Avaya Fabric Orchestrator Release Notes

Release 1.1

Issue 02.03

January 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on its hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.

CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/ LicenseInfo under the link “Heritage Nortel Products”. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits

installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

Each virtual appliance has its own ordering code. Note that each instance of a virtual appliance must be ordered separately. If the end-user customer or Business Partner wants to install two of the same type of virtual appliances, then two virtual appliances of that type must be ordered.

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software that may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http:// support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation and Product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Contents

1 Introduction 6
1.1 Intended Audience 6
1.2 About Avaya Fabric Orchestrator 6
2 Terminology 7
3 New in this Release 8
3.1 Support for VXLAN tunnel management 8
3.2 Device License Manager 9
3.3 Northbound Interface 9
3.4 Out-of-band Management 10
3.5 High Availability 10
3.6 Support for Fabric Attach in Fabric Connect view 11
3.7 Improvements to Fabric Topology view 11
3.8 Client Support 11
3.9 Device Support 11
3.10 Customizable Dashboard and New Dashboard Widgets 12
3.11 Enhanced Reports 13
3.12 Improved Scalability 13
3.13 New add-on licenses 14
3.14 Discovery Domain used by Configuration 14
3.15 Device Software Management now uses Configuration Device Inventory 14
3.16 AFO Backup & Restore 14
3.17 AFO Upgrade 15
3.18 Data Migration from legacy VPFM and COM 18
4 Avaya Fabric Orchestrator hardware and software requirements 20
4.1 Other software requirements 20
5 AFO Release 1.1 device support 21
6 Release distribution and license information 23
7 Installation procedure 26
8 Known problems and workarounds 27
9 Resolved issues in AFO Release 1.1 29

10 Operational notes 30
11 Document list 33
12 Technical support 34

1 Introduction

Purpose

Avaya Fabric Orchestrator (AFO) Release 1.1 is a minor release that adds several new features to the product and resolves issues found in Release 1.0. This document provides information about new features, supported products, known issues and workarounds, and other important notices for Avaya Fabric Orchestrator (AFO) Release 1.1.

1.1 Intended Audience

The primary audience for this document is anyone who is involved with deployment, administration, maintenance and troubleshooting activities of Avaya Fabric Orchestrator at a supported site. The audience includes, but is not limited to, implementation engineers, field technicians, business partners, solution providers, and customers. This document does not include optional or customized aspects of a configuration.

1.2 About Avaya Fabric Orchestrator

Avaya Fabric Orchestrator is a scalable, easily deployable integrated management solution which allows you to to manage a network domain in a single web based application.

AFO is delivered as a rack mountable hardware appliance for easy deployment and configuration in less than an hour. All software necessary to use AFO is pre-packaged and configured for use once the initial deployment completes.

The AFO hardware appliance runs RedHat Enterprise Linux 7.1 based KVM hypervisor with all management functions running in various virtual machines on the KVM hypervisor.

2 Terminology

Term	Description
ADM	Appliance Device Manager
AFO	Avaya Fabric Orchestrator
APLS	Avaya Private Label Switching
Appliance	A single hardware server contains one or more virtual machines.
EDM	Enterprise Device Manager
ERS	Ethernet Routing Switch
FA	Fabric Attach
HA	High Availability
KVM	Kernel-based Virtual Machine
Migration	A migration consists of a specific subset of upgrades you perform when you move a customer from one product to another. Migration may also require the customer to obtain new hardware.
MSC	Management Server Console
SCP	Secure Copy
SMGR	System Manager
SSH	Secure Shell Protocol
Upgrade	The process of taking a product from one release to a higher release.
VM	Virtual Machine
VNI	VXLAN Network Identifier
VOSS	VSP Operating System Software
VSP	Virtual Services Platform
VTEP	VXLAN Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network

3 New in this Release

The following section provides a list of the new features, enhancements, and changes in AFO Release 1.1.

AFO new features summary:

- VXLAN tunnel management
- Device License Manager
- Northbound Interface
- Out of Band Device Management
- High Availability
- Support of Safari browser on macOS v10.8

AFO enhancements summary:

- Support for Fabric Attach in AFO Configuration Fabric Connect view
- Improvements to Fabric Topology view
- Device Support enhancements
- Customizable Dashboard and new dashboard Widgets
- Improved Scalability
- Monitoring report enhancements
- Backup and Restore enhancements
- Data migration enhancements
- New Licenses

AFO changes:

- **AFO** default domain name changed to **Default**
- Backup & Restore → Device Software Management inventory change
- CLI Manager tool removed

3.1 Support for VXLAN tunnel management

VXLAN is a protocol for running a Layer 2 network and stretching it over a Layer 3 network utilizing MAC-in-UDP encapsulation, which can be referred to as a VXLAN tunnel. A VXLAN tunnel provides an ability to separate, abstract and decouple the physical topology from a logical or virtual topology through encapsulated tunneling.

VOSS 6.0 software for Avaya VSP and APLS devices introduces VXLAN VTEP functionality. The VTEP can to do VXLAN to VLAN, VXLAN to VXLAN and VXLAN to SPBm gateway functionality.

VXLAN tunnel management allows you to view and configure the VTEP functionality on Avaya VSP and APLS devices and create and manage full mesh VNI tunnels.

VXLAN management feature has the following main capabilities:

- Discover devices that are capable of supporting VXLAN, based on the logged in user's device group context.
- Discover all existing VTEPs and VNIs based on the logged in user's device group context.
- Display VTEP operational mode (base or full internetworking) of VXLAN capable device.
- Enable and disable VTEP configuration on a VXLAN capable device.
- Auto-create or auto-delete remote VTEPs on the neighbor devices.
- Create and delete VNIs.
- Add VTEPs to the existing VNIs.
- Support Read-only and Read-write based on logged in user's Role.
- Configure Full Mesh Topology on a VNID with the neighboring VTEP capable device.
- Run consistency check on a VNI, to check if it forms a Full mesh or is missing any neighboring VTEP Device(s).
- Add, update or delete non-Avaya VTEPs to the VXLAN manager.
- Add non-Avaya VTEPs to an existing VNI.

3.2 Device License Manager

Device License Manager can help you manage the licenses of all Avaya network devices from a centralized user interface in Avaya Fabric Orchestrator. In AFO Release 1.1 a read-only view of the licenses installed on the Avaya L2 and L3 switches is provided.

3.3 Northbound Interface

AFO Release 1.1 introduces Northbound web service APIs for the consumption of other Avaya applications and 3rd party applications. AFO Northbound APIs feature uses REST based web service. Access to the APIs is restricted only to registered clients and users of the NBI APIs.

The following are the highlights of this feature:

- Authentication and Authorization (using oAuth based RBAC) for accessing the APIs.
- Users, Roles, and Permissions administration for access control of Northbound APIs.
- AFO GUI for on-boarding the clients using Client registration.

This release provides the following Northbound web service APIs

API	Description	End point URL
Discovery API	1. Provides list of all the domains 2. Provides statistics of the domain like number of IP phones, switches, routers etc	1. https://<AFO FQDN>/nbi/api/v1/domains 2. https://<AFO FQDN>/nbi/api/v1/domains/{domain}
Devices API	Provides list of devices	https://<AFO

	present in a domain	FQDN>/nbi/api/v1/devices/{domain}
Device Inventory API	Provides the hardware inventory details of a specific device	https://<AFO FQDN>/nbi /api/v1/{domain}/inventory/{device-id}

Northbound API documentation and code examples (java and python) are available at https://<AFO FQDN>/nbi/docs/index.html

Note:

1. AFO Northbound APIs are secured with oAuth 2 protocol. Contact your AFO system administrator to get yourClient_ID, Client_Secret, user/password.
2. For Client credential flow, you need to create role with the same name as the client-name and assign necessary permissions to it.

3.4 Out-of-band Management

This feature allows you to provision separate networks for –

- the management of AFO appliance and web access to the appliance
- the network switches to be managed using AFO

This feature is configured by one of the following ways.

- During deployment you can specify whether to use out-of-band management or not.
- A script is provided which can be run to switch from single network to out-of-band management or vice-versa at any time after deployment (provided the NICs connected appropriately support the network configuration).

Refer to the document ***Troubleshooting Avaya Fabric Orchestrator (NN48100-702)*** for the steps to enable or disable the Out of Band network.

3.5 High Availability

AFO Release 1.1 introduces an optional High Availability (HA) feature. HA requires two AFO appliances and also a HA license installed on the Leader server. AFO HA feature uses the Active-Standby model. Existing AFO appliances can be a part of a HA setup after upgrading to AFO Release 1.1.

For details on HA Configuration please refer to the document ***Deploying Avaya Fabric Orchestrator (NN48100-101).***

3.6 Support for Fabric Attach in Fabric Connect view

AFO Release 1.0 provided the capability to configure Fabric Attach (FA) feature on a per-device basis using the EDM plugins. AFO Release 1.1 introduces a consolidated multi-device view and provisioning of Fabric Attach feature in the Fabric Connect Configuration view. This feature can be accessed using the menu hierarchy **Configuration → Fabric Connect**. Use this feature to:

- Enable/disable FA feature on multiple devices from one UI view.
- Enable/disable FA feature on a per-port basis on multiple devices from a single view
- View FA servers, FA proxies and the FA link between them in the existing Fabric Topology.

3.7 Improvements to Fabric Topology view

Following improvements have been made to the Fabric Connect Topology map.

- The Fabric Topology tab is the default tab and is always open in Fabric Connect view.
- FA and FE links are displayed using different colors; FA Proxy nodes also displayed using different color.

Note: To see Fabric Extend (FE) links in different color, a discovery should be performed in Fabric Extend view prior to displaying (or refreshing) the Fabric Topology map.

3.8 Client Support

Support of Safari as a client browser has been added in AFO Release 1.1. The AFO user interface supports the following web browsers:

Client Browser	Supported Versions
Firefox	v47 and above
Internet Explorer	v11
Safari	Safari on macOS v10.8 (Mountain Lion) and above

Note:

Safari blocks popups without informing the user. Popups can be enabled by manually adding all of the AFO FQDN addresses into exclusions in Safari settings.

3.9 Device Support

The following table shows the new devices and device software versions for which support has been added in AFO Release 1.1.

Device Family	Software Version	Notes
APLS	4.3.1	New Models: DSG6248, DSG6248P, DSG6248CFP, DSG7648, DSG7648C, DSG7480, DSG8032
	6.0	Partial support (Discovery, EDM and VXLAN)
VSP 9000	4.1, 4.1.1	
VSP 4000 VSP 7200 VSP 8000	4.2.2, 4.2.3	
	5.1	Port-Licensed 7200 models.
	5.1.1	
	6.0	Partial support (Discovery, EDM and VXLAN)
VSP 70XX	10.4	
ERS 5900	7.0.1	
ERS 4900, ERS 5900	7.1	New Models: ERS4950GTS, ERS4950GTS-PWR+, ERS4926GTS, ERS4926GTS-PWR+, ERS5928GTS-uPWR
	7.2	New Models: ERS59100GTS, ERS59100GTS-PWR+
ERS 5500, ERS 5600	6.3.5, 6.3.6	
	6.6.2, 6.6.3	
ERS 4500, ERS 4800	5.7.2, 5.7.3	
ERS 4800	5.8.2, 5.8.3	
	5.9.2	
ERS 3500	5.1.3	
	5.2.3	
	5.3	New Models: ERS3550T, ERS3550T-PWR+
	5.3.1, 5.3.2	
WLAN 9100	7.5.6	WLAN 9100 Solution : WOS and AP (Monitoring support only)

3.10 Customizable Dashboard and New Dashboard Widgets

AFO Release 1.1 supports customization of the Home Dashboard. The enhanced dashboard provides the following capabilities:

- View mode and an edit mode. Edit mode can be used to customize the dashboard view.
- Multiple layout options.

- You can select the dashboard widgets from a library of widgets.
- A widget can be maximized. When maximized, the single widget will be displayed in a popup which occupies maximum space on the window.
- A widget can be minimized or restored to normal size.
- Based on the widgets, individual widgets support their own customization.

AFO Release 1.1 supports the following new dashboard widgets:

- **Device Backup Summary widget:**
  The Device Backup Schedule Summary widget shows a graphical representation of device backup schedule repeat interval vs device count. The widget provides the information about how many devices have their backup schedule repeat intervals within a specified range (for example, how many devices have backup schedule repeat interval between 1 to 2 weeks).

- **Device Inventory widget:**
  The Device Inventory widget shows a tabular view of the Avaya L2/L3 switches discovered in the Default domain. The view can be customized by selecting one of the several GroupBy options provided. The table supports the ability to expand and collapse the groups.

3.11 Enhanced Reports

The following enhanced reports are available in AFO Release 1.1

- Built-in reports
  - VM Resource Pool Utilization and VMs using over 50GB Storage
  - Network Node System Uptime and Server System Uptime
  - Predictive Capacity Reports
    - Top 5 Capacity – 1 Week Average
    - Top File Systems – 1 Week Average
  - SPB VLAN Index to ISID Mapping
  - Inventory Active Endpoints by Node
- Custom Hypercube report enhancement
  - Improved usability by removing the need for scripting when generate the hypercube reports. A much user-friendly interactive mode of picking and choosing of options and fields has been introduced.

3.12 Improved Scalability

- Support monitoring of up to 30000 nodes (up from 20000 nodes in AFO 1.0)
- Increased number of concurrent user sessions:
  - For 250 node license, maximum 10 user sessions
  - For 1500 node license, maximum of 20 user sessions of which up to 15 can be working on configuration features

- For 5000 node license, maximun of 30 user sessions of which up to 15 can be working on configuration features

3.13 New add-on licenses

Following new add-on (feature) licenses have been introduced in this release –

- License for High Availability feature
- License for monitoring additional 10000 nodes

For more details please refer to section on ***Release distribution and license information***.

3.14 Discovery Domain used by Configuration

The name of the pre-created domain used to perform Avaya-only discovery has been changed from ***AFO*** to ***Default***.

3.15 Device Software Management now uses Configuration Device Inventory

In AFO Release 1.1 the Device Software manager uses the Configuration inventory directly for all DSM features. Devices used in DSM will be always in sync with the devices discovered by the Default domain.

In AFO Release 1.0, Device Software Management (DSM) was having its own device inventory though its inventory was imported from Configuration Device Inventory. Except for the first time DSM is opened (in which case the devices were automatically imported), user had to manually import the devices using a toolbar button in the DSM Inventory portlet. As a result, there was possibility of the DSM inventory getting out of sync with the AFO (Default) domain.

Because DSM does not have its own inventory any more, the device inventory portlet has been removed from DSM. The common device inventory can be viewed using the **Configuration → Network Table** view.

3.16 AFO Backup & Restore

AFO Release 1.1 backup and restore module supports backing up and restoring data for single node as well as for HA cluster. AFO Release 1.1 adds support for the backup and restore of Cluster Engine VM along with all other AFO VMs.

The backup script performs backup of the following applications:

- Platform data (*Users, Roles, Password and Session Policies, Certificates*)
- Common Services Data (*Credentials, Licenses*)

- Application data (*the content as decided by application*) (database tables, log files, any device configuration backup archives etc.)

Please refer to the document ***Administration using Avaya Fabric Orchestrator (NN48100-600)*** for further details.

3.17 AFO Upgrade

The procedure for upgrading AFO 1.0 to AFO 1.1 has been updated and simplified since the release of AFO 1.1. As a result, the upgrade procedure provided in the document ***Deploying Avaya Fabric Orchestrator (NN48100-101)*** is now ***obsolete.***

Use the following new procedure for upgrading AFO Appliance from AFO 1.0 to AFO 1.1.

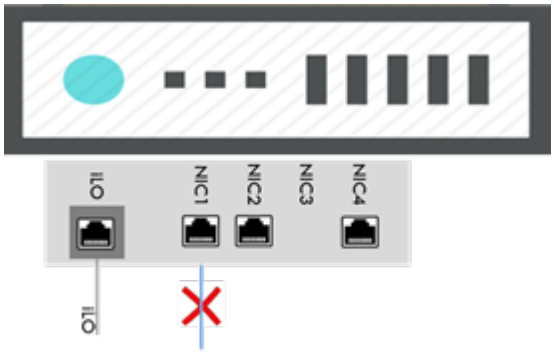
Prerequisites:

- Download the following from PLDS to a client machine (e.g. your laptop).
  - "AFO 1.0 to 1.1 Infrastructure and applications upgrade bundle", PLDS ID: **AFO00000012**
  - "AFO 1.0 to 1.1 Upgrade Utility", PLDS ID: **AFO00000014**
- After downloading the bundle from PLDS ensure checksum matches.

Procedure:

Step 1: Using Winscp or FileZilla or SCP/SFTP client transfer the downloaded bundles from the client machine to AFO KVM server under ***/opt/*** folder as root user.

Step 2: Detach the NIC1 Network cable from the AFO Server.



Step 3: Login to KVM using console as root user.

- Login using ILO or connect directly using monitor to server.

Step 4: Unzip the KVM Upgrade CLI Utility in the console.

#cd /opt

#unzip KVM-UPG-CLI-UTILITY-<version>.zip

Step 5: Run the below command to begin the upgrade from console.

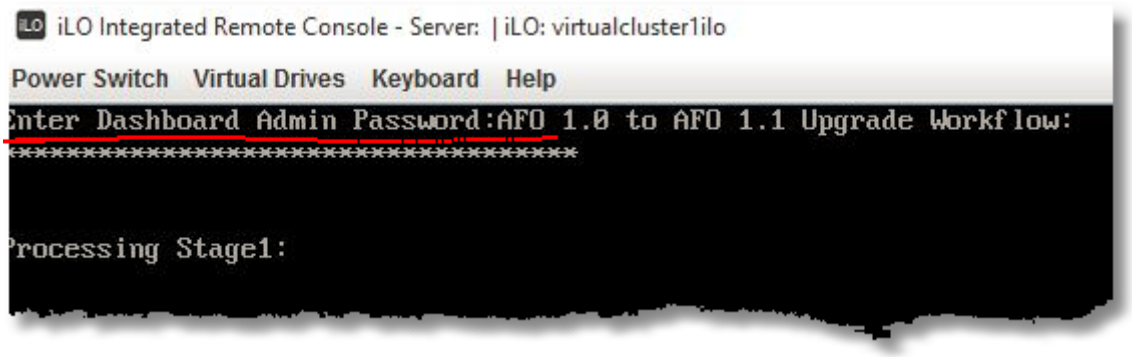
#cd /opt

#bash upgradeSystem

Step 6: Upgrade process will take approximately 150 minutes. Upgrade Progress can be tracked in the console. Wait till the upgrade process completes.

Step 7: After successful upgrade connect back the NIC1 network cable to the AFO appliance.

We have intermittently noticed the below mixed up message while accepting Dashboard Admin password. Please enter Dashboard admin password and continue.



Troubleshooting

Trouble Description	Probable Cause	Where to look for	Recovery
After upgrade complete, unable to login to application. Browser reports "too many redirects"	Member trust across AFO cluster could have failed.	Run the following command from KVM console and collect the logs: */usr/local/infra/bin/collectlogs.sh*	1. It is possible to revert the AFO 1.1 to day1 configuration with no customization by running the following command: bash */opt/avaya/afo/infra/scripts//imageRecovery.sh restore* 2. Select the last available backup point and initiate the image recovery.

Trouble Description	Probable Cause	Where to look for	Recovery
AFO server rebooted during the upgrade.	CTRL+ALT+DEL could have been pressed from the client laptop while the focus in HP Console	'last' command on hypervisor to confirm reboot.	Restart the upgrade procedure again by running 'upgradeSystem' command.
Upgrade fails to come out of "Waiting for deployment to Complete…"	NIC1 has not been disconnected and 1. Two parallel AFO upgrades initiated within 5 minutes 2. The upgrade site has IP address in 10.10.0.0/16 subnet.	No logs required	1. Disconnect the NIC1 2. Rebooting the server will initiate the upgrade process
Upgrade seems to take unusually long time during the backup process	If the Monitoring contains huge amount of data (in GBs) the backup process will run for a few hours.	1. Run the following command to confirm the space issue on the Monitoring VM *du -skh /opt/avaya/smgr/vpfm/acqHistory* 2. zip the files from "*/opt/avaya/smgr/log/"* from MSC VM	1. The Backup has not hanged or failed. It is still proceeding to take the backup of the applications. 2. Wait for a few hours for the backup process to complete and the upgrade to resume. Note: If backup takes long time, then subsequent upgrade will also take long time.
Repeated authentication failure while providing the admin password	The admin password contains '\' as one of the characters. OR You have just deployed or reset the system and haven't changed the Web UI password for the first time.	Check the password for backslash character OR Login using the Web UI as 'admin' user	1. Reset the admin password if prompted OR to one without any '\' character if it contains that character 2. Restart the upgrade.

Note:

In some cases user may encounter one or more of the following minor problems after upgrade.

1. Issue: Monitoring is turned off on the Default domain after restart of monitoring service.

   Workaround: From the discovery page turn monitoring off then back on in the Default domain.

2. Issue: In Network → Action Console, the action and next occurrence for some reports may be blank under Action Schedules.

   Workaround: Remove and recreate the report schedule in the Schedules page.

3. Issue: Empty AFO domain may remain under Network Discovery and Network Topology pages.

   Workaround: Delete the AFO domain from Discovery page.

4. Issue: Monitoring Overrides created in the AFO domain in release 1.0 will not work in release 1.1. "Domain element not found for <device>" is displayed in the Parameter Overrides section of the page.

   Workaround: Recreate the monitoring overrides in the Network →Monitoring Overrides page and then delete the old ones.

5. Issue: Private dashboard created on 'AFO' domain in release 1.0 shows no data after upgrade.

   Workaround: Modify/reconfigure the dashlet by selecting the 'Default' domain.

3.18 Data Migration from legacy VPFM and COM

Migration is the process of carrying over data from an older application to a newer version of Avaya Fabric Orchestrator (AFO). You can choose to migrate to AFO if you are currently using any legacy application as mentioned in the table below.

AFO Release 1.1 supports the migration from following legacy application versions.

Applications	Version number
Configuration & Orchestration Manager (COM)	3.0.2 and 3.1.3
Virtualization Provisioning Service (VPS)	1.0.2, 1.0.3, and 1.1
IP Flow Manager (IPFM)	2.0.2 and 2.1
Visualization, Fault & Performance Manager (VPFM)	3.0.3.1, 3.0.3.2, 3.0.3.3, and 3.0.4

Data migration tool can migrate following data on the AFO cluster.

- Users; The system migrates users associated with the System Administrator, UCM System Administrator, UCM Operator, and Network Administrator.
- Device credentials; The system can automatically restore the device credentials file from the backed up file or user can perform a manual restore.
- Application data

When the same user id or device credentials name is present in multipe legacy application instances being migrated to AFO, the values from the last instance of legacy application will overwrite the values from other instances of legacy applications.

Note:

Data migration tool does not support migration of the following data on the AFO Cluster:

- Custom roles created by the admin user in legacy application.
- Access control rules mapped to the particular user.
- Seeds created in the Configuration & Orchestration Manager (COM).

For further details on Data Migration, please refer to the document ***Deploying Avaya Fabric Orchestrator (NN48100-101).***

4 Avaya Fabric Orchestrator hardware and software requirements

There is no specific hardware (except for power cords) and software requirement for Avaya Fabric Orchestrator (AFO). AFO is shipped as a pre-configured hardware appliance. The appliance has all the required hardware and software for AFO to work properly.

Note:

The Avaya Fabric Orchestrator appliance server does not ship with AC power cords. You can use any 100–240V IEC 60320 AC power cord with a C13 connector that meets the regulations for your geographic region and operating environment.

Avaya recommends one of the following AC power cords. Avaya material codes are as follows:

Material Code	Description
AA0020062E6	POWER CORD IEC C13 TO NEMA 5-15P NORTH AMERICA (2.5M 10A/125V) ERS3500 ERS4500 ERS5500 ERS5900_450W VSP7000 VSP8000 SECURE ROUTER POE_INJECTORS
AA0020063E6	POWER CORD IEC C13 TO BS1363 UK (2.5M 10A/250V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS
AA0020064E6	POWER CORD IEC C13 TO CEE 7/17 EU (2.5M 10A/250V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS
AA0020065E6	POWER CORD IEC C13 TO CEI23-16 ITALY (2.5M 10A/125V) ERS3500 ERS4500 ERS5500 ERS5900_450W VSP7000 VSP8000 SECURE ROUTER POE_INJECTORS
AA0020066E6	POWER CORD IEC C13 TO GB2099 CHINA (2.5M 10A/250V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS
AA0020067E6	POWER CORD IEC C13 TO BS546 INDIA (2.5M 10A/250V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS
AA0020068E6	POWER CORD IEC C13 TO AS 3112 AUSTRALIA (2.5M 10A/250V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS
AA0020069E6	POWER CORD IEC C13 TO JIS 8303 JAPAN CNS-10917 TAIWAN (2.5M 12A/125V) ERS3500 ERS4500 ERS5500 VSP7000 SECURE ROUTER POE_INJECTORS

4.1 Other software requirements

The following software is required by an administrator to connect to the AFO appliance and move files (such as backup archive, log archive) to and from the appliance.

- SCP software, such as WinSCP on the client machine used by the administrator
- An SSH client, such as puTTY on the client machine used by the administrator

5 AFO Release 1.1 device support

The following devices are supported in AFO release 1.1 (Versions in **bold** are those for which support was newly introduced in AFO 1.1 release).

***** - indicates support is not completely verified yet.

Device	Software Releases
APLS (Private Label Switch)	**4.3.1, 6.0***
Virtual Services Platform 4000	3.0, 3.0.1, 3.1, 4.0, 4.0.40, 4.0.50, 4.1, 4.2, 4.2.1, **4.2.2, 4.2.3,** 5.0**, 5.1, 5.1.1, 6.0***
Virtual Services Platform 7200	4.2.1, **4.2.2, 4.2.3,** 5.0, **5.1, 5.1.1, 6.0***
Virtual Services Platform 8000	4.0, 4.0.1.1, 4.1, 4.2, 4.2.1, **4.2.2, 4.2.3,** 5.0, **5.1, 5.1.1, 6.0***
Virtual Services Platform 9000	3.0, 3.1, 3.2, 3.3, 3.4, 3.4.5.0, 4.0.1, **4.1, 4.1.1**
Ethernet Routing Switch 8600 & 8800 including the following hardware: 8681XLW module, 8681XLR module, 8616GTE module, 8672ATME MDA, 8608GBM module, 8608GTM module, 8632TXM module, 8648TXM module, 8672ATMM module, 8683POSM module.	4.0, 4.1, 5.0, 5.1, 7.0, 7.1, 7.1.3, 7.1.5, 7.2, 7.2.10, 7.2.13, 7.2.14.x, 7.2.15
Virtual Services Platform 7000 (70XX)	10.1, 10.2, 10.2.1, 10.3, 10.3.1, 10.3.2, 10.3.3, **10.4**
Ethernet Routing Switch 5900	7.0, **7.0.1, 7.1, 7.2**
Ethernet Routing Switch 5600	5.1, 6.0, 6.1, 6.2, 6.3, 6.6, 6.3.4**, 6.3.5, 6.3.6**, 6.6.1, **6.6.2, 6.6.3**
Ethernet Routing Switch 5500	5.1, 6.0, 6.1, 6.2, 6.3, 6.6, 6.3.4, **6.3.5, 6.3.6**, 6.6.1, **6.6.2, 6.6.3**
Ethernet Routing Switch 4900	**7.1, 7.2**
Ethernet Routing Switch 4800	5.2 , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, **5.7.2, 5.7.3,** 5.8, **5.8.2, 5.8.3,** 5.9, **5.9.2**
Ethernet Routing Switch 4500	5.2 , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, **5.7.2, 5.7.3**

Device	Software Releases
Ethernet Routing Switch 3500	5.0, 5.0.1, 5.0.2, 5.1, 5.1.1, **5.1.3,** 5.2, **5.2.3, 5.3, 5.3.1, 5.3.2**
Ethernet Routing Switch 2500	4.1.x, 4.2, 4.3, 4.4
Ethernet Routing Switch 1600	2.1.5.x, 2.1.6.x
WLAN	23xx, AP 23xx
WLAN 9100 WOS + AP	7.5.6
Belden	6.0.2

Note:

1. Following is a list of SMGR traps prior to v7.0.1 that will not get correlated in AFO 1.1

avAuraSysMgrMemErr	.1.3.6.1.4.1.6889.2.35.0.204
avAuraSysMgrMemCLR	.1.3.6.1.4.1.6889.2.35.0.205
avAuraSysMgrCpuErr	.1.3.6.1.4.1.6889.2.35.0.206
avAuraSysMgrCpuCLR	.1.3.6.1.4.1.6889.2.35.0.207
avAuraSysMgrDiskErr	.1.3.6.1.4.1.6889.2.35.0.208
avAuraSysMgrDiskCLR	.1.3.6.1.4.1.6889.2.35.0.209
avAuraSysMgrHttpErr	.1.3.6.1.4.1.6889.2.35.0.210
avAuraSysMgrHttpCLR	.1.3.6.1.4.1.6889.2.35.0.211
avAuraSysMgrSwapErr	.1.3.6.1.4.1.6889.2.35.0.212
avAuraSysMgrSwapCLR	.1.3.6.1.4.1.6889.2.35.0.213

2. "Install required plugins" option in Device Plugin Management view requires the first 3 decimal numbers of device software version and the corresponding EDM plugin version to match. If it does not, then the corresponding plugin should be installed manually using the "Install plugin" option.

6 Release distribution and license information

Avaya Fabric Orchestrator Release 1.1 is distributed as a hardware appliance. It is also available as an upgrade bundle for existing AFO 1.0 appliances.

AFO has the following licensing scheme:

Code	Description	Long Description
700510943	AFO APPLIANCE STARTER KIT	Avaya Fabric Orchestrator (AFO) Appliance Starter Kit. AFO is a unified network management appliance delivering full FCAPS functionality of Avaya networking products.
382178	AFO LICENSE FOR 1500 NODES	Avaya Fabric Orchestrator (AFO) License to manage 1500 nodes. Requires 700510943.
382179	AFO LICENSE FOR 5000 NODES	Avaya Fabric Orchestrator (AFO) License to manage 5000 nodes. Requires 700510943.
382480	AFO UPGRADE FROM 1500 TO 5000	Avaya Fabric Orchestrator (AFO) License to upgrade from 1500 nodes to 5000 nodes. Requires 700510943 and 382178.
382481	COM 250 TO AFO UPGRADE	License to upgrade from COM Enterprise 250 (AH2735003) to Avaya Fabric Orchestrator (AFO) Starter Kit & 250 node license. Requires 700510943.
382482	COM 1200/1500 TO AFO UPGRADE	License to upgrade from COM Enterprise 1200 or 1500 to Avaya Fabric Orchestrator (AFO) 1500. Requires 700510943. Need one of the following COM Licenses to qualify: AH2735004, AH2735005, AH2735013-3.0, AH2735014-3.0, AH2735013-3.1, AH2735014-3.1
382483	COM & VPFM TO AFO UPGRADE	Combo License to upgrade from COM Enterprise 250 (AH2735003) AND VPFM Base (AH3313109) to Avaya Fabric Orchestrator (AFO) Starter Kit & 250 node license. Requires 700510943.
382484	COM & VPFM TO AFO 1500 UPGRADE	Combo license to upgrade from COM Enterprise 1200/1500 AND VPFM Incremental (AH3313111) to AFO 1500. Requires 700510943. Need one of the following COM licenses to

Code	Description	Long Description
		qualify:AH2735004,AH2735005, AH2735013-3.0, AH2735014-3.0, AH2735013-3.1, AH2735014-3.1
382485	VPFM BASE TO AFO UPGRADE	License to upgrade from VPFM Base (AH3313109) to to Avaya Fabric Orchestrator (AFO) Starter Kit & 250 node license. Requires 700510943.
382486	VPFM INCREMENTAL 2000 TO AFO UPG	License to upgrade from VPFM Incremental (AH3313111) to Avaya Fabric Orchestrator (AFO) 1500. Requires 700510943
382487	VPFM ENTERPRISE TO AFO 5000 UPGRADE	License to upgrade from VPFM Enterprise (AH3313113) to Avaya Fabric Orchestrator (AFO) 5000. Requires 700510943.
382488	AFO ADV MONITORING FOR STARTER KIT	License to add advanced discovery and monitoring functionality to AFO Starter Kit (250 nodes). Functionality includes network baselining, advanced actions, dashboard builder and many other features. Requires 700510943 and any 250 node license.
382489	AFO ADV MONITORING FOR 1500 NODES	License to add advanced discovery and monitoring functionality to AFO for 1500 nodes. Functionality includes network baselining, advanced actions, dashboard builder and many other features. Requires 700510943 and any 1500 node license.
382490	AFO ADV MONITORING FOR 5000 NODES	License to add advanced discovery and monitoring functionality to AFO for 5000 nodes. Functionality includes network baselining, advanced actions, dashboard builder and many other features. Requires 700510943 & 5000 node license.
382491	AFO ADV MONITOR FR 1500 to 5000 UPG	License to upgrade advanced discovery and monitoring functionality in AFO from 1500 to 5000 nodes. Requires 382489.
383569	AFO LICENSE FOR 250 NODES	Avaya Fabric Orchestrator (AFO) License for Appliance Starter Kit - 250 nodes. Requires 700510943.
390768	**AFO MONITORING LIC FOR ADDL 10K NODE**	**License to monitor additional 10,000 nodes in AFO. Requires 382179 or 382480.**

Code	Description	Long Description
390769	**AFO LICENSE FOR HIGH AVAILABILITY**	**High Availability license for AFO. Requires 700510943.**

The last two licenses (**in bold**) are new for AFO Release 1.1; others are same as in AFO Release 1.0.

7 Installation procedure

See *Getting started and locating the latest software and product release notes for Avaya Fabric Orchestrator* (NN48100-102) for getting started once you receive the appliance.

See *Deploying Avaya Fabric Orchestrator* (NN48100-101) for Avaya Fabric Orchestrator installation and configuration information.

8 Known problems and workarounds

The following table provides the details of known issues in this release and workarounds, if any.

Issue ID	Component	Problem	Workaround (if any)
FABRICMGR-1061	Deployment	Delete and Backspace keys cannot be used in the console during the appliance configuration	Enter a special character (#,$,*..) and pressing ENTER will invalidate the current option and ask for entering new inputs.
FABRICMGR-2070	Network Discovery	Discovery abort takes more time (about 30mins) after licensed node limit is reached	
FABRICMGR-3167	Network Topology	Custom-monitoring may not get triggered if the customization is modified multiple times	From the Network Discovery view, perform a “stop monitoring” followed by a “start monitoring” on the domain.
FABRICMGR-3920	Cluster VMs	No warning or error message if a user tries to login to any VM when max session limit is reached	The problem is seen when establishing SSH sessions to any of the VM in AFO cluster using Putty. Workaround is to make sure that the “Close window on exit” option in Putty is set to “Never”.
FABRICMGR-3927	Network Topology	Network Panel in Topology page occasionally freezes, not letting the device icons to be clickable.	Press the manual refresh button on the topology page.
FABRICMGR-3983	Network Events	Events page is not showing any data after launching it second time	Drag the browser page outward slightly from the lower right hand corner.
FABRICMGR-4128	ADS	Certificate error when launching ADS in Firefox	Try launching ADS from IE
FABRICMGR-4148	Security	RealVNC 5.3.x and above is not supported for VM console	Use RealVNC 4.x, UltraVNC or TightVNC

Issue ID	Component	Problem	Workaround (if any)
FABRICMGR-4169	Dashboard	IE does not reflect changes done to dashboard widgets in FF browser	Following settings needs to be done in IE browser - Select Tools >> Internet Options. - Click the 'Settings' button in Browsing History. - Select the 'Every time I visit the webpage' radio button. - Click OK to close the Settings dialog. - Click OK to close the Internet Options dialog. - Set the Disk space to use (1024)
FABRICMGR-4314	Network Discovery	When Network Discovery data is erased in the 'Default' domain, Configuration inventory data doesn't sync with Default domain data.	Click on 'Reload' on Configuration Network Map page, it will sync up after the operation completes
FABRICMGR-4373	Network Discovery	When system is in quiesce state, nothing happens if discovery start button is pressed.	Though no feedback is given to the user, the requested discovery is queued.
FABRICMGR-4492	Network Response	Continuous actions will be triggered if Event Types "Self Event" is selected when creating a Response	Exclude 'Action Event', 'Action Failure' and 'Client Connection Failure' sub-events from 'Self Events'.
FABRICMGR-4493	Network Events	"Go to Device" command opens schematic on Events page	Refresh the entire page (can use F5).
FABRICMGR-4624	Configuration Network Map	Configuration status bar does not get updated immediately following upgrade to AFO 1.1	To see the updated status bar, perform a Reload in Configuration → Network Map view.

9 Resolved issues in AFO Release 1.1

The following table provides the details of issues that have been resolved in AFO 1.1.

Issue ID	Component	Problem	Comment (if any)
FABRICMGR-3534	Monitoring	High CPU events displaying for ERS 4000 and 5000	
FABRICMGR-3557	Configuration Device Software Management	AFO 1.0 SVU sporadically fails on upgrades for ERS 4K's and 5K's when using ssh	
FABRICMGR-4238	Configuration	Cannot clear BCM inventory; Clearing domain devices does not clear BCM inventory	Device Software Management (a.k.a BCM) inventory will use the Configuration Inventory
FABRICMGR-4345	Netwrok Discovery	Discovery of network using seed group with both subnet seeds and router seeds is taking very long (>24 hours)	

10 Operational notes

This section provides details of operational considerations to follow while using AFO.

10.1.1 Configuration and Device Software Management

- **Reload** in Configuration Network Map synchronizes the configuration inventory data with data from Network Discovery
- **Device Software Management** related backed up files will be located under `/opt/avaya/afo/shared/config/`
- **File Inventory** related backed up files will be located under `/opt/avaya/afo/shared/config/FileInventory/`
- VSP 7000 device limitations affecting configuration functionality:
    - TACACS settings and Web Password settings related SNMP MIBs are not supported in VSP 7000 series switches. These operations result in a `noCreation` SNMP error.
- VSP 7000 configuration support limitations:
    - Inventory Manager actions can cause error (`noCreation` SNMP error) for ASCII config file upload/download for VSP 7000 series switches. Inventory Manager binary config upload/download may require increasing the SNMP timeout in the preferences to 10 sec or more. (Applies to VSP 7000 release 7.2.x and older).
- Changing snmp-community string via Device Password Manager (DPM) portlet of Device Software Management only changes the default snmpv1-read and snmpv1-write community string which have the indexes:-
  1) first (group:v1v2grp and security name: readview) for snmp-read
  2) second (group:v1v2grp and security name: initialview) for snmp-write

  In case, in the absence of these default entries on the device, community string change via DPM may not happen properly. As of now DPM takes care of only the changes to these default entries, and if default entries are not present appropriate error message will be thrown in the logs, once the DPM task is activated.

  Affected device family : VSP 4K, VSP72xx, VSP8K, APLS and VSP 9K

10.1.2 VOSS device software management backup and restore

On VOSS software version 4.2 and 4.2.1.0, SCP is not supported by the devices. Device Software Management backup and restore operations on SSH fail with Error: /opt/avaya/afo/shared/config/BackupAndRestore/archive/<backup_directory_name>/config.cfg (No such file or directory).

If Device Software Management operations are needed, Avaya recommends use of telnet credentials for the VOSS devices on software version 4.2 & 4.2.1.0.

10.1.3 Network Discovery and Network Topology

1. A `Discovery Partially Successful` status means that a full discovery could not be performed due to license not being available or one of the discovery seeds not being reachable.
2. Discovery uses the write community strings to discover the device if both read and write community strings are provided, It will not fall back to read community strings if write fails.
3. The SPBM view in Network Topology uses SNMP write access to retrieve the SPB L2 MIBs.

10.1.4 Virtualization

1. If there are changes to the device hardware (adding or removing devices from the network, adding or removing units from a stackable), you need to complete the following tasks:
    a. Check if snmp is enabled on the new or existing ESX server and update the snmp and ssh credentials in AFO credential tab for ESX server. Below is the command to enable snmp.
        - `esxcli system snmp set –e yes`
        - `esxcli system snmp set –c public`
    b. AFO network discovery must be executed. Once the AFO Network discovery is completed successfully, AFO Virtualization Inventory Audit and Hypervisor connectivity is auto triggered.
    c. If new network devices are added to the network, then AFO Network discovery must be followed by a device reassignment (manage or unmanage) using AFO Virtualization Device Management.
2. AFO Virtualization Component does not support virtual machine configurations involving vApp.

3. AFO Virtualization supports the following options of Port Group VLAN IDs:
    a. vSwitch Port group
        - 1-4094 — You can define a rule using the specific VLAN ID as the PortGroup VLAN ID for this port group.
    b. dvSwitch Port group
        - VLAN — You can define a rule using the specific VLAN ID as the PortGroup VLAN ID for this port group
4. AFO Virtualization does not configure the network for EST and VGT mode settings. The network administrator must configure EST and VGT settings manually. If some of the VMs are designated to use EST mode, then the network administrator must manually configure the ports on both source and destination switches.
5. You cannot directly export an AFO Virtualization report to an HTML format using the **export report** feature. However, you can save the report in a HTML format using the **Print Report** feature. For more information, see *Virtualization Configuration for Avaya Fabric Orchestrator* (NN48100-503).
6. See *Virtualization Configuration for Avaya Fabric Orchestrator* (NN48100-503) for information about the vCenter events that AFO Virtualization can manage.
7. AFO Virtualization blocks the network traffic for a VM when used in EST mode
8. If one of the uplink is down amongst the available, AFO Virtualization shows failed in Monitor Event for the particular VM transaction.
9. While configuring rules based on a port group, best practice is to consider the port group name along with the port group VLAN ID.

AFO Virtualization Hot Migrate of VM is not detected after HA-DRS as a result of Host shutdown or physical failure.

11 Document list

The following are the documents available for AFO Release 1.1.

Item	Document Identification	Document Title
1	NN48100-100	Avaya Network Management Solution Description
2	NN48100-102 (A-852078 rev2)	Getting started and Locating the latest software and Release Notes for Avaya Fabric Orchestrator
3	NN48100-101	Deploying Avaya Fabric Orchestrator
4	NN48100-600	Administration using Avaya Fabric Orchestrator
5	NN48100-500	Network Monitoring using Avaya Fabric Orchestrator
6	NN48100-501	Network Configuration using Avaya Fabric Orchestrator
7	NN48100-504	IP Flow Configuration using Avaya Fabric Orchestrator
8	NN48100-502	Bulk Device Configuration Management using Avaya Fabric Orchestrator
9	NN48100-503	Virtualization Configuration using Avaya Fabric Orchestrator
10	NN48100-700	Avaya Network Management Traps and Trends Reference
11	NN48100-701	Avaya Network Management Supported Devices Reference
12	NN48100-702	Troubleshooting Avaya Fabric Orchestrator
13	N/A	Avaya Fabric Orchestrator Northbound API user guide (HTML zip)
13	N/A	Avaya Fabric Orchestrator Release Notes

Documents download links:

https://support.avaya.com/products/P1618/fabric-orchestrator

https://support.avaya.com/documents/ ; Enter AF0 as the product name.

12 Technical support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.