NetApp ONTAP
SnapVault / SnapMirror / Unified Replication
Plugin Configuration Guide

Contents

NetApp ONTAP

This is a guide for the Bocada NetApp ONTAP plugin for NetApp Appliances. Bocada also offers a NetApp SnapCenter backup management software plugin for which is documented in a separate Configuration Guide.

NetApp Configuration Checklist

Detailed preparation and installation steps are included below, this is an overview of the steps to configure NetApp collections on your Bocada Data Collection Server:

For NetApp 9.x:

- ☐ Install PuTTY (plink) on the Bocada Data Collection Server and restart service
- ☐ HTTP username & password for NetApp SPI web link
- ☐ SSH username & password for NetApp access
- ☐ Verify required TCP ports have been opened

For NetApp 8.x:

- ☐ CIFS enabled & running for log file access
- ☐ Username & password for NetApp log file access
- ☐ Username and password for Web API access
- ☐ Required TCP ports have been opened

Supported Collection Types

The plugin currently supports the following collection types from NetApp servers, known as *nodes* in NetApp:

Collection Type	Supported	Description
Backup	✓	Collects transactional details about replication jobs. Example metrics include, start times, durations, bytes, files, errors etc.
Storage	✓	Collects point-in-time inventory information. Example metrics include, total recoverable gigabytes (occupancy), media volume count, media volume status, etc.
Policy		Collects and stores information on policy attributes, schedules, storage units, storage groups, storage lifecycle policies and clients.

For reporting on NetApp SnapCenter backups, please use the Bocada NetApp ONTAP plugin.

Data Sources

The plugin relies on the following NetApp data sources based on NetApp version.

Backup Data Data Source

9.x versions

- Files accessed via NetApp SPI (Service Processor Interface). SPI is a Web page with Web links to logs, NetApp plugin uses those links to download log files to mine backup data. The files used are https://<ServerName-IP>/spi/<NodName>/etc/log/snapmirror_audit*
- *Version, snapmirror show* commands

8.x versions Cluster-Mode

- /mroot/etc/log/mlog/snapmirror.log
- /mroot/etc/log/mlog/snapmirror_audit*
- /mroot/etc/log/mlog/snapmirror_error*

8.x in 7-Mode

- /etc/log/snapmirror[.x]

These files and locations can be NetApp version dependent. A NetApp reference that may be helpful is: https://kb-stage.netapp.com/app/answers/answer_view/a_id/1002423

Storage Data Source

9.x versions

- Commands method using commands such as: *version, storage aggregate show, volume show, volume snapshot show, snapmirror show* commands.

- It may be possible to mine storage in NetApp 9.x with NetApp Web API.

8.x versions

- NetApp Web API only

Requirements

This section lists requirements that must be met prior to collecting data with the Bocada plugin for NetApp.

NetApp 9.x

Backup & Storage Data

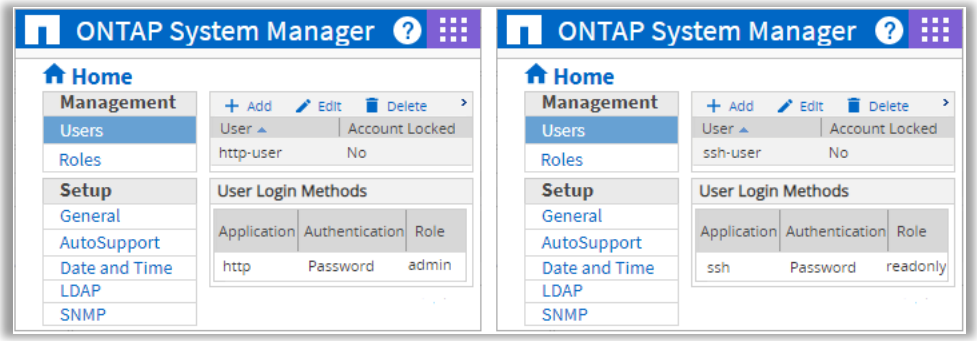
PuTTY Install

You must restart the Bocada Data Collection Service after installing PuTTy. Download and install the latest 64-bit version (the 32-bit version is not supported) of PuTTy on the Bocada DCS for communication with UNIX/Linux Cell Managers: https://www.putty.org/
You must restart the Bocada Data Collection Service after installing PuTTy.

Backup Data

SPI (Service Processor Interface) and SnapMirror show command

User Name(s) & Password(s) created in the NetApp Console are required. The plugin requires a user with *admin* role to HTTP. A user with at least *readonly* role for SSH is also required. These can be separate users as shown in the screenshots, or the same user if you allow *admin* access for both HTTP and SSH; ONTAP will not allow a single user to have multiple roles.



Storage Data

A user with at least *readonly* role for SSH is required. The same "SSH User Name" and "SSH User Password" should be used for both Backup and Storage Collections.

NetApp 8.x CIFS

CIFS must be enabled and running on any filers for the plugin to have access to log files for backup job data mining. A user account with administrative access to the CIFS share is also required. This access is required for Backup Job data mining. Access is typically needed to log files in the /etc/log directory and to the /etc directory on the filer. See Appendix A for more information.

Ports

The Bocada Data Collection Server must be able to connect to the NetApp Server on these ports:

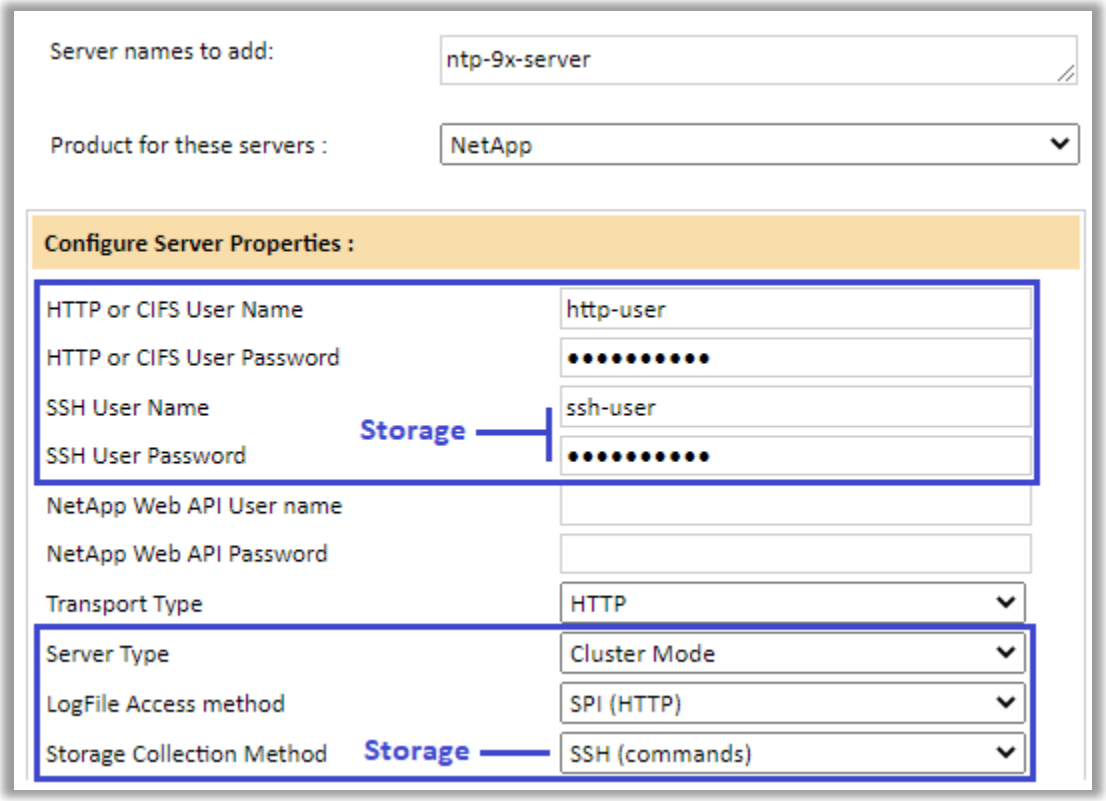
Service	Default Port	Note
HTTP	80 TCP	NetApp 9.x only
HTTPS	443 TCP	NetApp 9.x only
SSH	22 TCP	NetApp 9.x only
CIFS	445 TCP	NetApp 8.x only

Setup

Server Properties:

Backup Server Properties determine how the plugin will interface with NetApp and are managed through the Backup Servers view.

NetApp 9.x



Field Definitions for NetApp 9.x

The following apply to NetApp 9.x:

HTTP or CIFS User Name & Password

For NetApp 9.x enter user credentials as created in the NetApp Console with *admin* access role to HTTP and SPI web page. For NetApp 8.x enter the credentials for accessing the CIFS LogFile Share with administrative privileges. For notes and alternatives to using admin credentials for 8.x versions, see Appendix A.

SSH User Name & Password

For NetApp 9.x enter user credentials as created in the NetApp Console with *readonly* or greater access role to SSH.

Server Type

Chose cluster Mode for NetApp 9.x versions.

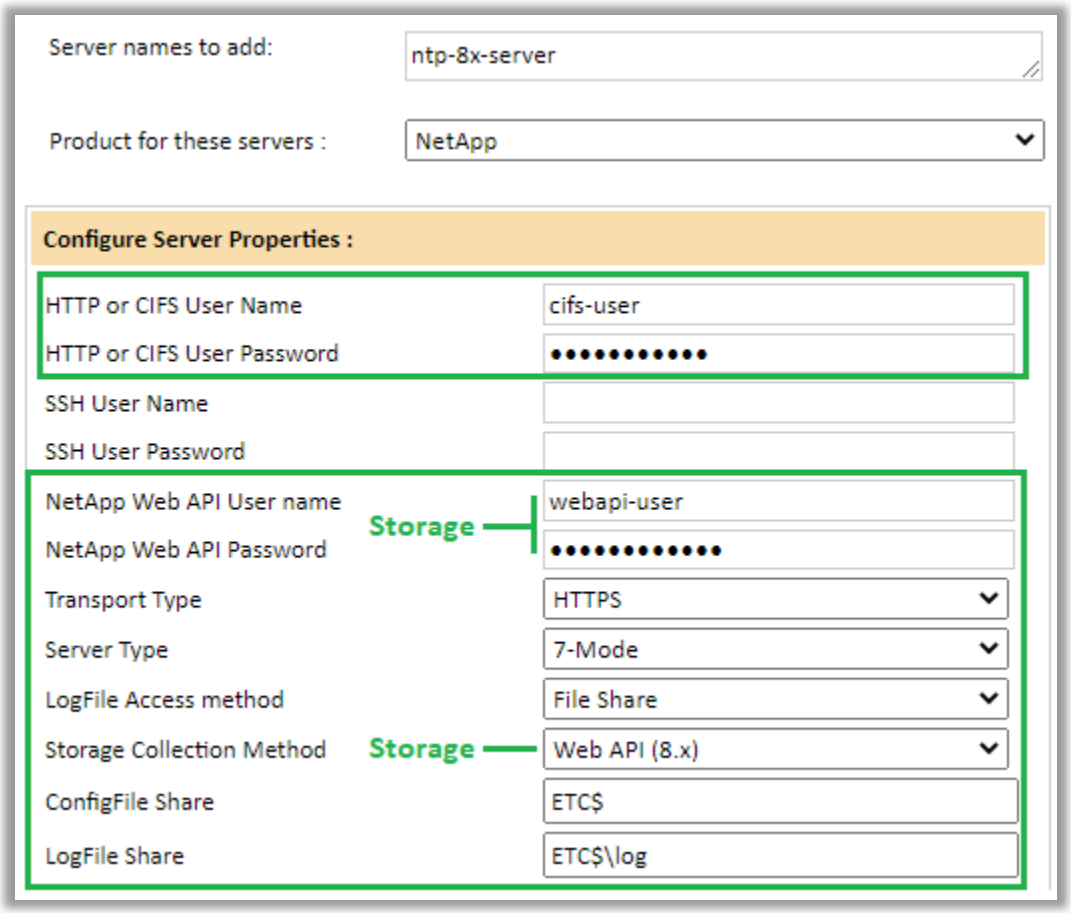
Log File Access method
Use SPI (HTTP) for 9.x NetApp clustered servers. Root SPI URL is (please verify that the root URL page, https://<server name or IP>/spi/ can be accessed with User Name & Password in server properties above.

Storage Collection Method
Choose SSH (commands) for 9.x NetApp 9.x clustered servers.

Cleanup captures (days)
This sets the number of files stored on the Bocada Data Collection Server that were created during data collection. Leave this setting as the default unless otherwise instructed by Bocada Support.

Time Zone
Select the time zone where the NetApp filer resides. This setting ensures times are displayed consistently in environments that span multiple time zones.

NetApp 8.x



Field Definitions for NetApp 8.x

The following apply to NetApp 8.x including 7-mode and CDOT.

HTTP or CIFS User Name & Password

Enter the credentials for accessing the CIFS LogFile Share with administrative privileges. For notes and alternatives to using admin credentials for 8.x versions, see Appendix A.

NetApp Web API User Name & Password

Enter the credentials to access the NetApp Web API.

Transport Type

Match the HTTP or HTTPS of the filer web service.

Server Type

Chose cluster Mode for NetApp 8.x versions in Cluster-Mode, otherwise chose 7-mode.

Log File Access method

Set to File Share for NetApp 8.x servers.

Storage Collection Method

Set to Web API (8.x).

ConfigFile Share

Enter the shared location where the NetApp snapmirror.conf file is located. By default, this file is in the /etc directory on your filer. Please see Appendix A if Admin access to the /etc directory is not possible.

LogFile Share

Enter the shared location where the NetApp snapmirror logs reside.

Use IP Address

Select “yes” if you have trouble resolving the filer name to IP within your domain(s).

LogFile Share (NetApp 8.x only)

Enter the shared location where the NetApp SnapMirror logs reside.

Use IP Address (NetApp 8.x only)

Select “yes” if you have trouble resolving the filer name to IP within your domain(s).

Reporting Notes

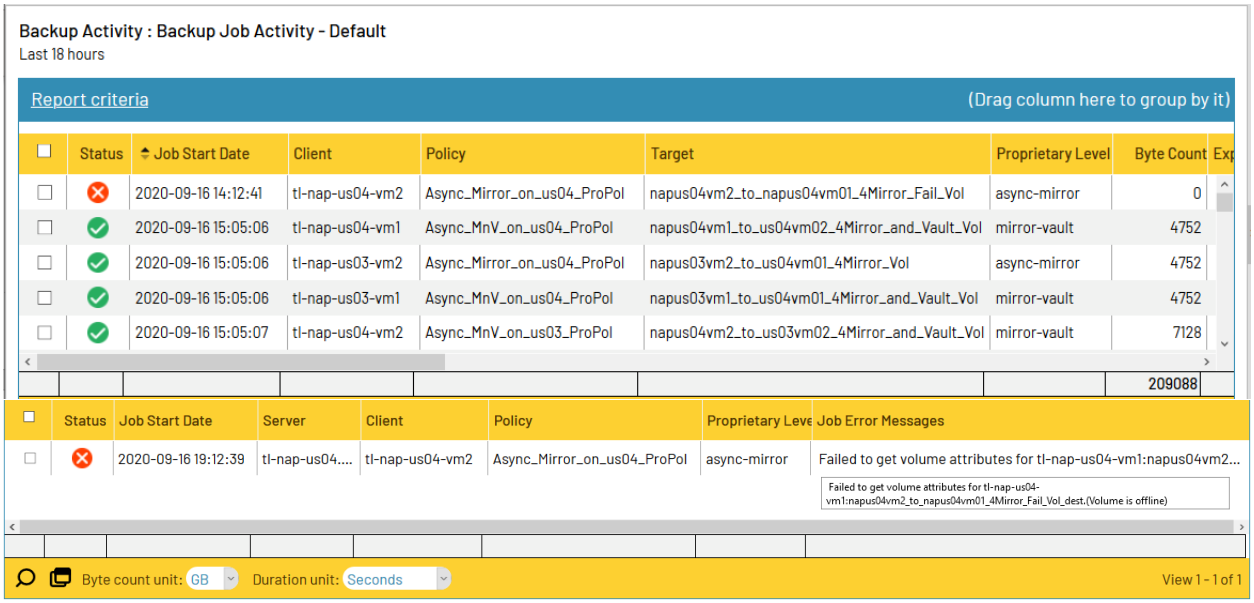
The usual sets of Bocada reports are useful for monitoring NetApp. Client sources being backed up and replication jobs between NetApp servers are in Bocada jobs based reports including Job Trends, Backup Failures, Backup Activity, Backup Trends, etc. Note that Bocada only mines the receipt of replication jobs from the destination NetApp device receiving replication data. No jobs will be shown for the NetApp that is sending the data.

Mapping of data

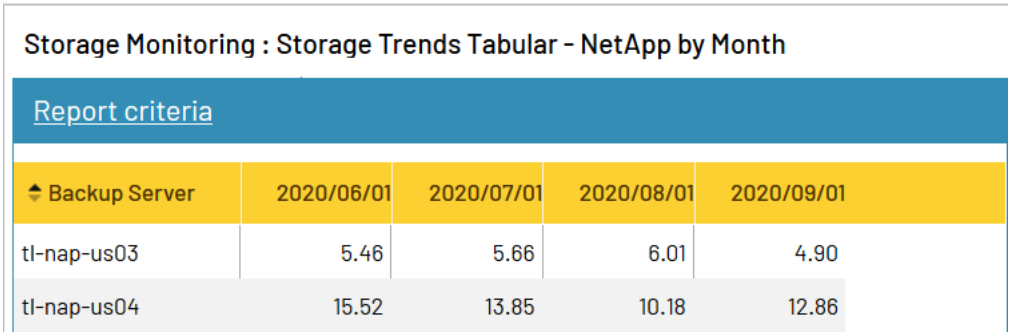
Bocada maps backup data from NetApp as follows:

Bocada	NetApp
Server	NetApp Destination device
Client	NetApp virtual storage item, Netapp Source Device
Target	Volume, Disk, or LUN being backed up

An example screenshot of a Backup Activities report, followed by a Backup Failures detail report, is shown below.



Storage usage data can also be seen in the standard Bocada storage reports. For example, the screenshot below shows storage capacity usage trends over the past 4 months for two NetApp devices.



Troubleshooting

NetApp 8.x Backup collection fails because of NetApp WebAPI credentials failed. Thought the WebAPI credentials are primarily used for Storage data collection, there are some secondary data points collected using the API for Backup data, including volume and schedule information.

If the Web API credentials cannot be resolved, they can be bypassed for backup collection by removing the *Web API User Name* from the plugin properties.

Appendix A: Admin Access to /etc Directory (NetApp 8.x)

Some Bocada installations with NetApp are not able to grant the needed ADMIN level access to the /etc directory on a filer due to security considerations. Data collection through the NetApp plugin requires Administrator level access the /etc directory for reading of the snapmirror.conf file. If you are unable to grant Admin level access to the /etc directory on a filer then you can configure a regular file copy of the snapmirror.conf file to /etc/log directory and specify a user with access to the /etc/log directory.

The Bocada NetApp plugin reports on SnapMirror as well as SnapVault and expects to be able to access the snapmirror.conf file /etc/snapmirror.conf via an ADMIN level share.

The snapmirror.conf file contains SnapMirror backup definitions and that is all. If you are only using SnapVault job types, no direct SnapMirror configuration, the you can copy the file over to the /etc/log location. One static copy will then fill the need, so long as you never configure SnapMirror jobs. You can confirm the contents here, Snapmirror log info:
https://library.netapp.com/ecmdocs/ECMP1196991/html/GUID-6AE226D5-BAAD-431F-B89F-EB1BBCA0636B.html

If you are not using SnapMirror then the file should not ever be updated, and this will be a permanent workaround. If you are using SnapMirror then another possibility would be to schedule a regular file copy within the filer, such as once or twice per day. If you are using SnapMirror in addition to SnapVault the up-to-date snapmirror.conf is a required file to get all backup jobs, and access must be obtained.

Here are the steps in order:

1. Copy /etc/snapmirror.conf to /etc/log/snapmirror.conf
2. Allow the needed access permission to /etc/log
3. Put the same entry for the ConfigFile Share as the LogFile Share in the Bocada NetApp server properties, e.g.: ETC$\log

Note: This may only be relevant for 7-Mode filers and requirements may be different for NetApp C-DOT.

More information about the NetApp snapmirror.conf can be found on NetApp support:
https://library.netapp.com/ecmdocs/ECMP1196991/html/GUID-6AE226D5-BAAD-431F-B89F-EB1BBCA0636B.html

Technical Support

For technical support or a copy of our standard support agreement, please contact us.

Support Portal: https://bocada-support.force.com
E-mail: support@bocada.com
Phone: +1-425-898-2400

Copyright © 2020 Bocada LLC. All Rights Reserved. Bocada and BackupReport are registered trademarks of Bocada LLC. Vision, Prism, vpConnect, and the Bocada logo are trademarks of Bocada LLC. Other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Protected by U.S patents 6,640,217; 6,708,188; 6,745,210; 7,457,833; 7,469,264; 7,496,614; 8,407,227

The material in this manual is for information only and is subject to change without notice. While efforts have been made to ensure accuracy, Bocada LLC assumes no liability resulting from errors or omissions in this document, or from the use of information contained herein.

Bocada LLC reserves the right to make changes in the product design and documentation without reservation and without notification to its users. 2021-10-28