IT Analytics Certified Configuration Guide

Release 11.7

VERITAS
now part of Cohesity

IT Analytics Certified Configuration Guide

Last updated: 2026-05-05

Legal Notice

Cohesity Support

Reach Cohesity Support

There are several ways to create a Cohesity support case.

- Go to Cohesity Support, to search in our knowledge base; or contact us by phone - United States and Canada: 1-855-9CO-HESI (926-4374), option 2.
- Log in to the Cohesity Support Portal to create a new case.
- Click the (**?**) icon on the Cohesity UI and select Support Portal.

Support/Service Assistance

First, contact the Service Provider that you have contracted for service and support. If you work directly with Cohesity and have a product warranty/entitlement, repair pricing, or technical support-related question, see your options below:

- To find solutions to your product issues or for suggestions or best practices, visit the Cohesity Knowledge Base.
- Log in to the Cohesity Support Portal to create a new case.
- To monitor your open cases, log in to the portal and click the **Cases** tab on the home page. This page should have all the case statuses and updates. You can also view individual case status.

Cohesity Software Running on Partner Hardware

For Cohesity software running on qualified third-party hardware, the following support workflow applies:

1. The customer may contact Cohesity Support first if the issue cannot be determined as a hardware issue.

   Note: Cohesity cannot process hardware replacement requests for partner hardware.

2. Cohesity Support triages the issue. If it is a software issue, Cohesity Support continues to work on it.
3. If it is a hardware/firmware issue or is suspected to be a hardware/firmware issue, Cohesity provides information about the issue to the customer and requests that the customer open a support ticket with the appropriate partner.
4. If needed, Cohesity Support can join a three-way call with the partner and the customer.
5. The customer informs Cohesity Support on the progress of the partner's case.

Contents

Chapter 1

Introduction

This chapter includes the following topics:

IT Analytics Overview

IT Analytics provides you visibility into everything with predictive analytics software for multi-vendor backup, storage, and virtual infrastructures.

It maximizes the value of your IT Environment by minimizing the costs and improved management of the resources. IT Analytics is the only IT Analytics platform to offer unified insights for all major storage, backup, and virtual infrastructures through a single plane of glass in both on-premises and multi-cloud environments.

Purpose of this document

The document covers the recommended component deployment configurations of the product like Portal, Database and Data Collector. This document also covers the various specific configurations required for the attributes of the product.

This document is a guidance document for IT Analytics administrators who wish to use IT Analytics in a certified and secure configuration.

The IT Analytics Certified Configuration Guide is a document intended for system administrators seeking information on the configurations of various attributes required for the product. The focus of this document is more technical in nature.

Software and hardware disclaimer

The supported vendor hardware and software versions in this *IT Analytics Certified Configuration Guide* (CCG) have been specifically qualified and approved by Cohesity. Hardware and software versions that do not appear on this list are not supported.

Chapter 2

Portal and database servers

This chapter includes the following topics:

Portal Supported Operating Systems

The Portal supports the following 64-bit platforms:

Table 2-1 Portal Supported Operating Systems

Operating Systems	Version
Red Hat Enterprise Linux	7, 8.6 (update 10), and 9
SUSE Linux Enterprise Server	■ SLES 12 SP3, SP4, SP5 ■ SLES15 SP4
Windows	2016, 2019, and 2022
OEL	7, 8, and 9

Recommended portal configurations

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

Table 2-2 Portal configuration on a virtual machine

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 GB of usable disk space (SAN or DAS, not NAS)	■ Capacity < 10 PB and ■ Backup < 10,000 clients

Table 2-3 Portal configuration on a physical server

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 GB 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 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 GB.

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

Supported Browsers and Display Resolution

Display Resolution: The minimum resolution for the Portal is 1920 x 1200 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 2-4 Supported Browsers

Browser	Apple Macintosh	Microsoft Windows	Linux
Microsoft Edge Version 133.0.3065.59 (Official build) (64-bit)	✓	✓	
Mozilla Firefox Version 91.3 and later (91.3 is the extended support version)	✓	✓	✓
Google Chrome Version 133.0.6943.98 (Official Build) (64-bit)	✓	✓	
Apple Safari 18.3	✓		

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 or Edge) 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.

Third-party and Open Source Products Used

When you install the portal and reporting database, you install a compilation of software, which includes open source and third-party software.

For a list of open source components and licenses, see the license.txt file on the portal server.

Table 2-5 Open Source Products Used

Software Product	Linux	Windows
Apache HTTP Web Server	2.4.66	2.4.66

Table 2-5 Open Source Products Used *(continued)*

Software Product	Linux	Windows
Apache Tomcat Java Servlet Engine	10.1.53	10.1.53
Java	Amazon Corretto 17.0.18.9.1	Amazon Corretto 17.0.18.9.1
Kafka	3.4.0.11	3.4.0.11
Oracle 19c	19c: 19.3.0.0.0	19c: 19.3.0.0.0

Note: If your environment has IT Analytics portal server and Data Collector installed on separate Linux servers and use Cohesity-provided Oracle, ensure the Oracle client RPM is installed or upgraded to 21.21.0.0.0-1.el8.x86_64.

If other versions of the above components are already running on the designated IT Analytics system, or other components are utilizing resources (such as specific ports) typically used by 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 3

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 3-1 Data Collector supported operating systems

Operating System	Version
Red Hat Enterprise Linux	7, 8.6 (update 10), and 9
SUSE Linux Enterprise	■ SLES 12 SP3, SP4, SP5 ■ SLES15 SP4
OEL	7, 8, and 9
Windows Server	2016, 2019, and 2022

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
- Number of NetBackup hosts enabled for File Analytics

Data Collector prerequisites

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

- 64-bit OS.
- When the IT Analytics system collects data from any vendor subsystem, the collection process expects name/value pairs to be in US English and requires the installation to be done by an Administrator with a US English locale. The server's language version can be non-US English.
- Supports Amazon Corretto 17. 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 IT Analytics Portal.
- 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 3-2 Components: Default Ports

Component	Default Ports
Apache Web Server	http 80 https 443
Jetty Server on Data Collector Server	443
Kafka	9092
Linux Hosts	SSH 22
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 3-2 Components: Default Ports *(continued)*

Component	Default Ports
ZooKeeper	2181 **Note:** IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the local host where IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

Table 3-3 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 4443
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	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

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

Storage Vendor	Default Ports and Notes
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
Hitachi Vantara All-Flash and Hybrid Flash Storage	Hitachi Ops Center Configuration Manager REST API: 23450 for HTTP and 23451 for HTTPS. HIAA : 22015 for HTTP, and 22016 for HTTPS
IBM Enterprise	TCP 1751, 1750, 1718 DSCLI
IBM SVC	SSPC w/CIMOM 5988, 5989
IBM XIV	XCLI TCP 7778
Microsoft Windows Server	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

Table 3-4 Data protection: Default ports

Data Protection Vendor	Default Ports and Notes
Cohesity DataProtect	REST API on Port 80 or 443

Table 3-4 Data protection: Default ports *(continued)*

Data Protection Vendor	Default Ports and Notes
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
HP Data Protector	5555 WMI ports SSH 22 (Linux)
IBM Spectrum Protect (TSM)	1500
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

Table 3-5 Network & Fabrics: Default Ports

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

Table 3-6 Virtualization Vendors: Default Ports

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

Table 3-7 Replication Vendors: Default Ports

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

Table 3-8 Cloud Vendors: Default Ports

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

Chapter 4

Capacity Manager configurations

This chapter includes the following topics:

Supported systems 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
- On Windows, administrator privileges for WMI.

Table 4-1 Data Collection Prerequisites

Vendor	Subsystems	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	PowerStore	REST API Version: 4.0.0.0 and 4.1.0.0	■ User with Admin privileges ■ Add access is read-only ■ Add each PowerStore appliance's IP / name to the Connector dialog box.	The default port number is 23451 for SSL communication and 23450 for non-ssl communications.	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Dell EMC	Unity	330/300F, 400/400F, 500/500F, 600/600F, 350F, 450F, 550F and 650F.	■ User credentials with "security administrator" role is required to connect to Dell EMC Unity storage array using REST API. ■ Array detail is default activated and execuete every day at 2:01.	REST API version 4.3.0 on Port 443 or 8443.	
EMC	Elastic Cloud Storage (ECS)	3.x	■ User must belong to Management Users with System Monitor privilege	REST API on Port 80 or 4443.	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
EMC	VNX (Block)	Naviseccli, Navicli, v7.30, 7.31, 7.32.	■ IP address/hostname ■ Customize: <ip address>:<port>	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`
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, 7.2, 7.6, 7.7, 7.10, 8.1.		Port 22 (SSH)	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
EMC	Isilon	PowerScale OneFS: 6.5, 7.0, 7.1, 7.1.1, 7.2, 8.0, 9.1.0.4, 9.5, and 9.9.	■ 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.
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, 9.2.4.3, and 10.1.0.1 (Storage systems: PowerMax 2000, 8000, and 9.1) ■ Unimax 10.1.0.1	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` to verify symcfg is installed. Unisphere 8.3 is used for Performance collection. Array detail is default activated.

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
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
Hitachi	Hitachi Content Platform (HCP)	■ versions 9.3, 9.4, and 9.6.xx.	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 4-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	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 Supported versions ■ 10.x ■ and 11.x ■ 14.6 and 14.9	■ 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 4-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Hitachi Vantara	All-Flash and Hybrid Flash Storage ■ Hitachi Virtual Storage Platform (VSP Gx00 models) G200, G350, G370, G400, G600, G700, G800, G900 ■ Hitachi Virtual Storage Platform (VSP Fx00 models) F350, F370, F400, F600, F700, F800, F900 ■ Hitachi Virtual Storage Platform 5000 Series (5200, 5200H, 5600, 5600H) ■ Hitachi Virtual Storage Platform E Series (E590, E590H, E790, E790H, E1090, E1090H) **Note:** VSP (R700), USP_V(R600), VSP E790 or older models before USP_V are **NOT** supported.	CM-REST 10.5.1 (REST API Version 1.23.0 and 1.36.1) CCI version : 01-53-03/XX or later.	For Array Details and HDT Probe : User with Storage Administrator (View Only) permissions is required to access Hitachi Ops Center Configuration Manager REST API Server. For HIAA Array Performance probe : Use the Admin username for accessing the Hitachi Infrastructure Analytics Advisor. CCI version : 01-53-03/XX or later.	For the Array Details probe: 23450 is used for HTTP and 23451 is used for HTTPS. For the HIAA Array Performance probe: 22015 is used for HTTP and 22016 is used for HTTPS.	REST API

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
HPE	3PAR	■ InForm 2.3.1, 3.1.1, 3.1.2, 3.2.2, 3.3.1, 3.3.2, 4.5.15, 4.5.21, and 9.5.15 ■ HPE Alletra 9000 ■ HPE GreenLake for Block	■ 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
	Primera	4.1 and 4.2			
	XP Models: XP7, XP8, and P9500	CM-REST 10.5.1 (REST API Version 1.23.0) CCI version : 01-53-03/XX or later.	For Array Details : User with Storage Administrator (View Only) permissions is required to access HPE XP Ops Center Configuration Manager REST API Server. For HIAA Array Performance probe : Use the Admin username for accessing the HPE XP Ops Center Analyzer for Storage (HIAA). CCI version : 01-53-03/XX or later.	For the Array Details probe: 23450 is used for HTTP and 23451 is used for HTTPS. For the HIAA Array Performance probe: 22015 is used for HTTP and 22016 is used for HTTPS.	REST API

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
HPE	Storeonce	Supported with StoreOnce appliance running software version 4.1.x and newer.It is not compatible with StoreOnce appliances running software versions 3.x or older.	■ Server name or IP address of the HPE storeonce management server ■ User name and password ■ Additionally, any management console Local User shall be able to collect the data from the StoreOnce subsystem	HTTPS Port 443	No installations required on the Data Collector server.
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.
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.

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
HPE	Nimble Storage	■ 5.0.7.1.0.0.607338.opt ■ REST API Reference Version 5.0.1.0 ■ HPE Alletra 6000 ■ HPE Alletra 5000	Storage System Addresses	5392	
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 40.	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 41.	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 4-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	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, FlashSystem 840/900, FlashSystem 7200	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 primary console (from which data will be collected). ■ Super User ID & pwd for CIMOM. Super User ID refers to the user ID of the SVC primary 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.
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	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
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	
IBM	Cloud Object Storage	v3.14.9.47, REST API	User credential with "Super User" role for IBM Cloud Object Storage.	443	
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	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
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 41.	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.
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.
NetApp	StorageGRID	Rest API	▪ IP address / hostname ▪ Grid Account credentials ▪ Tenant Account credentials	Default: 443	Rest API calls over HTTPS

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, 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	■
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

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Veritas	NetBackup 5xxx Appliances.	NetBackup Appliance 3.1.2, 3.2, 3.2.1, and 5.3.		1556	**Note:** Cohesity NetBackup Appliances version 5.3 and above supports MFA enabled data collection.
	Cohesity Flex Appliance models: ■ 5150 ■ 5250 ■ 5340 ■ 5350	Cohesity Flex Appliance versions 2.0, 2.1, 3.0, 3.1, 3.2, 4.0, 5.0, 6.1, and 6.2. **Note:** IT Analytics supports multi-factor authentication (MFA) integrated in Cohesity Flex Appliance version 4.0.	■ FQDN of the Flex appliance ■ Administrator user credentials	443	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
					The data collection supported for each Cohesity Flex Appliance version is as indicated below. ■ **Appliance Details** probe: 2.0, 2.1, 3.0, 3.1, 3.2, 4.0, 5.0, 6.1, and 6.2. ■ **Performance Statistics** probe: 2.0, 2.1, 3.0, 3.1, 3.2, 4.0, 5.0, 6.1, and 6.2. ■ **Storage Statistics** probe: 2.0, 2.1, 3.0, 3.1, 3.2, 4.0, 5.0, 6.1, and 6.2. ■ Data collection through service account using short-lived token: 5.0 onwards.

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Fujitsu	■ Eternus CS8000 ■ The following models of Eternus DX/AF are supported: ■ Dx600 S4, ■ AF50 S3, ■ AF250 S1, ■ Dx100 S4 ■ DX8700 S3	Fujitsu Eternus CLI	■ IP address/host name of the Fujitsu Eternus System. ■ User ID and password for the Fujitsu Eternus System ■ Model of the Eternus System.	■ ssh: 22	

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

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
NEC	HYDRAstor [support model] ■ Japan ■ iStorage HS3-50, HS3-50S ■ iStorage HS6-50A, HS6-50AS ■ iStorage HS8-50, HS8-50S ■ iStorage HS Lite ■ Except for Japan ■ NEC Storage HS6-50A, HS6-50AS ■ NEC Storage HS8-50, HS8-50S ■ NEC Storage HS Virtual Appliance (HSVA)	Rest API execution for supported version - V5.7.0 + P5.7.0-N002 and V5.7.1.	■ NEC Storage HS (HYDRAstor) Floating IP addresses or host names. ■ User ID and password for the HYDRAstor ■ System Administrator credentials	Default port: 5080	The user must be with the administrative role. In Array Performance probe, File-System capacity detail will be collected once a day.

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.

See the section called “Array/LUN performance notes” on page 43.

Table 4-2 Array Family

Array Family	Rd/Wrte IO/sec	Total IO/sec	Rd/WrteMB / sec	Rd/Wrte Cache Hits/sec	Rd/Wrte Respond(ms)	Total Respond(ms)
Dell Compellent	X	X	X	X	--	--
EMC VNX	X	Calc.	X	X	X	Calc.
EMC Symmetrix	X	X	X	X	--	--
EMC XtremIO	Calc.	Calc.	Calc.	--	X	X
HDS Tuning Manager	X	Calc.	X	X	X	X
HP 3PAR	X	X	X	X	X	X
IBM SVC	X	X	X	--	--	--
IBM XIV	X	X	X	X	X	X
NetApp ONTAP 7-Mode (Block only)	X	Calc.	X	--	--	Avg Latency
Pure Storage FlashArray	X	Calc.	X	--	X	Calc.

Array/LUN performance notes

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

Table 4-3 Array families supporting block storage LUN performance and port performance data collection.

Array Family	Notes
EMC VNX	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.

Table 4-3 Array families supporting block storage LUN performance and port performance data collection. *(continued)*

Array Family	Notes
EMC XtremIO	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.
HDS Tuning Manager	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.
NetApp ONTAP 7-Mode (Block only)	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.

Port performance metrics

Table 4-4 Matrics of post performance of arrays

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	Not Supported	Not Supported	Not Supported	Not Supported	
EMC Symmetrix	--	X	--	X	
EMC XtremIO	--	Calculated	--	Calculated	
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 array performance metrics

Isilon performance data is collected from SNMP MIB statistics. For example, collected data includes such metrics as cluster, node, protocols (CIFS, SMB, FTP, HTTP), and disk performance.

Isilon array performance statistics are captured for the following intervals:

- raw data, as collected
- hourly
- daily

The following metrics are collected for EMC Isilon arrays.

- See "EMC Isilon Array Performance" on page 45.
- See "EMC Isilon Disk Performance" on page 46.
- See "EMC Isilon Node Performance" on page 47.
- See "EMC Isilon OneFS Performance" on page 49.
- See "EMC Isilon Protocol Performance" on page 49.

EMC Isilon Array Performance

Table 4-5 EMC Isilon Array Performance

Metric	Description
Avg CPU %	Average CPU usage (percent) across the cluster at collection time.
Max Single CPU %	Single highest CPU usage (percent) in the cluster at collection time.
Avg Idle CPU %	Average CPU idle (percent) across the cluster at collection time.
Avg Interrupt CPU %	Average interrupt CPU usage (percent) across the cluster at collection time.
Avg Nice CPU %	Average nice CPU (CPU scheduling priority) usage (percent) across the cluster at collection time.
Avg System CPU %	Average system CPU usage (percent) across the cluster at collection time.
Avg User CPU %	Average user CPU usage (percent) across the cluster at collection time.

Table 4-5 EMC Isilon Array Performance *(continued)*

Metric	Description
Avg Disk Busy %	Average disk busy (percent) across the cluster at collection time.
Avg Disk Latency	Average disk latency (milliseconds) across the cluster at collection time.
Avg Disk Writes Rate	Disk rate: Average disk write performance (bytes/second) across the cluster at collection time.
Avg Disk Writes IOPS	Disk rate: Average disk write performance (IOPS) across the cluster at collection time
Avg Disk Reads Rate	Disk rate: Average disk read performance (bytes/second) across the cluster at collection time.
Disk Reads Rate IOPS	Disk rate: Average disk read performance (IOPS) across the cluster at collection time.
External Network Received	Total network rate (in bytes/second) for all external interfaces in the cluster at collection time.
External Network Transmit	Total network rate out (bytes/second) for all external interfaces in the cluster at collection time.
Internal Network Received	Total network rate (in bytes/second) for all internal interfaces in the cluster at collection time.
Internal Network Transmit	Total network rate out (bytes/second) for all internal interfaces in the cluster at collection time.
# Active Clients	Total number of clients actively transferring to/from the cluster at collection time.
# Connected Clients	Total number of clients connected to the cluster at collection time.

EMC Isilon Disk Performance

Table 4-6 EMC Isilon Disk Performance

Metric	Description
Interval Secs	Time interval, in seconds, for which the Isilon disk performance data was collected.
Disk Busy %	Disk busy (percent) at collection time.
Disk Latency	Disk latency (milliseconds) at collection time.

Table 4-6 EMC Isilon Disk Performance *(continued)*

Metric	Description
Disk Writes Rate	Disk rate: Disk write performance (bytes/second) at collection time.
Disk Reads Rate	Disk rate: Disk read performance (bytes/second) at collection time.
Interval Type	Interval type of the disk performance collection.
Drive Bay ID	Drive Bay ID, for internal use by the Portal database.
Node ID	Node ID, for internal use by the Portal database.
Storage System ID	Storage system ID, for internal use by the Portal database.
Log Date	Date and time the samples were collected.
Disk Writes IOPS	Disk rate: Disk write performance (IOPS) at collection time.
Disk Reads IOPS	Disk rate: Disk read performance (IOPS) at collection time.

EMC Isilon Node Performance

Table 4-7 EMC Isilon Node Performance

Metric	Description
Avg CPU %	Average CPU usage (percent) across the node at collection time.
Avg Disk Busy %	Average disk busy (percent) across the node at collection time.
Avg Disk Latency	Average disk latency (milliseconds) across the node at collection time.
Avg Disk Writes Rate	Disk rate: Average disk write performance (bytes/second) across the node at collection time.
Avg Disk Writes IOPS	Disk rate: Average disk write performance (IOPS) across the cluster at collection time.
Avg Disk Reads Rate	Disk rate: Average disk read performance (bytes/second) across the node at collection time.
Avg Disk Reads IOPS	Disk rate: Average disk read performance (IOPS) across the cluster at collection time.
Avg Idle CPU %	Average CPU idle (percent) across the node at collection time.
Avg Interrupt CPU %	Average interrupt CPU usage (percent) across the node at collection time.

Table 4-7 EMC Isilon Node Performance *(continued)*

Metric	Description
Avg Nice CPU %	Average nice CPU (CPU scheduling priority) usage (percent) across the node at collection time.
Avg System CPU %	Average system CPU usage (percent) across the node at collection time.
Avg User CPU %	Average user CPU usage (percent) across the node at collection time.
External Network Received	Total network rate (in bytes/second) for all external interfaces in the node at collection time.
External Network Transmit	Total network rate out (bytes/second) for all external interfaces in the node at collection time.
File System Data Written (KB)	Cumulative data (KiB) written to the OneFS file system on the node since node boot.
File System Data Read (KB)	Cumulative data (KiB) read from the OneFS file system on the node since node boot.
File System Write Transfer Rate IOPS	Transfer rate of writes to the OneFS file system on the node (IOPS) at collection time.
File System Read Transfer Rate IOPS	Transfer rate of reads from the OneFS file system on the node (IOPS) at collection time.
File System Write Transfer Rate	Transfer rate of writes to the OneFS file system on the node (bytes/second) at collection time.
File System Read Transfer Rate	Transfer rate of reads from the OneFS file system on the node (bytes/second) at collection time.
Internal Network Received	Total network rate (in bytes/second) for all internal interfaces in the node at collection time.
Internal Network Transmit	Total network rate out (bytes/second) for all internal interfaces in the node at collection time.
Max CPU %	Single highest CPU usage (percent) in the node at collection time.
Memory Cache	Memory used for cache (KiB) on the node at collection time.
Memory Free	Memory free (KiB) on the node at collection time.
Memory Used	Memory used (KiB) on the node at collection time.

Table 4-7 EMC Isilon Node Performance *(continued)*

Metric	Description
# Active Clients	Total number of clients actively transferring to/from the node at collection time.
# Connected Clients	Total number of clients connected to the node at collection time.
Total Disk Writes Rate	Disk rate: Total disk write performance (bytes/second) across the node at collection time.
Total Disk Writes IOPS	Disk rate: Total disk write performance (IOPS) across the cluster at collection time.
Total Disk Reads Rate	Disk rate: Total disk read performance (bytes/second) across the node at collection time.
Total Disk Reads IOPS	Disk rate: Total disk read performance (IOPS) across the cluster at collection time.

EMC Isilon OneFS Performance

Table 4-8 EMC Isilon OneFS Performance

Metric	Description
File System Data Written	Cumulative data (KiB) written to the OneFS file system.
File System Data Read	Cumulative data (KiB) read from the OneFS file system.
File System Write Transfer	Transfer rate of writes to the OneFS file system (bytes/second) at collection time.
File System Read Transfer	Transfer rate of reads from the OneFS file system (bytes/second) at collection time.

EMC Isilon Protocol Performance

Table 4-9 EMC Isilon Protocol Performance

Metric	Description
Avg Latency	The average latency in (milliseconds) for all operations for the protocol on this node.

Table 4-9 EMC Isilon Protocol Performance *(continued)*

Metric	Description
Avg Ops Input Size	The average input size (bytes) of all operations for the protocol on this node.
Avg Ops Output Size	The average output size (bytes) of all operations for the protocol on this node.
Interval Secs	Time interval, in seconds, for which the Isilon protocol performance data was collected.
Interval Type	Interval type of the protocol performance collection.
Max Latency	The maximum latency in (milliseconds) for all operations for the protocol on this node.
Max Ops Input Size	The largest input size (bytes) of all operations for the protocol on this node.
Max Ops Output Size	The largest output size (bytes) of all operations for the protocol on this node.
Min Latency	The minimum latency (milliseconds) for all operations for the protocol on this node.
Min Ops Input Size	The smallest input size (bytes) of all operations for the protocol on this node.
Min Ops Output Size	The smallest output size (bytes) of all operations for the protocol on this node.
# Active Clients	Number of clients actively transferring to/from the node via this protocol at collection time.
# Connected Clients	Number of clients connected to the node via this protocol at collection time.
Transfer Rate IOPS	Transfer rate (IOPS) for this protocol on this node at collection time.
Transfer Rate In	Transfer rate (in bytes/second) for this protocol on this node at collection time.
Transfer Rate Out	Transfer rate out (bytes/second) for this protocol on this node at collection time.

NetApp Cluster-Mode performance metrics

A large variety of NetApp Cluster-Mode performance data is collected. For example, collected data includes such metrics as system, protocols (CIFS and NFS), volume, LUN, and target port performance.

NetApp Cluster-Mode performance statistics are captured for the following intervals:

- raw data, as collected
- hourly
- daily

The following metrics are collected for NetApp Cluster-Mode systems.

- See "NetApp Cluster-Mode Aggregate Performance" on page 51.
- See "NetApp Cluster-Mode CIFS Performance" on page 53.
- See "NetApp Cluster-Mode Fiber Channel Protocol Logical Interface Performance" on page 56.
- See "NetApp Cluster-Mode LUN Performance" on page 56.
- See "NetApp Cluster-Mode NFS Performance" on page 57.
- See "NetApp Cluster-Mode Processor Node Performance" on page 59.
- See "NetApp Cluster-Mode RAID Performance" on page 60.
- See "NetApp Cluster-Mode SMB (Server Message Block) Performance" on page 60.
- See "NetApp Cluster-Mode System Performance" on page 62.
- See "NetApp Cluster-Mode Target Port Performance" on page 63.
- See "NetApp Cluster-Mode Volume Performance" on page 64.

NetApp Cluster-Mode Aggregate Performance

Table 4-10 EMC Cluster-Mode Aggregate Performance

Metric	Description
# Read Blocks	Number of blocks read per second during a consistency point (CP) count check on the aggregate.
# Read Blocks HDD	Number of blocks read per second during a consistency point (CP) count check on the aggregate hard disk drive (HDD) disks.

Table 4-10 EMC Cluster-Mode Aggregate Performance *(continued)*

Metric	Description
# Read Blocks SSD	Number of blocks read per second during a consistency point (CP) count check on the aggregate solid state drive (SSD) disks.
# Reads	Number of reads per second done during a consistency point (CP) count check to the aggregate.
# Reads HDD	Number of reads per second done during a consistency point (CP) count check to the aggregate hard disk drive (HDD) disks.
# Reads SSD	Number of reads per second done during a consistency point (CP) count check to the aggregate solid state drive (SSD) disks.
Total Transfers	Total number of transfers per second serviced by the aggregate.
Total Transfers HDD	Total number of transfers per second serviced by the aggregate hard disk drive (HDD) disks.
Total Transfers SSD	Total number of transfers per second serviced by the aggregate solid state drive (SSD) disks.
# User Read Blocks	Number of blocks read per second on the aggregate.
# User Read Blocks HDD	Number of blocks read per second on the aggregate hard disk drive (HDD) disks.
# User Read Blocks SSD	Number of blocks read per second on the aggregate solid state drive (SSD) disks.
# User Reads	Number of user reads per second to the aggregate.
# User Reads HDD	Number of user reads per second to the aggregate hard disk drive (HDD) disks.
# User Reads SSD	Number of user reads per second to the aggregate solid state drive (SSD) disks.
# User Write Blocks	Number of blocks written per second to the aggregate.
# User Write Blocks HDD	Number of blocks written per second to the aggregate hard disk drive (HDD) disks.
# User Write Blocks SSD	Number of blocks written per second to the aggregate solid state drive (SSD) disks.
# User Writes	Number of user writes per second to the aggregate.

Table 4-10 EMC Cluster-Mode Aggregate Performance *(continued)*

Metric	Description
# User Write HDD	Number of user writes per second to the aggregate hard disk drive (HDD) disks.
# User Write SSD	Number of user writes per second to the aggregate solid state drive (SSD) disks.

NetApp Cluster-Mode CIFS Performance

Table 4-11 NetApp Cluster-Mode CIFS Performance

Metric	Description
# Active Searches	Number of active searches over SMB and SMB2.
# Auth Rejected	Authentication refused after too many requests were made in rapid succession.
# Out Change Notification	Number of active change notifications over SMB and SMB2.
Avg CIFS Latency	Average latency for CIFS operations.
CIFS Latency Operations	Total observed CIFS operations to be used as a base counter for a CIFS average latency calculation.
CIFS IOPS	Total number of CIFS operations.
CIFS Read IOPS	Total number of CIFS read operations.
CIFS Write IOPS	Total number of CIFS write operations.
# CIFS Commands Outstanding	Number of SMB and SMB2 commands in process.
# CIFS Connected Shares	Number of SMB and SMB2 share connections.
# CIFS Connections	Number of connections.
# CIFS Connections Established	Number of established SMB and SMB2 sessions.
# Open Files	Number of open files over SMB and SMB2.

Table 4-11 NetApp Cluster-Mode CIFS Performance *(continued)*

Metric	Description
# Signed Sessions	Number of signed SMB and SMB2 session.

NetApp Cluster-Mode Disk Performance

Table 4-12 NetApp Cluster-Mode Disk Performance

Metric	Description
Disk Busy	Time base for the disk-busy calculation.
Consistency Point Read Blocks	Number of blocks transferred for consistency point read operations per second.
Consistency Point Read Blocks Avg	Average number of blocks transferred in each consistency point (CP) read operation during a CP check.
Consistency Point Latency	Average latency per block in microseconds for consistency point read operations.
Consistency Point Read	Number of disk read operations initiated each second for consistency point processing.
Disk Busy %	Percentage of time there was at least one outstanding request to the disk.
Disk Capacity	Disk capacity. Values are stored as KiB in the database and rendered according to your user profile preferences.
Guaranteed Read Blocks	Number of blocks transferred for guaranteed read operations per second.
Guaranteed Read Blocks Avg	Average number of blocks transferred in each guaranteed read operation.
Guaranteed Read Latency	Average latency per block in microseconds for guaranteed read operations.
Guaranteed Read	Number of disk read operations initiated each second for RAID reconstruct or scrubbing activities.
Guaranteed Write Blocks	Number of blocks transferred for guaranteed write operations per second.
Guaranteed Write Blocks Avg	Average number of blocks transferred in each guaranteed write operation.

Table 4-12 NetApp Cluster-Mode Disk Performance *(continued)*

Metric	Description
Guaranteed Write Latency	Average latency per block in microseconds for guaranteed write operations.
Guaranteed Write	Number of write read operations initiated each second for RAID reconstruct or scrubbing activities.
Blocks Skipped IOPS	Number of blocks skipped in skip-mask write operations per second.
# Disk IOPS	Total number of disk operations per second involving initiated data transfer.
User Read Blocks	Number of blocks transferred per second for user read operations.
User Read Blocks Avg	Average number of blocks transferred in each user read operation.
User Read Latency	Average latency per block in microseconds for user read operations.
User Read	Number of disk read operations initiated each second for retrieving data or metadata associated with user requests.
User Skip Writes	Number of disk skip-write operations initiated each second for storing data or metadata associated with user requests.
User Write Blocks	Number of blocks transferred per second for user write operations.
User Write Blocks Avg	Average number of blocks transferred in each user write operation.
User Write Latency	Average latency per block in microseconds for user write operations.
User Write	Number of disk write operations initiated each second for storing data or metadata associated with user requests.
User Skip Mask Write	Number of disk write IOs that were executed as part of a skip-mask write.

NetApp Cluster-Mode Fiber Channel Protocol Logical Interface Performance

Table 4-13 NetApp Cluster-Mode Fiber Channel Protocol Logical Interface Performance

Metric	Description
Avg Total Latency	Average latency for fibre channel protocol (FCP) operations.
Avg Other Latency	Average latency for operations other than read and write.
Array Port ID	Name of the port.
Avg Read Latency	Average latency for read operations.
Avg Write Latency	Average latency for write operations.
Other IOPS	Number of operations that are not read or write.
Read Rate	Read rate in bits per second.
Read IOPS	Number of read operations.
Total IOPS	Total number of operations.
Write Rate	Write rate in bits per second.
Write IOPS	Number of write operations.

NetApp Cluster-Mode LUN Performance

Table 4-14 NetApp Cluster-Mode LUN Performance

Metric	Description
Avg Total Latency	Average latency in milliseconds for all operations on the LUN.
Avg Other Latency	Average other operations latency in milliseconds for all operations on the LUN.
Avg Read Latency	Average read latency in milliseconds for all operations on the LUN.
Avg Write Latency	Average write latency in milliseconds for all operations on the LUN.
Other IOPS	Number of other operations.
Queue Full Responses	Queue full responses.

Table 4-14 NetApp Cluster-Mode LUN Performance *(continued)*

Metric	Description
Read Rate	Read rate in bits per second.
Read IOPS	Number of read operations.
Total IOPS	Total number of operations on the LUN.
Write Rate	Write rate in bits per second.
Write IOPS	Number of write operations.

NetApp Cluster-Mode NFS Performance

Table 4-15 NetApp Cluster-Mode NFS Performance

Metric	Description
NFSv3 IOPS	Total number of NFSv3 procedure requests per second.
NFSv4 IOPS	Total number of NFSv4 procedures per second.
NFSv41 IOPS	Total number of NFSv4.1 operations per second.
Avg Read Latency	Average latency of read procedure requests.
Avg Read Dir Latency	Average latency of read directory procedure requests.
# Read Dir Errors	Number of erroneous read directory procedure requests.
Read Dir %	Percentage of read directory procedure requests.
Avg Read Dir Plus Latency	Average latency of read directory plus procedure requests.
# Read Dir Plus Errors	Number of erroneous read directory plus procedure requests.
Read Dir Plus %	Percentage of read directory plus procedure requests.
# Read Dir Plus Post-op Errors	Number of failed post-op read directory plus procedures.
# Read Dir Plus Success	Number of successful read directory plus procedure requests.

Table 4-15 NetApp Cluster-Mode NFS Performance *(continued)*

Metric	Description
Read Dir Plus Total	Total number of read directory plus procedure requests.
# Read Dir Post-op Errors	Number of failed post-op read directory procedures.
# Read Dir Success	Number of successful read directory plus procedure requests.
Read Dir Total	Total number of read directory plus procedure requests. Counter for NFSv3.
# Read Errors	Number of erroneous read procedure requests.
Avg NFSv4.1 Read Link Latency	Average latency of NFSv4.1 Read Link operations.
# NFSv4.1 Read Link	The number of failed NFSv4.1 Read Link operations.
NFSv4.1 Read Link %	Percentage of NFSv4.1 Read Link operations.
# NFSv4.1 Read Link Success	The number of successful NFSv4.1 Read Link operations.
# NFSv4.1 Read Link Total	Total number of NFSv4.1 Read Link operations.
Read %	Percentage of read procedure requests.
# Read Success	Number of successful read procedure requests.
Avg Read Sym Link Latency	Average latency of Read Sym Link procedure requests.
# Read Sym Link Errors	Number of erroneous Read Sym Link procedure requests.
Read Sym Link %	Percentage of Read Sym Link procedure requests for NFSv3.
# Sym Link Success	Number of successful Read Sym Link procedure requests.
# Sym Link Total	Total number of Read Sym Link procedure requests.
# Read Total	Total number read of procedure requests.

Table 4-15 NetApp Cluster-Mode NFS Performance *(continued)*

Metric	Description
Avg Write Latency	Average latency of write procedure requests.
# Write Errors	Number of erroneous write procedure requests.
Write %	Percentage of write procedure requests.
# Write Success	Number of successful write procedure requests.
# Write Total	Total number of write procedure requests.

NetApp Cluster-Mode Processor Node Performance

Table 4-16 NetApp Cluster-Mode Processor Node Performance

Metric	Description
Process Busy %	Percentage of elapsed time that the processor is executing non-idle processes.
Processor Elapsed Time	Wall-clock time since boot used for calculating processor utilization.
SK Switches	Number of sk switches per second.

NetApp Cluster-Mode Processor Performance

Table 4-17 NetApp Cluster-Mode Processor Performance

Metric	Description
Processor Busy %	Percentage of elapsed time that the processor is executing non-idle processes.
Processor Elapsed Time	Wall-clock time since boot used for calculating processor utilization.
SK Switches	Number of sk switches per second.

NetApp Cluster-Mode RAID Performance

Table 4-18 NetApp Cluster-Mode RAID Performance

Metric	Description
Blocks Read	Blocks read per second.
Blocks Write	Blocks written per second.
Full Stripes Write	Full stripes written per second.
Partial Stripes Write	Partial stripes written per second.
Avg RAID Latency	Average latency for all reads operations sent by Write Anywhere File Layout (WAFL) to RAID in microseconds.
RAID Read IOPS	Read operations per second issued by Write Anywhere File Layout (WAFL) to RAID.
RAID Read IOPS	Number of tetrises sent to RAID per second.
AvgTetris Latency	Average latency for tetris as seen by Write Anywhere File Layout (WAFL) in microseconds.
Stripes Write	Stripes written per second.
Tetris Write	Tetrises written per second.

NetApp Cluster-Mode SMB (Server Message Block) Performance

Table 4-19 NetApp Cluster-Mode SMB (Server Message Block) Performance

Metric	Description
# Active Searches	Number of active searches over SMB1/SMB2.
# SMB Commands Outstanding	Number of SMB1/SMB2 commands in process.
# SMB Connect Shares	Number of SMB1/SMB2 share connections.
# SMB Connect Established	Number of established SMB1/SMB3 sessions.
Avg SMB Latency	Average latency for SMB1/SMB2 operations.

Table 4-19 NetApp Cluster-Mode SMB (Server Message Block) Performance *(continued)*

Metric	Description
# Observed SMB Total	Total observed SMB1/SMB2 operations to be used as a base counter for SMB average latency calculation.
Max # of Open Files	Maximum number of open files over SMB2 achieved.
# SMB Total	Number of SMB1/SMB2 operations.
Avg SMB1 COM READ ANDX Latency	Average latency for SMB1_COM_READ_ANDX operations.
# SMB1 COM READ ANDX	Number of SMB1_COM_READ_ANDX operations used as a base for latency calculations.
Avg Read Class Latency	Average latency for SMB1/SMB2 read class operations.
# SMB Read Class	Total number of SMB1/SMB2 read class operations.
Avg Read Latency	Average latency for SMB1_COM_READ/SMB2_COM_READ operations.
# Read Latency	Number of SMB1_COM_READ/SMB2_COM_READ operations used as a base for latency calculations.
Avg SMB1_COM_WRITE_ANDX Latency	Average latency for SMB1_COM_WRITE_ANDX operations.
# SMB1 COM WRITE ANDX	Number of SMB1_COM_WRITE_ANDX operations used as a base for latency calculations.
# SMB Write Class	Total number of SMB1/SMB2 write class operations.
Avg Write Latency	Average latency for SMB1_COM_WRITE /SMB2_COM_WRITE operations.
# Write Latency	Number of SMB1_COM_WRITE/SMB2_COM_WRITE operations used as a base for latency calculations.
SMB Type	Possible values: SMB1 or SMB2.

NetApp Cluster-Mode System Performance

Table 4-20 NetApp Cluster-Mode System Performance

Metric	Description
Avg Processor Busy %	Average processor utilization across all processors in the system.
CIFS IOPS	CIFS operations per second.
CPU Busy %	System CPU resource utilization.
CPU Elapsed Time	Elapsed time since boot.
CPU Elapsed Time1	Elapsed time since boot.
CPU Elapsed Time2	Elapsed time since boot.
Disk Read	Disk read rate in Kbps.
Disk Write	Disk write rate in Kbps.
FCP Data Received	Fibre Channel Protocol (FCP) data received rate in Kbps.
FCP Data Sent	Fibre Channel Protocol (FCP) data sent rate in Kbps.
FCP IOPS	Fibre Channel Protocol (FCP) operations per second.
HDD Disk Read	Hard disk drive (HDD) read rate in Kbps.
HDD Disk Write	Hard disk drive (HDD) write rate in Kbps.
HTTP IOPS	HTTP operations per second.
iSCSI IOPS	iSCSI operations per second.
Network Data Received	Network data received rate in Kbps.
Network Data Sent	Network data sent rate in Kbps.
NFS IOPS	NFS operations per second.
# Processors	Number of active processors in the system.
Read IOPS	Read operations per second.
SSD Disk Read	Solid state drive (SSD) disks read rate in Kbps.

Table 4-20 NetApp Cluster-Mode System Performance *(continued)*

Metric	Description
SSD Disk Write	Solid state drive (SSD) disks write rate in Kbps.
System Avg Latency	Average latency for all operations in the system in milliseconds.
System Read Latency	Average latency for all read operations in the system in milliseconds.
System Write Latency	Average latency for all write operations in the system in milliseconds.
Total IOPS	Total operations per second.
Total Processor Busy %	Total processor utilization of all processors in the system.
Write IOPS	Write operations per second.

NetApp Cluster-Mode Target Port Performance

Table 4-21 NetApp Cluster-Mode Target Port Performance

Metric	Description
Busy %	Percentage of time that there are commands outstanding on the indicated array target port from this controller.
Read KBPS	The average read throughput in K bytes per second read by this controller from the indicated array target port.
Read OPS	The number of I/O read operations per second performed by this controller on the indicated.
Read Latency	The average latency for I/O read operations performed by this controller on the indicated array target port.
Total Rate	The average total throughput in K bytes per second read or written by this controller to or from the indicated array target port.
Total IOPS	The total number of I/O read and write operations per second performed by this controller on the indicated array target port.
Total Latency	The average latency for I/O operations performed by this controller on the indicated array target port.
Disk Busy	Time base for the disk-busy calculation.

Table 4-21 NetApp Cluster-Mode Target Port Performance *(continued)*

Metric	Description
Waiting %	Percentage of time that there are commands queued waiting to be sent to the indicated array target port from this controller.
Write Rate	The average write throughput in K bytes per second written by this controller to the indicated array target port.
Write IOPS	The number of I/O write operations per second performed by this controller on the indicated array target port.
Write Latency	The average latency for I/O write operations performed by this controller on the indicated array target port.

NetApp Cluster-Mode Volume Performance

Table 4-22 NetApp Cluster-Mode Volume Performance

Metric	Description
Avg Latency	Average latency in microseconds for the WAFL (Write Anywhere File Layout) file system to process all the operations on the volume; not including request processing or network communication time.
Avg Other Latency	Average latency in microseconds for the WAFL (Write Anywhere File Layout) file system to process other operations to the volume; does not include request processing or network communication time.
Other IOPS	Number of other operations per second to the volume.
Read Rate	Bytes read per second from the volume.
Read Latency	Average latency in microseconds for the WAFL (Write Anywhere File Layout) file system to process read requests.
Read IOPS	Number of reads per second to the volume
Total IOPS	Number of operations per second serviced by the volume.
Write Rate	Bytes written per second to the volume.
Write Latency	Average latency in microseconds for the WAFL (Write Anywhere File Layout) file system to process write request to the volume; not including request processing or network communication time.
Write IOPS	Number of writes per second to the volume.

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. The metrics can be accessed in the Dynamic Template Designer and the SQL Template Designer to generate report templates.

- Unisphere records performance metrics in 5-minute intervals and this interval is not configurable. IT Analytics reporting assumes that this is a fixed interval.
- The IT Analytics Data Collector captures EMC Symmetrix performance metrics every 15 minutes, by default. This interval is configurable. Whatever interval length is used (15-minute default or customer-specified), IT Analytics captures and exposes whatever 5-minute intervals were exposed by Unisphere since the last successful completion (maximum last 8 hours). On the first successful data collection, IT Analytics captures and exposes 8 hours of historical 5-minute intervals.
- IT Analytics reports typically group the 5-minute intervals into broader time intervals, such as hours, days, or weeks. In these cases, reports display Symmetrix performance values (I/Os, MBps, and Latency) as an average, calculated from the 5-minute interval records that are provided by Unisphere.

The following additional EMC Symmetrix performance metrics are collected from the Unisphere API:

- See "EMC Symmetrix Array Performance" on page 66.
- See "EMC Symmetrix Backend Director Performance" on page 67.
- See "EMC Symmetrix Front-end Port Performance" on page 68.
- See "EMC Symmetrix Storage Group Performance" on page 68.
- See "EMC Symmetrix Database Performance" on page 69.
- See "EMC Symmetrix Disk Group Performance" on page 69.
- See "EMC Symmetrix Disk Performance" on page 70.
- See "EMC Symmetrix Device Groups Performance" on page 71.
- See "EMC Symmetrix Disk by Technology Performance" on page 71.
- See "EMC Symmetrix Storage Tier Performance" on page 72.
- See "EMC Symmetrix Thin Tier Performance" on page 73.
- See "EMC Symmetrix Thin Pool Performance" on page 73.

Create enhanced EMC Symmetrix Performance report templates

These enhanced EMC Symmetrix performance metrics are retrieved by a Data Collector that was developed using the IT Analytics SDK. The metrics can be accessed in the Dynamic Template Designer and the SQL Template Designer to generate report templates.

- The database views that support these additional metrics have an SDK prefix for the database view names. For example, in the Dynamic Template Designer, you will see **SDK_ESYM_THIN_TIER_PERF**. In the SQL Template Designer, you will see **sdk_v_esym_thin_tier_perf**.
- When developing a report template in the Dynamic Template Designer, select a Product of EMC Symmetrix and search fields for SDKto list fields that are relevant for reporting performance metrics.

EMC Symmetrix Array Performance

Table 4-23 EMC Symmetrix Array Performance

Metric	Description
Host IOs	The number of host I/O operations per second by all Symmetrix volumes. This includes random and sequential reads, and writes to the volume.
Host MBs	The total requests per second (from all front-end directors) that were satisfied from cache.
Host MBs Read	The number of MB per second read by all Symmetrix volumes.
Host MBs Written	The number of MB per second written by all Symmetrix volumes.
BE Reqs	The number of a read or write data transfers between cache and the back-end director.
WP Count	The number of system cache slots that are write-pending.
Percent Cache WP	The % of system cache that is write-pending.
Avg Fall Thru Time	The average time it takes a cache slot in LRU0 to be freed up. This value represents the average time from the first use of the contents to its reuse by another address.

EMC Symmetrix Backend Director Performance

Table 4-24 EMC Symmetrix Backend Director Performance

Metric	Description
Percent Busy	The % of time that the director is busy.
IOs	The number of I/O commands accessing the disk.
Reqs	The number of read/write requests between the cache and the director.
MBs Read	The read transfers per second, in MB.
MBs Written	The write transfers per second, in MB.
Percent Non IO Busy	The total % of time that the directory is busy serving non-I/O requests.

EMC Symmetrix Frontend Director Performance

Table 4-25 EMC Symmetrix Frontend Director Performance

Metric	Description
Percent Busy	The % of time that the director is busy.
Host IOs	The number of host I/O operations per second for director data transfers.
Host MBs	The size of the data transfer from the host in MB per second.
Reqs	The data transfer read/write requests between the director and the cache. An I/O may require multiple requests depending on I/O size, alignment, or both. The requests rate should be either equal to or greater than the I/O rate.
Read Response Time	A calculated average response time for reads.
Write Response Time	A calculated average response time for writes.

EMC Symmetrix Front-end Port Performance

Table 4-26 EMC Symmetrix Front-end Port Performance

Metric	Description
IOs	The number of I/O commands accessing the disk.
MBs	The total read and write I/Os per second in MBs.
Speed GBs	The gigabits per second through the port.
Percent Busy	The % of time the port is busy

EMC Symmetrix Storage Group Performance

Table 4-27 EMC Symmetrix Storage Group Performance

Metric	Description
Host MBs	Cumulative number of host MB per second reads/writes for the storage group.
Host MB Reads	Cumulative number of host MB per second reads by the storage group.
Host MB Written	Cumulative number of host MB per second written by the storage group.
Read Response Time	The average time taken by the Symmetrix array to serve one read I/O for this group.
Write Response Time	The average time taken by the Symmetrix array to serve one write I/O for this group.
Read Miss Response Time	The average time taken by the Symmetrix array to serve one read miss I/O (not found in cache) for this group.
Write Miss Response Time	The average time taken by the Symmetrix array to serve one write miss I/O (not found in cache) for this group.
Percent Hit	The % of I/O operations that were satisfied immediately from cache.
Allocated Capacity	The capacity of the storage group, in GB.

EMC Symmetrix Database Performance

Table 4-28 EMC Symmetrix Database Performance

Metric	Description
Host IOs	The number of host operations performed each second by the group.
Host Reads	The number of host read operations performed each second by the group.
Host Writes	The number of host write operations performed each second by the group.
Read Response Time	The average time taken by the Symmetrix array to serve one read I/O for this group.
Write Response Time	The average time taken by the Symmetrix array to serve one write I/O for this group.
Percent Hit	The % of I/O operations that were satisfied immediately from cache.
Response Time	The average response time for the reads and writes.
Allocated Capacity	The capacity of the storage group, in GB.

EMC Symmetrix Disk Group Performance

Table 4-29 EMC Symmetrix Disk Group Performance

Metric	Description
Percent Busy	The % of time that the disk group is busy serving I/O requests.
Total SCSI Commands	The total number of commands performed by the disk group each second: read, write, skip mask, verify, XOR write, and XOR write-read.
Disk Reads	The number of reads per second for the disk group.
Disk Writes	The number of writes per second for the disk group.
MB Read	The read throughput of the disk group, in MB per second.
MB Written	The write throughput of the disk group, in MB per second.
Read Response Time	The average time taken by the disk group to serve one read command.
Write Response Time	The average time taken by the disk group to serve one write command.

Table 4-29 EMC Symmetrix Disk Group Performance *(continued)*

Metric	Description
MBs	The total number of MB per second for the disk group.
IOs	The total number of read and write I/Os per second for the disk group.
Total Capacity	Total capacity of all the disks in the disk group.
Used Capacity	Total capacity allocated from all the disks in the disk group.

EMC Symmetrix Disk Performance

Table 4-30 EMC Symmetrix Disk Performance

Metric	Description
Percent Busy	The % of time that the disk group is busy serving I/O requests.
Avg Queue Depth	Calculated value: Accumulated queue depth/total SCSI commands per second.
Total SCSI Commands	Total number of commands performed by the disk each second: read, write, skip mask, verify, XOR write, and XOR write-read.
Disk Reads	The number of reads per second for the disk.
Disk Writes	The number of writes per second for the disk.
MB Read	The read throughput of the disk, in MB per second.
MB Written	The write throughput of the disk, in MB per second.
Read Response Time	The average time taken by the disk to serve one read command.
Write Response Time	The average time taken by the disk to serve one write command.
IOs	The total number of read and write I/Os per second for the disk.

EMC Symmetrix Device Groups Performance

Table 4-31 EMC Symmetrix Device Groups Performance

Metric	Description
Host Reads	The number of host read operations performed each second by the group.
Host Writes	The number of host write operations performed each second by the group.
Host Read Hits	The number of host read operations performed each second by the group that were immediately satisfied from cache.
Host Write Hits	The number of host write operations performed each second by the group that were immediately satisfied from cache.
Host Read Misses	The number of host read operations performed each second by the group that were not satisfied from cache.
Host Write Misses	The number of host write operations performed each second by the group that were not satisfied from cache.
Host MB Reads	The cumulative number of host reads by the group, in MB per second.
Host MB Written	The cumulative number of host writes by the group, in MB per second.
Read Response Time	The average time taken by the Symmetrix array to serve one read I/O operation for this group.
Write Response Time	The average time taken by the Symmetrix array to serve one write I/O operation for this group.
WP Count	The number of tracks that are write-pending for the group.

EMC Symmetrix Disk by Technology Performance

Table 4-32 EMC Symmetrix Disk by Technology Performance

Metric	Description
Read Response Time	The average time taken by the disk to serve one read I/O operation.
Write Response Time	The average time taken by the disk to serve one write I/O operation.
Percent Busy	The % of time that the disk is busy serving I/O requests.

Table 4-32 EMC Symmetrix Disk by Technology Performance *(continued)*

Metric	Description
Total Capacity	The total capacity of the disk, in GB.
Total SCSI Commands	The total number of commands performed by the disk each second: read, write, skip mask, verify, XOR write, and XOR write-read.
Used Capacity	Total used capacity of the disk, in GB.
Reads	The number of disk reads.
Writes	The number of disk writes.

EMC Symmetrix Storage Tier Performance

Table 4-33 EMC Symmetrix Storage Tier Performance

Metric	Description
Percent Disk Busy	The % of time that the disk is busy serving I/O requests.
Total SCSI Commands	The total number of commands performed by the disk group each second: read, write, skip mask, verify, XOR write, and XOR write-read.
Host Reads	The number of host reads performed each second by the disk.
Host Writes	The number of host writes performed each second by the disk.
MB Read	The read throughput of the disk, in MB per second.
MB Written	The write throughput of the disk, in MB per second.
Read Response Time	The average time taken by the disk to serve one read I/O operation .
Write Response Time	The average time taken by the disk to serve one write I/O operation .
Total Disk Capacity	Total capacity of the disk, in GB.
Used Disk Capacity	Total used capacity of the disk, in GB.

EMC Symmetrix Thin Tier Performance

Table 4-34 EMC Symmetrix Tier Performance

Metric	Description
Host Reads	The average time it took the disk to serve one read command.
Host Writes	The average time it took the disk to serve one write command.
Host Hits	The number of host read/write operations performed each second by the group that were immediately satisfied from cache.
Host MBs	Cumulative number of host read/writes per second by the group, in MB per second.
Read Response Time	The average time taken by the array to serve one read I/O operation.
Write Response Time	The average time taken by the array to serve one write I/O operation.
Total Pool Capacity	Total physical capacity of the pool of storage. This is derived from the sum of capacities of data devices (enabled or disabled) in the pool.
Enabled Pool Capacity	The some of all the enabled data devices in the pool.
Used Pool Capacity	The amount of capacity that has been used from the bound pool.
Allocated Pool Capacity	From the enabled capacity, this is the amount of capacity that is bound to thin devices.

EMC Symmetrix Thin Pool Performance

Table 4-35 EMC Symmetrix Thin Pool Performance

Metric	Description
Host Reads	The average time it took the disk to serve one read command.
Host Writes	The average time it took the disk to serve one write command.
Host Hits	The number of host read/write operations performed each second by the group that were immediately satisfied from cache.
Host MBs	Cumulative number of host read/writes per second by the group, in MB per second.

Table 4-35 EMC Symmetrix Thin Pool Performance *(continued)*

Metric	Description
Read Response Time	The average time taken by the array to serve one read I/O operation.
Write Response Time	The average time taken by the array to serve one write I/O operation
Total Pool Capacity	Total physical capacity of the pool of storage. This is derived from the sum of capacities of data devices (enabled or disabled) in the pool.
Enabled Pool Capacity	The some of all the enabled data devices in the pool.
Used Pool Capacity	The amount of capacity that has been used from the bound pool.
Allocated Pool Capacity	From the enabled capacity, this is the amount of capacity that is bound to thin devices.

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. The metrics can be accessed in the Dynamic Template Designer and the SQL Template Designer to generate report templates.

- Unisphere records performance metrics in 5-minute intervals and this interval is not configurable. IT Analytics reporting assumes that this is a fixed interval.
- The IT Analytics Data Collector captures EMC Symmetrix performance metrics every 15 minutes, by default. This interval is configurable. Whatever interval length is used (15-minute default or customer-specified), IT Analytics captures and exposes whatever 5-minute intervals were exposed by Unisphere since the last successful completion (maximum last 8 hours). On the first successful data collection, IT Analytics captures and exposes 8 hours of historical 5-minute intervals.
- IT Analytics reports typically group the 5-minute intervals into broader time intervals, such as hours, days, or weeks. In these cases, reports display Symmetrix performance values (I/Os, MBps, and Latency) as an average, calculated from the 5-minute interval records that are provided by Unisphere.

The following additional EMC Symmetrix performance metrics are collected from the Unisphere API:

- See "EMC Symmetrix Array Performance" on page 66.
- See "EMC Symmetrix Backend Director Performance" on page 67.
- See "EMC Symmetrix Front-end Port Performance" on page 68.
- See "EMC Symmetrix Storage Group Performance" on page 68.
- See "EMC Symmetrix Database Performance" on page 69.
- See "EMC Symmetrix Disk Group Performance" on page 69.
- See "EMC Symmetrix Disk Performance" on page 70.
- See "EMC Symmetrix Device Groups Performance" on page 71.
- See "EMC Symmetrix Disk by Technology Performance" on page 71.
- See "EMC Symmetrix Storage Tier Performance" on page 72.
- See "EMC Symmetrix Thin Tier Performance" on page 73.
- See "EMC Symmetrix Thin Pool Performance" on page 73.

Hitachi Vantara array performance metrics

The REST API collects the following additional data points from the Hitachi Arrays. Even though the data from these data points is currently not persisted in any of the reports, they can be used in the custom RTDs. These data points are collected for all Hitachi Arrays probed using the Hitachi Ops Center Configuration Manager REST APIs.

Table 4-36 Additional data points collected

Field	Description
Total Efficiency Ratio	The ratio of the total saving effect achieved by accelerated compression, capacity saving (compression and deduplication).
Data Reduction Ratio	The data reduction ratio before and after performing the accelerated compression function and the capacity saving function (compression and deduplication).
Provisioning Efficiency %	The efficiency ration achieved by Dynamic Provisioning.
Software Saving Ratio	The capacity reduction ratio of the data which is before and after performing the capacity saving function.

Table 4-36 Additional data points collected *(continued)*

Field	Description
Software Compression Ratio	The capacity compression ratio of the data which is before and after performing the capacity saving function.
Software Deduplication Ratio	The capacity deduplication ratio for the data which is before and after performing the capacity saving function.
Software Pattern Matching Ratio	The capacity reduction ratio for data before and after performing pattern matching of the capacity saving function.
FMD Pattern Matching Ratio	The capacity reduction ratio for data which is before and after performing pattern matching of the accelerated compression.
FMD Saving Ratio	The capacity reduction ratio for data which is before and after performing the accelerated compression function.
FMD Compression Ratio	The capacity compression ratio for data which is before and after performing the accelerated compression function.
Calculation Start Time	The start date and time for the calculation. The time based on the system date and time.
Calculation End Time	The end date and time for the calculation. The time based on the system date and time.

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 77.

See "WMI proxy requirements for Windows host Data Collection" on page 77.

See "Host resources supported configurations" on page 78.

See "Supported host bus adapters (HBAs)" on page 82.

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 4-37 Table 3.1 Host Resources Prerequisites by Operating System

Host OS	Host Access Requirements	Port Requirements	Notes
Linux RH Linux SUSE CentOS AIX	ssh 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	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 4-38 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 4-39 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 4-39 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	■ RedHat Linux Enterprise Server, CentOS, SUSE ■ Solaris ■ Windows Server ■ IBM AIX		In general, these operating systems up to and including the latest OS patch level are supported.

Table 4-39 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, Windows) ■ Solaris Volume Manager ■ Linux Logical Volume Manager ■ AIX 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

Pure Storage Flash Array performance metrics

In addition to LUN performance metrics that can be collected from Pure Storage Flash Arrays, data collection gathers the following performance metrics by accessing storage devices via a REST API.

Table 4-40 Pure Array Performance

Metric	Description
Write Rate	The write transfer rate (MiB/s written).
Read Rate	The read transfer rate (MiB/s read).
Queue Depth	The average number of queued I/O requests.
Read IOPS	Number of read requests processed per second by the array (updated every 30 seconds).
Write IOPS	Number of write requests processed per second by the array (updated every 30 seconds).
Read Latency	Average latency in microseconds for processing read requests (updated every 30 seconds).
Write Latency	Average latency in microseconds for processing write requests (updated every 30 seconds).
Last Updated	Time at which Pure array performance data was collected.

Supported host bus adapters (HBAs)

Table 4-41 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	HBA information is obtained using OS commands. No product-specific commands are used; therefore, Capacity Manager supports all HBAs supported by these operating systems.	None.
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 5

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
- On Windows, administrator privileges for WMI.

Table 5-1 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		https 443 for read-only access to the data	AWS reports are under Capacity Manager and Virtualization Manager.

Table 5-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
			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 and provide the mandatory privileges. **Note:** For mandatory privileges, see *IT Analytics Data Collector Installation Guide for the Cloud >> Pre-Installation Setup for Amazon*		

Table 5-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
			Web Services (AWS) >> Mandatory probe user privileges section. **5** Generate Access Keys. **6** Link AWS Accounts for Collection of Consolidated Billing Data.		

Table 5-1 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. **Note:** A maximum of 105 subscriptions can be selected in a policy.

Table 5-1 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, 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	

Table 5-1 Data Collection Prerequisites *(continued)*

Vendor	Subsystems	Dev Mgr/API/CLI	Access Requirements	Ports	Notes
Google cloud platform	■ Virtual Machine Details - Secure and customizable compute service that lets you create and run virtual machines on Google's infrastructure. ■ Storage Buckets (Details and Usage) - Cloud Storage is a service for storing your objects in Google Cloud. ■ Billing Records - Usage and corresponding charges, by service.	REST API	**1** Create a billing data access role . **2** Create an IAM service account user and create key. **3** Enable billing account access. **4** Enable billing export. **5** Enable the cloud API's. **6** Grant access of each project to the service account.	443	Data collector policy requires service account email and private key.

Chapter 6

Virtualization Manager configurations

This chapter includes the following topics:

Supported versions

Note: Refer to the *Software and hardware disclaimer* supported and tested by Cohesity.

See "Software and hardware disclaimer" on page 8.

- VMware
  - ESX or ESXi Servers 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, and 8.0.
  - Virtual Center (vCenter) Server 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, and 8.0.
- 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.
- VMware vSAN
  - vSAN 7.0 Update 2.

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 7

File Analytics configurations

This chapter includes the following topics:

Data Collector probes by storage type

Note: Refer to the *software and hardware disclaimer* supported and tested by Cohesity.

See "Software and hardware disclaimer" on page 8.

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 7-1 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		

Table 7-1 File Analytics Data Collector Probes by Storage Type *(continued)*

Storage Type	CIFS (File Analytics Collector)	Windows (Host Probe)	UNIX/Linux (Host Probe)
NetApp - NFS			
NetApp - FC LUNs		X	X
NetApp - iSCSI LUNs		X	X
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 2016, 2019, 2022.
  - 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 are supported.

File Analytics probe

IT Analytics supports data collection from the following NetBackup versions:

- Veritas NetBackup 8.1, 8.2, 8.3, 9.0, 9.0.0.1, 9.1, 9.1.0.1, 10.0, 10.1, 10.1.1, 10.2, 10.3, 10.4, and 10.5.
- Cohesity NetBackup Appliance: 2.6 and later

Chapter 8

Fabric Manager configurations

This chapter includes the following topics:

Switch vendors

Note: Refer to the *Software and hardware disclaimer* supported and tested by Cohesity.

See “Software and hardware disclaimer” on page 8.

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.

Table 8-1 Switch information to collect

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 REST API exposed by Brocade Switches with FOS version - 8.1.x and above and 9.0.x **Collection Method**: Command Line Interface (CLI) exposed by Brocade Switches with Brocade FOS versions 7.4.x, 8.x, 9.0.x, 9.1.x, and 9.2.x	■ 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. IT Analytics 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 ■ On Brocade Switch Policy, select Collection Method - REST API. In Brocade Rest API server address populate comma separated list of switch FQDN/IP Address:port. Ideally, IP address/FQDN of principal switch for a fabric must be populated. Brocade Server Address*: This field is enabled if Collection Method is Command Line Interface (CLI). Specify only one Principal Switch IP address or fully qualified one Switch name for the Brocade Switch. **Note:** The port number is optional. The format should be: <ip_address>[:port_number]. **Note:** When collection method is Command Line Interface, TCP port 22 and UDP port 161 on Brocade Switch must be open, and those must be accessible to Data Collector.
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 Preferred REST-based collection method: MDS 9000 NX-OS v8.5, v9.2, v9.3, v9.4	■ 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 97. ■ 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 9

Backup Manager configurations

This chapter includes the following topics:

Backup solutions and versions

Note: Refer to the *Software and Hardware Disclaimer* supported and tested by Cohesity.

See "Software and hardware disclaimer" on page 8.

Table 9-1 Supported Backup Solutions

Backup Solution	Version	Notes and Access Requirements
Cohesity DataProtect	6.6.x , 6.8.x, 7.1.2 U3, 7.2.1, 7.2.2, 7.3, and 7.4.	REST API on Port 80 or 443

Table 9-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
Commvault Simpana	11.x (up to 11.28)	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	19.1 through 19.13	Port 9090 (Used for NetWorker REST API connection) EMC NetWorker data collection policies are implemented based on vendor version number. For EMC NetWorker versions post 9.2.1.x, collection is done using the policy titled: DELL EMC NetWorker Backup & Recovery.
Dell PowerProtect Data Manager	19.15.xx to 19.18.xx	REST API on Port 8443 User with Administrator role.
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, 19.3, 19.4, 19.10	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, 7.2, 7.6, 7.7, 7.10, 8.1	■ Port 22 (SSH)

Table 9-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
HP Data Protector	8.1, 9.0	■ 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
IBM Spectrum Protect Plus	10.1.6 and 10.1.7	Port: 443 IBM Spectrum Protect Plus user with self-service role for all resource groups.
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	v 7.0.4 and above	Port 443
Veeam Backup & Replication	■ 11.0 ■ 12.0	■ Port 9392

Table 9-1 Supported Backup Solutions *(continued)*

Backup Solution	Version	Notes and Access Requirements
Veritas NetBackup including: ■ Sun StorageTek ■ ACSLS Manager ■ SLP	8.1, 8.2, 8.3, 9.0, 9.0.0.1, 9.1, 9.1.0.1, 10.0, 10.1, 10.1.1, 10.2, 10.3, 10.4, 10.5, 11.0, 11.1, and 11.1.0.2. SLP, NetBackup v7.7 and higher.	■ The 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 IT Analytics requires that they are operational as per the NetBackup specifications. ■ NetBackup Application data collection is supported on NetBackup BYOD and Appliances form factors like NetBackup Appliances (equivalent versions 2.7.x version onwards), Flex, and Flex Scale Appliances. Centralized data collection is supported using CLI method as well as SSH/WMI interface. For centralized data collection: See "Centralized NetBackup Data Collection requirements" on page 102.
ExaGrid Subsystem ■ TieredBackupStorage	6.4 and above	Dev Mgr/API/CLI: ■ SNMP Server Identification Access Requirements: ■ SNMP Enabled on each appliance ■ Default or custom Community Sting ■ Standard SNMP UDP ports 161 & 162 must be accessible on each appliance ■ Each appliance's SNMP "Appliance Location" should be set to the same value as the ExaGrid "system"/"site" name as seen in the navigation tree ■ All access is read-only ■ Add each ExaGrid appliance's IP/name to the Connector configuration dialog Ports: ■ Standard SNMP UDP ports 161 & 162 must be accessible on each ExaGrid Appliance

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 Primary Servers and the Data Collector Server, ensure that the port communication is open on ports 443, 1556 and 13724 on NetBackup Primary Server.

  Note: Based on the connection, ssh - requires TCP/22 and API - requires 80 / 443 / 1556. NBU binaries are not required when collection method on NetBackup is SSH or WMI protocol to NetBackup Primary Server.

- 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 Primary Server binaries to be installed on the Data Collector server. The CLI is available only with the Primary Server binaries. Note that the installation of these binaries may require you to acquire a NetBackup Primary Server license from Veritas.
- See "Veritas NetBackup 8.1 (and later) requirements for centralized collection" on page 103.
- The NetBackup software version on the Data Collector must match the major and minor version of the NetBackup software that is installed on the Primary or Media Server that is being probed. When the Data Collector starts, it checks versions and halts collection for the Primary 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 104.

Note: If all NetBackup Primaries 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 Primary. 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 Primary 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 Primary 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 Primary 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 Primary 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 Primary 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 9-2 NetBackup 7.6 or earlier

NetBackup 7.6 or earlier: Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Primary	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Primary 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.

Table 9-2 NetBackup 7.6 or earlier *(continued)*

NetBackup 7.6 or earlier: Centralized Data Collector	Windows Data Collector	Linux Data Collector
Linux NetBackup Primary	NetBackup Windows Remote Administration Console (RAC) installed on the Data Collector server.	NetBackup Primary Server software installed on the Data Collector server.

Table 9-3 NetBackup 7.7 or later

NetBackup 7.7 or later: Centralized Data Collector	Windows Data Collector	Linux Data Collector
Windows NetBackup Primary	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Primary Server software installed on the Data Collector server.	NetBackup Primary 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 Primary	NetBackup Windows Remote Administration Console (RAC) is no longer available in NetBackup 7.7. You must therefore have NetBackup Primary Server software installed on the Data Collector server.	NetBackup Primary Server software installed on the Data Collector server.

Chapter 10

ServiceNow configurations

This chapter includes the following topics:

ServiceNow configurations

The IT Analytics ServiceNow App has been certified by ServiceNow for the following releases:

- Xanadu
- Yokohama
- Zurich

For more information about the IT Analytics ServiceNow App, refer to the ServiceNow store at https://store.servicenow.com

Chapter 11

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 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 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 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 11-1 Standard TCP ports used by the Portal Server and any embedded third-party software products.

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 11-2 Internal data collector ports

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

Table 11-2 Internal data collector ports *(continued)*

Product	Port	Description
EMC VNX	9223 9224+	
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
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 IT Analytics
Message Relay Server	8883	Used by data senders to communicate with the Message Relay Server.
Kafka Server	9092	Kafka Server Port
ZooKeeper	2181	ZooKeeper Port **Note:** IT Analytics uses standalone installation of single-node Apache ZooKeeper server. For secure communications, ZooKeeper single-node cluster must be protected from external traffic using network security such as firewall. This is remediated by ensuring that the ZooKeeper port (2181) is only accessible on the localhost where IT Analytics Portal/Data Collector is installed (that includes Apache ZooKeeper).

+ indicates an Admin port