Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network

Release 3.0.2
NN48014-501
Issue 03.01
March 2013

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.

Licence 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.

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.

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

Avaya Aura® is a registered trademark of Avaya Inc.

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.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose

This document provides information for using Avaya Unified Communications Management (UCM) to manage the Converged Voice and Data Network.

This document is intended for providing administrators comprehensive management capabilities for key products in your Avaya Enterprise portfolio, and simplifies functionality associated with managing subscribers, faults, configuration, performance and security.

Related resources

Related topics:

Documentation on page 7
Training on page 8
Avaya Mentor videos on page 8
Support on page 9

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
Avaya Visualization Performance and Fault Manager VPFM SCOM Connector Fundamentals (NN48014–101)	Fundamentals	http://support.avaya.com

Title	Purpose	Link
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 Discovery Best Practices (NN48014–105)	Best Practices	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 Fault and Performance Management (NN48014–700)	Administration	http://support.avaya.com

Training

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

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Go to http://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 site.

Support

Visit 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.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Visualization Performance and Fault Manager Using Unified Communications Management to Manage the Converged Voice and Data Network* (NN48014–501) for release 3.0.2.

Features

See the following section for information about feature changes.

Related topics:

Supported environments on page 11

Supported environments

Avaya Aura Virtual Environment (Aura VE), including non-VE, SMGR-VE 6.2 is supported as part of the converged data and voice Avaya UCM solution. Communication Server 1000 (CS 1000) is also supported.

Other information

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

Introduction chapter

The Introduction chapter replaces the Purpose of this document chapter.

Chapter 3: Overview

The Avaya Unified Communications Management (Avaya UCM) portfolio provides comprehensive management capabilities for key products in the Avaya Enterprise portfolio, and simplifies functionality associated with managing subscribers, faults, configuration, performance and security. Through features like single sign-on, common look and feel, information sharing, heterogeneous network support, and consistent user interfaces, Avaya UCM provides decreased complexity, lowered capital and operational expenses, improved workflows, reduced error potential, and quicker time-to-resolution.

Key management products that have adopted the Avaya UCM solution model include data products and voice products.

Data products supported on Avaya UCM include the following:

- Avaya Visualization Performance and Fault Manager (Avaya VPFM) version 3.0.2
- Avaya Configuration and Orchestration Manager (COM) version 3.0.1
- Avaya Bulk Configuration Manager (BCM)
- IP Flow Manager (IPFM) version 2.0.2
- Virtualization Provisioning Service (VPS) version 1.0.2

Voice products supported on Avaya UCM include the following:

- Avaya Communication Server 1000 (Avaya CS 1000) Release 6.0 and Release 7.0 system management applications (such as, Business Element Manager, Deployment Manager, NRS Manager)
- Subscriber Manager Release 2.0

Upon initial release of the above mentioned products, full integration/co-residency of Voice management products with Data management products (that is, within a single UCM security infrastructure), was not immediately supported, as full solution verification had not yet been complete. However, final solution-level verification of UCM-based voice management applications (CS 1000 Release 6.0 and Release 7.0 applications and Subscriber Manager 2.0) and data management applications (VPS 1.0.2, VPFM 3.0.2, IPFM 2.0, COM, and BCM) have now been completed. This guide provides key information required to unify these voice and data management applications within a single UCM deployment.

Note:

The terms Data product and Voice product are used in this document to identify a group of system and network management applications that are most closely associated to Avaya's Enterprise Data and Enterprise Voice product portfolios respectively. Applications such as Avaya VPFM and Subscriber Manager have been developed to provide more general functionality, and the usefulness of these products and applications spans more than just one Avaya portfolio area. Avaya retains the Voice and Data distinction primarily because, until now, these applications could not coexist in a single management domain, and it remains a convenient nomenclature in a discussion about Avaya UCM

solution convergence. The distinction between Data and Voice management becomes increasingly less meaningful as Avaya's system and network management products become increasingly integrated.

Chapter 4: Deploy a converged data and voice Avaya UCM infrastructure

The following topics are covered in this chapter.

Before deploying a converged Data and Voice Avaya UCM solution

Before you proceed with deployment of a converged data and voice Avaya UCM deployment, you must first be very familiar with UCM, including the concept of Primary, Backup, and Member UCM Servers, and the process of deploying individual UCM-based applications.

You must be very familiar with the following documentation:

- Avaya UCM documentation for Voice Network Management. For more information, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001–116), Release 7, Document Revision 04.01.
- Avaya CS 1000 Linux Base documentation for Voice Network Management. For more information, see *Avaya Communication Server 1000 Linux Platform Base and Applications Installation and Commissioning* (NN43001–315), Release 7, Document Revision 04.01.
- Avaya UCM documentation for Data Network Management. For more information, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100), Release 2.0, Document Revision 02.01.

You can obtain the latest version of these documents from the Avaya Technical Support portal: www.avaya.com/support.

Converged data and voice Avaya UCM deployments supported scenarios

Avaya extends support to a number of Avaya UCM deployment scenarios that span both voice and data management products. All supported scenarios require the use of an Avaya CS 1000-based system as the UCM Primary security server.

Note:

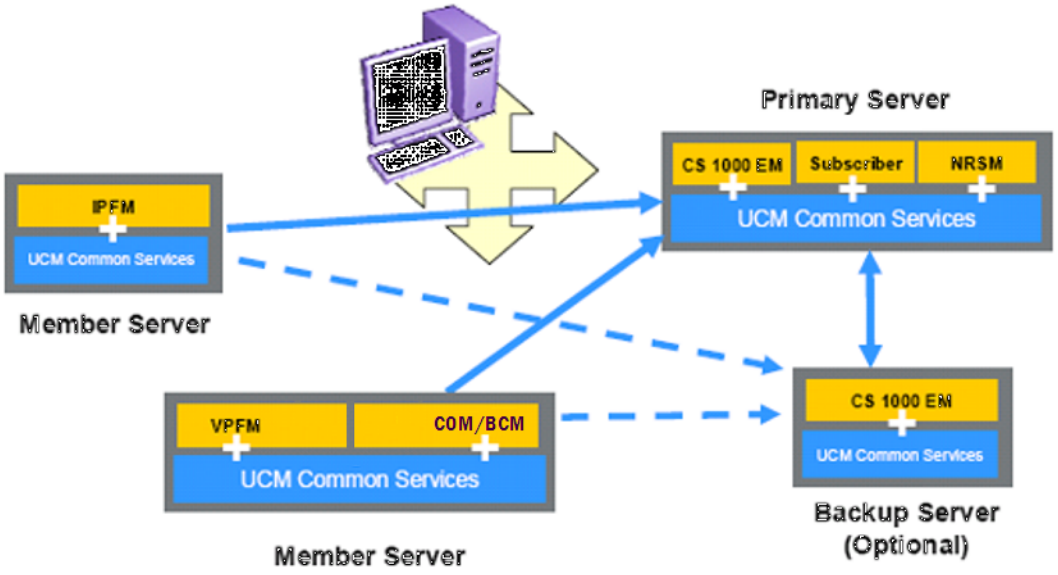
In addition to the support of Avaya CS 1000 as the primary server, Avaya also supports System Manager (SMGR) 6.2 VE and non-VE as the primary server. The CS 1000 workflow described in the following sections remains the same for System Manager 6.2. However, the UCM login page is different; you log on to the System Manager landing page.

The use of an Avaya UCM Backup security server is an optional piece of the security domain and is deployed to provide redundancy for the authentication and authorization service. The Backup security server role can be held by either a CS 1000-based system, such as a Voice system, or on a server hosting one or more of the Data management applications. You can join any combination of Member servers, such as Voice and Data, to the security domain lead by a CS 1000 primary.

For more information about the security domain, the types of UCM servers that can participate in the domain (Primary, Backup, and Member), and engineering recommendations and limitations, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

Avaya CS 1000 is deployed as Avaya UCM Primary and Backup UCM servers

The following figure outlines a typical Avaya UCM security domain topology when a Primary and a Secondary server are both hosted on Avaya CS 1000 (Voice) systems.



The following table outlines the typical deployment scenario described in the preceding figure.

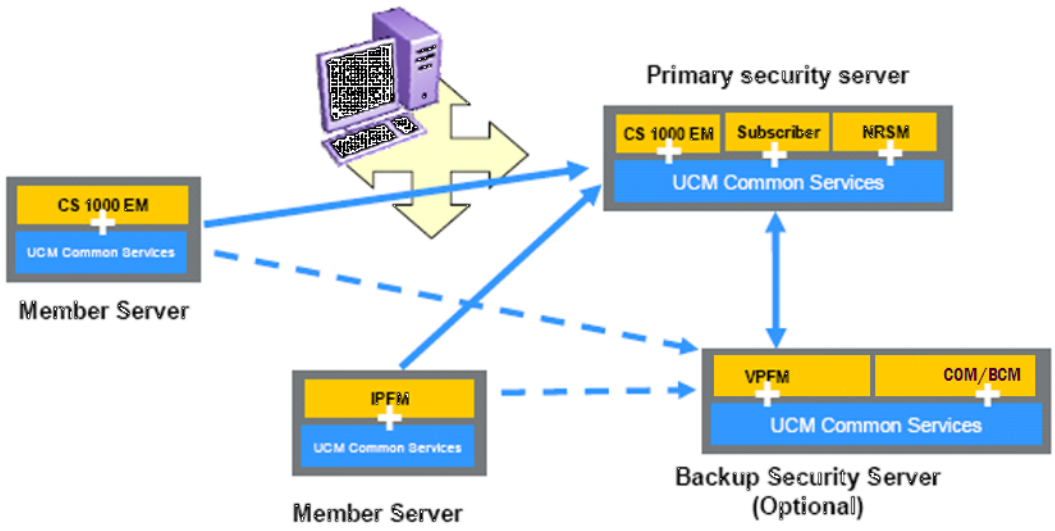
Primary	Backup	Each Member
CS 1000	CS 1000	(VPFM and/or VPS and/or COM/BCM and/or IPFM) or CS 1000)

The following list outlines characteristics of a typical deployment of Avaya CS 1000 as a Primary server and Backup server.

- The Backup server is optional, and is deployed to provide authentication and authorization redundancy in the event that Primary is failed and unreachable.
- CS 1000 is any valid combination of CS 1000-based system management applications, including Subscriber Manager.
- CS 1000 is only supported in RHEL 5.2.
- VPFM/VPS/COM/BCM/IPFM is supported in RHEL 5.2, Windows 2003 Server, and Windows 2008 Server.
- VPFM, VPS, COM, and BCM can be co-resident within a single server acting as a member.
- Due to resources requirements, Avaya strongly recommends to not install IPFM co-resident with the other data products.

Avaya CS 1000 is deployed as a Primary server and one of data network management products is deployed as a Backup server

The following figure outlines a typical Avaya UCM security domain topology when a Primary server is hosted on a Voice system and the Backup server is hosted on a Data system; that is, a server hosting one or more data-focused management applications.



The following table outlines the typical deployment scenario described in the preceding figure

Primary	Backup	Each Member
CS 1000	VPFM and/or VPS and/or COM/BCM and/or IPFM	(VPFM and/or VPS and/or COM/BCM and/or IPFM) or CS 1000

The following list outlines characteristics of a typical deployment of Avaya CS 1000 as a Primary server and Data Server as a Backup server.

- The Backup server is optional, and is deployed to provide authentication and authorization redundancy in the event that Primary is failed or unreachable.
- All data network management products must have the same OS to work with each other in the same security domain.
- CS 1000 is any valid combination of CS 1000-based system management applications, including Subscriber Manager.
- CS 1000 is only supported in RHEL 5.2.
- VPFM/VPS/COM/BCM/IPFM is supported in RHEL 5.2, Windows 2003 Server, and Windows 2008 Server.

- VPFM, VPS, COM, and BCM can be co-resident within a single server acting as a member or as a backup.
- Due to resources requirements, Avaya strongly recommends to not install IPFM co-resident with the other data products.

Browser support

In a converged data and voice Avaya UCM deployment, only Internet Explorer 8 and 9 are supported across all the products.

Installing a patch for System Manager UCM deployment

Perform the following procedure to install the patch to make a VPFM 3.0.1 member server point to the System Manager (SMGR) 6.2 primary server.

Before you begin

- This patch works with VPFM 3.0.1 only. If you have an older version of VPFM, you must upgrade to 3.0.1 and then apply this patch.
- If you upgrade System Manager, repeat step 1 in the following procedure.
- If you have multiple member servers pointing to a SMGR primary server, the first member server installs and hosts the Device and Server Credentials and the Licensing Administration modules. Therefore, when you install multiple member servers, you must provide the FQDN of the first member server when prompted by the installer for this information.
- Ensure that both System Manager and the member servers are part of the same network domain.
- Uninstalling the first member server, which hosts the Device Credentials and Licensing Administration modules, warns you about removing these modules; the applications are not usable without these modules. If you choose to continue, these modules are uninstalled with the application. For more information about accessing Device and Server Credentials and Licensing Administration, see Accessing Device and Server Credentials and Licensing Administration on page 22.

Procedure

1. On the SMGR 6.2 server, backup the navigationTree.xml file located in `/opt/Avaya/JBoss/4.2.3/jboss-4.2.3.GA/jboss-as/server/avmgmt/deploy/jboss-web.deployer/ROOT.war/WEB-INF/classes`. Copy the navigationTree.xml file from this archive to the same folder.

Note:

Do not restart JBoss or any other service.

2. Install VPFM as a member, and then point it to a SMGR 6.2 primary server when prompted during the installation.

   (Optional) To make an existing VPFM server a member to a SMGR 6.2 primary, you must perform the full security server configuration on the VPFM server by logging into that server using a local login.

3. Stop the JBOSS service on the VPFM server.
4. Backup the ecc.ear file located in the `JBOSS_HOME\server\default\deploy` folder on the VPFM server. Copy the ecc.ear file from this archive to the same folder.
5. Backup the ecc-module-common.jar file located in the `JBOSS_HOME\server\default\lib` folder on the VPFM server. Copy the ecc-module-common.jar file from this archive to the same folder.
6. Start the JBOSS and VPFM services on the VPFM server.
7. If you are logged in to SMGR, then logout and clear the browser cache.
8. Log in to SMGR to see the effective changes.

Accessing UCM through System Manager

Through Unified Communications Management (UCM) you can access services to manage UCM applications and navigation such as CS 1000 deployment, patching, ISSS and SNMP.

Perform the following procedure to access UCM through System Manager.

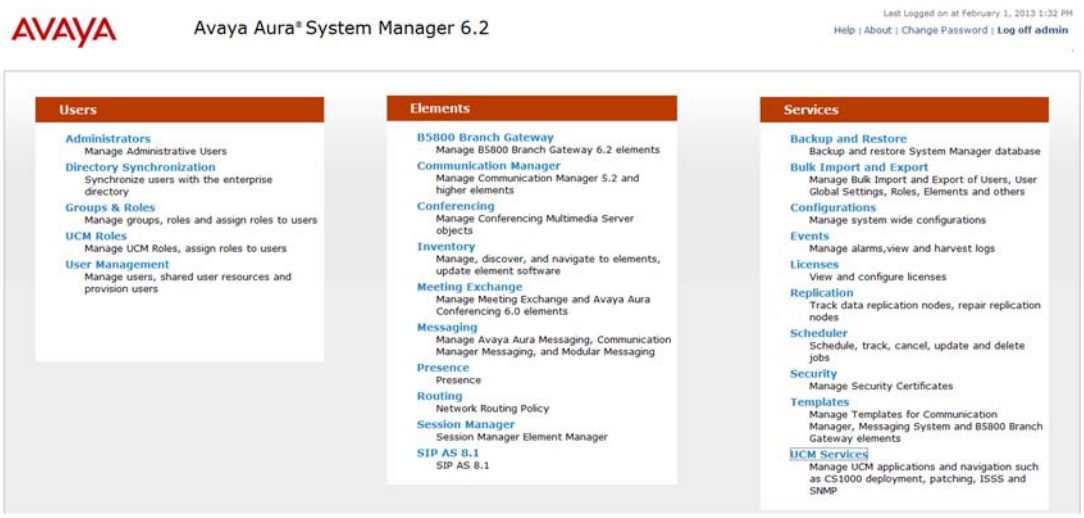
Before you begin

- You must have UCM or System Manager operator privileges.

Procedure

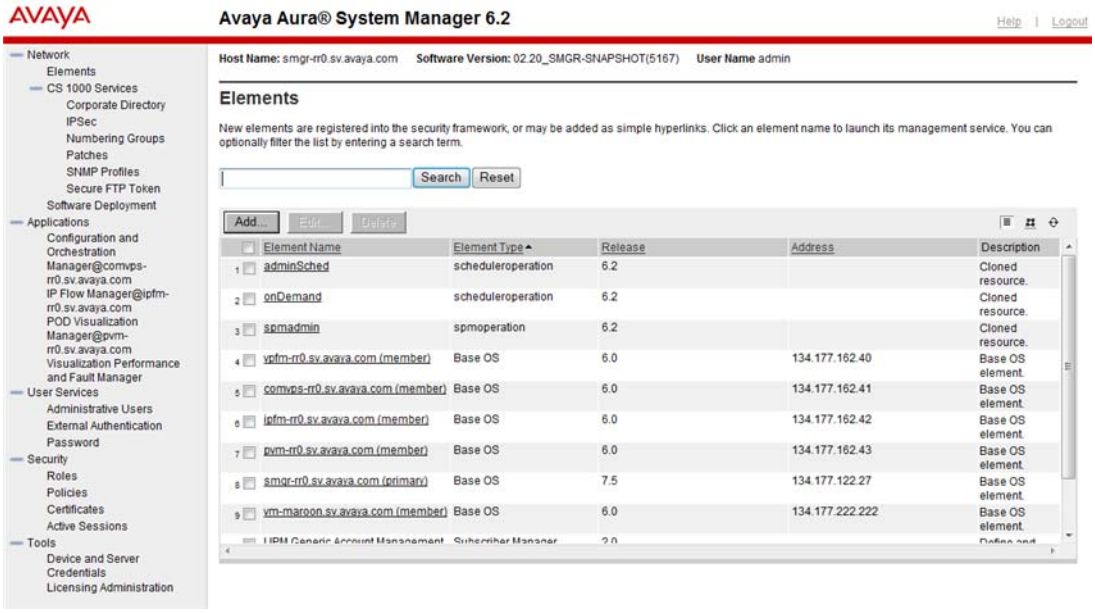
1. Log on to System Manager.

   The following figure is an example of the System Manager landing page.



2. From the Services pane on the System Manager landing page, click **UCM Services**.

   The following figure is an example of the UCM landing page.



Accessing Device and Server Credentials and Licensing Administration

Perform the following procedure to access Device and Server Credentials or Licensing Administration through System Manager.

Before you begin

- You must have System Manager operator privileges. To enable users who have only the UCM Operator privileges to login, you must set a flag in the System Manager configuration. For more information about accessing the flag, see Configuring System Manager operator privileges on page 23.

Procedure

1. Log on to System Manager.
   - If you are logged on to VPFM, click the **UCM** link to return to System Manager.
2. From the Users pane, click **Administrators**.
   - If you have UCM operator privileges only, from the Services panel, click **UCM Services**.
3. Select **Tools** > **Device and Server Credentials** or **Tools** > **Licensing Administration**.

   Note:

   If you are logged out due to inactivity, or you are redirected to the System Manager landing page, exit the browser and then log in again.

Accessing VPFM

Perform the following procedure to access Visualization Performance and Fault Manager (VPFM) through System Manager.

Before you begin

- You must have System Manager operator privileges. To enable users who have only the UCM Operator privileges to login, you must set a flag in the System Manager configuration.

For more information about accessing the flag, see Configuring System Manager operator privileges on page 23.

Procedure

1. Log on to System Manager.
2. From the Users panel, click **Administrators**.
   - If you have UCM operator privileges only, from the Services panel, click **UCM Services**.
3. From Applications, click **Visualization Performance and Fault Manager**.

Note:

If you are logged out due to inactivity, or you are redirected to the System Manager landing page, exit the browser and then log in again.

Configuring System Manager operator privileges

If a user has UCM Operator privileges only, the following three links are enabled on the System Manager landing page: Administrators, UCM Roles, and UCM Services. To obtain System Manager operator privileges for a user, you can set a flag in the System Manager configuration.

Perform the following procedure to obtain System Manager operator privileges for a user.

Note:

If you are logged out due to inactivity, or you are redirected to the System Manager landing page or login page, exit the browser and then log in again.

Before you begin

- You must have administrator privileges.

Procedure

1. Log on to System Manager.
2. From the Services panel, click **Configurations**.
3. Navigate to **Settings** > **SMGR** > **Common Console**.
4. Click **Edit**.
5. In the UCM Configured field, change the value to true.
6. Click **Commit**.

7. Click **Done**.

Integration workflows

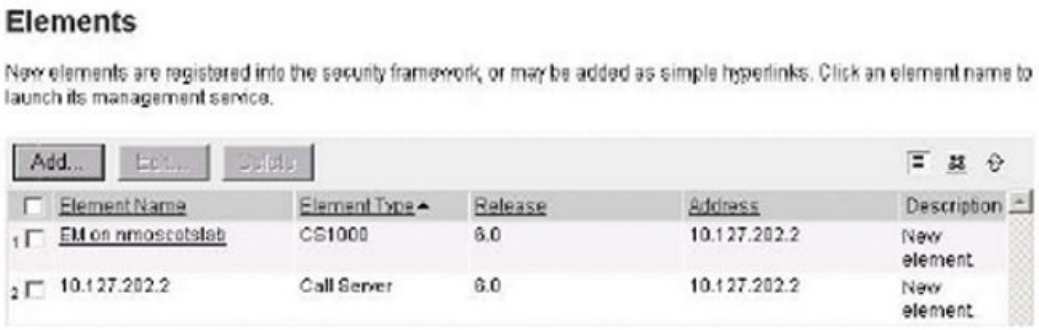
The following workflows are applicable only when there is already an Avaya CS 1000-based Primary server deployed in the network. For more information about installation and deployment of an Avaya UCM security domain lead by a CS 1000-based Primary server, which may or may not include CS 1000-based Secondary and Member servers, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

- Joining a new data product (VPFM VPS COM BCM IPFM) member server to an Avaya CS 1000 based primary server on page 24
- Demoting an existing data product primary server to a member server on page 31
- Demoting an existing data product backup server to a member server on page 32
- Promoting an existing data product member server to a backup server on page 34
- Assigning voice and data products related roles and permissions to a single user on page 36

Joining a new data product (VPFM/VPS/COM/BCM/IPFM) member server to an Avaya CS 1000 based primary server

This workflow applies when Avaya CS 1000 (a combination of CS 1000 EM, NRSM, and Subscriber Manager) is the first product installed and is configured as a primary server. If a data product (VPFM/VPS/COM/BCM/IPFM) is already installed as a primary server or a backup server in a separate security domain, the data product must be uninstalled first before joining the CS 1000 security domain.

The following figure is an example of the Avaya CS 1000 installed as a primary server.



Before you begin

Avaya CS 1000 must be the first product installed and configured as a primary server.

About this task

To install a data network management product, perform the following procedure.

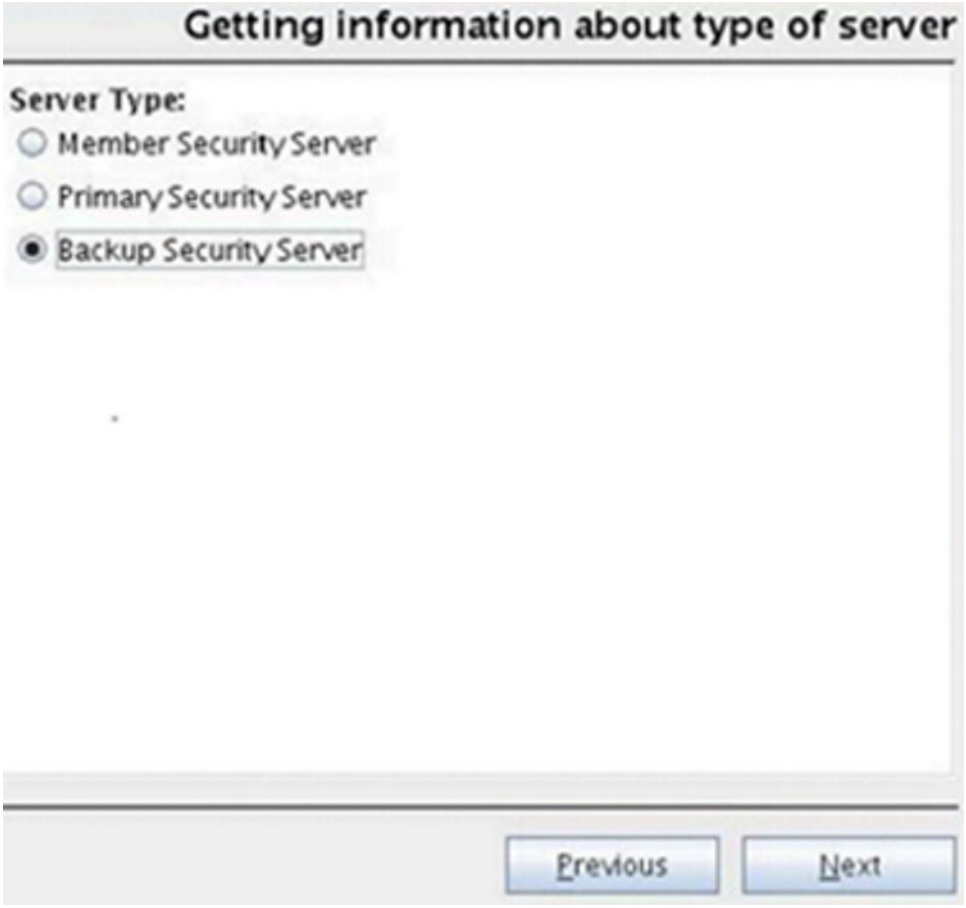
Procedure

1. Configure the server type.

   You can install data network management products as either a member or a backup.

   The following figure is an example of a data network management product installed as a member.

The following figure is an example of a data network management product installed as a backup.



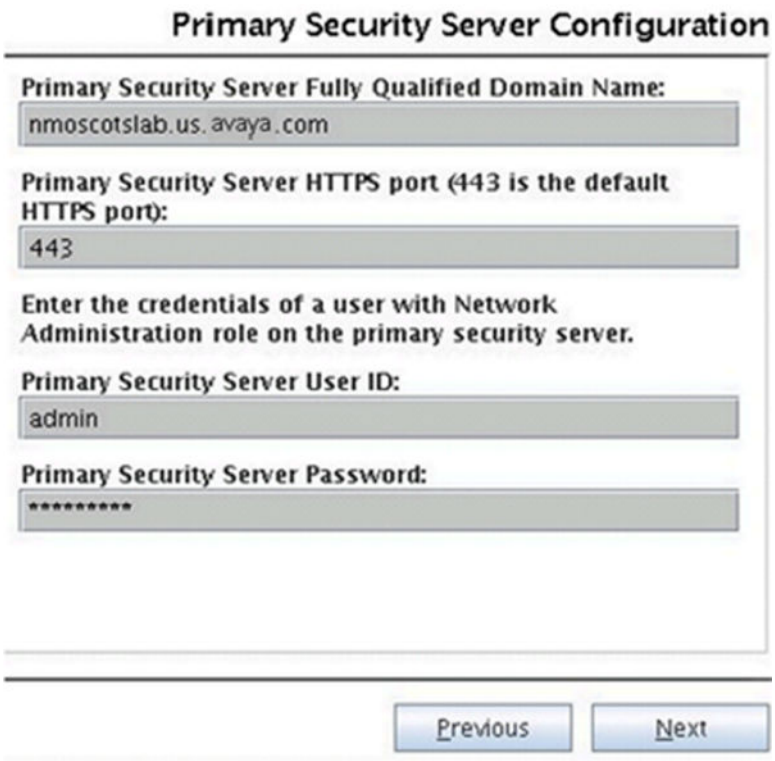
Note:

If another CS 1000 product is already deployed as a backup server, the data network management products are only installed as members.

2. Configure the primary server information.

   Enter the CS 1000 primary server FQDN, HTTPS port number, admin user ID and password.

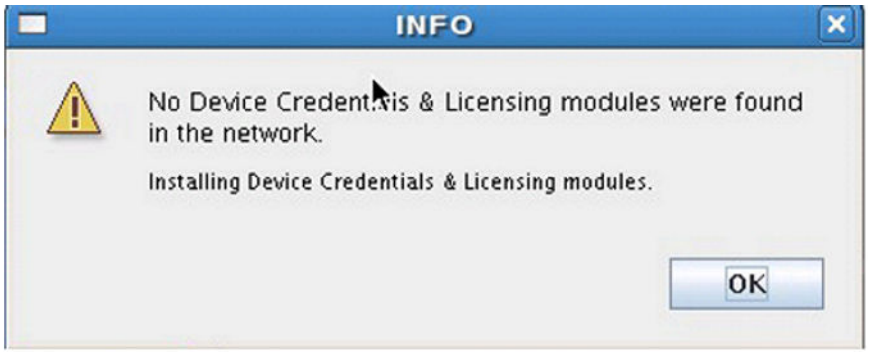
   The following figure is an example of a Primary Security Server Configuration screen.



3. Install device credentials and licensing modules.

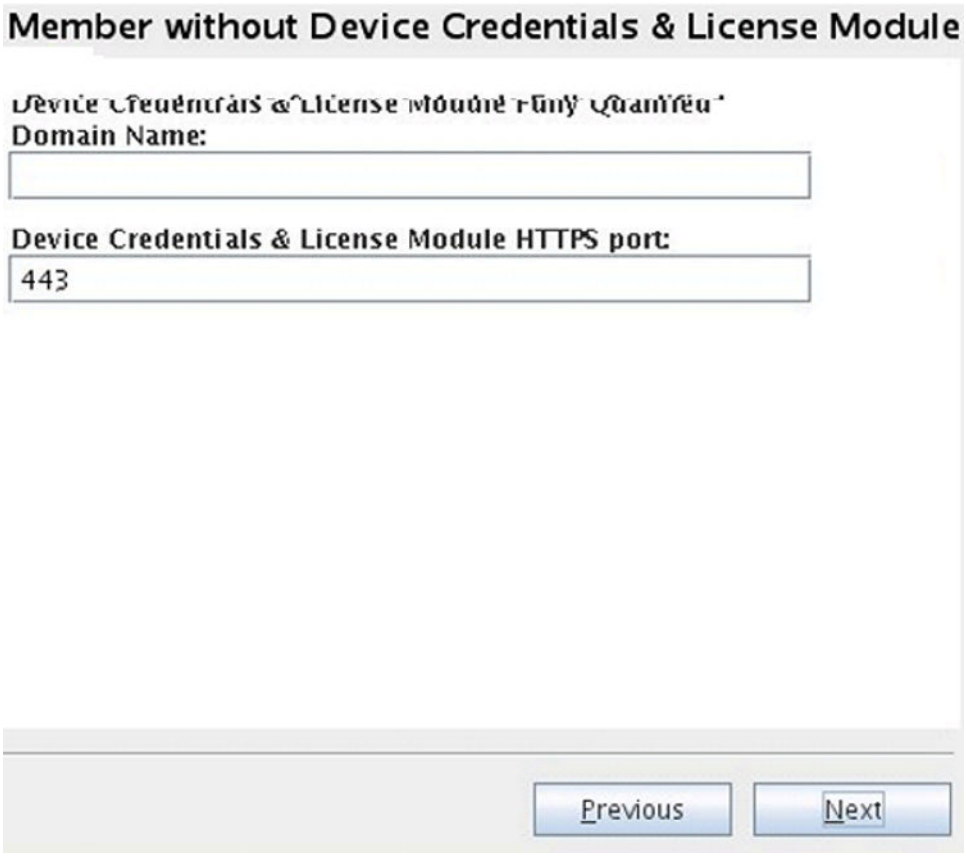
   After the first data network management product is deployed in the CS 1000 security domain, device credentials and licensing modules are installed. If the device credentials and licensing modules cannot be found, a dialog box appears prompting you to install them.

   The following screen appears if the device credentials and licensing modules are not detected in the security domain.



   If the device credentials and licensing modules are detected, the installer prompts you for the FQDN and HTTPS port number of the server where the device credentials and licensing modules reside.

   The following screen appears prompting you to configure the FQDN and HTTPS port number for device credentials and license module.



4. Set administrative password.

   Configure the server database password and UCM admin password.

   The following figure is an example of the Set Administrative Password (Member/ Backup) screen.

Note:

After installing each application, launch UCM and ensure the related launch points are added to UCM navigator before installing another application.

Next steps

After upgrading to Avaya Visualization Performance and Fault Manager (Avaya VPFM) 3.0.2, in a distributed environment, you must restart all servers (primary, backup, member) in the following order:

1. Primary
2. Backup
3. Member

Demoting an existing data product primary server to a member server

Perform this procedure to demote an existing data product (VPFM/VPS/COM/BCM/IPFM) primary server to a member server status to join the data product to an Avaya CS 1000–based primary server.

About this task

This workflow applies when a data network management product is deployed in a separate security domain and must be reconfigured to join another Avaya CS 1000-based security domain. To demote an existing data product primary server to a member server status, you must uninstall the product entirely and reinstall the product with a member server type configuration. Additionally, the provided backup and restore utilities must be invoked to preserve the applications data and configurations.

Procedure

1. Invoke the backup process.

   Use the following backup script to backup the product data and configurations.

   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.

2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.

3. Install the same product with member server type configuration.

   For installation procedure, see Joining a new data product (VPFM VPS COM BCM IPFM) member server to an Avaya CS 1000 based primary server on page 24.

4. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

   The restore script prompts for the name of the backup .jar file.

Demoting an existing data product backup server to a member server

Perform this procedure to demote an existing data product (VPFM/VPS/COM/BCM/IPFM), backup server to a member server status.

About this task

This workflow applies after a data network management product is deployed in the same security domain as the Avaya CS 1000 and must be reconfigured from backup server to member server. You must uninstall the product entirely and reinstall the product with a different server type configuration. The provided backup and restore utilities must be invoked to preserve the applications data and configurations.

Procedure

1. Invoke backup process.

   Use the following backup script to backup the product data and configurations.

   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.

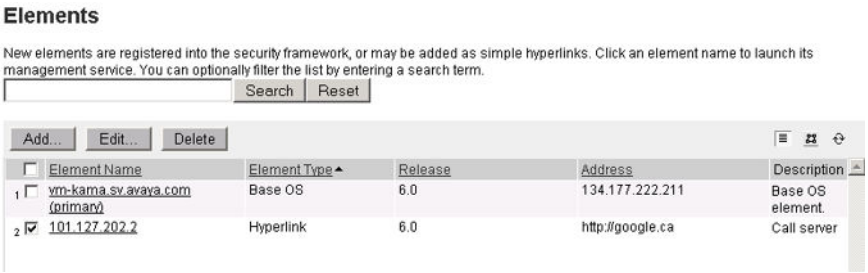
2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.

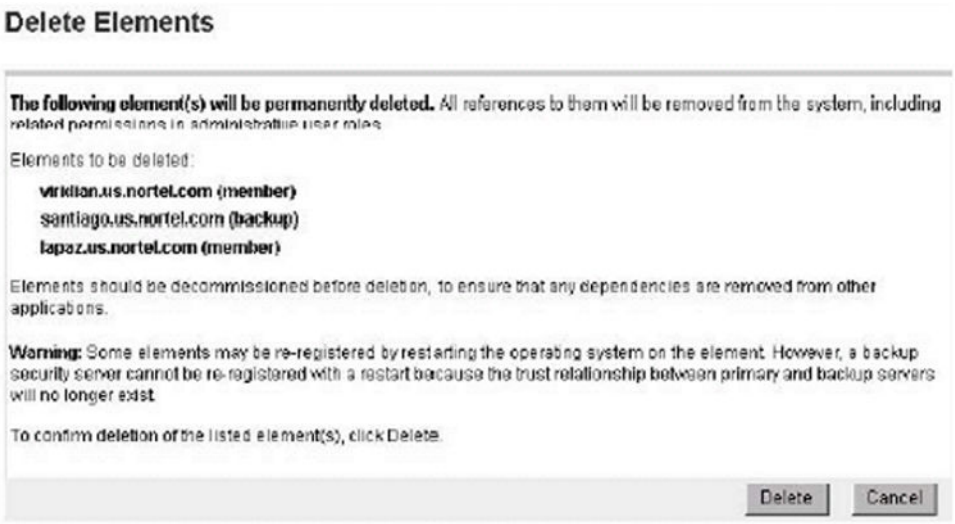
3. Cleanup the Elements Table from the GUI.

   The current uninstaller does not remove the added elements from the GUI, therefore you must remove the added elements manually. The following figures illustrate the before, during and after states of the manual cleanup.

   The following figure is an example the screen that appears before the manual removal of the Elements.



   The following figure is an example of the screen that appears during the manual removal of the Elements.



Note:

Deleting elements from the UCM in this workflow is the expected behavior, and should not be a concern if the product data and configurations have been properly backed up in the step 1.

The following figure is an example of the screen that appears after the manual removal of the Elements.

4. Roles and permissions remain.

   The current uninstaller does not remove the added data products roles and permissions, and you cannot remove them manually. They remain in the system.

5. Install the same product with a different server type configuration.

   For installation procedure, see Joining a new data product (VPFM VPS COM BCM IPFM) member server to an Avaya CS 1000 based primary server on page 24.

6. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

The restore script prompts for the name of the backup .jar file.

Promoting an existing data product member server to a backup server

Perform this procedure to promote an existing data product (VPFM/VPS/COM/BCM/IPFM), member server to backup server status.

About this task

This workflow applies when a data network management product is deployed in the same security domain as the Avaya CS 1000 and must be reconfigured from member server to backup server. You must uninstall the product entirely and reinstall the product with a different server type configuration. The provided backup and restore utilities must be invoked to preserve the applications data and configurations.

Procedure

1. Invoke backup process.

   Use the following backup script to backup the product data and configurations.

   - In Linux: `$UCM_HOME/bin/backupAllData.sh`
   - In Windows: `%UCM_HOME%\bin\backupAllData.bat`

   The backed-up data is stored as a .jar file inside folder UCM_HOME/backups.

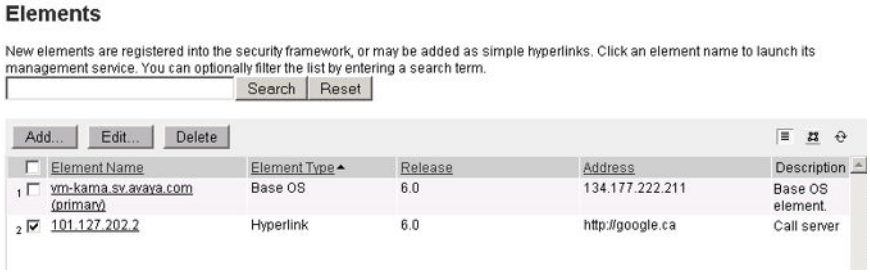
2. Uninstall the existing data product.

   Use the provided uninstaller executable to uninstall the product.

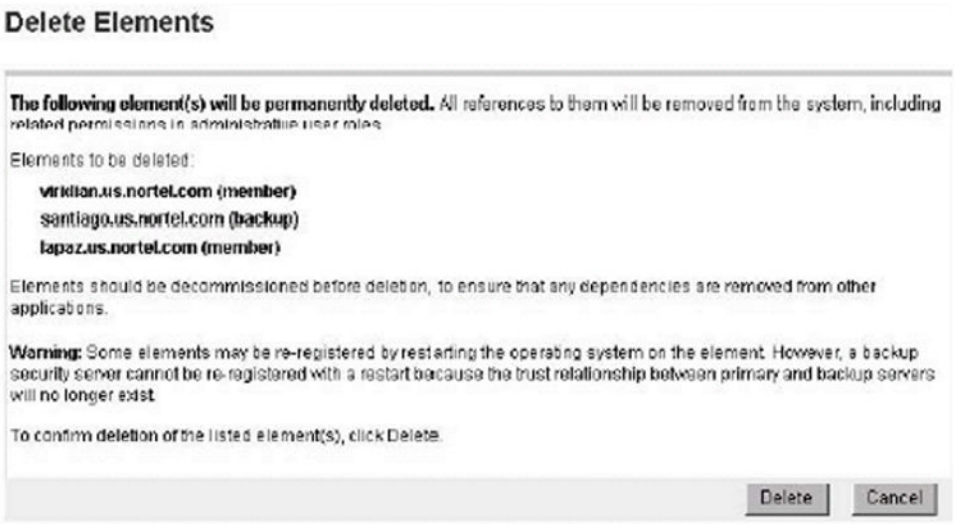
3. Cleanup the Elements Table from the GUI.

   The current uninstaller does not remove the added elements from the GUI, therefore you must remove the added elements manually. The following figures illustrate the before, during and after states of the manual cleanup.

   The following figure is an example the screen that appears before the manual removal of the Elements.



   The following figure is an example of the screen that appears during the manual removal of the Elements.



Note:

Deleting elements from the UCM in this workflow is the expected behavior, and should not be a concern if the product data and configurations have been properly backed up in the step 1.

The following figure is an example of the screen that appears after the manual removal of the Elements.

4. Roles and permissions remain.

   The current uninstaller does not remove the added data products roles and permissions, and you cannot them manually. They remain in the system.

5. Install the same product with a different server type configuration.

   For installation procedure, see Joining a new data product (VPFM VPS COM BCM IPFM) member server to an Avaya CS 1000 based primary server on page 24.

6. Invoke the restore process.

   Use the following restore script to restore the product data and configurations.

   - In Linux: `$UCM_HOME/bin/restoreAllData.sh`
   - In Windows: `%UCM_HOME%\bin\restoreAllData.bat`

The restore script prompts for the name of the backup .jar file.

Assigning voice and data products related roles and permissions to a single user

About this task

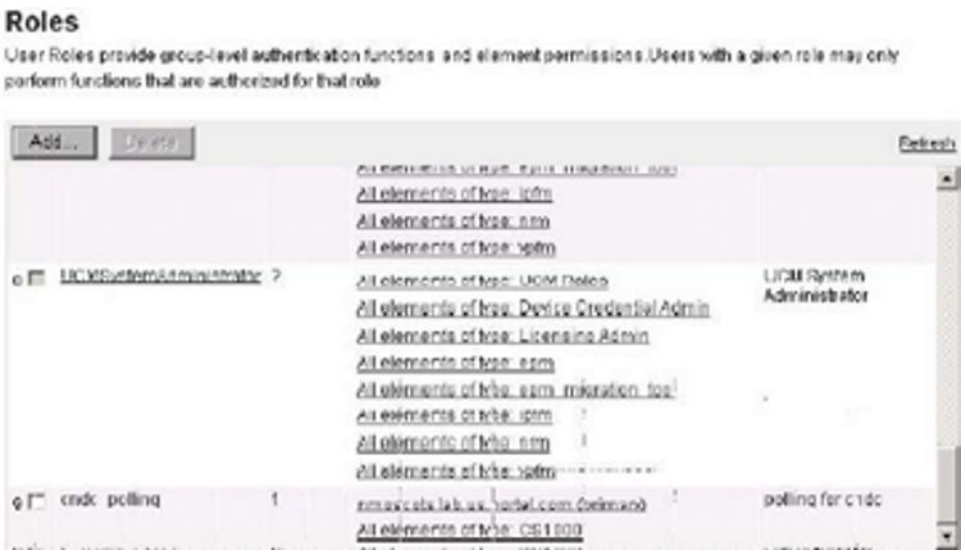
If a single user is required to manage both data and voice network, use this procedure to assign voice and data management roles and permissions to the single user.

Procedure

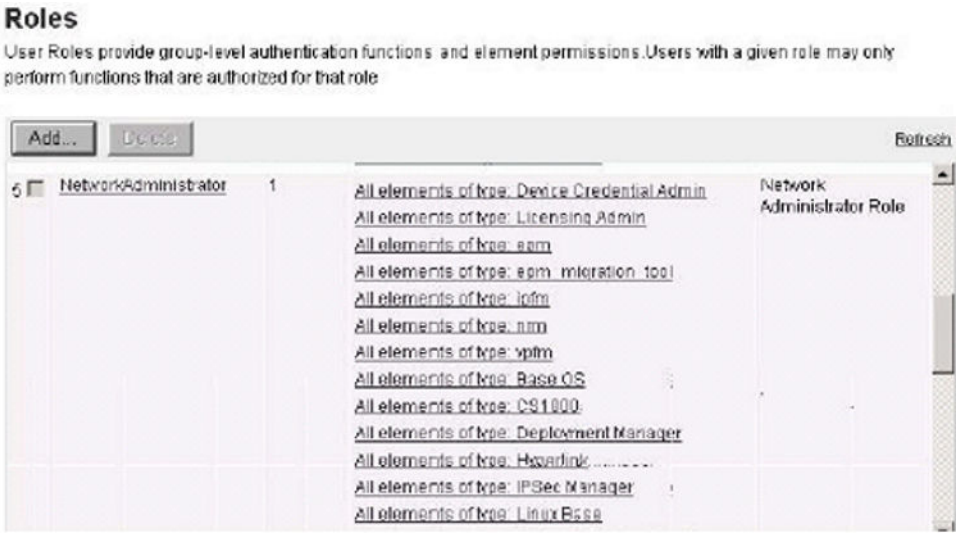
1. Assign elements permissions to roles

   Data products use three predefined roles: UCMOperator, UCMSystemAdministrator, and NetworkAdministrator. For more information about these roles, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014–100). Only the data elements permissions are assigned to UCMOperator and UCMSystemAdministrator, but both data and voice elements permissions are assigned to the NetworkAdministrator.

   The following figure is an example of data elements permissions assigned to UCMSystemAdministrator.

   The following figure is an example of voice and data elements permissions assigned to the NetworkAdministrator.



Voice products use predefined and administrator configurable roles. For more information about Management of Voicecentric roles and permissions, see *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116).

2. Assign roles to users.

   The following figure illustrates how the data related roles, such as UCMSystemAdministrator, and voice related roles, such as CS 1000 Admin, are assigned to the same user (NMOS).

Chapter 5: Application server coresidency

This document outlines the extension of support to various scenarios in which Avaya Unified Communications Management (Avaya UCM) Security domains contain both voice applications on one or more servers, and data applications on one or more servers. However, while domain coresidency support is being introduced, support is not currently being extended to the installation of voice and data functionality onto the same server, that is, server coresidency.

Existing support for coresidency of voice management applications on a single server remains unchanged. For more information, see the following documents:

- *Avaya Call Server 1000 Unified Communications Management Common Services Fundamentals* (NN43001-116)
- *Avaya Communication Server 1000 Linux Platform Base and Applications Installation and Commissioning* (NN43001-315)

Existing support for coresidency of data management applications on a single server remains unchanged. For more information, see *Avaya Unified Communications Management Common Services Fundamentals* (NN48014-100).

Chapter 6: Converged Avaya UCM deployments – known issues and resolutions

The following section provides resolutions to known issues with converged Avaya Unified Communications Management (Avaya UCM) deployments.

1. **Issue**

   No data network management application links (VPFM, VPS, COM, BCM, or IPFM) are added to the Avaya Communications Server 1000 (Avaya CS 1000) primary server if these data network management applications are installed as backup or member to the primary, then uninstalled and then reinstalled.

   Resolution

   After the backup/member data management applications are uninstalled, perform the following steps:

   - Stop the primary server
   - Stop the backup server
   - Stop all member servers
   - Start the primary server
   - Start the backup server
   - Start all member servers

2. **Issue**

   When a data application (VPFM, VPS, COM, BCM, or IPFM) is installed as the first member server and points to an Avaya CS 1000 primary server, sometimes the Avaya UCM roles (UCMOperator and UCMSystemAdministrator) do no appear on the Roles page. But, while creating a new role, and adding permissions mapping, the UCM permissions appear in the list. (CR Q02060973).

   Resolution

   Perform the following steps:

   - On the member server, go to the following folder:

     ```
     /opt/avaya/ucm/jboss-4.2.3.GA/server/default/conf/
     elementRegistry/elementType/deployed
     ```

- Modify version number from 1.0 to 1.1 (that is, <version>1.1<version>) in the following xml files:
  - UCMRolesElementType.xml
  - deviceCredentialAdminElementType.xml
  - licensingAdminElementType.xml
  - VPFMmoduleElementType.xml (only for VPFM)
  - VPSmoduleEleemntType.xml (only for VPS)
  - VPS_MIGRATION_TOOLmoduleElementType.xml (only for VPS)
  - COMmoduleElementType.xml (only for COM)
  - BCMmoduleElementType.xml (only for BCM)
  - IPFMmoduleElementType.xml (only for IPFM)
- Go to `https://[member-server-fqdn]/local-login`, where `[member-server-fqdn]` is the fully qualified domain name of the member server.
- Enter User ID as `root` (Linux), or `Administrator` (Windows), and the corresponding password of the system user. You must have administrative rights to the server, otherwise contact your system administrator.
- Choose the **Full security configuration** option, and click on the **Security Configuration** button. This reregisters the member server to the primary server and republishes the roles element types.
- You are only required to restart the primary server if you notice incorrect localization words for the above element types permission name.

3. **Issue**

   In a security domain where Avaya CS 1000 is installed as primary and the data applications (VPFM, VPS, COM, BCM, or IPFM) are installed as backup or member servers, occasionally the user cannot access the UCM login page after the CS 1000 primary server is restarted (CR Q02082801).

   Resolution

   Perform the following steps:

   - Stop the primary server.
   - Stop the backup server (if deployed).
   - Stop all member servers.
   - Start the primary server.
   - Start the backup server (if deployed).
   - Start all member servers.