Broadcom

Cloud Insights

NetApp
April 16, 2024

This PDF was generated from https://docs.netapp.com/us-en/cloudinsights/task_dc_brocade_bna.html on April 16, 2024. Always check docs.netapp.com for the latest.

Table of Contents

Broadcom . . . 1
Brocade Network Advisor data collector . . . 1
Brocade FC Switch data collector . . . 2
Brocade FOS REST Data Collector . . . 5

Broadcom

Brocade Network Advisor data collector

Cloud Insights uses the Brocade Network Advisor data collector to acquire inventory and performance data from Brocade switches.

Terminology

Cloud Insights acquires the following inventory information from the Brocade Network Advisor data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
Virtual Fabric, Physical Fabric	Fabric
Logical Switch	Logical Switch

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

The following are required to configure this data collector:

- The Cloud Insights Acquisition Unit will initate connections to TCP port 443 on the BNA server. BNA server must be running version 14.2.1 or higher.
- Brocade Network Advisor Server IP address
- User name and password to an administrator account
- Port requirement: HTTP/HTTPS 443

Configuration

Field	Description
Brocade Network Advisor Server IP	IP address of the Network Advisor Server
User Name	User name for the switch
User Name	Administrator user name
Password	Administrator password

Advanced configuration

Field	Description
Connection Type	HTTPS (default port 443) or HTTP (default port 80)
Override Connection Port	If blank, use the default port in the Connection Type field, otherwise enter the connection port to use
Password	Password for the switch
Inventory poll interval (min)	The default is 40
Report Access Gateway	Check to include devices in Access Gateway mode
Performance Poll Interval (sec)	The default is 1800

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
Receive a message that more than 1 node is logged into the Access Gateway port, or data collector fails to discover Access Gateway device.	Check that the NPV device is operating correctly and that all connected WWNs are expected. Do not directly acquire the NPV device. Instead, acquisition of the core fabric switch will collect the NPV device data.

Additional information may be found from the Support page or in the Data Collector Support Matrix.

Brocade FC Switch data collector

Cloud Insights uses the Brocade FC Switch (SSH) data source to discover inventory for Brocade or rebranded switch devices running Factored Operating System (FOS) firmware 4.2 and later. Devices in both FC switch and Access Gateway modes are supported.

Terminology

Cloud Insights acquires the following inventory information from the Brocade FC Switch data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
Virtual Fabric, Physical Fabric	Fabric
Zone	Zone
Logical Switch	Logical Switch

Vendor/Model Term	Cloud Insights Term
Virtual Volume	Volume
LSAN Zone	IVR Zone

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- The Cloud Insights Acquisition Unit (AU) will initiate connections to TCP Port 22 on Brocade switches to collect inventory data. The AU will also initiate connections to UDP port 161 for collection of performance data.
- There must be IP connectivity to all switches in the fabric. If you select the Discover all switches in the fabric check box, Cloud Insights identifies all the switches in the fabric; however, it needs IP connectivity to these additional switches to discover them.
- The same account is needed globally across all switches in the fabric. You can use PuTTY (open source terminal emulator) to confirm access.
- Ports 161 and 162 must be open to all switches in the fabric for SNMP performance polling.
- SNMP read-only Community String

Configuration

Field	Description
Switch IP	IP address or fully-qualified domain name of the EFC Server
User Name	User name for the switch
Password	Password for the switch
SNMP	SNMP version
SNMP Community String	SNMP read-only community string used to access the switch
SNMP User Name	SNMP user name
SNMP Password	SNMP password

Advanced configuration

Field	Description
Fabric name	Fabric name to be reported by the data collector. Leave blank to report the fabric name as WWN.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 15.
Excluded Devices	Comma-separated list of device IDs to exclude from polling
Admin Domains Active	Select if using Admin Domains

Field	Description
Retrieve MPR Data	Select to acquire routing data from your multiprotocol router.
Enable Trapping	Select to enable acquisition upon receiving an SNMP trap from the device. If you select enable trapping, you must also activate SNMP.
Minimum Time Between Traps (sec)	Minimum time between acquisition attempts triggered by traps. The default is 10.
Discover all switches in the fabric	Select to discover all switches in the fabric
Choose Favoring HBA vs. Zone Aliases	Choose whether to favor HBA or zone aliases
Performance Poll Interval (sec)	Interval between performance polls. The default is 300.
SNMP Auth Protocol	SNMP authentication protocol (SNMP v3 only)
SNMP Privacy Password	SNMP privacy password (SNMP v3 only)
SNMP Retries	Number of SNMP retry attempts

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
The inventory acquisition of the Brocade datasource fails with the error: <date> <time> ERROR [com.onaro.sanscreen.acquisition.framework.datasource.BaseDataSource] Error 2 out of 2: <datasource name> [Internal error] - Unable to generate the model for device <IP>. Error detecting prompt ([Device name <name>]: Unable to generate the model for device <IP>. Error detecting prompt)	The issue may be caused when the Brocade switch takes too long to return with a prompt, exceeding the default timeout of 5 seconds. In the data collector's Advanced Configuration settings in Cloud Insights, try increasing the *SSH Banner Wait Timeout (sec)* to a higher value.
Error: "Cloud Insights received Invalid Chassis Role"	Check that the user configured in this data source has been granted the chassis role permission.
Error: "Mismatched Chassis IP Address"	Change the data source configuration to use chassis IP address.
Receive a message that more than 1 node is logged into the Access Gateway port	Check that the NPV device is operating correctly and that all connected WWNs are expected. Do not directly acquire the NPV device. Instead, acquisition of the core fabric switch will collect the NPV device data.
Performance collection fails with "Timed out during sending SNMP request".	Depending on query variables and switch configuration, some queries may exceed the default timeout. Learn More.

Additional information may be found from the Support page or in the Data Collector Support Matrix.

Brocade FOS REST Data Collector

Cloud Insights uses the Brocade FOS REST collector to discover inventory and performance for Brocade switch devices running FabricOS (FOS) firmware 8.2 and later.

By default, this collector will attempt to discover all the FOS devices that are a part of all the fabrics the switch is part of.

Terminology

Cloud Insights acquires the following inventory information from the Brocade FOS REST data collector. For each asset type acquired by Cloud Insights, the most common terminology used for this asset is shown. When viewing or troubleshooting this data collector, keep the following terminology in mind:

Vendor/Model Term	Cloud Insights Term
Switch	Switch
Port	Port
Virtual Fabric, Physical Fabric	Fabric
Zone	Zone
Logical Switch	Logical Switch
Virtual Volume	Volume
LSAN Zone	IVR Zone

Note: These are common terminology mappings only and might not represent every case for this data collector.

Requirements

- There must be TCP connectivity to all switches in the fabric. This data collector type will seamlessly try both HTTP and HTTPS for each device in the fabric. If you select the *Discover all switches in the fabric* check box, Cloud Insights identifies all the switches in the fabric; however, it needs TCP connectivity to these additional switches to discover them.
- The same account is needed globally across all switches in the fabric. You can use the device's Web interface to confirm access.

Configuration

Field	Description
Switch IP	IP address or fully-qualified domain name of the FOS switch
User Name	User name for the switch
Password	Password for the switch

Advanced configuration

Field	Description
Excluded Devices	Comma-separated list of device IPv4 addresses to exclude from polling.
Inventory Poll Interval (min)	Interval between inventory polls. The default is 60.
Discover all switches in the fabric	Select to discover all switches in the fabric.
Choose Favoring HBA vs. Zone Aliases	Choose whether to favor HBA or zone aliases.
Connection type	HTTP or HTTPS.
Note that this setting only changes which protocol CI attempts to use per device first - CI will attempt the opposite protocol automatically if the default fails	Override TCP Port
Specify a port if not using the default.	Performance Poll Interval (sec)

Troubleshooting

Some things to try if you encounter problems with this data collector:

Inventory

Problem:	Try this:
The Test feature warns me that a protocol is inaccessible	A given Brocade FOS 8.2+ device will only want to speak on HTTP or HTTPS - if a switch has a digital certificate installed, the switch will throw HTTP errors if one attempts to communicate to it with unencrypted HTTP versus HTTPS. The test feature attempts communication with both HTTP and HTTPS - if the Test tells you that one protocol passes, you can safely save the collector and not worry that the other protocol was unsuccessful - the collector will attempt both protocols during collection, and only fail if neither works.
Error: “Cloud Insights received Invalid Chassis Role”	Check that the user configured in this data source has been granted the chassis role permission.
Error: "Mismatched Chassis IP Address"	Change the data source configuration to use chassis IP address.
Receive a message that more than 1 node is logged into the Access Gateway port	Check that the NPV device is operating correctly and that all connected WWNs are expected. Do not directly acquire the NPV device. Instead, acquisition of the core fabric switch will collect the NPV device data.
Performance collection fails with "Timed out during sending SNMP request".	Depending on query variables and switch configuration, some queries may exceed the default timeout. Learn More.

Additional information may be found from the Support page or in the Data Collector Support Matrix.

Copyright information

Copyright © 2024 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.