Security Configuration Guide

Dell RecoverPoint for Virtual Machines 6.0.3 and later

Introduction

Rev. 01
August 2025

This document provides detailed information of the security issues in RecoverPoint for Virtual Machines6.0.3. Topics include:

DELL Technologies

Revision History

The following table shows the revision history of this document:

Table 1. Revision history

Revision	Date	Description
01	February 2025	First release of RecoverPoint for Virtual Machines version 6.0.2.

Overview

RecoverPoint for Virtual Machines provides a comprehensive data protection solution for enterprise and commercial customers, providing integrated business continuity and disaster recovery solutions to recover application data to any point in time.

This guide provides an overview of the security provisions and settings available in RecoverPoint for Virtual Machines, particularly of the operating system and the network. This document is intended primarily for company personnel responsible for system administration and network security.

Related documents

The documents listed here provide additional information about operating and configuring RecoverPoint for Virtual Machines.

RecoverPoint for Virtual Machines documentation is available at Dell Support. The following documents are especially relevant:

- *Dell RecoverPoint for Virtual Machines Release Notes*
- *Dell RecoverPoint for Virtual Machines Quick Start Installation Poster*
- *Dell RecoverPoint for Virtual Machines Installation and Deployment Guide*
- *Dell RecoverPoint for Virtual Machines Scale and Performance Guide*
- *Dell RecoverPoint for Virtual Machines Product Guide*
- *Dell RecoverPoint for Virtual Machines HTML5 Plugin Administrator's Guide*
- *Dell RecoverPoint for Virtual Machines CLI Reference Guide*
- *Dell RecoverPoint for Virtual Machines Security Configuration Guide*
- *Dell RecoverPoint for Virtual Machines RESTful API* at Explore APIs

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Copyright

Security certification

The Certification Body for the Canadian Common Criteria Evaluation and Certification Scheme (CCS) has accepted RecoverPoint v4.4 into its certification program. The evaluation file number is 383-4-351.

FIPS 140-2 compliance

The following Federal Information Processing Standard (FIPS) 140-2 validated cryptographic modules are used in RecoverPoint for Virtual Machines:

- RSA BSAFE® Crypto-C Micro Edition (FIPS certificate 2056)
- RSA BSAFE® Crypto-J, JSAFE, and JCE Software Modules (FIPS certificate 2057)
- OpenSSL® FIPS Object Module (FIPS certificate 1747)

All modules were installed according to their respective security policies.

All encrypted network connections to and from RecoverPoint for VMs appliances use only the above FIPS 140-2 validated cryptographic modules. On new installations, the vRPA communication security level is set to *Authenticated and Encrypted* by default. To make the RecoverPoint for VMs system FIPS-140-2 compliant, verify that the vRPA communication security level is set to *Authenticated and Encrypted* on all vRPAs.

Operating system and networking

The following section broadly describes the RecoverPoint for Virtual Machines operating system and networking aspects that relate to security.

RecoverPoint for Virtual Machines operating system

The RecoverPoint for VMs operating system is based on a standard Debian GNU/Linux 10 distribution that has been modified according to RecoverPoint for VMs functional and security requirements. Unessential Debian packages were removed (for operating system hardening), required packages were added, and the latest security updates from Debian were applied.

RecoverPoint for VMs operates the Linux at runlevel 2, full multi-user mode.

All extraneous default Linux daemons were disabled to decrease the attack surface. The following daemons are running:

- connectemc
- cron
- dbus-daemon
- getty
- init
- iscsid
- ipmievd
- ntpd
- snmpd (only when the snmp agent is enabled; disabled by default)
- startpar
- sshd
- rsyslogd
- tomcat
- udev

All RecoverPoint for VMs user space applications are started automatically when the vRPA starts up.

Additional services may run to support hardware monitoring on some platforms (for example, Dell).

Security hardening of third-party components

Third-party components that are deployed as part of the RecoverPoint for Virtual Machines operating system were hardened.

Networking

Learn about differentRecoverPoint for Virtual Machines networking components and their roles in RecoverPoint for VMs environment.

Each vRPA has these virtual network interfaces:

- local area network (LAN)
- wide area network (WAN)
- 2 data network adapters (vNICs)

Each ESXi server has the following interfaces for connectivity between the splitter and the vRPAs:

- 1 or 2 VMkernel ports

For security information related to ESXi servers, refer to vSphere Security and the vSphere Security Hardening Guide for your version of vCenter and vSphere.

Logs

Events

RecoverPoint for Virtual Machines generates a log in response to events in the RecoverPoint for VMs system.

The events in the log may be viewed in the Management Application UI or in the CLI.

To access the events using the CLI, create an SSH session to the vRPA management IP address, and enter your RecoverPoint for VMs username and password to log in to the CLI. Run the `get_events_log` command.

Event notification

RecoverPoint for Virtual Machines offers the following options for external notification of events:

Email notification	The email notification (alert) mechanism sends specified event alerts to addresses when the SMTP (email) settings are enabled.
SNMP notification	Users can configure RecoverPoint for VMs to generate SNMP traps (notifications) of system events. The RecoverPoint for VMs MIB can be downloaded from the following location: Dell Support
Syslog notification	RecoverPoint for VMs uses syslog to support event notification to a remote management application.

Consider the appropriate network settings for each event notification method that you want to configure.

System internal logs

In addition to event logs, the RecoverPoint for Virtual Machines system maintains log files for internal use by Customer Support and technical services personnel. The Installation Manager menu option **Collect system info** is provided to allow automatic collection and retrieval of all logs from the various appliances and attached splitters into one archive. The collected logs are retrievable over FTP, or FTPS or as a web download.

Splitter logs

Learn about splitter logs with the VMware® vSphere Web Client.

RecoverPoint for Virtual Machines splitter logs are part of the ESXi logs. Instructions for retrieving ESXi logs using the vSphere Web Client are provided in the “Troubleshooting” section of the *RecoverPoint for VMs HTML5 Plugin Administrator’s Guide*.

Audit logs

The log auditing facility captures all user actions in all user interfaces and logs the user actions that can be collected using log collection.

The Sysmgmt CLI can be used to collect the audit logs.

The audit logs are collected as part of a full collection of vRPA logs, or can be specified for collection in a partial collection.

The following parameters are collected for each user action:

- Timestamp

- Username
- Origin IP
- Endpoint
  - CLI
  - SSH
  - FAPI
  - DAPI
  - Flex plug-in
  - HTML plug-in
  - New RESTful API
  - Installation Server

The collected audit logs can be found under `home/kos/auditlog` in the log collection archive.

User access control

Learn about different user interfaces and secured authentication guidelines for using RecoverPoint for Virtual Machines.

RecoverPoint for Virtual Machines is designed to be accessed via the vSphere Web Client. When a user is authenticated with vCenter Single Sign-On, that user can access all installed vCenter services to which the user has been granted access. In addition, through the RecoverPoint for VMs vSphere Web Client plug-in, the user will have admin access to manage RecoverPoint for VMs.

Access to vSphere plugin

The vCenter administrator controls whether a vCenter user shall be able to use the RecoverPoint for VMs vSphere HTML5 plugin.

To use the plugin, you must have the Manage custom attributes privilege (Global.Manage custom attributes) on the vCenter. The vCenter administrator can disable use of the plugin for any user by removing this privilege for that user. In that case, the system prevents you from doing anything through the plugin (and new RESTful API).

User access methods

This section describes the RecoverPoint for Virtual Machines user interfaces using command-lines.

RecoverPoint for VMs is designed to be accessed using the RecoverPoint for VMs vSphere plug-in. Direct access to RecoverPoint for VMs has not, however, been disabled in this version. The security aspects of the following direct-access methods are discussed below.

Admin CLI	The RecoverPoint for VMs Sysmgmt CLI is a keyboard-interactive tool that allows you to modify and manage existing vRPA configurations, and test and diagnose the settings and connectivity of those configurations before and after they are attached to RPA clusters. Use SSH, with admin user and password, to access the RecoverPoint for VMs Admin CLI.
Sysmgmt CLI	The RecoverPoint for VMs Sysmgmt CLI provides a command-line interface for nearly all the functions that are needed to manage the RecoverPoint for VMs system. It is useful for creating and running automated scripts. Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI.
REST API	The RecoverPoint for VMs REST API exposes a simple application programming interface that allows developers to integrate RecoverPoint for VMs with their own applications and to write scripts that automate RecoverPoint for VMs operations.

User authentication

Each RecoverPoint for Virtual Machines user is defined by a username, a password, and a single role. A role is a named set of access permissions. By assigning a role to users, the users receive all the access permissions that are defined by the role.

RecoverPoint for VMs provides two independent mechanisms for authenticating direct access of users: vRPA-based authentication and authentication via the organization's LDAP (Lightweight Directory Access Protocol) server. The two authentication mechanisms can be used simultaneously or vRPA-based authentication can be used exclusively.

Predefined users

The vRPA is shipped with the admin user already defined:

Table 2. Predefined users for new installs

User	Role	Initial Password	Permissions
admin	administrator[a]	admin [b]	Array Configuration; Boxmgmt; Data Transfer; Failover; Group Clear Settings; Group Configuration; Splitter Configuration; System Configuration; Target Image; SE; Security; Upgrade; View; Web Download

a. The administrator role has all access permissions.
b. The admin user password serves as password also for the root user.

NOTE: The following predefined users are removed when upgrading to RecoverPoint for Virtual Machines 6.0.3:

- security-admin
- boxmgmt
- SE

For new installs, the admin user cannot be removed.

It is always recommended that you change initial default passwords, whether your system is a new install or an upgrade from a RecoverPoint for VMs version earlier than 5.2.

You must set the admin password (which is also the root password) during installation.

If, for any reason, you need to change a password, follow this procedure:

1. Create an SSH connection to the vRPA management IP address, using your RecoverPoint for VMs admin username and password to log into the Boxmgmt CLI. Then select **System management CLI** to open the Sysmgmt CLI.

   Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI.

2. In the Sysmgmt CLI, run the `set_password` command to change the password for the current user, or run the `set_user` command to change the password of another user, if your user role includes the security permission.

Only users with security permission can add users, and can remove and edit permissions for users that have previously been added.

Changing the root password

For best system security, you must replace the default password for the root user with a strong password that is unique to your system.

Steps

- Beginning with RecoverPoint 5.1.2, your admin user password serves also as the root password, Follow the password policy of your organization to set a strong password for these users.
- For earlier versions of RecoverPoint, contact Customer Support for assistance with changing the default root password. See Dell EMC Knowledge Base Article 520937 for details.

Security permission

Making changes to users, roles, security levels or configuring LDAP requires the security permission. For a new install of RecoverPoint for Virtual Machines, the predefined admin user has security permission.

You cannot edit roles or permissions for the predefined admin user, or for the user you are currently logged in as. You cannot delete a role that is currently assigned to a user.

Configuring local users

Use CLI commands to configure local users. You must be logged into the Sysmgmt CLI to use the CLI commands.

Perform the following steps to access Sysmgmt CLI to run the CLI commands:

1. Create an SSH connection to the vRPA management IP address.
2. Enter your RecoverPoint for Virtual Machines admin username and password to log in to the Sysmgmt CLI.
3. Select **System management CLI** to open the Sysmgmt CLI.

Alternatively, if you have created a user with the sysmgmt role, log in directly to the Sysmgmt CLI.

The following CLI commands can be used to add, delete, modify, or view users and passwords:

Table 3. Permissions for CLI commands used for configuring local users

CLI command	Permissions required
`add_user`	Security
`get_users`	View
`remove_user`	Security
`set_password`	Users can set only their own password.
`set_user`	Security

Configuring LDAP-based authentication

Configure the LDAP-based authentication for RecoverPoint for Virtual Machines using CLI commands.

Prerequisites

For RecoverPoint for VMs to be able to work with an LDAP server, RecoverPoint for VMs vRPAs must have access to either the LDAP port (by default, TCP port 389) or the LDAPS port (by default, TCP port 636) on the LDAP server.

The following best practices are highly recommended when using LDAP authentication:

- Assign the least possible permissions to the Bind Distinguished Name; namely, Read All Properties and List Content permissions for Search Base and its child objects only.
- Use LDAP over SSL (LDAPS). The LDAP protocol sends passwords over the network in plaintext. Using SSL avoids this issue.
- Avoid using the term "admin" in the username (for example, "myname.admin").

About this task

For detailed instructions on configuring RecoverPoint for VMs to work with LDAP authentication, see Manage User Authentication section in the *RecoverPoint for VMs Administrator's Guide*.

NOTE: RecoverPoint for VMs implementation of LDAP does not support Kerberos authentication.

For detailed instructions on the use of each of the CLI commands, see the User Commands chapter of the *RecoverPoint for VMs CLI Reference Guide*.

Steps

1. Create an SSH connection to the vRPA management IP address.
2. Enter your RecoverPoint for VMs admin username and password to log in to the Sysmgmt CLI.

3. Select **System management CLI** to open the Sysmgmt CLI.

   NOTE: If the user is configured with the sysmgmt role, log in to Sysmgmt CLI directly.

4. Run the following commands to configure LDAP authentication:

Table 4. Permissions for CLI commands used for LDAP authentication

CLI command	Permission required
`clear_ldap_configuration`	Security
`config_ldap`	Security
`get_ldap_configuration`	View
`test_ldap_connection`	Security

Local users' security level

When installing RecoverPoint for Virtual Machines, you are prompted to set the **Local users' security level** to either **`Basic`** or **`High`**. It is recommended to set the **Local users' security level** to **`High`** to meet relevant security standards, such as those of the US Department of Defense Security Technical Implementation Guides (DoD STIG).

High	User passwords to access the vRPA must have eight characters, they can only be reset once in 24 hours. At least two characters must be lower case, at least two must be upper case, and at least two must be non-alphabetical (either digits or special characters). All user passwords expire in 90 days; the same password cannot be reused until at least ten other passwords have been used. After changing the **Local users' security level** to **`High`**, all users must change their password the next time they log in to the system.
Basic	User passwords to access the vRPA must have a minimum of five characters.

NOTE: Keep passwords in a place where they are secure and available to you.

The command-line interface (CLI) command `set_security_level` can be used to change the **Local users's security level**.

Regardless of the security level, any user who tries unsuccessfully three times to log on will be locked out. To unlock the user, use the CLI command `unlock_user`. Only users with security permission can unlock a user.

When adding a cluster or vRPA to an existing cluster, the added cluster or vRPA receives the security settings (**Local users' security setting** = **`[ Basic | High ]`** of the existing cluster.

Password restrictions are implemented at the application level, not at the operating system level.

For instructions on configuring user authentication, refer to “Manage Roles” in the *RecoverPoint for VMs Administrator's Guide*.

Recovering forgotten passwords

Steps

- If users forget their passwords, a user with security privilege can reset the password.
- If all users with security role privilege have forgotten their passwords, contact Customer Support.

  Local access may be required.

  NOTE: Keep passwords in a place where they are secure and available to you.

User authorization

User authorization grants or denies users access to resources managed by RecoverPoint for Virtual Machines. User authorization is identical irrespective of the user authentication by RecoverPoint for VMs or the LDAP server. User authorization can be limited to specific consistency groups.

A username, a password, and a role are defined for each user. A role is a named set of access permissions. Assign a role to the users to ensure that the users receive all the access permissions that are linked to that role. The predefined administrator role has all the access permission. Also the predefined sysmgmt role has all the permissions, except for Web Download and SE.

To define roles and permissions, see "Configuring Authorization" and "User Authorization" sections in *RecoverPoint for VMs Administrator's Guide*.

Access permissions lists the permissions that may be assigned to a role, and the permissions that are granted or denied to a user.

Table 5. Access permissions

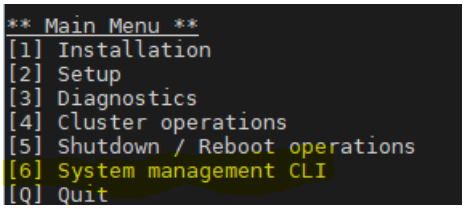
Permission	Description
Array Configuration Storage Management	Manage storage arrays including automatic journal creation, remote volume autoprovisioning, and snapshot integration.
Admin	Access to Sysmgmt CLI.
Data Transfer	Enable and disable access to image, and undo writes to the image access log.
Failover	Modify replication direction (use temporary and permanent failover), initiate failover, verify failover.
Group Clear Settings	To reset the system settings.
Group Configuration	Create and remove consistency groups, and modify all group settings except the groups that are in the Data Transfer, Target Image, and Failover permissions. A user with this permission may bookmark images and resolve settings conflict.
SE	Permission for use of full set of RecoverPoint for VMs support commands, which are displayed with `enable_advanced_support_commands` Sysmgmt CLI command.
Security	All UI actions and commands dealing with roles, users, LDAP configuration, and security level.
Splitter Configuration	Add or remove splitters, and attach or detach splitters to volumes.
System Configuration	Configure and manage email alerts, SNMP, System Reports, rules, licenses, serial number, account ID, syslog, and other system configuration parameters.
Target Image	Enable and disable access to an image, resume distribution, and undo writes to the image access log.
Upgrade	Install vRPA software, vRPA maintenance, including upgrading to a minor RecoverPoint for VMs release, upgrading to a major RecoverPoint for VMs release, replacing an vRPA, and adding new vRPAs.
View	View system information.
Web Download	Download logs from the vRPA.

Access permissions *Admin* and *Web Download* cannot be assigned to new roles. Every role includes the `View` permission by default.

Roles and launching CLIs

The role assigned to a user determines whether the Sysmgmt CLI is launched when you use that user to create an SSH connection to the vRPA.

When you use the predefined admin user, or any user with the administrator role, the Sysmgmt CLI opens, and its main menu includes the **System management CLI** option. Use that option if you want to access the Sysmgmt CLI later.



The Sysmgmt CLI is launched also when using any user with the admin role. In this case, the main menu does not include the **System management CLI** option.

Using a user with any other role launches the Sysmgmt CLI directly. The permissions that belong to that role determine which Sysmgmt CLI commands the user can run. The predefined sysmgmt role has the same permissions as the administrator role, except for Web Download and SE. Hence, if you create a local user with the sysmgmt role, you can use it to launch directly to the Sysmgmt CLI, and run almost all the Sysmgmt CLI commands.

Authorization using command-line interface

Use Sysmgmt CLI commands to modify user permissions, and define roles.

Create an SSH connection to the management IP address, and enter your RecoverPoint for Virtual Machines admin username and password to log in to the Sysmgmt CLI to use Sysmgmt CLI commands. Then, select **System management CLI** to open the Sysmgmt CLI.

Alternatively, if you have created a user with the sysmgmt role, use that user to log in directly to the Sysmgmt CLI.

The following Sysmgmt CLI commands can be used to modify user permissions and define roles:

Table 6. Sysmgmt CLI commands

CLI command	Permission required
`add_role`	Security
`get_roles`	View
`modify_role`	Security
`remove_role`	Security

Automatic logout from command-line interface

RecoverPoint for VMs users are automatically logged out of the CLI after 30 minutes.

Component access control

Software components on RecoverPoint for Virtual Machines vRPA communicate with each other using a proprietary communication protocol superimposed over the network layer, allowing access only to components that adhere to the same protocol. The RecoverPoint for VMs splitter (on each ESXi server) communicates with vRPA over TCP/IP.

You may choose to encrypt all communications between vRPAs and to require full authentication. This is recommended. For details, refer to About vRPA communication security level and Changing the RPA communication security level.

During deployment, RecoverPoint for VMs requires vCenter administrator credentials. These credentials are encrypted and persist in the RecoverPoint for VMs repository.

About vRPA communication security level

RecoverPoint for VMs supports Message Passing Interface (MPI) security for communication between vRPAs, between vRPA clusters, with storage, and with vCenters. This feature applies to vRPA communications within the cluster and communications between clusters over WAN (IP), but not to cluster communications over Fibre Channel. MPI security offers the following vRPA communication security levels. To view the vRPA communication security level of each cluster in the system, log in to the CLI as **user** = **admin** (or another user with security permission), and use the CLI command `get_security_settings`.

Table 7. vRPA communication security levels

vRPA communication security level	Description
Not authenticated, not encrypted	Communication between vRPA clusters is not authenticated or encrypted. However, vRPA clusters can communicate with each other only by adhering to the proprietary protocol.
Authenticated and encrypted (default)	vRPA clusters use certificates to authenticate each other before communicating. All communication between vRPA clusters is also encrypted using Advanced Encryption Standard (Rijndael) with 256-bit keys.

Changing the RPA communication security level

Procedure for changing the RPA communication (authentication and encryption) security level

Steps

1. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Change appliance communication security level**.
2. For best security (recommended), select **Authenticated and encrypted**. This level is the default.

   If improved performance is critical, select **Not authenticated nor encrypted**.

   When the vRPA is attached to a cluster, the security level of all vRPA clusters in the system are changed.

vCenter Server credentials

This section describes the importance of vCenter server credentials

The user enters VMware vCenter Servers credentials as part of RecoverPoint for Virtual Machines deployment. The credentials allow RecoverPoint for VMs to manage replication, to orchestrate operations, and to display VMware vCenter Server data in a RecoverPoint for VMs context.

To add additional vCenter Servers to a RecoverPoint for VMs cluster, refer to “Adding a vCenter” in the *RecoverPoint for Virtual Machines Installation and Deployment Guide*.

Accessing the plugin server

Use this procedure to enable SSH access to the plugin server.

Prerequisites

- Ensure that port 443 is open for communication with the plugin server VM and vCenter.
- Ensure that port 9443 is open for plugin server communication with the vRPAs.
- Port 22 is blocked by default. It can be opened and closed on demand.

NOTE: The plugin server does not have its own role-based access control (RBAC). Rather, use the username that you used to register the vCenter to the plugin server to perform all the needed operations on the HTML5 plugin and the new RESTful API.

Steps

1. Using VM console, log in to the plugin server as user **root**.

The default password for the **root** user is **admin**. Upon first login to the plugin server with VM console, replace this default password with a strong unique password.

2. Stop and disable the firewall. Run:
   a. `systemctl stop SuSEfirewall2`
   b. `systemctl disable SuSEfirewall2`
3. Connect to the plugin server using SSH.
4. When done, re-enable and restart the firewall. Run:
   a. `systemctl start SuSEfirewall2`
   b. `systemctl enable SuSEfirewall2`

Regenerating encryption keys

The `regenerate_encryption_keys` CLI command allows a user with security permission to regenerate the system encryption keys at any time. Perform the following steps to generate new encryption keys as required.

About this task

Regenerate encryption keys during the following scenarios:

- When there is a suspected security breach.
- When there is a communication problem such as when the WAN is down, the certificates are reset manually in each cluster.
- During a new installation, including vRPA addition or replacement, RecoverPoint for VMs automatically generates random SSH host keys. However, if any version of RecoverPoint for VMs was previously installed on the vRPA, the SSH keys are not regenerated.

Steps

1. Enable cluster isolation mode. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Enable/disable cluster isolation**.
2. Select **System management CLI** to open the Sysmgmt CLI of the vRPA and run `regenerate_encryption_keys`.
3. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **View cluster's certificate**. Copy the displayed certificate.
4. Log in to another vRPA cluster in the system: Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Change cluster certificate**. Paste the certificate copied from 3.
5. Repeat this process for every vRPA cluster in the system that is not communicating with a cluster that has already been updated.
6. Disable cluster isolation mode. In the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Enable/disable cluster isolation**.

Communication security

Communication security settings enable the establishment of secure communication channels between product components, as well as between product components and external systems or components.

Supported services

The vRPA supports the following services:

Firewall	The RecoverPoint for Virtual Machines OS runs an iptables firewall that blocks all unused ports on the machine.
SSH	Customers are encouraged to use a secure shell (SSH) when connecting to a vRPA. RecoverPoint for VMs runs OpenSSH.
Web server	• RecoverPoint for VMs uses Apache Tomcat for HTTPS.

- RecoverPoint for VMs uses HTTPS for communication between the RecoverPoint for VMs Management Application and the RecoverPoint for VMs vRPAs. This communication requires authentication. All UI traffic is fully encrypted using HTTPS. It is recommended that customers provide their own security certificate.

SNMP

- The vRPA is SNMP-capable; that is, the RecoverPoint for VMs system supports monitoring and problem notification using the standard Simple Network Management Protocol (SNMP).
- This includes support for SNMPv3, which adds security and remote configuration capabilities to the previous versions. The SNMPv3 architecture introduces the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. The architecture supports the concurrent use of different security, access control, and message processing models. The system supports various SNMP queries to the agent on RecoverPoint for VMs. In addition, the system can be configured so that RecoverPoint for VMs events generate SNMP traps which are sent to designated hosts (that is, NMS servers). For more information about RecoverPoint for VMs support for SNMP, see SNMP security.
- RecoverPoint for VMs supports the default MIB-II and, on selected platforms, hardware monitoring of the RecoverPoint for VMs platform. The RecoverPoint for VMs MIB can be downloaded from Dell Support.

Transport layer security

The Secure Socket Layer (SSL) interfaces of the RPA support Transport Layer Security (TLS) protocol versions 1.1 and 1.2 (recommended). For backward compatibility, they can support TLS 1.0.

About this task

If all other products in the system with which the RPAs communicate support TLS 1.1 or higher, it is recommended that users disable TLS 1.0 support. For details, see Knowledge Base Article 489544. Ensure that KVSS supports TLS 1.1 and 1.2 by upgrading KVSS to the KVSS version provided with your version of RecoverPoint for VMs.

Perform the following steps to reset the minimum TLS protocol version.

Steps

1. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **`admin`**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Set minimum Transport Layer Security protocol version**.
2. Set minimum TLS version.
3. Reboot RPA.
4. Repeat this change on every RPA at every cluster in the system.

Data network considerations

Communication between the splitter on the ESXi host and the vRPAs must be configured to be over TCP/IP.

To allow the ESXi host to communicate with the vRPA Data vNICs, create one or two VMkernel ports on each ESXi node in an ESXi cluster that has vRPAs, protected VMs, or copy VMs. For instructions, see the *RecoverPoint for Virtual Machines Installation and Deployment Guide*.

To ensure connectivity between splitters and vRPAs, open firewall ports for inbound and outbound TCP communication for each vRPA: 5020, 5040, 5042, 5044, and 5050. These ports are opened automatically in the ESXi firewall when you register an ESXi cluster in RecoverPoint for VMs.

Table 8. Data ports

Port	Source -> Destination	Protocol and description	Effect if closed
5020	splitter (on ESXi) -> vRPA Data vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between a splitter and a vRPA: • No replication. • No test or failover on replica side.

Table 8. Data ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
5040	splitter (on ESXi) -> vRPA Data vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between a splitter and a vRPA: • No replication. • No test or failover on replica side.
5042	splitter (on ESXi) -> vRPA Data vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between a splitter and a vRPA: • No replication. • No test or failover on replica side.
5044	splitter (on ESXi) -> vRPA Data vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between a splitter and a vRPA: • No replication. • No test or failover on replica side.
5050	splitter (on ESXi) -> vRPA Data vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between a splitter and a vRPA: • No replication. • No test or failover on replica side.

External ports

The external ports must be accessible to allow the cluster to communicate with servers outside the RecoverPoint for Virtual Machines system.

Table 9. External ports

Port	Source -> Destination	Protocol and description	Effect if closed
20	vRPA LAN vNIC -> FTP server	• Outgoing FTP communications (TCP) (output only). • Used during installation and upgrades to download ISO image, if FTP is specified as the source; not required if the Deployment Manager server is used as the ISO source (then HTTPs can be used). • Can be used to upload support logs to the	• Not possible to download ISO image or to upload logs using FTP. • Replication not affected.

Table 9. External ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
		specified FTP server; not required if the support logs are manually downloaded using HTTPS.	
25	vRPA LAN vNIC -> ESRS	• Used to register on the ESRS server.	• Not possible to register on the ESRS server. • Replication not affected.
21	vRPA LAN vNIC -> FTP server	• Outgoing FTP communications; for system info collection only (TCP) (output only). • Used during installation and upgrades to download ISO image, if FTP is specified as the source; not required if the Deployment Manager server is used as the ISO source (then HTTPs can be used). • Can be used to upload support logs to the specified FTP server.	• Not possible to download ISO image or to upload logs using FTP. • Replication not affected.
22	SSH client -> vRPA LAN vNIC	• SSH and communications between vRPAs (TCP). • Required for CLI access to vRPAs. The source is the Management Server, the destination is the vRPA.	• No remote connection to CLI. • Replication not affected.
25	vRPA LAN vNIC -> SMTP server	• Used for sending system mail (SMTP) email alerts from vRPA, if configured	• No email alerts sent. • No system reports sent. • Replication not affected.

Table 9. External ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
		(TCP) (output only); • Used for Call Home events, if configured.	
53	vRPA LAN vNIC -> DNS server	• DNS (TCP, UDP). • Used for name resolution. Only required if in the RecoverPoint for VMs configuration, domain names are used for external servers instead of IP addresses.	• No name resolution of remote servers, e-mail alerts, system reports.
68	DHCP server -> vRPA LAN vNIC	• Used to dynamically provide IP addresses to vRPAs connecting to the network (UDP).	• vRPA will not be assigned an IP if DHCP is used.
123	vRPA LAN vNIC ->NTP server or another vRPA	• NTP (UDP). • RecoverPoint for VMs: TCP is no longer used on this port and may be closed. • Used for synchronizing with Network Time Protocol server. • Used between vRPAs in a cluster for time synchronizatio n.	• No synchronization with time server. vRPAs may show incorrect time. Event time stamps may be incorrect. • Replication not affected, but snapshots may show incorrect times. Write-order of snapshots not affected.
161	MIB Browser -> vRPA LAN vNIC	• SNMP (TCP, UDP). • Used for SNMP notifications. Also see port 10161.	• There will be SNMP notification, but you will not be able to view or edit SNMP values. • Replication not affected.
389	vRPA LAN vNIC -> LDAP server	• LDAP (TCP) (output only). • Used for LDAP user	• No LDAP authentication (unless using SSL).

Table 9. External ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
		authentication and authorization. Only required if LDAP is configured. Also see port 636.	
443	Browser -> vRPA LAN vNIC vRPA LAN vNIC -> vCenter	• HTTPS for management (TCP). • Used to download vRPA logs, System Report alerts, EMC Secure Remote Services (ESRS), and communication with third-party hardware (such as ESXs and VMs).	No RecoverPoint GUI (unless port 80 using HTTP is available). • No vCenter Server information (ESXs and VMs) displayed in RecoverPoint
514	vRPA LAN vNIC -> Syslog server	• Syslog (TCP, UDP) (output only). • Used to send Syslog information to an external server. Only required if Syslog is enabled and an external server is specified.	• System logs not available. • Replication not affected.
623	Management client -> vRPA LAN vNIC	IPMI over WAN (UDP). Used by iDRAC/BMC for monitoring and managing remote vRPA operation.	No remote hardware management.
636	vRPA LAN vNIC -> LDAP server	• LDAP over SSL (TCP) (output only). • Used for LDAP over SSL user authentication and authorization. Required only if LDAP using SSL is configured.	• No LDAP over SSL authentication.

Table 9. External ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
989	vRPA LAN vNIC -> FTPS server	• FTPS (output only). • Used for System Reports alerts and reporting via FTPS. Only required if FTPS alerts or reports are configured.	• No FTPS transfers. • If system reports (SyR) is configured to transfer by FTPS, reports will not be transferred to System Reports database.
990	vRPA LAN vNIC -> FTPS server	• FTPS (output only). • Used for System Reports alerts and reporting via FTPS. Only required if FTPS alerts or reports are configured.	• No FTPS transfers. • If system reports (SyR) is configured to transfer by FTPS, reports will not be transferred to System Reports database.
3260	ESXi <--> vRPA LAN vNIC	• iSCSI (TCP)	• RecoverPoint: No iSCSI support. • RecoverPoint for VMs: No replication.
7115	SRM server -> RPA LAN vNIC	• RecoverPoint: For VMware Site Recovery Manager communication (TCP). • RecoverPoint: Used by the RecoverPoint Storage Replication Adapter to query and manage the RPA. Only required if Storage Replication Adapter up to version 2.2.0.0 is used.	• No vCenter Server information or commands available. • Replication not affected.
7225	Replication Manager -> RPA LAN vNIC KVSS -> RPA LAN vNIC Replication Enabler for Exchange -> RPA LAN vNIC	• HTTPS protocol for communicating with the functional API (TCP, UDP). • Used by third-party devices and services to	• No functional API.

Table 9. External ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
		communicate with the RPA.	
8082	Deployment Manager -> vRPA LAN vNIC	• HTTPS protocol for communication with the RecoverPoint for VMs Installation Server (TCP). • Used by the Deployment Manager during installation and upgrades. Deployment Manager needs to communicate with all RPAs in all clusters. Management ports preferred, WAN ports are used as fallback. • Used for log collection.	• No deployment tools. • No installations or upgrades. • Replication not affected. • No log collection.
9443	Plugin Server -> vRPA LAN vNIC	Required for plugin server communication with vRPAs (HTTPS).	RecoverPoint Plugin fails.
10161	MIB Browser ->vRPA LAN vNIC	• SNMP over TLS (TCP); SNMP over DTLS (UDP). • Used for SNMP reporting. Only required if SNMP is configured.	• No encrypted SNMP.

Inter-cluster ports

The following ports must be accessible to clusters in this RecoverPoint for Virtual Machines system, to allow inter-cluster communication. These ports need not be accessible to any server outside the RecoverPoint for VMs system.

Table 10. Inter-cluster ports

Port	Source -> Destination	Protocol and description	Effect if closed
ICMP echo requests	vRPA WAN vNIC -> vRPA WAN vNIC	• ICMP is required between vRPAs when installing vRPA clusters or adding vRPAs to existing clusters.	• Installation fails.

Table 10. Inter-cluster ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
			• Cluster management operations fail.
22	SSH client -> vRPA WAN vNIC	• Inbound SSH and communications between vRPAs (TCP). • WAN ports preferred, Management ports as fallback.	• Diagnostic tools fail. • Replication is not affected.
5001	vRPA WAN vNIC -> vRPAWAN vNIC	• `iperf`; performance measuring between vRPAs (inbound/outbound TCP). • Used for collecting diagnostic and performance information between clusters. Best practice is to make this port available, but it is not required.	• No performance measurement. • Replication is not affected.
5010	vRPA WAN vNIC -> vRPA WAN vNIC	• RecoverPoint for VMs (inbound/outbound TCP, UDP). • Required between vRPAs in different clusters for replication.	• No RecoverPoint for VMs system. • No replication.
5020	vRPA WAN vNIC -> vRPA WAN vNIC	• RecoverPoint for VMs (inbound/outbound TCP, UDP). • Required between vRPAs in different clusters for replication.	• No RecoverPoint for VMs. • No replication.
5040	vRPA -> WAN vNIC vRPA WAN vNIC	• RecoverPoint for VMs (inbound/outbound TCP, UDP). • Required between vRPAs in different clusters for replication.	• No RecoverPoint for VMs system. • No replication.
5060	vRPA -> WAN vNIC vRPA WAN vNIC	• `mpi_perf` (inbound/outbound TCP, UDP). • Used for collecting diagnostic and performance information between clusters. Best practice is to make this port available, but it is not required.	• No performance measurement. • Replication is not affected.
5080	vRPA WAN vNIC -> vRPA WAN vNIC	• Connectivity diagnostics tool (inbound/outbound TCP, UDP). • Used for collecting diagnostic and performance information between clusters. Best practice is to make this port available, but it is not required.	• No connectivity diagnostics. • No performance measurement. • Replication is not affected.
5081	vRPA WAN vNIC -> vRPA WAN vNIC	• Connectivity diagnostics tool (inbound/outbound UDP). • Used for collecting diagnostic and performance information between clusters. Best practice is to make this port available, but it is not required.	• No connectivity diagnostics. • No performance measurement. • Replication is not affected.
5100	vRPA WAN vNIC -> vRPA WAN vNIC	• Cluster connector (inbound/outbound TCP, UDP), for connecting additional clusters.	• Cannot add an additional cluster to the RecoverPoint for VMs system.
8082	vRPA WAN vNIC -> vRPA WAN vNIC	• Supports log collection (inbound/outbound TCP): connecting new vRPAs to cluster.	• Diagnostic tools fail • Replication is not affected. • Diagnostic tools fail • Replication is not affected. • Cannot collect support logs from multiple vRPAs.
8084	vRPA WAN vNIC -> vRPA WAN vNIC	• Used to communicate with configuration database on each vRPA (inbound/outbound TCP)	• No communication with configuration database

Table 10. Inter-cluster ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
9999	vRPA WAN vNIC -> vRPA WAN vNIC	• `udponger`; connectivity diagnostics tool (inbound/outbound UDP). • Used for diagnosing UDP connectivity between clusters. Best practice is to make this port available, but it is not required.	• No connectivity diagnostics. If tool is run, returns error. • Replication is not affected.

Intra-cluster ports

The following ports must be accessible to all RPAs in the same cluster, to allow intra-cluster communication. These ports need not be accessible to any server outside the cluster. Note that ICMP is required between vRPAs when installing vRPA clusters or adding vRPAs to existing clusters.

Table 11. Intra-cluster ports

Port	Source -> Destination	Protocol and description	Effect if closed
123	vRPA -> LAN vNIC vRPA LAN vNIC	• inbound/outbound TCP, UDP, used between vRPAs in a cluster for time synchronization.	• vRPAs may show incorrect time. Event time stamps may be incorrect. • Replication not affected, but snapshots may show incorrect times. Write-order of snapshots not affected.
5020	vRPA LAN vNIC -> vRPA LAN vNIC	• RecoverPoint for VMs (inbound/outbound TCP, UDP). • Required between vRPAs within the same cluster for cluster management.	• No RecoverPoint for VMs. • No replication.
5021	vRPA -> LAN vNIC vRPA LAN vNIC	• Used for storage process (TCP, UDP).	• Replication not affected.
5042	splitter -> vRPA LAN vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between splitter and vRPA: • No replication. • No test or failover on replica side.
5044	splitter -> vRPA LAN vNIC	Inbound and outbound TCP communication for each vRPA.	Without communication between splitter and vRPA: • No replication. • No test or failover on replica side.
5045	RPA LAN vNIC -> RPA LAN vNIC	• RecoverPoint (TCP, UDP). • Used between RPAs in the cluster for Symmetrix splitter functionality.	• RPA failure will cause a full sweep of volumes attached to the Symmetrix splitter in some disaster scenarios. The splitter itself will continue to function.
5050	RPA LAN vNIC -> RPA LAN vNIC	• RecoverPoint (TCP, UDP).	• No Symmetrix splitter.

Table 11. Intra-cluster ports (continued)

Port	Source -> Destination	Protocol and description	Effect if closed
	splitter <--> RPA	• Used between RPAs in the cluster for Symmetrix splitter functionality.	
6015	vRPA -> LAN vNIC vRPA LAN vNIC	• For cluster leader arbitration (UDP). • Required for cluster arbitration. Used for redundant communication between vRPAs. • RecoverPoint: WAN ports and Fibre Channel ports are also used for this purpose.	• Exposes system to single point of failure (namely, the repository volume) for leader arbitration when there is no communication with other vRPAs.
8082	vRPA LAN vNIC -> vRPA LAN vNIC	• Inbound/outbound TCP, supports log collection: connecting new vRPAs to cluster.	• Cannot collect support logs from multiple vRPAs.
8084	vRPA LAN vNIC -> vRPA LAN vNIC	• Required between vRPAs within the same cluster for cluster management (TCP). • Used to communicate with configuration database on each vRPA	• No RecoverPoint for VMs.

Secure administration

This topic provides recommendations about encrypting both communications within the RecoverPoint for Virtual Machines system and over the network.

Steps

- Only encrypted (HTTPS) mode can be used to administer RecoverPoint for VMs through the Management Application UI.

Changing the plugin server certificate

Use this procedure to change the plugin server certificate before the plugin server has been configured using **Deployment Manager**.

About this task

Use this procedure, for instance, if you want to use a certificate that has been signed by your organization's internal certificate authority.

Steps

1. Connect to the plugin server with root permissions.
2. Create a backup of the existing certificate and key files:
   `/etc/nginx/ssl/rpcenter.cert`
   `/etc/nginx/ssl/rpcenter.key`
3. Disable the firewall on the plugin server.
   Run the command **`/sbin/SuSEfirewall2 off`**
4. Upload the new certificate and key files to `/etc/nginx/ssl`.
5. Rename the new certificate file to **`rpcenter.cert`** and the new key file to **`rpcenter.key`**.
6. Reboot the plugin server VM.
7. In the **RecoverPoint for VMs Deployer**, click **Configure plugin server** home screen.
   Enter the **`plugin server IP address`** in IPv4 format, confirm the new certificate, and click **Configure**.
   For more information, see the "Configure the plugin server" in the *RecoverPoint for VMs Installation and Deployment Guide*.

Results

RecoverPoint for VMs is configured to use the new plugin server certificate.

Next steps

NOTE:

Check that the certificate is the same across all vRPAs of the same cluster before adding the vRPA to the cluster.

Log into vSphere Client from the relevant vCenter Server and check that the RecoverPoint for VMs HTML5 plugin is displayed.

Changing a registered plugin server certificate

Use this procedure to change the plugin server certificate after the plugin server has already been configured using **Deployment Manager**.

About this task

Use this procedure, for instance, if you want to use a certificate that has been signed by your organization's internal certificate authority.

Steps

1. Connect to the plugin server with root permissions.
2. Create a backup of the existing certificate and key files:
   `/etc/nginx/ssl/rpcenter.cert`
   `/etc/nginx/ssl/rpcenter.key`
3. Disable the firewall on the plugin server.
   Run the command **`/sbin/SuSEfirewall2 off`**
4. Upload the new certificate and key files to `/etc/nginx/ssl`.
5. Rename the new certificate file to **`rpcenter.cert`** and the new key file to **`rpcenter.key`**.
6. Power off the plugin server VM.
7. Unregister the RecoverPoint for VMs HTML5 plugin from the relevant vCenter Server.
   See "Unregistering the plugin from the Managed Object Browser" in the *RecoverPoint for VMs Installation and Deployment Guide*.
8. Power on the plugin server VM.
9. Navigate to `https://RPCIP/ui`.
10. Click **Authorize** and enter the vCenter Server Credentials.
11. Navigate to **DELETE /vcs/{vc-id}** near the bottom of the Swagger page.
12. Select **Try it Out**, enter the vCenter Server serial number, and select **Execute**.
    A 204 response is returned.
13. In the **RecoverPoint for VMs Deployer**, click **Configure plugin server** home screen.
    Enter the **`plugin server IP address`** in IPv4 format, confirm the new certificate, and click **Configure**.
    For more information, see the "Configure the plugin server" in the *RecoverPoint for VMs Installation and Deployment Guide*.

Results

RecoverPoint for VMs is configured to use the new plugin server certificate.

Next steps

NOTE:

Ensure the certificate is the same across all vRPAs of the same cluster before adding the vRPA to the cluster.

Log into vSphere Client from the relevant vCenter Server and check that the RecoverPoint for VMs HTML5 plugin is displayed.

Encrypted communications

Inter-RPA communication

Communication between vRPAs can be configured to require authentication and encryption (refer to Changing the RPA communication security level), even if they are in different clusters.

Network communication

RecoverPoint for Virtual Machines applies a checksum to all replicated data and control messages to prevent corruption while data is in transit over LAN and WAN IP networks. In addition, when the RPA communication security level is set to "Authenticated and encrypted", encryption and VPN authentication provide increased data protection and integrity.

SSH security

Administration of RecoverPoint for Virtual Machines through CLI is over SSH. Users who wish to do so can use the CLI command `add_ssh_key` to configure a public key that enables secure communications without entering a password. See the *RecoverPoint for Virtual Machines CLI Reference Guide* for more information about this command's parameters and usage.

Certificates handling

RecoverPoint for Virtual Machines uses certificates to establish secure communications between devices.

RPA verifying an external server

Steps

- When a vRPA initiates SSL communication with a server that is external to it, such as license server, or vCenter Server, it authenticates the server by verifying its certificate. supports certificate verification in the following flows:
  - Registration of vCenter Servers on which valid and trusted certificates are installed (from management UI and CLI).
  - Communication with licensing server (from Deployment Manager)
- The user may accept an untrusted certificate, even when RecoverPoint for VMs does not.
- vRPAs maintain a truststore of certificates that are signed by trusted certificate authorities (CAs).

Adding a certificate to a truststore

Perform the following steps to add a trusted certificate.

Steps

1. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **`admin`**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Certificates management** > **Truststore management** > **Add trusted certificate**.
2. Enter required information.
3. To ensure an effective security policy, repeat this change on every RPA at every cluster in the system.

Removing a certificate from a truststore

Perform the following steps to remove a trusted certificate.

Steps

1. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **`admin`**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security options** > **Certificates management** > **Truststore management** > **Remove trusted certificate**.
2. Enter required information.

3. To ensure an effective security policy, repeat this change on every RPA at every cluster in the system.

External client verifying an RPA

To enable secure communication between vRPA and clients that are external to them, such as Internet browsers, create a trusted certificate and install it on every vRPA in the RecoverPoint for Virtual Machines system.

Steps

- For the procedure for creating trusted certificates, see Creating a web certificate.

Installing a new web server certificate

Use this procedure to replace the current web server certificate.

Steps

1. Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced Options** > **Security Options** > **Certificates Management** > **Keystore Management** > **Change Web Server Certificate**.
   RecoverPoint for VMs requires RSA keys with 2048-bit modulus or longer.
2. Change the current web server certificate to a non-default certificate.
   Changing the certificate causes the web server to restart. Until it is fully operational again (a few minutes), the vRPA cannot be accessed through the web client, and the Installation Server is not available.
3. To ensure an effective security policy, repeat these changes on every vRPA at every cluster in the system.

Next steps

If you are using a non-default certificate, check that the certificate is the same across all vRPAs of the same cluster before adding the vRPA to the cluster.

HTTP Strict Transport Security (HSTS)

This topic explains the benefits of HTTP Strict Transport Security and how to activate it.

About this task

HTTP Strict Transport Security (HSTS) is a mechanism that protects secure (HTTPS) websites from being downgraded to nonsecure HTTP. This mechanism enables web servers to instruct their clients (web browsers or other user agents) to use secure HTTPS connections when interacting with the server, and never use the insecure HTTP protocol. HSTS is only available with certificates signed by a Certificate Authority. The best practice is to use a Certificate Authority so that Strict Transport Security can be used.

Steps

1. Create and install a web certificate that is signed by a Certificate Authority. Refer to Creating a user web certificate.
2. Activate HTTP Strict Transport Security: Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **admin**. From the **Main** menu, select **Setup** > **Advanced options** > **Security options** > **Change web server "HTTP Strict Transport Security" HSTS" mode**.

Results

Changing the HTTP Strict Transport Security mode causes the web server to restart. Until it is fully operational again (a few minutes), the vRPA cannot be accessed through the web client, and the Installation Server is not available.

Verifying when connecting a new vRPA cluster

To connect a new ("remote") vRPA cluster to an existing ("current") vRPA cluster, each side must authenticate the other.

Prerequisites

To ensure an effective security policy, including conclusive trust checks, it is recommended to replace default vRPA web server certificates with valid and trusted certificates on all vRPAs at both clusters.

Steps

1. The remote vRPA cluster authenticates the current cluster by verifying that the current cluster knows the remote cluster's **admin** password. The user should provide a password if the remote cluster credentials differ from the default and those of the current cluster.
2. The vRPA at the current cluster authenticates the vRPA at the remote cluster by verifying its certificate, similar to the verification an external server (see RPA verifying an external server).

   The user may be prompted to approve the verification.

Secure administration when directly accessing a vRPA

Accessing a vRPA through secure administration.

When accessing a vRPA directly (not through the RecoverPoint for VMs plug-in in the vSphere client), the following features and limitations are relevant to secure administration.

SNMP security

RecoverPoint for Virtual Machines supports encryption of the SNMP protocol, including the following features:

- SNMP with Advanced Encryption Standard (AES) support in the User-based Security Model.
- Ability to disable SNMPv1/v2 community strings.
- HTTPS web certificate will also service SNMP Transport Layer Security port.

Limitations

- Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP) are not supported.
- Secure Shell (SSH) transport is not supported for SNMP.
- MD5 based password hashes and DES-based privacy are not supported.

SNMP behavior

If **Agent enabled** is checked, hosts will be able to initiate SNMP queries to the RecoverPoint for VMs SNMP agent; and RecoverPoint for VMs system SNMP traps (event notification) will be enabled.

If **Send Event Traps** is enabled, the RecoverPoint for VMs system will send RecoverPoint for VMs system SNMP notifications to the specified location.

For optimal security, when defining SNMPv3 users, specify a user certificate and do not specify a password. The certificate file can contain more than one certificate; select one. All certificates in the file are equally valid.

Default SNMP behavior after new installations and upgrades

By default, SNMP is disabled in all new installations and disruptive upgrades.

After non-disruptive upgrade, SNMP will be enabled if and only if SNMP was enabled before the non-disruptive upgrade. User-access configuration will be the same as before.

WAN/LAN separation

The WAN, LAN and data traffic can be configured on different network adapters, and therefore on different subnets. RecoverPoint for Virtual Machines does not internally route IP traffic between the different interfaces. Network adapter topologies are available that route more than one traffic type on one network adapter. IP forwarding is always disabled on the vRPA.

Data security

Data security settings enable controlling the unauthorized disclosure of permanently stored data.

User data at rest

Replicated data does not persist on the vRPAs. Configuration information is saved on the repository volume in the SAN, where it is protected by standard SAN access controls; and on cluster leader vRPAs (1 and 2). Hashes of user passwords are saved on the local disks of all vRPAs.

Data erasure

The only customer data that RecoverPoint for Virtual Machines persists to disk are log events, authentication information, and RecoverPoint for VMs configuration data. The actual data replicated by RecoverPoint for VMs resides in the customer's SAN environment, not on the vRPA. For this reason, a powered down vRPA will not contain customer data beyond a portion of RecoverPoint for VMs own configuration, such as network addresses assigned to it.

Customers wishing to erase all data on an vRPA are advised to use the practice of wiping the disk, using a disk wiping utility.

Secure serviceability settings

This section includes information about user SE and system reports and alerts.

Customer support

User admin has the SE permission that enables access to the Sysmgmt CLI advanced support commands. These commands comprise a full set of tools for RecoverPoint for VMs system support. They are hidden by default, but can be displayed by using the `enable_advanced_support_commands` Sysmgmt CLI command.

Take care to always use advanced support commands correctly, since incorrect use can cause harm to your RecoverPoint for Virtual Machines. When you have finished using the advanced support commands, re-hide them by using the `disable_advanced_support_commands` command.

User root has full operating system privileges and is used by RecoverPoint for VMs engineering during service tickets escalations. Root access is logged using the standard Syslog mechanism, but due to the nature of root access, these logs can be manipulated by root.

Local access for user root is enabled using the relevant password. Local and remote support for user root is disabled by default on new installations. It can be enabled and disabled as follows: Use an SSH client to log in to the vRPA Sysmgmt CLI as **user** = **`admin`**. From the **Main** menu, select **Setup** > **Advanced options** > **Security options** > **Enable/Disable root access**. Root access should be disabled whenever it is not needed.

System reports and alerts

vRPA send weekly configuration reports and state reports, as well as system events (whose scope is normal), to the System Reports database, in real-time, through the System Alerts mechanism, using the SMTP settings configured. The system alert mechanism will filter these events to determine whether a service request should be opened with Customer Support. Only configuration and state data is sent; no customer data or statistics are collected. This mechanism is enabled by default, but can be disabled at any time through the RecoverPoint for VMs Management Application GUI or the CLI.

Details are provided in “Configure System Reports and Alerts” in the *RecoverPoint for VMs Administrator's Guide*.

System Reports enhanced

If the customer vRPAs are registered with the Secure Remote Support (Secure Remote Services) gateway, Customer Support can communicate with the customer vRPA over a VPN. This allows Customer Support to provide firsthand support, monitoring, and auditing.

Secure Remote Services is used in the following cases:

- Customers call Customer Support and request to open a Service Request.
- RecoverPoint for VMs automatically opens a Service Request (see *RecoverPoint for VMs Administrator's Guide*). In this case, Customer Support can connect to the customer vRPA, collect system information, and investigate the nature of the event before they contacted the customer about the nature of the event.

Secure deployment

The following procedure is the recommended practice for securely deploying and using RecoverPoint for VMs in typical customer environments.

Steps

1. Consider enabling high password security. Refer to Local users' security level.
2. Change the default passwords. Delete unneeded users. Refer to Predefined users.
3. Install an X.509 certificate. Refer to Secure administration.
4. Configure VMware to allow access to vRPAs only from a trusted administration console and remote vRPA clusters. Configure access for relevant servers (for example: to LDAP, NTP, DNS, SMTP; to and from SNMP, ESRS). proprietary TCP/UDP ports should only be accessible from other vRPAs. The best practice is to deploy vRPAs in a dedicated subnet or VLAN.
5. Control physical access to vSphere client and ESXi servers.
6. Control access to datastores on which the journals and repository are located.

Other security considerations

Secure Boot

RecoverPoint for VMs 5.3.2 and later versions support secure boot for the splitter and the JAM VIBs.

MD5 and SHA-256 checksums

All RecoverPoint for VMs entities that are available for download are signed with MD5 and SHA-256 checksums, which you can use to verify the integrity of your downloaded files.

OVA files signed by SRO

For RecoverPoint for VMs 5.3.1, and later, the OVA files that you download from Dell Support are signed using a certification file that is provided by SRO. The signatures validate the authenticity of the OVF package. For additional information, see the *RecoverPoint for VMs Installation and Deployment Guide.*

GPG signatures for ISO files

For RecoverPoint for VMs 5.3.1, and later, the ISO files that you download from Dell Support are signed by GnuPG, which implements the OpenPGP standard. The signatures validate the authenticity of the ISO files. For additional information, see the *RecoverPoint for VMs Installation and Deployment Guide.*

Resources beyond the control of RecoverPoint for Virtual Machines

The following resources are beyond the control of RecoverPoint for VMs. It is the responsibility of the customer to assure the availability, integrity, and security of these resources. Compromising these resources may negatively affect RecoverPoint for VMs operation and security.

- Passwords

  Ensure that passwords are sufficiently complex that brute-force attacks fail, and are kept secret.

- Physical security
- LUN masking

  Ensure that only RecoverPoint for VMs appliances have access to journals and the repository.

Troubleshooting and getting help

Product Information	For documentation, release notes, software updates, or information about products, go to Online Support at Dell Support.
Technical support	Go to Online Support and click **Service Center**. You can find several options for contacting Technical Support. To open a service request, you must have a valid support agreement. Contact your sales representative for details about obtaining a valid support agreement or with questions about your account.

Appendix

The main body of this document presents essential information about RecoverPoint for VMs security. This appendix provides additional detail on select topics.

Creating a user web certificate

Steps

1. In OpenSSL toolkit (from any computer except the vRPA), create a new private key, using the following command:

   ```
   openssl genrsa -out key.pem 2048
   ```

   NOTE: RecoverPoint for VMs requires RSA keys with a 2048-bit modulus or longer, and a sha512 hash.

2. Create a certificate signing request, using the following command:

   ```
   openssl req -new -key key.pem -out server.csr -sha512
   ```

3. Optionally, you may remove the passphrase from the key, using the following command:

   ```
   openssl rsa -in key.pem -out key_no_passphrase.pem
   ```

4. Sign the certificate. Use one of the following options:

Option	Description
Have a Certificate Authority sign	Send the certificate you created to a Certificate Authority for signing. This is the best practice, because it allows you to use HTTP Strict Transfer Security (refer to HTTP Strict Transport Security (HSTS)).
Self-sign	Use the following command: **`openssl x509 -req -days days_valid (default=365) -in server.csr -signkey key.pem -out server.crt -sha512`**