AVAYA CONFIGURATION AND ORCHESTRATION MANAGER

Release 3.1

Release Notes

August 14th, 2014
Issue 1.2
CID: 166573

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

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

License types

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

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

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

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

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

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

Heritage Nortel Software

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

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

Copyright

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

Virtualization

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

Third Party Components

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

1. Summary

COM 3.1 Release Date: 14-August-2014

Purpose: The Configuration & Orchestration Manager (COM) 3.1 Release Notes provide the following information:

- New features introduced in COM 3.1
- General release information including Changes/Bug fixes in COM 3.1
- Supported operating systems, hardware requirements and browser clients
- Known issues and limitations

2. Important Notes before Installing this Release

COM 3.1 is a major release that uses a new platform based on **Avaya Aura System Manager version 6.3** and also adds several new features and device support. It also contains several changes that improve the memory management of the application and changes to improve network discovery.

Important!

- **COM r3.1** ends the support for 32-bit Operating Systems.
- **Only Microsoft Windows Server 2008 R2 (64-bit standard and enterprise editions) and Red Hat Enterprise Linux (RHEL) v5.6 and v5.7 (both 64 bit) are supported**.
- **The hardware requirements for the server have changed in COM r3**.1. Refer to section 4 of this document for details.
- COM 3.1 can be installed only as a Primary SMGR-CS server.
- Installer supports fresh installation of COM 3.1, as well as upgrade from COM 3.0[.x].
- Manual data migration is supported from existing installations of COM 3.0[.x].
- COM 3.1 does not support co-residency with VPFM.
- Virtualization Provisioning Service (VPS) version (v1.1) is compatible with COM 3.1; older versions of VPS are not supported on COM 3.1.
- COM 3.1 requires new licenses.

General Instructions:

- Please read this Release Notes completely before installing COM 3.1.
- The Linux bin file needs to have appropriate permissions before installing. Use the command: *chmod 777 <filename>* before executing the Linux installer.

3. What is new in this release

3.1. New in this release

❖ Device support

- Full Support for -
  - ERS 3500 v5.1.1 and v5.2
  - ERS 4500/4800 v5.6.3 and v5.7
  - ERS 5500/5600 v6.2.7, v6.3.1, and v6.6
  - VSP 7000 v10.2.1, v10.3, and v10.3.1
  - VSP 4000 v3.0.1 and v3.1
  - VSP 8000 v4.0
  - VSP 9000 v3.4 – added support for Sapphire Chassis
  - VSP 9000 v4.0 (ROF)
- Partial (Discovery and EDM Plugin) Support for –
  - VSP 4000 v4.0
  - ERS 4800 v5.8
- Support for ERS 8600/8800 and ERS 8300 devices running in ACLI mode (tested with v7.2.x for ERS 8600/8800 and with v4.2 for ERS 8300).

❖ Platform upgrade

- COM has been migrated to the Avaya Aura Systems Manager (v6.3) platform from the Avaya Unified Communication Manager (UCM) platform
- New platform uses JBoss 6.1.0 (old one was using JBoss 4.2.3).
- COM 3.1 is a 64-bit application (older versions of COM were 32-bit).

❖ New Features

- Support for Transparent-UNI VSN configuration (feature available on VSP 4000 v3.1 and VSP 7000 v10.3 and above versions)
- Support for Private VLAN / ETREE configuration (feature available on VSP 4000 v3.0.1 and later)
- Support for IP Multicast over SPBm configuration (feature available on ERS 8000 7.2 and above, VSP 9000 v3.4 and above and VSP 4000 v3.1)

❖ Enhancements

- Configurable BCM backup archive location
- Traps and Syslog purge based on number of records.
- Improved Memory Management
  - Limit COM user sessions to 5
  - Memory cleanup on session timeout
  - Limit number of open tabs in COM UI to 12
  - Memory cleanup on manager tab close
- Improved Network Discovery
  - Solution to known Hub issues
  - Solution to discovery hang (or taking too much time) due to the presence of large number of LLDP capable devices that are not L2/L3 Switches (e.g. Wireless Access Points, Media devices, IP phones)
- Improvements to EDM Plugin Management
  - One-click installation of all available (bundled with COM) required EDM plugins.
  - One-click uninstall of installed plugins that are no more required.
  - Disable/enable of plugin minor version mismatch warning message popup.
- Ability to launch Wireless Orchestration Service (WOS) from COM (launch point under Tools Menu)
- Ability to launch SLA-Mon from COM (launch point under Tools Menu)

3.2. Issues Resolved in this release

Following GRIPs have been addressed in this release.

GRIP	Description
5531	COM install simplification
6200	Preloaded EDM plug-in's
6926	Remove BCM limitation not allowing to run ACLI mode on ERS 8600/8800/8300
9023	Support of the CUG for the VSP 7000 and ERS 4800
10184	COM Multicast Manager needs to be re-written for SPB Multicast

Following bugs have been fixed in COM 3.1 release

WI id	Description
wi00933007	COM BCM / Configuration Backup & Restore – fails on 8600 ACLI mode
wi01087197	COM3.0.1-unknown hubs displayed between devices in topology map.
wi01088682 (SR-1-4176903096)	COM discovery hangs when trying to discover lldp connected devices.
wi01112984	COM3.0.1-snmp v3 discovery of network fails
wi01136438	COM Discovery systematically fails at startup with "bean error" message
wi01139877	COM 3.0.2 - Read Only user can make configuration changes using off-box EDM
wi01141125	COM/BCM3.0.2-scheduler displays no tasks
wi01142834	BCM3.0.2-unable to run backups or CUG
wi01144086 (SR-1- 4727723646)	Discovery displays topology incorrectly
wi01146509	COM 3.0.2-UCM Put and Delete method vulnerability
wi01149860	COM 3.0.2- Device Inventory View/470/show port status displays wrong card #s
wi01149956	Phones displayed as Media End Points
wi01150415	COM 3.0.2 4524GT-PWR (mixed stack) does not display in device inventory show port status
wi01159494	COM-discovery fails for vsp 9Ks
wi01174064	java.net.UnknownHostException during LLDP based discovery

4. Server and Client Requirements

4.1. Server Requirements

Hardware:

Following hardware/VM configuration is recommended for COM primary server setup.

HW Component	Critical	Minimum	Recommended
CPU	Quad-core 2GHz	Quad-core 2GHz	Quad-core 2GHz
Memory	4 GB	6 GB	8 GB
Free Disk Space	60 GB	60 GB	80 GB

Important!

- In COM 3.1, the RAM requirement has gone up by 2 GB.
- Virtual Machine Host: ESXi 5.0 and later is required. Support for ESXi 4.x is discontinued.

Operating System:

Operating system	Version
Microsoft Windows	Windows Server 2008 R2 (standard and enterprise editions)
Linux	64-bit RHEL v5.6 / v5.7

Application memory:

The heap memory requirement for COM depends on the size of the network that will be managed using COM.

Network Size	Heap Memory Requirement for COM (Recommended)
Small (< 250 devices)	4 GB
Medium (250 to 750 devices)	6 GB
Large (750 to 1500 devices)	8 GB *(Physical RAM on the m/c also needs to be increased accordingly)*

The default heap size for COM 3.1 is set to 4GB. If as per the above table, a higher heap size is required, please contact Avaya Support team to have them make the required changes to COM setup.

4.2. Client Requirements

Browser	Version
Internet Explorer (IE)	Versions 8, 9 and 10
FireFox (FF)	Versions 19, 20 and 21

5. Licensing

In COM 3.1, the version of the base license has been changed to 3.1 (from earlier 3.0). Hence, new licenses should be obtained for COM 3.1 and installed.

Important!

- Make sure to obtain new licenses for COM 3.1.

6. Supported Manual Upgrade Scenarios in COM 3.1

The following table shows how existing COM installations can be moved to COM 3.1.

Current installation	Upgrade Using Installer	Manual Data Migration	Procedure for Migration
COM 3.0[.x] Running on 32-bit Windows OS (any supported flavor)	No, this cannot be upgraded	Yes, COM data needs to be migrated	*See the manual migration section for windows*
COM 3.0[.x] Running on 32-bit RHEL (any supported flavor)	No, this cannot be upgraded	Yes, COM data needs to be migrated	*See the manual migration section for RHEL*
COM 3.0[.x] Running on Windows server 2008 R2 (standard/enterprise) OS	Yes, COM 3.0[.x] running on 2008 R2 can be upgraded	Yes. In case need to install COM 3.1 on a new host.	*See the manual migration section for windows*
COM 3.0[.x] Running on 64-bit RHEL v5.6/5.7	Yes, this can be upgraded	Yes. In case need to install COM 3.1 on a new host.	*See the manual migration section for RHEL*
COM 3.0[.x] Running on 64-bit Windows other than Windows server 2008 R2 (standard/enterprise edition)	No, this cannot be upgraded	Yes, COM data needs to be migrated	*See the manual migration section for windows*
COM 3.0[.x] Running on 64-bit RHEL other than RHEL v5.6/5.7	No, this cannot be upgraded	Yes, COM data needs to be migrated	*See the manual migration section for RHEL*
COM 2.3[.x]	No, this cannot be upgrade	No, data migration is not supported	*N/A*

6.1. Upgrading COM 3.0[.x] Using COM 3.1 Installer

The procedure for upgrading COM 3.0[.x] to COM 3.1 using the installer involves two major steps – first one in which a data backup and an uninstall of COM 3.0[.x] is done and the second one in which a fresh installation of COM 3.1 followed by restore of the old data is performed.

Upgrade using COM 3.1 installer is possible only on Microsoft Windows server 2008 R2 or RHEL v5.6/v5.7 (64-bits) servers.

Following steps describe the process in more detail.

- Data Backup and Uninstall of existing COM 3.0[.x] software using COM 3.1 Installer
    1. Start COM 3.1 Installer, accept the license agreement.
    2. Next, you will see a "Detection of Avaya UCM Application" window, where you will enter the **admin** user's password for your COM 3.0[.x] installation.
    3. Next, pre-upgrade checks will be run. If any errors reported, take corrective actions and re-run the checks until no more errors are reported.
    4. Next, an "Upgrade Summary" screen will be displayed detailing steps that will be taken for upgrade. It will also display the location where the data backup will be stored.
    5. Start data backup. (If backup fails the location of the log file will be displayed and upgrade cannot proceed. You need to exit).
    6. Once data backup is successful, the process will continue to uninstall COM 3.0[.x].
    7. After uninstallation is complete –
        - If the server is a Windows server, then you will be asked to reboot the server and then to re-run COM 3.1 installer.
        - If the server is an RHEL server, then you will be asked to re-run COM 3.1 installer.
- Installation of COM 3.1 and Data Restore
    1. Start COM 3.1 installer (again) and accept the license agreement.
    2. Proceeding further will continue will COM 3.1 installation as explained in the Chapter 6 (Installing COM Application) of COM Installation Guide.
    3. After installation is completed, you will be informed that the installer has detected a data backup of the older COM installation. You will also be given an option to restore the data to the new COM 3.1 installation (there will be "**Restore**" button on the screen). You can exit the installer, if you don't want to proceed with restore.
    4. Before, clicking to **Restore** the data, you will have to login to COM application using a browser and change the **admin** user's password. (Default password is **admin123**). Once this is done, on the installer screen, click "Restore".
    5. The old COM installation's data will be restored to COM 3.1 installation and installer will inform the progress and completion of the action.

NOTE:

If you are using VNC client to connect to the RHEL server for performing COM upgrade or a re-install (uninstall and fresh install), you may encounter the following issue.

- After uninstall of older COM installation, the environmental variables related to COM are not cleared from the VNC server and as a result new installation will fail, if the new installation folder

is different from the earlier one. The workaround for this is to kill and restart the VNC server after uninstallation and then do the new installation.

- Following are the steps of this workaround –
    - Un-install COM build X
    - Need to restart VNC server (*this was holding up all the ENV variables)*
        - *Login to server with telnet/ssh (putty)*
        - *Run the command – "vncserver -kill <X-display>" for ex: "vncserver –kill :1"*
        - *Run the command – "vncserver" (starts vncserver again)*
    - Login in back to host with VNC client
    - Open the new terminal
    - Restart the installation under a new install path.

6.2. Manual Data migration from existing COM 3.0[.x] installation

When the older version of COM (r3.0[.x]) exists on a server with 32-bit OS or on a 64-bit OS that is incompatible with COM 3.1 (e.g. 64-bit Windows Server R or 64-bit RHEL 5.4), then there is a need to migrate the UCM/COM data from the older server to a new installation of COM 3.1. This section explains how this can be done.

The following scenarios are possible.

1) Moving to COM 3.1 from COM 3.0[.x] running on 32bit OS
2) Moving to COM 3.1 from COM 3.0[.x] running on 64bit OS incompatible with COM 3.1.

Following steps describe the workflow for migrating from older version of COM to COM 3.1.

Pre-requisite: Older version (release 3.0[.x]) of COM running as UCM Primary.

Steps for Windows servers:

1. Download the file `Migration_From_32Bit_UCM_To_SMGR-CS.zip` from the same Avaya Support page from which you downloaded COM 3.1 installer and unzip it. In its content you will find another zip file named - `ucm-to-smgr-migration-windows.zip`.
    a. Go through the **ReadMe** file in the main zip file you have downloaded, before proceeding further.
    b. Now unzip the file `ucm-to-smgr-migration-windows.zip`.
2. Back up the data on COM 3.0[.x].
    a. Take back up on UCM by running the script ***backupDataMigration.bat.***
    b. Upon successful completion, it will generate a jar file (like 2013-11-06_13.06.jar) and a zip file (as JbossQuantumMigration.zip) in the backups folder of UCM (<UCM-dir>\backups\).
3. Install COM 3.1 on a 64-bit Windows 2008 R2.
4. **Obtain new COM 3.1 License and install the license**.
5. Now Copy the backup data jar file to backups folder in SMGR-CS (<smgr-dir>\backups\>) and zip file to the **<smgr-dir>\core\tmp** folder on windows.
6. To restore the data on SMGR-CS, run ***restoreDataMigration.bat*** present in COM 3.1 <smgr-dir>\bin.
7. Upon successful completion, login to SMGR-CS and verify if the app is functioning as expected and that the data has been restored from UCM. The default username is "admin" and default password is "admin123" (both without quotes).
8. This completes the data migration from COM 3.0[.x] on UCM Primary to COM 3.1 on SMGR-CS Primary.

Steps for RHEL servers:

1. Download the file `Migration_From_32Bit_UCM_To_SMGR-CS.zip` from the same Avaya Support page from which you downloaded COM 3.1 installer and unzip it. In its content you will find another zip file named - `ucm-to-smgr-migration-linux.zip`.
    a. Go through the **ReadMe** file in the main zip file you have downloaded, before proceeding further.
    b. Now unzip the file `ucm-to-smgr-migration-linux.zip`.
2. Please, follow the instructions in it to back up the data on COM 3.0[.x].
    a. Take back up on UCM using ***backupDataMigration.sh***.
    b. Upon successful completion, it will generate a jar file (like 2013-11-06_13.06.jar) and a zip file(as JbossQuantumMigration.zip) in the backups folder of UCM (<ucm-dir>/backups/).
3. Install COM 3.1 on a 64-bit RHEL v5.6/v5.7 host.
4. **Obtain new COM 3.1 License and install the license**.
5. Now Copy the backup data jar file to backups folder in SMGR-CS (<smgr-dir>/backups/) and zip file to the **/tmp** folder.
6. To restore the data on SMGR-CS, run ***restoreDataMigration.sh*** present in COM 3.1 <smgr-dir>/bin.
7. Upon successful completion, login to SMGR-CS and verify if the app is functioning as expected and that the data has been restored from UCM. The default username is “admin” and default password is “admin123” (both without quotes).
8. This completes the data migration from COM 3.0[.x] on UCM Primary to COM 3.1 on SMGR-CS Primary.

7. Limitations and Known Issues

COM 3.1 has the following limitations and known issues.

7.1. Limitations

- No space character is allowed in the path name for the installation folder (pre-check exists in the installer) – a limitation inherited from JBoss 6.1.0
- Configuration Audit Tool (CAT) does not support ERS8k devices running in ACLI mode.

7.2. Known Issues

- Installation/Upgrade related:
    - COM installer requires the system language to be set to English(US).
- Discovery related:
    - Stop discovery does not stop the network discovery, but the discovery progress bar disappears giving a false impression to the user indicating discovery has stopped.
- EDM Manager:
    - JDM (for sw versions of devices that are old and do not have EDM plugin) does not work with Java 7. If your browser has Java 7 plugins/add-ons installed, you need to disable it and use Java 6 plugins.
- Limitations/issues in COM support for VSP7000:

- COM does not discover a VSP7k device which uses only Out-of-band management using the dedicated management port.
- Inventory Manager actions give error (“noCreation” SNMP error) for ASCII config file upload/download for VSP7k. Inventory Manager binary config upload/download may require increasing the SNMP timeout in the Preferences to 10sec or more. (Applies to VSP7k sw 7.2.x and older).

- VSP7000 Device Limitations affecting COM functionality:
  - SONMP packets are not sent on BEB-BCB ISIS links (even when device is SONMP enabled). Therefore, these links are not discovered by COM and to discover both devices, both of them need to be specified as seeds. “Dump Topology” does not show these links; but “Show Connections” do.
  - TACACS settings and Web Password settings related SNMP MIBs are not supported in VSP7k. So these operations will result in “noCreation” SNMP error.
- MLT Manager related:
  - Removing last VLAN from an active MLT could cause loss of connectivity to the device. COM does not show any warning when this is attempted.
- Tools related:
  - CLI*Manager tool (a Java Webstart application), when first launched creates <OS login name>.ppk file in the specified “working directory”. But the tool expects this file to be in the following location –
    - Windows – Same directory from where CLI*Manager is launched (typically the Desktop)
    - Linux – In the /root/ directory.

    So, move the file <OS login name>.ppk to the above directory from the specified “working directory” and re-launch CLI*Manager.
  - If Firefox is your default browser, then for CLI*Manager to work, you need to set the browser proxy settings to “Use System Proxy settings”.
  - TFTP Server tool – the “Root directory” and “Log file name” specified in the tool’s preferences do not indicate where they are located on the server. The location is dependent on the OS, and are relative to the following path –
    - Windows – they are relative to <JBOSS_HOME>/bin/
    - Linux – they are relative to the root directory /.
  - CAT Tool opens a blank page from IE9.x and IE10.x with a JavaScript error. It works fine on IE8 and also in all supported versions of FireFox browser.
- Browser support related:
  - License installation does not work with IE browsers when the absolute path to the license file to be installed contains a directory whose name has a dot (“.”) in it (e.g. C:\licenses\COM3.1\myLicense.lic).
- Virtual Machine related:
  - TFTP data transfer does not work properly (times out) when the VNIC used by the Virtual Machine is of type VMXNET3. It is recommended to use E1000 type of VNIC for the Virtual Machine.

8.Miscellaneous Information

8.1. General Info

- **Default User ID and Password** for accessing newly installed Aura System Manager based COM is **admin / admin123**
- After installation/upgrade completes successfully as well as after a restart of the COM application, it takes a few minutes (about 5mins) for the application to be available for client access.
- **By default, network discovery using LLDP is disabled in COM 3.1**. It can be enabled or disabled from the Preferences UI. Note, that the issue of discovery hang (taking too long) because of large number of LLDP enabled end point devices has been fixed in COM 3.1.
- BCM related:
    - BCM email alert feature is available only with COM upgrade 1200-1500 license. It is not obvious in the UI.
    - Make sure that your anti-virus software does not block “mass emails” for BCM email alert to work.
    - BCM Device Password Manager (DPM): When a device password/community is changed using DPM, the entry for the device in the Device Credentials table is updated with the new password/community value. If the device credentials is specified using an IP address range, then a new entry will be created for the device. This updating of the Device Credentials table will not happen if there exists more than one credential entry for that device and they have different (and non-empty) password/community value.

8.2. Recommendations for Improved Network Discovery

Along with the fixes provided in COM 3.1 to improve the Network Discovery in COM, to obtain a topology containing no hubs, the following recommendations need to be followed.

Following set of procedures to be followed on modular devices (ERS 8k series, VSP 9k series, VSP 4k series and VSP 8 k series) to force/prioritize a device to always send the configured management IP Address in the SONMP Discovery packets. This will result in the auto topology table on its neighbor devices to contain the management IP Address of the device instead of the IP Address of the interface of the device that connects to the neighbor.

This helps COM network discovery to clearly identify the end devices of each link, even when the interface IP addresses are duplicated in the network, resulting in significant reduction in the number of logical hubs (physically non-existing) being displayed in COM topology.

8.2.1. Procedure to force management IP:

ERS 8600/8800 (ACLI mode):

Using ACLI user interface, execute the following commands in the config mode:

```
(config)# sys force-topology-ip-flag enable
(config)# show sys setting
        …
        ForceTopologyIpFlag : true
        clipId-topology-ip: X
        …
```

(If clipId-topology-ip is not 0, then find out the IP address for the CLIP id X using 'show ip interface' command and run the following command)

```
(config)# no ip address x.x.x.x/x
(config)# show sys setting
        …
        ForceTopologyIpFlag : true
        clipId-topology-ip: 0
        …
```

ERS 8600/8800 (CLI mode):

Using CLI user interface, execute the following commands in the config mode:

```
(config)# sys set force-topology-ip-flag true
(config)# show sys set-topology-ip
        #------  TOPOLOGY-CLIP-IP  ------#
        clip-ip Set as Topology-ip : <ipaddr>
```

(If a clip-ip has been set, then use the command below to delete that clip)

```
(config)# ip circuitless-ip-int <id> delete <ipaddr>
(config)# show sys set-topology-ip
        #------  TOPOLOGY-CLIP-IP  ------#
```

VSP 9000, VSP 8000 and VSP 4000:

Using ACLI user interface, execute the following commands in the config mode:

```
(config)# sys force-topology-ip-flag enable
(config)# default sys clipId-topology-ip
(config)# show sys setting
      …
      ForceTopologyIpFlag : true
      clipId-topology-ip : 0
      …
```

8.3. Workaround for script running slowly - browser issue

COM uses java script technology which executes scripts on the client browser. However, for large configurations, the script may take longer to execute and may be seen by the browser as a loop that may need to be terminated by the user. This issue is more pronounced in IE. If such an issue is encountered, you will see pop-ups asking whether you want to terminate the script. You can select No (In IE) and Continue (in FF) to ignore this pop-up or you may permanently change the time after which the pop-up is seen (or disable it completely). To change your browser settings, use the following instructions:

For Firefox:

Type about:config in the address bar and filter for the string dom.max_script_run_time. The default setting is 20 (seconds), add some more time, raise it to 40 for instance.

For Internet Explorer:

Using a Registry Editor such as Regedt32.exe, open this key:
HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Styles

Note If the Styles key is not present; create a new key that is called Styles.
Create a new DWORD value called "MaxScriptStatements" under this key and set the value to the desired number of script statements. If you are unsure of what value you need to set this to, you can set it to a DWORD value of 0xFFFFFFFF to completely avoid the dialog.

By default the key doesn't exist. If the key has not been added, the default threshold limit for the time-out dialog box is 5,000,000 statements for Internet Explorer 4 and later.

More information is available at http://support.microsoft.com/kb/175500

8.4. General Recommendations

To circumvent some of the known issues, the following recommendations should be adhered to:

- For using the email feature in COM (including BCM) or to test email feature through the test button, the Firewall and Antivirus should have a rule to allow COM to send email. If email is blocked on the COM server, the user will see an error “Message Exception” and the email will not be sent.
- It is recommended to enable SONMP protocol on devices even if LLDP is enabled – since some types of devices do not support LLDP currently, they will not be discovered using seeds which have only LLDP enabled.
- It is recommended that you do not import Device Inventory xml file from an older versions of COM (COM 2.3, 2.3.x) into COM 3.1. Device inventory xml exported in COM 3.0[.x] is compatible with COM 3.1.
- IE9 and IE10 browser requires the setting of Tools/internet options/advanced – ‘Do not save encrypted pages to disk’ to be un-checked in-order for the JDM tool to be launched correctly.
- BCM operations such as CUG might require pagination to be disabled based on the user script. In case of ERS 35xx/4xxx/5xxx, check the terminal length on the device using CLI. Set terminal length to 0. In case of ERS 83xx/86xx/88xx, check the CLI settings on the device and make sure “more” is set to false.

9.List of COM documents

Following is a list of documents available for Configuration and Orchestration Manager (COM) Release 3.1.

1. Release Notes (this document) - Avaya Configuration and Orchestration Manager Release 3.1
2. NN47226-300 Issue 07.01, Avaya Configuration and Orchestration Manager Installation
3. NN47226-100 Issue 07.01, Avaya Configuration and Orchestration Manager Fundamentals
4. NN47226-600 Issue 08.01, Avaya Configuration and Orchestration Manager Administration
5. NN48021-100 Issue 05.01, Avaya Bulk Configuration Manager Fundamentals
6. NN48014-100 Issue 05.01, System Manager Common Services Fundamentals

These documents are available at Avaya Support site (support.avaya.com).

Appendix: Device Support (comprehensive list)

Following devices are officially supported by COM 3.1

Device	Software release
Virtual Services Platform 4000	3.0, 3.0.1, 3.1, 4.0(partial support)
Virtual Services Platform 8000	4.0
Virtual Services Platform 9000	3.0, 3.1, 3.2, 3.3, 3.4, 4.0
Ethernet Routing Switch 8600 & 8800 including the following hardware: 8681XLW module, 8681XLR module, 8616GTE module, 8672ATME MDA, 8608GBM module, 8608GTM module, 8632TXM module, 8648TXM module, 8672ATMM module, 8683POSM module.	4.0, 4.1, 5.0, 5.1, 7.0, 7.1, 7.1.3, 7.1.5, 7.2, 7.2.10
Virtual Services Platform 7000	10.1, 10.2, 10.2.1, 10.3, 10.3.1
Ethernet Routing Switch 55xx/56xx	5.1, 6.0, 6.1, 6.2, 6.3, 6.6
Ethernet Routing Switch 45xx/48xx	5.2 , 5.3, 5.4, 5.5, 5.6, 5.6.1, 5.6.2, 5.7, 5.8(partial support)
Ethernet Routing Switch 35xx	5.0, 5.0.1, 5.0.2, 5.1, 5.1.1, 5.2
Ethernet Routing Switch 25xx	4.1.x, 4.2, 4.3, 4.4
Ethernet Routing Switch 16xx	2.1.5.x, 2.1.6.x
WLAN	23xx, AP 23xx
WLAN WC8100, AP8120	1.0, 1.1, 1.2
Belden	6.0.2

NOTE: “partial support” implies device discovery, topology display and installation and launching of EDM plugin are the only features supported.

Following device support is available with COM 3.1 but the test coverage on these devices isn’t complete (should work but lacks official support)

Device	Software release
Ethernet Routing Switch 8600, including the following hardware: 8681XLW module, 8681XLR module, 8616GTE module, 8672ATME MDA, 8608GBM module, 8608GTM module, 8632TXM module, 8648TXM module, 8672ATMM module, 8683POSM module.	3.0, 3.0.x, 3.1.x, 3.2.0, 3.2.0.2, 3.2.1.0, 3.2.2, 3.3, 3.5, 3.7
Ethernet Routing Switch 8600 Web Switching Module	WebOS 9.x, 10.0.x
Ethernet Routing	2.0, 2.0.1.1, 3.1.x, 3.2.0, 3.2.0.2, 3.2.1.0, 3.2.2, 3.3

Switch 8100	
Ethernet Routing Switch 8300	2.0, 2.1, 2.2, 2.2.8, 2.3, 3.0, 4.0, 4.1, 4.2
Passport 1050/1150/1 200/1250	2.0.5.6, 2.0.5.7, 2.0.7.2, 2.0.7.3, 2.0.7.4, 2.1.0, 2.1.3
Ethernet Routing Switch 1424T	2.1
Ethernet Routing Switch 1612G, 1624G, 1648T	1.0, 1.2, 2.1
BayStack 350/410/ 450	3.0, 3.1, 4.0, 4.1, 4.2, 4.3, 4.4
Business Policy Switch 2000	1.0, 1.0.1, 1.1, 1.2, 2.x, 3.0, 3.1
BayStack 380-24 T	2.0, 3.0
BayStack 420	1.0, 1.0.2, 1.1, 1.1.1, 1.1.2,1.1.3, 3.0, 3.1
Ethernet Switch 460	2.3, 3.0, 3.1, 3.5, 3.6, 3.7
Ethernet Switch 470-24 T	3.0, 3.0, 3.1, 3.5, 3.6, 3.7
Ethernet Switch 470-48 T	2.1.0 (standalone only), 2.2.0, 2.2.1 (stack also supported), 3.0, 3.0, 3.1, 3.5, 3.6, 3.7
Ethernet Switch 425-24T	2.0, 3.0, 3.0, 3.1, 3.5, 3.6
Ethernet Switch 425-48T	3.1, 3.5, 3.6
Ethernet Routing Switch 5510, 5520	3.0, 3.0.0.1, 4.0, 4.1, 4.2, 4.3, 5.0
Ethernet Routing Switch 5530	4.2, 4.3, 5.0
Ethernet Routing Switch 3510	4.0
Ethernet Routing Switch 45xx	5.0
Ethernet Routing Switch 25xx	4.0, 4.1.x, 4.2
Alteon 2208, 2216, 2224, 2424, 2424 SSL, 3408	AOS 21.0
OPTera Metro 1200/1400/1450	1.0, 1.2, 1.3
WLAN 2200 AP	1.3