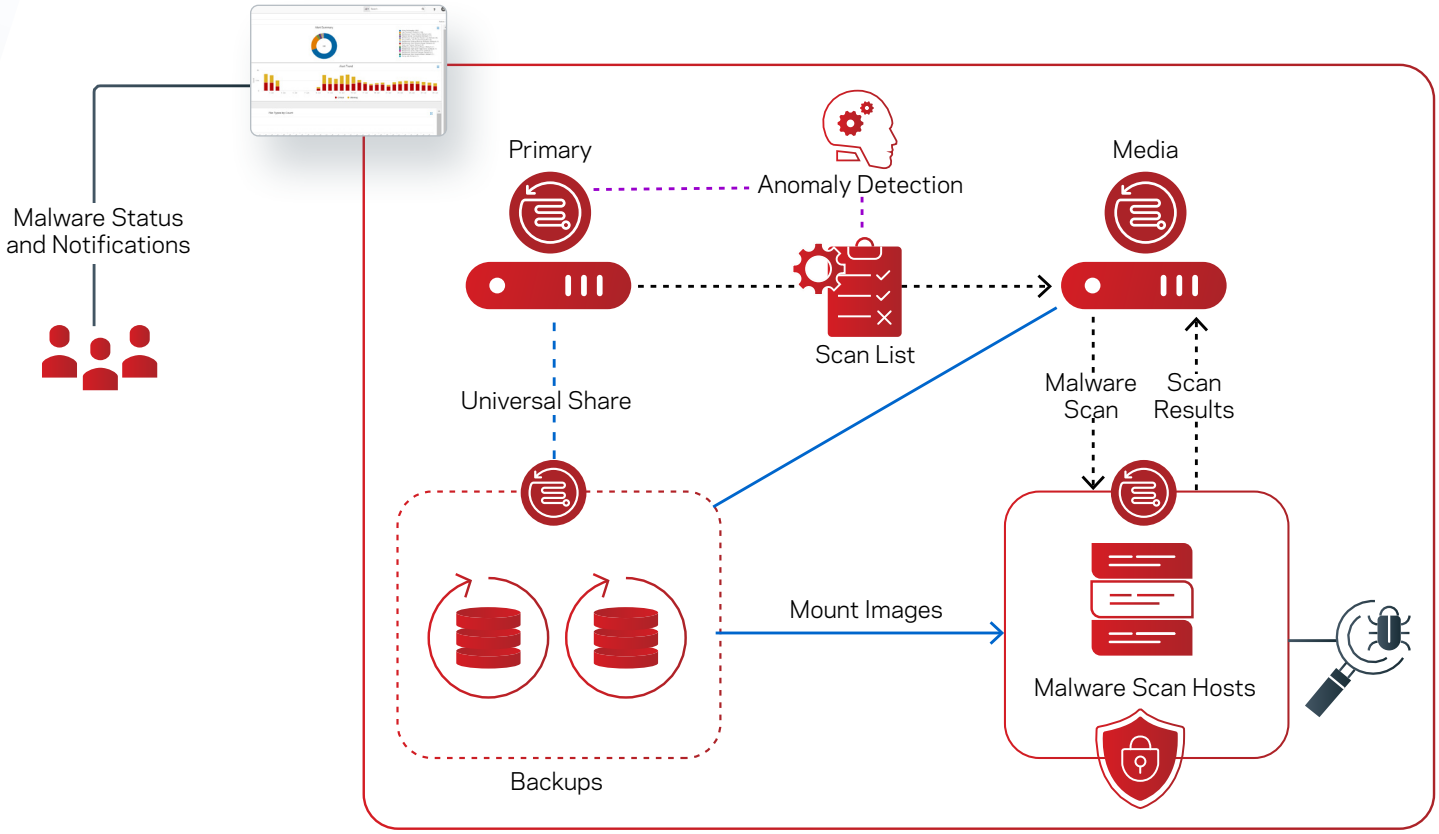


Malware scanners can be deployed on one or more hosts, depending upon concurrent scanning requirements. These scan hosts are grouped together into a scan pool that can inspect unstructured data of either MS-Windows or Standard data types.

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 prerequisites for Malware Detection and support SMB and NFS shares.

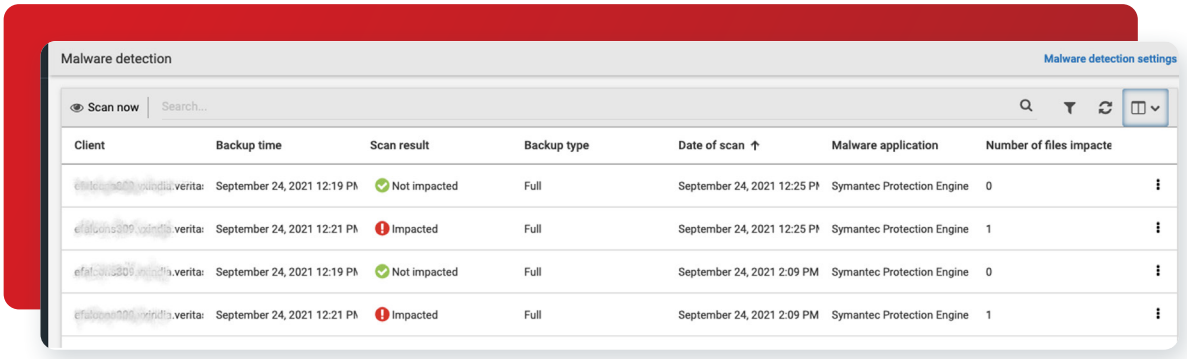
The MSDP host exposes the image to the scan host as a read-only share so there is no additional risk to read a potentially infected image. As an image passes through its Storage Lifecycle Policy (SLP), you can scan images once they reside on MSDP without interrupting the secondary SLP operations.



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, which 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.



Hybrid Cloud Resiliency with NetBackup Recovery Vault

NetBackup Recovery Vault streamlines multi-cloud storage processes – account creation, access tier definition, and protection policy selection. All resources are provisioned and managed from within NetBackup's locked-down security and role-based authentication policies, eliminating separate accounts and user interfaces across cloud providers and ensuring security and compliance policies are in check. You can run a recovery vault in the cloud while deploying an air-gapped IRE on-premises with Flex Appliances. This hybrid cloud approach provides stronger resilience and security while lowering your total cost of ownership by eliminating the unexpected data ingress and egress fees and paying for only what's used with a "pay-as-you-go" subscription service.

Flex Air Gap Deployment

You can configure an isolated recovery environment (IRE) on a Flex WORM storage server to create an air gap between your production environment and a copy of the protected data on the MSDP WORM storage server in the IRE. The air gap restricts network access to the IRE environment all the time. The production environment does not require any additional steps for this feature. All the commands below are executed on the MSDP WORM storage server shell. The following configuration was tested with:

- Flex Appliance 2.1.1
- NetBackup 10.1
- WORM storage server 17

Configuring the Air Gap

Get NBCA CA certificate and host certificate from production primary server if the environment is using NBCA, before enabling MSDP reverse connection,

```
setting certificate get-CA-certificate primary_server=<production primary server>
setting certificate get-certificate primary_server=<production primary server> token=<token>
```

1. Add the subnet of the IRE domain into network safe list to allow the IRE MSDP primary server and media servers and DNS server access the MSDP WORM storage server after the network is closed by airgap.

```
setting ire-network-control allow-subnets subnets=<subnet1>,<subnet2>,<IP address>
```

2. Before creating IRE schedule, if there are existing SLP for replicating backup images from the production domain to the WORM storage server, you may use the command below to check the SLP window related to the WORM storage server, and refer to the SLP window to create the IRE schedule.

```
setting ire-network-control show-slp-windows production_primary_server=<production primary
server name> production_primary_server_username=<production primary server username> ire_
primary_server=<target primary server name> ire_primary_server_username=<target primary server
username>
```

Configure IRE airgap schedule to open/close uni-directional network in a specific window.

```
setting ire-network-control set-schedule start_time=10:00:00 duration=4:00:00
[weekday=6]
```

The command opens network at 10AM every day for 4 hours. If weekday is specified, it only opens network for that single day. You can configure different open/close window for different weekday.

Enable MSDP Reverse connection

Once Airgap is enabled, the production MSDP servers are no longer able to access the IRE MSDP server. You need to enable MSDP reverse connection from the IRE Flex WORM storage server to the production MSDP server, so that you can replicate backup images from the production MSDP server to the IRE Flex WORM Storage server.

There's no special configuration if you are using ECA and the two domains use the same CA.

After NBCA is configured, you can enable MSDP reverse connection.

setting ire-network-control add-reverse-connection remote_addr=<source msdp server>

Sync Air Gap Schedule to SLP Window

1. Sync IRE window to production primary and provide production primary password.

```
setting ire-network-control sync-ire-window production_primary_server=<
production primary server name> production_primary_server_username=
<production primary server username> slp_window_name=<schedule name>
```

slp_window_name is an optional parameter. IRE_DEFAULT_WINDOW will be used if slp_window_name is not provided.

Note: Ensure that IRE schedule is having a gap of 24 hours between windows of two consecutive days. Otherwise, IRE schedule gets translated to multiple SLP windows on same day due to timezone difference and NBU does not support adding multiple SLP windows in a day.

2. Add replication target to production storage and replication operation to a BACKUP SLP. The import job at isolated environment will automatically start after the replication job completed.

```
setting ire-network-control add-replication-op production_primary_server=<production primary server
hostname> production_primary_server_username=<production primary server username> production_storage_
server=<production storage server> ire_primary_server_username=<ire primary server username> source_slp_
name=<source slp name>  target_import_slp_name=<target import slp name> target_storage_server=<target
storage server hostname> target_storage_server_username=<target storage server username> slp_window_
name=<slp window name> production_storage_unit=<msdp storage unit name used in source SLP>
```

add_replication_op calls add_replication_target which add replication target against given production storage server.

slp_window_name is an optional parameter. If not given, default slp window name will be IRE_DEFAULT_WINDOW which must be already created with sync_ire_window.

After providing required credentials, you can see "Operation completed successfully" message.

Summary

The combination of NetBackup's anomaly detection and malware scanning with Flex Appliances' multiple layers of security in an air-gapped configuration provides the easiest and most secure way to protect your important backup data. Recover your applications quickly with Universal Shares 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/NetBackup/10.0/Windows%20and%20UNIX/Documentation/

Versions

Flex Version	Date	Author	Key Updates
2.1	Mar 2022	Rachel Zhu	Original document
2.1.1	Aug 2022	Rachel Zhu	Added Pull method

VERITAS

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

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

V1543 08/22