APTARE IT Analytics Certified Configurations Guide

Release 10.4.00

VERITAS™

APTARE IT Analytics Certified Configurations Guide

Last updated: 2020-06-30

Legal Notice

Veritas Technologies LLC
2625 Augustine Drive.
Santa Clara, CA 95054

http://www.veritas.com

.

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Portal and Database Servers

This chapter includes the following topics:

Portal Supported Operating Systems

The following 64-bit platforms are supported:

Table 1-1

Operating System	Version
CentOS	7
Red Hat Enterprise Linux	7
SUSE Linux Enterprise	SUSE 12
Windows	Win 2016 Server

Recommended Portal Configurations

The following Portal configurations are recommended. Enterprise-specific requirements may warrant additional resources, as you fully deploy features and add APTARE IT Analytics licensed products to the Portal.

Table 1-2

Medium Portal (Virtual Machine)	Medium Portal Criteria
■ Windows 64-bit or Linux 64-bit ■ 4 vCPU cores with a minimum 32 GiB of memory recommended ■ maximum 2 physical CPU sockets (Oracle license limitation) ■ minimum of 200 GiB of usable disk space (SAN or DAS, not NAS)	■ Capacity < 10 PB and ■ Backup < 10,000 clients
Large Portal (Physical Server)	Large Portal Criteria
■ Linux 64-bit ■ Minimum of 4 Cores (8 Logical CPUs), with 96 GiB of RAM ■ Maximum 2 physical CPU sockets (Oracle license limitation) ■ Minimum of 500 GiB of usable disk space (SAN or DAS, not NAS)	■ Capacity > 20 PB or ■ Backup > 20,000 clients

Note: For File Analytics data collection, contact your technical sales consultant for disk space recommendations.

Oracle Database and Memory Requirements

The embedded Oracle Database license is a restricted license and may only be used or accessed in conjunction with APTARE IT Analytics software.

As a best practice, Oracle memory size should be at least 25% of the Portal server's total memory size, recommended in the above table, with a minimum of 12 GiB.

APTARE IT Analytics software is certified with the Oracle binaries embedded with the software product. Note that the use of the embedded binaries must comply with Oracle Database Standard Edition 2 license requirements, which permits use only on servers (including any virtual server platform) that have a maximum capacity of 2 physical CPU sockets (populated or not). If using a Cloud Provider, Oracle Database Standard Edition 2 may be licensed only on Authorized Cloud Environment

instances up to 8 virtual cores. Using non-embedded versions of Oracle (for example, installing in other pre-existing Oracle instances) is not a certified configuration and is not allowed by the license grant.

If explicitly licensed for the APTARE IT Analytics with Partitioning, the embedded Oracle binaries are Oracle Database Enterprise Edition with Partitioning. Note that the use of the embedded binaries must comply with Oracle Database Enterprise Edition with Partitioning. Using non-embedded versions of Oracle (for example, installing in other pre-existing Oracle instances) is not a certified configuration and is not allowed by the license grant.

If explicitly licensed for APTARE IT Analytics for Shared Services, the APTARE IT Analytics embedded Oracle binaries are not provided or licensed with the APTARE IT Analytics software and cannot be used with the APTARE IT Analytics for Shared Services. End Users are solely responsible for purchasing and licensing the Oracle database binaries required for the operation of the APTARE IT Analytics for Shared Services software.

For APTARE IT Analytics Managed Services Editions, the APTARE embedded Oracle binaries are not provided or licensed with the APTARE IT Analytics software and cannot be used with the Managed Services Editions of APTARE IT Analytics. Managed Services Partners are solely responsible for purchasing and licensing the Oracle database binaries required for the operation of the APTARE IT Analytics Managed Services Editions software.

Supported Browsers and Display Resolution

Display Resolution: The minimum resolution for the Portal is 1280 x 768 px.

The Portal was certified on the following browsers. Please note that if you are using other versions of these browsers your user experience may vary:

Table 1-3 Supported Browsers

Browser	Apple Macintosh	Microsoft Windows	Linux
Microsoft Internet Explorer 11.1		x	
Mozilla Firefox 68.5.0esr (64-bit)	x	x	x
Google Chrome 79.0.3945.130(64-bit)	x	x	
Apple Safari 13.0.5	x		

Browser Performance

Several factors can impact web browser performance and behavior, such as:

- client memory size and free memory
- number of objects to be displayed in the Inventory
- volume of data to be displayed
- browser vendor (such as Chrome, Firefox, or IE) and version

The Portal is designed to handle data in large-scale environments, however, your browser vendor/version may not be able to render all the objects. If your browser cannot accommodate the volume, you can reduce the total number of items displayed in the Inventory, or try a different browser.

For larger data sets, use a Google Chrome browser for an optimal experience. Based on browser performance testing using very large data sets, Firefox and IE are supported, but the performance may be degraded.

Compatibility Mode

For supported browsers, some windows may not display properly if you are running in compatibility mode rather than the preferred standard mode. Steps to change from compatibility mode to standard mode can be found by searching the Help in your vendor-specific browser window.

Linux Portal Server: Exported and Emailed Reports

On a Linux Portal server, to ensure proper rendering of reports that are emailed or exported as HTML images or PDF files, a graphics manager such as X Virtual Frame Buffer (XVFB) is required. Contact your IT organization to configure this capability, if you plan to export/email reports as HTML images or as PDF files.

Supported Third-Party and Open Source Products

When you install the Portal and Reporting Database software, you install a compilation of software, which includes open source and third-party software.

Open Source Software

For a list of open source components and licenses, see the LICENSE, NOTICE, and license.txt files on the Portal server.

Portal: Supported Software

Table 1-4

Software Product	LINUX	Windows
Oracle 12c Standard Edition 2	**Upgrading to 10.4.xx** ■ 12.1.02 **New Installation 10.4.xx** ■ 12.2.01	**Upgrading to 10.4.xx** ■ 12.1.02 **New Installation 10.4.xx** ■ 12.2.01
Java	Amazon Corretto 11.0.6.10.1 64-bit	Amazon Corretto 11.0.6.10.1 64-bit
VSphere Web Services SDK	5.5, 64-bit	5.5, 64-bit
Apache HTTP Web Server	**Upgrading to 10.4.xx** ■ Manual upgrade to 2.4.41 is supported. **New Installation 10.4.xx** ■ 2.4.41. ■ Apache 2.4.41 includes SafeLogic SSL for Linux environments.	**Upgrading to 10.4.xx** ■ Manual upgrade to 2.4.41 is supported. **New Installation 10.4.xx** ■ 2.4.41. Verify that the C++ Redistributable for Visual Studio 2015 is installed.* ■ Apache 2.4.41 includes OpenSSL for Windows environments.
Apache Tomcat Java Servlet Engine	**Upgrading to 10.4.xx** ■ 8.5.50*. If you have an older version of Tomcat installed, contact Veritas Support for assistance. **New Installation 10.4.xx** ■ 8.5.50*	**Upgrading to 10.4.xx** ■ 8.5.50*. If you have an older version of Tomcat installed, contact Veritas Support for assistance. **New Installation 10.4.xx** ■ 8.5.50*

If other versions of the above components are already running on the designated APTARE IT Analytics system, or other components are utilizing resources (such as specific ports) typically used by APTARE IT Analytics, the product usually can be reconfigured to work around these conflicts; however, this cannot be guaranteed.

*Refer to Support for updated binaries as they become available.

Chapter 2

Data Collector Server Configurations

This chapter includes the following topics:

Data Collector Supported Operating Systems

Install the Data Collector on a virtual machine (VM). The following 64-bit platforms are supported:

Table 2-1

Operating System	Version
Windows Server (Recommended)	2016 2019 **Note:** 2019 is only supported for Data Collectors. It is not supported for the Portal.
CentOS	7 8 **Note:** CentOS 8 is only supported for Data Collectors. It is not supported for the Portal.

Table 2-1 *(continued)*

Operating System	Version
Red Hat Enterprise Linux	7 8 **Note:** RHEL 8 is only supported for Data Collectors. It is not supported for the Portal.
SUSE Linux Enterprise	12

Data Collector Server Memory and CPU Guidelines

Use the following guidelines for Data Collector Servers.

- Installation on a VM is recommended
- CPU: 2 - 4 CPUs
- Memory: 32 GiB minimum; If collecting from more than 40 backup servers, contact Support for recommendations.
- Installation Directory Disk Space: 200 GiB minimum; If collecting File Analytics data, an additional minimum of 300 GiB of disk space is recommended. Windows default installation directory is: C:\Program Files\Aptare. Linux default installation directory is /opt/aptare.

Customize the Linux File Handle Setting for Large Collections

In Linux, a portion of memory is designated for file handles, which is the mechanism used to determine the number of files that can be open at one time. The default value is 1024. For large data collection policy environments, this number may need to be increased to 8192. A large environment is characterized as any collector that is collecting from 20 or more subsystems, such as 20+ TSM instances or 20+ unique arrays.

To change the number of file handles, take the following steps.

1. On the Linux Data Collector server, edit:

   ```
   /etc/security/limits.conf
   ```

   At the end of the file, add the following lines:

   ```
   root soft nofile 8192
   root hard nofile 8192
   ```

2. Log out and log back in as **root** to execute the following commands to validate all values have been set to 8192.

```
ulimit -n
ulimit -Hn
ulimit -Sn
```

3. Restart the Data Collector.

Factors Impacting Data Collector Performance and Memory Requirements

Because every environment has a unique set of resources, configured and tuned specifically for that environment, there is no one size fits all formula. Several factors can impact performance and memory requirements:

- Number of active Data Collector Policies
- Number of hosts and active probes per host
- Number and types of storage arrays
- Number of LUNs
- Polling frequency and number of devices polled
- Amount of data transmitted
- Performance of array device managers

Data Collector Prerequisites

This list includes the general Data Collector server prerequisites. Specific requirements are listed with each supported subsystem.

- 64-bit OS.
- Support Amazon Corretto 11. Amazon Corretto is a no-cost, multi- platform, production-ready distribution of the Open Java Development Kit (OpenJDK).
- For performance reasons, do not install Data Collectors on the same server as the APTARE IT Analytics Portal. However, if you must have both on the same server, verify that the Portal and Data Collector software do not reside in the same directory.
- Install only one Data Collector on a server (or OS instance).

- Verify the rpm fontconfig is installed. Fontconfig is a library designed to provide system-wide font configuration, customization and application access. If the rpm fontconfig is not installed, the installer will not be able to load User Interface Mode. This is a prerequisite for new Data Collector installations.

Firewall Configuration: Default Ports

The following table describes the standard ports used by the Portal servers, the Data Collector servers, and any embedded third-party software products as part of a standard “out-of-the-box” installation.

Table 2-2 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Linux Hosts	SSH 22, Telnet 23
Managed Applications	Oracle ASM 1521 MS Exchange 389 MS SQL 1433 File Analytics CIFS 137, 139
Oracle Oracle TNS listener port	1521
Tomcat - Data Receiver Apache connector port and shutdown port for Data Receiver instance of tomcat	8011, 8017
Tomcat - Portal Apache connector port and shutdown port for Portal instance of tomcat	8009, 8015
Windows Hosts	TCP/IP 1248 WMI 135 DCOM TCP/UDP > 1023 SMB TCP 445

Table 2-3 Storage Vendors: Default Ports

Storage Vendor	Default Ports and Notes
Dell Compellent	1433 SMI-S http (5988) SMI-S https (5989)
Dell EMC Elastic Cloud Storage (ECS)	REST API 80/443
Dell EMC Unity	REST API version 4.3.0 on 443 or 8443
EMC Data Domain Storage	SSH 22
EMC Isilon	SSH 22
EMC Symmetrix	SymCLI over Fibre Channel 2707
EMC VNX (CLARiiON)	NaviCLI 443, 2163, 6389, 6390, 6391, 6392
EMC VNX (Celerra)	XML API 443, 2163, 6389, 6390, 6391, 6392
EMC VPLEX	https TCP 443
EMC XtremIO	REST API https 443
HP 3PAR	22 for CLI
HP EVA	2372
HPE Nimble Storage	5392, REST API Reference Version 5.0.1.0
Hitachi Block Storage	TCP 2001 For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.
Hitachi Content Platform (HCP)	SNMP 161 REST API https 9090
Hitachi NAS (HNAS)	SSC 206
Huawei OceanStor Enterprise Storage	8080
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778

Table 2-3 Storage Vendors: Default Ports *(continued)*

Storage Vendor	Default Ports and Notes
INFINIDAT InfiniBox	REST API TCP 80, 443
Microsoft Windows Server	2012 R2, 2016 WMI 135 DCOM TCP/UDP > 1023
NetApp E-Series	SMCLI 2436
NetApp ONTAP 7-Mode and Cluster-Mode	ONTAP API 80/443
Pure Storage FlashArray	REST API https 443
Veritas NetBackup Appliance	1556

Table 2-4 Data Protection: Default Ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443
Commvault Simpana	1433, 135 (skipped files) 445 (CIFS over TCP) DCOM >1023
Dell EMC Networker Backup & Recovery	Port used for Dell EMC NetWorker REST API connection. Default: 9090.
EMC Avamar	5555 SSH 22
EMC Data Domain Backup	SSH 22
EMC NetWorker	■ NSRADMIN TCP 7937-7940 ■ WMI Proxy range of ports ■ SSH 22 (Linux)
HP Data Protector	5555 WMI ports SSH 22 (Linux)
IBM Spectrum Protect (TSM)	1500

Table 2-4 Data Protection: Default Ports *(continued)*

Data Protection Vendor	Default Ports and Notes
NAKIVO Backup & Replication	Director Web UI port (Default: 4443)
Oracle Recovery Manager (RMAN)	1521
Rubrik Cloud Data Management	REST API 443
Veeam Backup & Replication	9392
Veritas Backup Exec	1433
Veritas NetBackup	1556, 13724 WMI ports SSH 22 (Linux)

Table 2-5 Network & Fabrics: Default Ports

Network & Fabrics Vendor	Default Ports and Notes
Brocade Switch	SMI-S 5988/5989
Cisco Switch	SMI-S 5988/5989

Table 2-6 Virtualization Vendors: Default Ports

Virtualization Vendor	Default Ports and Notes
IBM VIO	SSH 22, Telnet 23
Microsoft Hyper-V	WMI 135 DCOM TCP/UDP > 1023
VMware ESX or ESXi,vCenter,vSphere	vSphere VI SDK https TCP 443

Table 2-7 Replication Vendors: Default Ports

Replication Vendor	Default Ports and Notes
NetApp ONTAP 7-Mode	ONTAP API 80/443

Table 2-8 Cloud Vendors: Default Ports

Cloud Vendor	Default Ports and Notes
Amazon Web Services	https 443
Microsoft Azure	https 443
OpenStack Ceilometer	8774, 8777 Keystone Admin 3537 Keystone Public 5000
OpenStack Swift	Keystone Admin 35357 Keystone Public 5000 SSH 22

Chapter 3

Capacity Manager Configurations

This chapter includes the following topics:

Supported Storage Arrays and Access Requirements

Capacity Manager currently supports the storage management products and storage arrays listed below. In general, any storage array that the device manager or command-line interface supports should work with Capacity Manager. For specific prerequisites and configuration requirements, see the specific Data Collector information.

Capacity Chargebacks can be configured for block storage only; file-based storage is not supported for Array Capacity Chargeback.

Data Collectors require the following privileges to access APIs and underlying details:

- On Linux, root privileges for SSH and Telnet
- On Windows, administrator privileges for WMI.

Table 3-1 Storage Array Data Collection Prerequisites

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Dell	Compellent	v6.4, 6.5, 6.5.1 Enterprise Manager,v6.2.2.8 and v14.2.2.6 for SMI-S provider and DB	▪ SMI-S Provider User ID. ▪ Enterprise Manager IP address. ▪ Enterprise Manager DB IP address.	5988 SMI-S over http 5989 SMI-S over https 1433 DB	No installations required on the Data Collector server.
Dell EMC	Unity	330/300F, 400/400F, 500/500F, 600/600F, 350F, 450F, 550F and 650F	▪ Read-only credentials (username and password) are required to connect to DELL EMC Unity storage array using REST API.	REST API version 4.3.0 on Port 443 or 8443	

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
EMC	Elastic Cloud Storage (ECS)	3.x	■ User must belong to Management Users with System Monitor privilege	REST API on Port 80 or 4443	
EMC	VNX (Block), CLARiiON	Naviseccli, Navicli, v7.30, 7.31, 7.32	■ IP address/hostname ■ Customize: <ip address>:<port> ■ View-only user ID & pwd for CLARiiON NaviSuite	Defaults:443, 2163, 6389, 6390, 6391, 6392	■ NaviSecCLI must be installed on the Data Collector server. ■ Enable statistics logging on the VNX system to collect LUN performance data. ■ A low security level for certificates is required. Ensure this setting by using the following command: `naviseccli security -certificate -setLevel low`

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
EMC	VNX (File), Celerra	v7.0.40.1, 7.0.50.2, 7.0.52, 7.1.56	■ XML API v2 access allowed must be enabled for Client Access. ■ XML API server must be running. ■ Read-only user (Operator role).	Defaults:443, 2163, 6389,6390, 6391,6392	No installations required on the Data Collector server.
EMC	Data Domain	5.0, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 6.0, 6.1, 6.2, 7.1		Port 22 (SSH)	
EMC	Isilon	Isilon OneFS 6.5, 7.0, 7.1, 7.1.1, 7.2, 8.0	■ Access to a single, externally addressable node in the cluster via SSH. ■ Root access required (for certain isi commands).	22	■ A sudo user, specific to this data collection, can be used for root-level access.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
EMC	Symmetrix	Solutions Enabler (Symcli), v7.1.3, 7.2, 7.3, 7.4, 7.5, 7.6.1, 7.6.2, 8.0, 8.1 Unisphere 8.3	No User ID & pwd required.	2707 5480	Data Collector must be installed on the server that manages the Symmetrix arrays. Symcli uses Fibre Channel (FC) to communicate; Data Collector must be installed on a server connected via FC to the Symmetrix array, by a switch, if necessary. Sample command: symcfg list -v Unisphere 8.3 is used for Performance collection.
EMC	VPLEX	5.3, 5.4	User ID & pwd for the VPLEX storage system.	https TCP 443	The VPLEX storage system should be reachable by the Data Collector server.
EMC	XtremIO	Management Server 3.0.x, 4.0.x X2 (V6.0.x)	Read-only user ID & pwd	80	REST API

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Hitachi	Hitachi Content Platform (HCP)	HCP Version 7.2.x.x, HCP Mib Version 7.2	Read-only user ID & pwd (Local User/AD User). Refer to the HCP-specific data collector information for all permissions.	SNMP:161 REST API: https 9090	SNMP v2/3 REST API
Hitachi	Virtual Storage Platform (VSP) Hitachi Universal Storage Platform V Hitachi Unified Storage (HUS) Model 100 Series (DF850) TagmaStore AMS, USP, WMS, Network Storage Controller Lightning 9900 V Series Thunder 9500 V Series HP Command View Advanced Edition	Hitachi Device Manager (HDvM), 5.5, 6.0, 6.1, 6.2, 6.3. 6.4, 7.0, 7.1.1, 7.2, 7.3, 7.4, 7.6, 8.0, 8.4, 8.5 Hitachi Dynamic Tiering (HDT) starting with HDvM v7.1; Valid only if your HDvM is managing VSP arrays running HDT.	▪ Name of Device Manager server. ▪ Admin User ID & pwd of Device Manager. ▪ For 7.1.1 thru 7.4, the User ID configured to access HDvM must have view permissions to HRpM and HTSM. ▪ Use the Admin username for accessing the Hitachi Infrastructure Analytics Advisor	TCP 2001. For the HIAA probe: 22015 is used for HTTP and 22016 is used for HTTPS.	XML API calls over HTTP HP XP arrays are treated as Hitachi Block Storage

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Hitachi	Hitachi Tuning Manager (for performance data collection)	Hitachi Tuning Manager (HTnM) versions 7.2, 7.3, 7.4, 8.1	Supported on Windows only.	N/A	Data Collector must be installed on the host where Tuning Manager is installed. Single Data Collector policy must be used to collect both capacity data from the Device Manager server and performance data from the Tuning Manager server.
Hitachi (HNAS)	BlueArc NAS HUS (File Module)	Hitachi NAS CLI HNAS versions 10.x and 11.x	■ Hitachi NAS Admin EVS addresses separated by commas. ■ The location of the SiliconServer Control (SSC) CLI. For example: Linux: `/usr/bin/ssc` Windows: `c:\program files\ssc` ■ Create a user with supervisor privileges for accessing the Hitachi NAS.	N/A	To collect block storage that is shared with HNAS, create a separate data collector policy for the relevant supported vendor storage; for example, Hitachi Storage.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
HP	3PAR	InForm 2.3.1, 3.1.1, 3.1.2, 3.2.2, 3.3.1	■ Comma-separated list of IP addresses or host names of the HP 3PAR servers from which to collect data. ■ User ID & Password must be the same for all servers listed in the Server Address field.	ssh: 22 for CLI	Uses CLI collection via ssh
HP	EVA	v8400, 6400, 6100, 4400	■ Server name or IP address of the HP EVA management server. ■ SSSU user name & password.	2372	HP Storage System Scripting Utility (SSSU) must be installed on the Data Collector server.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
HP	StorageWorks XP	Hitachi Device Manager (HDvM), 5.5, 6.0, 6.1, 6.2, 6.3. 6.4, 7.0, 7.1.1, 7.2, 7.3, 7.4, 7.6, 8.0 HP Command View Advanced Edition (CLI/SMI-S enabled) Hitachi Dynamic Tiering (HDT) starting with HDvM v7.1; Valid only if HDvM is managing VSP arrays running HDT.	■ Name of Device Manager server ■ Admin user ID & password of Device Manager. ■ For 7.1.1 & 7.2, user ID configured to access HDvM must have view permissions to HRpM & HTSM.	Ensure port 2001 is open	XML API calls over HTTP. For HP Command View Advanced Edition, HP XP arrays are treated as Hitachi Block Storage.
HPE	Nimble Storage	5.0.7.100-607338-opt REST API Reference Version 5.0.1.0	Storage System Addresses	5392	
Huawei	OceanStor Enterprise Storage	Huawei OceanStor DeviceManager REST APIs are used. OceanStor Model - 5300 V3, 5500 V3, 5600 V3, 5800 V3, 6800 V3, Storage versions - V300R003, V300R006.	■ IP address of the storage array to be accessed ■ User ID and password for the Huawei OceanStor storage system.	Huawei OceanStor Device Manager port that provides services. The port number is 8088.	

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
IBM	6000 & 8000 (Enterprise arrays)	DSCLI 5.2.2.272	▪ User account on the array with **monitor group** privileges See "IBM Arrays: Modify Profile" on page 33.	1751 1750 1718	DSCLI must be installed on the Data Collector server. Location: Linux: **/opt/ibm/dscli** Windows: **C:\Program Files\IBM\dscli**
IBM	N Series	Data ONTAP, versions 7.2, 7.3, 8, 8.1 7-Mode and Cluster-Mode, 8.3P1 Cluster-Mode, 9	Use an existing NetApp user or create one with the necessary privileges to access the API: **login-http-admin** **api-*** See "Creating a NetApp User with API Privileges" on page 34.	443	Typically, the root, admin user has all the capabilities, but it is not advisable to use root or admin passwords. If api-* does not meet your security requirements, contact Support for a list of exact required api privileges.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
IBM	SVC	v4.3.x, v5.1, v6.1 - 6.4. v7.4 Storwize V7000 FlashSystem V9000, 840/900 Performance data is collected only for SVC 6.x and 7.4, with an SMI-S version of 1.4 or above.	■ Namespace: /root/ibm ■ IP address or hostname of SVC master console (from which data will be collected). ■ Super User ID & pwd for CIMOM. Super User ID refers to the user ID of the SVC master console server. The same user is used to execute CLI commands via ssh. ■ Enable statistics collection via the SVC UI: Manage Clusters > Start Statistics Collection.	5988 5989 ssh: 22	SSPC (System Storage Productivity Center) with CIMOM agent is required OR embedded CIMOM for v5.1, v6.1 & v6.3. Known issue: v5.1.08 does not provide vdisk data. The data collector can run on any server that can access the SSPC server with CIMOM.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
IBM	VIO	v1.5, v2.1, Hardware Management Console (HMC) Version 7	■ IP Address/Hostname of LPAR Management Server of either HMC (Hardware Management Console) or IVM (Integrated Virtualization Manager). ■ User name & password for LPAR Management Server. For HMC, user name should have at least HMCViewer permissions.	ssh: 22 telnet: 23	
IBM	XIV, Model 2810/2812-A14 (Gen 2), Model 2810/2812-114 (Gen 3)	XIV Storage Manager, v10.1.x, v10.2.x	■ XCLI must be installed on the Data Collector server. ■ Read-only user credentials are sufficient for executing XCLI commands for data collection.	TCP 7778	
INFINIDAT	InfiniBox	2.0, 2.2, 3.0.12.0 (F4000)	■ user with read-only role	https: 443	

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
LSI	LSI 1532, 1932, 3992, 3994, 6994, 6998, 7900	IBM Storage Manager CLI: 3K series: 02.70.G5.15 & above 4K/5K series: 10.10.G5.05 & above 6K/8K series: DSCLI 5.2.2.272 & above	▪ See the corresponding IBM Array requirements.	N/A	
NetApp	FAS6000 Series, FAS3100 Series, FAS3000 Series, FAS2000 Series, V-Series	Data ONTAP, versions 7.2, 7.3, 8, 8.1, 8.2, 7-Mode and Cluster-Mode, 8.3P1 Cluster-Mode, 9	▪ Use an existing NetApp user or create one with the necessary privileges to access the API: **login-http-admin api-*** Typically, the root, admin user has all the capabilities, but it is not advisable to use root or admin passwords. See "Creating a NetApp User with API Privileges" on page 34.	TCP 80/443	Array performance data also can be collected via the ONTAP API. If api-* does not meet your security requirements, contact Support for a detailed list of exact api privileges that are required.

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
NetApp	E-Series: E2600, E2700, E5400, E5500, EF560, E2800	SANtricity SMcli: 10.86, 11.30		TCP 2436	SMCLI must be installed on the Data Collector server. Location: Linux: **/opt/SM8/client/** Windows: **C:\Program Files\SM8\client** This also applies to the IBM DS Series arrays.
OpenStack	OpenStack Swift (Juno10, TBC), SwiftStack v2.2		■ Keystone v2 ■ Proxy path for Swift configuration files must be specified. ■ Controller credentials that have access to tenants/projects. ■ Swift proxy server credentials with super-user privileges.	35357 for Keystone Admin 5000 for Keystone Public 22 for SSH	■ If multiple proxies exist, APTARE IT Analytics uses only one. Capacity reports will reflect only one proxy. ■ Configure the policy to use the address of the actual proxy server, not the server responsible for load balancing. ■ Capacity data is collected from devices mapped to OpenStack nodes.
OpenStack	OpenStack Ceilometer	REST API		8777	■

Table 3-1 Storage Array Data Collection Prerequisites *(continued)*

Vendor	Arrays/NAS	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Pure Storage	FlashArray	REST API	View-only User ID for the Pure Storage FlashArray storage system.	443	API calls for HTTPS
Sun	StorEdge 9900	Hitachi Device Manager (HDvM), 5.5, 6.0, 6.1, 6.2, 6.3. 6.4, 7.0, 7.1.1, 7.2, 7.3, 7.4, 7.6, 8.0	■ Device Manager server name. ■ Admin user ID & password of Device Manager.	2001	XML API calls over HTTP
Veritas	NetBackup Appliance 3.1.2, 3.2, 3.2.1 NetBackup Models: 5340,5240,5330			1556	

IBM Arrays: Modify Profile

For the IBM Enterprise arrays (6000 & 8000 Series), the profile must be modified. Locate the profile file, typically in the **/profile** sub-directory and named **dscli.profile**. In this file, uncomment the Output Format property and set it to XML, as shown in the following example.

```
# Output format type for ls commands, which can take one of the
following values:
#   default: Default output
#   xml    : XML format
#   delim  : delimit columns using a character specified by "delim"
#   stanza  : Horizontal table format
# "format" is equivalent to option "-fmt default|xml|delim|stanza".
format: xml
```

Creating a NetApp User with API Privileges

Use an existing NetApp user or create one with the necessary privileges to access the application programming interface (API). This role and user is required for collection from NetApp-7 systems. Typically, the root, admin user has all the capabilities, but it is not advisable to use root or admin passwords.

To create a new user, with the required privileges, on a NetApp system, use the following Command Line Interface (CLI) steps. For the **role** command, do **not** include a space after the comma.

```
filer> useradmin role add apifarole -a login-http-admin,api-*
filer> useradmin group add apifagroup -r apifarole
filer> useradmin user add apifauser -g apifagroup
```

If api-* does not meet your security requirements, additional File Analytics privileges can be configured using the following steps:

```
filer> useradmin role add apifarole -a api-volume-list-info,api-nfs-
exportfs-list-rules,api-cifs-share-list-iter-start,api-cifs-share-list-iter
-next,api-cifs-share-list-iter-end,api-snapdiff-iter-start,api-snapdiff-
iter-next,api-snapdiff-iter-end,login-http-admin,api-volume-options-list-
info,api-snapshot-list-info,api-snapshot-delete,api-snapshot-create,api-
nameservice-map-uid-to-user-name
filer> useradmin group add apifagroup -r apifarole
filer> useradmin user add apifauser -g apifagroup
```

Note: For the **role** command, do **not** include a space after the comma.

Creating a NetApp Cluster-Mode User with API Privileges

Data collection of NetApp Cluster-Mode requires a specific read-only role and user in order to collect data for a cluster.

To create a new user account with the required privileges, use the following Command Line Interface (CLI) steps. This set of commands creates a role as **apt_readonly** and then a user named **apt_user** with read-only access.

1. Create a read-only role using the following two commands.

```
security login role create -role apt_readonly -cmddirname DEFAULT
```

```
 -access readonly
security login role create -role apt_readonly -cmddirname security
 -access readonly
```

2. Create the read-only user using the following command. Once you have executed the create command, you will be prompted to enter a password for this user.

```
security login create -username apt_user -application ontapi
-authmethod password -role apt_readonly
```

The resulting role and user login will look something like this:

```
      Role            Command/                          Access
Vserver    Name          Directory                    Query Level
---------- ------------- --------- ------------------ --------
cluster1   apt_readonly  DEFAULT                       readonly
cluster1   apt_readonly  security                      readonly
cluster1::security login> show
Vserver: cluster1
                              Authentication                  Acct
UserName         Application  Method         Role Name        Locked
---------------- -----------  -------------- ---------------- ------
apt_user         ontapi       password       apt_readonly     no
```

Array/LUN Performance Data Collection

The following array families are supported for block storage LUN performance and port performance data collection.

Array Family	Read/Write IO/sec	Total IO/sec	Read/Write MB/sec	Read/Write Cache Hits/sec	Read/Write Response (ms)	Total Response (ms)	Notes
Dell Compellent	X	X	X	X	--	--	

Array Family	Read/Write IO/sec	Total IO/sec	Read/Write MB/sec	Read/Write Cache Hits/sec	Read/Write Response (ms)	Total Response (ms)	Notes
EMC VNX (CLARiiON)	X	Calculated	X	X	X	Calculated	For CLARiiON arrays: The minimum FLARE OS version required to capture response times is 04.30.000.5.524 A11. Note that VNX (Block) will have completely different FLARE releases and all support the collection of the counter fields needed for capturing response time, starting with FLARE version 05.31.000.5.006 A01. Enable statistics logging on the VNX system.
EMC Symmetrix	X	X	X	X	--	--	

Array Family	Read/Write IO/sec	Total IO/sec	Read/Write MBs/sec	Read/Write Cache Hits/sec	Read/Write Response (ms)	Total Response (ms)	Notes
EMC XtremIO	Calculated	Calculated	Calculated	--	X	X	For EMC XtremIO, the values obtained are averages over the time interval. The Read/Write/Total IOs and the Read/Write MBs are multiplied by the time interval and persisted.

Array Family	Read/Write IO/sec	Total IO/sec	Read/Write MB/sec	Read/Write Cache Hits/sec	Read/Write Response (ms)	Total Response (ms)	Notes
HDS Tuning Manager	X	Calculated	X	X	X	X	For Hitachi arrays: To collect performance data from Hitachi Tuning Manager, the Data Collector must be installed on the same server as Tuning Manager. And, a single Data Collector policy must be used to collect both the capacity data from the Device Manager server and the performance data from the Tuning Manager server.
HP 3PAR	X	X	X	X	X	X	
IBM SVC	X	X	X	--	--	--	
IBM XIV	X	X	X	X	X	X	

Array Family	Read/Write IO/sec	Total IO/sec	Read/Write MB/sec	Read/Write Cache Hits/sec	Read/Write Response (ms)	Total Response (ms)	Notes
NetApp ONTAP 7-Mode (Block only)	X	Calculated	X	--	--	Avg Latency	For NetApp ONTAP 7-Mode (Block only): Total response time is the average latency (ms) for all LUN read and write operations. Performance data is collected for both iSCSI LUNs and FC LUNs.
Pure Storage FlashArray	X	Calculated	X	--	X	Calculated	

Port Performance Metrics

Array Family	Read/Write MB	Total MB	Read/Write I/O	Total I/O	Notes
Dell Compellent	X	Calculated	--	X	For Dell Compellent: Only Fibre Channel port statistics are collected.
EMC VNX (CLARiiON)	Not Supported	Not Supported	Not Supported	Not Supported	
EMC Symmetrix	--	X	--	X	
EMC XtremIO	--	Calculated	--	Calculated	

Array Family	Read/Write MB	Total MB	Read/Write I/O	Total I/O	Notes
HDS Tuning Manager	X	X	X	X	
HP 3PAR	X	Calculated	--	X	
IBM SVC	Not Supported	Not Supported	Not Supported	Not Supported	
IBM XIV	X	X	X	X	
NetApp ONTAP 7-Mode (Block only)	X	Calculated	--	--	

Calculated = Calculated from collected data, X = Collected from the array, -- = Not Collected

EMC Isilon Metrics

Isilon performance data (raw, hourly, and daily) is collected from SNMP MIB statistics. For example, collected data includes such metrics as cluster, node, protocols (CIFS, SMB, FTP, HTTP), and disk performance. See the Array Performance Statistics Technical Note for an extensive list of collected metrics.

NetApp Cluster-Mode Metrics

A large variety of NetApp Cluster-Mode performance data (raw, hourly, and daily) is collected. For example, collected data includes such metrics as system, protocols (CIFS and NFS), volume, LUN, and target port performance. See the Array Performance Statistics Technical Note for an extensive list of collected metrics.

EMC Symmetrix Enhanced Performance Metrics

In addition to LUN and Port performance metrics that can be collected from EMC Symmetrix arrays, data collection gathers other performance metrics by accessing storage devices via the EMC Unisphere REST API.

Host Resources Prerequisites and Configurations

To gather data from hosts, the following privileges are required.

See "Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements" on page 41.

See "WMI Proxy Requirements for Windows Host Data Collection" on page 42.

See "Host Resources Supported Configurations" on page 42.

See "Supported Host Bus Adapters (HBAs)" on page 45.

Host Access Privileges, Sudo Commands, Ports, and WMI Proxy Requirements

If you are using sudo to elevate access to root privileges, update the sudoers file:

- Sudoers file: /etc/sudoers
- Use the lists of the sudo commands (per OS) that are located on the Portal server in:

  `<Home>/opt/aptare/updates`

- Comment out this line in the sudoers file: **Defaults requiretty**

Access Requirements by OS

Table 3-2 Table 3.1 Host Resources Prerequisites by Operating System

Host OS	Host Access Requirements	Port Requirements	Notes
Linux RH Linux SUSE CentOS AIX HP-UX	ssh or telnet must be enabled Some commands may require an account with super-user root privileges. **sudo**, **sesudo**, and **pbrun** are supported; ensure the user ID has required sudo, sesudo, or pbrun privileges.	ssh: 22 telnet: 23	Collection uses ssh/telnet to execute commands. OS and application commands require root privileges for HBA API access. The **sysstat** utility must be installed on Linux servers or storage nodes for Linux host performance data collection.
Windows	A WMI Proxy is required to collect from Windows hosts. All Windows hosts require a user ID with Administrator privileges for WMI.	RPC: TCP Port 135 for WMI DCOM: TCP/UDP 1024-65535 TCP/IP 1248, if WMI Proxy server is not the same as the Data Collector server	When the Data Collector Policy is configured to include file-level data, the Data Collector and WMI need to use a Windows Domain Administrator ID.

WMI Proxy Requirements for Windows Host Data Collection

A WMI Proxy server is required for collecting data from Windows hosts.

- WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service. To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.

Table 3-3 Host Resources Prerequisites by Operating System

Data Collector Server OS	WMI Proxy Requirements	Notes
Windows	WMI Proxy will be installed on the Data Collector server by default	
Red Hat Linux SUSE CentOS	Identify a Windows machine on which to install the WMI Proxy	Note the IP address of the server on which the WMI Proxy resides, as you will use it during the Portal configuration process.

Host Resources Supported Configurations

You can configure Capacity Manager to collect the following Host Resources data:

Table 3-4 Host Resources Supported Configurations

Host Resource	Supported Configurations/Versions	Port	Prerequisites and Notes
Applications	Exchange: Microsoft Exchange Server 2010	389	The user name must have privileges to search under the DN within the Active Directory. Typically, this is an Administrator. Microsoft Exchange 2010: Data collection requires PowerShell remoting to be enabled on the Exchange server. The Data Collector connects to PowerShell via the WMI Proxy to execute PowerShell commands. For details on remoting, see the Microsoft Administrator's Guide to Windows PowerShell Remoting.
	Oracle: Oracle 12c	1521	Oracle user must have SELECT_CATALOG_ROLE role granted
	Oracle ASM: Oracle ASM, v10gR1, 10gR2, 11gR1, 11gR2, 12c	1521	Oracle ASM requires a user with **SYSASM** (Oracle-supported only for 11g and above) or **SYSDBA** privileges
Containers	Oracle Containers		Sometimes referred to as Solaris Zones.
Clustering	Clustering technologies, both active-active and active-passive		Clusters are listed as Related Hosts in reports. This relationship is established when multiple servers are accessing the same storage.

Table 3-4 Host Resources Supported Configurations *(continued)*

Host Resource	Supported Configurations/Versions	Port	Prerequisites and Notes
File Systems	■ Solaris ZFS; Solaris Volume Manager (SVM) Metastat ■ AIX 5.2, 5.3 JFS and JFS2, with correlation to SAN disks ■ SUSE SLES 9, 10; 32 & 64 bit REISER FS & EXT3 & Logical Volume Manager (LVM & LVM2) ■ VxFS on all supported Operating Systems ■ Windows NTFS ■ Oracle ASM ■ Linux ext4 file systems		
Multi-pathing	■ EMC PowerPath ■ Hitachi Dynamic Link Manager (HDLM) ■ VERITAS Dynamic Multi-Pathing (VxDMP) ■ Device Mapper Multipath for Linux ■ Microsoft MPIO - Windows 2003, 2008 (R2), Windows 2012 (R2) drivers		If using a non-supported MPIO driver, storage capacity may be double-counted in capacity reports.
Operating Systems	■ Windows 2012 Server. ■ IBM AIX ■ HP-UX ■ SUSE		In general, these operating systems up to and including the latest OS patch level are supported.

Table 3-4 Host Resources Supported Configurations *(continued)*

Host Resource	Supported Configurations/Versions	Port	Prerequisites and Notes
Volume Managers	■ Veritas Volume Manager 5.0 and 5.1 (Supported OS: RedHat Linux, AIX, HP-UX, Windows) ■ Solaris Volume Manager ■ Linux Logical Volume Manager ■ AIX Logical Volume Manager ■ HP-UX Logical Volume Manager		Besides Veritas Volume Manager, each of the operating systems comes with its own built-in logical volume manager, so no specific version numbers are mentioned

Supported Host Bus Adapters (HBAs)

Table 3-5 Host Bus Adapters: Supported Configurations

HBA OS	Supported Configurations/Versions	Prerequisites
Windows	HBA information is obtained using OS commands, looking for specific operating system files and directories. Product-specific commands (Emulex and QLogic) are also used.	An internal probing mechanism is used to gather HBA data.
AIX & HP-UX	HBA information is obtained using OS commands. No product-specific commands are used; therefore, Capacity Manager supports all HBAs supported by these operating systems.	fcmsutil (used only for HP-UX HBA information; should already be installed by default)
Linux	HBA information is obtained using OS commands, looking for specific operating system files and directories. Product-specific commands (Emulex and QLogic) are also used.	scli or hbacmd (required only for HBA information)
Solaris	HBA information is obtained using OS commands such as **luxadm**. Product-specific commands (Emulex and QLogic) are also used.	scli or hbacmd (required only for HBA information)

Chapter 4

Cloud Configurations

This chapter includes the following topics:

Supported Systems and Access Requirements

For specific prerequisites and configuration requirements, see the Cloud Data Collector information.

Data Collectors require the following privileges to access APIs and underlying details:

- On Linux, root privileges for SSH and Telnet
- On Windows, administrator privileges for WMI.

Table 4-1 Data Collection Prerequisites

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Amazon Web Services	■ S3 Bucket (Details and Usage) - Simple Storage Service (S3) for storage in the cloud ■ EC2 Details - Elastic Cloud Compute (EC2) for computing services, much like virtual servers ■ Billing Records - Usage and corresponding charges, by service	AWS Java SDK	Before a Data Collector can gain read-only access to retrieve data the following steps are required in Amazon Web Services (AWS) **1** Configure an S3 Bucket to Receive Billing Reports. **2** Activate AWS detailed billing. **3** Select Cost Allocation Tags. **4** Create an AWS IAM User. **5** Generate Access Keys. **6** Link AWS Accounts for Collection of Consolidated Billing Data.	https 443 for read-only access to the data	AWS reports are under Capacity Manager and Virtualization Manager.

Table 4-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Microsoft	■ Azure Virtual Machine ■ Azure Storage Account ■ Azure Billing ■ Azure Backup	REST API	Prerequisite: Install the Azure Powershell client on a Windows computer. Execute Microsoft Azure Powershell as an administrator. **1** Find your Tenant ID and Azure Subscription ID **2** Register a new Application **3** Create a Principle and assign Contributor role to the application. **4** Find your Azure Application ID, Offer ID Application Password.	443	The Data Collector only supports Azure resources deployed with the Resource Manager model.

Table 4-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
OpenStack	OpenStack Swift (Juno10, TBC), SwiftStack v2.2		■ Keystone v2 ■ Proxy path for Swift configuration files must be specified. ■ Controller credentials that have access to tenants/projects. ■ Swift proxy server credentials with super-user privileges.	35357 for Keystone Admin 5000 for Keystone Public 22 for SSH	■ If multiple proxies exist, APTARE IT Analytics uses only one. Capacity reports will reflect only one proxy. ■ Configure the policy to use the address of the actual proxy server, not the server responsible for load balancing. ■ Capacity data is collected from devices mapped to OpenStack nodes.
OpenStack	OpenStack Ceilometer	REST API	■ Keystone v2 ■ Credentials that have admin access to tenants/projects.	35357 for Keystone Admin 5000 for Keystone Public 8777 for Ceilometer API Service 8774 for Compute	

Chapter 5

Virtualization Manager Configurations

This chapter includes the following topics:

Supported Versions

- VMware
  - ESX or ESXi Servers 5.0, 5.1, 5.5, 6.0, 6.5, 6.7 (vSphere)
  - Virtual Center (vCenter) Server 5.0, 5.1, 5.5, 6.0, 6.5, 6.7
- Microsoft Hyper-V
  - Hyper-V servers running Microsoft Windows Server 2012 R2, Microsoft Windows Server 2016
  - Microsoft Hyper-V Server 2012 R2 and 2016 are supported for collection

Virtualization Manager Data Collector Requirements for VMware

For Virtualization Manager data collection, VMware Tools (VM Tools) must be installed to enable collection of key properties of a VM Guest, such as the IP address, host name, mount points, disk path, available space on VM guest volumes, and guest operating system of the VM. Whenever data collection cannot retrieve

a host name, a VM Guest will not be treated as a host in the Inventory and Virtualization Manager reports will not be populated with host details. For example, a host name may not be available in the following situations: the VM may be down, VM Tools may not be installed on the VM Guest, or a VM template may have been collected.

The VMware Data Collector uses the VMware Infrastructure SDK to make XML API calls over HTTP to retrieve data from ESX servers. The VMware Data Collector is multi-threaded, enabling it to poll up to five vCenters in one polling cycle.

VMware requires the following access for data collection:

1. View-only VMware User ID that has a role with the following privileges:
   - Read-Only
   - Browse Datastore

   Note: Permissions can be granted to an existing local account or domain/AD user.

2. Assign the user to the root-level folder permissions of vSphere.

   The administrator user who provisions the read-only role for collection must be an administrator at the root level, not just at a data center or other level. If multiple vCenters are available for administration in the client (Linked Mode), that administrator user must be provisioned at the root level for each vCenter Server from which data is collected.

3. Port 443 must be open. Data collection uses HTTPS without certificate validation for encrypted connections. This allows the use of a self-signed certificate on the VMware server.

Creating a VMware Read-Only User

Permissions can be granted to an existing local account or domain/AD user. The following VMware user-creation steps are required only if you do not want to grant permissions to an existing user. Refer to the information specific to Virtualization Manager data collection for a detailed procedure for the following steps.

1. In VMware, clone a read-only role and create a Virtualization Manager Group role.
2. Add the **Browse Datastore** permission and add it to the root-level folder.
3. Create a User and assign it to the Virtualization Manager Group.

Virtualization Manager Data Collector Requirements for Microsoft Hyper-V

- The collector must have WMI network access to the Hyper-V servers. User credentials must allow access to the root\cimv2, root\virtualization\v2 and root\MSCluster WMI namespaces.
- The Data Collector Service that is initially installed uses the Local System as the Log in account. Sometimes this account does not have permissions to run remote WMI commands. You should instead change the Service configuration to use a Log in account that has Local Administrative privileges.
- The collector uses a PowerShell script that uses WMI to communicate with the Hyper-V, and makes a number of read-only calls to gather the information. PowerShell script execution needs to be enabled on the system running this script. The version of PowerShell on the system must be 5.0 or above.
- A full collection path to Hyper-V server attached SAN or NAS storage requires that Host Resource collection be run first against the Hyper-V servers.
- WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service.

To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.

Chapter 6

File Analytics Configurations

This chapter includes the following topics:

Data Collector Probes by Storage Type

In the following table, each check represents a valid configuration of a probe and storage type. Note that in many arrays, the file systems can have multiple protocols--both CIFS and NFS. If an array supports both, CIFS share collection may be able to be configured for NFS mounts. Also note that Other - CIFS refers to storage that has CIFS capability, such as Hitachi Unified Storage (HUS) and EMC Isilon storage.

Table 6-1 File Analytics Data Collector Probes by Storage Type

Storage Type	CIFS (File Analytics Collector)	Windows (Host Probe)	UNIX/Linux (Host Probe)
Windows	X	X	
UNIX/Linux	X		X
NetApp - CIFS	X		
NetApp - NFS			
NetApp - FC LUNs		X	X
NetApp - iSCSI LUNs		X	X

Table 6-1 File Analytics Data Collector Probes by Storage Type *(continued)*

Storage Type	CIFS (File Analytics Collector)	Windows (Host Probe)	UNIX/Linux (Host Probe)
Other - CIFS	X		

CIFS Shares

- The recommended Windows Data Collector server operating system is Windows server 2012.
- The Windows LAN Manager authentication level, in the local security policy security options, must be modified to: Send LM & NTLM - use NTLMv2 session security if negotiated. This allows the Data Collector to invoke the **net use** command with the password supplied on the command line. Without this setting, later versions of Windows will terminate with a system error 86 (invalid password).
- Windows CIFS Shares collection requires the Windows Domain User ID. This User ID must have Administrative privileges.
- UNIX CIFS Shares collection requires super-user root privileges. Access control commands, such as sudo, sesudo, and pbrun are also supported. If using any of the access control commands, verify that the User ID has sudo, sesudo, or pbrun privileges.
- The CIFS Data Collector uses ports 137 and 139.

Host Inventory Probe

- Windows servers: Supported versions include Windows Server 2012.
  - When the Data Collector Policy is configured to include file-level data, the Data Collector and associated WMI need to use a Windows Domain Administrator ID.
- Linux servers: Linux and AIX (but not HP-UX) are supported.

Chapter 7

Fabric Manager Configurations

This chapter includes the following topics:

Switch Vendors

Fabric Manager provides reports that include topological views of the interrelationships of objects attached to the switches--end-to-end paths for objects such as LUNs and File Systems. Fabric Manager can collect data for the following switches.

Vendor	Agent/Interface	Notes
Brocade	Preferred SMI Integrated Agents: DCFM (Data Center Fabric Manager) v10.4 CMCNE (EMC Connectrix Manager Converged Network Edition) v10.4 Network Advisor (BNA) v11.x, 14.4 Stand-alone host-based SMI Agent installed on a host that can communicate with the Fabric v120.9.0	■ Select SMI Agent-only option when installing DCFM or Network Advisor. ■ The Brocade host-based SMI Agent supports Brocade SAN infrastructures from a single access point by communicating with multiple switches and multiple fabrics. Consult the Brocade list of host-based SMI-S switches. APTARE supports the switches on this list, including Brocade DCX Backbones. For switches with firmware version 7, you must use the integrated SMI agent. ■ SMI-S ports 5988/5989
Cisco	Preferred SMI Agent: DCNM (Data Center Network Manager) v5.2.1 MDS 9000 SAN-OS v3.3.2 or higher MDS 9000 NX-OS v4.1 or higher	■ See www.cisco.com for details on the Cisco MDS 9000 Family switches supported by specific OS versions and releases. See “Download Cisco Data Center Network Manager” on page 56. ■ SMI-S ports 5988/5989

Download Cisco Data Center Network Manager

To download the preferred SMI Agent that is relevant to your OS:

1. Go to Cisco.com and click **Support** at the top of the home page.
2. In the Support Downloads page, search for **Cisco Data Center Network Manager**.
3. In the Products list, under Switches, click the **Cisco Data Center Network Manager** link and choose the 5.2 version that is relevant to your OS. See System Requirements in the DCNM 5.2 Release Notes.

Chapter 8

Backup Manager Configurations

This chapter includes the following topics:

Backup Solutions and Versions

Table 8-1 Supported Backup Solutions

Backup Solution	Version	Notes and Access Requirements
Cohesity DataProtect	4.x, 5.x, 6.3.x	REST API on Port 80 or 443

Table 8-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
Commvault Simpana	9.0, 10	At a minimum, read-only (db_datareader) database access with execute permission is required for the following functions: ■ dbo.GetDateTime ■ dbo.GetUnitTime ■ dbo.GetJobFailureReason ■ dbo.JMGetLocalizedMessageFunc Windows user name and password with administrative access to CommServe Server for WMI (to collect job detail logs). ■ Port 1433 for the MSSQL Server database instance This is usually 1433, but it can be any port. Other Ports, if collecting skipped files details: ■ File sharing: port 445 ■ WMI control channel: TCP port 135 ■ DCOM TCP/UDP: any port greater than 1023
Dell EMC NetWorker Backup & Recovery	9.2.1.x, 18.x, 19.x	Port 9090 (Used for NetWorker REST API connection) EMC NetWorker data collection policies are implemented based on vendor version number. Legacy versions of EMC NetWorker (pre version 9.2.1.x) are collected using the policy titled: EMC NetWorker. For EMC NetWorker versions post 9.2.1.x, collection is done using the policy titled: DELL EMC NetWorker Backup & Recovery.
EMC Avamar	4.x, 5.0, 6.0, 6.1, 7, 7.2, 7.3, 7.5, 18.1, 18.2, 19.1, 19.2	■ Ports 5555 and 22 (SSH)
EMC Data Domain	5.0, 5.1, 5.2, 5.4, 5.5, 5.6, 5.7, 6.0, 6.1, 6.2, 7.1	■ Port 22 (SSH)

Table 8-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
EMC NetWorker	7.2 - 7.6, 8.0, 8.1, 8.2	■ EMC NetWorker data collection policies are implemented based on vendor version number. Legacy versions of EMC NetWorker (pre version 9.2.1.x) are collected using the policy titled: EMC NetWorker. For EMC NetWorker versions post 9.2.1.x, collection is done using the policy titled: DELL EMC NetWorker Backup & Recovery. ■ If NetWorker is installed on a Windows server, the Data Collector must be on a Windows server. ■ NSRADMIN TCP 7937-7940 ■ WMI Proxy range of ports, Linux SSH 22
HP Data Protector	8.1, 9.0x	■ Port 5555 ■ WMI Proxy range of ports, Linux SSH 22 ■ A WMI Proxy is only needed if collecting from Windows hosts and when the Data Collector is on a server that is different from the Cell Manager server. ■ The HP Data Protector (HPDP) client software version must match the specific version (major and minor) of the HPDP server being probed. ■ If the Data Collector is installed on a Linux OS, a WMI Proxy Server must be installed on a Windows system in order to collect data from a Cell Manager that is installed on a Windows system.
IBM Spectrum Protect (TSM)	6.1, 6.2, 6.3, 7.1, 8.1	■ TSM instances running on z/OS are not supported. ■ TSM v6.3 is not supported on a Windows 2012 Data Collector. ■ Typically, Port 1500
NAKIVO Backup & Replication	9.1.1	■ Director Web UI port used during installation (Default: 4443)
Oracle Recovery Manager (RMAN)	11g, 12c	■ Typically Port 1521
Rubrik Cloud Data Management	v4.1 - v5.0	■ Port 443
Veeam Backup & Replication	9.5	■ Port 9392

Table 8-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
Veritas Backup Exec	2012, 15, 20 - all running on Windows OS	■ Port 1433 ■ The Backup Exec Administrator account used by the Data Collection policy must have the database role membership of **db_datareader** for the BEDB (Backup Exec Database). ■ Note that the version of Backup Exec that is reported by the Backup Exec 15 installation is version 14.2.
Veritas NetBackup including: Sun StorageTek ACSLS Manager SLP	6.5, 7.0, 7.1, 7.5, 7.6, 7.7.1, 7.7.2, 7.7.3, 8.0, 8.1, 8.2 NetBackup 5xxx appliances SLP, NetBackup v7.1 & higher	■ The APTARE Data Collector makes calls to various NetBackup CLI (Command Line Interface) commands, such as **bpdbjobs**. These commands are a standard component of the NetBackup product and APTARE IT Analytics requires that they are operational as per the NetBackup specifications. ■ Ports 1556 and 13724 For centralized data collection, See "Centralized NetBackup Data Collection Requirements" on page 60.

Centralized NetBackup Data Collection Requirements

- Minimum Requirements: 64-bit OS, 2 CPUs or vCPUs and 32 GiB RAM.
- If there is a firewall between the NetBackup Master Servers and the Data Collector Server, ensure that bi-directional port communication is open on ports 1556 and 13724.
- For a NetBackup Centralized Data Collector (Linux or Windows OS), the Data Collector needs access to the Admin commands (CLI). This typically requires the NetBackup Master Server binaries to be installed on the Data Collector server. The CLI is available only with the Master Server binaries. Note that the installation of these binaries may require you to acquire a NetBackup Master Server license from Veritas.
- See "Veritas NetBackup 8.1 (and later) Requirements for Centralized Collection" on page 61.
- The NetBackup software version on the Data Collector must match the major and minor version of the NetBackup software that is installed on the Master or Media Server that is being probed. When the Data Collector starts, it checks

versions and halts collection for the Master Server where the mismatch is found. Refer to the Veritas documentation for more information about major and minor version requirements.

- For SLP collection, a WMI Proxy Server is required. WMI uses DCOM for networking. DCOM dynamically allocates port numbers for clients. DCOM's service runs on port 135 (a static port) and any client communicating with a host connects on this port. The DCOM service allocates the specific port for the WMI service. To set up a fixed port for WMI, see http://msdn.microsoft.com/en-us/library/bb219447%28VS.85%29.aspx.

See "Required Software" on page 62.

Note: If all NetBackup Masters configured in the collection policy are using the Linux operating system, then a WMI Proxy is not required.

Veritas NetBackup 8.1 (and later) Requirements for Centralized Collection

Veritas NetBackup 8.1 introduces a series of changes to the way a NetBackup host (such as the Data Collector) communicates with NetBackup Masters. These changes incorporate an enhanced secured channel for communication and more sophisticated host identity verification.

These changes require installation steps on the centralized Data Collector system that are not required for collection from NetBackup Master Servers prior to version 8.1.

Requirements for successful collection from a NetBackup 8.1 (and later) system:

- As with all centralized NetBackup Data Collectors post NetBackup v7.7.3, the NetBackup software version on the Data Collector must match the major and minor version of the NetBackup software that is installed on the Master or Media Server that is being probed.
- After installing the correct Veritas software, the Data Collector server needs to be added as a trusted server to all NetBackup Master Servers from which you want to collect data. This is typically accomplished using the netbackup command nbcertcmd. If the Data Collector is NOT registered as a trusted server, collection will not work.
- A CA root certificate and a host ID-based security certificate must be installed on the Data Collector Server for each Master Server that will be accessed for data collection. Refer to the Veritas NetBackup Security and Encryption Guide, Version 8.1 for information on how to deploy CA and host ID-based certificates.

- The Data Collector Server must be added as a NetBackup Media Server in both NBDB and registry/bp.conf files, on each NetBackup Master that will be accessed for data collection. Refer to the Managing Media Servers section of the Veritas NetBackup Administrators Guide, Volume 1.
- The NetBackup media server software daemons on the Data Collector Server must be active.

Required Software

Table 8-2

NetBackup 7.6 or earlier: Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Master	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Master Server software installed on the Data Collector server. If SLP collection is required, a WMI Proxy Server must be set up on a Windows server.
Linux NetBackup Master	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Master Server software installed on the Data Collector server.

Table 8-3

NetBackup 7.7 or later: Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Master	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Master Server software installed on the Data Collector server.	NetBackup Master or Media Server software installed on the Data Collector server. If SLP collection is required, a WMI Proxy Server must be set up on a Windows server.
Linux NetBackup Master	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Master Server software installed on the Data Collector server.	NetBackup Master Server software installed on the Data Collector server.

Chapter 9

Internal TCP Port Requirements

This chapter includes the following topics:

Internal TCP Port Requirements

The Portal Server makes extensive use of TCP ports for inter-process communications. The ports listed in this section are internal to APTARE IT Analytics, used to communicate within the Portal server. They are listed here so that you can determine if there are port conflicts with other software in your environment. The standard ports used by APTARE IT Analytics are certified to work and operate in an environment where the customer or partner does not install any other software other than the underlying operating system and latest operating system patches.

In some special circumstances, the customer may elect to install the Portal Server software on a system that is running (or may have run in the past) another third party software product. Such third party software product might include NetBackup Advanced Reporter, Hitachi Storage Services Manager (HSSM), or any other product that also uses TCP ports for inter-process communications. In these circumstances, special care will need to be taken to ensure that port and directory/filename conflicts between the respective software products do not occur. These are uncertified and unsupported environments unless setup and certified by a support services technician. To set up and certify these “special case” environments, a port and directory/application conflict audit would need to be performed on the target portal system(s). Once the conflicts have been identified, where possible, a non-standard

installation ports for the APTARE IT Analytics software and any associated third-party components would be assigned.

Internal Portal Server Ports

The following table describes the standard TCP ports that are used by the Portal Server and any embedded third-party software products as part of a standard “out-of-the-box” installation:

Table 9-1

Product	Port	Description
Apache Web Server	80	HTTP listener port
Apache Web Server	443	HTTPS/SSL listener port
Oracle	1521	Oracle TNS listener port
Tomcat - Data Receiver	8011, 8017	Apache connector port and shutdown port for Data Receiver instance of tomcat
Tomcat - Portal	8009, 8015	Apache connector port and shutdown port for Portal instance of tomcat

Internal Data Collector Ports

The following table describes the standard internal TCP ports that are used by the Data Collector and any embedded third-party software products as part of a standard “out-of-the-box” installation:

Table 9-2

Product	Port	Description
Capacity Manager		
HDS Device Manager	9323 9324+	Hitachi Data Collector
EMC Symmetrix	9723 9724+	EMC Symmetrix Data Collector

Table 9-2 *(continued)*

Product	Port	Description
EMC CLARiiON	9223 9224+	EMC CLARiiON Data Collector
EMC VNX	9223 9224+	EMC VNX (Block) CLARiiON and EMC VNX (File) Celerra Data Collectors
NetApp	10223 10224+	NetApp Data Collector
Host Resources	9423 9425+	Host Resources Collector
WMI Proxy Server	1248	Used to communicate with the Host Resources Data Collector
Backup Manager		
Veritas NetBackup	9123	NetBackup agent
IBM Spectrum Protect (TSM)	9823 9824+ 9825+ 1500	Spectrum Protect (TSM) Data Collector event and meta collectors -Server port
EMC NetWorker	9623 9624+ 9625+	EMC NetWorker Data Collector event and meta collectors
Veritas Backup Exec	9123 9124+	Backup Exec event collector port
HP Data Protector	9523 9524+ 9554+	HP Data Protector Data Collector
Generic Backup	9923 9924+	Generic Backup for collection of data from backup products not native to APTARE IT Analytics

+ indicates an Admin port