Dell SRM 5.1.1.0

SolutionPack Guide

5.1.1.0

June 2025
Rev. A00

DELL Technologies

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.

Contents

Figures

Tables

Preface

NOTE: For the latest Dell SRM documentation, see the Dell SRM Product Documentation Index on the Dell Support Site.

Related documentation

The following Dell publications provide additional Dell SRM information and are available on Dell Support Site:

- Dell SRM Release Notes: This publication contains known issues and supplemental information related to Dell SRM.
- Dell SRM Support Matrix: This publication lists SolutionPack compatibility, prerequisites, data collection interfaces, and ports.

1

Getting Started

This chapter includes the following topics:

Topics:

What are SolutionPacks?

A SolutionPack is an installable application that provides data collection and reporting capabilities for specific entities in the infrastructure. The SolutionPacks support Dell storage systems along with many common third-party storage infrastructure components.

The SolutionPacks provide asset-specific support to an enterprise installation. Organization purchases licenses to provide visibility into only those assets that exist in its installed infrastructure.

With a new installation, most SolutionPacks are initially available for you to try for 30 days using a trial license. You can obtain a permanent license that enables any number and combination of available SolutionPacks in the environment.

After a SolutionPack is installed, its reports are available in the Report Library in the User Interface. Each asset-specific node contains many predefined reports to support that asset type.

Dell SRM discovers and collects data on hosts, hypervisors, and switches, as well as Dell and third-party storage devices. Global dashboards and reports roll up data from the SolutionPacks into views and reports such as topology views, path details, capacity reports, and explore views. Dell SRM offers support for hosts, hypervisors, switches, and arrays using SolutionPacks that provide in-depth reporting for the individual objects. Most of the available SolutionPack data is rolled up into the global reports and dashboards, although not all are included. As Dell normalizes the SolutionPack data, Dell continues to add data from those SolutionPacks to the global reports and dashboard views.

Licenses

You must have a license to install SolutionPacks.

To add SolutionPacks to an initial license, contact the Dell Account representative. They can help issue temporary licenses for evaluation purposes or set up the sale of additional SolutionPacks. New entitlements are added to the existing license. To obtain the updated license, download it from the license portal.

Browse and Install

You can browse SolutionPacks before installing them to learn more about what SolutionPack monitors and the kinds of reports and dashboards that it provides.

Steps

1. Browse SolutionPacks:
   a. Log in to the SRM Frontend and click **Administration** in the banner.
   b. Browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
   A list of available SolutionPacks appears.
   c. Click a SolutionPack name.
   A page opens describing the SolutionPack and its reports. Notice the install button at the bottom of the page.
2. To prepare to install a new SolutionPack:
   a. Ensure that you have a license.
   b. Obtain installation instructions for the SolutionPack from the *Dell SRM Installation Guide*.
   Each chapter in that guide describes installation and configuration steps for integrating a particular SolutionPack into an installed Dell SRM environment.
3. To install a new SolutionPack:
   a. Browse to the SolutionPack page as described in Step 1.
   b. To start the installation, click **Install** on the description page.
   c. Continue by following instructions in the installation guide.

Reconfigure an installed SolutionPack

You can change the configuration options that are initially set during a SolutionPack installation.

About this task

To reconfigure a SolutionPack:

Steps

1. Click **Administration**.
2. Browse to **CONFIG** > **SolutionPacks** > **Installed SolutionPacks**.
   A list of installed SolutionPacks appears.
3. Select a SolutionPack name that you want to reconfigure.
   A summary description of the SolutionPack opens, including a list of configured components associated with that SolutionPack.
4. Click **Edit** (the pencil icon) next to a component to access its configuration screen.
5. Change any of the settings on the resulting screen.
6. Click **Reconfigure**, and then **Ok**.

Results

The SolutionPack is reconfigured to use the new settings.

Update SolutionPacks

You can configure Dell SRM to automatically download updates and enhancements to SolutionPacks.

About this task

The Online Update feature helps you to quickly take advantage of new capabilities as they are provided in each SolutionPack. You can configure, enable, and disable automatic downloads of SolutionPack updates. You can also see available downloads and download history.

To enable the **Online Update** feature:

Steps

1. Click **Administration**.
2. Browse to **Config** > **Update System** > **Manage Online Update**.
3. For more information, see the *Dell SRM Administration Guide* on the Dell Support Site.

Where to find the latest SolutionPack software

Install the latest core software update for the product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request for a license. For the license, submit a Support Request (SR) form, which is available on the Dell Support Site.

Dell SRM and SolutionPack privileges

This section provides the privilege levels that are required to install and operate a SolutionPack.

Table 1. Dell SRM and SolutionPack privilege levels

SolutionPack	Privilege level
SolutionPack for Amazon AWS	AWS account with IAM User, IAM credentials and an IAM access key pair
SolutionPack for Block Chargeback	User with Admin level privileges.
SolutionPack for Brocade FC Switch	SMI-S: • For SMI-S, any user having SAN system administrator privileges and having access to all Fabrics SNMP: • For SNMP v1/v2c, configure SNMP community string. • For SNMP v3, configure an SNMP v3 username. REST: • Accounts/Users with `admin` or `user` RBAC role permissions are required to trigger REST-based switch discovery in SRM. SANNAV • For SANNAV, any user having SAN System Administrator privileges are required.
SolutionPack for Cisco MDS/Nexus	• For SNMP v1/v2c, configure the SNMP community string. • For SNMP v3, configure an SNMP v3 username.
SolutionPack for Cisco UCS	Role-read-only role is sufficient for the SolutionPack to work correctly. Create a new dedicated service account for SolutionPack integration.
SolutionPack for Configuration Compliance	User with Admin level privileges.
SolutionPack for Dell SC Series	User with Admin level privileges
SolutionPack for Dell CloudIQ	API Client with read-only access for the particular tenant.
SolutionPack for Dell Data Domain	• For SNMP v1/v2c, configure the SNMP community string. • For SNMP v3, configure an SNMP v3 username.
SolutionPack for Dell Data Protection Advisor	DPA user needs a custom role with Manage Scheduled Reports privileges that are enabled on the DPA server. Enabling the Manage Scheduled Reports also enables Run reports and View existing scheduled reports and schedules. These privileges are sufficient for the DPA SolutionPack to pull data from the DPA server.

Table 1. Dell SRM and SolutionPack privilege levels (continued)

SolutionPack	Privilege level
SolutionPack for Dell ECS	A user with System Monitor role is required for data collection.
SolutionPack for Dell PowerEdge	iDRAC user with read-only access to all Redfish APIs with persistent token.
SolutionPack for Dell PowerScale	• Collection works with root/admin users who have administrative privileges. • Collection also works for a non-admin user by creating a copy of the AuditAdmin role with an additional privilege `-Auth:Configure identities and authentication sources (ISI_PRIV_AUTH).`
SolutionPack for Dell PowerStore	PowerStore Management Cluster host user with Administrator privileges is required.
SolutionPack for Dell PowerSwitch	User with Admin level privileges
SolutionPack for Dell PowerVault	Local user with non-admin level privileges
SolutionPack for Dell RecoverPoint	• Monitor account - read-only privileges • Admin account - has all privileges except security and web-download.
SolutionPack for Dell Unity/VNX/VNXe	• Unity/VNXe2 -- User with Operator role or higher.
SolutionPack for Dell EMC VMAX	For Dell SRM to collect all masking views when Symmetrix Access Control (symacl) is enabled. The Solutions Enabler host must be added to an Access Group which has Access Type BASE and VLOGIX to all devices. For Dell SRM to collect all masking views when Symmetrix Authorization (symauth) is enabled the user performing the collection only needs the Monitor role. IMPORTANT: symauth Monitor role only works to retrieve all masking views with latest Solutions Enabler 7.6.2.25 (hotfix 1843/service alert 1708). Older versions of Solutions Enabler 7.6.2 (ex. 7.6.2.8 which was required in ViPR SRM 3.5 release) required Storage Admin or Admin role to retrieve all masking views. Windows-based collector host running VMAX SolutionPack and using remote SYMAPI Server: • The Windows System account runs the Collector service which performs the VMAX collection. • The Windows System account runs the SYMCLI commands to get the masking view. • In order for symauth to retrieve all masking views the collector host's System user account must at least have the Monitor role authorized. Again, this assumes Solutions Enabler 7.6.2.25 or higher is installed. • Otherwise if an older 7.6.2 Solutions Enabler is installed, then Storage Admin or Admin role would be required. Linux-based collector host running VMAX SolutionPack: • The apg user account runs the Collector service which performs the VMAX collection. • The apg user runs the SYMCLI commands to get the masking views. • In order for symauth to retrieve all masking views the SRM Dell Linux collector host's apg user account must at least have the Monitor role authorized. Again, this assumes Solutions Enabler 7.6.2.25 or higher is installed. • Otherwise, if an older 7.6.2 Solutions Enabler is installed, then Storage Admin or Admin role would be required.
SolutionPack for Dell VMAX/PowerMax	Collection requires the specified Unisphere user to have a minimum role of Monitor.

Table 1. Dell SRM and SolutionPack privilege levels (continued)

SolutionPack	Privilege level
SolutionPack for Dell VPLEX	Use the management CLI and the Linux shell account to browse on the management station. The service account that is used by default is both a Linux account and a CLI account. From the perspective of the management CLI, the service user is not read-only, because you can perform some provisioning operations on the VPLEX, although it does not have full administrative capabilities. From the perspective of the Linux shell, the service account is a regular user account so you cannot do operations that require root privilege. For a nonservice account, follow these additional steps once the user has been created. This is assuming the SolutionPack is already installed using the service account. If it is being installed for the first time with a nonservice user, you do not need this procedure. 1. Change the permission to the virt-volumes folder with the following command: `chmod g+w virt-volumes // run under /var/log/Vplex/cli/w4` 2. Reconfigure the VPLEX SolutionPack with the alternate account.
SolutionPack for Dell VxRail	● VxRail user minimum roles required: ○ Profile-driven storage view ○ Storage view ○ vSAN ■ Cluster - ShallowRekey ○ VxRail ■ Manage VxRail clusters. ■ View VxRail clusters. ○ _brand__ ○ Manage_brand_clusters ○ View_brand_clusters ■ (either VxRail or "_brand_" role will be available based on the customer environment)
SolutionPack for Dell PowerFlex	A user with Monitor role is required for data collection.
SolutionPack for Dell EMC XtremIO	Nonadmin account with read-only privileges
SolutionPack for Hitachi Device Manager	XML API and SMI-S: ● Nonprivileged accounts with rights to view all. REST: ● Roles required for Array User to fetch data from Configuration Manager REST APIs: ○ Storage Administrator (View Only) and ○ Either one of the below roles ■ Security Administrator (View Only or View and Modify) or ■ Audit Log Administrator (View Only or View and Modify). ● User roles required on Analyzer to fetch data through REST API: ○ Analyzer GUI local user
SolutionPack for HP 3PAR StoreServ	Nonprivileged accounts with browse privileges
SolutionPack for HPE Nimble	User with Admin/PowerUser/Operator Role and Guest user (Read Only) with limited access.
SolutionPack for HP StorageWorks	Nonprivileged accounts with rights to view all.
SolutionPack for Huawei OceanStor	User with Admin level privileges
SolutionPack for IBM DS	Nonadmin account with read-only privileges

Table 1. Dell SRM and SolutionPack privilege levels (continued)

SolutionPack	Privilege level
	Discover DS8000 devices with Monitor privileges.
SolutionPack for IBM FlashSystem	A user with Admin role is required for data collection.
SolutionPack for IBM LPAR	HMC credentials • User role or Operator (recommended), or HMC Viewer (minimum). • See table 4 at Power Systems - Managing the Hardware Management Console
SolutionPack for IBM SAN Volume Controller/ Storwize	All the performance, topology, and capacity metrics are supported for a user who is a member of the Administrator user group. Performance data such as CPU usage, Port traffic statistics of nonconfiguration nodes are not supported for a user who is not a member of the Administrator user group.
SolutionPack for IBM XIV	Discovery works with Read Only, Storage Administrator, Application Administrator access. Read Only is the minimum that is required. **NOTE:** Due to limitations with the IBM software, discovery using the LDAP users will not happen if there is no active IBM XIV UI user session, either by the corresponding LDAP user or a storage administrator.
SolutionPack for Kubernetes	Cluster-role read-only user with access to all APIs with persistent non-expiring token.
SolutionPack for Microsoft Azure	• Azure Service Principal with scope at Resource Group level or Subscription level • Storage Blob Data Owner Role required for Azure Service Principal
SolutionPack for Microsoft Hyper-V	• Admin rights are required to run unsigned PowerShell scripts. To do this, you must run the following command as an administrative user: `PowerShell -C Set-ExecutionPolicy Unrestricted` On Windows Server 2008 R2 and Windows Server 2012 Hyper-V hosts, the domain administrative user must be member of domain group Domain Admins. In other words, it is not enough to make a domain user member of local group Administrators in Hyper-V hosts. On Microsoft Hyper-V Server 2012, it is possible to collect data using a nonadministrative local or domain user. This user must be a member of local groups Hyper-V Administrators and Performance Log Users groups. • On Microsoft Hyper-V Server 2012, when using local or domain user for discovery, it is also necessary to give cluster access to the user to get CSV details. The below command must be run from the Administrator account in PowerShell prompt to grant cluster access. `Grant-ClusterAccess -User <Username> -Full` For example, `Grant-ClusterAccess -User srmuser -Full or Grant-ClusterAccess -User domain\srmuser -Full` • The hyper-v users(or the group they are part of) must have access to the following WMI classes: ○ root\cimv2 ○ root\wmi ○ root\MSCluster ○ root\virtualization(Windows 2008 only) ○ root\Microsoft\Windows\Storage(Windows 2012 onwards) ○ root\virtualization\v2(Windows 2012 onwards)
SolutionPack for Microsoft SQL Server	• SQL authentication requires that the user be a member of the SYSADMIN group.

Table 1. Dell SRM and SolutionPack privilege levels (continued)

SolutionPack	Privilege level

	• Windows user account requires the user be a member of the Guests group or the Domain Guests group.
	• The default database must be the master.
	• Windows user account must be imported into the Microsoft SQL Server with settings similar to these:
	  ○ Server roles of the public
	  ○ Securable grants for Connect SQL, View any definitions, and View server state

SolutionPack for NetApp FAS	SSH connection to the C-Mode NetApp devices with the following role: • Access level readonly for the commands : cluster, network interface, volume, snapshot policy, job schedule cron, snapshot, df, storage disk, node, aggr, cifs, system node, lun, quota, qtree, export-policy rule, network port, network connections, fcp adapter, fcp initiator, snapmirror, igroup, vol efficiency, iscsi nodename, vscan scanner-pool, storage encryption disk, storage aggregate, storage aggregate show-cumulated-efficiency, vserver object-store-server bucket • Access level 'all' for the commands: set, system, statistics
SolutionPack for Oracle Database	The Dell SRM collector must connect to each instance of Oracle databases and perform SQL queries. You can use either an administrator equivalent system account, or create a dedicated system account for the collector. If you want to use the last option, ask the DBA administrator to run the query described in the SolutionPack for Oracle chapter. This creates a Watch4net account, which specific grant for the collector.
SolutionPack for Oracle MySQL Database	This SolutionPack requires MySQL database user login privileges to collect information from MySQL database servers running remotely.
SolutionPack for Physical Hosts	Windows user privileges • Domain user in the local administrators group (recommended), or • Local administrator for the host UNIX user privileges • Sudo user with read/execute permissions for commands, or • SSH public/private key pair with execute permission for commands. See the SolutionPack for Physical Hosts chapter for more information. VIO server • SUDO user role with elevated (root) privileges to execute commands to be run on the VIOS host. • Note: The admin role is not required for VIO Servers. VIO Client/LPAR • SUDO user role (or) • SSH Keys (or) • Root user (optional)
SolutionPack for Pure Storage	REST: • Accounts/Users with admin or user RBAC role permissions are required to trigger REST-based discovery in SRM.
SolutionPack for System Health	User with Admin level privileges
SolutionPack for VMware vSphere vSAN & VxRail	VMware device discovery functions are flexible and can be used by: • Read-only non-admin users • Admin and non-admin users with different privilege levels **NOTE:** 1. Storage Policy will not collect with Read-Only User role, Its part of VxRail SP Roles.

Table 1. Dell SRM and SolutionPack privilege levels (continued)

SolutionPack	Privilege level
	2. For VxRail Device discovery in this VMware combined SP, see above “SolutionPack for Dell VxRail” SP table Privileges.

Alert consolidation configurations for Dell SRM SolutionPacks

This section identifies the alert sources for each Dell SRM SolutionPacks.

Table 2. Dell SRM SolutionPack alert consolidation requirements

SolutionPack	Alert source
SolutionPack for Amazon AWS	N/A
SolutionPack for Block Chargeback	N/A
SolutionPack for Brocade FC Switch	SNMP
SolutionPack for Cisco MDS/Nexus	SNMP
SolutionPack for Cisco UCS	N/A
SolutionPack for Configuration Compliance	N/A
SolutionPack for Dell SC Series	SNMP
SolutionPack for Dell CloudIQ	N/A
SolutionPack for Dell Data Domain	SNMP
SolutionPack for Dell Data Protection Advisor	REST
SolutionPack for Dell ECS	REST
SolutionPack for Dell PowerEdge	N/A
SolutionPack for Dell PowerScale	REST
SolutionPack for Dell PowerStore	SNMP
SolutionPack for Dell PowerSwitch	N/A
SolutionPack for Dell PowerVault	REST
SolutionPack for Dell RecoverPoint	SNMP
SolutionPack for Dell Unity/VNX/VNXe	REST
SolutionPack for Dell EMC VMAX	SNMP
SolutionPack for Dell VMAX/PowerMax	SNMP
SolutionPack for Dell VPLEX	SNMP
SolutionPack for Dell VxRail	SNMP
SolutionPack for Dell PowerFlex	REST
SolutionPack for Dell EMC XtremIO	REST
SolutionPack for Hitachi Device Manager	N/A
SolutionPack for HP 3PAR StoreServ	SNMP
SolutionPack for HPE Nimble	SNMP
SolutionPack for HP StorageWorks	N/A

Table 2. Dell SRM SolutionPack alert consolidation requirements (continued)

SolutionPack	Alert source
SolutionPack for Huawei OceanStor	SNMP
SolutionPack for IBM DS	SNMP
SolutionPack for IBM FlashSystem	SNMP
SolutionPack for IBM LPAR	N/A
SolutionPack for IBM SAN Volume Controller/Storwize	N/A
SolutionPack for IBM XIV	SNMP
SolutionPack for Kubernetes	N/A
SolutionPack for Microsoft Azure	N/A
SolutionPack for Microsoft Hyper-V	N/A
SolutionPack for Microsoft SQL Server	N/A
SolutionPack for NetApp FAS	SNMP
SolutionPack for Oracle Database	N/A
SolutionPack for Oracle MySQL Database	N/A
SolutionPack for Physical Hosts	SNMP
SolutionPack for Pure Storage	SNMP
SolutionPack for System Health	N/A
SolutionPack for VMware vSphere vSAN & VxRail	SNMP

For more details, see the Dell SRM Alert Matrix from Dell Support Site.

Configurations for collecting carbon emission data

The carbon emission data is computed by using the carbon Emission factor. This can be tagged to a device based on the device name, location, serial number, or any combination of properties by performing the following steps:

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **Groups & Tags** > **Manage Groups** > **Carbon Emission Factor Grouping**.
2. Click **Create**.
3. Enter the Carbon Emission Factor.
4. Add entries to the tables by providing the rules for the group. User can create rules based on location, device name, serial number, or any combination of properties.

   NOTE: It is mandatory to set the rule property `iscsr` as **`true`** to obtain the carbon emission data.

5. Click **Save**.
6. (Optional) **Export Groups**: You can export the group to your Downloads folder, update the Excel sheet with the required rule information, and then import the file using the **Import Groups** button.
   You can now see the Groups of Carbon Emission Factors for the devices, and the carbon emission data will be populated in SRM reports.

   NOTE: For SolutionPack report under **Operations** > **Power Consumption** > **Overview**, the data polling happens for every four hours through Web Service. Therefore, a minimum of three collections are required in order to populate this report. Check the Frontend Web Service configuration to populate the report.

   NOTE: The carbon emission data collection feature is currently limited to the following SolutionPacks:
   - SolutionPack for Brocade FC Switch
   - SolutionPack for Dell PowerEdge

- SolutionPack for Dell PowerScale
- SolutionPack for Dell PowerVault
- SolutionPack for Dell Unity
- SolutionPack for Huawei OceanStor
- SolutionPack for Pure Storage

Link and launch CloudIQ

To link and launch CloudIQ, perform the following steps:

Prerequisites

- The devices must be discovered in both SRM and CloudIQ.
- The browser session of CloudIQ should be active.
- The device identifier in CloudIQ and SRM should match. Issue may arise if the device's last contact time with CloudIQ was earlier than a significant amount of time.

From global reports

Steps

1. Go to **Explore** > **Storage** > **Storage Systems**.
2. Select the respective device row and right-click to choose **Launch CloudIQ**.
   You will be directed to the health dashboard of the respective device in CloudIQ.

From supported SolutionPacks

Steps

1. Go to **Report Library** > **[SolutionPack]** > **Summary** > **Card view**/**Table view**.
2. To select devices:
   - Under **Card view**: Mouse over on device.
   - Under **Table view**: Select the row of the respective device.
3. Right-click and select **Launch CloudIQ**.
   You will be directed to the health dashboard of the respective device in CloudIQ.

2

SolutionPack for Amazon AWS

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Amazon AWS collects storage and instances data from the Amazon AWS account and displays the data in easy-to-use reports in Dell SRM.

Installing the SolutionPack

Prerequisites

For Windows and Linux binary installations, the AWS Command Line Interface (CLI) tools are installed and configured on the collector server. Also, Windows binary installations require a minimum of Windows Management Framework 3.0. The AWS CLI tools are preinstalled on the Dell SRM vApp. For more information about installing AWS CLI, see: Get started with the AWS CLI.

The AWS CLI tools must be configured for user apg, with credentials and configuration files under `/opt/APG/.aws/`.

Ensure that the appliance has the correct date and time so that AWS does not reject requests. For more information about Configuring the AWS Command Line Interface, see: Get started with the AWS CLI.

For cost reports, the following reports must be enabled in the Amazon AWS account billing preferences:

- **Monthly cost allocation report** for monthly cost analysis
- **Detailed billing report with resources and tags** for hourly cost estimates

For more information about configuring reports, see: What is AWS Billing and Cost Management?.

NOTE: The SolutionPack downloads the files from the specified bucket to parse them. Standard AWS storage rates apply.

NOTE: Dell Technologies recommends using SSL for AWS from SRM version 5.0.0.0 onwards.

Ensure that the following details are available to configure the SolutionPack during installation:

- AWS CLI profile name to use for each collection configuration profile (see `/opt/APG/.aws/credentials`)
- Account Name (used to tag collected data. Example: john.doe)
- Account Number (used to tag collected data)
- S3 bucket name where Excel billing reports are located. You must be the owner of this bucket

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.

6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
8. Type the location of the Amazon AWS CLI bin file.
9. Optionally, specify any additional AWS CLI arguments to pass.
10. Optionally, select **Configure advanced settings** to configure topology and billing polling intervals.
11. Click **Next**.
12. Click **Install**.
13. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Discovering AWS accounts and services

Follow the procedure for each Amazon AWS account that you want to monitor.

Steps

1. Go to **Discovery Center** > **Manage Discovery** > **Amazon AWS Account**.
2. Select Amazon AWS Account and click **Add**.
3. Select the server and collector instance where you want to store the configuration details.
4. Select the Secure Vault checkbox to fetch the device credentials from the CyberArk server to discover the device. On selecting the Secure Vault checkbox, the Unique Key field appears and the Secret Access Key field is disabled.
   NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Secret Access Key is active.
5. Provide Amazon account details like Account ID, Account Name, IAM User Name, Access Key ID, and Secret Access Key.
6. If secure vault is enabled, enter the Unique Key.
7. Select the services that you want to monitor.
8. To validate access to the account and services, click **Validate and Add**.
9. Click **Ok**.
10. Click **Save**.

Limitations

When the AWS SolutionPack Collector is installed on a separate Linux server, and the AWS CLI is not installed on the default path, then the error is displayed in the collection log file.

Since there is no functionality impact due to this error, you can ignore this exception.

```
SEVERE - [2016-05-20 09:03:47 EDT] - AbstractStreamHandlerJob::prepareNextStep(): Error
executing handler Read billing file-FileOpener
 com.watch4net.apg.ubertext.parsing.StreamHandlerException: Error while creating the
stream for file /opt/APG/Collecting/Stream-Collector/amazon-aws-linux/./incoming/
150213616981-aws-billing-detailed-line-items-with-resources-and-tags-2016-05.csv
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.newFileToRead(FileReader
Retriever.java:370)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.access$200(FileReaderRet
riever.java:53)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever$FileOpenerHandler.handle
Execution(FileReaderRetriever.java:452)
 at
com.watch4net.apg.ubertext.parsing.concurrent.AbstractStreamHandlerJob.prepareNextStep(Ab
stractStreamHandlerJob.java:170)
 at
```

```
com.watch4net.apg.ubertext.parsing.concurrent.SimpleStreamHandlerJob.step(SimpleStreamHan
dlerJob.java:43)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor$SequentialJob.step(AbstractJobE
xecutor.java:421)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.executeJobRunner(AbstractJobExe
cutor.java:124)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.access$500(AbstractJobExecutor.
java:24)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor$JobRunnerImpl.run(AbstractJobEx
ecutor.java:276)
 at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
 at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
 at java.lang.Thread.run(Thread.java:745)
 Caused by: java.io.FileNotFoundException: /opt/APG/Collecting/Stream-Collector/amazon-
aws-linux/./incoming/150213616981-aws-billing-detailed-line-items-with-resources-and-
tags-2016-05.csv (No such file or directory)
 at java.io.FileInputStream.open0(Native Method)
 at java.io.FileInputStream.open(FileInputStream.java:195)
 at java.io.FileInputStream.<init>(FileInputStream.java:138)
 at
com.watch4net.apg.common.io.ActionOnCloseFileInputStream.<init>(ActionOnCloseFileInputStr
eam.java:170)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.newFileToRead(FileReader
Retriever.java:363)
```

3

SolutionPack for Block Chargeback

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Block Chargeback provides visibility into block storage usage and associated costs by host or by defined groups of hosts in the environment.

When you install the SolutionPack, it creates a chargeback preprocessor task that runs as configured during SolutionPack installation and collects block chargeback metrics for all physical hosts and virtual machines. Primary Used, Primary Presented, Total Used, and Total Presented are the four use cases. The reports display chargeable capacities and cost for every physical host, virtual machine, hypervisor cluster, and defined device group for each of these use cases. The reports also display chargeable capacity by service level.

Chargeable and nonchargeable metrics

This SolutionPack can generate both chargeable and nonchargeable metrics. Nonchargeable metrics are optional, and are disabled by default during SolutionPack installation.

If storage is not shared across hosts, there is no difference in chargeable and nonchargeable metric values.

The values are different when multiple hosts share a physical or virtual volume.

- Nonchargeable metrics are the values as seen directly by the host. The same values are duplicated for each of the hosts sharing that storage, without regard for how many hosts are sharing it.
- Chargeable metrics take host sharing into account, and divide the metrics by the number of hosts that are sharing it. The metrics are deduplicated, making them representative of chargeability.

Examples

If two hosts are sharing 500 GB of block storage from the same disk, and none of that storage is used, the capacity metrics are as shown in the following table.

Table 3. Shared disk with no storage used

Metric name	Host A - Disk1	Host B - Disk1
Non-Chargeable Presented (=total capacity of the disk)	500 GB	500 GB
Non-Chargeable Used (=used capacity of the disk)	0	0
Chargeable Presented (=total capacity of the disk ÷ # hosts sharing it)	250 GB	250 GB

Table 3. Shared disk with no storage used (continued)

Metric name	Host A - Disk1	Host B - Disk1
Chargeable Used (=used capacity of the disk ÷ # hosts sharing it)	0	0

Alternatively, if Host A uses 100 GB of this storage, the capacity metrics are as follows.

Table 4. Shared disk with some storage used

Metric name	Host A - Disk1	Host B - Disk1
Non-Chargeable Presented (=total capacity of the disk)	500 GB	500 GB
Non-Chargeable Used (it has changed 0 GB–100 GB)	100 GB	100 GB
Chargeable Presented (=total capacity of the disk ÷ # hosts sharing it)	250 GB	250 GB
Chargeable Used (=used capacity of the disk ÷ # hosts sharing it)	50 GB	50 GB

Installing the SolutionPack

Prerequisites

- Identify the collector host for the chargeback preprocessor.
- Identify the chargeback use case that you are interested in. Possible options are:
  - Presented—Only presented capacity and cost metrics are computed. Presented capacity is based on the total capacity that is provisioned to the host but not necessarily written.
  - Used—Only used capacity and cost metrics are computed. Used capacity is based on the actual capacity.
  - Both (Default)—Both used and presented capacity and cost metrics are computed.
- Identify whether non-chargeable capacity and cost metrics are needed. If the **Enable non-chargeable metrics** option is enabled, non-chargeable metrics are created in addition to the chargeable metrics. Non-chargeable metrics are key-performance indicators of storage, showing the capacities and costs for the storage before deduplication is applied for the hosts sharing that storage.
- Identify whether collection of component level chargeback metrics are needed. If the **Enable component level chargeable metrics** option is enabled, chargeback metrics are collected for every constituent component of the host or the virtual machine (including host devices, RDMs, and VMDK/log files).

  NOTE: Enabling this feature causes a significant increase in metrics that are produced and may result in the need for additional backends in larger environments.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
7. From the **How often should the chargeback calculations run?** drop-down list, select the desired frequency for the chargeback preprocessor task.

   The default value is **Every day**. The other options available are **Every 2 days**, **Every 5 days**, **Every 7 days**, and **Every 6 hours**.
8. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

9. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

   If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.

   NOTE: In a multi-server setup, ensure to select a Frontend server. Do not select **same-as-generic-chargeback-collect** or other choices that result in using `localhost`. The `localhost` in this SolutionPack refers to the Collector server for the chargeback preprocessor.

10. To configure various options, select **Use advanced settings**.
    a. From the **Compute Chargeback for Use-case** drop-down list, select the option for the desired use case.

       By default, both **used** and **presented** chargeback metrics are collected.

    b. Check or uncheck the **Enable non-chargeable metrics** option for the desired use case.

       This option is not enabled by default.

       If this option is enabled, the non-chargeable capacity and cost metrics are created in addition to the chargeable metrics. Non-chargeable metrics are key-performance indicators of storage, showing the capacities and cost for the storage before deduplication is applied for the hosts sharing that storage.

    c. Check or uncheck the **Enable component level chargeable metrics** option for what was identified earlier.

       This option is enabled by default.

       If this option is enabled, chargeback metrics are collected for every constituent component of the host or the virtual machine (including host devices, RDMs, and VMDK/log files).

       NOTE: Enabling this feature causes a significant increase in metrics that are produced and may result in the need for additional backends in larger environments.

    d. Check or uncheck the **Enable Parallel Execution** option for the desired use case.

       This option is not enabled by default.

    e. In the **Maximum Thread Pool capacity/processors to run chargeback preprocessor** field, enter the the number of processors for this configuration. The default value is 3.

    f. In the **Maximum Queue size to execute chargeback in parallel mode** field, enter the maximum chargeback process to be queued for parallel processing. The default value is 20.

    g. Check or uncheck the **Enable Batch Execution** option for the desired use case.

       This option is enabled by default. This option enables parallel batch execution of chargeback preprocessor. This flag should be enabled along with parallel execution. This enables group of hosts to be processed as a batch.

    h. In the **Maximum number of hosts to be processed as a batch** field, enter the maximum number of hosts to be batched for the execution. The default value is 50.

11. Click **Install**.
12. When the installation is complete, click **OK**.

Next steps

Chargeback reports are available under **Reports Library** > **Chargeback** and also under **Operations** > **Chargeback**.

The reports are empty immediately after the SolutionPack is installed. They start displaying data only after the chargeback preprocessor task completes successfully and data has had sufficient time to propagate through the environment. This task runs using the schedule that is selected during installation.

User configuration changes affect chargeback data, such as changes to service level tags and user-defined group definitions. In general, expect to wait 1 day plus the frequency of the chargeback task to see reconfigured chargeback data after such changes.

To shorten these wait times, wait for data collection to occur and then manually run the chargeback preprocessor task. For example, if the chargeback preprocessor task is scheduled to run every 5 days, wait the 1 day for data to settle and then manually run the task.

Running the chargeback preprocessor task manually

Run the chargeback preprocessor task manually instead of waiting for the scheduled run.

Steps

1. In **SRM Admin UI**, browse **CONFIG** > **Settings** > **Scheduled Tasks**.
2. Select the chargeback processor instance. The default instance name is `chargeback-processor-generic-chargeback`.
3. In the right pane, click **Run Now**.

Enable collecting component level metrics for a limited set of hosts

You can specify a list of hosts to the collector to limit collection.

About this task

Use this procedure to enable full collection of certain hosts regardless of SolutionPack configuration settings.

Steps

1. In **SRM Admin UI**, browse to **System Admin** > **Servers & Modules** > **Modules**.
2. Use the Search field to find **Chargeback Processor::Generic Chargeback**.
3. Click the arrow on the **Configuration files** row to expand it.
4. Select the file that is named `/conf/chargeback-processor.properties`, and click **Edit**.
5. In the editing window, add the following entry to the end of the file:

   ```
   cbp.usecase.whitelist=<hosts>
   ```

   where *<hosts>* is a comma-separated list of hostnames.

6. If the whitelist separator must be changed to a character other than comma, add the following additional entry:

   ```
   cbp.usecase.whitelist.separator=separator
   ```

   where separator is the character. For example, to use the pipe character as separator, type:

   ```
   cbp.usecase.whitelist.separator=|
   ```

   Here are example entries:

   ```
   #cbp.usecase.whitelist=host1,host2,host3
   #cpb.usecase.whitelist.separator=,
   ```

7. Click **Save**.

   NOTE: If the SolutionPack is reconfigured, direct changes to this file are lost. In that case, the changes must be reentered.

Chargeback optimization to reduce processing time

Chargeback preprocessor is optimized to reduce the processing time.

Steps

1. In **SRM Admin UI**, browse to **System Admin** > **Servers & Modules** > **Modules**.
2. Use the Search field to find **Chargeback Processor::Generic Chargeback**.
3. Click the arrow on the **Configuration files** row to expand it.
4. Select the file `/conf/chargeback-processor.properties`.
5. Click **Edit**.
   The following properties is added to support chargeback optimization:

```
cbp.parallel.execution=true
cbp.threadpool.maxqueuesize=20
cbp.threadpool.maxcapacity=3
cbp.parallel.batch.execution=true
cbp.threadpool.maxhostsize=50
```

   Max Capacity can be tuned based on the number of processors, ensure not to exceed the available processors.

Limitations

This section list the limitations of SolutionPack for Block Chargeback.

- When you upgrade from a previous version, the SolutionPack for Block Chargeback is not installed by default and the old chargeback reports reference a broken link. Install the SolutionPack for Block Chargeback to obtain chargeback reports and resolve this link.
- Hosts that are not completely discovered and hosts with only local disks do not show up in chargeback reports.
- Delegation of chargeable capacities to host disk capacity when the backend array is not discovered and not supported for passive hosts nor for Windows hosts discovered through the SolutionPack for Physical Hosts using a user with non-admin privileges.
- This SolutionPack does not support chargeback reporting for:
  - RDM level chargeable capacity is not shown for Hyper-V VMs, therefore the component level chargeback reports are empty
  - Hyper-V chargeback is supported at the hypervisor level, VM level chargeback is supported only for LUNs mapped to VM with NPIV configuration
  - Virtual Machines where the data store on which the VM resides is backed by BOTH a LUN and a virtual volume
  - Virtual Machines where the data store on which the VM resides is backed by BOTH a local virtual volume and a remote virtual volume
  - Virtual volumes that are backed by RAID 1 (mirrored) LUNs
  - Hosts with disks that are backed by a distributed virtual volume if any of the arrays contributing to the storage of that distributed virtual volume are undiscovered
- Chargeback data is missing for hosts that are discovered passively using the Hitachi Device manager SolutionPack and connected to arrays other than HDS arrays. Chargeback data for disks that are directly connected to such passive hosts from HDS show up correctly.
- When a `vmdk` file is backed up by Avamar and the VM which hosts Avamar is discovered by Dell SRM, Chargeback considers both the hosts (Actual host and Avamar backed VM) as connected to the `vmdk` file. As a result, chargeable capacity is shared between both the VMs. As a workaround, change/deny the permission from vCenter to collect data from Avamar backed VM. In this way, no metrics are collected from the VM, which hosts Avamar and no impact on the chargeable capacity happens.

4

SolutionPack for Brocade FC Switch

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Brocade FC Switch accesses performance data information that was automatically collected and interpreted (using resource grouping and mathematical calculations) from across multiple fabrics. Alerts are consolidated from Brocade FC Switches and shown on the **All Alerts Console**.

Data collection methods

SMI-S	Discover switch topology, zoning details, and some performance data through SMI-S.
SNMP + SMI-S (Zoning only through SMI-S)	Discover switch topology and all performance data through SNMP. SNMP does not support zoning discovery. Restrict SMI-S discovery to zoning details only.
REST	Discover switch topology, zoning details, and performance data through Fabric OS (FOS) REST API.
SANNAV	Discover switch and zoning details through SANnav management portal.

NOTE: To collect carbon emission data for a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

Brocade switch and SMI agent configuration

Configure Brocade switches and SMI agents for discovery and alert consolidation in Dell SRM.

- Configuring Brocade SMI Agents
- Configuring Brocade switches for alert consolidation
- Configuring Brocade Switches for SNMP discovery

Configuring Brocade SMI Agents

Install and configure the Brocade SMI agent for complete switch discovery or zoning discovery only.

Steps

Install Brocade SMI agent in one of the following modes:

Installation mode	Description
Integrated Brocade SMI Agent	The Brocade SMI agent is integrated with CMCNE, BNA, CMDCE, DCFM, and gets installed when you install any of these products.
Brocade SMI Agent only (headless installation)	Headless installation (silent mode installation) does not need a license and installs the SMI agent only.

Refer to the CMCNE/CMDCE installation guide for more details on installation and configuration of Brocade SMI agent.

Configuring Brocade switches for alert consolidation

Use the `snmpConfig` command to forward SNMP v1 traps from Brocade switches to Dell SRM.

About this task

Trap-based alerts for Brocade switches are supported through SNMP regardless of the discovery option you choose. Even if you choose not to restrict SMI-S to zoning discovery, configure the switches for SNMP trap forwarding.

Use the snmpConfig command to forward SNMP v1 traps from Brocade switches to Dell SRM.

Steps

1. Log in to the Brocade FC switch as the administrator.
2. Type **`snmpConfig --set snmpv1`** and press **Enter**.
3. Type the following details, when prompted:

Option	Input
Community	**`[public]`**
Trap recipient's IP address	In a single vApp installation, this option is the Dell SRM IP, and in a distributed environment, is the Primary Backend server's IP.
Trap recipient severity level	**`(0..5)`**
Trap recipient port	**`2041`**, which is the Dell SRM trap listening port.

4. If you have multiple Brocade FC switches in the storage environment, repeat this procedure on each switch.

NOTE: To forward SNMP v3 traps from Brocade switches to Dell SRM, use the **`snmpConfig --set snmpv3`** command and provide the above-mentioned inputs along with the SNMP v3 user credentials.

Configuring Brocade switches for SNMP discovery

If you choose SNMP+SMI-S (zoning only through SMI-S) discovery option, Brocade switches are configured with SNMP v1/v2c/v3 credentials.

Steps

1. Launch a command line interface for the Brocade switch and log in with Administrator credentials.
2. To configure the switch for SNMPv1/v2c, perform the following steps:

a. Type `snmpConfig --show snmpv1`.
   The community strings are listed.
b. If you want to change a community string, type `snmpConfig --set snmpv1`
c. Type the new community string and continue.

3. To configure the switch for SNMPv3, perform the following steps:
   a. Type `snmpConfig --show snmpv3`.
      The configuration parameters are listed.
   b. If you want to change the parameters, type `snmpConfig --set snmpv3`.
   c. Type the parameters and continue.
4. Repeat these steps for each Brocade switch in the storage environment.

Configuring Brocade switches for REST discovery

Launch a command-line interface for the Brocade switch and log in with Administrator credentials. To configure the switch for REST discovery, perform the following steps:

Steps

1. Log in with Administrator or User with RBAC role permissions.
2. To configure max rest sessions and sample requests evaluate this formula: (Number of VFs * 9) + and provide the value below for samplerequest option.

   Run the command with the value evaluated above.

   For < FOS 9.1.x version:

   ```
   mgmtapp --config -maxrestsession 3 -samplerequest <sample requests value evaluated above>
   ```

   For >= FOS 9.1.x version:

   ```
   mgmtapp --config -maxrestsession 3
   ```

3. Non-VF enabled Switch - To configure max rest sessions and sample requests.

   For <FOS 9.1.x version:

   ```
   mgmtapp --config -maxrestsession 3 -samplerequest <Default sample request values based on FOS version running on the switch>
   ```

   For >=FOS 9.1.x version:

   ```
   mgmtapp --config -maxrestsession 3
   ```

NOTE:

- FOS 9.1.x and above, see the respective version of Brocade Fabric OS REST API Reference Manual for the default values of REST throttling configuration values (For example: samplerequest).
- For Rest API configuration parameters sampletime, samplerequest and idletime are deprecated. Weblinker multi-threading is supported in FOS 9.1.0 onwards, so, rate-limiting and throttling were removed because of the number of requests processed by multiple threads with the dynamic rate-limiting/throttling with the cgroup introduction of CPU and memory usage monitoring.

Configuring Brocade switches for SANNAV discovery

NOTE: See the respective Brocade SANnav Management Portal User Guide, for configuring Brocade switches and discovering fabrics through SANNAV.

Installing the SolutionPack

About this task

- To discover the switch topology (switch details and switch port details) and switch performance using SNMP and zoning details through SMIS, you must be aware of SNMP v1/v2 community strings and SNMP ports, or SNMP v3 user details and privacy and authentication details for the v3 username. In addition, the username, password, port number, and SSL enabled/status for the SMI-S provider are required to discover the zoning details.
- To discover the switch topology, switch performance, and zoning details through SMIS, the username, password, port number, and SSL enabled/status for the SMI-S provider are required.
- The Dell SRM Alerting Guide explains how to configure alerts consolidation.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, choose an alerting web-service instance.
8. Click **Next**.
   The window displays Brocade data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
12. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
13. From the **SMI-S Discovery Configuration option** drop-down list, select existing settings that have been specified for other components, or add a new configuration. If required, select **Restrict SMI-S to zoning discovery only**.

    If the option is selected, SMI-S will be used to discover zoning details only. If cleared, SMI-S will be used to discover switch and zoning details completely.
14. From the **Passive Host Discovery Specific Configuration** drop-down list, select existing settings that have been specified for other components, or add a new configuration. If required, select **Enable Passive Host Discovery**.

    See Passive host discovery configuration options for additional details.
15. Optionally, select **Advanced settings for SMI-S** to configure polling settings.

    Beginning with ViPR SRM 4.2, the SolutionPack for Brocade FC Switch allows you to discover Brocade SNMP based switch discovery using Discovery Center. The advantage of using Discovery Center is that you can discover all the switches in a fabric by entering the IP address of just one switch in the fabric by using discovery groups. However, you can discover Brocade switches through SNMP using Device Discovery web application and the Generic-SNMP collector. This option has been provided for backward compatibility.
16. Select **Configuration settings for SNMP Discovery** option For SNMP discovery.

The advanced settings are applicable only for the SNMP based switch discovery using Discovery center using Brocade collector and are not applicable for the Generic-SNMP collector. Use caution when configuring these settings. Improper settings impact Brocade Collector performance.

On selecting **SNMP Discovery Configuration**, user can optionally configure the SNMP Collector name, SNMP Collector port, and Communication interface IP address.

Polling period configuration:

Performance data Polling period defines the frequency with which the Brocade Collector polls the performance related data from the switch.

Topology Polling period defines the frequency with which Brocade Collector polls the topology related data from the switch.

All the capabilities that are supported by the switch will be polled.

Polling Group configuration consists of a group of switches and some of the capabilities that are supported by those switches. You can optimize the resources that are consumed by the Brocade Collector by tuning these settings.

Property refresh time is the time at which the properties will be refreshed for a polling group. The property refresh time format is HH:MM:SS, where HH is hours, MM is minutes, and SS is seconds.

Start Polling Group at Defined period when enabled, will start the polling at the next "round" period. Raw value timestamps will be accurate. For example, if the polling period is set to 5 minutes, this would mean that the polling cycles will start at 00:00, 00:05, 00:10, and so on.

Polling Group Start Time offset (s) is used to start different polling groups at different times to avoid putting an excessive load on the Brocade Collector. The polling for the polling groups will start one after the other with a delay that is specified by this time offset. When setting a polling group start time offset, consider the shortest polling period (performance or topology), the time it takes for the Brocade Collector to poll the switch for the capabilities in the polling group, and the number of polling groups. If the polling group start time is too short, the load on the Brocade Collector will increase. If the polling group start time is too long, the polling groups might not be finished polling within the polling interval and the next polling period might start.

17. Optionally, to configure polling settings for discovery through SANNAV, select **Advanced settings for SANNAV**.
    a. Performance data Polling period: Default value - 15 minutes
    b. Topology polling period: Default value - 60 minutes
18. Click **Next**.
    The window displays report settings.
19. In **Administration Web-Service Instance**, select an existing instance or create a custom instance.
20. Click **Next**.
    The window displays a note about SNMP masks.
21. Click **Install**.
22. Click **Ok**.
    Monitor the installation logs to ensure that the installation completes successfully.

Discovery of Brocade Elements through Discovery center

The section describes how to add Brocade SMIS provider, SNMP based switch discovery, Brocade switch though REST and Brocade switch through SANNAV using Discovery Center. To add multiple Brocade elements at a time, use a discovery group.

About this task

The advantage of using a discovery group is that you can discover all the switches in a fabric by entering the IP address of just one switch per fabric or multiple SMIS providers. If the switches/provider shares credentials, the credentials must be entered once as well. For more information about creating discovery groups, see Add devices using discovery.

Steps

1. In the **SRM Admin UI**, browse to **Discovery** > **Discovery Center** > **Manage Discovery**.
2. Select **Brocade FC Switch** and click **Add** .
3. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE:

a. The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.
b. Secure Vault checkbox will not work for SANNAV Discovery Mode as SANnav does not support CyberArk.

4. In the **Device location** section, select the **Server** and **Instance** where you want to store the configuration details for this device.
5. Select **Discovery Mode**.
   - To discover Brocade switch though REST, select **REST** option from the drop-down.
     a. In the **SMI-S Provider/Switch IP Address** field, type the Brocade Switch name or IP Address.
     b. Type the access credentials.
     c. If required, select **Enable Secure Connection (SSL)**.
     d. Type the port number. The default ports are 80 for non-SSL and 443 for SSL.
     e. Click **Validate and Add**.
     f. Click **Ok**.
     g. Click **Save**.
   - To discover SANnav, select **SANNAV** from the drop-down.
     a. In the **SMI-S Provider/ SANnav/Switch IP Address** field, type the Brocade SANnav management portal IP Address.
     b. Type the access credentials.
     c. Type the port number. The default HTTPS port is 443.
     d. Click **Validate and Add**.
     e. Click **Ok**.
     f. Click **Save**.
   - To discover SMI-S provider, select **SMI-S** option from the drop-down.
     a. In the **SMI-S Provider/Switch IP Address** field, type the Brocade SMI Provider host.
     b. Type the access credentials.
     c. If required, select **Enable Secure Connection (SSL)**.
     d. Type the port number. The default ports are 5988 for non-SSL and 5989 for SSL.
     e. Click **Validate and Add**.
     f. Click **Ok**.
     g. Click **Save**.
   - To discover Brocade switch though SNMP, select **SNMP** option from the drop-down.
     a. In the **SMI-S Provider/Switch IP Address** field, type the IP address of the device that is supporting the SNMP agent.
     b. Switch name is optional.
     c. In **SNMP Port** field, type the device SNMP agent listening port.
     d. In the **SNMP Version** field, type the device SNMP agent version. If you select v3, select the authentication and encryption protocols, and specify the passwords.
     e. In the **Community String/User Name** field, specify the community name if the SNMP version is v1 or v2c. Specify the username if the SNMP version is v3.
     f. Timeout information is optional.
     g. Number of retries is optional.
     h. To trigger discovery, click **Validate and Add**.
        - Discovery fetches minimal information about the switch like the supported capabilities.
        - The validation tests connectivity to the device using the provided information. If an error indicator appears, correct the information and click **Test** to try again.
        - The **Status** column represents the discovery results. You can click the status icon to view the discovery results.
     i. To trigger polling, click **Save**. Polling is the periodic collection of the metrics and properties from the switch based on the supported capabilities that are discovered.

NOTE: For brocade switches discovered using FOS, each switch must be discovered separately one at a time in the Discovery Center.

Capabilities

When a switch is successfully discovered in Discovery Center, using SNMP discovery mode, the Collected Devices tab displays the Capabilities that are collected from the switch in abbreviations, as shown in the Capabilities Abbreviation table.

The number of capabilities that are discovered depends on the switch model and SNMP MIBs that are enabled. Manually adding capabilities that have not been discovered by the SolutionPack results in errors in the log files. Deleting discovered capabilities could result in blank reports.

Table 5. Capabilities Abbreviation

Abbreviation	Capability	Data collection method
SW	BROCADE_FCSWITCH_SYSTEM	Topology
SW-P	BROCADE_FCSWITCH_PORT	Performance
AG	BROCADE_ACCESSGATEWAY_SYSTEM	Topology
AG-P	BROCADE_ACCESSGATEWAY_PORT	Performance
P-STAT	BROCADE_FCSWITCH_PORT_STATUS	Performance
GIF	GENERIC-INTERFACES	Performance
NOIFX	GENERIC-INTERFACES-NO-IFXTABLE	Performance
SUTIME	GENERIC-SYSUPTIME	Performance

Passive host discovery configuration options

Enable passive host discovery to see end-to-end topology from hosts to arrays, and identify chargeback on SAN enabled hosts without active host discovery.

About this task

You can passively resolve hosts that are discovered through the SolutionPack for Brocade FC Switch from zoning records.

The default zone naming patterns in Dell SRM are:

z_%h%

z_%h%_*

z_%h%_*_*

%h%_*

After you enable passive host discovery, the following options for passive host configuration are available:

- Enable DNS Resolution: This option, which is enabled by default, resolves the "IP" property by using the DNS lookup handler. You can clear this option to avoid using the DNS lookup feature.
  - Exclude Passive hosts on DNS resolution failure: Enable this option to stop passive host data from being collected if the DNS resolution for the host fails.
- Exclude Passive Hosts that are actively discovered: Enable this option to stop passive host data from being collected if that host has been actively discovered.
- Customize zone naming patterns: This option allows you to customize the zone naming pattern. By default, this option is disabled, and Dell SRM uses the four default zone naming patterns. You can enable this option to add, delete, or modify the default zone naming patterns and hostname positions in zones.

You can enable passive host discovery while installing the SolutionPack, or you can enable it by reconfiguring the Brocade Data Collection component of an existing instance of the SolutionPack.

To enable and add/edit customized zone naming patterns:

Steps

1. Select the **Enable Passive Host Discovery** checkbox.
2. Select the **Customize zone naming patterns** checkbox.
   The system displays the four default zone naming templates.
3. To view the zone naming pattern and host position for a template, click the Add button (plus icon). Edit the pattern or position if wanted.

   Only Java-based zone naming patterns are supported.

Only plain numbers can be used for the position. Special characters (like $) are not required.

Regex is ^(z_)([A-Z0-9a-z]+)$ and hostname position is 2	Matches all the zone names that start with 'z_' and extracts the hostname from the rest of the string that follows 'z_' Example: For zone name z_lingz099, the hostname that is extracted is lingz099.
Regex is ^([^z_][A-Z0-9a-z]+)_([A-Za-z0-9]+) and hostname position is 1	Matches all the zone names that do not start with 'z_' and extracts the hostname from zone name that is before the first underscore. Example: For lgloe111_1106, the hostname that is extracted is lgloe111.

NOTE:

- All of the Capacity and Availability metrics that are related to passive hosts will go inactive after upgrading from a release before 4.1 to the latest release.
- Passive Host Discovery considers only the Physical Port WWNs with Format 1, Format 2, and Format 5 according to Network Address Authority (NAA) naming format.
- For an overview of physical host discovery mechanisms, see Physical host discovery.
- Starting from 4.2 release, Passive host discovery supports discovery of mapped WWNS (WWNs starting with C/D/E/F are referred to as Mapped WWNs).
- Passive host details will not be derived from peer zones.

For more information about writing Java's regular expression, see Regular expressions.

Passive host discovery from Brocade Peer Zoning configurations

About this task

In Brocade's Peer Zoning, the Principal Member is a device that manages a peer zone. It is allowed to communicate with the rest of the devices in the zone. Other non-principal devices in the zone can communicate with the principal device only; they cannot communicate with each other.

This feature allows users to discover hosts passively from the Peer Zoning configuration which is configured in Brocade FC Switch.

To create a Peer Zone configuration in Brocade switch, perform the following steps:

Steps

1. Connect to the switch as administrator.
2. To discover passive hosts from Brocade Peer Zoning configurations, set up alias names for all zone members.
   Use `alicreate` command to create new alias names for zone members. For example:

```
switch:admin> alicreate "peer_host",  "10:00:00:10:9B:D8:99:5E"    (Host WWN)
switch:admin> alicreate "peer_dev1",  "20:03:D0:39:EA:48:AE:9E"    (Array WWN)
switch:admin> alicreate "peer_dev2",  "10:00:00:10:9B:F6:58:85"    (Array WWN)
```

   NOTE: The alias names of the members should match the patterns that are available and enabled in **SRM Admin UI** > **Config** > **SolutionPacks** > **Installed SolutionPacks** > **Brocade FC Switch** > **Brocade Data Collection** > **Reconfigure** > **Alias Name Configuration**.
3. Create a Peer Zone configuration, using `zonecreate` command.
   You can choose the host as principal member and the storage devices as peer members. For example:

The Peer Zone is called `SRM_PEERZONE_Netapp_C1_02_H_R660_213`, which contains `peer_host` as the principal device and `peer_dev1` and `peer_dev2` as the non-principal devices.

```
switch:admin> zonecreate --peerzone "SRM_PEERZONE_Netapp_C1_02_H_R660_213" -principal
"peer_host" -members "peer_dev1; peer_dev2
```

4. Creating configuration, adding Peer Zone to configuration and enabling configuration:
   a. Create the configuration using `cfgcreate` command:

   ```
   switch:admin> cfgcreate "peer_zoneset", "SRM_PEERZONE_Netapp_C1_02_H_R660_213"
   ```

   b. To save the configuration, run the command:

   ```
   switch:admin> cfgsave
   ```

   c. Enable the configuration using `cfenable` command:

   ```
   switch:admin> cfgenable "peer_zoneset"
   ```

5. Using `zoneshow` command, verify that the configuration is enabled.
   For example:

```
switch:admin> zoneshow --peerzone all
```

Configuring Peer Zoning in SolutionPack for Brocade FC

You can enable the Peer Zoning feature while installing the SolutionPack, or you can enable it by reconfiguring the Brocade Data Collection component of an existing instance of the SolutionPack.

Steps

1. Select the **Enable Passive Host Discovery** checkbox.
2. Select the **Customize vendor OUIs** checkbox and add the relevant OUIs.
3. Select the **Customize alias naming patterns** checkbox.
   The system displays the two default alias naming templates.
4. To view the alias naming pattern and host position for a template, click the Add button (plus icon). If necessary, edit the pattern or position.

Regex is ^([A-Z0-9a-z-])([A-Za-z0-9])([A-Za-z0-9]+)$ and hostname position is 2	Matches all the alias names and extracts the hostname from the alias name. For example: For the alias name `peer_lingz099_host`, the hostname that is extracted is `lingz099`.
Regex is ^([A-Z0-9a-z-])_([A-Za-z0-9])$ hostname position is 1	For example: For alias name `lingz099_host`, the hostname that is extracted is `lingz099`.

NOTE:

a. For regex patterns for Passive Host discovery, see Sample zone naming patterns.

b. Currently this feature is supported with Alias zone naming patterns. The reports will appear with the existing Passive Hosts reports.

c. Use this online regex tool for verifying your patterns: Regex 101.

Brocade Virtual Fabrics discovery configuration options

Dell SRM can use SNMP or REST to pull in Virtual Fabric information.

SNMP

For SNMP to configure a Brocade switch with Virtual Fabric capabilities, additional configuration steps are required for the SRM suite to successfully discover Brocade switches with Virtual Fabric capabilities. This task provides command examples to guide you through the process.

Prerequisites

To retrieve information for a Virtual Fabric that is not the default logical switch (in other words, FID 128), the following must exist:

- An SNMP V3 user must exist with a valid SNMP V3 configuration.
- A user account must exist with access to the Virtual Fabric. This account must have a home Virtual Fabric and access to a list of Virtual Fabric IDs. This name must match the SNMP V3 username.
- An IP address is configured for each logical switch. It is not necessary to create separate SNMP V3 users to discover each logical switch.

Steps

1. To check the logical switches configured on a physical switch, type:

   ```
   switch xxxx:FID128:admin> lscfg --show
   ```

2. To list the SNMP V3 users configured on a switch, type:

   ```
   snmpconfig --show snmpv3.
   ```

   A user must exist with the same name as an SNMP V3 user. Create a user if none exists.

3. If a user does not exist, create one by typing:

   ```
   switch xxxx:FID128:admin>userconfig -- add <snmpadmin2> -r switchadmin -l 2-8,128 -h
   2 -c switchadmin
   ```

4. To view the users configured on a switch, type:

   ```
   switch xxxx:FID128:admin>userconfig --show -a
   ```

5. To only view the user `snmpadmin2`, type:

   ```
   switch x:FID128:admin> userconfig --show snmpadmin2
   ```

6. To set the IP address on each logical switch, type:

   ```
   ipaddrset -ls <FID> --add <IPv4_address/prefix>
   ```

7. To view the IP addresses configured on a switch, type:

   ```
   ipaddrshow
   ```

8. Use an SNMP V3 profile to discover logical switches in the SRM suite. While discovering logical switches, provide the SNMP V3 context, which is the VF ID. This should be entered in Dell SRM using the format `VF:XXX`, where `xxx` is the FID of the fabric that you want to discover.

As shown in the previous command examples, the SNMP V3 user is named `snmpadmin2`, and the contexts should be used to discover logical switches. If you do not specify an SNMP V3 context, then data that is returned using SNMP is for that user's corresponding home virtual fabric.

REST

If the Brocade Rest switch is configured with virtual fabric capabilities, it discovers all virtual fabrics by default.

Limitations

SMIS severe exceptions are seen in collecting logs while discovering an SMIS provider where there are no director class switches, FCOE switches, or AG switches added to it.

Example:

```
SEVERE – [2014-10-28 06:29:56 EDT] – n::run(): An error occurred while fetching data.
Data from collecting configuration Brocade_Ethernet_Port will not be collected in this
cycle.
```

```
SEVERE – [2014-04-22 10:17:05 GMT] – n::run(): An error occurred while fetching data.
Data from collecting configuration Brocade_ModulePort will not be collected in this
cycle.
```

```
SEVERE - [2016-09-07 13:14:43 BST] -- n::run(): An error occurred while fetching data.
Data from collecting configuration Brocade_AGSoftwareIdentity will not be collected in
this cycle.
```

5

SolutionPack for Cisco MDS/Nexus

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Cisco MDS/Nexus accesses performance data that was automatically collected and interpreted (using resource grouping and mathematical calculations) across multiple MDS/Nexus fabrics. Alerts are consolidated from Cisco MDS/Nexus Switches and shown on the **All Alerts Console**.

Data collection methods

The SolutionPack for Cisco MDS/Nexus uses SNMP to access performance data information that was automatically collected and interpreted (using resource grouping and mathematical calculations) from across multiple fabrics.

There are two methods for discovering Cisco MDS/Nexus devices:

- Device discovery UI using the Generic-SNMP Collector – With this approach you can perform the device discovery using the device discovery UI and the Generic-SNMP Collector. If you prefer this method, you do not need to install the Cisco SNMP data collection block.
- Discovery Center UI using the dedicated Cisco SNMP Collector – With this approach you must install the Cisco SNMP data collection block that is introduced in ViPR SRM 4.0. After installing this data collection block, you can use the Discovery Center UI to discover Cisco MDS/Nexus switches.

NOTE: Switches should not be discovered simultaneously from SNMP Device Discovery and Discovery Center.

NOTE: For an overview of physical host discovery mechanisms, see Physical host discovery.

Performing pre-configuration tasks

Before you discover a Cisco switch in Dell SRM perform the following checks.

About this task

All switches in the Cisco fabric must have SNMP credentials for use with Dell SRM. For example, if SNMPv1/v2c is used, all Cisco switches in the fabric should have the SNMPv1/v2c community name set with a role of network-admin or network-operator. For example, if SNMPv3 is used, all Cisco switches in the fabric should have the SNMPv3 user set with the role of network-admin or network-operator.

Steps

1. Ensure that all hardware and software is listed as supported in the *Dell SRM Support Matrix*.
2. Verify the TCP/IP connectivity to the switches to be discovered. Test by issuing a `ping` command to these switches.
3. Determine if SNMP traps are enabled. Log in to the switch and run the command `show snmp trap`.
4. Run the command `snmp-server enable traps` to enable SNMP traps.
   ```
   SWDevCisco8-9216i# config terminal
   ```
   Type configuration commands, one per line. End with `CNTL/Z`.
   ```
   SWDevCisco8-9216i (config)# snmp-server enable traps
   ```
5. Display the traps that are enabled. Run the show `snmp trap` command. The values in the `Enabled` column should be `Yes`.

Known issue with user-defined roles

About this task

If an SNMPv3 user or SNMPv1/v2c community string that is used for switch discovery is assigned to a role that has vSAN policy set to **deny**, there is a possibility of switch restart and supervisor fail-over.

This condition is due to an issue in Cisco NX-OS 5.2(6) through 6.2(x).

The workaround is to run the following commands in sequence:

```
linbge197#config t
linbge197#role name <name of the role>
linbge197#no vsan policy deny
linbge197#copy run start
linbge197#exit
```

Configuring switches for SNMPv1 and SNMPv2c

Configure Cisco switches for SNMPv1 or SNMPv2c to enable switch discovery, and alert consolidation for the switches. The SNMPv1 or SNMPv2c information you provide when performing discovery is necessary for Dell SRM to contact the switch to obtain information.

Prerequisites

If SNMPv1/v2c is used, all Cisco switches in the fabric should have the SNMPv1/v2c community name set with a role of network-admin/network-operator.

About this task

Dell SRM collects data from the switch using the SNMP community name. It uses the SNMP port for communication. The default port set is port 161.

NOTE: The Cisco documentation provides information on configuring Cisco switches for SNMPv1 and SNMPv2c management.

Steps

1. Log in to the switch as an administrator.
2. To configure the `snmp-server community`string with read-only privileges, run the following commands:
   ```
   Cisco8-9216i# config terminal
   ```
   ```
   Cisco8-9216i(config)# snmp-server community srmuser ro
   ```
   Type configuration commands, one per line.
3. To verify if the SNMPv1 community string exists, run the command `show snmp community`.
   A sample output of the command:

Community	Group/Access
srmuser	network-operator

Configuring switches for SNMPv3

Configure Cisco switches for SNMPv3 to enable discovery and alert consolidation for the switches. The SNMPv3 information that you provide when performing discovery is necessary for Dell SRM to contact the switch to obtain information.

About this task

Dell SRM collects data from the switch using SNMPv3 secure credentials. Dell SRM supports SNMPv3 with all the combinations of Auth (MD5, SHA) and Priv (AES, DES, NONE).

NOTE: Create the SNMPv3 users with authentication and privacy passwords on all physical switches in the fabric. The Cisco documentation provides information on creating SNMPv3 users on Cisco switches.

This procedure provides an example of creating an SNMPv3 user called srmuser with a network-operator role, SHA authorization, and AES128 authentication.

Steps

1. Log in to the switch as an administrator.

   ```
   Cisco8-9216i# config terminal
   ```

   Type configuration commands, one per line.

2. Run the `snmp-server user` commands as follows:

   ```
   snmp-server user srmuser network-operator auth sha <SHA-password> priv aes-128 <AES-password>
   ```

3. To verify the new user creation, run the command `show snmp user`.

Table 6. Sample output of show snmp user command

User	Auth	Priv(enforce)	Groups
SNMP USERS			
admin	md5	no	network-admin
srmuser	sha	aes-128(no)	network-operator
NOTIFICATION TARGET USERS (configured for sending V3 Inform)			
User	Auth	Priv	-
SWDevCisco8-9216i#	-	-	-

Configuring Cisco switches for alert consolidation

Use the `snmp-server` command to forward SNMP v1 alert traps from Cisco FC switches to Dell SRM.

Steps

1. Log in to the Cisco FC switch as the administrator.
2. To enter the global configuration mode, type **`# config`** at the terminal prompt and press **Enter**. For more information about global configuration mode, go to Cisco Support Site.
3. Type **`snmp-server host <trap recipient IP> traps <SNMP trap version> <Community String> udp-port <trap listening port >`**, and press **Enter**.

   In the command syntax:

Syntax element	Input
<trap recipient IP>	In a single vApp installation, this element is the Dell SRM IP, and in a distributed environment, is the Backend server's IP.
<SNMP trap version>	**`version 1`**
<Community String>	**`public`**
<trap listening port >	**`2041`**, which is the Dell SRM trap listening port.

Example: **`snmp-server host 10.247.24.190 traps version 1 public udp-port 2041`**

4. If you have multiple Cisco FC switches in the storage environment, repeat this procedure on each switch.

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The Dell SRM Alerting Guide explains how to configure alerts consolidation.

About this task

Beginning with ViPR SRM 4.0, the SolutionPack for Cisco MDS/Nexus includes a dedicated SNMP Data Collection Manager that allows you to discover Cisco MDS/Nexus switches via Discovery Center through this SNMP Data Collection block. The advantage of using Discovery Center is that you can discover all of the switches in a fabric by entering the IP address of just one switch in the fabric. In addition, topology and performance polling interval configurations only apply to devices discovered using Discovery Center. However, you can skip installing this block if you prefer to discover Cisco MDS/Nexus switches through SNMP Device Discovery and the Generic-SNMP collector. This option has been provided for backward compatibility.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.
   If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.
9. Click **Next**. The window displays SNMP data collection details.

   Beginning with ViPR SRM 4.0, the SolutionPack for Cisco MDS/Nexus includes a dedicated SNMP Data Collector that allows you to discover Cisco MDS/Nexus switches via Discovery Center through this SNMP Data Collection block. However, you can skip installing this block if you prefer to discover Cisco MDS/Nexus switches through SNMP Device Discovery and the Generic-SNMP collector. This option has been provided for backward compatibility.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use **`localhost`** on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.

12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

13. Specify the SNMP Collector name, SNMP Collector port, and the communication interface IP address. The default collector name is Watch4NetSnmpCollector-MDS and the default port is 2007.

14. From the **Passive Host Discovery Options** drop-down list, select existing settings that have been specified for other components, or add a new configuration. If desired, select **Enable Passive Host Discovery**.

    See Passive host discovery configuration options for additional details.

    If you opted not to install the Cisco SNMP data collection block, see Enabling passive host discovery through Generic-SNMP.

15. Select **Configure advanced settings** to configure polling period and polling group settings.

    The advanced settings are applicable only for the dedicated SNMP Data Collector and are not applicable for the Generic-SNMP collector. Use caution when configuring these settings. Improper settings will impact SNMP Collector performance.

    Performance data Polling period defines the frequency with which the dedicated SNMP Collector polls the performance related data from the switch.

    Topology Polling period defines the frequency with which the dedicated SNMP Collector polls the topology related data from the switch.

    All of the capabilities that are supported by the switch will be polled. For more information about capabilities, refer to Capabilities.

    Polling Group configuration consists of a group of switches and some of the capabilities supported by those switches. You can optimize the resources consumed by the dedicated SNMP Collector by tuning these settings.

    Property refresh time is the time at which the properties will be refreshed for a polling group. The property refresh time format is HH:MM:SS, where HH is hours, MM is minutes, and SS is seconds.

    Start Polling Group at Defined period when enabled, will start the polling at the next "round" period. Raw value timestamps will be accurate. For example, if the polling period is set to 5 minutes, this would mean that the polling cycles will start at 00:00, 00:05, 00:10, and so on.

    Polling Group Start Time offset (s) is used to start different polling groups at different times to avoid putting an excessive load on the dedicated SNMP Collector. The polling for the polling groups will start one after the other with a delay specified by this time offset. When setting a polling group start time offset, consider the shortest polling period (performance or topology), the time it takes for the SNMP Collector to poll the switch for the capabilities in the polling group, and the number of polling groups. If the polling group start time is too short, the load on the SNMP Collector will increase. If the polling group start time is too long, the polling groups might not be finished polling within the polling interval and the next polling period might start.

16. Click **Next**.
    The window displays reports settings.

17. In **Administration Web-Service Instance**, select an existing instance or create a custom instance.

18. Click **Next**.
    The window displays a note about SNMP masks.

19. Click **Install**.

20. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

The SolutionPack for Cisco MDS/Nexus dedicated SNMP Data Collection Manager must be installed. For more information about installing the SNMP Data Collection Manager, see Installing the SolutionPack for Cisco MDS/Nexus installation section.

About this task

The following procedure describes how to add switches individually using Discovery Center. To add multiple switches at a time, use a discovery group. The advantage of using a discovery group is that you can discover all of the switches in a fabric by

entering the IP address of just one switch per fabric to be discovered. If the switches share credentials, the credentials only need to be entered once as well. For more information about creating discovery groups, refer to Add devices using discovery.

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Select **Cisco MDS/Nexus** and click **Add**.
3. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure Vault checkbox is selected. When Secure Vault checkbox is not selected, Community String/ User Name is active.

4. Specify the details of the Cisco MDS/Nexus configuration. Do not enter spaces.
   a. In the Device location section, select the server and instance where you want to store the configuration details for this device.
   b. In the **Switch IP address field** field, type the IP address of the device that is supporting the SNMP agent.
   c. In **SNMP Port** field, type the device SNMP agent listening port.
   d. In the **SNMP Version** and field, type the device SNMP agent version. If you select v3, select the authentication and encryption protocols, and specify the passwords.
   e. In the **Community String/User Name**field, specify the community name if the SNMP version is v1 or v2c. Specify the username if the SNMP version is v3.
   f. If secure vault is enabled, in **Unique Key** enter the unique key.
5. To trigger discovery, click **Validate and Add**.
   Discovery fetches minimal information about the switch like the supported capabilities.
   The validation tests connectivity to the device using the provided information. If an error indicator appears, correct the information and click **Test** to try again.
   The **Status** column represents the discovery results. To view the discovery results, click the status icon.
6. To trigger polling, click **Save**.
   Polling is the periodic collection of the metrics and properties from the switch based on the supported capabilities that are discovered.

Capabilities

When a switch is successfully discovered in Discovery Center, the **Collected Devices** tab displays the **Capabilities** that are being collected from the switch in abbreviations. The number of capabilities that are discovered depends on the switch model and SNMP MIBs that are enabled. Manually adding capabilities that have not been discovered results in errors in the log files. Deleting discovered capabilities could result in blank reports.

Table 7. Capabilities

Abbreviation	Capability	Data collection method
ZN	CISCO-ACTIVE-ZONE	-
ZSET	CISCO-ACTIVE-ZONESET	-
PHOST	CISCO-ACTIVE-ZONE-PASSIVE-HOST	-
DALIAS	CISCO-DEVICE-ALIAS	-
FRU	CISCO-ENTITY-FRU	Performance
SNSR	CISCO-ENTITY-SENSOR	Performance
FCFE	CISCO-FCFE	Performance
FCFENPV	CISCO-FCFE-NPV	Performance
FCS	CISCO-FCS	Topology

Table 7. Capabilities (continued)

Abbreviation	Capability	Data collection method
FCSVSAN	CISCO-FCS-VSAN	Performance
FCTL	CISCO-FEATURE-CONTROL	Topology
FLASH	CISCO-FLASH	Performance
NPORT	CISCO-MDS-NEXUS-PORTS	Performance
NPSTAT	CISCO-MDS-NEXUS-PORTS-STATUS	Performance
NPROC	CISCO-MDS-NEXUS-PROCESS	Performance
NVSAN	CISCO-MDS-NEXUS-VSAN	Performance
NS	CISCO-MDS-NS-DM	Topology
VS-ZSET	CISCO-VSAN-ACTIVE-ZONESET	-
GIF	GENERIC-INTERFACES	Performance
NOIFX	GENERIC-INTERFACES-NO-IFXTABLE	Performance
SUTIME	GENERIC-SYSUPTIME	Performance
PPOST	CISCO-PROCESS-POST	Performance
PENTITY	CISCO-PHYSICAL-ENTITY	Topology
PCNLMEM	CISCO-PORT-CHANNEL-MEMBERS	Topology

Passive host discovery configuration options

Enable passive host discovery to see end-to-end topology from hosts to arrays, and identify chargeback on SAN enabled hosts without active host discovery.

About this task

You can passively resolve hosts that are discovered through the SolutionPack for Cisco MDS/Nexus from zoning records.

The default zone naming patterns in Dell SRM are:

z_%h%

z_%h%_*

z_%h%_*_*

%h%_*

After you enable passive host discovery, the following options for passive host configuration are available:

- Enable DNS Resolution: This option, which is enabled by default, resolves the "IP" property by using the DNS lookup handler. You can clear this option to avoid using the DNS lookup feature.
  - Exclude Passive hosts on DNS resolution failure: Enable this option to stop passive host data from being collected if the DNS resolution for the host fails.
- Exclude Passive Hosts that are actively discovered: Enable this option to stop passive host data from being collected if that host has been actively discovered.
- Customize zone naming patterns: This option allows you to customize the zone naming pattern. By default, this option is disabled, and Dell SRM uses the four default zone naming patterns. You can enable this option to add, delete, or modify the default zone naming patterns and hostname positions in zones.
- Customize vendor OUIs: This option allows you to customize the vendor OUIs. By default, this option is disabled and Dell SRM uses the following vendor OUIs by default: 0000C9, 000A38, 000E03, 00109B, 0090FA, 00C0DD, 00E08B, 001B32, 00E0D5, 001405, 0024FF, 001438, 0060B0, 8C7CFF. If required, you can enable this option to add additional vendor OUIs.

You can enable passive host discovery while installing the SolutionPack, or you can enable it by reconfiguring the SNMP Data Collection component of an existing instance of the SolutionPack.

To enable and add/edit customized zone naming patterns:

Steps

1. Select the **Enable Passive Host Discovery** checkbox.
2. Select the **Customized zone naming patterns** checkbox.
   The system displays the four default zone naming templates.
3. To view the zone naming pattern and host position for a template, click the Add button (plus icon). Edit the pattern or position if wanted.

   Only Java-based zone naming patterns are supported.

   Only plain numbers can be used for the position. Special characters (like $) are not required.

Regex is ^(z_)([A-Z0-9a-z]+)$ and hostname position is 2	Matches all the zone names that start with 'z_' and extracts the hostname from the rest of the string that follows 'z_' Example: For zone name z_lingz099, the hostname that extracted is lingz099.
Regex is ^([^z_][A-Z0-9a-z]+)_([A-Za-z0-9]+) and hostname position is 1	Matches all the zone names that do not start with 'z_' and extracts the hostname from zone name that is before the first underscore. Example: For lgloe111_1106, the hostname that extracted is lgloe111.

NOTE:

- All of the Capacity and Availability metrics that are related to passive hosts will go inactive after upgrading to the 4.1 release.
- Passive Host Discovery considers only the Physical Port WWNs with Format 1, Format 2, and Format 5 according to Network Address Authority (NAA) naming format.

For more information about writing Java's regular expression, see Regular Expressions.

Enabling passive host discovery through Generic-SNMP

If you opted not to install the Cisco SNMP data collection block, enable passive host discovery through the Generic-SNMP collector.

Steps

1. Edit the Generic-SNMP independent SolutionPack block instance.
2. Select the **Enable Passive Host Discovery** checkbox.
3. Click **Reconfigure**.

Limitations

- Maintenance operations that cause a large number of changes in the SAN environment, such as zoning changes and migrations, might degrade APG database performance. These operations generate new active metrics to represent the new SAN environment, and previous metrics become inactive. If active plus inactive metrics exceed 1.5 million entries, slower performance of the database is expected. If needed, you can clean the database to remove inactive metrics, or split the database if active metrics are greater than 1.5 million entries.
- The Dell SRM SNMP Collector causes the switch to restart and the supervisor to fail. The issue is due to a code bug in Cisco NX-OS from 5.2(6) through 6.2(x) and MDS configurations with Roles and vSAN policies. If SNMP V2c or V3 credentials that are used for switch discovery are assigned to a role which has vSAN policy denied, then the issue occurs. To check the vSAN policy for each role, run the following command:
  - `show role brief`

    - Workaround is implemented by using the following commands on the problematic roles and switches:
    - `config t`
    - `role name <name of the role>`
    - `no vsan policy deny`
    - `copy run start`
    - `exit`
- When triggering discovery for a discovery group, the status icon is not displayed.

6

SolutionPack for Cisco UCS

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Cisco UCS generates reports that encompass compute, network, and storage access components of the unified fabric.

The SolutionPack generates uptime reports for the UCS Managers and enables you to see into the solution as managed by the unified management domain. In addition, the SolutionPack for Cisco UCS obtains real-time and historical data through various reports that indicate events and faults in the system.

Data collection methods

UCS XML API

Main reports

Power Consumption over Time

Fabric Interconnects

Chassis

System Statistics, Fans, PSU, Interfaces

Events

Configuring the UCS Manager

Enable XML API for the Cisco UCS Manager.

Prerequisites

Steps

1. Log in to the Cisco UCS Manager web console.
2. Browse to **Admin** > **Communication Management** > **Communication Services**.
3. Verify that the HTTP and CIM XML services are enabled.
   If the **Redirect HTTP to HTTPS** option is enabled, use secure communication when configuring the SolutionPack block.
4. If you want to use secure communications between the collector and the UCS Manager:
   - Choose the secure communication option when adding the UCS Manager.
   - Configure HTTPS on the **Communication Services** page of UCS Manager.

Next steps

Dell Technologies recommends that you create a new dedicated service account for SolutionPack integration. Role-read-only role is sufficient for the SolutionPack to work correctly.

Installing the SolutionPack

Prerequisites

Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
11. From the **Topology Service** drop-down menu, select exiting settings that have been specified for other components, or select **Add a new data collection**. If you select **Add a new Topology Service**, type information about the Topology Service. In **Topology Service Hostname or IP address**, specify the Primary Backend host and select the appropriate **Gateway for Web-Service Gateway** dropdown.
12. Select the **Enable events collection** checkbox.
13. In the **Event server hostname or IP address** field, select the Backend host where the events server runs. The default port is 52007.
14. In the **Even server port number** field, enter a port number for events collection.
15. To configure polling settings, select **Configure advanced settings**.
16. Click **Next**.
    The window displays event settings.
17. Select an **Event database**. If you select **Add a new Events** database, type information for the new events database. Type the database information for the events database that runs on the Primary Backend host. The default **Database port** is 53306. The default **Event server port number** is 52007.
18. Click **Next**.
    The window displays reports settings.
19. In **Administration Web-Service Instance**, select an existing instance which is default.
20. Click **Install**.
21. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Discovery through Discovery center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Cisco UCS**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

5. Specify the details of the Cisco UCS configuration.
   a. In the Device location section, select the server and instance where you want to store the configuration details for this device.
   b. In the **UCS type** field, select UCS Manager (Blade Chassis) or UCS C-Series (Server).
   c. In **Hostname or IP address** type the UCS management host.
   d. In the **Username** and **Password/unique key** fields, type the credentials for the management server.
   e. Select **Enable secure connection**, if desired.
   f. In the **Communication port** field, type the port number for the management server.
6. To validate the credentials, click **Validate and Add**.
7. Click **OK**.
8. Click **Save**.

Next steps

If you want to discover the Cisco UCS Fabric Interconnects in your environment via SNMP, you must install the Cisco MDS / Nexus SolutionPack in your environment to provide full SNMP masks and capabilities for the SNMP discovery.

Cisco UCS events are commented out by default in frontend configuration files. To enable Cisco UCS events, uncomment Cisco UCS events in the following configuration files: APG.xml, APG-WS.xml, and report-generation-config.xml.

Importing the new database schema

About this task

Starting with core software Dell EMC M&R 6.2u4, schema is preloaded. If you installed from an earlier version, import the new database schema.

Steps

1. Load the events block file `Event-Processing/Generic-Live-Writer/cisco-ucs/ddl/my-ucs_live.sql`.
2. Run `mysql-client.sh` (`mysql-client.cmd` on Windows).
3. Type username, database name, and password.
4. Copy the contents of the `/my-ucs_live.sql` file and paste it into the mysql client at the `mysql>` prompt.

   The `ucs_live` table is created.
5. Start the event processing manager service.
6. To enable events reporting from the frontend:
   a. Edit the Web-Application configuration file `Web-Servers/Tomcat/Default/conf/Catalina/localhost/APG.xml`.
   b. If the `cisco-ucs-events` section is present, uncomment it with the below commented line under it. Perform the steps below.

```
<!-- ./bin/manage-resources.sh update dba/FLOW-UCS-LIVE '{"disabled":false}' -->
```

a. Log in to the frontend VM
b. Go to <APG_Install_DIR>/bin and execute ./manage-resources.sh list
c. If FLOW-UCS-LIVE is present then check the following
d. Go to <APG_Install_DIR>/bin and execute `./manage-resources.sh` get dba/FLOW-UCS-LIVE and check the status of the resource link
e. If "disabled": true, then execute `./manage-resources.sh` update dba/FLOW-UCS-LIVE '{"disabled":false}'

7. Restart the tomcat service.

Limitations

- The following message appears in the logs when the SolutionPack for Cisco UCS collector-manager is first started. This problem is resolved when a device is added for discovery and the collector-manager is restarted.

```
WARNING - [2016-04-10 11:26:24 EDT] - SocketConnector::init(): Can't connect socket
to localhost:52007
 java.net.ConnectException: Connection refused
```

- Events reports in the SolutionPack for Cisco UCS are specific to UCS Manager only.

7

SolutionPack for Configuration Compliance

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Configuration Compliance allows user to manage Configuration Compliance Policies, ESM Matching, Compliance Rule Definitions, and perform Configuration Planning. It also generates breach, track configuration changes, policy report, and Compliance Configuration Planning report. This enables the identification of any deviation from configuration best practices, including items that do not comply with the *Dell SRM Release Notes*. The compliance reports can be found under **Operations** > **Configuration Compliance**. Click **Administration** > **CONFIG** > **Configuration Compliance** to launch **Policy & Rules Management**, **Match to Support Matrix**, **Rule Definitions**, and **Configuration Planning** pages.

Where to find the latest SolutionPack software

Install the latest core software update for the product suite. SolutionPacks distributed with core software have a 30-day free evaluation period. If you plan to use the software longer than 30 days, you must install a SolutionPack license before the trial period ends.

This 30-day free evaluation only applies to new installations and is not available for upgraded installations. If you upgrade the core software and want to try a new SolutionPack, you must request for a license. For the license, submit a Support Request (SR) form, which is available on the Dell Support Site.

Installing the SolutionPack

Prerequisites

- Dell M&R uses SSH and a user account.
- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- If you are installing on a Windows host, stop the process `jucheck.exe`. This is a Java JRE update validator and uses the same port as the SolutionPack.
- Do not install multiple instances of the Configuration Compliance Backend because the same port would be used for each installation. This will lead to service startup failure.
- Alerting backend service should be available during installation; otherwise alerting definition will not be created. The SolutionPack for Configuration Compliance creates alerting definition for notifying mentioned users with email alerts for breaches/violations.
- Though the Compliance service comes up immediately, do not run ESM rules as the SolutionPack installation also populates the database with ESM data, for ESM rule validation, which takes some time to get the database populated (approximately 3-5 minutes).

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.

3. Click **Install**.
4. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
5. Click **Next**.
   The window displays compliance notification details.
6. Select an item in **Breach Notification Details**. If you select **Add a new Breach Notification Details**, select an instance to receive breach notifications.
7. Click **Next**.
8. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components or select **Add a new Frontend Web service**.

   If you select **Add a new Frontend Web service**, type information about the Frontend Web service.

   The **Tomcat port** should be 58443.

   The **Tomcat communication protocol** should be HTTPS.
9. Select a **Topology Service**. To add a new gateway configuration, select **Add a new Topology Service**.
10. Select a configuration for **Breach Notification Details**.

    Reuse the answers if another SolutionPack is using Alerting backend. Otherwise create a new configuration by selecting **Add a new Breach Notification Details**. In the **Alerting Backend hostname or IP address**, type the Primary Backend host. Type 2010 as the port.
11. Select a configuration for **Alert Consolidation Details**.

    Reuse the answers if another SolutionPack is using **Alert Consolidation Details**. Otherwise create a new configuration by selecting **Add a new Alert Consolidation Details**. In the **Alert Consolidation hostname** field, type the Primary Backend host. Type 2040 as the port.

    If SOM RCA installation needs to be done, the alert consolidation configuration is required. For more details, refer to the "How to" article for SOM.
12. Click **Next**.
13. On the **Compliance Rules** page, click **Next**.
14. From **Administration Web-Service Instance**, select Default.
15. In **Configuration for Compliance Backend Web-Service**, for 4 VM installations, type the Primary Backend host for Web-Service gateway hostname or IP address of Web-Service Gateway.
    a. The **Web-Service port number** should be 48443.
    b. The **Authentication schema** should be Certificate.
    c. The **Compliance Backend Instance** should be generic-compliance.
16. Click **Next**.
17. Click **Install**.
18. After Install of all the compliance components, click **Ok**.
    After installation is complete, you need to restart the Tomcat for Compliance Frontend to point to the configured Backend. If the Web Service password is changed, then the Compliance Backend block needs to be reconfigured.

8

SolutionPack for Dell SC Series

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell SC Series collects storage capacity, performance, and topology data from the Dell Storage SC series arrays and displays data in easy-to-use reports in Dell SRM.

Installing the SolutionPack

Prerequisites

- Dell Storage Center Operating System 7.1.x or later must be running. If previous versions to Dell SCOS 7.1.x are discovered, you might not see expected data as these versions are not supported.
- Dell Storage Manager Data Collector 2016 R2 or later must be installed and managing the Storage Centers that you intend to discover in Dell SRM.
- The Dell SC collector with the default heap size can manage one DSM Data Collector host across 10 Storage Centers up to 2000 volumes. If the number of volumes across the Storage Centers exceed 2000, the recommendation is to split the Storage Centers across two DSM Data Collector hosts.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

11. To configure the **Topology Polling Period**, **Performance Polling Period**, and **Volume Performance Polling Period** settings, select **Use advanced settings**.

    The default setting for the **Volume Performance Polling Period** is 15 minutes. If you have more than 1,000 volumes per DSM Data Collector host, Dell Technologies recommends that you set the polling period to 60 minutes. Performance data will be displayed after the completion of the polling period.
12. Click **Next**.
    The window displays reports settings.
13. Click **Install**.
14. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices in Discovery Center

To discover Dell SC series arrays that Dell Storage Manager Data Collector manages, follow the procedure.

Steps

1. Go to **Discovery** > **Discovery Center** > **Manage Discovery**.
2. Select **Dell SC Series** and click **Add**.
3. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Dell Storage Manager Data Collector Password is active.
4. Type the **Hostname or IP address** of the Dell Storage Manager Data Collector.
5. Type the **Host Port**.

   The default is 3033, which can be changed.
6. Type in the **Username** and **Password** of the Dell Storage Manager Data Collector.
7. If secure vault is enabled, in **Unique Key** enter the unique key.
8. To validate access to the account and services, click **Validate and Add**.
9. Click **Ok**.
10. Click **Save**.

Configuring Storage Center to send SNMP alerts

If you want to monitor Dell SC Series alerts, use the Dell Storage Manager Client to configure a Storage Center to send SNMP traps to Dell SRM.

Prerequisites

The Storage Center must be added to Enterprise Manager using a Storage Center user with Administrator privileges.

Steps

1. In the Dell Storage Manager desktop client, click **Storage**.
2. Select a Storage Center.
3. In the **Summary** tab, click **Edit Settings**.
4. Select **SNMP Server** from the menu.
5. In **SNMP Version**, select **SNMP v1/v2c**.
6. In **Read Only Community String**, type `public`.

7. In **Read Write Community String**, type **public**.
8. Click **Create SNMP Trap Destination**.
9. In **Trap Destination**, type the hostname or IP address of the Dell SRM Primary Backend or Alerting Backend.
10. From the **Type** drop-down, select the trap type to use.
11. In **Port**, type **2041**.
12. In **Community String**, type **public**.
13. To save the changes, click **OK**.
14. If the **Agent Running** status is Not Running, click **Start SNMP**.
15. To save the changes, click **OK**.

Limitations

When an array has a down disk that is waiting to be replaced, the individual capacity values (Configured Usable, Hot Spare, RAID Overhead, Unconfigured, Unusable) can add up to be more than the Total Raw Capacity Usage. This issue happens because the capacity of the down disk is counted as both Unusable capacity and Unconfigured capacity. Once the down disk is replaced, the individual capacity values will correctly add up to the Total Raw Capacity Usage.

9

SolutionPack for Dell CloudIQ

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell CloudIQ collects and interprets data on health scores from CloudIQ.

Installing the SolutionPack

Prerequisites

Create a REST API client. See CloudIQ Integrations for more details.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name if you want to change the default instance name of generic-host.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use **localhost** on port 2020, which is the Collector host where the Load Balancer Connector is installed.
8. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
   If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
9. To configure polling settings, select **Use advanced settings**.
10. Click **Next**.
    The window displays reports settings.
11. In **Administration Web-Service Instance**, select an existing instance which is default.
12. Click **Install**.
13. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices in Discovery

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.

2. Click **Dell CloudIQ**.
3. Click **Add...**.
4. In **Unique friendly name**, provide a unique friendly name for the CloudIQ client. This name is used to uniquely identify the system in reports.
5. In **Username**, type the ClientID of the CloudIQ API client.
6. 1In **Password**, type the ClientPassword of the CloudIQ API client.
7. Click **Validate and Add** to validate the credentials.
8. Click **OK**.
9. Click **Save**.

Limitations

The health score feature is currently limited to the following SolutionPacks:

- SolutionPack for Dell PowerScale
- SolutionPack for Dell PowerStore
- SolutionPack for Dell PowerMax
- SolutionPack for Dell Unity
- SolutionPack for Dell XtremIO

10

SolutionPack for Dell Data Domain

This chapter includes the following topics:

Topics:

Overview

The SolutionPack generates real-time and historical reports and accesses file system, compression, replication, and chassis inventory status details to gain insight into the management of an Dell Data Domain system.

Data collection method

SNMP

The SolutionPack for Dell Data Domain uses SNMP to access performance data information that was automatically collected and interpreted (using resource grouping and mathematical calculations).

There are two methods for discovering Dell Data Domain devices:

- Device discovery UI using the Generic-SNMP collector – With this approach you can perform the device discovery using the device discovery UI and the Generic-SNMP collector. If you prefer this method, you do not need to install the Dell Data Domain data collection block.
- Discovery Center UI using the dedicated DellData Domain SNMP Collector – With this approach you must install the Dell Data Domain data collection block that is introduced in ViPR SRM 4.2. After installing this data collection block, you can use the Discovery Center UI to discover DellData Domain systems.

NOTE: Dell Data Domain systems should not be discovered simultaneously from SNMP Device Discovery and Discovery Center.

REST

Device discovery UI using REST – With this approach, you can perform the device discovery using the device discovery UI and REST.

NOTE: Rest API support is limited to Summary and a few Inventory reports.

Configuring Data Domain systems for SNMPv1 and SNMPv2c

Configure Data Domain systems for SNMPv1 or SNMPv2c to enable device discovery, and alert consolidation for the devices. The SNMPv1 or SNMPv2c information you provide when performing discovery is necessary for Dell SRM to contact the device

to obtain information. Dell SRM collects data from the Data Domain system using the SNMP community name. It uses the SNMP port for communication. The default port is 161.

Prerequisites

Ensure that the SNMP timeout period is greater than 10,000 ms to prevent timeout from occurring while discovering the Data Domain system.

Steps

1. Log in to the Data Domain system as an administrator.
2. To configure the community string with specific privileges, run the following commands:

   snmp add ro-community <*community-string-list*> [hosts <*host-list*>]

   snmp add rw-community <*community-string-list*> [hosts <*host-list*>]

   Example:

   ```
   sysadmin@dd2200# snmp add ro-community <community-string> hosts <hostname>
   ```

3. To verify if the SNMPv1 or SNMPv2c community string exists, run the following command:

   snmp show config

Table 8. Sample output of snmp show config command

Community	Access	Hosts
watch4net	read/write	10.20.30.40
public	read-only	10.20.30.50

Configuring Data Domain systems for SNMPv3

Configure Data Domain systems for SNMPv3 to enable discovery and alert consolidation for devices. The SNMPv3 information you provide when performing discovery is necessary for Dell SRM to contact the device to obtain information. Dell SRM collects data from the Data Domain system using SNMPv3 secure credentials. Dell SRM supports SNMPv3 with all the combinations of Auth (MD5, SHA) and Priv (AES, DES, NONE). This procedure provides an example of creating an SNMPv3 user called watch4net, MD5 authorization, and AES128 authentication.

Prerequisites

Ensure that the SNMP timeout period is greater than 10,000 ms to prevent timeout from occurring while discovering the Data Domain system.

Ensure that the SNMPv3 user has a minimum of 8 characters.

Steps

1. Log in to the Data Domain system as an administrator.
2. Run the following command:

   snmp user add <user-name> access {read-only | read-write} [authentication-protocol {MD5 | SHA1} authentication-key <*auth-key*> [privacy-protocol {AES | DES} privacy-key <*priv-key*>]]

   Example:

   ```
   sysadmin@dd2200# snmp user add watch4net access read-only authentication-protocol MD5
   authentication-key <auth-key> privacy-protocol AES privacy-key <priv-key>
   ```

3. To verify the new user, run the following command:

   snmp show config

Table 9. Sample output of snmp show config command

User	Access	Authentication Protocol	Privacy Protocol
watch4net	read-only	MD5	AES
vipradmin	read/write	SHA1	DES

Configuring Data Domain devices for alert consolidation

To configure Data Domain appliances to send SNMP alert traps to Dell SRM, use the following methods:

From CLI

Use the `snmp add trap-host` command to forward SNMP v2 alert traps from Data Domain devices to Dell SRM.

Steps

1. Log in to the Data Domain as the administrator.
2. Type **snmp add trap-host community <*Community String*> version <*SNMP trap version*> <*trap recipient IP*>:<*trap listening port*>**, and press **Enter**.

   Where:
   - <*Community String*> is **public**
   - <*SNMP trap version*> is **v2c/v3c**
   - <*trap recipient IP*> in a single vApp installation, this parameter is the Dell SRM IP, and in a distributed environment, is the Primary Backend server's IP.
   - <*trap listening port* > is **2041**, which is the Dell SRM trap listening port.

   Example:

   ```
   snmp add trap-host community watch4net version v2c 10.247.24.190:2041
   ```

3. If you have multiple Data Domain devices in the storage environment, repeat this procedure on each device.

From the user interface

Steps

1. Login with Administrator credentials.
2. Go to **Administration** > **Settings**.
3. Select the **SNMP** tab and go to **SNMP V2C Configuration**.
4. Under **Trap Hosts**, click **Create** and configure the following details:

Option	Input
Host	In a single vApp installation, this option is the Dell SRM IP, and in a distributed environment, is the Primary Backend server's IP.
Port	2041, which is the Dell SRM trap listening port.
Community	Public

5. Click **Ok**.
6. If you have multiple Data Domain devices in the storage environment, repeat this procedure on each device.

Installing the SolutionPack

Prerequisites

- Data Domain must be configured to allow the Dell SRM collector host to communicate to it via SNMP.
  - To view the SNMP configuration, use the following command on the Data Domain system: `# snmp show config`
  - Use the following command to add the Dell SRM host: `# snmp add ro-community <public> hosts <emc m&r.collector.com>` where `<public>` is the read-only community string
- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- Beginning with ViPR SRM 4.2, the SolutionPack for Dell Data Domain includes a dedicated SNMP Data Collection Manager that allows you to discover Dell Data Domain devices via Discovery Center through this SNMP Data Collection block. Performance polling interval configurations only apply to devices discovered using Discovery Center. However, if you prefer to discover Dell Data Domain devices through SNMP Device Discovery and the Generic-SNMP collector, you can skip installing this block. This option has been provided for backward compatibility.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.
   If you select Add a new alerting on data collection, type information about the alerting configuration. In Alerting Backend hostname or IP address, specify the Primary Backend host.
9. Click **Next**. The window displays SNMP data collection details.
   The SolutionPack for Dell Data Domain includes a dedicated SNMP Data Collector that allows you to discover Dell Data Domain devices via Discovery Center through this SNMP Data Collection block. However, you can skip installing this block if you prefer to discover Dell Data Domain devices through SNMP Device Discovery and the Generic-SNMP collector. This option has been provided for backward compatibility.
10. From the Data collection drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use localhost on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. If you select **Frontend Web service**, drop-down list, select existing settings that have been specified for other components, or select Add a new Frontend Web service.
    If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
12. From the Topology Service drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.
    If you select Add a new Topology service, provide information about the topology service and the web service. In Topology Service hostname or IP address, specify the Primary Backend.
13. Select **Configuration settings for SNMP Discovery** option For SNMP discovery.

    Specify the SNMP Collector name, SNMP Collector port, and the communication interface IP address. The default collector name is DataDomain-SnmpCollector, and the default port is 2006.
14. To configure polling period and polling group settings, select **Configure advanced settings**.

    The advanced settings are applicable only for the dedicated SNMP Data Collector and are not applicable for the Generic-SNMP collector. Use caution when configuring these settings. Improper settings will impact SNMP Collector performance.

    Performance data Polling period defines the frequency with which the dedicated SNMP Collector polls the performance related data from the switch.

Topology Polling period defines the frequency with which the dedicated SNMP Collector polls the topology related data from the switch.

All the capabilities that are supported by the switch will be polled.

Polling Group configuration consists of a group of switches and some of the capabilities that are supported by those switches. You can optimize the resources that are consumed by the dedicated SNMP Collector by tuning these settings.

Property refresh time is the time at which the properties will be refreshed for a polling group. The property refresh time format is HH:MM:SS, where HH is hours, MM is minutes, and SS is seconds.

Start Polling Group at Defined period when enabled, will start the polling at the next "round" period. Raw value timestamps will be accurate. For example, if the polling period is set to 5 minutes, this would mean that the polling cycles will start at 00:00, 00:05, 00:10, and so on.

Polling Group Start Time offset (s) is used to start different polling groups at different times to avoid putting an excessive load on the dedicated SNMP Collector. The polling for the polling groups will start one after the other with a delay specified by this time offset. When setting a polling group start time offset, consider the shortest polling period (performance or topology), the time it takes for the SNMP Collector to poll the switch for the capabilities in the polling group, and the number of polling groups. If the polling group start time is too short, the load on the SNMP Collector will increase. If the polling group start time is too long, the polling groups might not be finished polling within the polling interval and the next polling period might start.

15. Optionally, to configure polling settings for discovery through REST, select **Advanced settings for REST**.
    a. Performance data Polling period: Default value - 15 minutes.
    b. Topology polling period: Default value - 60 minutes.
16. Click **Next**.
    The window displays reports settings.
17. In **Administration Web-Service Instance**, select an existing instance.
18. Click **Next**.
    The window displays a note about SNMP masks.
19. Click **Install**.
20. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Prerequisites

The SolutionPack for Dell Data Domain supports device discovery using SNMP and REST. If the devices are discovered using SNMP dedicated SNMP Data Collection Manager must be installed. For more information about installing the SNMP Data Collection Manager, see Installing the SolutionPack for Dell Data Domain installation.

The following procedure describes how to add devices individually using Discovery Center. To add multiple devices at a time, use a discovery group. If the devices share same credentials, the credentials are entered only once. For more information about creating discovery groups, see Add devices using discovery.

Steps

1. Click **Discovery** > **Discovery Center** > **Manage Discovery**.
2. Select **Dell Data Domain** and click **Add**.
3. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, Community String/User Name/Password is active.

4. Select **Discovery Mode**.
   - To discover Dell Data Domain though REST, select **REST** option from the drop-down.
     a. In the **IP Address** field, type the IP Address or Name of the device
     b. Type the access credentials.
     c. Click **Validate and Add**.
     d. Click **Ok**.
     e. Click **Save**.
   - To discover Dell Data Domain though SNMP, select **SNMP** option from the drop-down.

Specify the details of the Dell Data Domain configuration. Do not enter spaces.

a. In the **Device location** section, select the server and instance where you want to store the configuration details for this device.
b. In the **Device IP Address** field, type the IP address of the device that is supporting the SNMP agent.
c. In **SNMP Port** field, type the device SNMP agent listening port.
d. In the **SNMP Version** field, type the device SNMP agent version. If you select v3, select the authentication and encryption protocols, and specify the passwords.
e. In the **Community String/User Name** field, specify the community name if the SNMP version is v1 or v2c. Specify the username if the SNMP version is v3.
f. If secure vault is enabled, in **Unique Key** enter the unique key.

5. To trigger discovery, click **Validate and Add**.

   Discovery fetches minimal information about the device like the supported capabilities.

   The validation tests connectivity to the device using the provided information. If an error indicator appears, correct the information and click **Test** to try again.

   The **Status** column represents the discovery results. To view the discovery results, click the status icon.

6. To trigger polling, click **Save**.
   Polling is the periodic collection of the metrics and properties from the switch that is based on the supported capabilities that are discovered.

Limitations

- The **Device** column of the Alerts report (**Report Library >> Dell Data Domain >> Operations**) might be blank for some of the alerts. The source address that is received from the alert trap notification corresponds to the network interface on the Data Domain Replicator. The Data Domain Replicator might have multiple interfaces that are configured. The SNMP service always binds to one address and sends all traps using that address. There is no option to select the source address if the system has multiple interfaces.
- When discovering Data Domain Virtual Edition 3 (version 6.0.0.30-550720), the following reports will be empty:
  - **Report Library >> Dell Data Domain >> Inventory >> Chassis Status >> NVRAM Batteries**
  - **Report Library >> Dell Data Domain >> Inventory >> Disks >> device, part >> Temperature**
  - **Report Library >> Dell Data Domain >> Inventory >> Disks >> device, part >> Status >> Error Count**
  - **Report Library >> Dell Data Domain >> Inventory >> NVRAM**
- **Report Explore > Storage Systems > Dell Data Domain > Storage Connectivity > File Path Details** will not be visible for Data Domain systems as this report is not relevant to Data Domain and only applies for devices such as Unity. Consequently, parent report **Explore > Storage Systems > Dell Data Domain > Storage Connectivity** will be hidden from Explore reports for Data Domain systems.
- Not all metric data are supported in the Data Domain REST API.
- The REST API support is limited to summary and a few inventory reports.
- Metrics not available in the REST are marked as "NS".
- Graph reports are not supported.

NOTE: For comprehensive Data Domain reports, it is recommended to discover all Data Domain devices using the SNMP interface.

11

SolutionPack for Dell Data Protection Advisor

This chapter includes the following topics:

Topics:

Overview

This SolutionPack enables users to generate real-time and historical reports on replication technologies, Dell Data Domain backup-to-disk platform, backup technologies for Symantec Netbackup, and Dell EMC Avamar supported by Data Protection Advisor.

Data collection methods

The SolutionPack collector uses REST API requests to fetch XML report files from the DPA server (`<EMC DPA Installation directory>\EMC\services\shared\report-results\scheduled\<backuptechnology-selected>`). When DPA is added to Discovery Center, scheduled reports are created and generated once a week. Once the scheduled reports are generated, report data is collected hourly.

The Stream Collector uses REST APIs to collect the data for the following:

- Symantec-NetBackup
- Dell EMC-Avamar
- Dell EMC-NetWorker
- IBM-Tivoli-Storage-Manager
- Dell RecoverPoint
- Dell Data Domain

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- Ensure that libtinfo is present in `/lib64/libtinfo`. If not, then create a softlink using the command: `sudo ln -s /lib64/libncurses.so.5.6 /lib64/libtinfo.so.5`

Steps

1. Login to the Primary Backend server via the command line.
2. Browse to the following location:
   `/opt/APG/bin/`
3. Run the following command:

./mysql-client.sh

4. Type the root user password.
   The default root user password is `watch4net`
5. Run the following command:
   connect events;
6. Create the following table:

   NOTE: If you copy and paste the script, carriage return characters may exist at the end of each line in the pasted version. You must use a text editor such as Notepad to remove these characters.

```
CREATE DATABASE IF NOT EXISTS events;
GRANT ALL PRIVILEGES ON events.* TO apg@'localhost'
IDENTIFIED BY 'watch4net';
GRANT FILE ON *.* TO apg@'localhost' IDENTIFIED BY
'watch4net';
use events;
DROP TABLE IF EXISTS generic_backup;
CREATE TABLE IF NOT EXISTS `generic_backup` (
 `id` bigint(20) DEFAULT NULL,
 `appjobid` varchar(256) NOT NULL DEFAULT '',
 `openedat` int(11) NOT NULL,
 `datagrp` varchar(100) DEFAULT NULL,
 `prjobid` int(11) DEFAULT NULL,
 `bkpservr` varchar(100) DEFAULT NULL,
 `bkpos` varchar(100) DEFAULT NULL,
 `bkprev` varchar(100) DEFAULT NULL,
 `dpahost` varchar(100) DEFAULT NULL,
 `collhost` varchar(100) DEFAULT NULL,
 `collinst` varchar(100) DEFAULT NULL,
 `device` varchar(100) DEFAULT NULL,
 `clntos` varchar(100) DEFAULT NULL,
 `part` varchar(100) DEFAULT NULL,
 `ip` varchar(100) DEFAULT NULL,
 `partdesc` varchar(100) DEFAULT NULL,
 `parttype` varchar(100) DEFAULT NULL,
 `policy` varchar(100) DEFAULT NULL,
 `bkptech` varchar(100) DEFAULT NULL,
 `bkptype` varchar(100) DEFAULT NULL,
 `retlevel` varchar(100) DEFAULT NULL,
 `state` varchar(100) DEFAULT NULL,
 `mediasvr` varchar(100) DEFAULT NULL,
 `path` varchar(100) DEFAULT NULL,
 `lwatermk` varchar(100) DEFAULT NULL,
 `hwatermk` varchar(100) DEFAULT NULL,
 `stuid` varchar(100) DEFAULT NULL,
 `stutype` varchar(100) DEFAULT NULL,
 `capacity` varchar(100) DEFAULT NULL,
 `userdefined1` varchar(100) DEFAULT NULL,
`userdefined2` varchar(100) DEFAULT NULL,
 `userdefined3` varchar(100) DEFAULT NULL,
 `userdefined4` varchar(100) DEFAULT NULL,
 `userdefined5` varchar(100) DEFAULT NULL,
 `userdefined6` varchar(100) DEFAULT NULL,
 `userdefined7` varchar(100) DEFAULT NULL,
 `userdefined8` varchar(100) DEFAULT NULL,
 `userdefined9` varchar(100) DEFAULT NULL,
 `userdefined10` varchar(100) DEFAULT NULL,
 `userdefined11` varchar(100) DEFAULT NULL,
 `userdefined12` varchar(100) DEFAULT NULL,
 `userdefined13` varchar(100) DEFAULT NULL,
 `userdefined14` varchar(100) DEFAULT NULL,
 `userdefined15` varchar(100) DEFAULT NULL,
 `systemdefined1` varchar(100) DEFAULT NULL,
 `systemdefined2` varchar(100) DEFAULT NULL,
 `systemdefined3` varchar(100) DEFAULT NULL,
 `systemdefined4` varchar(100) DEFAULT NULL,
 `systemdefined5` varchar(100) DEFAULT NULL,
 PRIMARY KEY (`appjobid`, `openedat`)
) ENGINE=MyISAM DEFAULT CHARSET=utf8;
```

7. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
8. Select the SolutionPack.
9. Click **Install**.
10. Type the instance name.
11. Assign a server for each component.

    In a typical four server deployment, the recommended servers are selected automatically.
12. Click **Next**.
    The window displays a note about Alert Consolidation.
13. Click **Next**.
    The window displays data collection details.
14. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
15. In the **Event server hostname or IP address** text box, accept the default, which is the Primary Backend.
16. In the **Event server port number** text box, accept the default port of 22020.
17. From the **Event database** drop-down list, select the Primary Backend.
18. From the **Alert Consolidation** drop-down list, select existing settings that have been specified for other components, or select **Add a new Alert consolidation**.

    If you select **Add a new Alert consolidation**, type information about the alert configuration. In **Alerting HostName or IP address**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
19. Select the backup technologies to monitor.

    If you do not select any of these options, there will be no DPA reports to collect. If you select all of these options, data will be collected for all DPA reports.
20. Select **Enable Dell DataProtectionAdvisor Alerts**.
21. To configure the alert polling interval, select **Do you want to configure advanced settings**.

    By default, the polling interval for Data Protection Advisor backup alerts is 5 minutes. You can change the polling period to 30 minutes.
22. Click **Next**.
    The window displays reports settings.
23. Click **Install**.
24. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
25. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
26. Select **Dell Data Protection Advisor**.
27. Click **Add...**
28. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Dell DPA Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Dell DPA Password is active.
29. In **DPA appliance Host name or IP**, type the host information for the DPA appliance.
30. Provide the administrator access credentials for the DPA appliance.

    Administrator privileges are needed so that users can schedule reports on the DPA Server.
31. Provide the protocol and DPA server port.
32. To validate the credentials, click **Validate and Add**.
33. Click **Ok**.
34. Click **Save**.

    DPA requires specific licenses to monitor replication technologies, backup technologies, and Data Domain. These licenses must be installed on DPA for Dell SRM to monitor these technologies.

    DPA reports may take up to 1 hour to populate. Some of the performance data/graphs take two collection cycles for the graphs to be plotted.

After installing the SolutionPack for Dell Data Protection Advisor, there may be scheduling related errors in the collector logs.

Verifying scheduled reports in DPA

Once DPA is added to Discovery Center, Dell SRM connects to DPA with the username specified and creates scheduled reports for the backup technology selected.

Steps

1. Login to DPA.
2. Browse to **Reports** > **Report Jobs** > **Scheduled reports**.
   Report names starting with `W4N` – should be created hourly.
3. On the DPA server console, XML files should be seen in the directory `<Dell DPA Installation directory>\Dell\services\shared\report-results\scheduled\<backuptechnology-selected>`.

Troubleshooting report generation errors

Reconfigure the data collection options in the SolutionPack for Dell Data Protection Advisor if reports are not being generated. This procedure applies to each DPA instance for which reports are not being generated.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select **Dell Data Protection Advisor** and click **Install**.
3. Within the **Instance** column, click the edit icon to reconfigure the Data Collection component.
4. Select the technology that you want to collect data from.
5. Select **Do you want to configure advanced settings** and enable **Number of collecting threads**, if required.
6. Click **Reconfigure**.

Limitations

- When you click a device in the **Alerts** tab of the **Report Library >> Dell Data Protection Advisor >> Operations** report, the link incorrectly displays the **Explore All Hosts** summary report.
- There could be a difference in the number of jobs that are reported by the DPA UI and the SolutionPack for Dell Data Protection Advisor. This occurs when an All Jobs report for the last hour is scheduled in DPA. The scheduled All Jobs report causes completed and failed jobs to be dumped to an XML file on the DPA server, which is not counted by Dell SRM, hence the difference.
- When collecting data from newer versions of DPA, such as versions 6.2.2, 6.2.3, and 6.3, the following reports will be empty because these versions of DPA do not support them:
  - **Report Library >> Dell Data Protection Advisor >> Inventory >> Data Domain >> Hosts >> [*host*] >> Performance >> Fibre Channel Port Performance**
  - **Report Library >> Dell Data Protection Advisor >> Inventory >> Data Domain >> Hosts >> [*host*] >> Performance >> Total Throughput**
  - **Report Library >> Dell Data Protection Advisor >> Inventory >> Data Domain >> DD Modes**
  - **Report Library >> Dell Data Protection Advisor >> Inventory >> Data Domain >> Hosts >> [*host*] >> Statistics >> MTree Daily Compression Statistics**
  - **Report Library >> Dell Data Protection Advisor >> Inventory >> Replication >> RPO Compliance >> Compliance**

12

SolutionPack for Dell ECS

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell ECS collects inventory, capacity, performance, and health metrics for object storage on Dell ECS systems. Detailed metrics for the virtual data centers, nodes, and disks for object storage that ECS manages are included.

Installing the SolutionPack for Dell ECS

Prerequisites

- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- For each ECS Virtual Data Center (VDC) that you want to collect metrics for:
  - Have the public IP address for one of the nodes in one of the ECS racks (as a convention, you might use the first node in the first rack)
  - Have the username and password

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select the Primary Backend host.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. In **Alerting Backend hostname or IP address**, type the Primary Backend host.
12. In **Alert Listener Port**, type the port that is used for alert consolidation.

13. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology Service**, type information about the topology service. In **Topology Service hostname or IP address**, specify the Primary Backend host.
14. To configure polling settings or to disable a polling type, select **Use advanced settings**.
15. In each polling period drop-down list, select a polling period or select **Disabled** to turn off the polling.
16. Click **Next**.
    The window displays reports settings.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
19. In **SRM Admin UI** page, click **DISCOVERY**.
20. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
21. Select **Dell ECS**.
22. Click **Add**.

    For ECS, a *device* is a VDC, and the term *ECS system* refers to a VDC. A VDC consists of one or more ECS appliances (racks) with 4 or eight nodes each and attached storage systems.

    In a multi-site federation of VDCs, provide information for each VDC as a separate device.
23. Verify that the first two fields are correct for the collection instance.
24. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, ECS Password is active.
25. In **Virtual Data Center name**, type the VDC name as configured in ECS.
26. In **IP address or host name**, provide the public IP address for one of the nodes in one of the ECS racks in the VDC. For example, use the public IP address for the first node in the first rack in the VDC.
27. For **Username** and **Password**, provide the credentials that are configured for the VDC.

    User with System Monitor role is required as the minimum privilege.
28. If secure vault is enabled, in **Unique Key** enter the unique key.
29. For **Configured for remote replication**, check this box if the VDC is part of a geo-replicated federation of VDCs. When you check this box, the **Collect namespace and bucket data** field appears.
30. In **Collect namespace and bucket data**, check this box for only one of the VDCs in a geo-replicated federation of VDCs.

    This field configures the 1 VDC in the geo-replicated federation that provides the namespace and bucket metrics for reporting.

    NOTE: Enabling namespace and bucket data from multiple VDCs in a geo-replicated federation causes duplicate counting and duplication of billing data.
31. To validate the credentials, click **Validate and Add**.
32. Click **Ok**.
33. Click **Save**.
    It takes approximately 3 hours for data to start appearing on reports from the new VDC.
34. To add another VDC, click **Add new device** and provide information for another VDC.

    NOTE: In a multi-site federation, add each VDC in the federation, but collect namespace and bucket data for only one of them.

Expand ECS

About this task

You can expand an existing VDC by adding more storage, more nodes, or more ECS racks, without any additional configurations in Dell SRM.

A new VDC must be added into Discovery Center as a new device before Dell SRM can collect metrics for it.

Steps

1. Browse to **Discovery** > **Discovery Center** > **Manage Discovery**.
2. Click **Dell ECS**.
3. Click **Add**.
4. Verify that the first two fields are correct for the collection instance.
5. In **Virtual Data Center name**, type the VDC name as configured in ECS.
6. In **IP address or host name**, provide the public IP address for one of the nodes in one of the ECS racks in the VDC. For example, use the public IP address for the first node in the first rack in the VDC.
7. For **Username** and **Password**, provide the credentials that are configured for the VDC.
   User with System Monitor role is required as the minimum privilege.
8. For **Configured for remote replication**, check this box if the VDC is part of a geo-diverse federation of VDCs.
   When you check this box, the **Collect namespace and bucket data** field appears.
9. In **Collect namespace and bucket data**, check this box for only one of the VDCs in a geo-replicated federation of VDCs.
   Configure 1 VDC in the federation to provide the namespace and bucket metrics.

   NOTE: Enabling namespace and bucket data from multiple VDCs in a geo-replicated federation causes duplicate counting and duplication of billing data.

10. To validate the credentials, click **Validate and Add**.
11. Click **Ok**.
12. Click **Save**.
    It takes approximately take 3 hours for data to start appearing on reports from the new VDC.
13. To add another VDC, click **Add new device** and provide information for another VDC.

    NOTE: In a replicated federation, add each VDC in the federation, but configure namespace and bucket data for only one of them.

Limitations

- The SolutionPack for Dell ECS has visibility into the ECS storage capacity that is configured for objects, and not for other types of storage. Consequently, in the **Enterprise Capacity Dashboard**, the SolutionPack for Dell ECS only contributes to the Configured Usable, Used, Pool Free, Used For Object, and Primary Used capacities.

13

SolutionPack for Dell PowerEdge

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell PowerEdge collects and generates real-time and historical reports, and access system, storage, power, power usage, and environment probes status and reading details.

NOTE: To collect carbon emission data for a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

Installing the SolutionPack

Prerequisites

- Identify the iDRAC details.
- Identify the access credentials.

About this task

After you log in as an administrator, you can install a SolutionPack.

NOTE: Core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
8. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

   If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

9. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

   If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
10. Select **Do you want to configure advanced settings** to configure polling settings.
11. Click **Next**.
    The window displays Reports details.
12. In **Administration Web-Service Instance**, select an existing instance which is default.
13. Click **Install**.
14. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices in Discovery Center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Select **Dell PowerEdge**.
3. Click **Add...**
4. In **Dell PowerEdge Device IP address**, type the iDRAC IP Address, FQDN of the PowerEdge.
5. In **iDRAC username**, type the username for the PowerEdge REST Gateway.
6. In **iDRAC password**, type the password to access Dell PowerEdge.
7. To validate the credentials, click **Validate and Add**.
8. Click **Ok**.
9. Click **Save**.

14

SolutionPack for Dell PowerScale

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell PowerScale optimizes service availability for the Dell PowerScale scale-out NAS storage solution and displays the data in easy-to-use reports within Dell SRM.

This SolutionPack enables you to see and understand performance and utilization across Dell PowerScale devices in real-time, to know which node is the bottleneck in a cluster, what the peak/busy hours are, and more.

NOTE: To collect carbon emission data for a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

NOTE: To link and launch CloudIQ, follow the steps in Link and launch CloudIQ. To view the CloudIQ health score of the device, install and discover the CloudIQ SolutionPack as described in SolutionPack for CloudIQ.

Installing the SolutionPack

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

12. In **Alert Consolidation server hostname or IP address**, type the Primary Backend host.
13. In **Alert Consolidation server port number**, type the port that is used for alert consolidation.
14. Optionally, select **Use advanced settings** to configure polling.
15. Clear **Enable Snapshot collection** to disable snapshot collection for PowerScale arrays.
16. Click **Next**.
    The window displays reports settings.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
19. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
20. Select **Dell PowerScale**.

    These steps describe how to add hosts individually. For information about using discovery groups to use the same credentials to discover multiple hosts, see Adding devices to discovery groups

21. Click **Add**.
22. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
    When the Secure Vault checkbox is selected, the Unique Key and Safe fields appear.

    NOTE: The Unique Key and Safe fields are enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.

23. In the **Cluster hostname or IP address** field, type the hostname or IP address of the SmartConnect service, or of any node in the cluster.

    NOTE: Recommended using IP address.

24. Type the username (default is admin).

    NOTE: In Case of device discovery, if any JSON reserved special character is present in the username or password (such as a backslash in LDAP user account name), then JSON string escaping must be done that is those special characters such as Slash, backslash, or double-quotes must be preceded with a backslash character. For Example, domain\username must be keyed-in as domain\\username or pas"sword must be keyed-in as pas\"sword. For more detail, see this link.

25. Type the password.
26. If Secure Vault is enabled, in **Unique Key** enter the unique key.
27. If Secure Vault is enabled, in **Safe** enter the safe string.

    NOTE: Safe string can be given as input along with the Cyberark unique key when Secure Vault is checked. This input is optional and when no details are provided for safe, the default safe details that are provided in the Cyberark configuration will be used.

28. To validate the credentials, click **Validate and Add**.
29. Click **Ok**.
30. Click **Save**.

Limitations

- Dell PowerScale RestAPI has a limitation that it cannot get StoragePool information for OneFS 7.0. So the Dell PowerScale SolutionPack cannot show any StoragePool information on OneFS 7.0. StoragePool information is only available for OneFS 7.1 and above.
- When discovering Dell PowerScale OneFS 7.x arrays, it is possible that the following errors will occur when testing authentication with the device: `javax.net.ssl.SSLProtocolException: handshake alert: unrecognized_name`. These messages can be safely ignored unless they are also found in the SolutionPack for Dell PowerScale collecting logs.

- Starting from SRM 4.2, while discovering Dell PowerScale devices which now use Stream Collector for data collection, if BufferOverflowException is seen in logs with the error as shown, increase the buffer_size value set in socketconnector.xml with respective to Collector Manager. New value to be increased such that the issue no more occurs, considering the available system memory.

```
AbstractStreamHandlerJob::prepareNextStep(): Error executing handler XmlReader
java.nio.BufferOverflowException
at java.nio.HeapByteBuffer.put(HeapByteBuffer.java:189)
at java.nio.ByteBuffer.put(ByteBuffer.java:859)
at
com.watch4net.apg.v2.collector.plugins.SocketConnector.pushData(SocketConnector.java:3
92)
at
com.watch4net.apg.v2.collector.AbstractCollector.pushNext(AbstractCollector.java:56)
```

NOTE: If the size of the response that is obtained over API is greater than 32KB for any API request that is issued during Dell PowerScale data collection, increasing the buffer size value will fix the issue. Do not look into the metrics for incrementing the buffer size as the metrics will never get collected if parsing fails. `BufferOverFlowException` occurs in the stage of data parsing. Hence, if issue occurs, APIs responses to be examined and `buffer_size` set accordingly.

15

SolutionPack for Dell PowerStore

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for Dell PowerStore enables users to view:

- Block and File objects.
- Reports and alerts on capacity/performance/configuration/availability metrics.
- Enterprise capacity dashboard and capacity planning reports.
- End to end topology and mapping of hosts to PowerStore storage.
- Chargeback reporting and Configuration compliance
- Support for NVMe-oFC Arrays, including Host to Array connectivity details, NVMe-oFC configuration details.
- Reports and dashboards to track File System Performance KPIs.
- Monitor and report on VVOL replication metrics.
- Monitor and report on Block Volume replication metrics.
- Monitor and report on the Block Metro sync replication metrics.
- Monitor and report on File replication metrics.
- Monitor and report on NAS Server replication metrics.
- Monitor and report on Volume Group replication metrics.
- Threshold-based alert support on Lag Time for Virtual Volume, Metro, and File system.
- Hardware alerts support through SNMP Traps.

NOTE: To link and launch CloudIQ, follow the steps in Link and launch CloudIQ. To view the CloudIQ health score of the device, install and discover the CloudIQ SolutionPack as described in SolutionPack for CloudIQ.

Installing the SolutionPack

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.
6. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays a note about Alert Consolidation.
8. Click **Next**.
   The window displays pre-configured alert details.

9. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select Add a new alerting data collection.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown has default value. Do not change the value.
10. Click **Next**.
    The window displays data collection details.
11. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. To configure Topology Polling Period and Performance Polling Period, select **Use advanced settings**.

    Topology Polling Period defines the polling period of the capacity and topology data. The default value is 30 minutes.

    Performance Polling Period defines the polling period of the performance data. The default value is 5 minutes.
14. Clear **Enable Snapshot collection** to disable Snapshot collection of PowerStore SolutionPack arrays.
15. Click **Next**.
    The window displays Reports details.
16. In **Administration Web-Service Instance**, select an existing instance which is default.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **Dell PowerStore**.
3. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   When the Secure Vault checkbox is selected, the PowerStore Management Cluster Unique Key and Safe fields appear.

   NOTE: The Unique Key and Safe fields are enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the PowerStore Management Cluster Password is active.
4. Click **Add**.
5. Select the server instance where you want to store the configuration details for this device. And then, type the PowerStore Management Cluster IP address or hostname, port(default: 443), username (PowerStore Management Cluster host user with Administrator privileges is required), and password.
6. If Secure Vault is enabled, in **Powerstore Management Cluster Unique Key** enter the unique key.
7. If Secure Vault is enabled, in **Safe** enter the safe string.

   NOTE: Safe string can be given as input along with the Cyberark unique key when Secure Vault is checked. This input is optional and when no details are provided for safe, the default safe details that are provided in the Cyberark configuration will be used.
8. To validate the credentials, click **Validate and Add**.
9. Click **OK**.
10. Click **Save**.

SNMP Trap configuration in PowerStore SolutionPack

To populate hardware alerts in Dell SRM, the user must configure the SNMP trap recipient on the PowerStore appliance.

Steps

1. Log in to the PowerStore Manager.
2. Go to **Settings** > **Networking** and select **SNMP**. The SNMP window appears.
3. To add an SNMP Manager, click **Add** under SNMP Managers. The Add SNMP Manager slide-out appears.
4. Depending on the version of SNMP, configure the following information for SNMP Manager:
   - For SNMPv2c:

     Table 10. SNMPv2c configuration details in PowerStore Manager

Option	Description
Network Name or IP address	Enter the network name or IP address of the SNMP trap recipient.
Port	Enter the port number as 2041.
Minimal Severity Level of Alerts	Enter the minimal severity level of Alerts (Critical, Major, Minor, Info) as required.
Version	Enter version as V2c.
Trap Community String	Enter community string as Public.

   - For SNMPv3:

     Table 11. SNMPv3 configuration details in PowerStore Manager

Option	Description
Network Name or IP address	Enter the network name or IP address of the SNMP trap recipient.
Port	Enter the port number as 2041.
Minimal Severity Level of Alerts	Enter the minimal severity level of Alerts (Critical, Major, Minor, Info) as required.
Version	Enter version as V3.
Security Level	There are three levels of security options available to choose from: a. **None**: In this case, the user must provide Username only. b. **Authentication only**: In this case, the user must provide a Username, Password, and Authentication protocol (MD5/SHA256). c. **Authentication and privacy**: In this case, the user must provide a Username, Password, Authentication protocol (MD5/SHA256), and Privacy protocol (AES 256/TDES).

5. Click **Add**.
6. Optionally, click **Send Test SNMP Trap** to verify whether SNMP Manager destinations can be reached, and the correct information is received.

Limitations

- To monitor a PowerStore with SRM, the PowerStore's operating system needs to be at least version 3.0 to be compatible with SRM 4.7.1.0. However, SRM supports PowerStore OS versions up to the latest (v4.0 and beyond). This means if your PowerStore is running version 3.x to 4.x and beyond, it can be discovered by SRM 4.7.1.0 and any newer SRM versions.

- Hypervisors and Virtual Volumes discovery is not supported.

16

SolutionPack for Dell PowerSwitch

This chapter contains the following topics.

Topics:

Introduction

The SolutionPack for Dell PowerSwitch accesses performance data that was automatically collected and interpreted (using resource grouping and mathematical calculations) across multiple PowerSwitches.

Data Collection Methods:

REST - Discover the topology and performance data of PowerSwitch through PowerSwitch RESTCONF API.

NOTE: Keep your personal computer on charging mode.

Installing the SolutionPack

Prerequisites

- Enabling RESTCONF API service on the PowerSwitch in CONFIGURATION Mode.
- rest api restconf

About this task

Following are the steps to install PowerSwitch.

Steps

1. Click**Administration**
2. In the **SRM Admin UI**, click **CONFIG > SolutionPacks > Browse & Install SolutionPacks.**
3. Select the SolutionPack.
4. Click**Install**.
5. Under **Components to Install**, click **Next**.
6. Under **Pre Configured Alerts v4.8**, click**Next** .
7. Under **Data Collection v4.8**, click **Next**.
8. Under **Reports v4.8,** click **Install.**
9. You can monitor the installation process by clicking on **Pre Configured Alerts, Data Collection v4.8** and**Reports v4.8** , respectively to ensure that the installation completes successfully.
10. Click **OK.**
11. Now, on the left side, click **CONFIG > Installed SolutionPacks.**
12. Under **Installed SolutionPacks**, Dell PowerSwitch is visible.

Results

Dell PowerSwitch is successfully installed.

Adding and Configuring Devices

About this task

This part is the main thing after downloading the solution pack. Only after adding and configuring the devices, we will be able to get the data reports alerts and collections.

Steps

1. In **SRM Admin UI** page, click **DISCOVERY > Discovery Center > Manage Discovery**.
2. Click **Dell PowerSwitch**.
3. Click **Add.**
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Powerswitch Management Cluster Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

5. Input the values for **PowerSwitch Management IP, Username** and **Password/Powerswitch Management Cluster Unique Key**.
6. To validate the credentials click **Validate and Add.**
7. Click **OK.**
8. Click **Save**.
9. **Save Modifications** dialogue box will appear, click **OK**.

Limitations

- Topology map view is not supported.
- Support is for PowerSwitch S-Series and Z-Series models only.

17

SolutionPack for Dell PowerVault

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for Dell PowerVault enables users to:

- Discover and monitor Dell PowerVault Storage.
- Reports on inventory, capacity, performance, configuration, and availability metrics.
- Alerts to proactively monitor key capacity, performance, configuration, and health KPIs.
- Enterprise capacity dashboard and capacity planning reports.
- Visualize end to end Topology and mapping of hosts to Dell PowerVault array.
- Chargeback reports to show the capacity that is consumed by Applications and associated charges.
- Support for Configuration compliance and custom reports.

NOTE: To collect carbon emission data a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

Installing the SolutionPack for PowerVault

Steps

1. Click **Administration**.
2. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.
   Default name is `Dell PowerVault`.
6. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays a note about Alert Consolidation.
8. Click **Next**.
   The window displays pre-configured alert details.
9. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or make a selection in the **Alerting on data collection** field.
   If you select **Add a new Alerting on data collection**, select the appropriate value from the drop-down menu in the **Alerting Web-Service Instance** field.
10. Click **Next**.
    The window displays data collection details.
11. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. Enable **Configure Alert consolidation**. Enter the default values:
    - **Hostname or IP address**: localhost
    - **Network Port**: 2040
14. Clear **Enable Snapshot collection** to disable snapshot collection for PowerVault arrays.
15. Enable **Use advanced settingsUse advanced settings**. Enter the default values:
    - **Collection interval for Dell PowerVault Capacity and Topology**: 30 minutes
    - **Collection interval for Performance**: 5 minutes
    - **Collection interval for Alerts**: 5 minutes
16. Click **Next**.
17. In **Administration Web-Service Instance**, select an existing instance which is default.
18. Click **Install**.
19. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **Dell PowerVault**.
3. Click **Add**.
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
5. Select the server instance where you want to store the configuration details for this device and enter:
   a. **Server**: Select the server where the device will be dispatched
   b. **Instance**: Select the instance of the Dell PowerVault where the device will be dispatched
   c. **Primary Controller IP address**: Enter the IP address of the array
   d. **Secondary Controller IP address**: Enter the IP address of the array
   e. **Username**: Enter the username of the array
   f. **Password**: Enter the password of the array
   g. If secure vault is enabled, in **Unique Key**: Enter the unique key
6. To validate the credentials, click **Validate and Add**.
7. Click **OK**.
8. Click **Save**.

Limitation

“Port-related reports show empty values for the following columns: 'Type', 'WWPN', 'Status', 'Health' and 'Speed (GB/s)' for iSCSI ports. Masking and mapping details are also not available for the iSCSI ports".

18

SolutionPack for Dell RecoverPoint

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell RecoverPoint enables users to generate real-time and historical reports on the performance of the mechanisms that replicate data from any supported SAN-based arrays to other SAN-based arrays.

Summary reports for key components--such as RecoverPoint Appliance (RPA), Clusters, and Consistency Group Metrics, as well as I/O throughput analysis for SAN system traffic--provide a deeper understanding of replication schemes and the policies that govern them.

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- Ensure that the RecoverPoint appliance is reachable and that you can run REST API commands from the Collector host. The ports that are used by RecoverPoint and the Collector host should be unblocked. For more information about RecoverPoint REST API commands, see the *RecoverPoint REST API Guide* on Dell Support Site.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays preconfigured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Select **Do you want to configure advanced settings** to configure capacity and performance polling settings.
11. Click **Next**.
    The window displays reports settings.

12. From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add a new Web-Service Gateway**.

    If you select **Add a new Web-Service Gateway**, type information about the web-service gateway.
13. In **Administration Web-Service Instance**, select an existing instance which is default.
14. Click **Install**.
15. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
16. Click **Discovery** > **Discovery Center** > **Manage Discovery**.
17. Select **Dell RecoverPoint**.
18. Click **Add**.
19. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the RecoverPoint password is active.
20. Enter the FQDN hostname and authentication details for your RecoverPoint system.
21. Click **Validate and Add** to validate the credentials.
22. Click **Ok**.
23. Click **Save**.

    It takes approximately three hours for data to start appearing in reports.

    NOTE: Only one RPA Cluster management IP address is required to discover data from the whole RecoverPoint System. Adding each RPA Cluster in the RecoverPoint System as a separate device is not required.

Configuring RecoverPoint appliance for alert consolidation

To configure RecoverPoint appliances to send SNMP alert traps to Dell SRM, use the following methods:

From CLI

Steps

1. Log in to the Dell RecoverPoint appliance as an administrator.
2. Type `#get_snmp_settings`, and press Enter.
3. Type `#config_snmp_trap_dest`, and press Enter.
   - Type the **`clustname`** when prompted.
   - Type the primary backend: port (primary backend is the default node for installation of alerts blocks for RecoverPoint SolutionPack).

   Example: 10.10.10.10:2041 (where 10.10.10.10 is the IP of the primary backend, 2041 is the default port for alert processing in SRM. In a single vApp installation, this parameter is the Dell SRM IP, and in a distributed environment, is the Backend server's IP).
4. Type `#enable_snmp`, and press Enter.

Example

To test the configuration, enable SNMP Test in the alerting frontend (**Alert definitions -> Dell Recoverpoint alert definitions -> Test -> Other**).

Type the command `#test_snmp` on RecoverPoint console and this test alert will show up in **Report Library -> Dell RecoverPoint -> Operations -> Alerts**.

From GUI

Steps

1. Login with Administrator credentials.
2. Go to **Admin** > **System Notifications** > **Manage Event Filters**.
3. In the **SNMP** tab:
   a. Select **Enable SNMP Agent** checkbox.
   b. Select **Send Event Traps** checkbox.
   c. Under **Specify Trap destination for** in **cluster name**, type primary backend: port.
   Primary backend is the default node for installation of alerts blocks for RecoverPoint SolutionPack. In a single vApp installation, this parameter is the Dell SRM IP, and in a distributed environment, is the Backend server's IP.
4. Click **Apply.**
5. If you have multiple RecoverPoint devices in the storage environment, repeat this procedure on each device.

Limitations

- RecoverPoint SolutionPack displays one consolidated splitter per ESXi cluster.
- For RP4VM, the following metric will be missing:
  - Metric: JournalSizeLimit

19

SolutionPack for Dell PowerFlex

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell PowerFlex collects capacity, inventory, and performance data from Dell PowerFlex REST Gateways and displays the data in easy-to-use reports within Dell SRM.

Capacity reports provide details on free capacity, used capacity, and spare capacity at system level. Capacity reports per storage pools, per data servers, per drive, and per protection domain levels provide details on free capacity and used capacity. Inventory reports provide details on the data servers, storage pools, protection domains, drive components, snapshots, volumes, and FileSystem. Performance reports provide detailed Dell PowerFlex performance metrics.

Installing the SolutionPack for Dell PowerFlex

After you log in as an administrator, you can install a SolutionPack.

Prerequisites

- Core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
8. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

   If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
9. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

   If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

10. In **Alert consolidation server hostname or IP address**, select the Primary Backend host.
11. In **Alert consolidation server port number**, select the port that is used for alert consolidation (default: 2020)
12. Select **Do you want to configure advanced settings** to configure polling settings.
13. Clear **Enable Snapshot collection** to disable snapshot collection for PowerFlex arrays.
14. Click **Install**.
15. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices in Discovery Center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Select **Dell PowerFlex**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device. When the Secure Vault checkbox is selected, the Powerflex Unique Key and Safe fields appear.

   NOTE: The Unique Key and Safe fields are enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the PowerFlex Password is active.

5. In **Dell PowerFlex REST Gateway IP or hostname**, type the IP Address, name, or FQDN of the Dell PowerFlex REST Gateway host to be configured.
6. In **PowerFlex username**, type the username for the PowerFlex REST Gateway.
7. In **PowerFlex password**, type the password to access the PowerFlex REST Gateway.
8. If Secure Vault is enabled, in **Powerflex Unique Key** enter the unique key.
9. If Secure Vault is enabled, in **Safe** enter the safe string.

   NOTE: Safe string can be given as input along with the Cyberark unique key when Secure Vault is checked. This input is optional and when no details are provided for safe, the default safe details that are provided in the Cyberark configuration will be used.

10. To validate the credentials, click **Validate and Add**.
11. Click **Ok**.
12. Click **Save**.

Limitations

- CSV files that were exported from Discovery Center with a release earlier to ViPR SRM 3.7 cannot be used to import devices into ViPR SRM 4.0. To import devices using the earlier Dell SRM CSV file, delete the version column prior to importing.
- The Availability metric for PowerFlex disks is not available from the PowerFlex array. Therefore, the Availability metric cannot be displayed in the **All LUNs** and **IP based disk** host reports.
- If multiple Storage Pools have the same name, and the respective Protection Domains names are missing or null, only one of the Storage Pools will be listed in the Storage Pools report.
- In the **Operations >> Inactive Devices and Components >> Devices with Inactive Metrics** Global report, the count of inactive metrics is less than that shown in the **Report Library >> Dell PowerFlex >> Operations >> Inactive Metrics** report. This is because only the PowerFlex capacity related metrics are passed to the Global inactive metric report as others are filtered out by the w4ncert property. By design, the PowerFlex report has no such filter so that all of the inactive metrics are displayed.
- If alerts get cleared or acknowledged in the PowerFlex Dashboard (Element manager) the same will not be immediately reflected in the Dell SRM alerts dashboard. To clear the generated PowerFlex alert, you must either manually close/ acknowledge the alert in the Dell SRM alerts dashboard or wait for Dell SRM to clear the alert automatically."
- The UsedCapacity value for PowerFlex is temporarily increased with the addition of a PowerFlex Data Server Node. The UsedCapacity value returns to the correct value after some time.

- Storage Pool names in the reports are shown as prefixed with the respective protection domain names (*<PD name>-<SP name>*) to ensure uniqueness of Storage Pool names across different protection domains:
  - **Dashboards >> Storage >> Enterprise Capacity Dashboard >> Usable Capacity by Pool**
  - **Explore >> Storage Capacity >> Storage Pools**
  - **Explore >> Storage >> Storage Systems >> *<PowerFlex Device>* >> Capacity >> Usable Capacity by Pool**
  - **Report Library >> Dell PowerFlex >> Capacity >> Enterprise Capacity Dashboard >> Usable Capacity by Pool**
- `System Name` will be reported as `Serial Number` in case `System Name` is NULL in the device. To avoid this situation, `System Name` can be set by running following command in master MDM:

```
scli --rename_system --new_name <NAME>
```

- In SRM 4.8 Release, PowerFlex devices were identified as Block type devices. From SRM 4.9 release onwards, PowerFlex 4.x devices are identified as Unified devices. Due to this, a couple of new metrics are added and old metrics are turned inactive within 14-days. Until old metrics are turned inactive, few global reports continue to display data for both Block as well as Unified types. However, after the old metrics turn inactive, reports are displayed only for Unified type.

20

SolutionPack for Dell Unity/VNX/VNXe

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell EMC Unity allows you to visualize and report on performance and capacity data from your Unity systems.

The SolutionPack collects performance, topology, and capacity data from your Unity systems and displays the data in easy-to-use reports.

With this SolutionPack, you can unify your view of multiple Unity systems, including physical storage to host relationships. Capacity reports, such as Raw Capacity Usage, Usable Capacity, and Usable Capacity by Pool, help you to improve the availability of business critical applications and services by ensuring that those applications have the storage resources they need to operate effectively. Performance reports provide key performance indicators for such fundamental resources as LUNs, Disks, and File Systems.

NOTE: To collect carbon emission data for a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

NOTE: To link and launch CloudIQ, follow the steps in Link and launch CloudIQ. To view the CloudIQ health score of the Unity array, install and discover the CloudIQ SolutionPack as described in SolutionPack for CloudIQ.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Prerequisites

- Core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The Dell SRM Alerting Guide explains how to configure alerts consolidation.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.

7. Click **Next**.
   The window displays pre-configured alert details.
8. Make a selection in the **Alerting on data collection** field.
   If you select **Add a new Alerting on data collection**, select the appropriate value from the drop-down menu in the **Alerting Web-Service Instance** field.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.
    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.
    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. In **Event server hostname or IP address**, select the Backend host on which the Events Listener is installed.
14. In **Event server port number** select the port number for the event server.
15. Select **Configure Alert consolidation**.
16. In **Alert consolidation server hostname or IP address**, select the Primary Backend host.
17. In **Alert consolidation server port number**, select the port that is used for alert consolidation.
18. In **Naviseccli Path**, type the path if using a non-default path, or leave blank if you are using the default path.
19. Clear **Enable Snapshot collection** to disable Snapshot collection for Unity/VNXe arrays.
20. Optionally, select **Use advanced settings** to configure polling settings.
21. Click **Next**.
22. From the **Event database** drop-down menu, select existing settings that have been specified for other components, or select **Add a new Event database**.
    If you select **Add a new Event database**, type the information about the new event database.
23. Click **Next**.
24. In **Administration Web-Service Instance**, select the Frontend host.
25. Click **Install**.
26. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Next steps

After installing or updating a SolutionPack, new data will not be available for approximately three polling cycles. The data is available to the UI every hour with the Property Store task. This task can be run earlier, if wanted, by selecting the Property Store task found on the Frontend host.

Adding and configuring devices in Discovery

Steps

1. Go to **Centralized Management** > **Manage Discovery** > **Dell Unity/VNX/VNXe**.
2. Click **Add...**.
3. In **VNX type**, select **VNX Block Only**, **VNX NAS Gateway/eNAS**, **VNX Unified/File**, or **Unity/VNXe2**.
   If the following fields appear, enter the information that is specified:
   a. In **Unique friendly name for the Unity system**, type the name.

b. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key fields appear.
   NOTE: The unique Key field is enabled only when the Secure Vault checkbox is selected. When Secure Vault is not selected, there is no field to enter key and Password is active.
c. In **SP A IP**, type the IP address of the SPA.
d. In **SP B IP**, type the IP address of the SPB.
e. In **Use Naviseccli security file**, select this checkbox if you are using the security file.
f. In **Naviseccli User Scope**, select **LDAP**, **Global** or **Local**.
g. In **Naviseccli Username** and **Naviseccli Password**, type the Naviseccli credentials for the block storage systems.
h. If secure vault is enabled, in **Naviseccli Unique Key**, enter the unique key.
i. In **Primary control station IP**, type the IP address of the primary control station.
j. In **Secondary control station IP**, type the IP address of the secondary control station.
k. In **VNX File User Scope**, select **LDAP**, **Global**, or **Local**.
l. In **VNX File Username** and **VNX File Password**, type the credentials for the file storage system.
m. If secure vault is enabled, in **VNX File Unique Key**, enter the unique key.
n. In **Management IP or hostname**, type the IP address for the Unity/VNXe2 system.
o. In **Username**, type the username for the Unity/VNXe2 system.
p. In **Password**, type the password for the Unity/VNXe2 system.
q. If secure vault is enabled, in **Unique Key**, enter the unique key.

4. Click **Validate and Add** to validate the credentials.
   NOTE: This button tests array connectivity and credentials using the default user apg (Linux) or SYSTEM (Windows). If the VNX collector-manager is configured to run under a custom user (not the default) and uses a Naviseccli security file that is configured for that user, the test results will show failures. However, these can safely be ignored if the underlying collector-manager user & security file are correctly configured.
5. Click **Ok**.
6. Click **Save**.
7. Click **OK**.

Discovery troubleshooting

- Discovering same device again with a different “Unique Friendly Name” allows to add, but is not recommended since it results in duplicate reports in SRM frontend for the device.
- Dell Technologies does not recommend for “Unique Friendly Name” to contain “+” (plus sign) (Known issue SRS-33450 listed in SolutionPack Release Notes).
- The Test button results pop-up could incorrectly display Unity OE 4.1 as 4.0.2. This can happen if OE 4.0.1 was upgraded to 4.0.2 and then upgraded to 4.1.x (Known issue SRS-32062 listed in SolutionPack Release Notes).

Troubleshooting

Use this section to troubleshoot common errors.

Resolving creating stream errors

About this task

An error message, like the one shown below, will appear in the collection logs when the /opt/APG/Collecting/Stream-Collector/emc-vnx/./conf/output/vnxalerts-block-deviceid-1-laststarttime.xml files are deleted.

```
SEVERE - [2015-11-02 10:30:02 EST] - AbstractStreamHandlerJob::prepareNextStep(): Error
executing handler FileReaderRetriever containing 1 sub handlers
 com.watch4net.apg.ubertext.parsing.StreamHandlerException: Error while creating the
stream for file /opt/APG/Collecting/Stream-Collector/emc-vnx/./conf/output/vnxalerts-
block-deviceid-1-laststarttime.xml
```

```
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.newFileToRead(FileReader
Retriever.java:340)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.execute(FileReaderRetrie
ver.java:189)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.execute(FileReaderRetrie
ver.java:46)
 at
com.watch4net.apg.ubertext.parsing.AbstractForkingStreamHandler.handleExecution(AbstractF
orkingStreamHandler.java:122)
 at
com.watch4net.apg.ubertext.parsing.concurrent.AbstractStreamHandlerJob.prepareNextStep(Ab
stractStreamHandlerJob.java:180)
 at
com.watch4net.apg.ubertext.parsing.concurrent.ForkingStreamHandlerJob.step(ForkingStreamH
andlerJob.java:46)
 at
com.watch4net.apg.concurrent.executor.DefaultScheduledJobExecutor$ScheduledJob.step(Defau
ltScheduledJobExecutor.java:249)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.executeJobRunner(AbstractJobExe
cutor.java:122)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor.access$500(AbstractJobExecutor.
java:22)
 at
com.watch4net.apg.concurrent.executor.AbstractJobExecutor$JobRunnerImpl.run(AbstractJobEx
ecutor.java:274)
 at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1142)
 at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:617)
 at java.lang.Thread.run(Thread.java:745)
 Caused by: java.io.FileNotFoundException: /opt/APG/Collecting/Stream-Collector/emc-
vnx/./conf/output/vnxalerts-block-deviceid-1-laststarttime.xml (No such file or
directory)
 at java.io.FileInputStream.open0(Native Method)
 at java.io.FileInputStream.open(FileInputStream.java:195)
 at java.io.FileInputStream.<init>(FileInputStream.java:138)
 at
com.watch4net.apg.ubertext.parsing.retriever.FileReaderRetriever.newFileToRead(FileReader
Retriever.java:336)
 ... 12 more
```

To resolve this issue, follow the steps below.

Steps

1. Open an SSH (Linux) or RDP (Windows) session to the Storage Monitoring and Reporting server.
2. Navigate to `<install_location>/APG/bin`.
3. Type the following command:

   Linux: `./manage-modules.sh update emc-vmx-collect emc-vnx`

   Windows: `manage-modules.cmd update emc-vnx-collect emc-vnx`

Limitations

This section provides information about known limitations of the Dell EMC Unity SolutionPack.

Main Limitations:

- For the file system fields in the SMR report, source and destination file systems may show double entries instead of a single entry: **Report Library** > **Dell EMC VNX** > **Inventory** > **File Components** > **Replication**.
- DataMover fail-over leads to persistence of duplicate capacity metrics in the APG Database depending on the time period settings for changing the vstatus, these duplicate capacity metrics would become inactive.
- VNX Free Raw Disk Capacity values are not the same as Dell Unisphere Free Raw Capacity values. Unisphere Free Raw Capacity counts both internal operation space (vault drives) and the space available for user LUNs. Free Raw Disk Capacity only counts the space available for user LUNs.

- **Hot Spare** values are incorrect for VNX arrays running Operating Environment for Block/FLARE 05.33.x. In that version, the VNX series supports a new hot spare policy where any unbound disk is available for use as a hot spare. Therefore disks are not specifically marked as hot spares, but rather as unbound disks. As a result, hot spare disks are incorrectly counted as unconfigured capacity.
- .CSV files that were exported from Discovery Center with a release prior to Dell SMR 3.7 cannot be used to import devices into Dell SMR 4.0.
- During the first couple polling cycles when an array is discovered. The following error message appears in the logs; after that the message stops:

```
SEVERE   -- [2016-01-28 10:44:39 EST] -- FileDownloadingTask::run():
com.watch4net.apg.ssh.api.exception.SSHException: Remote directory './emc-srm/
server_2/3600' does not exist.
com.watch4net.apg.file.retriever.ClientException:
com.watch4net.apg.ssh.api.exception.SSHException: Remote directory './emc-srm/
server_2/3600' does not exist.
```

- The discovery of VNX/Unity/VNXe arrays using an IPv6 address in Discovery Center is not supported. Use the hostname which resolves to the respective IPv6 address when entering the details for SPA, SPB, and Control Station (for VNX) or for Management Host (for Unity/VNXe2).
- The following message appears in the logs when the SolutionPack collector-manager is first started. This problem is resolved when a device is added for discovery and the collector-manager is restarted.

```
WARNING – [2016-04-10 11:26:24 EDT] – SocketConnector::init(): Can't connect socket
to localhost:52001
 java.net.ConnectException: Connection refused
```

- The 'memberof' property displays multiple values for a while until the collection has time to normalize things if the `Current Owner` of a LUN on a Unity or VNXe2 array changes. The reports show multiple values for the 'memberof' property for Unity that means that for approximately one hour (by default or up to four hours if 60 minutes topology polling period is selected). The reports show multiple values for the 'memberof' property for VNXe2 that means that until the LUN metrics are marked inactive (approximately 24 hours),
- It is possible for existing VNX array LUNs to appear in the **Inactive Devices & Components** report. It occurs because the `memberof` property is part of the LUN variable id. The old instance of the metric will be tagged with an inactive `vstatus` property, if a LUN trespasses between storage processors.
- Rendering of workload placement reports for Dell Unity-VNXe2 Storage Pools and Dell EMC VNX Storage Pools may experience delays if the number of LUNs is large. This happens because performance metrics are aggregated from the LUNs within the Storage Pool, and these computations are performed during the report generation.

Difference in calculation of array-level Used Capacity between Unisphere and SMR

SMR Report Location: Explore -> Storage -> Storage Systems -> <Unity Array ID> -> Device Summary -> <Array Name> -> Capacity -> Storage Capacity Dashboard -> Charts with details -> Usable Capacity -> Used.

For Unified/Block Arrays:

Used (in Unisphere) = TotalCapacity - UnusedDiskCapacity - FreeRGCapacity - Free Space for File (applicable for Unified systems only)

Used (in SMR) = Sum of all LUNs' `UsedCapacity` metric where isused==1, plus PoolOverhead.

Reasons for LUN to be considered `Used` (isused==1):

- LUN is both masked and mapped – which means it is host accessible. It is for both thin and thick LUNs.
- System Resource
- Pool Contributor for snap pool and replica pool
- Used by File or Virtual system
- Part of a replica chain and its primary LUN is used – replica chain that is determined by Topology Service using replica LUN source/target.

For Unity Arrays:

Used (in Unisphere) = Sum of all Pools' consumed space

Used (in SMR): For calculation, considered LUNs where is used==1 only, (either (a) when it is both mapped and masked or (b) when it is Used by File or Virtual System.), and not all possible LUNs carved out of the pool.

Generally, the main interest when looking at the array-level `Used` capacity is to understand how much space is used across all Storage Pools and/or RAID Groups on the array. If it is the wanted information, go to **Explore > Storage Capacity > Enterprise Capacity** and scroll over to view the Pool Used (GB) column.

NOTE:

Unity Rest APIs are not capable of providing data for real-time metrics with polling interval more than 5 minutes. Due to this limitation, the performance polling period option that is provided in the UI Configuration will now be applicable for historical data collections only. For more information, see KB article KB000181934.

21

SolutionPack for Dell EMC VMAX

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell EMC VMAX collects and reports capacity, topology, alerts, and performance data for Symmetrix VMAX3 and VMAX All Flash arrays and components such as pools, disks, directors, ports, storage groups, devices, and replication.

Configuring the access credentials

Dell M&R uses different accounts when running SolutionPacks.

About this task

SMI-S Provider default credentials are provided during SolutionPack installation:

- Username - the default is **admin**
- Password - the default is **#1Password**

Unisphere for VMAX credentials:

- Username - the default is **smc**
- Password - the default is **smc**

Preparing Dell EMC VMAX for discovery and data collection

Identify the information that is required to support data collection before installing the SolutionPack for Dell EMC VMAX and perform the necessary pre-configuration.

The host running Unisphere for VMAX and the Dell SRM collector host must have the same date and time and must be in same time zone. Otherwise, if the Dell SRM collector host's clock is too far ahead of the Unisphere host's clock, the Dell SRM collector may not return performance data.

VMAX3/VMAX All Flash discovery scenario

Array Provider Host

VMAX3 and VMAX All Flash arrays are collected using Unisphere and optionally VMAX SMI-S Provider for VMAX. The SMI-S Provider is used to collect capacity, topology, basic performance data, and LUN performance data. Unisphere for VMAX can be used to collect the basic performance data as well as several additional performance data, but it cannot collect LUN performance data. Therefore, the VMAX collector should be configured to use both the SMI-S Provider and Unisphere for VMAX so that all VMAX report fields will have data. Dell Technologies recommends that both the SMI-S Provider and Unisphere for VMAX are installed to the same Array Provider Host. This Array Provider Host should have six or more dedicated gatekeepers for each VMAX array that is connected to it.

"Remote Discovery Configuration" is referred to when SMI-S Provider and Unisphere are installed on an Array Provider Host which is separate from the VMAX Collector Host. The minimum Array Provider Host configuration is 4 CPUs and 16 GB memory. More memory is required when managing more than 50k total devices, with a maximum of 100k devices per Array Provider Host. See the Unisphere for VMAX Release Notes to determine the Array Provider Host's scalability and CPU/Memory requirements.

The SMI-S Provider and Unisphere for VMAX can be installed on the Dell SRM Collector Host (this is referred to as "Local Discovery Configuration"). Local Discovery Configuration requires a minimum of 4 to 8 CPUs and 32GB memory to support the VMAX Collector as well as the SMI-S Provider and Unisphere for VMAX. Sufficient memory and CPU must be provided on the Collector Host to support all these components as well as any other hosted collectors or processes.

Unisphere for VMAX and the SMI-S Provider will gather performance data for arrays that are directly SAN-attached to the Array Provider Host (called a "Local connection" to the array). Performance data is not available for arrays that are indirectly attached to the Array Provider Host through another array's SRDF connection (called a "Remote connection" to the array). Arrays must be registered in the Unisphere for VMAX Performance UI to provide performance data. Once performance data is available in Unisphere/SMI-S and the array is collected, it may take 2 to 3 hours before the performance data will be seen in the VMAX reports.

Collector Host (Remote Discovery Configuration)

Collector Hosts are installed with the SolutionPack for Dell EMC VMAX and configured to connect to the SMI-S Provider and Unisphere for VMAX on the Array Provider Host. See the *Dell SRM Performance & Scalability Guidelines* for SolutionPack for Dell EMC VMAX planning based on the number of arrays and array configurations being managed. As a rule, Dell SRM Collector Hosts should be installed as near as possible to the Array Provider Host to avoid network latency between the collector and SMI-S Provider and Unisphere. Dell Technologies highly recommends that Collector Hosts be in the same data center as the Unisphere and SMI-S Provider. At minimum the Unisphere Host should be in the same time zone as the Collector Host. Or, the Unisphere Host should have its clock synchronized with the Collector Host.

Verifying the configuration

Verify the VMAX collector configuration is correct by using the Discovery Center Test option for each VMAX array. Tests performed include basic SMI-S/Unisphere connectivity tests, SMI-S/Unisphere version checks, and an array existence test. The configured discovery settings can be confirmed by using the Test utility as described in Troubleshooting Discovery Center connectivity failures. Alternately, the SMI-S `TestSmiProvider` utility's `dv` command can be used to confirm the software version and connected arrays on the Array Provider Host.

```
# cd /opt/emc/ECIM/ECOM/bin or ?:\Program Files\EMC\ECIM\ECOM\bin
#./TestSmiProvider or TestSmiProvider.exe
SolutionPack for EMC VMAX
Configuring the access credentials 103
Connection Type (ssl,no_ssl,native) [no_ssl]:
Host [localhost]:
Port [5988]:
Username [admin]:
Password [#1Password]:
Log output to console [y|n (default y)]:
Log output to file [y|n (default y)]:
Logfile path [Testsmiprovider.log]:
Connecting to localhost:5988
….
Namespace: root/emc
repeat count: 1
(localhost:5988) ? dv
```

```
++++ Display version information ++++
Solutions Enabler version: V8.x.y.z

Firmware version information:
(Local) VMAX 000283700466 (VMAX200K) : 5977.477.457
(Local) VMAX 000283700467 (VMAX200K) : 5977.477.457
(Local) VMAX 000283700472 (VMAX200K) : 5977.477.457
```

Verify connectivity with the SMI-S Provider and Unisphere on the Dell SRM Collector Appliance via Discovery Center using the **Test** button.

Creating collectors for discovery of Symmetrix arrays (local discovery configuration)

The following procedure describes how to create VMAX collectors for discovery of all Symmetrix arrays (VMAX3 and VMAX All Flash) in Dell SRM.

Steps

1. Create a Windows (2008, 2012, 2012R2) or Linux (RH 5+, Suse 10+) Vmguest with eight RDM gatekeepers allocated to the server from each local Symmetrix array (have been tested for 60,000 volumes total).
2. Size the server as follows: 4–8 CPUs, 32 GB RAM, 200 GB Storage.
3. Install Solutions Enabler with SMI-S and Unisphere for VMAX on the VMAX collector server. This server will only be used for Dell SRM data collection (no production allocation use).
4. Ensure that the server can see no more than 50,000 Symmetrix volumes (64,000 for jumbo arrays) and be sure to leave room for growth. Run symcfg list from Solutions Enabler to verify.
5. Create a symavoid file if too many Symmetrix arrays are visible until you get the volume count on the server below 50,000 volumes (64,000 for jumbo arrays) and be sure to allow for growth. You will be blocking the remote arrays as well in the symavoid file. Remote arrays will be discovered in remote datacenters locally by a VMAX collector server there.
6. Install Dell SRM collector software on this server. Add this server to Dell SRM as a scale out collector.
7. Install only the Dell EMC VMAX SolutionPack collector on this server.
8. Set the Java heap for the VMAX collector to 8 GB (8192).

   The VMAX Collector's default Java heap size is configured as 4 GB (4096). Additional heap may be required for large Solutions Enabler environments with multiple arrays. See the *Dell SRM Performance and Scalability guidelines* for more information.
9. In Dell SRM, use only the local discovery option and type the Solutions Enabler install directory, if it is not the default.
10. This server will be used to fill in the Unisphere for VMAX and SMI-S fields for discovery in Dell SRM.

Configuring VMAX arrays for consolidation of availability alerts

Use this procedure to configure forwarding of availability alert traps (SNMP v1) from VMAX arrays.

About this task

VMAX performance alerts are collected using the discovery data collection configuration.

Steps

1. Log into Solutions Enabler on the array provider host as an administrator.
2. Navigate to the `daemon_options` file in the `C:\Program Files\EMC\SYMAPI\config\` directory.
3. In the parameter section `SNMP_TRAP_CLIENT_REGISTRATION`:
   a. Uncomment the line `storevntd:SNMP_TRAP_CLIENT_REGISTRATION`
   b. Add the Dell SRM trap recipient IP to the trap filter. In a single vApp installation, this is the Dell SRM IP, and in a distributed environment, is the Primary Backend server's IP.

      The syntax is ***<IP>,<port>,<filter>,<state>***, where ***<filter>*** is the filtering level for trap forwarding defined in the `FCMGMT-MIB` file.

      Example: 1**0.31.90.148, 2041,10,ACTIVE**

4. In the parameter section `LOG_EVENT_TARGETS`, uncomment the line `storevntd:LOG_EVENT_TARGETS = snmp file`.
5. To identify the arrays from which traps should be forwarded to the suite, type **`symcfg list`**, and press **Enter**.
6. For each array that should forward alert traps to Dell SRM:
   a. Type **`symcfg list`**, and press **Enter**.
   b. In the parameter section `LOG_SYMMETRIX_EVENTS`, specify the appropriate event categories in the format:

      `sid=<SYM serial number>, <event category 1>, <event category 2>\`

      Example: `SID=000194900854, disk, device, device pool, director, srdf consistency group, srdfa session, srdf link, srdf system, service processor, environmental, diagnostic, checksum, status, events, array subsystem, groups, optimizer, thresh_critical=3, thresh_major=2, thresh_warning=1, thresh_info=0 ;\`
7. To reload the changes to the `daemon_options` file, type **`stordaemon action storevntd -cmd reload`**, and press **Enter**.
8. Ensure that the storevntd Event Daemon is running on the provider host.
9. If you have multiple VMAX array provider hosts in your storage environment, repeat this procedure on each array provider host.

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The *Dell SRM Alerting Guide* explains how to configure alerts consolidation.
- Data collection instances are based on the topology collection type.

NOTE: Use only one SolutionPack, either the SolutionPack for Dell EMC VMAX or the SolutionPack for Dell VMAX/PowerMax, to collect data from VMAX3 and VMAX All Flash arrays. Using both SolutionPacks to collect data from the same array consumes significant collector resources and can have potential consequences to reports and chargeback calculations.

The SolutionPack for Dell VMAX/PowerMax comes with some limitations when compared to the existing SolutionPack for Dell EMC VMAX. Notably, there is no LUN performance, Disk, Disk Group, or Data Pool metrics that will be collected. LUN capacity and topology metrics are still collected. Storage Group performance and SLO compliance metrics should be used in lieu of LUN performance metrics. And, Storage Resource Pool (SRP) capacity and performance metrics should be used as an alternative to the metrics for the SRP's underlying subcomponents (that is, Disks, Disk Groups, and Data Pools that make up the SRP).

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select **Dell EMC VMAX**.
4. Click **Install**.
5. Type the instance name.
   The instance is based on topology type SMI-S.
6. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays a note about Alert Consolidation.
8. Click **Next**.
   The window displays pre-configured alert details.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.

12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

13. From the **Type of topology collection** drop-down menu, select **SMI-S** (SYMCLI support removed for VMAX arrays).
14. Configure the collection intervals as needed.
15. Click **Next**.
    The window displays reports settings.
16. Click **Install**.
17. Click **Ok** when the installation is complete.

Adding and configuring devices in Discovery Center

Use the following procedures to add and configure VMAX3 and VMAX All Flash devices in Discovery Center.

Adding VMAX3 arrays

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Dell EMC VMAX**.
3. Click **Add...**.
4. In **Server**, select the server where the device is dispatched.
5. In **Instance**, select the instance of the emc-vmax-collect where the device is dispatched.
6. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the SMI-S Provider Unique Key and Unisphere Unique Key fields appear.

   NOTE: The SMI-S Provider Unique Key and Unisphere Unique Key fields are enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, SMI-S Provider Password and Unisphere Password are active.

7. In **Type of Symmetrix array to collect**, select **VMAX3**.
8. In **Array full serial number**, type the full serial number for which data is collected.
   To view the list of arrays, type * in place of the serial number and click **Validate and Add**.

   NOTE: Dell Technologies recommends not to exceed six medium-sized (30K-40K devices) VMAX arrays for each VMAX collector.

9. In **Type of performance collection (excluding LUN)**, select the type of source for performance metrics that are related to the array and its components (except LUN).

Option	Description
None	Do not collect performance metrics
SMI-S	Collect performance metrics using SMI-S
Unisphere for VMAX	Collect performance metrics using Unisphere for VMAX

10. In **Type of performance collection for LUN**, select the type of source for performance metrics that are related to the array LUNs.

Option	Description
None	Do not collect LUN performance metrics
SMI-S	Collect LUN performance metrics using SMI-S

11. Check **Enable SRDF groups collection** if you want to see fully populated SRDF reports.
12. Type the following settings in the **SMI-S configuration** section:
    a. In **SMI-S Provider/CIMOM host**, type the name, FQDN, or IP address of the SMI-S provider host.
    b. In **SMI-S Provider username** and **SMI-S Provider password**, type the SMI-S credentials to use.
    c. If the secure vault is enabled, in **SMI-S Provider Unique Key** enter the unique key.
    d. Check **Use advanced settings**.
    e. In **SMI-S Provider/CIMOM port**, type the port on which the SMI-S provider is listening if it is different from the default port.
    f. To enable SSL for all communications between the collector and the SMI-S provider, check **SMI-S Provider enable secure connection (SSL)**
13. If you are collecting performance data using Unisphere for VMAX, type the following settings in the **Unisphere for VMAX configuration** section:
    a. In **Unisphere hostname or IP address**, type the name, FQDN, or IP address of the Unisphere for VMAX host.
    b. In **Unisphere username** and **Unisphere password**, type the Unisphere for VMAX credentials to use.
    c. If the secure vault is enabled, in **SMI-S Provider Unique Key** enter the unique key.
    d. Check **Use advanced settings**.
    e. In **Unisphere network port**, type the port on which Unisphere for VMAX is listening.
    f. To collect additional performance metrics (maximum values of some of the metrics usually collected), check **Collect MAX values from Unisphere**.
14. To validate the credentials, click **Validate and Add**.

    For information about connectivity test failures, see Troubleshooting Discovery Center connectivity failures.
15. Click **Ok**.
16. Click **Save**.

    Performance data is displayed in about an hour.

    Discovery of large (> 20K devices) Symmetrix arrays may take long periods of time due to the number of volumes. To address this issue, discover the Symmetrix on its own instance. This prevents the discovery from impacting the discovery of other arrays on the same SYMAPI connection and allows the smaller arrays to complete during the polling schedule.

Adding VMAX All Flash Arrays

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Dell EMC VMAX**.
3. Click **Add...**
4. In **Type of array to collect**, select **VMAX ALL Flash**.
5. In **Array full serial number**, type the full serial number for which data is collected.
   To view the list of arrays, type * in place of the serial number and click **Validate and Add**.

   NOTE: Dell Technologies recommends not to exceed six medium-sized (30K-40K devices) VMAX arrays for each VMAX collector.
6. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the SMI-S Provider Unique Key and Unisphere Unique Key fields appear.

   NOTE: The SMI-S Provider Unique Key and Unisphere Unique Key fields are enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, SMI-S Provider Password and Unisphere Password are active.
7. Type the following settings in the **SMI-S configuration** section:
    a. In **SMI-S Provider/CIMOM host**, type the name, FQDN, or IP address of the SMI-S provider host.

b. In **SMI-S Provider username** and **SMI-S Provider password**, type the SMI-S credentials to use.
c. If the secure vault is enabled, in **SMI-S Provider Unique Key** enter the unique key.
d. Check **Use advanced settings**.
e. In **SMI-S Provider/CIMOM port**, type the port on which the SMI-S provider is listening if it is different from the default port.
f. To enable SSL for all communications between the collector and the SMI-S provider, check **SMI-S Provider enable secure connection (SSL)**.

8. Type the following settings in the **Unisphere for VMAX configuration** section:
   a. In **Unisphere hostname or IP address**, type the name, FQDN, or IP address of the Unisphere for VMAX host.
   b. In **Unisphere username** and **Unisphere password**, type the Unisphere for VMAX credentials to use.
   c. If the secure vault is enabled, in **SMI-S Provider Unique Key** enter the unique key.
   d. Check **Use advanced settings**.
   e. In **Unisphere network port**, type the port on which Unisphere for VMAX is listening.
   f. To collect additional performance metrics (maximum values of some of the metrics usually collected), check **Collect MAX values from Unisphere**.
9. To validate the credentials, click **Validate and Add**.

   For information about connectivity test failures, see Troubleshooting Discovery Center connectivity failures.
10. Click **Ok**.
11. Click **Save**.

    Performance data is displayed in about an hour.

    Discovery of large (> 20K devices) Symmetrix arrays may take long periods of time due to the number of volumes. To address this, discover the Symmetrix on its own instance. This prevents the discovery from impacting the discovery of other arrays on the same SYMAPI connection and allows the smaller arrays to complete during the polling schedule.

Troubleshooting Discovery Center connectivity failures

Discovery Center enables you to test connectivity between the Dell SRM VMAX collector and the VMAX array providers.

Viewing the Test button test results

Test results are displayed in the **Test Connectivity** button tool tip.

About this task

In addition to providing error and warning messages, the test results tool tip also provides useful information such as: SYMCLI version, SYMAPI version, SYMAPI Run Time version, SYMAPI Server version, number of dedicated gate keepers per array, and SYMAUTH users.

Steps

1. Go to **DISCOVERY** > **Discovery Center** > **Manage Discovery** > **Dell EMC VMAX**.
2. Select a device and click **Test Connectivity**.
3. Once the connectivity test is completed, click the status icon to display the test results tool tip.
4. Click **Click to show/hide the full result**.
   The tool tip expands to display the full test results.

Example test results

```
SYMCLI tests skipped: SYMCLI not configured on the selected instance

Testing SMI-S configuration
Trying to connect to SMI-S provider at https://losam033:5989/cimom
Successfully connected to SMI-S provider and verified it is an ECOM SMI-S Provider
Detected Solutions Enabler version V8.4.0.0
Detected SMI-S Provider version V8.4.0.0
Validated SE V8.4.0.0 with SMI-S Provider V8.4.0.0 is at or above the recommended version
```

```
Retrieved all array instance names
Validated serial number 000196701343 was found on SMI-S Provider
Detected 000196701343 microcode version: 5977.1124.1125
Detected VMAX3 array based on microcode >= 5977
Validated detected VMAX3 array type matches selected type.
Serial number 000196701343 is a VMAX3 array (SRP storage pool detected).
Serial number 000196701343 is LOCAL to SMI-S provider losam033

Testing Unisphere configuration(s)
Trying to connect to Unisphere at https://losam033:8443/univmax
Successfully connected to Unisphere
Found UNIVMAXPA version V8.4.0.4 registered with Unisphere
Validated Unisphere V8.4.0.4 is at recommended version 8.4.0.0 or a slightly higher
version.
Serial number 000196701343 is registered for Performance with Unisphere losam033
```

Understanding the test messages

This section describes common test result messages.

Serial number errors

```
>>>ERROR: Serial number <serial_number> NOT found on SYMCLI provider. Enter * to see the
list of available serial numbers.
```

The above message is displayed when the provided serial number cannot be found on the Solutions Enabler server.

To get a complete list of the available serial numbers behind the Solutions Enabler host, enter ***** in **Array Full Serial Number** and click **Test**.

```
>>>ERROR: <serial_number> was detected as VMAX3 based on microcode '5997' but VMAX/VMAX2
was selected.
```

The above message is displayed when a VMAX3 serial number is entered when VMAX/VMAX2 was selected during SolutionPack installation.

Unisphere connectivity failure

```
>>>ERROR: Could not connect to Unisphere at https://losam034:8443/univmax. Verify the
Unisphere configuration. Also ensure that the Unisphere Performance Analysis has been
licensed and enabled.
```

Ensure that the Unisphere's host's Unisphere service/daemon is running and is network accessible. Verify port, SSL, credentials, and firewall configuration. In order for Dell SRM to obtain all performance data, arrays should be registered with Unisphere for performance collection.

In order for performance to be available through Unisphere the array must have LOCAL connectivity. In other words, the array should have gatekeeper devices on the Unisphere host.

SMI-S Provider connectivity failure

```
>>> ERROR: Could not connect to SMI-S provider at https://losam034:5989/cimom. Verify
the SMI-S configuration.
```

Ensure that the SMI-S Provider host's ECOM service/daemon is running and is network accessible. Verify port, SSL, and firewall configuration.

Updating SolutionPack alert definitions

During SolutionPack update, any new alert definitions that are supported in the updated version do not get updated by default. This is expected behavior.

About this task

To add newly introduced alert definitions after updating, follow the steps below.

Steps

1. Go to **Config** > **SolutionPacks** > **Installed SolutionPacks** > **Dell EMC VMAX**.
2. In the table, click the pen icon button to the left of **Pre-configured alerts**.
3. Click **Reconfigure**.
   Go to **Config** > **Alerts** > **Manage Alert Definitions** > **Dell EMC VMAX** to see the newly added alert definitions.

Configuring Solutions Enabler client access for VMAX

Symmetrix Authorization using symauth provides secure user-based authorization and symacl provides host-based authorization. Use this procedure in environments in which Symmetrix Authorization is enabled.

Prerequisites

Ensure that you have configured an appropriate Solutions Enabler scenario as described in Preparing Dell EMC VMAX for discovery and data collection .

For more detailed information about Solutions Enabler, refer to the following documents:

- *Dell EMC Solutions Enabler Symmetrix Array Management Product Guide*
- *Dell EMC Solutions Enabler Symmetrix Security Configuration Guide*

About this task

The following configuration procedures are specific to a Solutions Enabler proxy configuration. However, you can also use these procedures for a local Solutions Enabler configuration in which the Dell SRM Collector software is installed directly on the existing SYMAPI Solutions Enabler server. The term "client" refers to the host where the Collector software has been installed.

When symauth is enabled, check that the user 'apg' is present in the user list and that the role is **Monitor** or **Storage Admin** or **Admin** to access masking and mapping data. You can check the user role using the Discovery Center **Test** button. For more information, see Viewing the Test button test results.

Steps

1. Validate if Symmetrix Authorization is enabled by running the `symauth list` command on the host that has direct FC connectivity to the arrays to be managed.
2. Check the status displayed in the the `Authorization Control` section to determine the required action:

Option	Description
Disabled	Symmetrix Authorization is not configured. In this case, do nothing.
Enabled	Symmetrix Authorization is configured. In this case, you must configure the apg user and Dell SRM hosts that will be issuing commands. Continue to step 3.

3. If Symmetrix Authorization is enabled, use the following procedures to complete the configuration:
   a. Configuring host access
   b. Adding client hosts to existing SYMAUTH configuration
   c. Enabling client authorization
   d. Validating Symmetrix access controls

Configuring host access

Enable the Dell SRM apg account to access the local Solutions Enabler resources and logs.

About this task

This procedure provides an example of configuring access on a host using the Linux operating system.

Steps

1. Log in to the Solutions Enabler client host.
2. Navigate to `/var/symapi`
3. Grant the `apg` user write access to the following Solutions Enabler directories and contents:
   a. **`chown -R apg <SYMAPI_HOME>/config`**
   b. **`chown -R apg <SYMAPI_HOME>/db`**
4. Repeat steps 1-3 for each VMAX Collector server.
5. Grant the `apg` user authorization for the Solutions Enabler storapid daemon by navigating to *`<SYMAPI_HOME>`*`/config/daemon_users` and adding the following line to the `storapid[Base Daemon]` section of the file:
   `apg storapid <all>`
6. Save and exit the `daemon_users` file.
7. Set a password for the `apg` user.
8. Repeat steps 5-7 for each VMAX collector server.
9. Log out and log in as the `apg` user and run **`symauth show -username`** to determine the fully-qualified account name.
10. Make note of the value displayed in `your current username`. For example: `H:`*`system_name`*`\apg`
11. Repeat steps 9-11 for each VMAX Collector server.

Adding client hosts to existing SYMAUTH configuration

Enable the apg user with read-only monitoring access for VMAX arrays using Solutions Enabler User Authorization.

Prerequisites

Complete the procedure described in Configuring host access.

You must be logged in as Root or Administrator.

About this task

Perform the following procedure for each VMAX you want to enable Dell SRM to access.

Steps

1. Run the **`symauth -sid <SID> list`** command to determine if User Authorization Control is enabled on the local client system.
   - If User Authorization Control is disabled (`Disabled`) for the specific VMAX, proceed to Enabling client authorization.
   - If User Authorization Control is enabled (`Enabled`) and in use (`Enforced`) for the specific VMAX, continue with this procedure.
2. Ensure that you are logged in with an existing privileged account (e.g., root or administrator).
3. Use the **`find / -name auth.txt`** command to find the `auth.txt` file.
4. Navigate to the folder with the `auth.txt` file.
5. Edit the file to include a line based on the results obtained from performing the procedure described in Configuring host access. For example:
   `assign user H:`*`system_name`*`\apg to role Admin;`
6. Save the file.
7. Use the **`symauth -sid <SID> -f auth.txt`** command to commit changes to the User Authorization User-to-Role map.
8. Repeat this procedure for each VMAX array.

Enabling client authorization

Use this procedure when User Authorization Control is disabled (`Disabled`) for the specific VMAX and you want to restrict the `apg` user to a monitoring role without limiting other accounts in the environment.

Prerequisites

You determined that User Authorization Control is disabled by performing the task described in Adding client hosts to existing SYMAUTH configuration.

You are logged in to the client host with local root or administrator credentials.

Steps

1. Create an `auth.txt` file with the following contents:

   ```
   assign user * to role Admin;
   set enforcement enforce;
   assign user H:system_name\apg to role Admin;
   ```

2. Repeat step 1 for each VMAX Collector server.
3. Use the **symauth -sid <SID> -f auth.txt** command to commit changes to the User Authorization User-to-Role map.
4. Repeat step 3 for each VMAX array.
5. Use the **symauth -sid <SID> enable** command to enable User Authorization Control for a specific VMAX array.
6. Repeat step 5 for each VMAX array.
7. Use the symauth list command to validate that User Authorization Control is enabled and enforced.

```
   S Y M M E T R I X   A U T H O R I Z A T I O N   S T A T U S

Symmetrix ID: 000195700363

  Authorization Control           : Enabled

  Time Enabled                    : Mon Aug  5 12:51:08 2013
  Time Disabled                   : Thu Aug  1 15:54:23 2013
  Time Updated                    : Mon Aug  5 12:51:08 2013

  Enforcement Mode                : Enforce
  Server Policy                   : Trust clients
```

Validating Symmetrix access controls

Validate that the Symmetrix Access Control (SymACL) security feature is enabled and in use on VMAX systems.

Prerequisites

You are logged in to the client host with local root or administrator credentials.

About this task

In order for all masking and mapping details to be collected, the Solutions Enabler host should belong to an Access Group that has been granted VLOGIX permissions for the ALL_DEVS access pool.

Steps

1. Run the `symacl list` command for each VMAX array. Status information is displayed.

```
   S Y M M E T R I X   A C C E S S   C O N T R O L   S T A T U S

Symmetrix ID: 000195700363

    Access     Session
    Control    Locked   Time Last Updated
```

```
    --------  -------  -------------------------
    N/A       N/A      N/A

Symmetrix ID: 000195700932

    Access    Session
    Control   Locked   Time Last Updated
    --------  -------  -------------------------
    N/A       N/A      N/A
```

- If the Access Control field indicates N/A, SymACL is not enabled on this VMAX system. No action is necessary.
- If the Access Control field indicates `Enabled`, continue this procedure to secure Dell SRM client systems from a host system in the existing `SymACL AdminGrp` for each VMAX system.

2. Create a SymACL access group appropriate to contain the Dell SRM client systems (e.g., SRMGRP)
3. Add each client system's unique identifier to the access group.
4. Repeat for each Dell SRM client host system.
5. Grant BASE access rights to the access group just created for all devices (ALL_DEVS).
6. Repeat this procedure for each VMAX system monitored by Dell SRM.

Limitation: some alerts not displayed

Dell SRM fails to receive and display some alerts

About this task

If a trap is lost in the network communication, Solutions Enabler is not aware of the host and is not able to resend the lost information.

Resolving SMI-S Provider port conflicts

Some versions of Microsoft Windows may have a WMI component that causes a port conflict with the SMI-S Provider. This has been observed on Windows Server 2012 R2 with the 8.x SMI-S Provider.

About this task

When there is a port conflict, the SMI-S Provider service will start and then immediately shut down. The cimom.log file on the Provider host will have errors similar to: `CIMOM: Failure to start listener on port - 5985`, as shown in the following example:

```
15-Sep-2015 14:39:26.474 -8488-E- WebServer: Http Server Listener unable to listen on
address and port: [0:0:0:0:0:0:0:0]:5985
15-Sep-2015 14:39:26.474 -8488-E- WebServer: NAVSocket::bind() returned error Permission
denied (on [0:0:0:0:0:0:0:0]:5985) :
15-Sep-2015 14:39:33.443 -2892-E- CIMOM: Failure to start listener on port - 5985,
interface - ::.
15-Sep-2015 14:39:33.458 -2892-E- NAVHTTPServerListenerJoiner::setTotal: Total
NAVHTTPServerListener threads: 18446744073709551615, code=1
15-Sep-2015 14:39:33.458 -2892-E- CIMOM: Shutting down ECOM...
```

Steps

1. Login to the SMI-S Provider host.
2. In Windows Explorer, navigate to `C:\Program Files\EMC\ECIM\ECOM\conf\Port_settings.xml`, right-click the file, select **Properties**, uncheck the **Read only** attribute, and click **OK**.
3. Open `C:\Program Files\EMC\ECIM\ECOM\conf\Port_settings.xml` in a text editor and change the `"Port2"` `<port>` value from `5985` to `6985`, as shown below:

```
<ECOMSetting Name="Port2">
<!--
       <portRange>5985</portRange>
-->
```

```
    <port>6985</port>
    <secure>false</secure>
    <slp>true</slp>
</ECOMSetting>
```

4. Restart the SMI-S Provider service and verify that it does not shutdown within a few seconds of being started.

Limitations

- CSV files that were exported from Discovery Center with Dell SRM 4.0 cannot be used to import devices into ViPR SRM 4.1 or later.
- When using SMI-S for data collection of VMAX2 devices, the **# Devices** column displays 0 for FICON Directors and FICON director ports. The SMI-S provider does not currently provide this information.
- After upgrading, it is possible that some VMAX devices will not collect Unisphere for VMAX performance metrics. This can occur because only the first Unisphere for VMAX host in the SolutionPack configuration is configured to collect metrics after the upgrade while others are ignored. Dell Technologies recommends running the Test script in Discovery Center on all VMAX devices to identify the devices that must be reconfigured.
- With the new support for Federated Tier Storage (FTS) in VMAX/XtremIO, the flash storage from XtremIO can be mapped into VMAX as external capacity. With both XtremIO and VMAX arrays discovered into Dell SRM, the FTS capacity is accounted for in both VMAX and XtremIO array capacities, which will result in the Total rows in the global reports double counting the capacities.
- The **Subscribed** column of the **Pools** report (**Report Library >> Dell EMC VMAX >> Inventory**) is incorrect when the pool is over subscribed. The SMI-S Provider included with the required Solutions Enabler 8.2.0.18 includes this fix.
- **Dell EMC VMAX > Inventory > Ports** report shows empty columns for the iSCSI virtual ports. Port, WWN, WWPN, Port Status, and Availability columns are empty for virtual ports. Masking and Mapping details are also not available for these iSCSI ports.
- **Performance > SG SLO Compliance** report is designed to exclude storage groups having an SLO Compliance of “NONE”.
- EMC VMAX SolutionPack only collects Storage Group performance using Unisphere. Storage Group performance is not collected using SMI-S Provider. Performance collection using SMI-S Provider only collects performance data for Array, BE director, FE Director, FE Ports, RDF Director, Disk, and Volume. Unisphere provides many additional performance metrics over the SMI-S Provider.
- Port Reports shows empty columns for the iSCSI virtual ports if the array has iSCSI virtual port that is attached to Directors. Port, WWNN, WWPN, Port status, and Availability columns are blank.
- Based on new metrics calculation in 9.0 SE, **Subscribed** and **Oversubscribed values** differs for Non-PowerMax arrays discovered under 9.0 SMI compared to 8.4 SMI.
- Rendering of workload placement reports for Dell EMC VMAX Storage Pools may experience delays if the number of LUNs is large. This happens because performance metrics are aggregated from the LUNs within the Storage Pool, and these computations are performed during the report generation.

22

SolutionPack for Dell VMAX/PowerMax

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell VMAX/PowerMax collects capacity, topology, and performance information for arrays using the PowerMax OS (microcode 5977). Supported array families include VMAX3 and VMAX All Flash arrays.

NOTE: VMAX/HyperMax SolutionPack is now called as the Dell VMAX/PowerMax SolutionPack. `emc-vmax-hypermax` is the instance name when this SolutionPack is installed.

NOTE: To link and launch CloudIQ, follow the steps in Link and launch CloudIQ. To view the CloudIQ health score of the PowerMax array, install and discover the CloudIQ SolutionPack as described in SolutionPack for CloudIQ.

Configuring the access credentials

Dell M&R uses different accounts when running SolutionPacks.

About this task

Unisphere for VMAX credentials:

- Username - the default is **smc**
- Password - the default is **smc**

Preparing Dell VMAX/PowerMax for discovery and data collection

Identify the information that is required to support data collection before installing the SolutionPack for Dell VMAX/PowerMax and perform the necessary pre-configuration.

VMAX3/VMAX All Flash discovery scenario

Array Provider Host

All the metrics for VMAX3 and VMAX All Flash arrays are collected using the Unisphere REST API. Hence the PowerMax collector should be configured to use Unisphere so that all PowerMax report fields will have data. This Array Provider Host should have six or more dedicated gatekeeper devices for each PowerMax array that is connected to it.

Remote discovery configuration is referred to when Unisphere is installed on an Array Provider Host which is separate from the PowerMax Collector Host. The minimum Array Provider Host configuration is 4 CPUs and 16 GB memory. More memory will be required when managing more than 50k total devices, with a maximum of 100k devices per Array Provider Host. Refer to the Unisphere for VMAX Release Notes to determine the Array Provider Host's scalability and CPU/Memory requirements.

The PowerMax Collector can be installed directly on an existing Unisphere for VMAX host (referred to as local discovery configuration) if it has enough resources to support the collector processes. Local Discovery Configuration requires a minimum of 4 to 8 CPUs and 32GB memory to support the PowerMax Collector as well as Unisphere for VMAX. More memory and CPU may be necessary to support other hosted collectors and/or any non-Dell SRM processes.

Unisphere performance

Unisphere for VMAX will gather performance data for arrays that are:

- Directly SAN-attached to the Array Provider Host
- Gatekeeper devices that are created on the Unisphere host (creating a "Local connection" to the array)
- Registered with Unisphere for performance collection

Performance data is not available for arrays that are:

- Indirectly attached to the Array Provider Host through a local array's SRDF connection (called a "Remote connection" to the array)
- Not registered with Unisphere for performance collection

Once performance data is available in Unisphere and the array is collected by the PowerMax collector, it may take 1 hour to 2 hours before the performance data will be seen in the PowerMax reports.

Collector Host (Remote Discovery Configuration)

Collector Hosts are installed with the SolutionPack for Dell VMAX PowerMax and configured to connect to the Unisphere for VMAX on the Array Provider Host. Refer to the Dell SRM Performance & Scalability Guidelines for SolutionPack for Dell VMAX/PowerMax planning that is based on the number of arrays and array configurations being managed. As a rule, Dell SRM Collector Hosts should be installed as near as possible to the Array Provider Host to avoid network latency between the collector and Unisphere. For example, if there is high network latency (100 ms or greater) from the local data center to the remote data center then the PowerMax Collector Host and Array Provider Host should be co-located within the remote data center. The host running Unisphere for VMAX and the Dell SRM collector host must have the same date and time and must be in same time zone, otherwise, the Dell SRM collector may not return performance data if the Dell SRM collector host's clock is too far ahead of the Unisphere host's clock.

Verifying the configuration

Verify that the PowerMax collector configuration is correct by using the Discovery Center Test option for each PowerMax array. Tests that are performed include basic Unisphere connectivity tests, Unisphere version checks, Unisphere performance

registration tests, and an array existence test. The configured discovery settings can be confirmed by using the Test utility as described in Troubleshooting Discovery Center connectivity failures.

Creating collectors for discovery of Symmetrix arrays (local discovery configuration)

The following procedure describes how to create PowerMax collectors for discovery of all VMAX3 and VMAX All Flash arrays in Dell SRM.

Steps

1. Create a Windows (2008, 2012, 2012R2) or Linux (RH 5+, Suse 10+) Vmguest with eight RDM gatekeepers that are allocated to the server from each local Symmetrix array (have been tested for 60,000 volumes total).
2. Size the server as follows: 4–8 CPUs, 32 GB RAM, 200 GB Storage.
3. Install Unisphere for VMAX on the PowerMax collector server. This server will only be used for Dell SRM data collection (no production allocation use).
4. Ensure that the server can see no more than 466,000 volumes and be sure to leave room for growth. Run *symcfg* list from Solutions Enabler to verify.
5. Create a *symavoid* file if too many Symmetrix arrays are visible until you get the volume count on the server below 466,000 volumes and be sure to allow for growth. You will be blocking the remote arrays as well in the *symavoid* file. Remote arrays will be discovered in remote datacenters locally by a PowerMax collector server there.
6. Install Dell SRM collector software on this server. Add this server to Dell SRM as a scale out collector.
7. Install only the SolutionPack for Dell VMAX PowerMax collector on this server.
8. Set the Java heap for the PowerMax collector to 2 GB (refer to the *Dell SRM Performance and Scalability guidelines* for more information). 2 GB is the default setting for this Collector.
9. In Dell SRM, use only the local discovery option and enter the Solutions Enabler install directory, if it is not the default.
10. This server will be used to fill in the Unisphere for VMAX for discovery in Dell SRM.

Configuring PowerMax arrays for consolidation of availability alerts

Use this procedure to configure forwarding of availability alert traps (SNMP v1) from PowerMax arrays to Dell SRM.

About this task

PowerMax performance alerts are collected using the discovery data collection configuration.

Steps

1. Log in to Solutions Enabler on the array provider host as an administrator.
2. Browse to the `daemon_options` file in the `C:\Program Files\EMC\SYMAPI\config\` directory.
3. In the parameter section `SNMP_TRAP_CLIENT_REGISTRATION`:
   a. Uncomment the line `storevntd:SNMP_TRAP_CLIENT_REGISTRATION`
   b. Add the Dell SRM trap recipient IP to the trap filter. In a single vApp installation, this parameter is the Dell SRM IP, and in a distributed environment, is the Primary Backend server's IP.

      The syntax is ***<IP>,<port>,<filter>,<state>***, where ***<filter>*** is the filtering level for trap forwarding that is defined in the `FCMGMT-MIB` file.

      Example: 1**0.31.90.148, 2041,10,ACTIVE**
4. In the parameter section `LOG_EVENT_TARGETS`, uncomment the line `storevntd:LOG_EVENT_TARGETS = snmp file`.
5. To identify the arrays from which traps should be forwarded to Dell SRM, type **`symcfg list`**, and press **Enter**.
6. For each array that should forward alert traps to Dell SRM:
   a. Type **`symcfg list`**, and press **Enter**.
   b. In the parameter section `LOG_SYMMETRIX_EVENTS`, specify the event categories in the format:

      `sid=<SYM serial number>, <event category 1>, <event category 2>\`

Example: `SID=000194900854, disk, device, device pool, director, srdf consistency group, srdfa session, srdf link, srdf system, service processor, environmental, diagnostic, checksum, status, events, array subsystem, groups, optimizer, thresh_critical=3, thresh_major=2, thresh_warning=1, thresh_info=0 ;\`

7. To reload the changes to the `daemon_options` file, type **`stordaemon action storevntd -cmd reload`**, and press **Enter**.
8. Ensure that the storevntd Event Daemon is running on the provider host.
9. If you have multiple PowerMax array provider hosts in the storage environment, repeat this procedure on each array provider host.

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The Dell SRM Alerting Guide explains how to configure alerts consolidation.

NOTE: Use only one SolutionPack, either the SolutionPack for Dell EMC VMAX or the SolutionPack for Dell VMAX/PowerMax, to collect data from VMAX3 and VMAX All Flash arrays. Using both SolutionPacks to collect data from the same array consumes significant collector resources and can have potential consequences to reports and chargeback calculations.

The SolutionPack for Dell VMAX/PowerMax comes with some limitations when compared to the existing SolutionPack for Dell VMAX. Notably, there is no LUN performance, Disk, Disk Group, or Data Pool metrics that are collected. LUN capacity and topology metrics are still collected. Storage Group performance and SLO compliance metrics should be used in lieu of LUN performance metrics. And, Storage Resource Pool (SRP) capacity and performance metrics should be used as an alternative to the metrics for the SRP's underlying subcomponents (that is, Disks, Disk Groups, and Data Pools that make up the SRP).

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use **`localhost`** on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

12. Configure the collection interval as needed.
13. Clear **Enable Snapshot collection** to disable Snapshot collection for VMAX/PowerMax.
14. Click **Next**.
    The window displays reports settings.
15. Click **Install**.
16. Click **Ok** when the installation is complete.

Adding and configuring devices in Discovery Center

Use the following procedure to add and configure VMAX3 and VMAX All Flash devices in Discovery Center.

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Dell VMAX/PowerMax**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   When the Secure Vault checkbox is selected, the Unique Key and Safe fields appear.
5. In **Unisphere hostname or IP address**, type the name, FQDN, or IP address of the Unisphere for VMAX host.
6. In **Unisphere network port**, type the port on which Unisphere for VMAX is listening.
7. In **Unisphere username** and **Unisphere password**, type the credentials.
8. In **VMAX3, VMAX All Flash and PowerMax serial numbers to collect**, type the full serial numbers for the arrays that will be collected.
   If multiple arrays will be collected from the same Unisphere instance, serial numbers may be separated by spaces.
   To view the list of arrays visible to the Unisphere instance and registered for performance collection, type * in place of the serial numbers and click **Validate and Add**.
9. If Secure Vault is enabled, in **Unique Key** enter the unique key.
   NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Unisphere password is active.
10. If Secure Vault is enabled, in **Safe** enter the safe string.
    NOTE: Safe string can be given as input along with the Cyberark unique key when Secure Vault is checked. This input is optional and when no details are provided for safe, the default safe details that are provided in the Cyberark configuration will be used.
11. To validate the credentials, click **Validate and Add**.
12. Click **Ok**.
13. Click **Save**.
    Performance data should be displayed in about an hour.

Troubleshooting Discovery Center connectivity failures

Discovery Center enables you to test connectivity between the Dell SRM VMAX/PowerMax collector and Unisphere.

Viewing the Test button test results

Test results are displayed in the **Test Connectivity** button tool tip.

About this task

In addition to providing error and warning messages, the test results tool tip also provides useful information such as: Unisphere version, VMAX3, and VMAX All Flash arrays visible to Unisphere, arrays registered with Unisphere for performance collection.

Steps

1. Browse to **DISCOVERY** > **Discovery Center** > **Manage Discovery** > **Dell VMAX/PowerMax**.
2. Select a device and click **Test Connectivity**.
3. Once the connectivity test is completed, click the status icon to display the test results tool tip.
4. Click **Click to show/hide the full result**.
   The tool tip expands to display the full test results.

Example test results

```
Execution steps

Testing Unisphere connection
Checking Unisphere Performance license
Checking Unisphere for VMAX3 and VMAX All Flash Array registrations
Checking Unisphere for performance registrations
Validating serial numbers to collect
Tests completed successfully. See details in full result.

Testing Unisphere configuration
Trying to connect to Unisphere at https://losam033:8443/univmax
Successfully connected to Unisphere
Found UNIVMAXPA version V8.4.0.4 registered with Unisphere
Validated Unisphere V8.4.0.4 is at recommended version 8.4.0.0 or a slightly higher
version.

Detected VMAX3 and VMAX All Flash arrays visible to Unisphere:
 - 000196701343
 - 000196701405

Detected arrays registered for Unisphere performance data collection:
 - 000195700949
 - 000195701185
 - 000196701343
 - 000196701405

Validating all entered VMAX3/VMAX All Flash serial numbers:
* All entered serial numbers are registered with Unisphere
* All entered serial numbers are registered for Unisphere Performance stats collection
```

Understanding the test messages

This section describes common test result messages.

Serial number errors

The message is displayed when the provided serial number cannot be found on the Solutions Enabler server.

```
>>>ERROR: Serial number <serial_number> NOT found on UNISPHERE. Enter * to see the list
of available serial numbers.
```

To get a complete list of the available serial numbers behind the Solutions Enabler host, type ***** in **Array Full Serial Number** and click **Test**.

```
>>>ERROR: One or more entered VMAX3/VMAX All Flash serial numbers were not found on the
Unisphere instance.
```

```
>>>ERROR: Serial number 000195700930 does not match any of these detected serial
numbers: 000196701343,000196701405,000196800574
```

The message is displayed when a serial number is entered when VMAX3/All Flash was selected during SolutionPack installation and the serial number was not included in the list of detected PowerMax array serial numbers that are returned from Unisphere.

Updating SolutionPack alert definitions

During SolutionPack update, any new alert definitions that are supported in the updated version do not get updated by default. This is expected behavior.

About this task

To add newly introduced alert definitions after updating, follow the steps:

Steps

1. Go to **CONFIG** > **SolutionPacks** > **Installed SolutionPacks** > **Dell VMAX/PowerMax** in the tree.
2. In the table, click the pen icon button to the left of **Pre-configured alerts**.
3. Click **Reconfigure**.

   Go to **Config** > **Alerts** > **Manage Alert Definitions** > **Dell VMAX/PowerMax** to see the newly added alert definitions.

Limitations

- The REST calls used by the SolutionPack for Dell VMAX/PowerMax do not collect some metrics, such as disk group capacity, unusable capacity, and hot spare capacity that are collected by the SolutionPack for Dell EMC VMAX. These values are used to calculate RAID overhead capacity, configured including RAID. Therefore, the values that are displayed in the SolutionPack for Dell VMAX/PowerMax for a VMAX array varies from the values that are displayed in the SolutionPack for Dell EMC VMAX.
- When both the SolutionPack for Dell VMAX/PowerMax and the SolutionPack for Dell EMC VMAX are installed, and alerts are enabled, both SolutionPacks process the alerts and either one of them will report the alert in the SolutionPack's **Operations > Alerts** report.
- **Performance > SG SLO Compliance** report is designed to exclude storage groups having an SLO Compliance of NONE.
- In the SRM 4.8.0.0 release, the LUN performance feature was supported in the Dell VMAX/PowerMax SolutionPack for PowerMaxOS 10.0 and above arrays. However, starting from SRM 5.0.0.0, LUN performance is supported for arrays that are compatible with Unisphere 10.0 and above. LUN performance metrics collection is disabled by default. To enable LUN performance metrics collection:
  1. Go to `/opt/APG/Collecting/Collector-Manager/emc-vmax-hypermax/conf` on the Collector VMs where emc-vmax-hypermax or Dell VMAX/PowerMax SolutionPack is installed.
  2. Open `collecting.xml` file and search for the line with text `Unisphere-LUN-PERF` and edit as below:

     ```
     <collector enabled="false" name="Unisphere-LUN-PERF"
     next="File VMAX_PTF_LUN_PURPOSE" config="Stream-Collector/emc-vmax-hypermax/conf/
     streamcollector-lun-perf-unisphere.xml" />
     ```

     To

     ```
     <collector enabled="true" name="Unisphere-LUN-PERF"
     next="File VMAX_PTF_LUN_PURPOSE" config="Stream-Collector/emc-vmax-hypermax/conf/
     streamcollector-lun-perf-unisphere.xml" />
     ```

  3. Restart collector manager services for the emc-vmax-hypermax Solution Pack (Dell VMAX/PowerMax).

  NOTE: Before enabling the LUN Performance collection, see Dell SRM Performance and Scalability Guidelines for changes in the collector configurations.

- Rendering of workload placement reports for Dell PowerMax Storage Pools may experience delays if the number of LUNs is very large. This happens because performance metrics are aggregated from the LUNs within the Storage Pool with all the computations done during the report generation.
- In the Dell PowerMax 2500 and 8500 models, the available port types are OR, EF, DF, and EM. Older port types (such as FA, FE, RF, RA, RE, FN, etc.) have mostly been merged into the new OR emulation, allowing OR ports to support multiple protocols. However, if an OR port is configured with an older emulation, SRM does not support that configuration because it cannot distinguish between the different protocol configurations of OR ports.

23

SolutionPack for Dell VPLEX

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Dell VPLEX collects performance, topology, and capacity data from your VPLEX systems and displays the data in easy-to-use reports.

With this SolutionPack, you can unify your view of multiple VPLEX systems, including physical storage to virtual storage relationships. Capacity reports, such as Thick, Thin, Allocated and Not Allocated, help you to improve the availability of business critical applications and services by ensuring that those applications have the storage resources they need to operate effectively.

Installing the SolutionPack

Prerequisites

- Before installing, confirm that the VPLEX model is supported.
- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- Identify the VPLEX type (Metro or Local), VPLEX Cluster IP/Hostname, VPLEX Cluster Serial Number, and valid credentials.
- Check that a sink file is listed for each of the directors on the cluster. If the sink file is not listed for a director, check that the clusters and their associated directors are operating correctly. If the monitors are not created the SolutionPack can still be installed, but the performance data will be missing for the corresponding directors. For instance, if cluster-2 is down then you could still install the SolutionPack but it will not collect any performance data for directors on that cluster.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Alerting Consolidation** drop-down menu, select the Primary Backend host.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use **localhost** on port 2020, which is the Collector host where the Load Balancer Connector is installed.

10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
12. To configure polling settings, select **Use advanced settings**.
13. Click **Next**.
    The window displays reports settings.
14. Click **Install**.
15. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Troubleshooting Performance Data collection Issues

This topic provide details on troubleshooting procedure for performance data collection issues.

Ensure that on each VPLEX cluster, VPLEX Perpetual monitors are not stopped and are logging director and virtual volume performance data. To do this, login to VPLEX and look for the Perpetual Monitor log files located at `/var/log/VPlex/cli/director*PERPETUAL*.log`. There are separate perpetual monitor log files for VPLEX Directors and VPLEX virtual volumes. And for each type, there is one log file per director. These log files are used to collect performance data. Ensure that the last modified time stamp for all such log files is not older than a few minutes.

In case the perpetual monitor log files are old, it means that the perpetual monitors have stopped and you may not this data be collected. VPLEX KB articles have more information on how to resolve this issue.

Adding and configuring devices in Discovery

Prerequisites

- While adding a new device, ensure that cluster 1 IP and serial number are not interchanged with the cluster 2 IP and Serial Number.

Steps

1. Go to **Centralized Management** > **Manage Discovery** > **Dell VPLEX**.
2. Click **Add...**.
3. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

4. In the **VPLEX** section, provide the cluster host and authentication details for your VPLEX system.
   The default username for the VPLEX is **service** and the default password is **Mi@Dim7T**. For the Dell SMR username to have all the required permissions on the array, you must use **service** as the username. The password can be changed from the default.

   If secure vault is enabled, in **Cluster #1 Unique Key and #2 Unique Key** enter the unique key.

   It is important to enter the cluster information correctly, clusters are mapped to their correct number. Interchanging cluster IPs and SN results in a failure to collect performance data.

   Be sure to select the correct VPLEX type while adding the device. If you are adding a VPLEX Metro, select the **Metro** VPLEX type from the drop-down and enter both VPLEX cluster details. If you are adding a VPLEX Local, select the **Local** VPLEX type from the drop-down and enter the VPLEX cluster details. Do not add a Metro VPLEX System as two separate Local VPLEX Systems.

5. Click **Validate and Add** to validate the credentials.
6. Click **Ok**.
7. Click **Save**.
   It will approximately take three hours for data to start appearing on reports.

Next steps

NOTE: Threshold-based alerts are disabled by default. To manually enable threshold-based alerts, go to **CONFIG** > **Alerts** > **Manage Alert Definitions** > **Dell VPLEX** . (SNMP-based alerts are enabled by default.)

Configure VPLEX SNMP

Configure your VPLEX server to send SNMP traps to Dell Storage Monitoring and Reporting on port 2041.

About this task

For more information about configuring SNMP on VPLEX, refer to the Dell VPLEX Administration Guide.

Steps

1. Log in to the VPLEX CLI.
2. From the `VPlexcli:/>` prompt, enter: **`cd notifications/call-home/snmp-traps/`**
3. Create a trap using the command: **`create <trap-name>`**
   Where <*trap-name*> is any string that you want to use.
4. cd to <*trap-name*>.
5. Configure the trap to send notifications to Dell Storage Monitoring and Reporting using the command: **`set remote-host <IP address>`**
   Where <*IP address*> is the IP address of the server receiving the traps. For example, on a four VM deployment, this is the IP address of the Primary Backend.
6. Configure the trap to send data to port 2041 using the command: **`set remote-port 2041`**
7. Start sending notifications by using the command: **`set started true`**

Limitations

This section provides information about known limitations of the Dell VPLEX solution pack.

- This SolutionPack supports the following backend arrays: Dell EMC VMAX, Dell Unity, NetApp, Dell EMC XtremIO, IBM XIV, Hitachi Device Manager, HP StorageWorks, and HP 3PAR. This SolutionPack does not support Dell PowerFlex, IBM DS arrays, or Dell PowerScale at the backend of Dell VPLEX.
- Only encapsulated virtual volumes are supported. LVM virtual volumes are not supported.
- Chargeback, path details, and end-to-end reports only support encapsulated virtual volumes. Virtual Volumes that are created using logical volume management are not supported.
- When an underlying virtual disk, on which the virtual volume is created, is also contributing to other virtual volumes, VPLEX, and Host path details show incorrect values in the Storage View column for that particular virtual volume. Instead of listing only the Storage Views that it belongs to, it shows a pipe-separated list of all the Storage Views that the underlying virtual disk is contributing to.
- Go to **Operations** > **Workload Placement** > **Virtual Storage** > **Dell VPLEX Front-End Ports** > **Bandwidth Utilization (%)**, column is empty since ifspeed is not available in the 7.0 version of VPLEX.
- Metro node no longer supports SNMP alerts from version 7.1 onwards.

Recommendations

- VPLEX cluster names should be retained as default cluster names for successful discovery and data collection in SRM. If VPLEX cluster names are modified, respective data collection will be impacted.

24

SolutionPack for Dell VxRail

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for Dell VxRail enables users to:

- Discover and monitor Dell VxRail Appliances.
- Reports on inventory, capacity, performance, configuration and availability metrics.
- Alerts to proactively monitor key capacity, performance, configuration and health KPIs.
- Enterprise capacity dashboard and capacity planning reports.
- Visualize end to end Topology and mapping of nodes to Dell VxRail.
- Chargeback reports to show capacity consumed by Applications and associated charges.

Added support to:

- Report library -> Dell VxRail -> Inventory -> Nodes -> Availability (%)
- Report library -> Dell VxRail -> Inventory -> Storage Policy
- Report library -> Dell VxRail -> Capacity -> Clusters -> External Capacity
- Report library -> Dell VxRail -> Capacity -> Clusters -> External Used Capacity
- Report library -> Dell VxRail -> Capacity -> Clusters -> External Free Capacity
- Report library -> Dell VxRail -> Operations -> Alerts Details
- Dell VxRail -> Custom Report

NOTE: User must configure SNMP Trap Receivers at vCenter

Installing the SolutionPack

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.
6. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select Add a new alerting data collection.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown will have default value. Do not change the value.

9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
    If you select **Add a new Frontend Web service**, type the information about the Frontend Web service.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. To customize the polling period, enable **Do you want to capture advanced settings**. The default values for the advanced settings are:
    a. **Capacity Polling period**: 30 minutes (Default)
    b. **Number of collecting threads**: 10
    c. **Number of collecting threads for VM files**: 1
    d. **Polling interval for Vmware vCenter collection**: 30 minutes (Default)
    e. **Polling interval for VM files only**: 1 Hour (Default)
    f. **Re-Sync interval**: 1 hour (Default)
    g. **Metrics Collection Level**: Collect Level 2 (Default)
14. Click **Next**.
    The window displays Reports details.
15. In **Administration Web-Service Instance**, select an existing instance which is default.
16. Click **Install**.
17. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **Dell VxRail**.
3. Select the server instance where you want to store the configuration details for this device and click **Add**.
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key and vCenter Unique Key fields appear.

   NOTE: Unique Key and vCenter Unique Key fields are enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Dell VxRail Manager Password and vCenter password is active.
5. Enter the Dell VxRail Manager IP address or hostname, port (default: 5392), username, and password/unique key. Also provide vCenter IP address, username, and password/unique key.
6. To validate the credentials, click **Validate and Add**.
7. Click **OK**.
8. Click **Save**.

SNMP Trap Configuration in VxRail Solution Pack

SNMP Trap Configuration in VxRail SolutionPack includes the following procedures

1. Configuring SNMP Trap Receivers

2. Enabling SNMP Alarms or Traps for the Alerts

Configuring SNMP Trap Receivers

Prerequisites

You must configure **SNMP Trap Receivers** at vCenter where VxRail cluster is managed.

- Verify that the vSphere Client is connected to a vCenter Server instance.
- Ensure that you have the domain name or IP address of the SNMP receiver, the port number of the receiver, and the community string required for configuration.

Steps

1. In the Client, go to a vCenter Server instance.
2. Click the **Configure**tab.
3. Under Settings, click **General** .
4. On the vCenter Server Settings central pane, click **Edit**. The **Edit vCenter Server Settings** wizard opens.
5. Click **SNMP receivers** to edit their settings.
6. Enter the following information for the primary receiver of the SNMP traps.

Table 12. SNMP trap configuration details

Option	Description
Primary Receiver URL	Enter the SRM Primary Backend Server (PBE) hostname.
Enable receiver	Select the check box to enable the SNMP receiver.
Receiver port	Enter the port number as 2041.
Community string	Enter the community string that is used for authentication. You can leave it empty or select **Public**.
Receiver 2 URL	Leave this field blank.
Receiver 3 URL	Leave this field blank.
Receiver 4 URL	Leave this field blank.

7. Click **Save**.

Results

The vCenter Server system is now ready to send traps to the management system you have specified.

Enabling SNMP Alarms/Traps for the Alerts:

Prerequisites

- Existing pre-configured Alarms exists at Datacenter level.
- Ensure that you have edit access to add new alarms or modify alarms as required.

Steps

1. In the vSphere Client, go to a vCenter Server instance.
2. Click the **Configure** tab.
3. Click **Alarm Definitions.**
4. Add new Alarm definition:
   a. On the Alarm Definitions central pane click **Add.**
   b. In the **Alarm Name and Target** wizard enter the Alarm name, Description, and Alarm type.
   c. Click **Next**.

d. In the Alarm Rule window, provide the Trigger condition, appropriate Alarm severity, and enable **Send SNMP traps** option.
e. Enable **Repeat** check box if you want the trap to be sent for repetitive occurrence.
f. Click **Next**.
g. In the **Reset Rule** Window, you can enable the option to reset the alarm to green based upon your defined condition in the given wizard.
h. Click **Next**.
i. In the **Review** Window, review your Alarm definition and click **Create**.

NOTE: To edit an existing Alarm definition, go to the alarm definition you want to edit, click **EDIT**, make the required changes, and click **Save**.

Recommendations and limitations

- Do not discover VMware vCenter devices under both Dell VxRail and VMware vSphere vSAN & VxRail discovery. Simultaneous discovery results in duplicate data collection.
- vSAN must be enabled for complete VxRail Data collection.
- If both SolutionPacks are used together, ensure that VxRail Manager IPs are discovered in VxRail SolutionPack, and the same VxRail IPs and the vCenter are not present/active in VMware SolutionPack simultaneously.
- The Dell SRM recommends that existing VxRail customers use the recently enhanced VMware vSphere vSAN & VxRail SolutionPack, which has improved reporting capabilities.
- For more information about how to rediscover VxRail Clusters from VxRail SolutionPack to VMware vSphere vSAN & VxRail SolutionPack in SRM 4.10.0.0, see KB article.

25

SolutionPack for Dell EMC XtremIO

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for XtremIO generates real-time and historical reports and access capacity, performance, and inventory details. This feature gives insight into the management of the Dell EMC XtremIO flash based storage platform.

NOTE: To link and launch CloudIQ, follow the steps in Link and launch CloudIQ. To view the CloudIQ health score of the device, install and discover the CloudIQ SolutionPack as described in SolutionPack for CloudIQ.

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection.
   - **FailOver-Filter** must be enabled, which is the default.
   - **Hostname or the IP address to send data to** must point to the host where the collector is installed (localhost in a one-VM deployment and collector host in a multi-VM deployment).
   - **Network port to send data to** must be set to the port to which the collected data is sent. Specify the Arbiter port or legacy Backend data port. If you have chosen a port other than 2020 for Arbiter, then the same port has to be configured in this field.

10. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
11. Clear **Enable Snapshot collection** to disable snapshot collection for XtremIO arrays.
12. To configure polling settings, select **Do you want to configure advanced settings**.

    For XtremIO 4.0 arrays, use **Performance Polling Interval (4.0 or later)** to configure the performance interval separately. Intervals of 5 (default), 15, and 30 minutes are available.
13. Click **Next**.
    The window displays reports settings.
14. Click **Install**.
15. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Dell EMC XtremIO**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, XtremIO Password is active.
5. From **Server**, select the server where the device will be dispatched.
6. From **Instance**, select the instance of the *emc-xtremio-collect* where the device will be dispatched.
7. In the section **Dell EMC XtremIO configuration**, type the IP and credentials of the XtremIO array's Management IP address or hostname.
   - In **Management IP address or hostname**, type the array management IP or hostname.
   - Add the username and password of the XtremIO array
   - If secure vault is enabled, in **Unique Key** enter the unique key.
8. To validate the credentials, click **Validate and Add**.
9. Click **Ok**.
10. Click **Save**.
11. Click **Ok**.

Limitations

- CSV files that were exported from Discovery Center with a release earlier to ViPR SRM 4.2 cannot be used to import devices into ViPR SRM 4.2 as is. To import devices using the earlier CSV file, delete "version" column in the CSV file.
- As part of XtremIO 4.0 support, the following new reports have been added to the SolutionPack: Battery Backup Unit, Disk Array Enclosure, Local Disks, and Folders.
- Performance and capacity polling is separated starting in ViPR SRM 3.7 due to the new XtremIO 4.0 RESTful API Ver. 2.0. While discovering, you can configure the performance interval separately (the default is 5 minutes).
- As part of XtremIO X2 support, DAE Row Controllers and NVRAM are the new reports added to the SolutionPack. When XtremIO 5.x or earlier arrays are discovered, these new reports will not be displayed.
- As part of XtremIO 6.1 support, Replication(Local, Remote, IP Links, Volume Pairs), Data Reduction Ratio(DRR) for volumes are the new reports added to the SolutionPack. When XtremIO 6.0 or earlier arrays are discovered, these new reports will not be displayed.

- For XMS V2 API, the logic to identify metrics is changed to reduce inactive metrics due to change in xmsip. It will have implications on all existing metrics. Post upgrade, all XtremIO metrics go inactive and the historical data will not be displayed in default reports. New reports are added for users to access inactive metrics that are related to capacities for array and volume. These reports are hidden by default and are available at **Report Library>Dell EMC XtremIO>Capacity**. This scenario is applicable only for Dell EMC XtremIO SolutionPack.

26

SolutionPack for Hitachi Device Manager

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Hitachi Device Manager accesses performance data, configuration data, and capacity planning data pertaining to the Volumes, Disks, Ports, Dynamically Provisioned Pools, and Parity Groups of Hitachi storage systems.

Data collection methods

XMLAPI and SMI-S	Discover topology and capacity data through Hitachi Device Manager XMLAPI and performance data through SMI-S.
REST	Discover topology and capacity data through Hitachi Ops Center Configuration Manager RESTAPI and performance data through Hitachi Ops Center Analyzer RESTAPI.

Preparing Hitachi Device Manager for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for Hitachi Device Manager

About this task

Dell SRM communicates with the Hitachi Device Manager to poll information for HDS arrays.

Steps

1. Identify read only account credentials with the ability to view all on the Hitachi Device Manager system
2. Record the IP address/hostname for SSH and CIMOM communication

Preparing Hitachi Ops Center Configuration Manager and Hitachi Ops Center Analyzer for discovery and data collection through REST

Pre-requisites for REST API based discoveries:

- Array needs to be registered with the Ops Center Configuration Manager
- Configure Probe and RAID Agent for the array on Analyzer
- Roles required for Array User to fetch data from Configuration Manager RESTAPIs:
  - Storage Administrator (View Only) and
  - Either one of the below roles
    - Security Administrator (View Only or View & Modify) or
    - Audit Log Administrator (View Only or View & Modify)
- User roles required on Analyzer to fetch data through RESTAPI
  - Analyzer GUI local user

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown has default value. Do not change the values.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
11. Leave **Enable Topology Backend on data collected** checked.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

13. Remove Point e. REST API data timeout: Default value - 2 minutes
14. To configure polling and alert settings for discovery through REST, select **Use advanced settings for REST**.
    a. Topology polling period: Default value - 2 hours
    b. Performance polling period: Default value - 30 minutes
    c. REST API data timeout: Default value - 15 minutes
15. Click **Next**.
    The window displays reports settings.
16. In **Administration Web-Service Instance**, select an existing instance which is default.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Discovery of Hitachi Device Manager through Discovery center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Hitachi Device Manager**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

5. In the **Device location** section, select the **Server** and **Instance** where you want to store the configuration details for this device.
6. Select **Discovery Mode**.
   - To discover through **REST**, select from the drop down and enter:
     a. Unique friendly name for the HDS system
     b. Configuration Manager IP
     c. Enable Secure Connection (SSL)
     d. Configuration Manager port
     e. Array Serial Number
     f. Array Username
     g. Array Password/Unique key
     h. Enable Performance Collection: If the option is selected, enter:
        i. Analyzer IP
        ii. Enable Secure Connection (SSL)
        iii. Analyzer port
        iv. Analyzer Username
        v. Analyzer Password
     i. Click **Validate and Add**.
     j. Click **Ok**.
     k. Click **Save**.
   - To discover through **XMLAPI and SMI-S** and HDS type as **Device Manager Collection**, select from the drop down and enter:
     a. Unique friendly name for the HDS system
     b. Hitachi Device Manager
     c. Username
     d. Password/Unique key
     e. Discover Single Array: If the option is selected, enter:

i. Array Serial Number

f. Enable Secure Connection (SSL):
   i. If option is selected, enter XML/API SSL port
   ii. If option is not selected, enter XML/API port

g. Enable Passive Hosts & Logical Groups Discovery

> **NOTE:** Dell Technologies recommends that you only enable this option once for arrays that are managed by a single Hitachi Device Manager instance that is configured against a collector. If the arrays discovered on a collector host are managed by different Hitachi Device Managers, you should enable this option on one array for each Hitachi Device Manager.

h. Enable Performance Collection: If the option is selected, enter:
   i. Enable Secure Connection (SSL)
      i. If option is selected, enter SSL port
      ii. If option is not selected, enter port

> **NOTE:** Dell Technologies recommends that you only enable this option once for arrays that are managed by a single Hitachi Device Manager instance that is configured against a collector. If the arrays discovered on a collector host are managed by different Hitachi Device Managers, you should enable this option on one array for each Hitachi Device Manager.

i. Click **Validate and Add**.
j. Click **Ok**.
k. Click **Save**.

- To discover through **XMLAPI and SMI-S** and HDS type as **Embedded Performance Collection**, select from the drop down and enter:
  a. Unique friendly name for the HDS system
  b. Array IP Address or FQDN

> **NOTE:** For the **Array IP Address or FQDN** type the IP address of the array. For additional details, see Embedded Performance Collection.

  c. Username
  d. Password/Unique key
  e. Enable Secure Connection (SSL)
     i. If option is selected, enter SSL port
     ii. If option is not selected, enter port
  f. Click **Validate and Add**.
  g. Click **Ok**.
  h. Click **Save**.

Troubleshooting Device Manager collection

Learn how to troubleshoot Device Manager collection issues.

Steps

1. Use a web browser to log in to Device Manager with `http://<hitachi device manager IP or hostname>:<port #(example:23015)>/DeviceManagerWebService/index.jsp`
2. Type the same username and password credentials that is used for Dell SRM discovery.
3. Validate that you can view all of the expected Hitachi Storage Systems under the **Resources** tab.

Embedded Performance Collection

Performance statistics are provided for the HUS VM, VSP, and VSP G1000 through the Embedded SMI-S Provider.

The following components are supported:

- Storage system
- Front end port
- Volume

An SMI-S license is required, but it comes with the array for free. It must be enabled in Storage Navigator.

In Hitachi Storage Navigator, a user with the role of "Storage Administrator with view only permission" is required.

Enabling the SMI-S certificate

Learn how to enable the SMI-S certificate on the array.

Steps

Refer to the *Hitachi Command Suite Administrator Guide* for details.

The following chapters are related to enabling the SMI-S certificate:

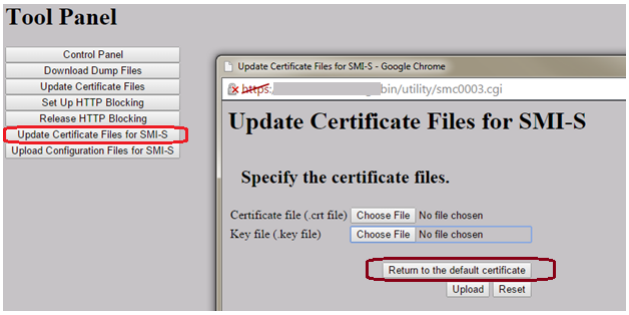
- Uploading the signed certificate
- Returning the certificate to the default

Restarting the SMI-S provider

Learn how to restart the SMI-S provider.

Steps

1. Close all of the Device Manager - Storage Navigator sessions on the SVP (service processor).
2. Start the web browser.
3. In the browser on the Device Manager - Storage Navigator computer, type the following URL:
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
4. Click **Update Certificate Files for SMI-S**.
5. In the **Login** dialog box, type the administrator user ID and password, and click **Login**.
6. Click **Return to the default certificate**, and click **OK**.

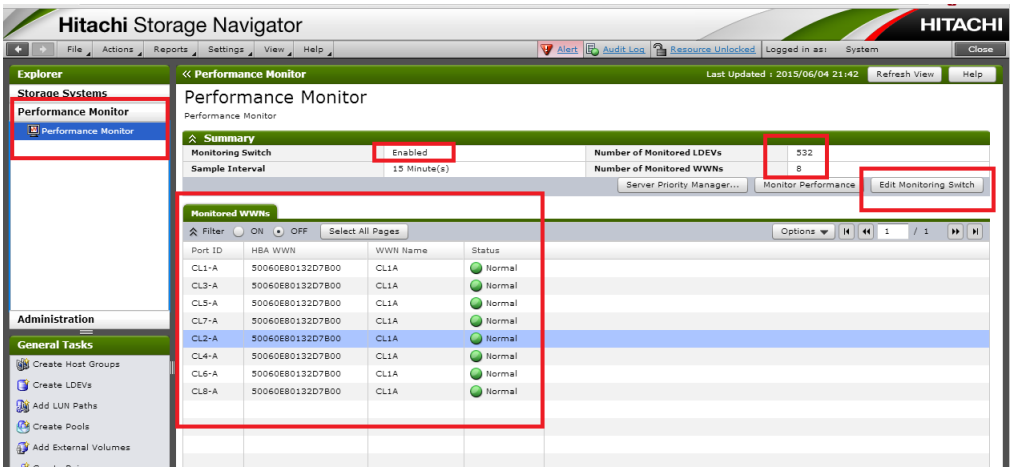


Enabling performance monitoring in Storage Navigator

Learn how to enable performance monitoring in Storage Navigator.

Steps

1. Open **Performance Monitoring** and check to see if **Monitoring Switch** is set to **Enabled**.
2. If **Monitoring Switch** is not set to **Enabled**, enable it by clicking **Edit Monitoring Switch**.



Configuring embedded performance monitoring

Learn how to configure embedded performance monitoring.

Steps

1. Navigate to **Discovery Center** > **Inventory Management** > **Hitachi Device Manager**.
2. Discover the Device Manager that manages the arrays that you want to monitor.
   a. Click **Add new device**.
   b. For **HDS type**, select **Device Manager Collection**.
   c. Enter the configuration details for the device manager, and select the **Collect performance** check box.
   d. Click **Test** to verify the connection.
3. Discover embedded performance collection.
   a. Click **Add new device**.
   b. For **HDS type**, select **Embedded Performance Collection**.
   c. Enter the configuration details for the array.
   d. Click **OK**.
4. Click **Save**.

Troubleshooting the Embedded SMI-S Provider

Use ECOM Explorer (or any CIM/SMI-S browser) to verify that the Embedded SMI-S Provider is enabled and performance statistics are populated on the array.

Steps

1. Open ECOM Explorer and choose **File** > **Login**.
2. In the **Host Name** field, type the IP address or FQDN of the array.
3. Type the port number. The default is 5988 or 5989 (SSL) depending on the configuration.
4. In the **Interop Namespace** field, type **`interop`**.
5. Type the same username and password that you used for Dell SRM discovery.
6. Once you have successfully logged in, ensure that the following classes are listed under the `root/hitachi/smis` tree:
   - Classes:
     - HITACHI_BlockStaticsticalDataStorageSystem
     - HITACHI_BlockStaticsticalDataFCPort
     - HITACHI_BlockStaticsticalDataStorageVolume

Limitations

Limitations for XMLAPI and SMIS based Hitachi array discovery

- LUNs from Hitachi AMS200 arrays do not appear in path details and end-to-end reports.
- The Performance Collection Troubleshooting report does not apply to the performance metrics pulled from the Embedded Performance Collector.
- Enterprise capacity numbers are incorrect when all the capacity for the Hitachi storage system is provided by the external storage.

Limitations for RESTAPI based Hitachi array discovery

Details listed below are not supported through REST based discovery:

- Local Replica and Remote Replica details
- Hosts details
- Logical Groups details
- Performance Collection Troubleshooting details
- Data flow into Global reports
- Chargeback reports

Migration to REST based discovery:

- Existing SMI-S/XMLAPI based discovery -> TO -> REST
  - All the Historical data will go into Inactive state
- Discover Arrays with any one of the discovery options. Do not use all the options simultaneously

27

SolutionPack for HP 3PAR StoreServ

This chapter includes the following topics:

Topics:

Overview

This SolutionPack enables you to generate real-time and historical reports and access capacity, performance, and inventory details about the HP 3PAR StoreServ systems.

Preparing the system for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for HP 3PAR StoreServ.

About this task

Dell SRM communicates with the HP 3PAR StoreServ system using an account with read-only privileges on the system.

Steps

1. Identify an account with browse privileges for the HP 3PAR StoreServ system.
2. Ensure that the array can be accessed on port 22 using SSH.
3. Ensure that the CIM server is enabled and can be accessed on the array.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The windows displays alert details.
7. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.

8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
12. Select **Use Advanced Settings** to configure the polling interval, specify the number of collecting threads, or enable the collection of logical drives.
13. Click **Next**.
    The window displays reports settings.
14. In **Administration Web-Service Instance**, select an existing instance which is default.
15. Click **Install**.
16. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
17. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
18. Click **HP 3PAR**.

    These steps describe how to add hosts individually. For information about using discovery groups to use the same credentials to discover multiple hosts, see Adding devices to discovery groups
19. Click **Add...**
20. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
21. Select the server and collector instance where you want to store the configuration details for this device, and then type the IP address of the array, supply the login credentials, and specify the appropriate configuration settings.
22. To validate the credentials, click **Validate and Add**.
23. Click **OK**.
24. Click **Save**.

Next steps

Depending on the numbers of Storage elements that is managed, you may need to edit the `unix-services.properties` file to increase the Heap Memory to a suitable level. The file is at: `/APG/Collecting/Collector-Manager/your_instance/conf/unix-services.properties`.

Configuring HP 3PAR StoreServ systems for alert consolidation

To forward SNMP alert traps from HP 3PAR StoreServ systems to Dell SRM, perform the steps below:

Steps

1. Log in to the 3PAR CLI.
2. Add the SNMP manager using the command:

```
addsnmpmgr <manager ip address>
```

The above command should be sufficient for most situations, but if your manager server requires a password or other configurations different from the default you can use the following options:

Table 13. SNMP configuration details in 3PAR CLI

Options	Description
`-p <port_number>`	Specifies the port number where the manager receives traps. The default port 162.
`-pw <password>`	Specifies the manager's access password, if the manager has one.
`-r <number>`	Specifies the number of times the system will attempt to resend the trap if the manager is not available. The default is 2.
`-t <seconds>`	Specifies the number of seconds to wait between retries. The default is 200.

3. When using the `addsnmpmgr` command the community name is set to public. To set a custom community name or change the access permissions, type the following command:

   ```
   setsnmppw -r|-w|-rw <community name>
   ```

   Where:

   - -r = read-only privileges
   - -w = write-only privileges
   - -rw = read-write privileges

4. To view the SNMP configuration for your 3PAR system, type the following command:

   ```
   showsnmpmgr
   ```

5. To verify the connection, send a test trap using the following command:

   ```
   checksnmp
   ```

28

SolutionPack for HPE Nimble

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for HPE Nimble enables users to view:

- Reports on inventory, capacity, performance, configuration and availability metrics.
- Alerts to proactively monitor key capacity, performance, configuration, health, and availability metrics.
- Enterprise capacity dashboard and capacity planning reports.
- End to end topology and mapping of hosts to HPE Nimble storage.
- Chargeback reports to show capacity consumed by Applications and associated charges.

Installing the SolutionPack

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.
6. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select Add a new alerting data collection.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown will have default value. Do not change the value.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

12. To configure Topology Polling Period and Performance Polling Period, select **Use advanced settings**.

    Topology Polling Period defines the polling period of the capacity and topology data. The default value is 30 minutes.

    Performance Polling Period defines the polling period of the performance data. The default value is 5 minutes.
13. Clear **Enable Snapshot collection** to disable snapshot collection for HPE Nimble arrays.
14. Click **Next**.
    The window displays Reports details.
15. In **Administration Web-Service Instance**, select an existing instance which is default.
16. Click **Install**.
17. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **HPE Nimble**.
3. Click **Add**.
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the HPE Nimble Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, HPE Nimble Password is active.
5. Select the server instance where you want to store the configuration details for this device. And then, type the HPE Nimble Management IP address or hostname, port (default: 5392), username, and password/unique key.
6. To validate the credentials, click **Validate and Add**.
7. Click **OK**.
8. Click **Save**.

Configuring HPE Nimble devices for alert consolidation

To configure HPE Nimble devices to send SNMP alert traps to Dell SRM, use the following methods:

From CLI

Steps

1. Type `ssh admin@<IP/Hostname>`
   Where:
   - *IP*: **`IP of the HPE Nimble Device`**
   - *Hostname*: **`Hostname of the HPE Nimble device`**

   Example:

   ```
   ssh admin@10.251.43.27
   ```
2. Type `'group --edit --snmp_trap_enabled <option> --snmp_trap_host <trap recipient IP> --snmp_trap_port <snmp_trap_port>'`
   Where:

- *<Option>*: **yes/no**
- *<trap recipient IP>*: **Single vApp installation, this parameter is the Dell SRM IP, and in a distributed environment it is the Primary Backend server IP.**
- *<snmp_trap_port>* : **Port number of the SNMP trap destination. The default destination port is 162.**

Example:

```
group --edit --snmp_trap_enabled yes --snmp_trap_host  10.247.24.190 --snmp_trap_port
162
```

If you have multiple HPE Nimble devices in the storage environment, repeat the steps on each device.

From GUI

Steps

1. Login with Administrator credentials.
2. Go to **Administration** > **Alerts and Monitoring** > **SNMP**.
3. In the **SNMP TRAP** tab:
   a. Select the **Enable SNMP Trap** checkbox.
   b. In **Trap Destination**, enter the IP address of the trap recipient.
      In a single vApp installation, this parameter is the Dell SRM IP address. In a distributed environment, it is the Primary Backend server IP address.
   c. In **Trap Destination Port**, enter the port number of the SNMP trap destination. The default destination port is 162.
4. Click **Save**.
5. If you have multiple HPE Nimble devices in the storage environment, repeat the steps on each device.

Limitations

- Replication feature is not supported.
- iSCSI reporting is not supported.

29

SolutionPack for HP Storageworks XP

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for HP StorageWorks enables you to access performance, configuration data, and capacity planning data pertaining to the volumes, disks, ports, dynamically provisioned pools, and parity groups of arrays monitored by the HP StorageWorks software.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown will have default values. Do not change the values.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
11. Leave **Enable Topology Backend on data collected** checked.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

13. To configure polling and alert settings, select **Use advanced settings**.
14. Click **Next**.
    The window displays reports settings.
15. Click **Install**.
16. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
17. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
18. Click HP **StorageWorks**.

    These steps describe how to add hosts individually. For information about using discovery groups to use the same credentials to discover multiple hosts, see Adding devices to discovery groups.

19. Click **Add...**
20. Select the **Secure Vault** checkbox to validate and add using Secure Vault.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

21. Select the server and collector instance where you want to store the configuration details for this device.
22. From the **HP type** drop-down list, select **Device Manager Collection**, and type a unique friendly name (such as the host or IP address) for the system.
    a. Supply the login credentials, and specify the configuration settings.
    b. If you want to discover a single array (than all of the devices that are managed by HP StorageWorks), check **Discover Single Array**, and specify the serial number of the array that you want to discover.
    c. If you want to enable the discovery of passive hosts and logical groups from HP StorageWorks, check **Enable Passive Hosts & Logical Groups Discovery**.

       NOTE: Dell Technologies recommends that you only enable this option once for arrays that are managed by a single HP StorageWorks instance that is configured against a collector. If the arrays discovered on a collector host are managed by different HP StorageWorks, you should enable this option on one array for each HP StorageWorks.

    d. If you want to collect array performance data from the specified HP StorageWorks, check **Enable Performance Collection**.

       NOTE: Dell Technologies recommends that you only enable this option once for arrays that are managed by a single HP StorageWorks instance that is configured against a collector. If the arrays discovered on a collector host are managed by different HP StorageWorks, you should enable this option on one array for each HP StorageWorks.

23. If you want to configure Performance Collection against a specific array, select **Embedded Performance Collection** from the **HP type** drop-down list, and type a unique friendly name (such as the host or IP address) for the system. Supply the login credentials, and specify the configuration settings. For the **Array IP Address or FQDN**, type the IP address of the array. For additional details, see Embedded Performance Collection.
24. To validate the credentials, click **Validate and Add**.
25. Click **OK**.
26. Click **Save**.

Troubleshooting Device Manager collection

Learn how to troubleshoot Device Manager collection issues.

Steps

1. Use a web browser to log in to HP Command View Advanced Edition Suite (CVAE):
   `http://<HP CVAE suite IP or hostname>:<port # (example:23015)>/DeviceManagerWebService/index.jsp`
2. Type the same username and password credentials that you used for Dell SRM discovery.

3. Validate that you can view all of the expected HP Storage Systems under the **Resources** tab.

Embedded Performance Collection

Performance statistics are provided through the Embedded SMI-S Provider.

The following components are supported:

- Storage system
- Front end port
- Volume

An SMI-S license is required, but it comes with the array for free. It must be enabled in Storage Navigator.

In Storage Navigator, a user with the role of Storage Administrator with view only permission is required.

Enabling the SMI-S certificate

Learn how to enable the SMI-S certificate on the array.

Steps

Refer to the *HP Command View Advanced Edition Administrator Guide* for details.

The following chapters are related to enabling the SMI-S certificate:

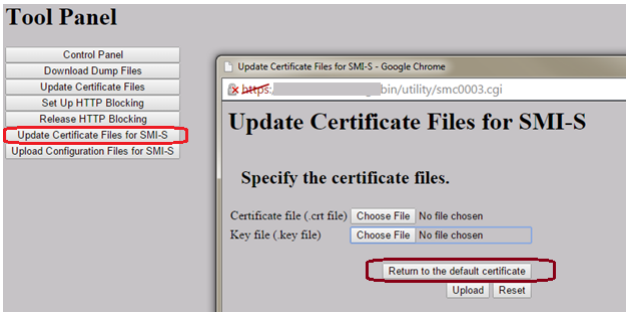
- Uploading the signed certificate
- Returning the certificate to the default

Restarting the SMI-S provider

Learn how to restart the SMI-S provider.

Steps

1. Close all of the Device Manager - Storage Navigator sessions on the SVP (service processor).
2. Start the web browser.
3. In the browser on the Device Manager - Storage Navigator computer, type the following URL:
   http://IP-address-or-host-name-of-SVP/cgi-bin/utility/toolpanel.cgi
4. Click **Update Certificate Files for SMI-S**.
5. In the **Login** dialog box, type the administrator user ID and password, and click **Login**.
6. Click **Return to the default certificate**, and click **OK**.

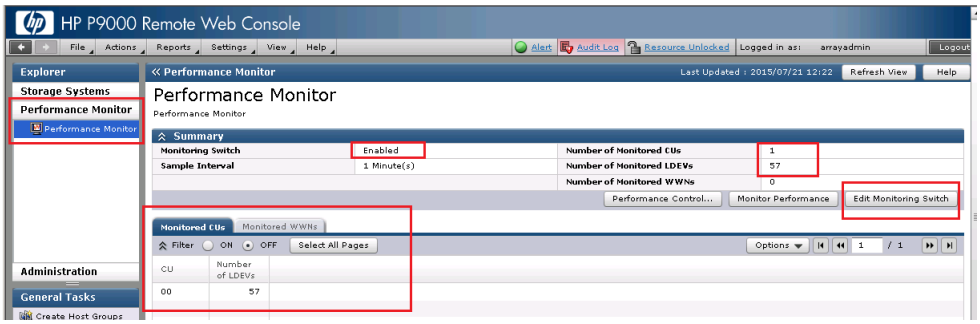


Enabling performance monitoring in Storage Navigator

Learn how to enable performance monitoring in Storage Navigator.

Steps

1. Open **Performance Monitoring** and check to see if **Monitoring Switch** is set to **Enabled**.
2. If **Monitoring Switch** is not set to **Enabled**, enable it by clicking **Edit Monitoring Switch**.



Configuring embedded performance monitoring

Learn how to configure embedded performance monitoring.

Steps

1. Browse to **Discovery Center** > **Inventory Management** > **HP StorageWorks**.
2. Discover the CvAE that manages the arrays that you want to monitor.
   a. Click **Add new device**.
   b. For **HP type**, select **Device Manager Collection**.
   c. Type the configuration details for the CvAE, and select the **Collect performance** checkbox.
   d. To verify the connection, click **Test**.
3. Discover embedded performance collection.
   a. Click **Add new device**.
   b. For **HP type**, select **Embedded Performance Collection**.
   c. Type the configuration details for the array.
   d. Click **OK**.
4. Click **Save**.

Troubleshooting the Embedded SMI-S Provider

Use ECOM Explorer (or any CIM/SMI-S browser) to verify that the Embedded SMI-S Provider is enabled and performance statistics are populated on the array.

Steps

1. Open ECOM Explorer and choose **File** > **Login**.
2. In the **Host Name** field, type the IP address or FQDN of the array.
3. Type the port number. The default is 5988 or 5989 (SSL) depending on the configuration.
4. In the **Interop Namespace** field, type `interop`.
5. Type the same username and password that you used for Dell SRM discovery.
6. Once you have successfully logged in, ensure that the following classes are listed under the `root/hitachi/smis` tree:
   - Classes:
     - HITACHI_BlockStaticsticalDataStorageSystem
     - HITACHI_BlockStaticsticalDataFCPort
     - HITACHI_BlockStaticsticalDataStorageVolume

Limitations

- The Performance Collection Troubleshooting report does not apply to the performance metrics pulled from the Embedded Performance Collector.

30

SolutionPack for Huawei OceanStor

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for Huawei OceanStor enables users to:

- Discover and monitor Huawei OceanStor Dorado All Flash Storage.
- Reports on inventory, capacity, performance, configuration, and availability metrics.
- Alerts to proactively monitor key capacity, performance, configuration, and health KPIs.
- Enterprise capacity dashboard and capacity planning reports.
- Visualize end to end Topology and mapping of hosts to Huawei OceanStor Storage.
- Chargeback reports to show the capacity that is consumed by Applications and associated charges.
- Support for Configuration compliance and custom reports.

NOTE: To collect carbon emission data a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

Installing the SolutionPack

Prerequisites

- Polling must be done to Huawei Oceanstor.
- REST API must be enabled on Huawei Oceanstor.

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.
6. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays detail on Alert Consolidation.
8. Click **Next**.
   The window displays pre-configured alert details.
9. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select Add a new alerting data collection.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown will have default value. Do not change the value.
10. Click **Next**.

The window displays data collection details.

11. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

12. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
    If you select **Add a new Frontend Web service**, type the information about the Frontend Web service.

13. To forward a subset of the collected metric to the topology Backend, **Enable Topology Backend on data collected** is selected.

14. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

15. To configure Performance Polling interval and Capacity Polling interval, enable **Do you want to capture advanced settings** .

    The default value is 15 minutes for Performance Polling interval and 60 minutes for Capacity Polling interval.

16. In **Do you want to enable LUN performance collection**, enable the checkbox or leave it as default based on the requirement

17. Clear **Enable Snapshot collection** to disable snapshot collection for Huawei OceanStor arrays.

18. Click **Next**.
    The window displays Reports details.

19. In **Administration Web-Service Instance**, select an existing instance which is default.

20. Click **Install**.

21. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **Huawei OceanStor**.
3. Click **Add**.
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.

5. Select the server instance where you want to store the configuration details for this device. And then, type the Huawei OceanStor Management IP address or hostname, port (default: 8088), username, password, and enter the unique key if secure vault is enabled.
6. To validate the credentials, click **Validate and Add**.
7. Click **OK**.
8. Click **Save**.

   NOTE: The pre-configured default values of threshold alerts included in the alert configurations are set as examples only and may not suit all the use cases. Hence, for optimal monitoring of alerts, it is recommended to configure these threshold values based on the specific requirements. To adjust the threshold values, go to: **Admin UI** > **CONFIG** > **Manage Alert Definitions** > **Huawei OceanStor**, right-click the respective threshold alert, select **Configure options**, and set the values accordingly.

Configuring Huawei OceanStor for alert consolidation

To forward SNMP alert traps from Huawei OceanStor to Dell SRM, perform the steps below:

Steps

1. Log in to the array management console at https://<array_management_hostname>:8088/home.
2. Go to **Settings** > **Alarm Settings** > **Alarm Notification** >**Trap** and click **Add**. The **Add Trap Server** window appears.
3. Configure the trap server with the following information:

Table 14. Trap server configurations in Huawei OceanStor array management console

Option	Description
Server Address	Enter the SRM Primary Backend hostname/IP
Port	Port number of SRM's SNMP manager
Version	SNMP version used by the SRM's SNMP manager
Community	For SNMPv1 or SNMPv2c, specify the community name
USM User	For SNMPv3, specify username
Type	Type of alarms sent by the storage device to the rap server

4. Click **OK**.

31

SolutionPack for IBM DS

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for IBM DS enables you to generate real-time and historical reports and access capacity, performance, and inventory details about the IBM DS systems.

Preparing the IBM DS system for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for IBM DS.

About this task

Dell SRM communicates with the IBM CIM/SMI-S provider that queries the storage array.

Steps

1. Depending on the IBM DS model, do one of the following:
   - IBM DS 6K/8K models: The CIM/SMI-S provider is built into the Hardware Management Console (HMC).

     NOTE: Ensure that the CIM agent is enabled, as it was disabled by default in releases earlier to Release 4, Bundle 62.0.175.0.
2. Identify the CIM username and password that is used to access the array.
3. Record this information for use when you install the SolutionPack.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.

   The window displays a note about Alert Consolidation.

7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select the Primary Backend host.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend host.
12. From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. To configure polling settings, in the IBM DS specific configuration section, click **Use advanced settings**.
14. Clear **Enable Snapshot collection** to disable snapshot collection for IBM DS arrays.
15. Click **Next**.
    The window displays reports settings.
16. In **Administration Web-Service Instance**, select an existing instance which is default.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
19. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
20. Click IBM DS.
21. Click **Add...**
22. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, CIM Password is active.
23. From the IBM DS Model drop-down list, select the respective model. Type the hostname or IP address of the host, supply the login credentials, enter the unique key if secure vault is enabled and specify the configuration settings.
24. To validate the credentials, click **Validate and Add**.
25. Click **OK**.
26. Click **Save**.

32

SolutionPack for IBM FlashSystem

This chapter includes the following topics:

Topics:

Introduction

The SolutionPack for IBM FlashSystem enables users to:

- Discover and monitor IBM FlashSystem A9000 storage platforms.
- Reports on inventory, capacity, performance, configuration and availability metrics.
- Alerts to proactively monitor key capacity, performance, configuration and health KPIs.
- Enterprise capacity dashboard and capacity planning reports.
- Visualize end to end Topology and mapping of hosts to IBM FlashSystem storage.
- Chargeback reports to show capacity consumed by Applications and associated charges.
- Support for Configuration compliance.

Preparing the IBM FlashSystem for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for IBM FlashSystem.

About this task

Dell SRM communicates with IBM FlashSystem using the command-line interface (CLI) of IBM FlashSystem A9000/ A9000R(IBM XCLI utility).

Steps

1. Ensure that the XCLI with is installed on SRM collector.
2. Identify the access credentials.
3. Provide the XCLI utility installation path during SolutionPack installation.

Installing the SolutionPack

Steps

1. Click **Administration**.
2. In the **SRM Admin UI** page, click **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
3. Select the SolutionPack.
4. Click **Install**.
5. Type the instance name.

6. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
7. Click **Next**.
   The window displays pre-configured alert details.
8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select Add a new alerting data collection.

   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** dropdown has default value. Do not change the value.
9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
    If you select **Add a new Frontend Web service**, type the information about the Frontend Web service.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.
13. Enter **Path to the xcli installation directory**.
14. To customize the polling period and collection threads, enable **Do you want to capture advanced settings** .

    The default value is 60 minutes for Topology Polling interval and 15 minutes for Performance Polling interval.
15. Click **Next**.
    The window displays Reports details.
16. Clear **Enable Snapshot collection** to disable Snapshot collection for IBM FlashSystem 9x00 series.
17. In **Administration Web-Service Instance**, select an existing instance which is default.
18. Click **Install**.
19. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI** page, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **IBM FlashSystem** .
3. Click **Add**.
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the IBM FlashSystem Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
5. If **FlashSystem Mode** selected is `FS-Series`, enter:
   - **Management IP address or hostname of the Array**
   - **Port** - Default value is **7443**
   - **Username**
   - **Password/IBM FlashSystem Unique Key**
6. If **FlashSystem Mode** selected is `A-Series`, enter:
   - **Management IP address or hostname of the Array**
   - **Username**
   - **Password/IBM FlashSystem Unique Key**
   - **IBM Hyper-Scale Manager Hostname or IP address**
   - **IBM Hyper-Scale Manager REST API Port** - Default value is **8443**

7. To validate the credentials, click **Validate and Add**.
8. Click **OK**.
9. Click **Save**.

Limitations

- Windows collector is not supported for IBM FlashSystem SolutionPack.
- The IBM FlashSystem series does not support Snapshot Group, Consistency Group, or Grid Controller.
- IBM FlashSystem for Port Performance does not support Throughput and Latency columns.
- IBM FlashSystem Rest API service cannot respond to more than 45 requests at a time, which limits SRM data collection and affects SRM reports.
- The FS-series array does not support Storage-Pool Performance reports.
- IBM's capacity unit representation differs between the A series and FS series arrays. As a result, SRM Reports display the correct value and unit for the FS series but show slight differences in capacity data and unit for the A9000 arrays. The SRM reports are aligned with the FS series arrays.
- SRM version 5.1.0.0 and above supports Performance KPIs for Volumes and Ports using REST APIs for IBM FS array version 8.6.3.x and later.

33

SolutionPack for IBM LPAR

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for IBM LPAR discovers and collects Inventory details about IBM's Power-Servers managed by Hardware Management Console (HMC) and displays the data in easy-to-use reports in Dell SRM.

With this SolutionPack, you can generate reports to highlight key relationships in the virtual environment such as:

- Power Systems managed by an HMC
- LPARs and VIOS residing on a Power System
- LPARs to the VIOS that provide the resource sharing capabilities for constituent LPARs

Capacity reports, such as File System Usage, help you to improve the availability of business critical applications and services by ensuring that applications have the storage resources they require to operate effectively.

NOTE: SolutionPack for IBM LPAR only discovers HMC data. SolutionPack for Physical Host is required to discover each VIO Server and Clients (LPARS) managed by HMC.

Configuring HMC for discovery

HMC can be discovered through the following authentication mechanism:

- Password based: *hscroot* user is used for discovery. No other pre-requisites are required.
- Public key based: Public-Private key pair that is required to be generated for *hscroot* user.

Generating a public and private key pair for HMC

For the public key method of discovering HMC hosts, you must generate a valid public and private key pair. You can choose any key generation tool to generate a valid public and private key pair.

Prerequisites

Before you begin HMC discovery, you must have a public key present on HMC to be discovered using the private key.

About this task

These steps describe the procedure to generate a public and private key pair for HMC using the *ssh-keygen* tool.

Steps

1. A Public-Private key can be generated using the following command:

ssh-keygen -t rsa -f <location_of_the_private_key/name_of_ private_key_file> -N ""

For example: **ssh-keygen -t rsa -f /root/.ssh/id_rsa -N ””**

2. Ensure that the public and private key pair that is generated has the following permissions:
   - **chmod 600 /root/.ssh/id_rsa**
   - **chmod 644 /root/.ssh/id_rsa.pub**

   The private key file is `id_rsa`.

   The public key file is `id_rsa.pub`.
3. To make the key pair functional, append the public key to *<user's home directory>*`/.ssh/authorized_keys` in the target UNIX host using the command `mkauthkeys --add "string"` where string is the content of id_rsa.pub file.

   Next, import the private key to the Collector used for discovery.

   NOTE: The public key is to be added to the authorized_keys or authorized_keys2 (depending on the HMC version) file on the target HMC hosts intended for discovery. The private key is to be imported to the collector VMs where discovery is triggered.

Importing a private key into the Collector

Steps

1. The private key should be placed inside APG's HOME directory (where APG is installed).

   For example: UNIX: `/opt/APG/`.
2. Type **chown apg:apg *<private_key_file>***.

   This command changes the owner.

   The HMC is now ready for successful data collection.

Configuring LPARs for discovery

Configuring LPARs (VIO Server and Clients) is similar to discovering individual physical hosts.

Dell SRM requires non-root user credentials or an SSH public/private key pair (keys can be created for root/non-root users) to discover VIO Servers and VIO Clients.

When the VIOS Server is installed, the padmin user is automatically created and this user provides restricted shell access. The Dell SRM host data collection mechanism does not work in the restricted shell environment, so you must create a non-root user and configure the non-root user through Sudo, PowerBroker, or Centrify's dzdo to elevate the privileges to run certain commands as root. Provide the non-root user credentials to Dell SRM while discovering the VIO Server.

NOTE: Dell SRM does not require padmin credentials to discover the VIO server.

There are many tools available to elevate the privileges of a non-root user to run commands as root, but Dell SRM 4.x and higher supports only Sudo, Powerbroker, and dzdo.

Preparing VIO Server and Client hosts for discovery is similar to how a Physical UNIX host is prepared, follow SolutionPack for Physical host for more details: Unix host/LPAR (VIO Server/Client) configuration for discovery and data collection

Verify adapter IDs in NPIV configuration

About this task

In the NPIV configuration if a VFC Server Adapter is created on the VIOS and a VFC Client Adapter on the VIOC, ensure correlation between the Physical HBA ports and the Virtual FC Client Adapter ports.

Steps

1. On the HMC, go to the Virtual Adapters tab in the partition Properties of the VIOS/VIOC on which the VFC Server/Client Adapter is created.
2. Verify that a match exists between the Adapter ID of VFC Server Adapter and the Adapter ID of VFC Client Adapter.

Installing the SolutionPack for IBM LPAR

Prerequisites

- Dell SRM core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
8. If you want to change the default HMC polling interval, click **Do you want to configure advanced settings**.
9. Click **Next**.
   The window displays reports settings.
10. In **Administration Web-Service Instance**, select an existing instance which is default.
11. Click **Install**.
12. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring HMC device in Discovery Center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **IBM LPAR**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

   On selecting Secure Vault checkbox, the IBM LPAR Unique Key field appears.

   NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
5. From the **Server** drop-down list, select the collector VM where the Data Collection block for the SolutionPack for IBM LPAR is installed.
6. Select the ibm-lpar instance.
7. Type the HMC hostname or IP Address.
8. Select the **Authentication Type** as:

Option	Description
Password based	Authenticates with password.
Public key based	Authenticates with SSH public private key.

9. Provide the username:
   a. Provide the password of the host for password based authentication.
   b. If secure vault is enabled, in **IBM LPAR Unique Key** enter the unique key.
   c. Provide the location of the private key for public key based authentication.
10. On successful completion, click **Save** and then **Ok**.

Adding and configuring VIO Server/Client in Discovery Center

About this task

The user credentials of VIO Server and VIO Clients should be configured in **Discovery Center > Host configuration**.

Steps to add VIO Server or Client is similar to that of adding physical hosts for discovery. Refer to Add devices using discovery

SolutionPack Reconfiguration

If you want to change the answers that were provided during SolutionPack installation the first time through, you could change them by reconfiguring the SolutionPack.

About this task

Steps

1. Click **Administration**.
2. Go to **CONFIG** > **SolutionPacks** > **Installed SolutionPacks** > **IBM LPAR** and select the instance for LPAR.
3. In the table, click the pen icon button to reconfigure.
4. Change the configuration as desired.
5. Click **Reconfigure**.

34

SolutionPack for IBM SAN Volume Controller/Storwize

This chapter includes the following topics:

Topics:

Overview

The IBM System Storage SAN Volume Controller (SVC) is a member of the IBM Storwize family, which provides storage virtualization with a single point of control for storage resources.

The SolutionPack for IBM SAN Volume Controller/Storwize enables you to generate real-time and historical reports and access capacity and performance details to gain insight into the management of the underlying Storwize storage environment.

Preparing for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for IBM SAN Volume Controller/Storwize .

Prerequisites

- Confirm that the IBM SVC model and version are supported.
- Dell SRM core modules must be up-to-date on all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- An SMI-S provider must be running on the IBM SVC server on port 5989.

Steps

1. Record the IBM SVC/Storwize cluster IP address and hostname (for SSH and CIMOM communication).
2. Record the username and password for the cluster.

   Note: All performance, topology, and capacity metrics are supported for users who are members of the Administrator or SecurityAdmin user group. Performance data (such as CPU usage and port traffic statistics of non-configuration nodes) are not supported for users who are members of the Service or CopyOperator or Monitor user groups.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.

5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.
7. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
12. To configure polling settings, select **Use advanced settings**.
13. Click **Next**.
    The window displays reports settings.
14. In **Administration Web-Service Instance**, select an existing instance which is default.
15. Click **Install**.
16. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
17. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
18. Click **IBM SAN Volume Controller/Storwize**.
19. Click **Add...**
20. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the IBM SAN Volume Controller Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
21. Select the server instance where you want to store the configuration details for this device. And then, type the hostname or IP address of the host, supply the login credentials, and specify the configuration settings.
22. Leave **Enable performance synchronization** checked.

    Enable performance synchronization allows Dell SRM to collect and report performance statistics across all of the nodes. The performance statistics files are copied from the non-config nodes to the config node, and the copied files are purged after they are processed. None of the original performance statistics on any node is purged. Disabling performance synchronization will allow collection and reporting only on the config node.
23. To validate the credentials, click **Validate and Add**.
24. Click **OK**.
25. Click **Save**.

Limitations

- Backend Arrays Dell Unity, Dell EMC XtremIO, Dell PowerScale, Dell PowerFlex, IBM DS, HP XP are not supported.
- Internal Storage is not supported in the Raw Capacity Usage and Configured Usable reports. Service Level and Chargeback are not supported for mdisks (virtual disks) based on internal storage.
- Replication is not supported.

35

SolutionPack for IBM XIV

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for IBM XIV enables you to monitor the status and performance of the IBM XIV disk storage system, and access performance and configuration data pertaining to the volumes, disks, pools, and ports of IBM XIV systems.

Preparing the IBM XIV system for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for IBM XIV.

About this task

Dell SRM communicates with IBM XIV using the CIM agent.

Steps

1. Ensure that the CIM agent is installed.

   Starting with IBM XIV Storage System V10.1.0, the CIM agent is pre-installed on the administrative module. The embedded CIM agent is automatically enabled and preconfigured.
2. Identify the access credentials.
3. Record this information for use when you install the SolutionPack.

Installing the SolutionPack

After you log in as an administrator, you can install a SolutionPack.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.

The window displays pre-configured alert details.

8. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.

9. Click **Next**.
   The window displays data collection details.
10. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

    If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

11. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, provide the required information about the Frontend Web service.

12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

13. Clear **Enable Snapshot collection** to disable snapshot collection for IBM XIV arrays.
14. To configure polling settings, select **Configure advanced settings**.
15. Click **Next**.
    The window displays reports settings.
16. In **Administration Web-Service Instance**, select an existing instance which is default.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
19. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
20. Click IBM XIV.

    These steps describe how to add hosts individually. For information about using discovery groups to use the same credentials to discover multiple hosts, see Adding devices to discovery groups.

21. Click **Add...**
22. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

23. Select the server instance where you want to store the configuration details for this device. And then, type the hostname or IP address of the host, supply the login credentials, enter the unique key if secure vault is enabled and specify the configuration settings.
24. To validate the credentials, click **Validate and Add**.
25. Click **OK**.
26. Click **Save**.

Limitations

Discovery of LDAP users requires active GUI session

Due to limitations in the IBM software, discovery using the LDAP users account will not succeed unless there is an active IBM XIV GUI user session. The session must be active either for the corresponding LDAP user or for a storage administrator.

Max Storage Volume Response Time metric not collected

The SolutionPack does not collect the Max Storage Volume Response Time (ms) metric that is needed for the **Explore** > **Hosts** > **[host]** > **Device Summary** > **[host]** report.

No support for Used for File, LUN alias, and Replica 2 and Replica 3 details

'Used for File' metrics are not supported. Therefore, the respective columns in the following reports are empty.

- **Dashboards** > **Storage** > **Enterprise Capacity Dashboard** > **Usable Capacity by Pool**
- **Operations** > **Chargeback** > **Chargeback by Group**
- **Explore** > **Storage Capacity** > **Storage Pools**

'LUN Alias' column is empty in the following report:

- **Explore** > **Storage** > **LUNs**

Remote Replication data is not exposed through the SMI provider, therefore, Replica 2 and Replica 3 columns details are empty in the following report:

- **Explore** > **Storage** > **Replication**

36

SolutionPack for Kubernetes

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Kubernetes collects real-time and historical reports and access capacity, performance, and inventory details to gain insight into the management of your Kubernetes platform.

Creating an SRM service account

About this task

Dell Technologies recommends that you create a dedicated service account for SolutionPack integration with the following criteria:

Access	Read-only access to all resources
Role	Cluster role
Secret	Non-expiring persisted API token

Steps

1. Run the following command to create a cluster role.

```
kubectl create clusterrole <<role-name>> --verb=get,list,watch --resource=
```

2. Run the following command to create a new service account.

```
kubectl create serviceaccount <<serviceaccountname>>
```

3. Assign a read-only role to the service account using the command:

```
kubectl create clusterrolebinding <<serviceaccountname>>-binding --clusterrole=<<role-name>> --serviceaccount=<<namespace>>:<<serviceaccountname>>
```

4. Create a non-expiring, persisted API token for the service account. See Create additional API tokens for more information.

Prerequisites for collecting performance metrics

Steps

1. Enable the API aggregation layer to allow the Kubernetes apiserver to be extended with additional APIs, which are not part of the core Kubernetes APIs.

   For more details, see Configure the Aggregation Layer.
2. Register the API Service for the `metrics.k8s.io` API.

   For more details, see APIService.
3. Deploy the metrics-server. See metrics-server for more information or run the command:

```
kubectl apply -f https://github.com/kubernetes-sigs/metrics-server/releases/latest/
download/components.yaml
```

Installing the SolutionPack

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name if you want to change the default instance name of generic-host.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
   If you select **Add a new data collection** and then type information about the data collection. In **Hostname or IP address to send data to**, type localhost and in **Network port to send data to**, type 2020. It is the Collector host where the Load Balancer Connector is installed.
8. Configure the collection interval as needed.
9. Select **Do you want to enable additional inventory collection** to enable Pods, Container, InitContainer, and Jobs data collection of the Kubernetes cluster.
10. Click **Next**.
    The window displays Reports details.
11. In **Administration Web-Service Instance**, select an existing instance which is default.
12. Click **Install**.
13. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices in Discovery

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Kubernetes**.
3. Click **Add..**.
4. In **Unique Friendlyname**, provide a unique friendly name for the cluster.
   This name is used to uniquely identify the system in reports.
5. In **Management IP address**, provide the Hostname/IP of the master node.
6. Type the port number where the API Server is enabled.
7. In **API Token**, enter the token created for the SRM service account.
8. Click **Validate and Add** to validate the API token.

9. Click **OK**.
10. Click **Save**.

37

SolutionPack for Microsoft Azure

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Microsoft Azure enables users to view:

- Summary of Microsoft Azure storage accounts
- Inventory of Storage Accounts, Containers, Blobs, File Shares, and Disks
- Capacity analysis and forecasting
- Operations (Device and Collector Instances, Inactive metrics)

Installing SolutionPack

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each of the components.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays the data collection details.
7. From the **Data Collection** drop-down list, select existing settings that have been specified for other components or select **Add a new data collection**.
8. If you select **Add a new Data collection**, type information about the data collection.
   a. In the **Hostname or IP address to send data** field, enter `localhost`.
   b. In the **Network port to send data to** field, enter `2020`.
9. If you select **Configure advanced settings**, you have the below options:
   a. To enable the option to store blob information in SRM, select **Store Blob Details**.
   b. **Inventory Data polling period** defines the polling interval for data collection from Microsoft Azure storage account. Enter the default value which is set at **60 minutes**.
   c. **REST API data timeout** is applicable for data collections performed through Microsoft Azure REST APIs. Enter the default value which is set at **2 minutes**.
10. Click **Next**.
    The window displays reports settings.
11. In the **Administration Web-Service instance**, select an existing instance which is default.
12. Click **Install**.
13. Click **OK**.

    Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI**, click **DISCOVERY** > **Discovery Center** > **Manage Discovery** .
2. Click **Microsoft Azure Account**.
3. Click **Add...**.
4. To define the location of a Microsoft Azure account device collector, enter the options:
   a. To select the server where the device will be dispatched, enter the **Server** and **Instance name**.
   b. Select the Secure Vault checkbox to fetch the device credentials from the CyberArk server to discover the device. On selecting the Secure Vault checkbox, the Unique Key field appears and the Client Secret field is disabled.
      NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Client Secret is active.
   c. Enter **Subscription Id**.
   d. Enter **Resource Group Name**.
   e. Enter **Account Names** - You have multiple options to enter **Account Names**:
      - Option 1: You can enter one of the account names under a **Subscription Id** and **Resource Group Name**.
      - Option 2: You can enter multiple account names under a **Subscription Id** and **Resource Group Name** separated by comma (**,**).
      - Option 3: You can enter ***** to collect information across all the account names under a **Subscription Id** and **Resource Group Name**.
   f. Enter **Tenant Id**.
   g. Enter **Client Id**.
   h. Enter **Client Secret**.
   i. If secure vault is enabled, in **Unique Key** enter the unique key.
5. To validate the credentials, click **Validate and Add**.
6. Click **OK**.
7. Click **Save**.

38

SolutionPack for Microsoft Hyper-V

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Microsoft Hyper-V generates real-time and historical reports so you understand Hyper-V performance through global and detailed status of Hyper-V hosts and underlying virtual machines.

Main reports

Inventory	Displays the inventory of devices, parts and metrics from Hypervisors and Virtual Machines
Virtual Disk Use Analysis	Tool to analyze the utilization profile of Virtual Hard Disk images
All Hosts | All Virtual Machines	Displays all available performance graphs for Hypervisors and Virtual Machines
Global Status	Shows the global status of all hosts and running virtual machines in the environment, detailed by component type
SLA Detailled View	Shows the current and forecasted SLA values for Hypervisors and Virtual Machines
Virtual Machines Running On Snapshot Disks	Shows all virtual machines running on snapshot disks. They impact disk performance and impact storage performance when it is time to commit changes on the original virtual disk.

Configuring credentials for SolutionPack for Microsoft Hyper-V

About this task

- Hyper-V Collector Manager must have the right to query WMI objects from Hyper-V hosts
- PowerShell must allow the execution of unassigned PowerShell scripts

Requirements for data collection

In order to collect data from Microsoft Hyper-V hosts, the environment needs to meet the following requirements:

- The Collect SolutionPack Block must be installed in a server using Windows Server 2008 R2 Service Pack 1 or later.
- The Collect SolutionPack Block must be able to query WMI objects in remote Microsoft Hyper-V hosts.
- The Collect SolutionPack Block machine must allow the execution of unsigned PowerShell scripts. To provide this capability, run the following command as an administrative user: **`PowerShell -C Set-ExecutionPolicy Unrestricted`**.

Installing the SolutionPack

Prerequisites

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays data collection details.
7. From the **Alerts** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
8. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use **`localhost`** on port 2020, which is the Collector host where the Load Balancer Connector is installed.
9. Leave **Enable Topology Backend on data collected** checked.
10. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
11. To configure polling settings, select **Configure advanced settings**.
12. Click **Next**.
    The window displays reports settings.
13. In **Administration Web-Service Instance**, select an existing instance which is default.
14. Click **Install**.
15. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
16. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
17. Click Microsoft Hyper-V.
18. Click **Add...**
19. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.
20. Select the server and collector instance where you want to store the configuration details for this device. Type the hostname or IP address of the host, supply the login credentials, and specify the configuration settings.

    Clicking the **Test** button results in a warning message that can be ignored.
21. Click **OK**.

22. Click **Save**.

Using a test script to query WMI objects

The Test feature that is located in the **Manage Discovery** under the **Discovery** UI supports only required functionality for the test button such as host reachability and credentials verification.

SolutionPack for Microsoft Hyper-V provides a script that can be used to check if it is possible to query all required WMI objects using the provided user. The script is in the folder `<APG_FOLDER>/Collecting/Stream-Collector/<SolutionPack_instance_name>/conf/`. Run the script from the Collect SolutionPack Block server. Use the following syntax to run the script:

```
TestWMI.ps1 -Computer <ip-or-hostname>
            -Username <domain-or-machine\username>
            -Password <password> [-NoPing]
```

-Computer	Remote Hyper-V host IP address or hostname
-Username	Username that is used to perform remote WMI queries, in the format *DOMAIN\username* for domain users or *MACHINE\username* for local users
-Password	Password of the user which is specified with the `-Username` parameter
-NoPing	(optional) If the remote Hyper-V host is blocking ping requests, you must use this parameter to skip connectivity tests

iSCSI Support

Table 15. Array platform Ssupported for iSCSI

SolutionPack	Array platform supported for iSCSI	
	Dell VMAX/PowerMax	**Dell EMC XtremIO**
SolutionPack for Microsoft Hyper-V	Yes	Yes

NOTE:

- Dell EMC VMAX 3 arrays onwards are supported.

Limitations

- The Storage Connectivity tab does not show data for Hyper-V VMs.
- Topology and Chargeback are not supported for ScaleIO and Hyper-V.
- Pass through disk capacity not collected/displayed for Hyper-V guests.
- NAS shares on Hyper-V guests/VMs are not supported with Hyper-V SolutionPack.
- VM Chargeback reports are only seen for VMs using N_Port ID Virtualization(NPIV).
- Disk data is not collected when VMs are using pass-through disks.

39

SolutionPack for Microsoft SQL Server

This chapter includes the following topics:

Topics:

Overview

This SolutionPack includes reports for unified monitoring of Microsoft SQL Database using SQL queries against targeted servers. The reports give key information on status, performance and availability of databases, datafile capacities, and performance metrics such as Index, IO, Wait, and Memory pressure.

SQL commands

This SolutionPack uses these commands:

- SELECT
- CONNECT
- INSERT
- CREATE TABLE
  - This command creates temporary tables that are used when gathering the capacity-related information of databases. The temporary tables are created in the `tempdb` table. These tables are later dropped.
- EXEC
  - Executes a stored procedure that lists disks and their available free space.
- DROP
  - Removes temporary tables created earlier in the `tempdb` table.

User privilege requirements for SolutionPack for Microsoft SQL

The Microsoft SQL Server can be discovered with SQL Authentication or Windows Authentication.

Microsoft SQL authentication

SQL authentication works for users having either SYSADMIN privileges or an unprivileged account.

NOTE: An unprivileged account can be created and used to discover the Microsoft SQL Server. For more information, refer to Configuring the SolutionPack with an unprivileged account.

Windows authentication

A Windows user account must be imported into the Microsoft SQL Server with the following settings:

- Server role of **Public**
- Securable grants for **Connect SQL**, **View any definitions**, and **View server state**

NOTE: A non-admin account can be created and used to discover the Microsoft SQL Server. For more information, refer to Granting permission to a non-admin user .

Configuring the SolutionPack with an unprivileged account

Create a `watch4net` account for Microsoft SQL SolutionPack collector with specific grants.

About this task

The collector must connect to each instance of MS-SQL Server and perform SQL queries. You can use either an administrator equivalent system account or create a dedicated system account for the collector. If you want a dedicated system account, please ask the DBA administrator to create a `watch4net` account with specific grants for the collector.

To create a `watch4net` account:

Steps

The default database must be used as the *[master]* database in this procedure.

```
USE [master]
GO

CREATE LOGIN [watch4net]
WITH PASSWORD=N'<securepassword> ',
DEFAULT_DATABASE=[master],
DEFAULT_LANGUAGE=[us_english],
CHECK_EXPIRATION=OFF,
CHECK_POLICY=OFF
GO

EXECUTE master.sys.sp_MSforeachdb
'USE [?];
CREATE USER watch4net FOR LOGIN watch4net
GO

GRANT VIEW SERVER STATE TO watch4net
GO

GRANT VIEW ANY DEFINITION TO watch4net
GO
;
```

Results

Dedicated account is configured.

Granting permission to a non-admin user

If you want a dedicated system account, have your DBA administrator create a DOMAIN\watch4net account with specific grants for the collector.

Steps

Follow this example to create a `DOMAIN\watch4net` account. The default database must be used as the *[master]* database in this procedure.

```
USE [master];
```

```
GO
CREATE LOGIN [DOMAIN\watch4net]
FROM WINDOWS
WITH DEFAULT_DATABASE=[master];
GO
CREATE USER [watch4net] FOR LOGIN [DOMAIN\watch4net];
GO
GRANT VIEW SERVER STATE TO [DOMAIN\watch4net]
GO
GRANT VIEW ANY DEFINITION TO [DOMAIN\watch4net]
GO
```

Results

Your dedicated account is configured.

Installing the SolutionPack for Microsoft SQL

Prerequisites

- Ensure the core modules, such as the Module-Manager, are up-to-date on all servers since not all module dependencies are validated during the SolutionPack installation. The installation guide for the product provides more information.
- Ensure that you create a `watch4net` user earlier to installing the SolutionPack. Ensure that correct credentials are added to Microsoft SQL Server Inventory Management during the installation process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each of the components.
6. Click **Next**.
   The window displays pre-configured alerts details.
7. From the **Pre-Configured Alerts** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
8. Click **Next**.
   The window displays the data collection details.
9. Make a selection in the **Data Collection** drop-down list.

   Select existing settings that have been specified for other components or select **Add a new data collection**.
10. If you select **Add a new Data collection**, type information about the data collection. In the **Hostname or IP address to send data** field, use **`localhost`** on default port 2020.

    This is the Collector host where the Load Balancer Connector is installed.
11. Select the **Frontend Web Service** option.

    Select existing settings that have been specified or choose **Add a new Frontend Web Service**.
12. If you select **Configure Collector advanced settings**, you have the option to select different polling periods.

    The default polling period is 15 minutes. To set the polling period that is based on the number of SQL Server instances that are being polled by this collector manager instance, consult with the database administrator. For example, you have the option to select 5 minutes, 15 minutes, 30 minutes, or 1 hour.
13. Click **Next**.
14. Provide information about the web-service gateway if it is different from pre-populated information.
15. In the **Administration Web-Service instance**, select an existing instance which is default.
16. Click **Install**.
17. Click **OK**.

Monitor the installation logs to ensure that the installation completes successfully.

18. Click **Discovery Center** > **Inventory Management**.
19. Click **Microsoft SQL Server**.
20. Click **Add new device**.

    NOTE: Threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **MS-SQL Alert definition**.

21. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.
    On selecting Secure Vault checkbox, the Microsoft SQL Server Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

22. Select the server and collector instance where you want to store the configuration details for this device.
23. Set these values:
    - Type the Hostname or IP address of the SQL server.
    - Specify the **Database Port** and **Database Instance** name. For example, type **`Default`** for the SQL Server Instance name or type the named instance.
    - Specify the mode of authentication that is used for the SQL Server: **SQL Authentication** or **Windows Authentication**
    - If using SQL Server authentication, type the username and password for the SQL Server.
    - If using Windows authentication, provide the Windows domain, username, and password. Use either the local or domain username.
    - If secure vault is enabled, in **Microsoft SQL Server Unique Key** enter the unique key.
24. To check connectivity with the SQL Server, click **Validate and Add**.
25. Click **OK**.
26. Click **Save**.

Enabling SSL enabled MS-SQL instance discovery

Steps

1. On Linux:
   a. Run:
      `export _JAVA_OPTIONS=-Djsse.enableCBCProtection=false -Linux`
   b. Restart all services:
      `./manage-modules.sh service restart all`
2. On Windows:
   a. Locate the following registry entry:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\APGCollectorManagerMicrosoftsqlserver\Parameters\Java`
   b. Open the `Options` key and append with:
      `-Djsse.enableCBCProtection=false`
   c. Locate the following registry entry:
      `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\APGScriptEngineDefault\Parameters\Java`
   d. Open the `Options` key and append with:
      `-Djsse.enableCBCProtection=false`
   e. Restart the MS-SQL Collector service:
      `manage-modules.cmd service restart collector-manager microsoft-sqlserver`
   f. Restart the Script engine service:
      `manage-modules.cmd service restart script-engine Default`

Limitations

- The Related Host report is not populated for hosts that are discovered via the EMC Host Interface agent.
- If Database is residing on VM VMFS/NFS data store, end to end topology is not supported.
- Case Sensitive collation that is used on the database instance is not supported.
- In Dell EMC SRM 4.2, topology of Microsoft SQL end to end connectivity is available but the details in the table are not available for arrays.

40

SolutionPack for NetApp FAS

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for NetApp FAS enables users to get a deeper understanding of the performance and storage capacity parameters of NetApp FAS devices through a unified monitoring of NetApp FAS devices distributed in the network.

The SolutionPack generates reports regarding performance and capacity metrics.

Configuring access credentials

About this task

Dell SRM communicates with NetApp FAS arrays using the NetApp CLI over SSH.

The following SSH connections are required:

- SSH connection to the C-Mode NetApp devices with the following roles: Access level read-only for the commands cluster, network interface, volume, snapshot policy, job schedule cron, snapshot, df, storage disk, node, aggr, cifs, system node, lun, quota, qtree, export-policy rule, network port, network connections, fcp adapter, fcp initiator, snapmirror, igroup, vol efficiency, iscsi nodename, vscan scanner-pool, storage encryption disk, storage aggregate, storage aggregate show-cumulated-efficiency, vserver object-store-server bucket and access level 'all' for the commands set, system, statistics.

Verify that you are polling the real filer (not a vFiler).

NOTE: Ensure that the host names are consistent.

Preparing NetApp FAS for discovery and data collection

Identify the information that is required to support resource discovery and data collection before installing the SolutionPack for NetApp FAS.

About this task

Dell SRM communicates with NetApp FAS arrays using the NetApp CLI over SSH.

Steps

1. Identify the IP, username, password, SSH Port no (default is 22), and NetApp FAS Mode (7-Mode or C-Mode).
2. Identify the Cluster management IP for C-Mode FAS discovery.

3. Record this information for when you add the Netapp devices to Discovery Center.

Configuring NetApp arrays for alert consolidation

Configure the forwarding of health alert traps (SNMP v1) from NetApp arrays to Dell SRM.

About this task

NOTE: SNMP traps are sent to port 162.

Steps

1. Log in to the NetApp array.
2. To enable SNMP trap forwarding, type the following command:
   `options snmp.enable`
3. To check which hosts have registered for SNMP traps, type the following command:
   `snmp traphost`
4. To receive SNMP traps, add the Dell SRM primary backend by entering the following command:
   `snmp traphost add <hostname>`
5. To verify that the host was added, type the following command:
   `snmp traphost`

Installing the SolutionPack

Prerequisites

- Dell SRM core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays pre-configured alert details.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. Leave **Enable Topology Backend on data collected** checked.
11. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.
    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

12. Clear **Enable Snapshot collection** to disable Snapshot collection of NetApp FAS array.
13. Select **Enable Additional Collection** to enable additional capacity and performance metrics.
14. To configure polling settings, select **Do you want to configure advanced settings**.
15. Click **Next**.
    The window displays reports settings.
16. In **Administration Web-Service Instance**, select an existing instance which is default.
17. Click **Install**.
18. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
19. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
20. Click **NetApp**.
21. Click **Add...**
22. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.

23. Select the server instance where you want to store the configuration details for this device. And then, type the hostname or IP address of the host, supply the login credentials, enter the unique key if secure vault is enabled and specify the configuration settings.
24. To validate the credentials, click **Validate and Add**.
25. Click **OK**.
26. Click **Save**.

Supported use cases

Table 16. Supported use cases

Use case	Support (C mode)
Discovery	Yes
Maps, Path, and Connectivity details	Yes C-mode topology Not supported: External storage array
Global Capacity reports	Yes
Explore reports	Yes
Chargeback	Yes
Performance	Yes
Alerting	Yes
Compliance	No
Detailed reports for File and Block at SP level	Yes
Qtree and Quota Reports	Yes
CIFS shares and NFS shares report	Yes

Limitations

- NetApp FAS SolutionPack does not support discovery of metro cluster configuration.

Limitations in global reports

- Used capacity is the same as the total capacity for Ontap 7.x versions of the following reports:
  - **Explore** > **Storage Capacity** > **Service Level Capacity**
  - **Explore** > **Storage Capacity** > **Array by Service Level**
- In **Dashboards** > **Storage** > **Enterprise Capacity Dashboard** > **Usable Capacity by Type** > **Used for Block**, the OnTap 7.x CLI does not provide LUN used capacity hence the total capacity is used for computation.
- The following global reports/metrics are not applicable:
  - In **Explore** > **Storage** > **NAS File Systems**, **Snapshot Total**, **Snapshot Used**, and **Snapshot Utilization** are not applicable.
  - In **Explore** > **Storage Capacity** > **Storage Pools**, **Overhead Capacity** is not applicable in the **File Systems/Flex Vols** report and **Pool Enabled** and **Pool Overhead** are not applicable in the **Subscriptions** report.
  - **Explore** > **Storage** > **RAID/Parity Group**
  - **Explore** > **Storage Capacity** > **NAS Pools**
- In **Dashboards** > **Storage** > **Enterprise Capacity Dashboard** > **Used Capacity by Type** and **Explore** > **Storage** > **More Reports** > **Enterprise Capacity**, the "Used for HDFS" and "Used for Object" metrics are blank for NetApp.
- In **Explore** > **Storage** > **NAS File Systems**, for filers running OnTap 8.2 or higher, the total capacity of a thin file system is the same as its used capacity.

Limitations in the inventory reports

- SVM is not reported if there are no volumes that include the root volume that is associated with that SVM.
- Shares that are associated with Vfiler are not reported on the Shares tab. This data is reported on the Vfiler tab.
- Volume capacity is shown for the shares, but the share is created on a Qtree with different Quota specifications.
- Shares that are created on root ($, etc, /) are not supported.
- Shares that are created on the same path/volume are displayed on the same row. As a result, the number of shares that are reported might be less than the actual number of shares.
- CIFS shares that are created on Snapshots are not supported.
- Interfaces that are configured without IP are not reported.
- The Capacity of broken disks is not reported.
- Volume level capacities are displayed for all CIFS and NFS shares.
- The maximum length of variable ID in SRM is 255 characters. As a result, information about capacity will be missing, a truncated volume name will be displayed. To avoid data inconsistency, the length of the volume name is required to be in the range of 150-170 characters which will allow remaining portion of variable ID to be used for mandatory system data.
- For ONTAP 9.10.0 and earlier, capacity units are shown in decimal (KB/MB/GB/TB), which do not match SRM reports. For ONTAP 9.10.1 and later, capacity units are shown in binary (KiB/MiB/GiB/TiB).
- From ONTAP version 9.14, the value for `PhysicalUsed from volume` command includes other compaction metrics. As a result, in SRM, we have adjusted the metrics that rely on it to use used capacity. The affected metrics are `EffectiveUsedCapacity`, `LogicalUsedCapacity`, `DataReductionRatio`, `CompressionRatio`, `DeduplicationRatio`, and `PhysicalFreeCapacity` at the volume level. Consequently, all the corresponding reports and dashboards will be impacted.

41

SolutionPack for Oracle Database

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Oracle Database monitors the status and performance of an Oracle database.

This SolutionPack specializes in Oracle monitoring and provides a proactive set of reports that get right to the heart of any ongoing Oracle capacity and performance issue. The SolutionPack can be used both by database and storage administrators and comes with a complete monitoring package for databases that includes reports for availability, database and table sizes, cache ratios, and other key metrics. This SolutionPack also has complementary features that allow rich KPIs like the End to End view of the Oracle Database Topology by mixing Oracle database queries and server monitoring. To use this feature, Dell Technologies recommends installing the SolutionPack for Physical Hosts or the SolutionPack for VMware vSphere vSAN & VxRail (depending on the Oracle setup) along with the corresponding SolutionPack for the array where Oracle is deployed.

Installing the SolutionPack

Prerequisites

- The core modules must be up-to-date on all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- The appropriate JDBC driver jar file must be in the …/APG/Databases/JDBC-Drivers/Default/lib folder. Refer to the support matrix for additional details.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each of the components. For Oracle ASM deployments, specify the server where the system will install ASM Data Collection. For additional details about the ASM script and configuring ASM, refer to the SolutionPack for Oracle Database section of the support matrix.
6. Click **Next**.
   The window displays pre-configured alerts details.
7. From the **Pre-Configured Alerts** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
8. Click **Next**.
   The window displays data collection details.

9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.

10. Leave **Activate the FailOver-Filter** checked.
11. From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add a new Web-Service Gateway**.

    If you select **Add a new Web-Service Gateway**, type information about the web-service gateway.

12. The Topology Service automatically includes the standard settings. You should only add a new Topology Service if the Topology Mapping service is installed in a non-default location.
13. If you select **Configure collector advance settings**, you have the option of selecting from polling periods of 5 minutes, 15 minutes, 30 minutes, and 1 hour. The default polling period is set to 15 minutes. To set the polling period based on the number of Oracle Database instances that are being polled by this particular instance of the collector manager, consult with the database administrator.
14. Click **Next**.
    The window displays reports settings.
15. In **Administration Web-Service Instance**, select an existing instance which is default.
16. Click **Next**.
    The windows displays ASM Data Collection settings.
17. Specify the default collection level for ASM Data Collection. In this case, the default option is Standard.
18. Click **Install**.
19. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
20. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
21. Click **Add...**

    NOTE: Threshold based alerts are disabled by default. To manually enable threshold based alerts, go to **Administration** > **Modules** > **Alerting** > **Alert Definitions** > **Oracle Alert Definitions**.

22. Click **Oracle Database**.
23. Select the **Secure Vault** checkbox to fetch the device credentials from CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when Secure vault checkbox is selected. When Secure Vault checkbox is not selected, Password is active.

24. Select the server and collector instance where you want to store the configuration details for this device, and then type the hostname or IP address of the host, supply the login credentials, and specify the configuration settings.

    Dell Technologies recommends adding a watch4net user beforehand so that the correct credentials are added to Oracle Database Inventory Management. For details about the required grants, refer to Configuring the SolutionPack with an unprivileged account.

    For each Oracle Database instance being polled, it is useful to have the following information on hand before it is added to the Collection devices list:
    - Oracle service name
    - Oracle instance name (in case of a RAC setup)
    - Username (watch4net user)
    - Password/Unique key
    - Port
    - Server details (Windows, Linux, or Solaris)
    - Server details (Physical or VM)
    - Oracle setup (ASM or non ASM)
    - Oracle setup (RAC or non RAC)
    - Oracle version
    - RAC version (if installed)

25. To validate the credentials, click **Validate and Add**.
26. Click **OK**.
27. Click **Save**.

Topology for the SolutionPack for Oracle Database

The SolutionPack for Oracle Database includes features that allow rich KPIs (like the end-to-end view of the Oracle Database topology) by mixing Oracle database queries and server monitoring.

The SolutionPack is used to poll the vast majority of metrics through SQL queries against individual databases.

To support the end-to-end use-case from Oracle ASM to the backend array LUN, it is necessary to connect on the OS layer (via ssh or wmi).

Configuring the SolutionPack with an unprivileged account

About this task

The collector must connect to each instance of Oracle databases and perform SQL queries. You can use either an administrator equivalent system account or create a dedicated system account for the collector. If you want to create a dedicated system account, ask the DBA administrator to run the following query against every instances/RAC cluster. This creates a `watch4net` account with specific grants for the collector.

Steps

1. Create the watch4net user:

```
create user watch4net identified by <securepassword> default tablespace users
temporary tablespace temp;
```

2. Grant the necessary privileges to the watch4net user by running the following grants:

```
grant create session to watch4net;
grant select on dba_data_files to watch4net;
grant select on dba_free_space to watch4net;
grant select on dba_libraries to watch4net;
grant select on dba_objects to watch4net;
grant select on dba_segments to watch4net;
grant select on dba_tablespaces to watch4net;
grant select on gv_$sysmetric to watch4net;
grant select on v_$asm_disk to watch4net;
grant select on v_$asm_diskgroup to watch4net;
grant select on v_$asm_diskgroup_stat to watch4net;
grant select on v_$asm_disk_stat to watch4net;
grant select on v_$database to watch4net;
grant select on v_$dispatcher to watch4net;
grant select on v_$filestat to watch4net;
grant select on v_$instance to watch4net;
grant select on V_$instance_recovery to watch4net;
grant select on v_$latch to watch4net;
grant select on v_$librarycache to watch4net;
grant select on V_$LOCK to watch4net;
grant select on v_$locked_object to watch4net;
grant select on v_$lock_type to watch4net;
grant select on v_$log to watch4net;
grant select on v_$logfile to watch4net;
grant select on v_$parameter to watch4net;
grant select on V_$PGASTAT to watch4net;
grant select on v_$rollstat to watch4net;
grant select on v_$rowcache to watch4net;
grant select on v_$session to watch4net;
grant select on v_$sesstat to watch4net;
grant select on v_$sess_io to watch4net;
grant select on v_$sgainfo to watch4net;
grant select on v_$statname to watch4net;
grant select on v_$sysmetric to watch4net;
grant select on V_$SYSSTAT to watch4net;
```

```
grant select on V_$SYSTEM_event to watch4net;
grant select on v_$system_wait_class to watch4net;
grant select on V_$version to watch4net;
```

Results

Your dedicated account is configured.

Discovery Center requirements

Under **Discovery** > **Discovery Center** > **Manage Discovery**, ensure that there is an entry for the same Oracle server under both **Oracle Database** and **Host Configuration**.

Once the Oracle Instance is correctly added in the Inventory Management configuration, validate the connectivity by clicking **Test Connectivity**. A successful test ensures that the correct host along with the oracle configuration has been added. The test also checks for the correct version of the jdbc driver and that it is in the right folder. The test results can be expanded to show all of the grants that are provided to the user 'watch4net'. If there are any collection errors, these grants can be validated with the ones in this document.

The server must be under **Host Configuration** so the ASM Script (`oracle-asm-disk.pl` for Linux and `ASMDiskDetection.ps1` for Windows) can be pushed to the server to retrieve the internal Disk/Array WWN information.

Configuring sudo rights for ASM scripts

On a Linux server, if a non-root user is used in the Discovery Center host configuration, you must create an entry in the `/etc/sudoers` file so that the `oracle-asm-disk.pl` Oracle ASM script can retrieve all the required information.

Steps

1. Run the following script:

   ```
   ssh -v user@oracle_server 'cd /home/user/emcsrm ; /usr/bin/perl ./oracle-asm-disk.pl debug=1
   ```

   The end of the script output contains the recommended settings for configuring the `/etc/sudoers` file.
2. Optionally, you can edit the `/etc/sudoers` file directly with the following lines:

   ```
   'Defaults:user !requiretty'
   'Defaults:user env_keep += "ORACLE_SID"'
   'user ALL=(root) NOPASSWD: /usr/local/bin/inq -wwn -dev  *, /bin/raw -qa, /lib/udev/scsi_id --page\\=0x83 *'
   'user ALL=(oracle) NOPASSWD: /u01/app/oracle/product/12.1.0/grid/bin/asmcmd lsdsk'
   ```

3. Replace `/u01/app/oracle/product/12.1.0/grid/bin` with the `ORACLE_HOME` to reflect the Oracle install.

   NOTE: If the Linux server does not support the scsi_id command, install the inq application. On Windows, the ASM script will only work for a user with Admin rights.

Limitations

- The Related Host report is not populated for hosts that are discovered via the Dell Host Interface agent.
- On a Windows server, the `ASMDiskDetection.ps1` script must be run using an account that belongs to the 'Administrators' group. With non-admin discovery on Windows, reports such as ASM Datafile Distribution and ASM Disks (under Database Summary) will not work.
- Discovery Center **Test** button fails with the following error: `Cannot locate driver 'oracle.jdbc.driver.OracleDriver' !`
  1. After installing the SolutionPack, put the Oracle driver (ojdbc jar) in the following directory: `/opt/APG/Databases/JDBC-Drivers/Default/lib`
  2. Restart the script Engine.

- If Database is residing on VM VMFS/NFS data store, end to end topology is not supported.
- If profile parameter like IDLE_TIME, SESSIONS_PER_USER and so on for the Oracle Database SolutionPack user is set, recommend that the user should be used by SRM only. Ideally IDLE_TIME should be set to 'UNLIMITED'.
- Dell SRM does not support multiple instances of the same Host and Service Name for Oracle Database.

Troubleshooting

About this task

Test button failures between the collector and the Oracle database can occur in the following conditions:

- Host not reachable
- Port not accessible
- Policy setting

Steps

1. Ping the host and verify that it is reachable.
2. Check to see if any policy set is preventing connecting through the ports.

Next steps

If the output is `bash-3.2# ./asmcmd Connected to an idle instance. ASMCMD>`, validate and update the following environment variables: ORACLE_HOME and ORACLE_SID.

If the test button fails in Discovery Center and the output is related to grants, connect to the sqlplus sys user and run the following command: select * from `dba_tab_privs where grantee='WATCH4NET'`. Validate that the grants are present.

42

SolutionPack for Oracle MySQL Database

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Oracle MySQL Database provides management capabilities typically found in database-centric tools along with management support from other technologies. You can measure client activity by reporting on data from your database tier alongside your business logic and presentation tiers. A SRM collector will collect information about MySQL database and the collector is required to be granted access to the Database.

Preparing MySQL database for discovery and data collection

Before installation, prepare the MySQL Databases to be discovered.

Prerequisites

For this procedure, you need to log into the MySQL using a root privileged user.

About this task

The following procedure describes how to create an unprivileged account to be used by the SolutionPack.

Steps

1. Identify the Collector IP or FQDN.
2. Connect to one of the MySQL databases and get and generate a non-plain text password using the command:

   ```
   SELECT PASSWORD('mypass');
   ```

3. Take the result string (for example: *6C8989366EAF75BB670AD8EA7A7FC1176A95CEF4) and grant the privileges on each of the databases as shown in the example:

   ```
   CREATE USER 'watch4net'@'%'IDENTIFIED BY PASSWORD
   *6C8989366EAF75BB670AD8EA7A7FC1176A95CEF4;
   GRANT ALL ON *.* TO 'watch4net'@'%';
   ```

   Updates for MySQL8.0: In MySQL8.0 after creating user, you need to ALTER USER (password), run `Support Mysql -8.0`

4. Run the below CLI to create the user on MySQL 8.0 setup and is used to create, alter the user, and password on the setup:

   ```
   CREATE USER 'testuser129'@'%' IDENTIFIED WITH mysql_native_password BY 'Password121!'
   ALTER USER 'testuser129'@'%' IDENTIFIED WITH mysql_native_password BY 'Password131!';
   ```

NOTE: To run the queries for 8.0 setup, you need to have the latest version of MySQL workbench. For the device discovery, the jar should be greater than or equal to `mysql-connector-java-5.1.4.7.jar`.

Installing the SolutionPack

Prerequisites

- Determine whether you need a SolutionPack license file by checking the feature names and expiration dates that are listed in **System Admin** > **License** > **Manage Licenses**. If the license is not listed, obtain one by completing a Support Request (SR) form, which you can find on the Dell Support Site.
- Ensure the core modules, such as the Module-Manager, are up to date on all servers since not all module dependencies are validated during the SolutionPack installation.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Edit the default instance name **`oracle-mysql-database`**, and click **Next**.
6. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
7. If you select **Configure Collector advanced settings**, you have the option to select different polling periods. Click **Next**.
8. From the **Web-Service Gateway** drop-down, select existing settings that have been specified for other components, or select **Add a new Web-Service Gateway**.
9. Select **Administration Web-Service Instance** as the default and click **Install**.
10. When a check mark appears next to the Collector and the Report, click **OK.**

    Monitor the installation logs to ensure that the installation completes successfully.
11. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
12. Click Oracle MySQL Database.
13. Click **Add...**
14. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.

    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, Password is active.
15. Select the server and collector instance where you want to store the configuration details for this device.
16. Set the following values:
    - Type the Hostname or IP address of the MySQL server.
    - Specify the Database Port.
    - Provide the username and password/unique key.
17. To validate the credentials, click **Validate and Add**.
18. Click **OK**.
19. Click **Save**.

Limitation

- Oracle MySQL Database SolutionPack does not provide or support alerts.
- From Oracle MySQL 8.0.3 onwards, performance graph and Q_cache report is coming blank as Qcache metrics is removed.

43

SolutionPack for Physical Hosts

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for Physical Hosts discovers physical hosts, individual LPARS (AIX), and allows you to monitor and generate real-time and historical reports on the performance of physical hosts. The SolutionPack can report information about host performance, capacity and utilization, connectivity, path details, and inventory.

High-level prerequisites for host discovery:

- UNIX:
  - SSH and its subsystem SFTP enabled
  - Perl v5.6.1 or later
  - Sudo, powerbroker, or centrify dzdo configured according to the environment
  - Latest vendor specific SNIA libraries for all the HBAs installed on the hosts
- Windows:
  - Powershell v2.0 or later
  - WSMAN listeners over http or https

You can discover physical hosts with the following mechanisms:

- **Agentless (for both Windows and Unix):** To discover hosts via agentless discovery, configure the hosts to support discovery and data collection as described in Preparing your hosts for discovery and data collection.
- **Host Agent for Unix/Linux:** If you do not want to configure the hosts for agentless discovery, you can use the Host Agent for UNIX/Linux. This mode requires the following steps:
  - Download the release specific `srmhostagent.sh` file from Dell Support Site and run it as the 'root' user on the target host that you want to discover. For additional details, see Discovery via Host Agent for Unix/Linux.
  - Create a non-privileged/non-root user with read-only access to the `/tmp` directory on the target host to be discovered. Use this user to discover the host in Dell SRM. To install the SolutionPack and add devices to Dell SRM, see Installing the SolutionPack and configuring devices for discovery.
- **EHI Host Agent for Windows** (See the SolutionPack for EMC Host Interface chapter)
- **Windows Host Agent**:
  - Windows Host Agent is a new Agent based mechanism to discover Windows Host from SRM. This new agent will eventually replace the EHI agent.
  - Windows Host Agent does not require a separate Solution Pack. Discovery details for the Host can be provided using Generic RSC Host Configuration.
  - Pre-requisite for a new discovery is to have SRM Windows Host Agent installed and running on Windows host.
  - Download the Dell SRM Windows Host Agent.msi file and Installation & Help Guide from Dell Support Site.

Regardless of which discovery mechanism you choose, the authentication mechanism from Dell SRM to the host remains the same. The following table lists the authentication methods that are supported by the SolutionPack for Physical Hosts when you are adding a device to Dell SRM for discovery:

Table 17. Authentication methods for Physical Hosts

OS Type	Protocol	Password based	Key based	Certificate based
All UNIX/Linux	SSH	Yes	Yes	No
Windows	http/https	Yes	No	Yes
Windows	SSH	Yes	No	No

NOTE: For an overview of physical host discovery mechanisms that includes passive discovery, see Physical host discovery.

Preparing the hosts for discovery and data collection

Configure the hosts to support resource discovery and data collection.

Refer to the following sections for additional details about configuring the hosts:

- Windows host configuration for discovery and data collection
- UNIX host/LPAR (VIO Server/Client) configuration for discovery and data collection
- Configuring ESX hosts to collect PowerPath metrics

Guidelines for SNIA libraries and HBA drivers

To discover SNIA-qualified HBA-related information for all the host platforms you should ensure the right versions of SNIA library, drivers and firmware are in place.

About this task

- Ensure that you have Dell-supported host bus adapter (HBA) drivers and firmware. *Dell SRM Support Matrix* provides information for the supported SNIA compliant version of the HBA driver.
- HBA Model and the compatible driver versions that are qualified by Dell can also be verified on Dell Support Site > **Product and Support Tools** > **Elab Interoperability Navigator**. The vendor websites also list the Dell compatible drivers.
- The vendor-specific SNIA libraries must be installed on the target host.
- The HBA model number and part number should be verified before updating the hosts with SNIA libraries for HBA.
- You can install the SNIA library as part of HBA driver installation package or install the latest version of HBAnywhere or OneCommand Manager (for Emulex installations) or SAN Surfer (for Qlogic installation). To discover an HP-UX host with a multi-port Fibre Channel card, the package CommonIO bundle 0812(December 2008) or later should be present on the host to obtain the updated FC-SNIA file set. INQ is dependent on binaries from CommonIO bundle.

  NOTE: All Unix/Linux flavored hosts to have vendor specific SNIA libraries that are installed to get all HBA related information except Cisco UCS hosts with VIC HBA cards and Linux operating system. On Linux flavored hosts, partial information would be populated when SNIA is not installed.

Windows host configuration for discovery and data collection

Required software

- Install Powershell 2.0 or later on Windows hosts. User should have permissions to run powershell scripts. To provide permissions to run scripts, run the following command on the powershell terminal: **`Set-ExecutionPolicy RemoteSigned`**

Required user permissions

The following user credentials are required for successful host discovery:

- Local administrator
- Domain user who is part of administrator's group

- Non-admin user

A non-admin user is identified by Dell SRM as a service account user or domain user who is neither a part of the Administrator group or domain Administrators group.

For additional details, see Types of discovery allowed by different privilege levels.

Host configuration

To prepare Windows hosts for Dell SRM discovery of objects using WinRM services, hosts must be pre-configured with the WSMAN settings.

Configure one of the following listeners:

- WinRM HTTP listener:
  - Negotiate authentication mode set to true
  - Firewall exception added for port 5985
- WinRM HTTPS listener:
  - Negotiate authentication mode set to true
  - Certificate that is generated and placed in the personal store. See Generating a .pfx certificate.
  - Firewall exception added for port 5986.

These changes can be completed via two methods:

- Host Configuration utility (run on each host). Using the Host Configuration Utility
- Group policy configuration (run on the domain servers). Generating a .pfx certificate

Configuring Centrify on Windows host

Refer to the *Centrify Suite Evaluation Guide for Windows* in the Centrify documentation or contact the server administrator.

Types of discovery allowed by different privilege levels

The term "non-admin user" refers to a service account user or domain user who is not part of the Administrators group on a Windows host.

The following table applies to Windows 2008 and 2012:

Table 18. Allowed discovery types

Data in reports	Non-Admin user	Local Admin user
Discovery of host names, IP	Supported	Supported
MPIO/Powerpath	Not supported	Supported
Device Details/ Attributes	Supported	Supported
HBA Details	Supported	Supported
End to end reports - Maps	Supported	Supported
Path Details & Connectivity	Supported	Supported
File Systems to Disks	Not supported	Supported
System Performance	Supported	Supported
Disks Performance	Supported	Supported
FileSystem Usage	Supported	Supported
VolumeGroups	Supported	Supported

Table 18. Allowed discovery types (continued)

Data in reports	Non-Admin user	Local Admin user
Internal & SAN Disks	Not supported	Supported
Chargeback by Physical host	Supported	Supported
Network Interface	Not supported	Supported
iSCSI	Supported	Supported

Chargeback reports for non-admin users are supported on VMAX, Unity, and XtremIO array devices. See the release notes for any limitations on third-party array LUNs masked to Windows hosts.

Customizing a WinRM URL prefix

Prerequisites

EMC supports use of a custom WinRM URL prefix. You can change the URL prefix from the default "wsman" to any other by using following command on the target host.

Steps

Type the following command:

For	Use
Non-SSL communication	`winrm set winrm/config/listener?Address=*+Transport=HTTP @ {URLPrefix="EMC"}`
SSL-based communication	`winrm set winrm/config/listener?Address=*+Transport=HTTPS @{URLPrefix="EMC"}`

Prerequisites for discovering a Windows host using non-admin user credentials

To prepare Windows hosts for discovery, you can configure privileges in these ways:

- Provide the option `-user nonadmin` as an input to the Host Configuration utility
- Manually

The following checklist summarizes the configuration changes required on Windows hosts:

1. WinRM configuration settings:
   a. Adding a non-admin user to a group
   b. Retrieving the SID of a non-admin user
   c. Adding a non-admin SID to root SDDL

If you decide to use Host Configuration utility, the script performs these operations on the host.

- For Windows 2008 and Windows 2012, the Host Configuration utility sets both WinRM and WMI configurations.

These procedures are only available in Dell SRM 3.5.1.

Adding a non-admin user to a group

Prerequisites

On a Windows 2008/2012 host a non-admin user should be part of the following groups:

- Performance Monitor Users

- Performance Log Users
- Add non-admin users to the group WinRMRemoteWMIUsers__ . If that group does not exist, add the user to the Distributed COM Users group.

Steps

1. Go to **Start**.
2. Right-click **Computer name** and click **Manage**.
3. On the **Computer management** window, click **Local Users and Groups**.
4. Right-click the non-admin user and select **Properties**.
5. Select the **MemberOf** tab.
6. Click the **Add** button and key in the group name.
7. Click **Ok**, then click **Apply**.
8. Repeat these steps to add Performance Monitor Users, Performance Log Users.
9. Click **Ok**.

Retrieving the SID of a non-admin user

Steps

1. Run the command `wmic useraccount get name,sid` at a command prompt.
2. From the output of the command, capture the SID of the non-admin user.

Adding a non-admin SID to root SDDL

Steps

1. Open a command prompt.
2. Type the following command to add the SID.
   winrm set winrm/config/service @{RootSDDL="O:NSG:BAD:P(A;;GA;;;BA)(A;;GA;;;*<non-admin-sid>*)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)"}
   Replace *<non-admin-sid>* in this command with the SID you obtained.

Using the host configuration utility

The host configuration utility allows you to configure and/or verify the WSMAN settings that Dell SRM requires for Windows host discovery. It is available at `<APG Home Directory/Collecting/Stream Collector/Generic-RSC/scripts/windows>`

The script verifies and performs the following actions:

- Ensures that the WINRM service is running
- Creates a listener port for accepting WS-MAN requests
- Adds firewall exceptions to open port 5985 as non-SSL and 5986 as SSL
- Sets Basic or Negotiate authentication mode, based on an input argument to the script (`-authType <Authentication_type>`), to true. (Dell Technologies recommends Negotiate.)
- Sets MaxTimeout value to 300000 ms.
- Checks whether fcinfo package is present on the host, if Windows 2003
- Verifies the presence of INQ on the host and checks its version, if Windows 2003

Usage

```
./hostconfig-srm.ps1 <-verify | -set | -set -force> [-authType <authentication_type>] [-ssl
[-thumbprint <thumbprint_value>] [-CN <certificate_hostname>]] [-user <username>][-help]
```

Table 19. Host Configuration utility command options

Options	Description
-help	Displays the help menu of the script.
-verify	Verifies current settings on the Windows host.
-set	Configures settings on the Windows host.
-set -force	Changes configuration settings without prompting the user. The -force option must be used with the -set option.
-authType *authentication-type*	Provide this option to set the authentication type for WS-MAN to Negotiate or Basic.
-ssl	Configures and verifies the SSL certificate specific settings on the host for WS-MAN discovery with SSL. For secure communication, the data transport should be made secure where SOAP packets would need to be encrypted with certificates.
-thumbprint *thumbprint_value*	Configures the SSL certificate with the specified thumbprint_value on the host. This option must be used only with the -ssl option.
-certhostname *certificate_hostname*	Configures the SSL certificate with the specified certificate_hostname value on the host. This option must be used only with the -ssl option.
-user *username*	Configures the host to enable discovery using the non-admin username provided.

Sample usage of hostconfig-srm.ps1 script

The following screens show how to perform actions with the Host Configuration Utility.

- Verify whether host is ready for discovery with HTTP using Negotiate authtype by running the following command on the target windows host to be discovered: `.\hostconfig-srm.ps1 -verify -authType Negotiate`
- Set Negotiate authtype for a successful discovery with HTTP on Windows 2008: `.\hostconfig-srm.ps1 -set -authType Negotiate`

Configuring group policy

Use a group policy if you do not want to set the configuration on each and every host (either manually or using a script). The group policy lets you apply a set of configurations across a set of hosts. You have to configure the group policy so that it can be applied across hosts as required.

Steps

1. Right-click **Computer** and select **Manage**.
2. Go to **Features** > **Group Policy Management** > **Forest Domain name** > **Domains** > **Domain Name** > **Default Domain Policy**.
3. Right-click **Default Domain Policy** and select **Edit**.
   The group policy editor appears.
4. Select **Default Domain Policy** > **Computer Configuration** > **Policies** > **Administrative Templates** > **Windows Components** > **Windows Remote Management**.
5. Modify the following parameters as required:
   - Enable `Allow automatic configuration of listeners`.
   - Enable `Allow Negotiate Authentication` (for domain user).
   - Add Windows Firewall exception for Port 5985 - HTTP
   - Add Windows Firewall exception for Port 5986 - HTTPS

   NOTE: HTTPS listener configuration is not possible from Group Policy.

Configuring firewall port exception using group policy

Using group policy, you have to configure firewall port exception if you are not using default ports.

Steps

1. Click **Computer**.
2. Go to **Computer Configurations** > **Policies** > **Windows Settings** > **Windows Firewall with Advanced Security** > **Inbound Rules**
3. Create a new inbound rule
   This enables the WinRM communication.

Updating group policy

If you update the group policy on a domain controller, the changes are reflected on the computers that are part of the domain in approximately 90-120 minutes. Use this procedure to force update the group policy on the member computers.

Steps

You can use any of the options for force update of group policy:

Option	Comment
Run the command `gpupdate/force` on all the member computers. This command results in a fetch operation for the group policy	This command has to be run on all the hosts and hence maybe cumbersome.
Change the Group Policy Refresh Interval in the Group Policy Management editor under **Computer Configuration** > **Administrative Templates** > **System** > **Group Policy**	Minimum possible time is 7 minutes. Reducing refresh interval is not recommended as it increases the load on the network.

Generating a certificate

WinRM HTTPS requires a local computer server authentication certificate or self-signed certificate with a CN name installed on the host. The certificates should not have expired or been revoked.

About this task

Perform the following to create certificates:

Steps

1. Generate a .pfx certificate
2. Exporting the .pfx certificate
3. Importing the .pfx certificate
4. Generate a .cer file
5. Import the .cer file

Generating a .pfx certificate

You can generate the required certificate using any certificate generator. This procedure demonstrates generating a certificate using `makecert`.

Steps

1. From the command prompt, run `C:\>makecert.exe -ss MY -sr LocalMachine -n "CN=<certificatename>" -sky exchange -pe -a sha1 -eku 1.3.6.1.5.5.7.3.1`

The above makecert command can only be used for operating system versions prior to Windows Server 2012 and not including Windows Server 2012.

a. To generate a certificate for Windwos Server 2012, run the command: `New-SelfSignedCertificate -CertStoreLocation cert:\LocalMachine\My -DnsName "<host-name>"`

   Here DnsName is considered as the Certificate Name(CN) so the hostname is compulsory.

b. To generate a certificate for Windows Server 2016, run the command: `New-SelfSignedCertificate -CertStoreLocation cert:\LocalMachine\My -Subject "CN=<host-name>" -KeySpec KeyExchange -KeyExportPolicy Exportable -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.1") -HashAlgorithm SHA256`

   Hostname is compulsory for certificate name(CN=hostname) for -Subject parameter.

This creates a certificate under the personal store. Use the following steps to verify the certificate created using `makecert` and `New-SelfSignedCertificate`.

2. On a Windows host, click **Start** > **Run**.
3. Type **mmc** and click **OK**.
   The Console window appears.
4. Click **File** > **Add/Remove Snap-in**.
5. Select **Certificates** under **Available snap-ins** and click **Add**.
6. Select **Computer account**.
7. Click **Finish**.
8. Click **OK** in the **Add or Remove snap ins** window.
9. On the left pane, double click **Certificates (Local Computer)** > **Personal** > **Certificates.**
10. On the right pane double click the certificate listed.
11. Navigate to **Details** tab. Select **Subject** to get the CN Name and **Thumbprint** to get the Thumbprint of the certificate.

    Note the **CN Name** and **Thumbprint** value, which will be used later while creating a WSMAN listener for HTTPS.

Exporting the .pfx certificate

To use the same certificate on multiple hosts, the generated certificate has to be imported on other hosts.

Steps

1. On a Windows host, click **Start** > **Run**.
2. Type **mmc** and click **OK**.
3. In the Console window, click **Certificates (local Computer)** > **Personal** > **Certificates**.
4. Double-click **Certificates**.
5. Under **Details**, click **Copy to File**.
6. In the **Certificate Export Wizard** select **Yes, export the private key**. and click **Next**.
7. Select **Include all certificates in the certification path if possible** and click **Next**.
8. Type a password for the private key.
   This password is used when you import this certificate on other hosts.
9. Type a filename and save the `.pfx` file.

Importing the .pfx certificate

You have to import the `.pfx` on other hosts if you want to use the same certificate on multiple hosts.

Prerequisites

The `.pfx` certificate must be copied on the host where it is to be imported.

Steps

1. On a Windows host, click **Start** > **Run**.

2. Type **mmc** and click **OK**.
3. In the Console window, click **Certificates (Local Computer)** > **Personal** > **Certificates**
4. Right-click and select **All Tasks** > **Import**.
5. In the browse window, select the `.pfx` certificate and click **OK**.

Generating a .cer file

The `.cer` file is created from a .pfx certificate with only a public key, which is used along with the private key for a successful handshake between the client and server.

Steps

1. Go to **Start** > **Run** > **mmc** > **Certificates (Local Computer)** > **Personal** > **Certificates**
2. Double-click **Certificates**.
3. Under **Details**, click **Copy to File**.
4. Select **No, do not export the private keys.**
5. Selecting the **Encoding type** as DER or Base-64, and click **Next**.
6. Type a file name and click **Save**.

Importing a .cer file

You have to import the .cer file on the collector host to enable a successful handshake between the server and the client.

Steps

1. Copy the .cer file on the collector host.
2. Log in to the collector.
3. Run the command `/opt/APG/Java/Sun-JRE/6.0u45/bin/keytool -import -file` *<Public_Certificate_File>* `-keystore /opt/APG/Java/Sun-JRE/6.0u45/lib/security/cacerts -alias` *<Name>*

   The command prompts for keystore's password. The default password is **changeit**.

   A sample output returned by the command:

```
Owner: CN=<CN Name>
Issuer: CN=Root Agency
Serial number: 522200243f029a894c741bcb83d58a5d
Valid from: Tue Dec 10 11:59:03 EST 2013 until: Sat Dec 31
18:59:59 EST 2039
Certificate fingerprints:
MD5: 99:2A:6E:DC:CD:D7:7E:7D:07:C3:E2:8A:8F:E1:BB:DD
SHA1:
17:29:F4:45:99:AE:DC:C5:08:C6:73:D4:CF:A6:BE:7E:79:48:50:76
Signature algorithm name: SHA1withRSA
Version: 3
Extensions:
#1: ObjectId: 2.5.29.1 Criticality=false
#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
serverAuth
]
Trust this certificate? [no]: yes
```

UNIX host/LPAR (VIO Server/Client) configuration for discovery and data collection

Dell SRM supports discovery of several UNIX variants. Each UNIX environment requires configuration for Dell SRM to collect data consistently.

Software to preinstall on UNIX hosts for discovery

The following software must be available/installed on UNIX hosts for successful Dell SRM discovery:

- INQ binary (an EMC command line executable). You can acquire INQ in the following ways:
  - Enable the Push INQ check-box on the generic-rsc block to allow Dell SRM to push inq directly to a host. This is enabled by default.
  - Preinstall INQ at a user-specified location on the host at a location provided to Dell SRM during SolutionPack installation.
  - INQ 9.0 needs to be made available on the host. Platform-specific INQ can be downloaded from `ftp://ftp.emc.com/pub/symm3000/inquiry/`.

    NOTE: Note: INQ 9.0 is supported only on 64-bit OS platforms. INQ 7.6.2 must be manually copied onto 32-bit target hosts.

  - The downloaded platform-specific binary should be renamed to inq and placed in any user-defined location. The location where the INQ binary is placed must be provided to Dell SRM during installation of the SolutionPack for Physical Hosts under Advanced settings: Location_inq.

    NOTE: The INQ binary should have executable permissions on the host.

- System Activity Report (SAR): SAR command is used by Dell SRM to collect performance metrics from hosts/LPARS. 'sar' is a part of systat package, identify the compatible version of systat package corresponding to the operating system and install it on hosts/LPARS required for discovery, if not already installed on the host/LPARS.

  NOTE: The SolutionPack for Physical Hosts does not package the SAR utility.

Configuring sudo for host/LPAR (VIO Server/Client) discovery

Due to security constraints, Dell SRM must be able to discover Linux and UNIX hosts in a data center even with non-root credentials. SUDO is a tool on UNIX hosts that can temporarily elevate user to execute command as root. Administrators can add specific commands in the sudoers file to enable Dell SRM to execute those commands and collect host information.

Prerequisites

Supported sudo versions

Linux Fedora distribution	sudo-1.8.6 and above
Other operating systems	any version of sudo

Steps

1. Include the path of sudo command in the environment variable $PATH for the sudo user.
   The variable $PATH can be set either in `/etc/environment` or `/etc/default/login` or any other OS specific file.
2. Include the paths of OS commands in the environment variable $PATH for sudo user.
   By default, most of the OS commands are located at the following location: `/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin`
3. Verify that the $PATH is correct.
   a. Log in as sudo user
   b. Type **`which sudo`**.

```
[lgloe239@lglbw017 ~]$ which sudo
/usr/bin/sudo
[lgloe239@lglbw017 ~]$
```

4. Ensure that the sudoers file is available.

   By default, the sudoers file is available in `/etc or /opt/sfw/etc/ or /usr/local/etc/sudoers`

5. Add the following line to the defaults section of the sudoers file:

   ```
   Defaults !requiretty #for all users
   ```

   or

   ```
   Defaults : SRMADMIN !requiretty #for a specific user
   ```

6. For AIX hosts, if inq gives partial information, add the following line:
   `Defaults env_keep += "ODMDIR"`
7. Ensure that the sudo user has root privilege to run the following commands on a given host.

   Ensure the absolute path to the packages are provided in sudoers file.

   Dell Technologies recommends to use visudo to edit sudoers file. Some packages are not installed by default.

AIX	sar, inq, powermt, vxdisk, swap, kdb (kdb is only for VIO Clients)
Linux	sar, inq, powermt, vxdisk, dmidecode, lvs, pvs, vgs, multipath
HPUX	sar, inq, powermt, vxdisk, /opt/sfm/bin/CIMUtil (CIMUtil is required only in Dell SRM 3.5.1 or higher)
Solaris	sar, inq, powermt, vxdisk, mpstat

```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname

## rather than USERALIAS
User_Alias SRMADMIN = srmadmin

## Command Aliases
## These are groups of related commands...
Cmnd_Alias SRMCMD = /usr/local/bin/sar,/usr/sbin/lvdisplay,/usr/sbin/p
vs,/home/srmadmin/inq,/usr/sbin/dmidecode,/usr/sbin/vxdisk,/usr/sbin/v
gs,/sbin/powermt,/sbin/multipath

# Defaults specification
#
# Disable "ssh hostname sudo <cmd>", because it will show the password
 in clear.
#         You have to run "ssh -t hostname sudo <cmd>".
#
Defaults   !requiretty

## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL
SRMADMIN ALL=NOPASSWD:SRMCMD
```

Figure 1. Sample sudoers file for Linux OS

Configuring PowerBroker for host/LPAR(VIO Server/Client) discovery

PowerBroker for UNIX & Linux allows system administrators to delegate UNIX and Linux privileges and authorization without disclosing passwords for root or other accounts. Administrators can add specific commands in the configuration/policy files to enable Dell SRM to execute those commands and collect host information.

Steps

1. Include the path of the pbrun command in the environment variable $PATH for the powerbroker submit/run host.
2. Include the paths of the OS commands in the environment variable $PATH for the pbrun user. By default, most of the command files have the following location:

   `/usr/local/:sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin`
3. Verify that the $PATH is correct.
   a. Log in to the submit/run host.
4. Type "which pbrun".

```
-bash-3.2$
-bash-3.2$ which pbrun
/usr/local/bin/pbrun
-bash-3.2$
```

Figure 2. Screenshot 1: which pbrun

5. The configuration/policy files exist on the master host and they must include the pbrun user name and the associated commands for host discovery. The following screenshot displays the policy files for a configuration in which the master/submit/run host is on the same host:

```
#=====================================================================
# Purpose:
# This policy defines a list of user-defined variables. These variables
# become visible through out all of included policy files.

#=====================================================================

# This user-defined procedure performs house-cleaning work to ensure that
# the PowerBroker eventlog is not cluttered with auxiliary policy data
# This procedure must be called before every explicit accept or reject
# as well as after every implicit reject
procedure CleanUp() {

    for (i = 0; i < length(UserVars); i++) {
        unset(UserVars[i]);
    }
    unset("i");
    unset("UserVars");

}

# When in the same policy file, all intructions (assigments and other policy
# constructs) must follow any user-defined function or procedure,
RootUsers  = {"cmguser", "UserTwo"};
PBShellUsers = RootUsers + { "UserThree", "qatester" };
PbShells   = { "*pbksh*", "*pbsh*" };
IologProgs = {"pbvi", "bash", "sh", "ksh", "csh", "fdisk", "telnet", "ssh"}
             + PbShells;
RootProgs  = {"kill", "chmod", "chgrp", "chown", "rmdir", "mkdir", "ls", "id",
              "pbreport", "inq", "dmidecode", "vgs", "lvdisplay", "pvs"};
UserVars   = { "RootUsers", "PbShells", "IologProgs", "RootProgs" };
```

Figure 3. Screenshot 2: Policy Files for a configuration

In this screenshot, the RootUsers variable includes "cmguser", which is the submit user (the Dell SRM user used for discovering the host details) and the RootProgs variable includes the various commands required by Dell SRM to discover the host. Note that the commands mentioned in the section about configuring sudo apply here as well.

NOTE: The configurations above are sample configurations for reference. Contact your host admininistrator to make changes according to your environment.

Configuring centrify dzdo for host/LPAR(VIO Server/Client) discovery

Refer to the Centrify Suite Evaluation Guide for Linux and UNIX in the Centrify documentation or contact your server administrator.

Generating a public and private key pair

About this task

For the SSH key method of discovering UNIX hosts/LPAR (VIO Server/Clients), you must generate a valid public and private key pair. You can choose any key generation tool to generate a valid public and private key pair.

Before you begin:

Before you begin host discovery, you must have a public key present on all the UNIX hosts/LPARS that are to be discovered using the private key. You can create SSH keys in any Unix environment and import them onto the Dell SRM collector. Dell Technologies recommends that you create public-private SSH keys on Dell SRM collectors (Linux VMs) where host discovery will be initiated.

These steps describe the procedure to generate a public and private key pair for UNIX hosts/LPARS using the ssh-keygen tool.

NOTE: The public key is to be added to the authorized_keys file on the target hosts intended for discovery and the private key is to be imported to the collector VMs where discovery is triggered.

Steps

1. A Public-Private key can be generated using the following command:
   ssh-keygen -t rsa -f <location_of_the_private_key/name_of_ private_key_file> -N ""

   For example: **ssh-keygen -t rsa -f /root/.ssh/id_rsa -N ””**
2. Ensure that the public and private key pair that is generated has the following permissions:
   - **chmod 600 /root/.ssh/id_rsa**
   - **chmod 644 /root/.ssh/id_rsa.pub**

   The private key file is `id_rsa`

   The public key file is `id_rsa.pub`
3. To make the key pair functional, append the public key to *<user's home directory>*`/.ssh/authorized_keys` in the target UNIX host using the command `mkauthkeys --add "string"` where "string" is the content of id_rsa.pub file.

   Next, import the private key to the Collector used for discovery.

   NOTE: The public key is to be added to the authorized_keys or authorized_keys2 (depending on the HMC version) file on the target hosts intended for discovery and the private key is to be imported to the collector VMs where discovery is triggered.

Importing a private key into the Collector

Steps

1. The private key should be placed inside APG's HOME directory (where APG is installed).

   For example: UNIX: `/opt/APG/`.
2. Type **chown apg:apg *<private_key_file>***.

   This command changes the owner.

   The HMC is now ready for successful data collection.

Configuring SSH authentication

Do the below changes if SSH authentication fails on any UNIX Host/LPAR. Modify the `/etc/ssh/sshd_config` file and restart the sshd service to allow successful SSH authentication.

Steps

Change the following value to **`yes`**:

```
#PasswordAuthentication no <--- original
#PasswordAuthentication yes <--- modified
```

Uncomment the `PasswordAuthentication yes` after modification.

Discovery via Host Agent for UNIX/Linux

The Host Agent for UNIX/Linux allows you to discover hosts via a non-privileged user with read-only access to the `/tmp` directory. You can provide a non-admin/service account user with read-only permission to Dell SRM to authenticate the host and collect metrics generated by the host agent.

Prerequisites

NOTE: Create a non-privileged user account with read only rights on the target host to be discovered.

The host agent is provided as a self-extracting shell script (`srmhostagent.sh`) that upon execution extracts the `LUNMappingDdetection.pl` script, supporting perl modules, and `inq-archive.tar` on the target host in the `/opt/emcsrm` directory.

NOTE: Host agent installation on server will support only for English locale, any other language will not be supported.

The following items should be available and running as root user on the target host:

- `srmhostagent.sh` – A self-extracting script file with the following components:
  - `LunMappingDetection.pl`
  - `LunMappingDetection_conf.txt`
  - `RSC.pm`
  - `RSCPP.pm`
  - `PerfMon.pl`
  - `inq-archive.tar`
  - `startup_config.pl`
  - `RSC_Block.pm`
- A cron job entry that you will configure while extracting `srmhostagent.sh` for the scheduled run of `LMD.pl` (procedure explained below).
- The Reports component of the SolutionPack for Physical Hosts must be installed on the Frontend server.

Steps

1. Download `srmhostagent.sh` to a temporary directory on the target host.
2. As the root user, run `srmhostagent.sh`. The script creates a folder named `emcsrm` in the `/opt` directory and extracts the perl scripts and modules used for discovery to the `/opt/emcsrm` directory.

   For example, `./srmhostagent.sh customize=yes cronadd=yes`

   `customize=yes` allows you to configure advanced settings. You can reconfigure all of those questions that are asked during the installation of the SolutionPack for Physical Hosts with `customize=yes`.

   `cronadd=yes` adds a cronjob that triggers the host discovery script based on the polling interval (the default is 15 minutes).

   ```
   # ./srmhostagent.sh customize=yes cronadd=yes
   Verifying archive integrity...  100%   All good.
   Uncompressing Extracting LunMappingDetection.pl and supporting perl modules  100%
   ```

```
Collect performance metrics Point in time data [y/n] Default [y]:
Collect performance metrics for PowerPath LUNs [y/n] Default [y]:
Collect performance metrics for PowerPath Bus [y/n] Default [y]:
Collect performance metrics Average over time [y/n] Default [n]: y
Collect performance metrics for Networks ports [y/n] Default [n]: n
Collect performance metrics for PowerPath range-bound [y/n] Default [n]: y
Creating "/opt/emcsrm" and extracting all files within, proceed..? [Y/n] Default [y]:
Successfully updated cron entry
```

`./srmhostagent.sh` -h displays help on how to use `srmhostagent.sh`.

NOTE: Avoid using any of the other options while running the ./srmhostagent.sh command except --quiet option.

When run without any parameters, you can run the script any number of times without consequence and it will re-extract the files under `/opt/emcsrm`. When run with parameters such as “customize=yes” and “cronadd=yes”, there is a possibility that the configuration settings provided with a customized installation will be overwritten with subsequent executions of the `srmhostagent.sh` script. Dell Technologies recommends that you always use the “customize=yes” and “cronadd=yes” options together to prevent the possibility of overwriting the customizations. If the script is run without the “customize=yes” option, all configuration settings are set to their default values.

3. To upgrade `srmhostagent.sh`, download and execute the latest version as shown above. All the files in `/opt/emcsrm` location will be overwritten with the latest version.
4. To cleanup/purge `smrhostagent.sh` related files, use `cleanup=yes` option.

Results

The `LunMappingDetection` script creates an output file in `/tmp/hostdata_LunMappingDetection_<hostname>` that is read by the non-admin user credentials supplied to Dell SRM for discovery of the target host.

NOTE: Dell SRM release specific `srmhostagent.sh` is uploaded to Dell Support Site whenever there are any new changes. Download and execute the latest version to upgrade the Host Agent for UNIX/Linux binary: `srmhostagent.sh`.

Configuring ESX hosts to collect PowerPath metrics

This procedure describes how to configure ESX hosts to collect PowerPath metrics.

Prerequisites

- Ensure that PowerPath/VE remote CLI (rpowermt) is installed on the host and enable performance collection by running the `rpowermt set perfmon={on [interval=<#seconds>] | off} host=HOST_FQDN` command. The *Dell SRM Support Matrix* provides more information on supported PowerPath versions.
- Register ESX and enable performance for reporting. Refer to the Powerpath /Ve or RTOOLS documentation about how to register an ESX server and enable performance.
- Configure the host where RTOOLS resides in generic-RSC based on the operating system type (ESX-LINUX or ESX-Windows).

About this task

You can discover ESX and VMs running on the ESX server using the SolutionPack for VMware vSphere vSAN & VxRail. However, the vCenter API does not provide all PowerPath metrics. Therefore, if you want PowerPath metrics, you need to provide the IP addresses of the RTOOLS host (physical host or VM) in addition to discovering the VMs using the SolutionPack for VMware vSphere vSAN & VxRail. Depending on whether the RTOOL host is running on Windows or Linux OS, you have to configure the generic-rsc collector with OS type as ESX Windows or ESX Linux, respectively, to collect PowerPath metrics.

Steps

1. Create a lockbox.
2. Update host username and password in the lockbox.

   The PowerPath/VE for VMware vSphere Installation and Administration Guide provides detailed description of performing the above steps. PowerPath reports can also be accessed from **Explore View** > **Host** > **Storage Connectivity.**

   PowerPath reports are available for the SolutionPack for IBM LPAR.
3. In **Host configuration** under **Device Management**, add one of the following options for the RTOOLS host:

- **ESX Linux** if the RTOOL application is running on a physical host or VM running Linux.
- **ESX Windows** if the RTOOL application is running on a physical host or VM running Windows.

Configuring hosts to collect PowerPath metrics

Provides information about configuring host to collect PowerPath metrics.

About this task

To collect PowerPath metrics, do the following:

Steps

1. Install PowerPath CLI (powermt) on the host.

   NOTE: The PowerPath CLI is installed by default during the PowerPath installation.

2. Enable performance collection by running the `powermt set perfmon={on [interval=<#seconds>] | off}` command.

   NOTE: The *Dell SRM Support Matrix* provides more information on supported PowerPath versions.

Installing the SolutionPack

Prerequisites

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- For non-admin users, the SolutionPack for Physical Hosts will report an authentication error during discovery if the user is not part of the remote admin users group. To avoid this issue, add non-admin users to the WinrMRemoteWMIUsers__ group. If that group does not exist, add non-admin users to the DCOM group on the Windows host.

About this task

The steps below assume a typical four server deployment: Primary Backend, Additional Backend, Collector, and Front End.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name if you wish to change the default instance name of generic-host.
5. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays a note about Alert Consolidation.
7. Click **Next**.
   The window displays a note about pre-configured alerts.
8. Click **Next**.
   The window displays reports settings.
9. In **Administration Web-Service Instance**, select an existing instance which is default.
10. Click **Next**.
    The window displays script settings.
11. Select the performance metrics that you want to collect. Click **Use advanced settings** to configure the absolute paths of the binaries.
12. Click **Install**.

13. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.

SolutionPack reconfiguration

About this task

If you want to change the answers that were provided during the SolutionPack installation, you can change them by reconfiguring the SolutionPack.

Steps

1. Click **Administration**.
2. Navigate to **Discovery** > **SolutionPacks** > **Installed SolutionPacks** > **Physical Hosts**.
3. Within the Instance column, click the edit icon to reconfigure the component that you want to modify.
   The Reconfiguring dialog box appears.
4. Change the configuration as desired.
5. Click **Reconfigure.**

Adding and configuring devices in Discovery Center

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click on the SolutionPack.
   These steps describe how to add hosts individually. For information about using discovery groups to use the same credentials to discover multiple hosts, see Adding devices to discovery groups.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE:
   - The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.
   - Secure Vault is not supported for public key-based device discovery mode scenarios in SolutionPack for Physical Hosts.

5. Select the Server and Instance where you want to store the configuration details for this device.
   - Server: If multiple collectors are deployed, then choose the collector from the drop-down where "generic-host: script block" is installed.
   - Instance: Generic-RSC is the default instance name unless an additional "generic-rsc" block is installed.
6. Enter the hostname.
7. Select the discovery mode from the **Specify the discovery mode** drop-down menu.
   If you select **Host Containers**, enter one or more HBA port WWNs in the Host Port WWN field. Multiple WWNs must be separated by a semicolon (;). This field is not case-sensitive.
8. If you select Agentless or HostAgent UNIX/Linux discovery, or HostAgent Windows discovery, select the OS type from the **Specify the OS type** drop-down menu.

   NOTE: For HostAgent UNIX/Linux, UNIX is the only option and it applies to all the UNIX/Linux flavors.

9. For AIX, ESX-Linux, HPUX, Linux, or Solaris hosts, from the **Authentication Type** drop-down menu, select:
   - Password based if you are using password-based authentication.
   - Unique key based if you are using secure vault-based authentication.
   - Public key based if you are using key-based authentication.

   NOTE: Agentless device discovery for ESX-Linux/ESX-Windows based systems is supported for ESX versions up to and including ESX 4.0.

10. For ESX-Windows or Windows hosts, from the **Connection Type** drop-down menu, select:

- HTTPS if you intend to use SSL certificates for authentication.
- HTTP if you intend not to use SSL certificates for authentication.

11. For Windows, if you have a custom WinRM URLPrefix, enter the same. Leave it blank if wsman is the default URLPrefix.
12. Provide the username (root/non-root/administrator/non-admin/service account user).
13. If you are using password-based authentication (UNIX) or HTTP-based Connection type (Windows), provide the password for the host.
14. If you are using secure vault, provide the unique key.
15. If you are using key-based authentication, provide the absolute location of the private key: /opt/APG/<Name of private key>
16. Type the network port.

Table 20. Network Default Port

Protocol	Default Port
SSH	22
HTTP	5985
HTTPS	5986
SSH (Windows Host)	5989

17. Keep the default settings for the Collection level and Force collection.
18. Click **Validate and Add** to validate the credentials.
19. Click **OK**.
20. Click **Save**.

Adding devices to discovery groups

Discovery groups simplify the process of working with a large number of devices and their corresponding IP addresses/hostnames and discovery credentials. For example, if you have set of four user/password credentials used among twenty devices, using a discovery group allows you to enter each set of credentials and all of the IP addresses/hostnames, and the discovery group will match the correct credentials to each device.

Steps

1. Click **System Admin** > **Settings** > **Manage Discovery Backends**.
2. Select the Backend server.
3. Click **Register**.
4. Select the collector you want to use for discovering your SolutionPack objects.
5. If you are collecting VMware vCenter events, select the primary backend you want to use for discovering the events.
6. Click **Register**.
7. Navigate to **Discovery** > **Discovery Center** > **Manage Discovery**.
8. Click **<Device Name>**.
9. Click the **Discovery Groups** tab.
10. Click **Add new Discovery group**.
11. Provide a name for the group and click **Ok**.
12. Click the newly created group.
13. Under **Credentials**, click **Add new entry**.
14. Type the username.
15. If required, select the authentication type.
16. If you are using password authentication, provide the password and click **Ok**.
17. If you are using key-based authentication, provide the absolute location of the private key and click **Ok**.
18. Repeat the previous five steps to add as many username/password (or key) combinations as you would like.
19. Under **Hostname or IP address**, click **Add new entry**.
20. Provide the Hostname/IP Address of the device. If required, provide the Network Port. Click **Ok**.

21. Repeat the previous two steps to add as many devices as you would like.
22. Click **Save**.
23. Click the **Collected Devices** tab.
24. Click **Discover**.
25. Select the **Discovery group** and **Discovery Mode** and click **Ok**.
    The progress bar is displayed above the Collected Devices tab.
26. When the progress bar is gone, click the**Discovery Results** tab.
27. Click the group name that you added.
28. Under the group name, you can see the status of all the devices that you added.
29. Click **Import to Collected Devices**.
30. Merge the devices if you want to retain older devices that were added previously.
31. Click **Ok**.
32. Select the action and click **Continue**.
33. Click **Save**.

Next steps

Review your devices and credentials to avoid lockout of devices due to multiple attempts of incorrect credentials. Dell Technologies recommends that you create groups in such a way that devices have a minimal set of credentials to be tried against. Dell Technologies recommends using common public-private key pairs for multiple devices.

Configuring Dell SRM to search for additional paths for INQ

About this task

To configure Dell SRM to look in additional paths for INQ, use the following procedure:

Steps

1. Log into the Dell SRM UI with an account that has administrator privileges.
2. Click the **Administration**.
3. Navigate to **Discovery** > **SolutionPacks** > **Installed SolutionPacks**.
4. Select the SolutionPack.
5. Click the pencil icon to edit the scripts component of the SolutionPack for Physical Hosts. The **Reconfiguring** page displays.
6. Select the **Use advanced settings** checkbox to display the **Location of the inq binary** field.
7. Type the path where INQ is located on the target host into the **Location of the INQ binary** field. For example, `/usr/site/bin`.
8. Click **Reconfigure** and apply the change.

Recommendations

- Do not discover the same host using agentless discovery, EHI agent-based discovery, and HostAgent Windows.. Simultaneous discovery results in duplicate data collection. If you switch from agentless discovery to EHI agent-based discovery (or vice versa), the metrics collected from the previous discovery mechanism become inactive.

iSCSI Support

iSCSI is supported on Windows and Linux platforms with the following arrays.

Table 21. iSCSI Support

SolutionPack	Array Platform Supported for iSCSI	
	Dell VMAX/PowerMax	Dell EMC XtremIO
SolutionPack for Physical Hosts	Yes	Yes

NOTE:
- Dell EMC VMAX 3 arrays onwards are supported.

Limitations

This section lists the limitations of SolutionPack for Physical Hosts.

- For **Dashboards** > **Hosts**:
  - Distribution by operating system: The total count will not match the All Hosts (Excluding ESX) if "devdesc" (Operating system details) is not collected for VMs.
  - Distribution by Multipath: Windows hosts that have native DMP or PowerPath installed, but are not using it to manage disks, will not be visible in this report.
- This SolutionPack does not identify LUNs from the Hitachi AMS200 array, due to the unavailability of WWN using in-band SCSI mechanisms accessible to the hosts, hence the LUNs associated with the array cannot be matched with the disks from the hosts.
- On Windows hosts, if the multipathing software on the host does not support any array, the LUN from that array may show up as multiple host physical drives.
- Physical hosts connected to IBM DS 8000 do not show "Connected array" and "LUN" in the SAN disks report.
- For Windows Server 2008 host discovery with non-admin user using *WinRMRemoteWMIUsers* group, SAN Disks and Internal Disks report will not be reported. Reports exist only above Windows Server 2012 onwards.
- For SRM 3.7.1 and higher, if you are using the aes256-ctr encryption algorithm for enhanced security, follow the instructions in KB article 000463134.
- If the same performance data is represented in multiple ways on the same report (such as on a standard table and a simple chart), if data collection stops for 24 hours, it is possible for one of the displays to contain data while the other is blank. This is caused by different time management settings between the two displays.
- End to End use cases like "Topology" and "Storage connectivity > Connectivity" are not supported on UNIX platforms (other than Linux) configured on CISCO UCS Servers mounted with CISCO VNIC HBAS. This is due to inherent dependencies on inq and in-turn SNIA libs.
- iSCSI is supported for Windows and Linux platforms only.
- Agentless discovery on Windows hosts does not support non-admin domain accounts. It only supports domain users who are part of the administrator's group.

44

SolutionPack for Pure Storage

Topics:

Overview

The SolutionPack for Pure Storage enables users to view capacity, performance, and inventory information across multiple Pure Storage systems.

Installing SolutionPack

Prerequisites

- Respective PURE storage `array_name` should be uniquely configured for each Pure storage array as SRM considers the real `array_name` for data collection purposes.
- Pure Storage `array_name` can be viewed and/or edited by navigating to **Settings** > **System** in the respective Pure Storage array element manager.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Leave the **Instance name** as default.
5. Assign a server for each component.
   The recommended servers are selected automatically in a typical four server deployment.
6. Click **Next**.
   The window displays a note about **Alert Consolidation**.
7. Click **Next**.
   The window displays **pre-configured alert** details.
8. In the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting on data collection**.
   If you select **Add a new alerting on data collection**, **Alerting Web-Service Instance** drop-down should be left as default. Do not change the value.
9. Click **Next**.
   The window displays data collection details.
   a. In the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.
      If you select **Add a new data collection**, provide the information about the data collection. In **Hostname or IP address to send data to** field, enter the preferred localhost IP address. In **Network port to send data to** field, enter **2020** port number. It is the Collector host where the Load Balancer Connector is installed.
   b. In the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

If you select **Add a new Frontend Web service**, provide the required information about the **Frontend Web service**.

c. In the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

If you select **Add a new Topology Service**, provide information about the **Topology Service hostname or IP address** and the relevant **Web-Service Gateway**. In **Topology Service hostname or IP address** field, specify the Primary Backend host.

d. In the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.

10. Select a polling period in the polling period drop-down list for **Collection interval for Pure Capacity and Topology**, and **Collection interval for Performance** fields respectively.
11. Clear **Enable Snapshot collection** check box in order to disable Snapshot collection for Pure arrays.
12. Click **Next**.

The window displays reports settings.

Leave **Administration Web-Service Instance** field as default.

13. Click **Install**.
14. Click **Ok**.

Monitor the installation logs to ensure that the installation completes successfully.

Adding and configuring devices

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Pure Storage**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.

On selecting Secure Vault checkbox, the Unique Key field appears.

NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Token is active.

5. From the **Pure Type** drop-down list, select **Pure Storage**.
6. In **Management IP address**, provide the Management IP address of the Pure Array System.
7. For **Token**, provide API token for the respective user.

NOTE: For more information about the API token, see the respective Pure Storage User Guide.

When the user is unaware of the API token [or when the API token is regenerated because of recent password change], the user must log in to the Pure array ssh session [using appropriate credentials] and run the below command in order to get the respective API token.

```
pureadmin list --api-token --expose
```

8. If the secure vault is enabled, in **Unique Key** enter the unique key.
9. To validate the credentials, click **Validate and Add**.
10. Click **OK**.
11. Click **Save**.

Adding Pure1 for power consumption data

About this task

To obtain power consumption reports for Pure Storage arrays, the user must configure Pure1 management details.

NOTE: Power consumption data will be collected from Pure1 for only those arrays that are discovered in SRM.

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Pure Storage**.
3. Click **Add...**
4. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
   On selecting Secure Vault checkbox, the Unique Key field appears.

   NOTE: The Unique Key field is enabled only when the Secure Vault checkbox is selected. When the Secure Vault checkbox is not selected, the Token is active.

5. From the **Pure Type** drop-down list, select **Pure1**.
6. In **Management IP address**, provide the Management IP address of the Pure1 management host.
7. For **Token**, provide a Subject token for the respective user.

   NOTE: For more information about the Subject token, see the respective Pure Storage User Guide.

8. If the secure vault is enabled, in **Unique Key** enter the unique key.
9. To validate the credentials, click **Validate and Add**.
10. Click **Ok**.
11. Click **Save**.

    NOTE: To collect carbon emission data for a device, ensure that the Carbon Emission Factor is tagged to it. See Configurations for collecting carbon emission data for more details.

Configuring Pure Storage arrays for alert consolidation

To forward SNMP alert traps from Pure Storage arrays to Dell SRM, perform the steps below:

Steps

1. Log in to the Pure Storage array at https://<array_management_ip>.
2. Go to **Settings** > **System**.
3. In the SNMP panel, click the menu icon for the SNMP manager object and select **Edit**. The **Edit SNMP Manager** dialog box appears.
4. Configure the hostname as Dell SRM primary backend hostname.
   - For SNMP v2c - Configure the SNMP Manager with the following information: **Name**, **Host**, **SNMP Version**, **SNMP Notification**, and **Community**.
   - For SNMP v3 - Configure the SNMP Manager with the following information: **Name**, **Host**, **SNMP Version**, **SNMP Notification**, **User**, and **Auth Protocol**.
5. Click **Save**.

Limitations

- Added a new column called **type** to support the new discovery type. As a result, CSV file imports will not work on SRM versions prior to 5.0.0.0. To ensure a successful import, it is necessary to include the **type** column before the **host** column. Set the values to **`pure1`** for Pure1 and **`pure`** for Pure Storage array.
- The Pure REST API 2.x does not support the following properties and metrics:

Table 22. Unsupported properties and metrics in Pure REST API 2.x

Component	Type	Name
Disk	Metric	`LastEvacCompletedDate`
Disk	Metric	`LastFailureDate`

Table 22. Unsupported properties and metrics in Pure REST API 2.x (continued)

Component	Type	Name
Disk	Property	`degraded`
Array	Property	`revision`

45

SolutionPack for ServiceNow

This chapter includes the following topics:.

Topics:

Overview

The SolutionPack for ServiceNow generates reports for the tickets that are raised in ServiceNow.

Integrating SRM with ServiceNow

Prerequisites

- Download the ServiceNow plugin from the Dell Support Site and ensure that you have access to a ServiceNow instance and an admin role in that instance.
- To forward existing System Health alerts to the ServiceNow URL, the Alert-Consolidation module must be reconfigured as follows:
  1. In **SRM Admin UI**, go to **Config** > **SolutionPacks** > **Installed SolutionPacks** > **Other Components**.
  2. Click the edit icon next to the **Alert-Consolidation** instance.

     The Reconfiguration dialog box appears.
  3. Select the **Enable Alert Notification** checkbox.
  4. Click **Reconfigure**.

Steps

1. Log in to the ServiceNow developer portal.
2. Activate the **Event Management** plugin from **My Instance** > **Instance action** > **Acivate Plugin**.
   Once the activation process is finished, you will receive an email notification.
3. Go to **System Update Sets** > **Retrieved Update Sets**.
4. Click **Import Update Set from XML**.
5. Click **Choose File** and select the provided XML file.
6. Click **Upload**.
   The plugin is now available as a retrieved update set in the **Loaded** state.
7. Click on the **Dell SRM integration** plugin.
8. Click **Preview Update Set**.
   The Update Set Preview page displays results and lists any problems that may have been detected.
9. If any problems are detected:
   a. Select all the listed problems.
   b. From the **Actions on selected rows...** drop-down list, select **Accept remote update**.
10. Click **Commit Update Set**.
    To verify, ensure that the **Dell SRM integration** tree is accessible now.

Installing the SolutionPack

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
5. Click **Next**.
   The window displays Backend settings.
6. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.
   If you select **Add a new Frontend Web service**, type information about the Frontend Web service.
7. Click **Next**.
   The window displays Frontend settings.
8. In **Administration Web-Service Instance**, select an existing instance which is default.
9. In **Configuration for Servicenow Backend Web-Service**, for four VM installations, From the **Web-Service Gateway** drop-down list, select the Primary Backend host for Web-Service gateway hostname or IP address of Web-Service Gateway.
10. In the **Servicenow Backend Instance**, select an existing instance which is default.
11. Click **Next**.
    The window displays reports settings.
12. In **Administration Web-Service Instance**, select an existing instance which is default.
13. Click **Install**.
14. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
    After installation is complete, you must restart Tomcat for the changes to reflect.

    NOTE: With SRM 5.0.0.0 release, the ServiceNow SolutionPack no longer supports device selection; customers must buy a production license to continue.

Configuring ServiceNow

To integrate SRM with ServiceNow, configure the following details:

Prerequisites

Before configuring, make sure that you have uploaded your license in **System Admin** > **License** > **Manage Licenses**.

NOTE: In SRM 5.0.2.0, a new property called "issue Details" has been added to show alert descriptions in ServiceNow. On SRM upgraded setups where the Service Now is already configured at either 5.0.0.0 or 5.0.1.0, add the "issue Details" property in the ServiceNow configuration page to display alert descriptions. Follow the steps below to add the property:

1. Navigate to **SRM Admin UI** > **CONFIG** > **ServiceNow** > **Configure ServiceNow**.
2. In the **AlertContent** section, select the **Issue Details** property and click **Add**.
3. Perform **Test Action** to verify the configuration and save it.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **ServiceNow** > **Configure ServiceNow**.
2. In **Custom certificate**, select No.

   NOTE: Currently, SRM does not support custom certificates.

3. In **URL**, enter the REST endpoint URL of ServiceNow.
4. In **Secret**, enter the secret string.
5. For **Username** and **Password**, provide the ServiceNow credentials.
6. From the **AlertContent** list, select the alert parameters that must be pushed to ServiceNow.

7. To verify the configuration, click **Test Action**.
8. Click **Save**.

Selecting the devices for alerts

Steps

1. Go to **CONFIG** > **ServiceNow** > **Device Selection**.
2. Type a name for the filter.
3. Right-click the **Filter Criteria** field and choose the appropriate criteria.
4. Click **Save**.
   The created device filters are displayed in a table.
5. Select the filter and click **Show Devices**.
   Based on the filter, the device list is fetched from the inventory database and the list of devices will be displayed.
6. Select the required devices and click **Save**.
   NOTE: Ensure that your selected devices do not exceed the maximum number of devices that are allowed in the license. If the maximum number of devices is reached, the remaining devices will be grayed out.

Configuring alerts for the selected devices

Steps

1. Go to **CONFIG** > **ServiceNow** > **Device Alert Configuration**.
   The window displays the previously selected devices.
2. Select the required severity level (1 = Critical, 2 = Major, and 3 = Minor) for each device.
3. Click **Save**.
   Monitor the alerting logs to ensure that the alerts are being triggered properly.

Retrieving alert details from ServiceNow

About this task

When an alert is pushed to ServiceNow, it is treated as an event. Upon successful saving in ServiceNow, the system returns an event ID, which is then updated in the *snoweventid* column of the **Generic Events Live** table. To retrieve this data, perform the following steps:

Steps

1. In **SRM Admin UI**, browse **CONFIG** > **Settings** > **Scheduled Tasks**.
2. Select the ServiceNow scheduled task and click **Run Now**.
   The scheduler task will initially retrieve the *snoweventid*s of active alerts from the event database. It will then fetch the corresponding data from ServiceNow, including the alert status, alert ID, incident ID, and incident status based on the *snoweventid*s.
3. The following new data columns are updated in the event database:
   - *snowalertid* – ServiceNow Alert ID
   - *snowalertstatus* – ServiceNow Alert Status
   - *snowincid* – ServiceNow Incident ID
   - *snowincstatus* – ServiceNow Incident Status
4. The UI report reflects these updates within 180 seconds. The updates are visible in the following reports:
   - **Report Library** > **ServiceNow** > **Summary** > **Alerts**: Captures all alerts that are forwarded to ServiceNow.
   - **Report Library** > **ServiceNow** > **Summary** > **Devices**: Displays alerts organized by device categories and offers visual representations including Alerts by Severity, Alerts by Category, and Trend Analysis.

   NOTE: If ServiceNow is pre-configured, you must restart Tomcat after upgrading to SRM 5.1.0.0 and higher versions for the changes to reflect in the reports.

46

SolutionPack for System Health

This chapter includes the following topics:

Topics:

Overview

This SolutionPack monitors the health of Dell M&R infrastructure. Take advantage of this no-charge SolutionPack to keep the Dell M&R services performing optimally, so you have instant access to performance data and reports when you need it.

Supported systems

Dell M&R 6.8u1 and later

Data collection methods

JMX

Main reports

Modules Performance

Collecting Level Performance

Backend & Databases events and utilization

Server summary

Installing the SolutionPack

Install this SolutionPack on all core software hosts in your environment.

Prerequisites

- Core modules must be up-to-date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.

Steps

1. In the **SRM Admin UI**, browse to **Config** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Type the instance name.
5. Assign a server for each component.
   In a typical four server deployment, the recommended servers are selected automatically.
6. Click **Next**.
   The window displays pre-configured alert details.

7. Click **Next**.
   The window displays data collection details.
8. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
9. From the **Alerting on data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new alerting data collection**.

   If you select **Add a new alerting on data collection**, Alerting Web-Service Instance dropdown will have default value. Do not change the value.
10. Select **Configure advanced settings** to configure polling settings.
11. Click **Next**.
    The window displays reports settings.
12. Click **Install**.
13. Click **Ok** once installation is complete.

    Performance data will displayed in about an hour.

    The following message might appear in the collection log during operation: WARNING -- [2014-04-25 05:26:38 EDT] -- f::a(): JVM IO ERROR 'No such process'. ID: '17032', NAME: 'lib/module-manager.jar exit'. You can ignore this message.

47

SolutionPack for VMware vSphere vSAN & VxRail

This chapter includes the following topics:

Topics:

Overview

The SolutionPack for VMware vSphere vSAN & VxRail generates real-time and historical reports that help you understand VMware performance for VMware Hosts, Virtual Machines, virtual networks and DataStores.

Configuring the SolutionPack to collect PowerPath data

This procedure is required to collect PowerPath data from ESX servers.

About this task

For monitoring PowerPath performance and path status, an RTools host is required. RTools is the remote CLI software for managing the PowerPath software on ESXi (or other) hosts. The Collector uses the Generic-RSC Collector to issue RTools command scripts to the RTools host to collect PowerPath data directly from the ESXi servers.

Steps

1. Add the hostname and credential of every ESXi host to the RTools default lockbox. Commands fail if the lockbox is not populated.

   The first use of the command creates the lockbox if necessary.
2. Generic-RSC Collector discovers the RTools host. Discover it through the SolutionPack for Physical Hosts using the ESX Linux or the ESX Windows host type. Choose the Linux or Windows type appropriate for the RTools host so that the collector can issue the correct format scripts.
3. Create the default lockbox on RTools Host and add ESXi hostname credentials:
   `rpowermt setup add_host host= username= password=`
4. Turn on performance monitoring on ESXi host from Rtools (if needed):
   `rpowermt set perfmon=on interval= host=`
5. For PASSWORD based discovery Suse Linux hosts from 3.0 RSC, it requires edits to the sshd_config file. Note that this file is located under /etc/ssh directory on discovery hosts. Enable "PasswordAuthentication" and restart sshd service on the host.

   ```
   lglah196:~/.ssh # grep Password /etc/ssh/sshd_config #PasswordAuthentication no
   #PermitEmptyPasswords no
   ```

```
lglah196:~ # /etc/init.d/sshd restart Shutting down SSH daemon done Starting SSH daemon
done
lglah196:~ #
```

Installing this SolutionPack

Prerequisites

- Core modules must be up to date in all servers because not all module dependencies are validated during the SolutionPack installation or update process.
- vSAN license will be available on demand, and vSAN report on SRM will be visible after adding the license.

Steps

1. In the **SRM Admin UI**, go to **CONFIG** > **SolutionPacks** > **Browse & Install SolutionPacks**.
2. Select the SolutionPack.
3. Click **Install**.
4. Assign a server for each component.

   In a typical four server deployment, the recommended servers are selected automatically.
5. Click **Next**.
   The window displays a note about Alert Consolidation.
6. Click **Next**.
   The window displays pre-configured alert details.
7. To receive alerts, select **Enable the Host PowerPath Alerts**.
8. Click **Next**.
   The window displays data collection details.
9. From the **Data collection** drop-down list, select existing settings that have been specified for other components, or select **Add a new data collection**.

   If you select **Add a new data collection**, type information about the data collection. In **Hostname or IP address to send data to**, use `localhost` on port 2020, which is the Collector host where the Load Balancer Connector is installed.
10. From the **Frontend Web service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Frontend Web service**.

    If you select **Add a new Frontend Web service**, type information about the **Frontend Web service**.
11. Leave **Enable Topology Backend on data collected** checked.
12. From the **Topology Service** drop-down list, select existing settings that have been specified for other components, or select **Add a new Topology Service**.

    If you select **Add a new Topology service**, provide information about the topology service and the web service. In **Topology Service hostname or IP address**, specify the Primary Backend.

    From the **Web-Service Gateway** drop-down list, select existing settings that have been specified for other components, or select **Add new gateway**. If you select **Add new gateway**, provide information about the web-service gateway where the topology service resides.
13. Optionally, select **Do you want to configure advanced settings** to configure the metric collection level, polling intervals, collection thread settings, and the re-synch interval.
    a. In **Metric Collect Level**, select the level of metrics you want the SolutionPack to collect per VMware collector block. The Metric Collect Level is an internal setting that tells the SolutionPack for VMware vSphere vSAN & VxRail how much data to collect. This setting is not related to vCenter statistics levels.

       Collect-Level 1 collects the minimum required metrics that are related to capacity, topology, memory, and CPU.

       Collect-Level 2 collects all metrics that are supported by Collect-Level 1 and also all metrics that are related to disks and memory.

       Collect-Level 3 collects all supported metrics, which include metrics that are collected under Collect-Level 1 and Collect-Level 2.
    b. In **Polling interval for VMware vCenter collection**, select a polling interval.
    c. In **Polling interval for VM files only**, select a polling interval.
    d. In **Number of collecting threads**, type the number of collection threads.
    e. In **Number of collecting threads for VM files**, type the number of collection threads.

f. In **Re-Sync interval**, select an interval.

Table 23. Metric collection level, polling intervals, collection thread settings, and the re-synch interval configuration

VMware vSphere vSAN & VxRail SolutionPack	-	-	Include Collection Level 1	Include Collection Level 1 and 2
Data Group (datagrp)	**Component (parttype)**	**Collection Level 1**	**Collection Level 2**	**Collection Level 3**
Hypervisor	Disk	1	7	1
	Diskpath	2	0	0
	Interface	1	5	0
	Memory	6	4	0
	Multipath	0	0	1
	Port	1	0	6
	PortGroup	0	0	1
	Processor	3	0	0
	Sensor	0	0	3
VirtualMachine	Datastore	1	0	0
	Disk	1	5	0
	File	1	0	0
	FileSystem	2	5	0
	Interface	2	0	4
	Memory	6	1	0
	Processor	2	1	0
	Virtual Disk	0	6	0
	No parttype	3	0	0

14. Click **Next**.
15. From **Event database**, select a database.

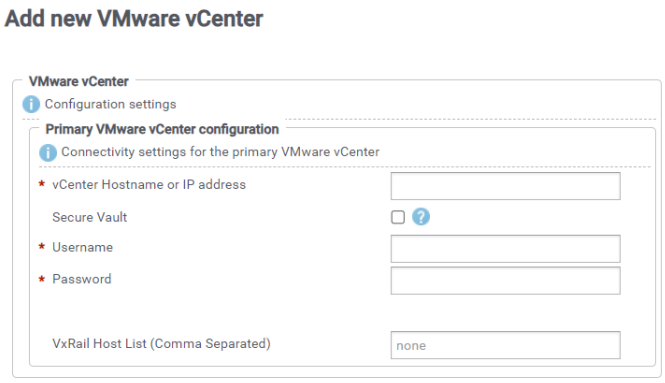
    If you select **Add a new Event Database**, add the Primary Backend host in the **Database hostname or IP address** field.
16. Click **Next**.
    The window displays reports settings.
17. Click **Next**.
18. To collect performance metrics for all the logical Bus that is managed by PowerPath agent, select **Collect performance metrics for PowerPath Bus**.
19. To collect performance metrics for all the logical devices that are managed by PowerPath agent, select **Collect performance metrics for PowerPath LUNs**.
20. To collect range-bound performance metrics, select **Collect PowerPath range-bound performance metrics**. Selecting this option increases the metric count significantly. Be sure to correctly size your application before enabling this option.
21. To set the absolute path location of the sudo and pbrun binaries, select **Do you want to configure advanced settings**.
22. Click **Install**.
23. Click **Ok**. Monitor the installation logs to ensure that the installation completes successfully.
24. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
25. Click **VMware vCenter (vmware-vcenter-collect <version>)** for data collection and/or **VMware vCenter (vmware-vcenter-events <version>)** for vCenter events collection.

    These steps describe how to add VMware vCenter hosts individually. For information about using discovery groups to use the same credentials to discover multiple VMware vCenter hosts, see Adding devices to discovery groups.

26. Click **Add...**
27. Select the **Secure Vault** checkbox to fetch the device credentials from the CyberArk server to discover the device.
    On selecting Secure Vault checkbox, the Unique Key field appears.

    NOTE: The Unique Key field is enabled only when the Secure vault checkbox is selected. When the Secure Vault checkbox is not selected, the Password is active.

28. From **Server**, select the server where the device is dispatched.
29. From **Instance**, select the instance of the vmware-vcenter-collect where the device is dispatched.
30. In **vCenter Hostname or IP address**, type the vCenter service host. Type the **Username** and **Password** used to poll vCenter.
31. In **VxRail Host List (Comma Separated)** enter the list of VxRail Manager Hosts separated by commas to poll VxRail Clusters for the respective vCenter.
    This is an optional field added to support VxRail discovery. The default value is none.



32. If secure vault is enabled, in **Unique Key** enter the unique key.
33. Click **Ok**.
34. Click **Save**.

Post-install requirements

Perform these operations after the installation is complete.

About this task

To enable PowerPath LUN or Path performance data collection on Linux, browse to the `/opt/APG/Collecting/Stream-Collector/<Instance Name>/conf/scripts/` directory.

Steps

1. In the `LunMappingDetection.pl` script, set `want_powerpath_lun_performance=1`.
   By default, this flag is set to zero.
2. To enable the PowerPath LUN or Path performance data collection on Windows:
   a. Browse to the `C:\Program Files\APG\Collecting\Stream-Collector\<Instance Name>\conf\scripts\windows` directory.
   b. In the `LunMappingDetection.ps1` script, set `powerPathPerformanceCollection=enabled`.
      By default, this flag is set to disabled.
3. To enable events reporting, open the Web-Application configuration file (`APG.xml`) and uncomment the `vmware-vcenter` section and the `ResourceLink` tag.
4. Restart the Tomcat service.

Enable vSAN reports

To enable vSAN Reports:

Steps

1. Add the vSAN license through the license management UI.
2. Synchronize the license to all the servers.
3. Restart the collector manager service.
   The collector manager logs will state the detection of vSAN license and collect the vSAN data.

iSCSI Support

Table 24. Array platform supported for iSCSI

SolutionPack	Array platform supported for iSCSI	
	Dell VMAX/PowerMax	Dell EMC XtremIO
SolutionPack for VMware vSphere vSAN & VxRail	Yes	Yes

NOTE:
- Dell EMC VMAX 3 arrays onwards are supported.

SNMP Trap Configuration in VMware vSphere vSAN & VxRail Solution Pack

SNMP Trap Configuration in VMware vSphere vSAN & VxRail SolutionPack includes the following procedures:

1. Configuring SNMP Trap Receivers
2. Enabling SNMP Alarms or Traps for the Alerts

Configuring SNMP Trap Receivers

Prerequisites

You must configure **SNMP Trap Receivers** at vCenter.

- Verify that the vSphere Client is connected to a vCenter Server instance.
- Ensure that you have the domain name or IP address of the SNMP receiver, the port number of the receiver, and the community string required for configuration.

Steps

1. In the Client, go to a vCenter Server instance.
2. Click the **Configure** tab.
3. Under Settings, click **General**.
4. On the vCenter Server Settings central pane, click **Edit**. The **Edit vCenter Server Settings** wizard opens.
5. Click **SNMP receivers** to edit their settings.
6. Enter the following information for the primary receiver of the SNMP traps.

Table 25. SNMP trap configuration details

Option	Description
Primary Receiver URL	Enter the SRM Primary Backend Server (PBE) hostname.

Table 25. SNMP trap configuration details (continued)

Option	Description
Enable receiver	Select the check box to enable the SNMP receiver.
Receiver port	Enter the port number as 2041.
Community string	Enter the community string that is used for authentication. You can leave it empty or select **Public**.
Receiver 2 URL	Leave this field blank.
Receiver 3 URL	Leave this field blank.
Receiver 4 URL	Leave this field blank.

7. Click **Save**.

Results

The vCenter Server system is now ready to send traps to the management system you have specified.

Enabling SNMP Alarms/Traps for the Alerts:

Prerequisites

- Existing pre-configured Alarms exists at the Datacenter level.
- Ensure that you have edit access to add new alarms or modify alarms as required.

Steps

1. In the vSphere Client, go to a vCenter Server instance.
2. Click the **Configure** tab.
3. Click **Alarm Definitions**.
4. Add a new Alarm definition:
   a. On the Alarm Definitions central pane, click **Add**.
   b. In the **Alarm Name and Target** wizard enter the Alarm name, Description, and Alarm type.
   c. Click **Next**.
   d. In the Alarm Rule window, provide the Trigger condition, appropriate Alarm severity, and enable **Send SNMP traps** option.
   e. Enable the **Repeat** check box if you want the trap to be sent for repetitive occurrence.
   f. Click **Next**.
   g. In the **Reset Rule** Window, you can enable the option to reset the alarm to green based on your defined condition in the given wizard.
   h. Click **Next**.
   i. In the **Review** Window, review your Alarm definition and click **Create**.

   NOTE: To edit an existing Alarm definition, go to the alarm definition you want to edit, click **EDIT**, make the required changes, and click **Save**.

Limitations

- The Host Attributes report is missing the IP Address for VMware vSphere vSAN & VxRail.
- Incomplete information for HBA driver, firmware, and HBA model in the discovered value column in the Match ESM screen.
- If a VM is discovered using both the SolutionPack for VMware vSphere vSAN & VxRail and the SolutionPack for Physical Hosts, the VM appears only in the SolutionPack for VMware vSphere vSAN & VxRail reports and is tagged according to its real device type which is VM. Dell Technologies does not recommend discovering VMs using the SolutionPack for Physical Hosts.
- Discovering ESXi hosts using the SolutionPack for Physical Hosts does not provide any incremental value and is not a supported configuration. All available data is collected using the SolutionPack for VMware vSphere vSAN & VxRail.

- NAS shares on ESXi guests/virtual server are not supported with VMware vSphere vSAN & VxRail SolutionPack.

Recommendations

- Do not discover VMware vCenter devices under both Dell VxRail and VMware vSphere vSAN & VxRail discovery. Simultaneous discovery results in duplicate data collection.
- vSAN must be enabled for complete VxRail Data collection.
- If both SolutionPacks are used together, ensure that VxRail Manager IPs are discovered in VxRail SolutionPack, and the same VxRail IPs and the vCenter are not present/active in VMware SolutionPack simultaneously.
- The Dell SRM recommends that existing VxRail customers use the recently enhanced VMware vSphere vSAN & VxRail SolutionPack, which has improved reporting capabilities.
- For more information about how to rediscover VxRail Clusters from VxRail SolutionPack to VMware vSphere vSAN & VxRail SolutionPack in SRM 4.10.0.0, see KB article.

48

Discovery Center

This chapter includes the following topics:

Topics:

Discovery Center

Discovery Center provides a central location to view and manage all devices which are monitored by the SolutionPacks. In Discovery Center, you can add new devices to be monitored, change device connection credentials and parameters, and test connectivity to devices.

Starting Dell SRM 4.5, Discovery Center is case insensitive. This feature is added to avoid discovery of the same device which can lead to discrepancies in reporting and also helps in avoiding redundant collection cycles. The Discovery Center search feature is case insensitive and displays the discovered devices irrespective of the case of Search text box. While trying to add devices, Discovery Center checks if the device is already present in any other case. If it is, the device is not added.

- Add feature would generate a message mentioning that Device is already present.
- Import CSV feature only allows device attributes to be changed, but a new device in a different case is not added.

There are several ways to add new devices:

- Add a single device manually
- Add devices in bulk by importing a CSV file
- Add devices using discovery

Discovery Center contains two sections:

- The **Manage Discovery** section is where you perform all add device and manage device activities.
- The **Discovery Wizard** section contains collector information that is required by the automatic discovery operations.

Manage Discovery

The **Manage Discovery** is organized by device type. You perform all device management activities on this page.

The list of device types on the **Manage Discovery** page is based on the SolutionPacks that are installed.

Click a device type row to manage devices of that type. Management activities include:

- Review the list of devices that are actively being monitored.
- View and change connection credentials and other device-specific parameters.
- Test connectivity to each device.
- Add or delete devices.

Viewing all known devices and testing connectivity

You can view a list of the devices that are known to the system. You can verify the connection parameters and availability for a device.

Steps

1. Go to **Administration** > **Discovery** > **Discovery Center** > **Manage Discovery**.
   The table lists all the SolutionPacks of which devices are being monitored and the number of devices in each type.
2. Click the SolutionPack for which you want to test the device.
   The **Collected Devices** tab lists all the devices currently being monitored.
3. Select a device to test connectivity to it.
4. Click **Test Connectivity** to verify that the device can be reached.

Changing device configuration

You can change the connection parameters and other configurations for a device.

Steps

1. Browse to **Administration** > **Discovery** > **Discovery Center** > **Manage Discovery**.
2. Click the device type of the device you want to test.
3. On the **Collected Devices** tab, click the row of the device to test.
   The configuration dialog box for that device appears.
4. Change the parameters as needed.
   See the product SolutionPack documentation for information.
5. Click **Test and Rediscover** to verify connectivity.
6. Click **OK** to save the changes and exit the dialog box.
   The device row now appears blue and in italics, indicating that the changes must be distributed to the collector servers.
7. Click **Save**, and then **OK** to confirm the save.

Adding a new device manually

Using **Discovery Center** you can manually add a new device to be monitored.

Prerequisites

To add a new device, you must already have a SolutionPack installed that supports that device type.

Steps

1. Browse to **Administration** > **Discovery** > **Manage Discovery**.
2. Select the SolutionPack.
3. On the **Collected Devices** tab, click **Add**.
4. In the device configuration dialog box, type the parameters for the new device.
   The configuration dialog box is device-specific. See the product SolutionPack documentation for information about each field.
5. Click **Validate and add**.
   The validation tests connectivity to the device using the provided information. If an error indicator appears, correct the information and click **Test** to try again.
6. Click **OK** to confirm addition of device.
   The new device appears in the Collected Devices table in blue and italicized, indicating that it is not yet saved in the system.
7. Click **Save**.
8. Click **Ok** to confirm the save.
9. Click **Ok**.

The **Status** column represents the discovery results. You can click the status icon to view the discovery results.

If the connectivity status is a green check, the new device is now being monitored.

Adding devices using CSV files

You can import a properly formatted CSV file to add devices.

Each device type provides a template that describes the required format of the CSV file for the device type. You can also export existing devices into a CSV file.

Importing a CSV file

You can import a CSV file containing information about new devices to be monitored.

Prerequisites

- To import new devices, you must already have a SolutionPack installed that supports the device type to be imported.
- Due to the addition of fields **Secure Vault** and **Unique Key** in the **Manage Discovery** page, the older CSV files that are used for devices will not work. To import devices in Discovery Center, use the new CSV template from the Discovery Center and move the data from old CSV files to the new template.
- The fields **Secure Vault** and **Unique Key** should not be left empty in the CSV files during import. Use the default value * for Unique Key and **false** for Secure Vault, in case the values are not available.

About this task

To get a template of the CSV file for a specific device type, use the **Export Template** button.

Steps

1. Browse to **Administration** > **Discovery** > **Manage Discovery** > ***SolutionPack***.
2. On the **Collected Devices** tab, click **Import**.
   The **Import new devices** popup appears.
3. For **Merge the devices to the existing ones?**

Option	Description
Do not check the option	Overwrite the current list of devices with the devices from the CSV file.
Check the option	Keeps the current list of devices and add (merge) devices that are contained in the CSV file to the current list.

4. Click **Choose File**.
5. Browse to the CSV file.
6. Click **Ok**.
7. Click **Continue**.
   The new devices appear in the Collected Devices table in blue and italicized.
8. Click **Save**.
   The **Save Devices** popup is displayed.
9. To overwrite or merge the devices, click **Ok**.
10. Click **Ok**.

Exporting devices

You can export the list of devices currently being monitored.

Steps

1. Browse to **Administration** > **Discovery** > **Manage Discovery** > ***SolutionPack***.
2. On the **Collected Devices** tab, click **Export**.

Follow the browser's prompts to save the file.

Exporting a CSV file template

A template shows the expected format of the CSV file for the bulk import of devices. The template includes headers.

Prerequisites

To export a CSV template file, there must already be one device of that device type available.

Steps

1. Browse to **Administration** > **Discovery** > **Manage Discovery** > ***SolutionPack***.
2. Click **Export**.
   Follow the browser's prompts to save the file.

Add devices using discovery

The discovery feature uses saved information in discovery groups to find new devices. A discovery group is specific to a device type.

The following procedures are required to implement discovery for a device type:

1. Register a collector server that supports discovery for the device type.

   NOTE: The discovery method is supported by many, but not all, device types.

2. Create one or multiple discovery groups for the device type.
3. Trigger discovery for a discovery group.
4. Distribute the discovery results to the collector.

Registering a new collector server

To use the automatic discovery features, you must first register the collector server that supports the device type you want to discover.

Steps

1. Go to **Administration** > **CONFIG** > **Settings** > **Manage Discovery Backends**.
   The table lists the system's Backend servers.
2. Click the row for a Backend server.
   The collector servers that are registered to perform discovery are listed. The table also shows the discoverable device types that are supported by each collector server.

   NOTE: If the table is empty, no collectors are registered.

3. To see a list of unregistered collector servers, click **Register**.
4. Select one or more servers from the list, and click **Register**.

   If you are collecting VMware vSphere vSAN & VxRail events, select the primary backend that you want to use for discovering the events.

   When registration finishes, all the currently registered collectors are shown, with their supported discoverable device types.

Create a discovery group

A discovery group stores the connection information, credentials, and other configuration information that is required to discover a group of devices. For example, you might set up discovery groups to store IP address ranges or subnets and appropriate connection credentials.

Prerequisites

Before you can create discovery groups and use the discover feature, the collection server that is associated with the device type must be registered.

- If the **Discovery Groups** and **Discovery Results** tabs are grayed out, the collection server is not registered.
- If the **Discovery Groups** and **Discovery Results** tabs are not shown, discovery is not supported for the device type.

Steps

1. Go to **Administration** > **Config** > **Groups & Tags** > **Manage Groups** > ***device_type***.
2. Click **Create**.
3. Type a name for the discovery group and click **OK**.
4. Add entries into the tables to provide the discovery information for the group.

   NOTE: The discovery group fields are different for each device type. For information about the fields, see the SolutionPack installation documentation.

   Use the following buttons to add information into the tables:

Button	Description
Add new entry...	Add discovery information manually.
Import...	Import a file containing discovery information.
Export	Export discovery information to take a backup or reuse it for other discovery groups.
Export template	Export a template to your Downloads folder. You can complete the template with discovery information, and then import the file with the **Import** button.

5. Click **Save**.
   You can now choose the group in a discover operation.

Discover devices

Discovery finds devices based on the seed information in a discovery group.

Prerequisites

Use the **Discovery Group** tab to create a discovery group or research the settings in discovery groups.

Steps

1. Go to **Administration** > **Config** > **Groups & Tags** > **Manage Groups** > ***device_type***.
2. On the **Collected Devices** tab, click **Discovery.**

   If the **Discover** button is not available, ensure that the appropriate collector is registered and that at least one discovery group is defined.
3. Select a **Discovery Group** name.
4. Select a **Discovery Mode**.
   - Use **Full Discovery** the first time you discover a group.
   - Use **Incremental Discovery** to discover a newly added device.
5. For **Automatically distribute results?**:
   - Select this option to distribute the results of discovery to the collector.
   - Do not select this option if you want to review and approve the discovery results before incorporating them into the system.

6. Click **OK**.
   If you requested automatic distribution, the results of the discovery are visible on the **Collected Devices** tab, and also on the **Discovery Results** tab.
7. If you did not request automatic distribution, go to the **Discovery Results** tab to review the results and distribute them.

Distribute (import) discovery results

If you did not request the discovery process to distribute results, you can examine and distribute the results on the **Discovery Results** tab.

About this task

Steps

1. Go to **Administration** > **Config** > **Groups & Tags** > **Manage Groups** > ***device_type***.
2. Click the **Discovery Results** tab.
   The table shows an overview of discovery requests, by discovery group.
3. To see details about the discovered devices, click a discovery group name.
4. To import the discovered devices into the system (so that monitoring activities can start on them), click **Import to Collected Devices**.
5. Complete the pop-up dialog box as follows:

Option	Description
To delete all existing devices of this device type, and add the results of this discover group discovery	Click **OK**.
To retain existing devices, add the newly discovered devices, and update any existing devices if configuration changes were discovered	Click the **Merge** checkbox and then click **OK**.

6. To view the new set of devices being monitored, click the **Collected Devices** tab.
   Review the devices and credentials to avoid lockout of devices due to multiple attempts of incorrect credentials. Dell Technologies recommends creating groups in such a way that devices have a minimal set of credentials to be tried against. Dell Technologies recommend using common public-private key pairs for multiple devices.

Physical host discovery

Dell SRM supports several mechanisms for physical host discovery.

The following table summarizes the operating systems and SolutionPacks that apply to each type of discovery:

Table 26. Physical host discovery methods

Discovery Mechanism	OS	SolutionPack
Agentless	Windows/UNIX	SolutionPack for Physical Hosts
Agent based	Windows	SolutionPack for EMC Host Interface SolutionPack for Physical Hosts (Reports)
Agent based	UNIX	SolutionPack for Physical Hosts (Reports)
Passive (via zoning information from Brocade and Cisco switches or Device Manager for HDS)	All	SolutionPack for Brocade/Cisco/HDS
Passive (via host containers)	All	Not applicable (only requires the Generic-RSC collector)

Passive host discovery

Passive host discovery is a capability where hosts are intelligently guessed from SAN zoning records. SAN zoning discovery yields hostnames, IP addresses, and HBA port WWN values from zoning records. Dell Technologies recommends discovering hosts primarily with passive discovery in order to recognize SAN attached hosts. Once the hosts are resolved, storage administrators can obtain additional credentials from server administrators to completely discover hosts.

NOTE: Passive discovery through Brocade and Cisco SolutionPacks is disabled by default.

Enabling passive host discovery

About this task

You can enable passive host discovery while installing the SolutionPack, or by reconfiguring the SolutionPack.

For the SolutionPack for Brocade FC Switch, reconfigure the SMI Data Collection block.

For the SolutionPack for Cisco MDS/Nexus, edit the Generic-SNMP independent SolutionPackBlock instance.

Discovering hosts via host containers

Use the host containers mode of discovery if you are interested in end-to-end topology and chargeback, but you do not want to actively poll the host.

Prerequisites

To view the end-to-end topology, the fabric and the array from which the host has been allocated storage must be fully discovered via Dell SRM. To view chargeback reports, the array from which the host has been allocated storage must be discovered in Dell SRM.

Steps

1. In **SRM Admin UI**, go to **DISCOVERY** > **Discovery Center** > **Manage Discovery**.
2. Click **Host configuration**
3. Click **Add New Device**.
4. Enter the IP address (optional).
5. Enter the hostname.
6. Select **Host Containers** from the **Specify the discovery mode** drop-down menu.

   Enter one or more HBA port WWNs in the **Host Port WWN** field. Multiple WWNs must be separated by a semicolon (;). This field is not case sensitive.

49

Device Config Wizard

Device Config Wizard can be accessed by entering the SRM FrontEnd IP or Hostname, in a fresh setup, which has no discoveries done. From SRM 4.0 onwards, Device Config Wizard can also be accessed from `Discovery->Discovery Center->Discovery Wizard` in the administration page.

This is intended to help new users discover all their elements in one go, that is, the Storage Devices, Fabric, and Compute elements. It verifies the P&S recommendation for each device whenever it gets added or discovered and allow discovery only when a new device being discovered does not exceed the recommended P&S guideline.

Storage Collection

- Helps discover all major Arrays.
- Supported Arrays - Dell SC, Dell PowerScale, Dell Unity, Dell EMC VMAX3/Dell VMAX All Flash, Dell VPLEX, Dell EMC XtremIO.

Fabric Collection

- Helps discover Switches and Fabrics.
- Supported Vendors - Cisco (SNMP), Brocade (SNMP + SMI-S)

Compute Collection

- Helps discover VMware vCenter.
- Supports the collection of Topology, Capacity, and Performance data for vCenter.

Collection Status

- Presents the user with the collection status in the form of a progress bar, and provides an option to notify by email, once all data gets populated in the reports.

50

Troubleshooting

This chapter includes the following topics:

Topics:

Confirming report creation

After you install a SolutionPack, you can view its reports.

About this task

To view the reports:

Steps

1. Go to **User Interface** > **Report Library**.
2. To view its reports, click the SolutionPack.

Results

It may take up to an hour to display all relevant information in these reports.

What to do if data does not appear in any reports

Troubleshooting steps if data does not appear in any reports.

Steps

1. After the completion of at least three collection cycles, verify if data is populating into the reports. If there is still no data in the reports, continue to the next step.
2. To import data into reports, run the scheduled task. If there is still no data in the reports, continue to the next step.
3. To view the log files for errors, browse to **System Admin** > **Logs & Diagnostics** > **Log Files** > **Collector-Manager::<*instance name*>**.

Running a scheduled task to import data into reports

After you push a new configuration into a collector, a scheduled task runs and populates the reports with new data. You can manually run the scheduled task to import the data more quickly.

Prerequisites

Allow at least three polling cycles to pass before manually running the scheduled task.

Steps

1. Click **System Admin**.
2. Click **Settings**.
3. Expand **Scheduled Tasks**.
4. Select **Database**.
5. Click **Run Now**.
6. Confirm success in running the task in the **Last Result** and **Last Result Time** columns.

What to do if data does not appear in some reports

Troubleshooting steps if data does not appear in some reports.

Steps

1. Run the scheduled task to import data into reports. If there is still no data in the reports, continue to step 2.
2. Search for the metric in the database.
3. To view the log files for errors, **System Admin** > **Logs & Diagnostics** > **Log Files** > **Event-Processing_Manager::Instance name**.

   To troubleshoot the errors, enable the Event-Spy for the Event Processing Manager.

Searching for metrics in the database

You can verify that a metric is being collected and used for reporting when you search and find the metric in the database.

Steps

1. Click **Administration** .
2. Under **System Admin** > **System Operations**, click **Manage Database Metrics**.
3. On the **Metric Selection** page, create the filter, type the number of results, and select the properties to display for the metric.
   For example, to list up to 100 results of the Capacity metric with the properties of device and IP, type **`name=='Capacity'`** in the **Filter** field, **`100`** in the **Maximum results** field, and select device and IP for the **Properties to show**.
4. Click **Query.**

   A list of the metric results appears. If nothing displays, the metric is not being collected.

External storage capacity is double counted in capacity reports

Enterprise capacities for a storage array include any external array capacity or Federated Tier Storage (FTS) Capacity.

To avoid double counting of external storage capacity in the enterprise capacity reports, do not discover the external storage array.

Authorization fails for passwords having special characters

Passwords for Dell SRM users with the following characters are not supported: "?(~ ' | { }$%^&*()_+)

Troubleshooting discovery issues, slow reports, and missing data

Learn how to troubleshoot discovery issues, slow reports, and missing data in reports or topology maps.

Steps

1. Locate entries for the SolutionPack, find the element with the issue, and validate its discovery status using the Test button utility.
2. Locate the SolutionPack collector appliance, select it, select the Collector-Manager instance, and ensure that there are no errors in Collector-Manager log files.
3. Locate the SolutionPack collector appliance, select it, select Topology-Mapping-Service instance, and under Log Files, ensure that there are no errors in the `topology-mapping-sevice.log` file. Any issues here could be related to a topology map issue.
4. Locate the SolutionPack collector appliance, select it, select the Load-Balancer instance, and ensure that there are no errors in the load-balancer logs. Any issues in pushing data to the backend can cause missing data in reports.
5. Select the Primary Backend host, select the Load-Balancer instance, and ensure that there are no errors in the load-balancer logs. Any issues in pushing data to the backend can cause missing data in reports.
6. Select the Primary Backend host, select the Topology-Service instance, and ensure that there are no errors in the `topology-service.log` file. Any issues in pushing data to the backend can cause topology map issues.
7. Under **Scheduled Tasks**, ensure that all tasks are completing in reasonable time and that there are not any status problems. Any issues here can cause slow reports or missing data.

   If you are experiencing issues with discoveries, slow reports, or missing data in reports, Dell SRM includes System Health SolutionPack that can be very helpful. Ensure that each of the Dell SRM appliance hosts have the System Health SolutionPack installed and data has been collected for 2 to 3 collection cycles. The System Health reports are available at **All** > **Report Library** > **System Health**. The reports at **All** > **Report Library** > **System Health** > **Misc. Reports** > **JVMs Sizing Recommendation** are useful to assign the correct amount of memory for SolutionPacks. Additionally, refer to Managing Dell SRM System Health for details about interpreting system health reports.

Viewing collector errors in the Collector-Manager log files

Review the Collector-Manager log files to troubleshoot problems with data collection.

Steps

1. To view the log files for errors, **Admin** > **System Admin** > **Log Files**.
2. Expand **Collecting**.
3. Click the Collector-Manager for the collector instance.
   Collector-Manager:*<Collector-Manager instance> - <host_ID>*

Troubleshooting agentless host discovery for Windows

This section describes troubleshooting methods that you can use when configuring agentless host discovery for Windows.

Troubleshooting authentication failures

Use the following procedure to troubleshoot authentication failures.

Steps

1. From the Dell SRM user interface, browse to **Administration** > **Discovery Center** > **Host Configuration**.
2. If the host is already added for discovery, click the instance and verify that the credentials were entered correctly.
3. If the credentials are correct, click the **Test** button to troubleshoot any authentication or authorization problems.

Performing a configuration check

To perform a configuration check, ensure that the following conditions are met.

Steps

- Ensure that the host configuration utility runs successfully to troubleshoot any environment problems on the host.
- Ensure that the host OS is supported in Dell SRM.

Using Logs on a Windows host

Initially, review the `Generic-RSC collecting-0-0.log` in the logs folder

About this task

Further troubleshooting requires the support mode logs:

Steps

1. Enable support mode in the `LunMappingDetection.ps1` script on the host. Run the following command:

   ```
   $supportOption="enabled"
   ```

2. Run the command for support mode:

   ```
   powershell.exe -noprofile -file LunMappingDetection.ps1 > test.log
   ```

   NOTE: Run the support mode with the user that was used for discovery.

Checking SNIA library installation on a Windows host

To verify if SNIA library is correctly installed, ensure the following pointers:

Steps

- If the HBA is an Emulex model, check whether HBAAnyware or OneCommand Manager is installed.
- If the HBA is a Qlogic model, check whether SAN Surfer is installed.

Gathering HBA information

About this task

To gather HBA information:

Steps

1. Run `wbemtest` tool.
2. Connect to root/cimv2 and run the following query:

```
 select Name from Win32_SCSIController where ProtocolSupported=10 or
Manufacturer='EMC Corporation' or Manufacturer='Emulex' or Manufacturer='QLogic'
```

3. Double-click the rows that are returned by the query and click show MOF.
4. Note the HBA make and model information.

Verifying HBA installation

About this task

Verify that the HBAs are installed by using the following procedure:

Steps

1. Right-click **My Computer**.
2. Select **Manage** from the **Server Manager** window.
3. Expand the **Diagnostics** tab.
4. Click **Device Manager**.
5. Expand **Storage Controllers** within the **Device Manager** window and note the HBA make and model.

Installing OneCommand Manager

Prerequisites

If you are running the OneCommand/HBAAnyware Vision application, you must stop the services before installing the OneCommand Manager application.

About this task

To stop the services:

Steps

1. Select **Start** > **Programs** > **Administrative tools** > **Services**
2. Stop the EmulexSensor service.
3. Stop the EmulexWMIAgent service.
4. Stop the Emulex PDH agent service.
5. Stop the EmulexScope agent service.
6. Install the OneCommand Manager/HBAAnyware application.
7. To restart the sensor after the installation is complete:
   a. Stop SNMP service in case of SNMPv2c [Stop Net-SNMP Agent in case of SNMPv3].
   b. Start SNMP service in case of SNMPv2c [Start Net-SNMP Agent in case of SNMPv3].
   c. Start the EmulexSensor service.

Installing or modifying QLogic drivers on a Windows host

Refer to the procedure provided in the ReadMe provided with the downloaded package.

Troubleshooting UNIX Agentless Host Discovery

This section describes some troubleshooting methods you can use when configuring UNIX agentless host discovery.

Environment check for non-root configurations

Ensure that the host OS is supported in Dell SRM and the configurations pertaining to non-root users are correct. Non-root users can be configured using sudo, pbrun, or dzdo.

Using logs on a UNIX host

Prerequisites

Initially, you should review the `Generic-RSC collecting-0-0.log` in the logs folder.

About this task

For further debugging, you need the support mode logs.

To retrieve support mode logs, run the following command on the host:

```
./LunMappingDetection.pl support=test_log
```

SNIA Library check

To verify that the SNIA library is correctly installed, check the contents of `hba.conf`.

Check the contents of hba.conf

```
more /etc/hba.conf
qla2xxx /usr/lib/libqlsdm.so
qla2xxx64 /usr/lib64/libqlsdm.so
```

Verify libHBAAPI.so in 64 bit machines

In 64 bit machines, verify the presence of libHBAAPI.so:

```
ls /usr/lib64/libHBAAPI.so
```

Verify libHBAAPI.so in 64 bit machines

```
linbgm103:/lib # more /etc/hba.conf
com.emulex.emulexapilibrary /usr/lib64/libemulexhbaapi.so
com.emulex.emulexapilibrary /usr/lib/libemulexhbaapi.so
```

Another way to verify that Emulex HBA related software is installed is to check whether `/usr/sbin/hbanyware` or `/usr/sbin ocmanager` is present or not.

Gathering information about AIX HBAs

About this task

To gather information about AIX HBAs, use the following procedure:

Steps

1. Verify that HBA instances are installed:

```
/usr/sbin/lsdev -Cc adapter
```

2. Verify the HBA model:

```
lscfg -vl fcs
```

Gathering information about HP-UX HBAs

Steps

1. Look for the HBA instances that are installed in the host. The following command looks for both types of HP drivers (fcd and td):

```
ls /dev | egrep "fcd|td"
```

or

```
/usr/sbin/ioscan -knfC fc
```

2. Gather product data about each HBA instance such as the part number and model. The HBA type and number should be replaced with #:

```
/opt/fcms/bin/fcmsutil /dev/<fcd#/td#> vpd
```

3. Gather useful data about each HBA instance such as WWN:

```
/opt/fcms/bin/fcmsutil /dev/<fcd#/td#>
```

Gathering information about Solaris HBAs

About this task

Show the HBA model and firmware level for all of the instances with the following command:

```
fcinfo hba-port
```

Gathering information about Linux HBAs

About this task

To gather information about Linux HBAs, use the following procedure:

Steps

1. Verify that the HBA instances are installed:

```
lspci | grep "Fibre Channel"
```

2. Verify the HBA model:

```
dmesg | grep scsi
```

Installing or modifying Emulex HBA drivers on Linux

Prerequisites

The following must be installed before you can install the utilities:

- The driver for the operating system:
  - Linux driver version 8.2.0.33.3p or later (For RHEL5 and SLES10 operating systems.)
  - Linux driver version 8.2.8.x or later (For SLES11 operating systems.)
  - Linux driver version 8.3.5.X or later (For RHEL 6 SLES 11 SP1 operation systems.)
- Previous versions of the Linux driver must be uninstalled. Run the uninstall script that shipped with the version of the Linux driver you want to remove.

About this task

To install the OneCommand Manager application in Linux, use the following procedure:

Steps

1. Log in to the host as root.
2. Download the utilities from the Emulex website or copy them to the system from the installation CD.
3. Copy the installation and uninstallation scripts to a known location, for easy access by other users.
4. Copy the OneCommand `elxocm-<Platform>-<AppsRev>.tgz` file to a directory on the install host.
5. Change (use `cd` command) to the directory to which you copied the tar file.
6. Untar the file.
   - For RHEL 5 and RHEL 6 type the following:

     ```
     tar zxvf elxocm-rhel5-rhel6-<apps_ver>-<rel>.tgz
     ```

   - For SLES 10 and SLES 11 type the following:

     ```
     tar zxvf elxocm-sles10-sles11-<apps_ver>-<rel>.tgz
     ```

7. Change (use `cd` command) to the elxocm directory created in step 6.

   For RHEL 5 and RHEL 6 type:

   ```
   cd elxocm-rhel5-rhel6-<apps_ver>-<rel>
   ```

8. Run the install script.

Installing or modifying Emulex HBA drivers on UNIX

Prerequisites

The following must be installed before you can install the utilities:

- The Solaris FC/FCoE driver version 2.50 or later.
- The NIC driver version 1.10 or later for NIC capability.

About this task

To install the OneCommand Manager application in Solaris:

Steps

1. Copy the Solaris utility kit to a temporary directory on the system.
2. Untar the utility kit:

```
tar xvf elxocm-solaris-<version>.tar
```

3. Change to the newly created `elxocm-solaris-<version>` directory:

```
cd ./elxocm-solaris-<version>/
```

4. Run the install script to begin installation. If the HBAnyware utility, OneCommand Manager Core or OneCommand Manager Enterprise applications or the Solaris driver utilities are already present on the system, the install script tries to remove them first:

```
./install
```

5. When prompted, enter the type of management you want to use:
   - 1 Local Mode : HBAs on this Platform is managed by OneCommand clients on this Platform Only.
   - 2 Managed Mode: HBAs on this Platform is managed by local or remote OneCommand clients.
   - 3 Remote Mode : Same as '2' plus OneCommand clients on this Platform can manage local and remote HBA'

Installing or modifying QLogic HBA drivers on UNIX/LINUX

About this task

The SNIA API library package (example: `qlapi-<api_version>-rel.tgz`) is in the driver combo package (example: `qla2x00- vx.yy.zz-dist.tgz`) or (`qla2x00-vx.yy.zz-fo-dist.tgz`).

Using the files that you downloaded from Qlogic website, copy the tgz file (example: `qla2xxx-vx.yy.zz-dist.tgz`) distribution file to `/qla2x00`.

The following example shows how the package is installed. Type the following commands, as outlined in the following steps, from the `/ (root)` directory:

Steps

1. `mkdir qla2x00`
2. `cd qla2x00*`
3. `mount /mnt/floppy`
4. `cp /mnt/floppy/*.tgz.`

   NOTE: The period at the end is required.

5. `tar -xvzf *.tgz`
6. `cd qlogic`
7. To install and set up the API library, type the following command:

   `in ./libinstall`

   This installs/sets up HBA API library.

Troubleshooting passive host discovery

This section contains information on troubleshooting passive host discovery.

Verifying passive hosts from the collection logs

Steps

1. Enable the file connector in the corresponding Brocade or Cisco SolutionPack.
2. Review the collection information in the `file-connector.log`, and look for PassiveHost as the devtype in the collection details.

   For example:

```
 1421139292: group::Brocade-
Collectorz_losan239_110000000C93995CF1000000533E94F01-0000AFFF00000008({isremote=true,
 partsn=0000AFFF00000008, part=10000000C93995CF, ip=10.247.22.239,
zmemid=10000000C93995CF, source=Brocade-Collector, w4ncert=1.0, hasDevice=Yes,
parttype=Disk, zname=z_losan239_1, devtype=PassiveHost, hostname=losan239,
vendrcode=0000C9, name=ZoneMemIdentifier, actdisc=0, hostwwn=10000000C93995CF,
device=losan239, datagrp=BROCADE_ZONEMEMBER})=0.0
```

Verifying passive hosts from the RDF/topology store

About this task

If you have Sesame windows client, execute the following query:

```
PREFIX SRM: <http://ontologies.emc.com/2013/08/SRM#>
SELECT ?s ?p ?o
WHERE {
?s a SRM:PassiveHost .
?s ?p ?o
} LIMIT 1000
```

Verifying that LUNs from an array are being mapped to host

About this task

The partsn value (with LUNWWNS) is retrieved using a sparql query on the Topology RDF store. When searching for this value in Dell SRM, note that both the passively-discovered host and the connected array both need to have been discovered. For example:

```
1421139292: group::Brocade-
Collectorz_losan239_110000000C93995CF1000000533E94F01-0000AFFF00000008({isremote=true,
partsn=0000AFFF00000008, part=10000000C93995CF, ip=10.247.22.239,
zmemid=10000000C93995CF, source=Brocade-Collector, w4ncert=1.0, hasDevice=Yes,
parttype=Disk, zname=z_losan239_1, devtype=PassiveHost, hostname=losan239,
vendrcode=0000C9, name=ZoneMemIdentifier, actdisc=0, hostwwn=10000000C93995CF,
device=losan239, datagrp=BROCADE_ZONEMEMBER})=0.0
```

51

Documentation Feedback

Dell Technologies strives to provide accurate and comprehensive documentation and welcomes your suggestions and comments. You can provide feedback in the following ways:

- Online feedback form — **Rate this content** feedback form is present in each topic of the product documentation web pages. Rate the documentation or provide your suggestions using this feedback form.
- Email—Send your feedback to SRM Doc Feedback. Include the document title, release number, chapter title, and section title of the text corresponding to the feedback.

To get answers to your queries related to Dell SRM through email, chat, or call, go to Dell Technologies Technical Support page.