# Avaya Visualization Performance and Fault Manager Discovery Best Practices

Release 3.0.3
NN48014-105
Issue 04.02
January 2015

**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 may generally make available to users of its products and Hosted Services. 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 Avaya hardware and software. 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 or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

**Licenses**

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

**Licence types**

Designated System(s) License (DS). End User may install and use each copy or an Instance 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, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

**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” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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 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, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, 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.

**Third Party Components**

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service 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”). As required, 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 products, Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. 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 or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**Trademarks**

Avaya Aura® is a registered trademark of Avaya Inc.

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation, Hosted Service(s), 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, Hosted Service(s) 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. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

**Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

**Contact Avaya Support**

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

# Contents

# Chapter 1: Introduction

**Related Links**

Related resources on page 5

## Purpose

This document describes the best practices guidelines for discovery using Avaya Visualization Performance and Fault Manager (Avaya VPFM) to discover your network.

This document is intended for administrators who are able to accurately discover your network at a high level using Avaya VPFM.

## Related resources

**Related Links**

Introduction on page 5
Documentation on page 5
Training on page 6
Viewing Avaya Mentor videos on page 6
Support on page 7

### Documentation

See the following related documents:

| Title | Purpose | Link |
|---|---|---|
| *Avaya Visualization Performance and Fault Manager — Common Services Fundamentals Unified Communications Management* (NN48014–100) | Fundamentals | http://support.avaya.com |

| Title | Purpose | Link |
|---|---|---|
| *Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Fundamentals* (NN48014–101) | Fundamentals | http://support.avaya.com |
| *Avaya VPFM Traps and Trends* (NN48014–103) | Reference | http://support.avaya.com |
| *Avaya VPFM Supported Devices, Device MIBs, and Legacy Devices* (NN48014–104) | Reference | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager Installation* (NN48014–300) | Installation | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Installation* (NN48014–301) | Installation | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager Quick Start* (NN48014–302) | Quick Start | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager Configuration* (NN48014–500) | Administration | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network* (NN48014–501) | Deployment | http://support.avaya.com |
| *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014–700) | Administration | http://support.avaya.com |

**Related Links**

Related resources on page 5

## Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com/.

**Related Links**

Related resources on page 5

## Viewing Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

### About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

**Related Links**

Related resources on page 5

# Support

Go to the Avaya Support website at http://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.

**Related Links**

Related resources on page 5

# Chapter 2: New in this release

## Features

See the following sections for information about features changes.

### New and updated device support

The following Avaya data devices are added:

- ERS 3500 v5.1.1
- VSP 4000 series v3.0.1.0
- Avaya SRA firewall Sw:1.0.1

The following Avaya data devices are updated:

- VSP 7000 series v10.2.1

The following Avaya Voice Devices (Aura VE) are added:

- Avaya Aura Messaging (AAM) release v6.3
- Avaya Aura Contact Center Control Manager (ACCCM) release 7.0
- Avaya Navigator (A-NAV) release 4.1
- Avaya Contact Recorder (ACR) release 12.0
- Contact Center (CC) Elite Multi Channel (EMC) release 6.3
- Avaya Call Management System (CMS) release 17.0
- Avaya Session Border Controller (Sipera SBC) release 6.2
- Avaya G860 Media Gateway (M3K) release 6.2
- Avaya Meeting Exchange (MX) release 6.2
- Avaya Aura Experience Portal (AAEP) release 6.0.2

The following Avaya Aura Virtual Environment (Aura VE) devices are updated:

- Presence Service (PS) release 6.2.2

- Agile Communication Environment (ACE/AIE) release 6.3
- Avaya Application Enablement Services (AES) release 6.3.1
- Avaya CM duplex or simplex release 6.3.2
- Session Manager release 6.3.4
- System Manager release 6.3.4
- Utility Services (US) release 6.3

The following third party devices are updated:

- VMware ESXi v5.1
- VMware VSphere v5.1
- VMware VCenter v5.1

The following third party devices are added:

- Acme Packet Net-Net 4000 (SBC) release 6.3
- Sentry Smart CDU power supply firmware 7.0j

# Upgrades

You can upgrade directly from VPFM release 3.0.1 to release 3.0.3, or from release 3.0.2 to release 3.0.3. If you want to upgrade from a release older than 3.0.1, you must first upgrade to release 3.0.1, then upgrade to release 3.0.3.

### Upgrade on a VM environment

When you upgrade VPFM from a release older than VPFM 3.0.2 to release 3.0.3 on a VM environment, Unified Communication Management (UCM) removes the license associated with the application from the license file. Therefore, make a copy of the license file before you perform the upgrade; you can use the copy of the license file to return to the older release, if required.

# VPFM hardware requirements

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports a 64-bit Linux system using a 64-bit VPFM application.

# Client browsers

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 supports the following browsers:

- Internet Explorer (IE), versions 9 and 10.
- Mozilla Firefox (FF), versions 24 and 25.

## Dashboard enhancements

Enhancements to the Avaya Visualization Performance and Fault Manager (VPFM) dashboard include the following:

- addition of a Power Savings dashboard that displays dashlets containing information about total network power savings and top switch watt reduction.

## Reporting enhancements

Enhancements to Avaya Visualization Performance and Fault Manager (VPFM) reporting include the following:

- introduction of Pod specific Inventory Reports
- addition of three new Event browser columns to display Pod specific information:
  - Host
  - VM Host
  - Pod
- introduction of Power Savings reporting
- ability to aggregate statistics per stack and per domain

## Discovery features

Avaya Visualization Performance and Fault Manager (VPFM) 3.0.3 introduces the following discoveries:

- discovery of Unified Communications as a Service (UCaaS) Collaboration Pod — discovering and visualizing the UCaaS Collaboration Pod as a single logical unit
- discovery of Contact Center as a Service (CCaaS) Collaboration Pod — discovering and visualizing the CCaaS Collaboration Pod as a single logical unit
- discovery of UCaaS and CCaaS Collaboration Pod components
  - VSP 4000 series
  - Avaya Aura Messaging (AAM)
  - Avaya SRA firewall Sw : 1.0.1
  -
- discovery of UCaaS and CCaaS Collaboration Pod applications
  - Call Management System (CMS) VE and correlated traps
  - Avaya Aura Experience Portal (AEP) and correlated traps

  - Elite Multi Channel (EMC) and correlated traps
  - Work Force Optimization (WFO)
  - A-NAV
  - Avaya Contact Center Control Manager (ACCCM)
  - Meeting Exchange (MX)
  - Avaya Contact Recorder (ACR)
- discovery of third party devices
  - Avaya Media Gateway G860: software version: AudioCodes MEDIANT5000; sw version 5.8.103
  - Acme Packet Net-Net Session Border Controller (SBC)
  - Sipera Session Border Controller (SBC)
  - Sentry smart PDU power supply
- discovery of additional phone properties (for managed phones that support SNMP)
  - serial numbers of phones
  - OEM model name

Avaya VPFM 3.0.3 introduces the following Advanced Discovery Options:

- Abort hung queries after (minutes)
- SNMP timeout (seconds)
- Max SNMP retries
- Estimated max request time (2-126)

## Fault and diagnostics enhancements

Enhancements to fault and diagnostics include the following:

- VoIP Fault performance management now displays trunk utilization on CM, SBC, and gateways.

## Supporting operating systems

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 supports the following operating systems:

- Windows Server 2003 Standard or Enterprise Service Pack 2, 32-bit or 64-bit version. VPFM supports Windows 2003 through upgrade only.
- Windows Server 2008 Enterprise and Datacenter editions R2 Service Pack 2, 32-bit or 64-bit versions.

- Red Hat Enterprise Linux 5.6, 32–bit or 64-bit. VPFM supports RHEL only.

## Topology and GUI enhancements

Avaya Visualization Performance and Fault Manager (VPFM) release 3.0.3 displays an extension pod shown in the topology as an aggregate icon.

Avaya VPFM introduces the following enhancements to the central browser panel:

- ability to launch VMware vCenter by right clicking on a virtual machine (VM) host

  **Note:**

  Beginning with Release 3.0.3, you must manually set the IP address of vCenter into action after the VPFM installation. You must manually edit the sample action named "VMware vCenter" replacing the host name in the URL with the name or IP address of a real vCenter server. You can configure one vCenter server to manage all VMs on all VHs, i.e., the same vCenter server can be the destination for all VM hosts.

- ability to launch EMC Unisphere by right clicking on a storage device

Avaya VPFM release 3.0.3 adds the following enhancements to the SNMP MIB Query page menu bar:

- **Switch to columns** menu item
- **Clear** menu item
- history to SNMP MIB query is maintained with multiple tab support

# Other information

See the following sections for information about changes that are not feature-related.

## UCaaS Pod OVA and CCaaS Pod OVA

This release introduces the Unified Communications as a Service (UCaaS) Collaboration Pod OVA version of VPFM 3.0.3 and the Contact Center as a Service (CCaaS) Collaboration Pod OVA version of VPFM 3.0.3.

# Chapter 3: Avaya VPFM discovery philosophy

This chapter describes the philosophy of Avaya Visualization Performance and Fault Manager (Avaya VPFM) discovery.

### Heterogeneous

Avaya VPFM is a best-in-class discovery and monitoring solution for networks consisting of Avaya devices, and devices from various vendors.

### Standards based

To achieve heterogeneity, Avaya VPFM is completely standards based in its approach to discovery. That is, VPFM uses MIB-2 Management Information Bases (MIB) as opposed to enterprise specific MIBs whenever possible. For more information, see MIB tables for a device discovery on page 20.

### Easy segregation and management

Avaya VPFM uses domains to contain the topology and monitoring data for a discovery. You can create multiple domains in VPFM, which permits you to discover and manage portions of your network independent of other portions.

### Adapting to your network

If devices do not implement standard link discovery protocols, Avaya VPFM uses a weighted algorithm for inferring links. The more traffic that is present between these devices, which equates to more entries in the neighboring switches Forwarding database (FDB) tables, the better the accuracy with which VPFM performs the inference.

# Chapter 4: Plan your discovery

To achieve the best results from Avaya Visualization Performance and Fault Manager (Avaya VPFM), it is important to plan your discovery before starting a discovery with Avaya VPFM.

The following is a list of points to consider when planning a discovery.

- Decide on the parts of the network you want to discover.
- Choose a seed router, any layer-3 device, from which all parts of your network are reachable either directly or indirectly.
- If a subnet does not have any layer-3 device, provide the subnet itself as a seed.
- Avaya VPFM can perform WAN crawls across the supported devices; for example, Contivity devices and Avaya Secure Routers. But, if the connectivity is across a service provider network, then you must provide a seed device from the remote networks, in addition to the seed you have already specified.
- Specify how far you want the discovery to reach out to by providing subnet limits.
- If there are any device types or specific devices you want to exclude from discovery, specify these in the exclusions criteria.
- Make sure that autotopology, such as SynOptics Network Management Protocol (SONMP) and Cisco Discovery Protocol (CDP), is enabled on all the devices that support these protocols.
- If you have an out-of-band network setup for management, ensure that the devices Address Resolution Protocol (ARP) cache reflects the out-of-band addresses. Otherwise, VPFM tries to access the devices using the in-band addresses, if these are present in the ARP cache.

# Chapter 5: Discover your network

To accurately discover your network with Avaya Visualization and Fault Manager (Avaya VPFM) at a high level, perform the following procedures in the order they appear.

- Provide the Simple Network Management Protocol (SNMP) and Telnet device credentials in Avaya Unified Communications Management (Avaya UCM). For more information, see Supplying credentials for a discovery on page 16.
- Create a discovery domain and provide the discovery seed. For more information, see Configuring a seed for a discovery on page 17.
- Configure the subnet limits and any exclusions. For more information, see Excluding a device from discovery on page 19.

For other information relevant to discovering your network, see the following sections.



**Related Links**


Enabling the Net-SNMP Service on page 23

Discovery of EMC Storage on page 25

SPBM diagnostic tests for VSP 7000 devices on page 35

# Supplying credentials for a discovery

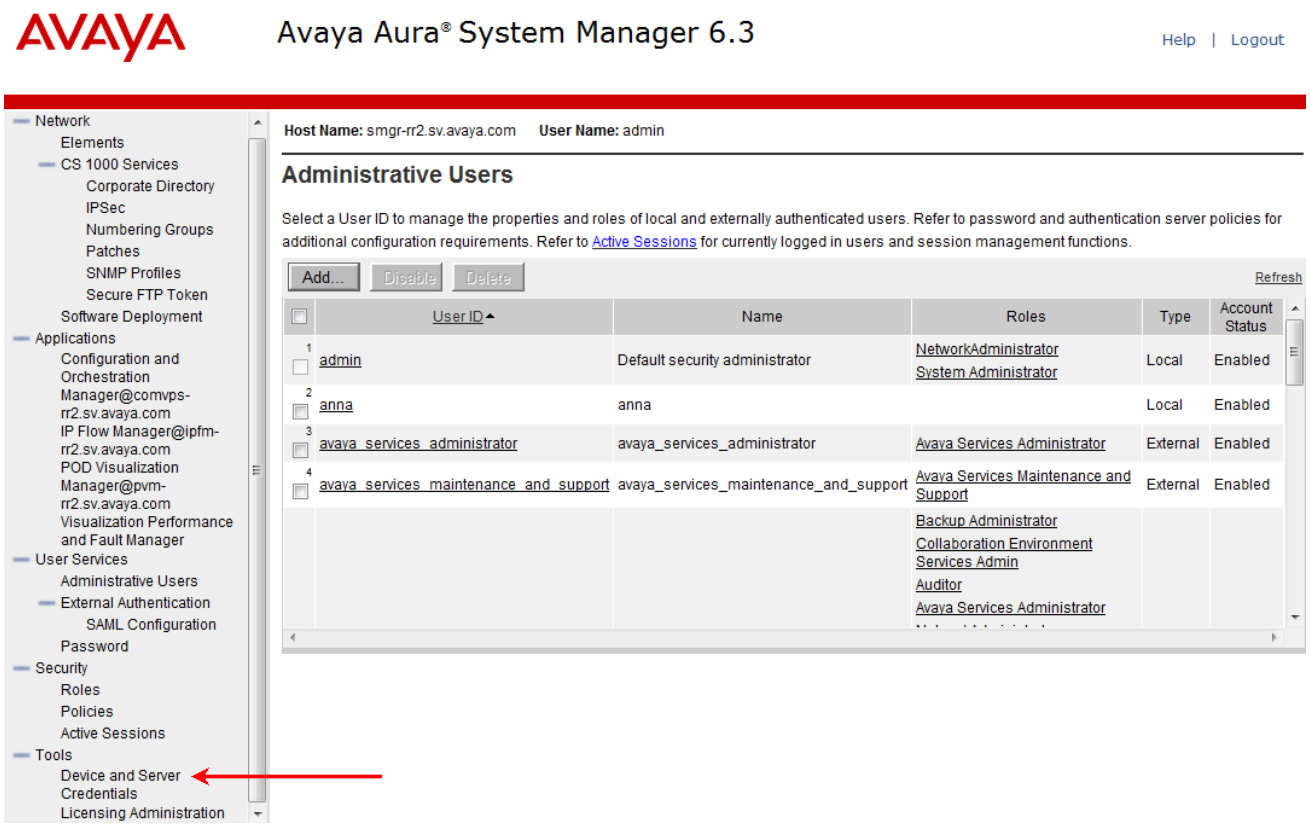
## About this task

Before starting a discovery, you must supply SNMP, and in some cases, Telnet credentials for all the devices that you are required to discover and manage using Avaya VPFM.

**Note:**

The Avaya applications PS, US and ACE do not support SNMP. For IP availability status check, VPFM only provides support for ICMP ping, and does not send an SNMP query to the server where the applications reside.

To supply credentials for a discovery, navigate to the Avaya UCM Device Credentials page, as shown in the following figure.




To discover the links between ESXi hosts and vCenter in the pod, enter the CIM credentials of the Vcenter and the ESXi hosts in the Credentials Editor. The CIM username and password are the same as the SSH username and password.

**Note:**

Avaya VPFM uses a seed to begin the search for devices within your network, using an Address Resolution Protocol (ARP) cache, and communicates with all these devices to discover their properties and connectivity. Therefore you must supply credentials for your discovery seed, and for all devices within your network that you are required to discover and manage with VPFM.

No credentials are provided by default (for example, SNMP v1/v2c credentials of public/private for *.*.*.* must be entered).

To enable an SNMP v3 based discovery, make sure that you provide only the SNMP v3 credentials for the device. If you provide SNMP v1 credentials, VPFM uses only the v1 credentials during discovery.

Avaya VPFM requires SNMP (v1, v2c, and v3) credentials to discover most devices in your network. In some cases, VPFM goes beyond SNMP and uses other protocols such as, Telnet, Common Information Model (CIM), Port Scanning, and Windows logon credentials for a more accurate discovery.

Avaya VPFM uses Telnet for discovering and associating Internet Protocol (IP) deskphones to their registered Avaya Communication Server 1000 (Avaya CS 1000) Signaling Servers. Avaya VPFM uses the CIM for associating IP deskphones to their registered Avaya Business Communications Manager (Avaya BCM) systems. For discovery of Wireless Local Area Network (WLAN) access points and IP deskphones, VPFM scans for open ports on those devices. For more information, see Voice application discovery on page 32.

**Important:**

After installation, Avaya Communication Server 1000 (Avaya CS 1000) uses the default name, System Name. To display the Internet Protocol (IP) deskphones that are registered to the Avaya CS 1000 in VPFM, you must change the default name to a unique name. If you have a large Avaya CS 1000 deployed, you must increase the discovery thread size and the SNMP timeout values. For assistance, contact Avaya Support: http://support.avaya.com.

For discovering Windows servers, VPFM uses the Windows logon credentials provided.

**Note:**

If you change the device credentials any time after discovery has been completed, a rediscovery must be performed in order for VPFM features to work properly on the device.

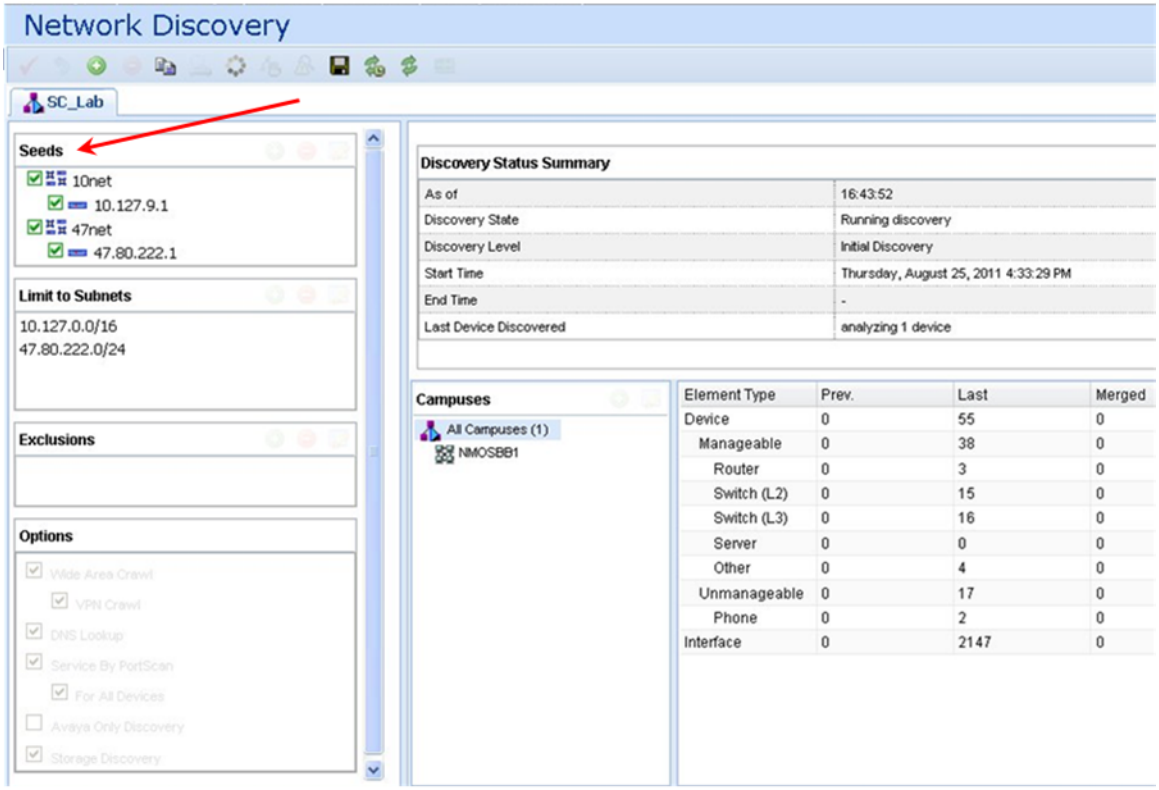
**Important:**

To discover file systems and logical volumes for AAM, SSH timeout must be increased. For assistance, contact Avaya Support: http://support.avaya.com.

# Configuring a seed for a discovery

## About this task

To discover your network with Avaya VPFM, provide the seed routers or seed subnets that VPFM uses to contact the devices requiring discovery. The discovery seeds can accompany any exclusions that are provided in the Discovery Configuration page as shown in the following figure.




**Note:**

Avaya recommends that you do not use overly large subnet seeds for discovery.

Avaya recommends that you use router seeds, and only use subnet seeds in situations when they are the actual LAN in the network or when a layer-3 device is not present in the network to be discovered.

If you specify more than one subnet-based seed, some of subnet-based seeds are ignored if one of the seeds results in the discovery of a router which has routing interfaces in the other subnets.

For example: The subnet seeds specified are 10.127.1.0/24, 10.127.2.0/24 and 10.127.3.0/24. If the first seed results in the discovery of a router, such as 10.127.1.1 which also has an interface 10.127.3.1, then the 10.127.3.0/24 is ignored. Avaya VPFM discovers the network using the routing interface ARP entries.

You must specify a subnet-based seed or provide other router seeds for the subnets you want discovered.

The following table outlines the recommended seeds based on the network topology.

| Topology | Recommended seed |
|---|---|
| Layered topology containing Core, Distribution and Access Switches | One of the core or distribution switches (must be a layer-3 switch or a router) |
| Pure Layer-2 network (no layer-3 device) | Provide the entire subnet as the seed; for example, 10.127.22.0/24 |

| Topology | Recommended seed |
| --- | --- |
| Remote networks without supported WAN routers (like Avaya Secure Router or Avaya VPN Gateway) | In addition to the seed for the main office, provide a seed in the remote site as well. |

In certain cases, providing multiple seeds creates multiple campuses, even for a flat network. If VPFM is unable to link all switches within an even topology, VPFM creates multiple campuses. To prevent VPFM from creating multiple campuses, combine the seeds within a seed group.

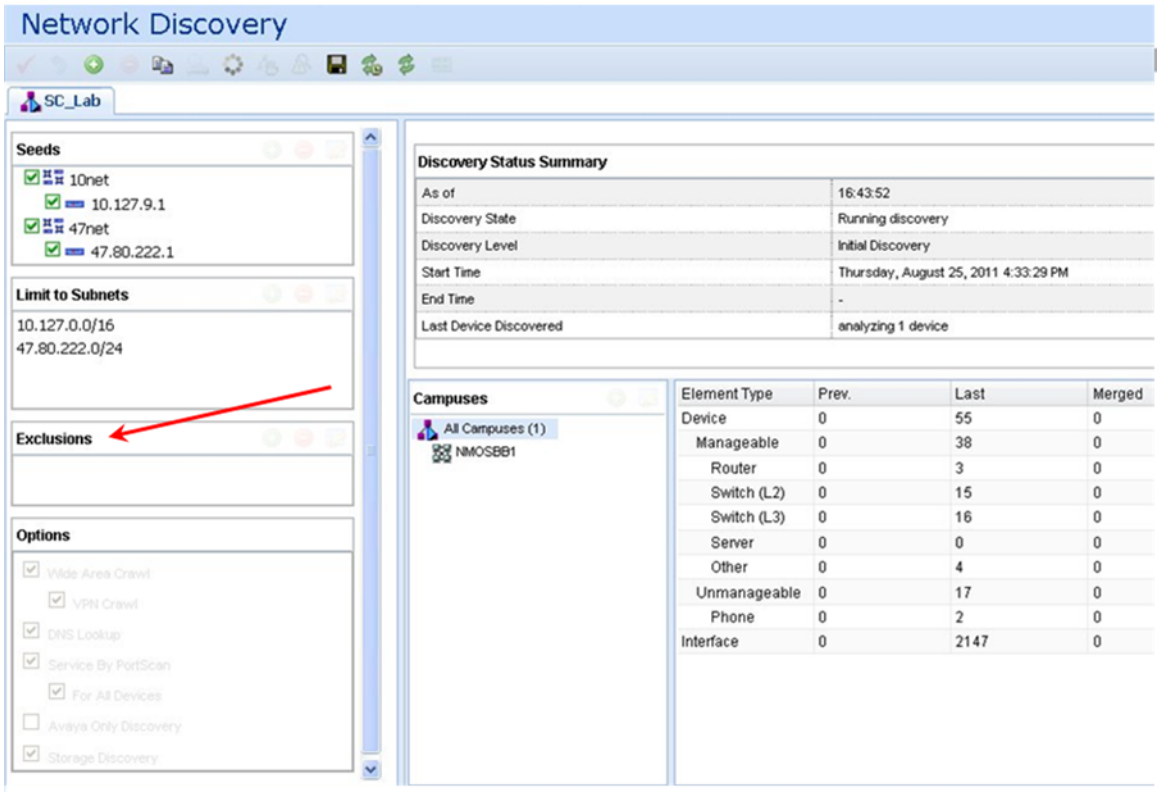
VPFM can accept devices that have only circuitless IP (CLIP) addresses as seed routers. CLIP addresses have 32-bit masks and are used in SPBm implementations. To enable accurate discovery of SPBm networks with one of the SPBm switches as seed, VPFM performs device discovery using entries in the SONMP table.

# Excluding a device from discovery

### About this task

In some situations, certain devices may need to be excluded from discovery. Reasons to exclude a device from discover include, bad SNMP agents that cause loops during discovery, devices that send incomplete traps that cause issues with the Avaya VPFM trap browser, and multiple Virtual Router Redundancy Protocol (VRRP) addresses showing up as unmanaged causing clutter on the Network Browser.

To exclude devices from discovery, in the Discovery Configuration page, provide the IP addresses of the devices, as shown in the following figure.




To exclude a device from discover, all the IP interfaces of the device must be in the exclusion list. If you do not enter all the interfaces in the exclusion list, a device intended for exclusion may be discovered if any of the other interfaces fall in the discovery range.

To prevent device circuits, containing VRRP IP addresses and other unmanaged devices, from appearing in the topology, specify Unmanaged Devices as an exclusion criteria for discovery.

# MIB tables for a device discovery

For Avaya VPFM to discover a device completely and reach out to other devices within the subnet, VPFM requires the following Management Information Bases (MIB) tables to be implemented on each device.

Avaya VPFM requires the following standard (MIB-2) MIB tables for a device discovery.

### Interfaces Table (ifTable)

Avaya VPFM uses the Interfaces Table (ifTable) for discovering physical interfaces (ports) of a device.

The following figure is an example of an Interfaces Table.

.mgmt.mib-2.interfaces.ifTable.ifEntry

| [ifIndex] | ifIndex | ifDescr | ifType | ifMtu | ifSpeed | ifPhysAddress | ifAdminStatus | ifOperStatus | ifLastChange | ifInOctets | ifInUcastPkts |
|---|---|---|---|---|---|---|---|---|---|---|---|
| .64 | 64 | 10/100BaseTX Port 1/1 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:00 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .65 | 65 | 10/100BaseTX Port 1/2 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:01 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .66 | 66 | 10/100BaseTX Port 1/3 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:02 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .67 | 67 | 10/100BaseTX Port 1/4 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:03 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .68 | 68 | 10/100BaseTX Port 1/5 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:04 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .69 | 69 | 10/100BaseTX Port 1/6 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:05 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .70 | 70 | 10/100BaseTX Port 1/7 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:06 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .71 | 71 | 10/100BaseTX Port 1/8 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:07 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .72 | 72 | 10/100BaseTX Port 1/9 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:08 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .73 | 73 | 10/100BaseTX Port 1/10 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:09 | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .74 | 74 | 10/100BaseTX Port 1/11 Name | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:0a | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |
| .75 | 75 | 10/100BaseTX Port 1/12 | ethernetCsmacd(6) | 1950 | 0 | 00:e0:7b:b0:48:0b | up(1) | down(2) | 0 days, 0:00:17.00 | 0 | 0 |

## IP Addresses Table (ipAddrTable)

Avaya VPFM uses the IP Addresses Table (ipAddrTable) for discovering all the IP interfaces of a device. In conjunction with the ifTable, VPFM uses the ipAddrTable to map IP addresses to actual physical interfaces (by using an index value in both tables).

Any mismatches or inability to associate an IP interface with a physical interface could result in inconsistent discoveries.

The following figure is an example of an IP Addresses Table.

.mgmt.mib-2.ip.ipAddrTable.ipAddrEntry

| [ipAdEntAddr] | ipAdEntAddr | ipAdEntIfIndex | ipAdEntNetMask | ipAdEntBcastAddr | ipAdEntReasmMaxSize |
|---|---|---|---|---|---|
| .8.8.8.1 | 8.8.8.1 | 2051 | 255.255.255.0 | 1 | 1500 |
| .10.4.20.12 | 10.4.20.12 | 320 | 255.255.255.0 | 1 | 1500 |
| .10.127.22.12 | 10.127.22.12 | 2049 | 255.255.255.0 | 1 | 1500 |

## ARP Cache (ipNetToMediaTable)

The ARP Cache (ipNetToMediaTable), is queried on all routing interfaces to find all IP addresses within a routing interface subnet (Layer-2). Avaya VPFM then tries to discover this set of IP addresses.

Address Resolution Protocol (ARP) cache entries are dynamic in nature and expire routinely if certain elements (mostly end nodes) are not discovered consistently.

The following figure is an example of an ARP Cache Table.

| .mgmt.mib-2.ip.ipNetToMediaTable.ipNetToMediaEntry | | | | |
|---|---|---|---|---|
| [ipNetToMediaIfIndex, ipNetToMediaNetAddress] | ipNetToMediaIfIndex | ipNetToMediaPhysAddress | ipNetToMediaNetAddress | ipNetToMediaType |
| .2049.10.127.22.1 | 402720769 | 00:80:2d:c7:1a:15 | 10.127.22.1 | dynamic(3) |
| .2049.10.127.22.2 | 402720769 | 00:e0:7b:88:9a:00 | 10.127.22.2 | dynamic(3) |
| .2049.10.127.22.3 | 402720769 | 00:80:2d:ac:9a:00 | 10.127.22.3 | dynamic(3) |
| .2049.10.127.22.12 | 2049 | 00:e0:7b:b0:4a:00 | 10.127.22.12 | other(1) |
| .2049.10.127.22.13 | 402655233 | 00:e0:7b:c9:5e:00 | 10.127.22.13 | dynamic(3) |
| .2049.10.127.22.90 | 402720769 | 00:01:02:74:0e:59 | 10.127.22.90 | dynamic(3) |
| .2049.10.127.22.102 | 402720769 | 00:e0:7b:a8:9a:00 | 10.127.22.102 | dynamic(3) |
| .2049.10.127.22.103 | 402720769 | 00:01:81:28:7e:00 | 10.127.22.103 | dynamic(3) |
| .2049.10.127.22.112 | 402720769 | 00:04:38:96:a2:00 | 10.127.22.112 | dynamic(3) |
| .2049.10.127.22.113 | 402720769 | 00:0e:40:03:92:00 | 10.127.22.113 | dynamic(3) |
| .2049.10.127.22.122 | 402655233 | 00:01:02:74:14:1f | 10.127.22.122 | dynamic(3) |
| .2049.10.127.22.133 | 403572737 | 00:01:02:73:fe:60 | 10.127.22.133 | dynamic(3) |
| .2049.10.127.22.255 | 2049 | ff:ff:ff:ff:ff:ff | 10.127.22.255 | other(1) |
| .2051.8.8.8.1 | 2051 | 00:e0:7b:b0:4a:01 | 8.8.8.1 | other(1) |
| .2051.8.8.8.2 | 402655235 | 00:e0:7b:c9:5e:01 | 8.8.8.2 | dynamic(3) |
| .2051.8.8.8.255 | 2051 | ff:ff:ff:ff:ff:ff | 8.8.8.255 | other(1) |

### Synoptics Auto-topology Table (s5EnMsTopNmmEosTable)

In addition to using the ARP cache for seeding discovery, VPFM also uses the entries in the SONMP table if the device supports SONMP.

| .private.enterprises.synoptics.products.series5000.s5EnMsTop.s5EnMsTopNmm.s5EnMsTopNmmTable.s5EnMsTopNmmEntry | | | | | | |
|---|---|---|---|---|---|---|
| [s5EnMsTopNmmSlot, s5EnMsTopNmmPort, s5EnMsTopNmmIpAddr, s5EnMsTopNmmSegId] | s5EnMsTopNmmSlot | s5EnMsTopNmmPort | s5EnMsTopNmmIpAddr | s5EnMsTopNmmSegId | s5EnMsTopNmmMacAddr | s5EnMsTopNmmChassisType |
| .0.0.10.127.45.20.0 | 0 | 0 | 10.127.45.20 | 0 | 00:24:b5:1f:64:01 | mWC8180(188) |
| .1.1.10.127.45.4.279 | 1 | 1 | 10.127.45.4 | 279 | 00:e0:7b:da:98:63 | mBayStack450(48) |

# Discovery of Avaya Aura components

Avaya Visualization and Performance Fault Manager (Avaya VPFM) automatically discovers Avaya Communication Manager (CM), Avaya System Manager (SM) , Avaya SMGR, Avaya CS 1000, Avaya Gateway, and IP Deskphones.

Discovery key features include the following:

- Router or Subnet seed for discovery
- Campus or branch office discovery
- Port scan during discovery detects services on servers
- Storage and file-system discovery

  **Note:**

  To discover the storage such as file systems, disks, and inodes of a host or server, you must provide the SSH credential of the Linux server, and for Windows, SNMP service must be enabled.
- Discovery of both managed and unmanaged devices

Avaya Aura discovery key features include the following:

- Discovery of CM, SM, SMGR and Gateways
- Discovery at application level

- Port scan during discovery detects services and process
- Discovery of Aura file-system
- Discovery of H.323 and SIP IP Phones
- Discovery of gateways and trunks

For Avaya Aura discovery of the CM, SM, SMGR, Media Gateways, and Avaya IP Phones, you must provide SNMP credentials. For association of the H.323 phones to the registered CM, VPFM gathers information using SNMP. For association of the SIP phones to the registered SM, you must provide SNMP and SSH credentials for the SM.

For a VM discovery, that identifies an IP address as a VM or VM host , VPFM does not require SNMP. A VM discovery uses the MAC information in the forwarding table of the connecting switch. However, if you want to manage the discovered VMs, for storage statistics and interface statistics, you must provide SNMP credentials.

# Enabling the Net-SNMP Service

Perform the following procedure to ensure the Net-SNMP service of the Avaya applications, for example WebLM, is enabled, and starts automatically, when the VM is restarted.

### Procedure

1. Log in as `su – root`.
2. Enter the following command:

   ```
   Service snmpd start
   ```

3. Enter the following command:

   ```
   chkconfig snmpd on
   ```

4. Enter the following command:

   ```
   reboot
   ```

### Related Links

Discover your network on page 15

# Discovery of Avaya Communication Manager

The following list outlines the Avaya Visualization Performance and Fault Manager (Avaya VPFM) discovery key features for the Avaya Communication Manager.

- Classifies the device type as Avaya Communication Manager
- Shows both physical and virtual interfaces

- Shows applications on the Avaya Communication Manager
- Shows services operating on the Avaya Communication Manager
- Launches the dashboard from all interfaces to start monitoring
- Provides icons in the navigation tree for easy navigation
- Shows or hides events and properties

For more information about the discovery of Avaya Communication Manager, see *Avaya Visualization Performance and Fault Manager Fault and Performance Management* (NN48014–700).

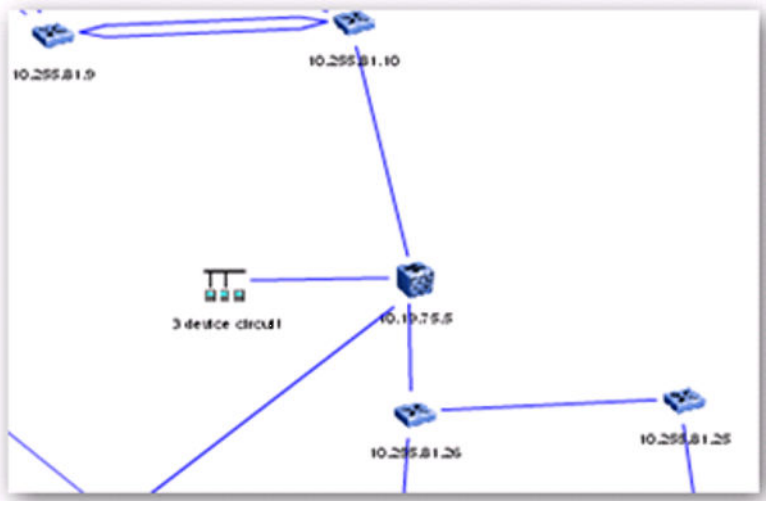
# Discovery of clusters

Avaya VPFM discovers device clusters as single devices. Device clusters are typically comprised of more than one hardware unit, managed with a single Management IP. Traps from device clusters are handled correctly, as long as they are received from the same management IP that was discovered. This is true even if a failover happens after discovery.

Because clusters are not discovered as separate components, links to the multiple components may not be fully and correctly discovered.

Some examples of such clusters are the Switched Firewall cluster (comprised of director and accelerator appliances) and Secure Network Access clusters. In the case of the Switched Firewall cluster, only links to the Master accelerator component are discovered.

In the following figure, the firewall device 10.19.75.5 is connected to 10.255.81.10 and 10.255.81.26. In the network, the firewall device is connected to 10.255.81.25 and 10.255.81.9 as well, but VPFM shows the connectivity only to the switches connected to the master accelerator.



# Discovery of EMC Storage

With VPFM, you can discover EMC VNX 5300 storage arrays.

**Related Links**

Discover your network on page 15
Enabling SNMP on the VNX Service Processors on page 25

# Enabling SNMP on the VNX Service Processors

Perform the following procedure to enable SNMP on the VNX service processors for VPFM discovery of EMC VNX 5300 storage arrays.

### Procedure

1. Log on to EMC Unisphere.

   Invoke EMC Unisphere from the web browser by pointing the browser to the Service Processor A or B IP addresses.
2. On the EMC Unisphere dashboard, click on the VNX system.
3. Click **Settings**.
4. Configure SNMP for each of the service processors.
   a. From the Network Settings panel on the right side of the screen, click on a service processor.
   b. From the SNMP Settings section, select **Enable processing of SNMP MIB read requests**.
   c. Enter an SNMP Community name.
   d. Click **Apply**, and then click **OK**.
5. Provide SNMP credentials for the two VNX service processor IP addresses in the Device and Server Credentials editor.
6. Install the CIM SMI-S block provider for the VNX.
   a. Download the CIM SMI-S block provider from http://support.emc.com.
   b. Install on Windows or RHEL.
   c. Search for SMI-S Provider 4.5 for SMI-S 1.5.
7. Provide the CIM credentials for the server where the SMI-S provider is installed in the Device and Server Credentials editor.

   The default CIM username is admin.

   The default CIM password is #1Password.
8. To add the storage arrays to the SMI-S provider for discovery and monitoring, run the TestSmiProvider program.

### Example

The following is a sample session that describes how to use the TestSmiProvider program to register your storage arrays with the SMI-S provider.

```
C:\Program Files\EMC\ECIM\ECOM\bin>TestSmiProvider.exe
Connection Type (ssl,no_ssl) [no_ssl]:
Host [localhost]:
Port [5988]:
Username [admin]:
Password [#1Password]:
Log output to console [y|n (default y)]:
Log output to file [y|n (default y)]:
Logfile path [Testsmiprovider.log]:
Connecting to localhost:5988
Using user account 'admin' with password '#1Password'

################################################################################
##                                                                            ##
##                  EMC SMI Provider Tester                                   ##
##   This program is intended for use by EMC Support personnel only.          ##
##   At any time and without warning this program may be revised               ##
##   without regard to backwards compatibility or be                           ##
##   removed entirely from the kit.                                            ##
################################################################################
  slp    - slp urls                    slpv    - slp attributes
  cn     - Connect                     dc      - Disconnect
  disco  - EMC Discover                rc      - RepeatCount
  addsys - EMC AddSystem               remsys  - EMC RemoveSystem
  refsys - EMC RefreshSystem

  ec     - EnumerateClasses            ecn     - EnumerateClassNames
  ei     - EnumerateInstances          ein     - EnumerateInstanceNames
  ens    - EnumerateNamespaces         mine    - Mine classes

  a      - Associators                 an      - AssociatorNames
  r      - References                  rn      - ReferenceNames

  gi     - GetInstance                 gc      - GetClass

  ci     - CreateInstance              di      - DeleteInstance
  mi     - ModifyInstance              eq      - ExecQuery
  gp     - GetProperty                 sp      - SetProperty

  tms    - TotalManagedSpace           tp      - Test pools
  ecap   - Extent Capacity             pd      - Profile Discovery

  im     - InvokeMethod                active  - ActiveControls
  ind    - Indications menu            tv      - Test views

  st     - Set timeout value           lc      - Log control
  sl     - Start listener              dv      - Display version info
  ns     - NameSpace                   vtl     - VTL menu

  chp    - consolidated host provider menu


  q      - Quit                        h       - Help
################################################################################
Namespace: root/emc
repeat count: 1
(localhost:5988) ?
(localhost:5988) ? addsys
Add System {y|n} [n]: y
```

```
ArrayType (1=Clar, 2=Symm) [1]: 1
One or more IP address or Hostname or Array ID

Elements for Addresses
IP address or hostname or array id 0 (blank to quit): 47.80.237.31
IP address or hostname or array id 1 (blank to quit): 47.80.237.32
IP address or hostname or array id 2 (blank to quit):
Address types corresponding to addresses specified above. IP address or hostname or array
id 2 (blank to quit):

(1=URL, 2=IP/Nodename, 3=Array ID)
Address Type (0) [default=2]:
Address Type (1) [default=2]:
User [null]: sysadmin
Password [null]: sysadmin
++++ EMCAddSystem ++++
OUTPUT : 0
Legend:0=Success, 1=Not Supported, 2=Unknown, 3=Timeout, 4=Failed
       5=Invalid Parameter
       4096=Job Queued, 4097=Size Not Supported
Note: Not all above values apply to all methods - see MOF for the method.

System : //47.80.237.75/root/emc:Clar_StorageSystem.CreationClassName="Clar_Stor
ageSystem",Name="CLARiiON+APM00120402442"

In 15.041860 Seconds

Please press enter key to continue...
(localhost:5988) ? dv
++++ Display version information ++++

CIM ObjectManager Name: EMC:47.80.237.75

CIMOM Version: EMC CIM Server Version 2.7.1.0.0.2

SMI-S spec version: 1.6.0

SMI-S Provider version: V4.4.0.1

SMI-S Provider Location: Proxy

SMI-S Provider Server:
Windows_NT vpfm 6.1.7601 Service Pack 1 x86_64 VM Guest OS (64bit Libraries)

Solutions Enabler version: V7.4-1506 0.6

Firmware version information:
(Remote) CLARiiON Array APM00120402442 (Rack Mounted VNX5500) : 05.31.000.5.704


Retrieve and Display data - 1 Iteration(s) In 0.112006 Seconds

Please press enter key to continue...
```

The following table describes key commands and system outputs for using the TestSmiProvider program.

| Command or system output | Description |
|---|---|
| `C:\Program Files\EMC\ECIM\ECOM \bin>TestSmiProvider.exe` | The path you enter to start the TestSmiProvider program. |

| Command or system output | Description |
|---|---|
| `Username [admin]:` | The default username for the provider. Use the web interface to add more users. |
| `Password [#1Password]:` | The default password for the provider. Use the web interface to add more users. |
| `(localhost:5988) ? addsys` | The command you enter to add system. |
| `IP address or hostname or array id 0 (blank to quit): 47.80.237.31` | The IP Address of SP_A. |
| `IP address or hostname or array id 1 (blank to quit): 47.80.237.32` | The IP Address of SP_B. |
| `User [null]: sysadmin` | The username for SP_A and SP_B. |
| `Password [null]: sysadmin` | The password for SP_A and SP_B. |
| `(localhost:5988) ? dv` | The command you enter to display version information. |
| `Firmware version information:` | The system displays information about the VNX that was added. |

**Related Links**

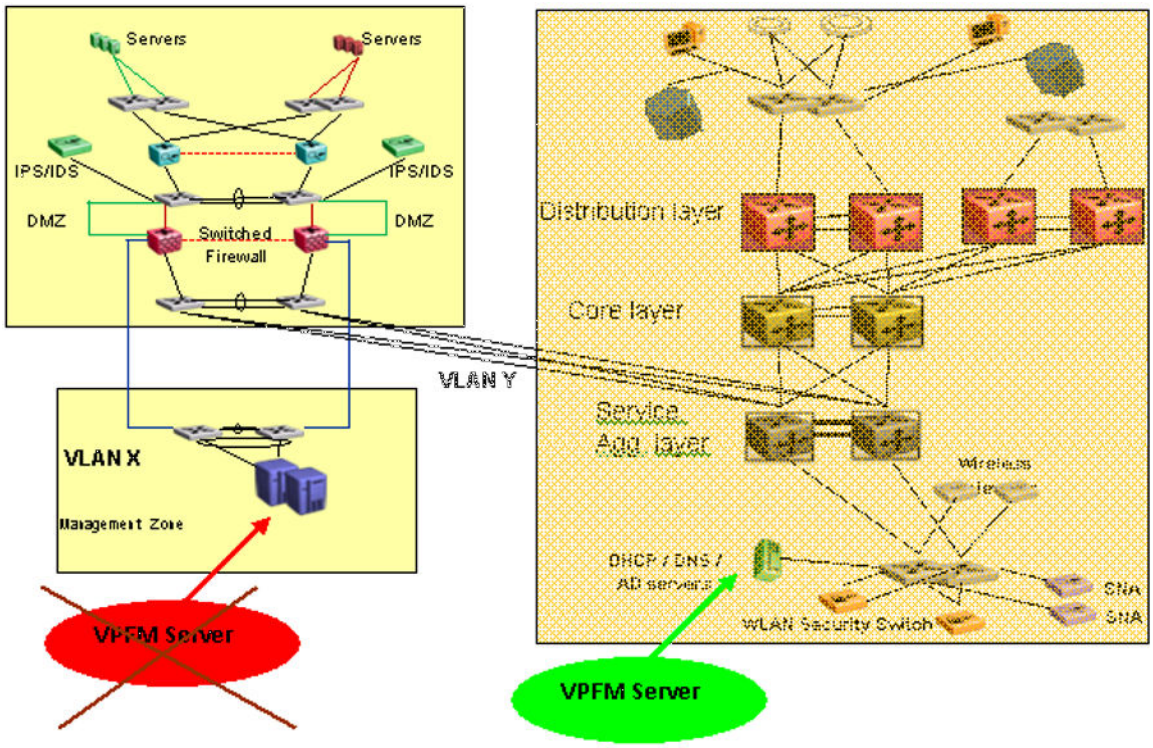
Discovery of EMC Storage on page 25

# Switched Firewall discovery

To discover the Switched Firewall discovery device successfully, you must configure the following SNMP configuration options on the device:

- /cfg/sys/adm/snmp/adv/allinf y
  - Ensures that the Switched Firewall can respond to SNMP requests sent to any of its IP addresses.
- /cfg/sys/adm/snmp/adv/getsrcip auto
  - Sets the source IP of the SNMP response to that of the outgoing interface. You must ensure that the IP address of the Switched Firewall that Avaya VPFM sends the SNMP request to, is the outgoing interface through which the SNMP response is sent. For this purpose, Avaya recommends that you place the server hosting the VPFM service appropriately with respect to the Switched Firewall device.

The following diagram demonstrates an Switched Firewall discovery.




In the preceding diagram, the VPFM Server is placed in Virtual Local Area Network (VLAN) X with the Switched Firewall interface (the VPFM Server default gateway). After VPFM learns the IP address of the firewall in VLAN Y from the routers in the Distribution (Core or Service Aggregation layer–one of these was selected as the seed route), VPFM attempts to send SNMP requests to the VLAN Y interface of the firewall. The firewall responds to the VPFM server through the VPFM outgoing interface in VLAN X. A mismatch in the destination and source IP addresses in the SNMP request and response occurs, and VPFM ignores the responses from the Switched Firewall and does not discover the device.

To correct the mismatch in the destination and source IP addresses in the SNMP request and response, choose one of the following options:

- Place the VPFM server in VLAN Y.
- Provide a seed router from VLAN X (if available) so that VPFM learns about the Switched Firewall VLAN X interface.

# Discovering devices behind the Switched Firewall

### About this task

To discover the devices behind the firewall, Avaya VPFM queries the private ARP cache of the Switched Firewall device. To ensure that the SNMP query does not time out (causing the non-discovery of some of the devices), the Switched Firewall device must operate software 4.2.6.0 or

later. You can obtain the latest Switched Firewall image from the Avaya Support Web Site: http://www.avaya.com/support.

# WLAN Security Switch 2300 discovery

Avaya VPFM discovers each of the IP addresses of the WLAN Security Switch (WSS) 2300 as a separate element, because the WSS 2300 does not implement the ipAddrTable MIB (IP Address Table). Avaya VPFM requires the ipAddrTable MIB to identify multiple IP addresses belonging to a device and to create only one element for the device. In the absence of the ipAddrTable MIB, VPFM is unable to identify the IP addresses as belonging to a single device and ends up creating multiple elements.

Avaya VPFM may not discover the links between the WSS 2300 and the switch that WSS 2300 is connected to, because the WSS 2300 does not provide forwarding database (FDB) information through SNMP. Avaya VPFM attempts to use only the FDB information from the connected switch to draw the link, but the operational state of the WSS 2300 interfaces may prevent VPFM from drawing the link.

Avaya VPFM can still manage and monitor the device.

# Discovery of links

Avaya VPFM discovers links using the following three protocols:

- Avaya SONMP (s5EnMsTopNmmEosTable MIB)
- LLDP (802.1ab)
- FDB inference (dot1dTpFdbTable MIB)

The following table outlines the Avaya devices that support SONMP and LLDP (802.1ab).

| Device type | SONMP | LLDP (802.1ab) |
|---|---|---|
| ERS 25xx | Yes | Yes |
| ERS 35xx | Yes | Yes |
| ERS 45xx | Yes | Yes |
| ERS 55xx | Yes | Yes |
| ERS 56xx | Yes | Yes |
| ERS 16xx | Yes | No |
| ERS 83xx | Yes | Yes |
| ERS 86xx | Yes | No |
| VSP 4000 | Yes | No |

| Device type | SONMP | LLDP (802.1ab) |
|---|---|---|
| VSP 7000 | Yes | Yes |
| Wireless LAN Security Switch | No | No |
| Wireless LAN Controller WC 8180 | Yes | No |
| Secure Network Access Switch (SNAS) | Yes | No |

For devices that do not implement SynOptics Network Management Protocol (SONMP) or Link Layer Discovery Protocol (LLDP), VPFM uses the FDB table to infer the links. For switches, both the devices FDB tables must have an entry for each other. For links between a switch and an end-node, the switch FDB entries are sufficient.

To accurately discover links with the FDB table inference algorithm, VPFM depends on the presence of traffic on the links, and uses a weighted algorithm; the more traffic that is present (which equates to more entries in the neighboring switches FDB tables), the better the accuracy with which VPFM can perform the inference.

# Device circuits in Avaya VPFM

On a regular basis, Avaya VPFM creates device circuits; objects that contain other devices and end-nodes.

Device circuits complete your network topology map. Avaya VPFM uses device circuits to ensure that all discovered devices are available in the topology map, and places the device circuits in the correct network.

Device circuits are created when there is no logical information (SONMP, LLDP, or FDB entries) to connect a device or end-node to a switch. Device circuits are created based on routing interface ARP information, which is why device circuits are always attached to a layer-3 device and never to a layer-2 switch.

If there is more than one routing interface for the subnet, there is no definite way to know which routing interface the device circuits are attached to.

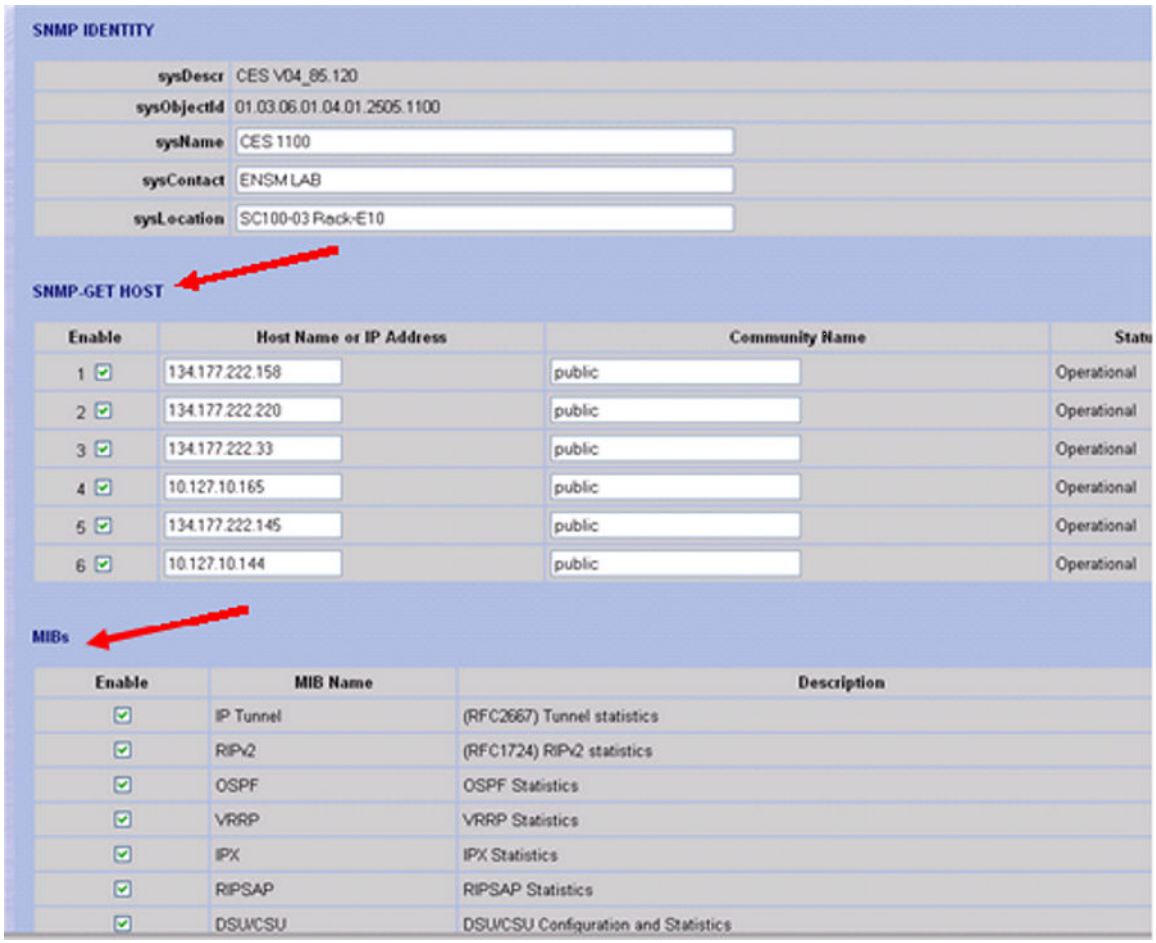
**Note:**

If devices have multiple VRRP addresses, VPFM discovers some of the addresses separately as unmanaged devices that end up in device circuits. To remove unwanted device circuits, add Unmanaged devices to the exclusion list in your discovery seed configuration.

# Avaya VPN Gateway discovery

For discovery of Virtual Private Network (VPN) routers, ensure that the management station IP address is provided as an SNMP manager to the device (by using the Business Element Manager), and that SNMP MIBs (specifically the Tunnel MIB) are enabled in the Business Element Manager.

The following figure is an example of the Avaya VPN Gateway Business Element Manager page.




# Voice application discovery

Avaya VPFM discovers Nortel branded IP deskphones by querying open ports on the IP deskphones, not SNMP. The Avaya branded phones respond to SNMP; therefore, VPFM discovers Avaya branded IP deskphones using standard SNMP MIBs.

After an IP address does not respond to SNMP, VPFM queries the device to check if certain ports are open.

You can identify Avaya IP deskphones by the following open ports: 5000, and 5001.

The Avaya Secure Router 4134 (Avaya SR 4134) can include a VoIP module. To ensure that VPFM discovers and lists the VoIP module as a Voice Application in VPFM, enter telnet credentials for the Avaya SR 4134 on the Avaya Unified Communications Manager (Avaya UCM) credentials page.

To associate the discovered IP deskphones with their respective Avaya Communication Server 1000 (Avaya CS 1000) systems, ensure that you enter the telnet credentials for the Signaling Server in the Avaya UCM credentials page.

To associate the discovered IP deskphones with their respective Avaya Business Communications Manager (Avaya BCM) systems, make sure that the CIM credentials are entered for the Avaya BCM in the Avaya UCM credentials page.

# Discovery of third party devices

Avaya VPFM discovers and manages any device that responds to ping and SNMP. The only requirement is that third party devices implement standard MIBs (also called MIB-2 MIBs) to ensure that VPFM accurately discovers and connects the third party devices in the topology.

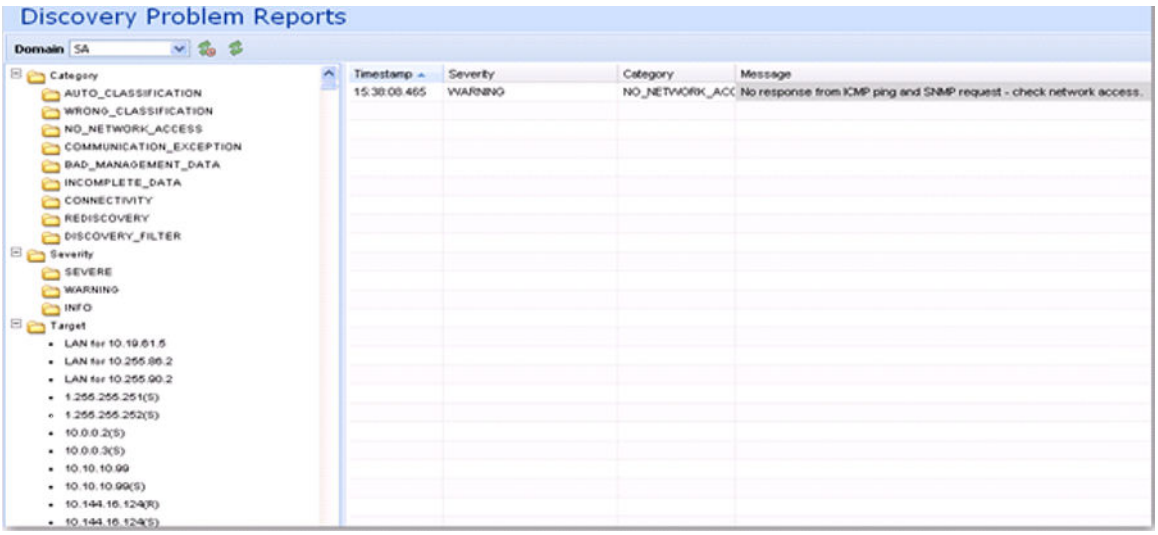
Because of various differences in the way certain configurations, such as clustering, are implemented in different devices, the devices are exposed through enterprise MIBs (non-standard MIBs). There is no guarantee that VPFM can accurately discover and visualize these configurations in the VPFM topology maps.

# Analyzing Avaya VPFM logs

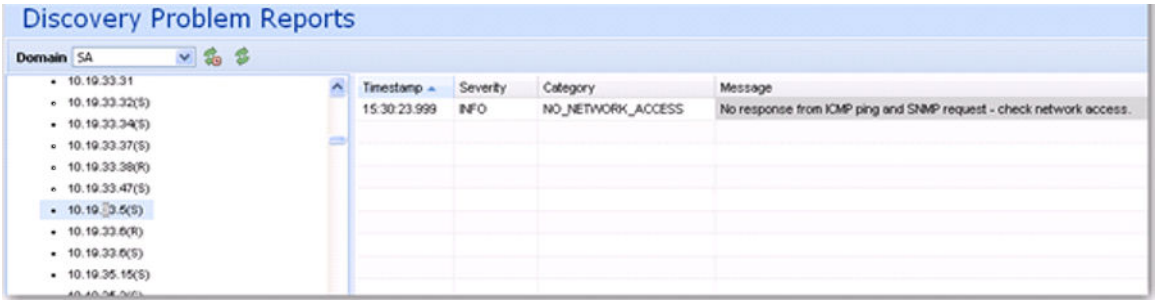
### About this task

To view logs related to a discovery, on the tool bar of the Network Discovery page, click **Discovery Problem Report**, represented by the following icon:  . Then select a node from the navigation panel.

The following is an example of a Discover Problem Reports page.




The left hand navigation pane on the Discovery Problem Reports page organizes log messages based on category, severity, and IP address.




To troubleshoot why a particular IP address is not discovered or is discovered as unmanaged, locate the IP address in the left navigation pane.

One common reason for not discovering a device is the lack of response from the device from ping or SNMP requests sent from Avaya VPFM. In this case, check the UCM device credentials to make sure they are correct.

If the credentials are correct, then check for SNMP access using the SNMP MIB browser.

Some of the common messages that you encounter in the logs are as follows:

- Device did not respond to SNMP or ICMP

  If the device does not respond to SNMP or ICMP, then perform the following procedures:

  - Check if the device responds to ping.
  - Check if the device responds to SNMP from the VPFM MIB browser.
  - Check with Wireshark to determine if the device is sending back a response.
  - If all of the above is occuring, check UCM credentials and rerun the discovery

- Potential managed device was excluded from discovery

If the potential managed device is excluded from discovery, then perform the following procedures:

- Check discovery constraints to ensure that the device IP is not excluded by subnet limits or other constraints
- You may also see this message, or a similar message, if the topology table of one device includes this device, but this device is not found in the ARP table of any of the routers in that subnet. In this case, check the ARP table of the routers and fix any related issues. Avaya VPFM discovers a device only if the device is found in the ARP table.

• There is no log entry for an undiscovered device

- Make sure that UCM credentials exist for that IP and that they are correct
- Make sure that the device's IP address in present in the ARP tables of one or more discovered layer-3 devices in your network.

# SPBM diagnostic tests for VSP 7000 devices

For VPFM to perform Shortest Path Bridging MAC (SPBM) diagnostic tests on VSP 7000 devices, you must configure the sysName of the VSP 7000 device.

**Related Links**

Discover your network on page 15