Overview of Avaya Aura® System Platform

Release 6.2.1
July 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notices

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 Web sites 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 Web site: 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.

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 End User a license within the scope of the license types described below. 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 End User. “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. “Software” means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. “Hardware” means the standard hardware originally sold by Avaya and ultimately utilized by End User.

License types

Designated System(s) License (DS). End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified 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 communicate 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 by Avaya 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). End User 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). Customer 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”). (see “Third-party Components” for more information).

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

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright.

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 Web site: 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.

All non-Avaya trademarks are the property of their respective owners.

PuTTY is copyright 1997-2009 Simon Tatham.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support Web site: 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 Web site: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: System Platform overview 7
Chapter 2: What's new in System Platform Release 6.2 13
Enhanced High Availability 13
SAL deployment on Services Virtual Machine 14
SNMP MIB-2 support 14
Customer provided hardware 15
Kernel and RPM patching and rollback 15
Index 17

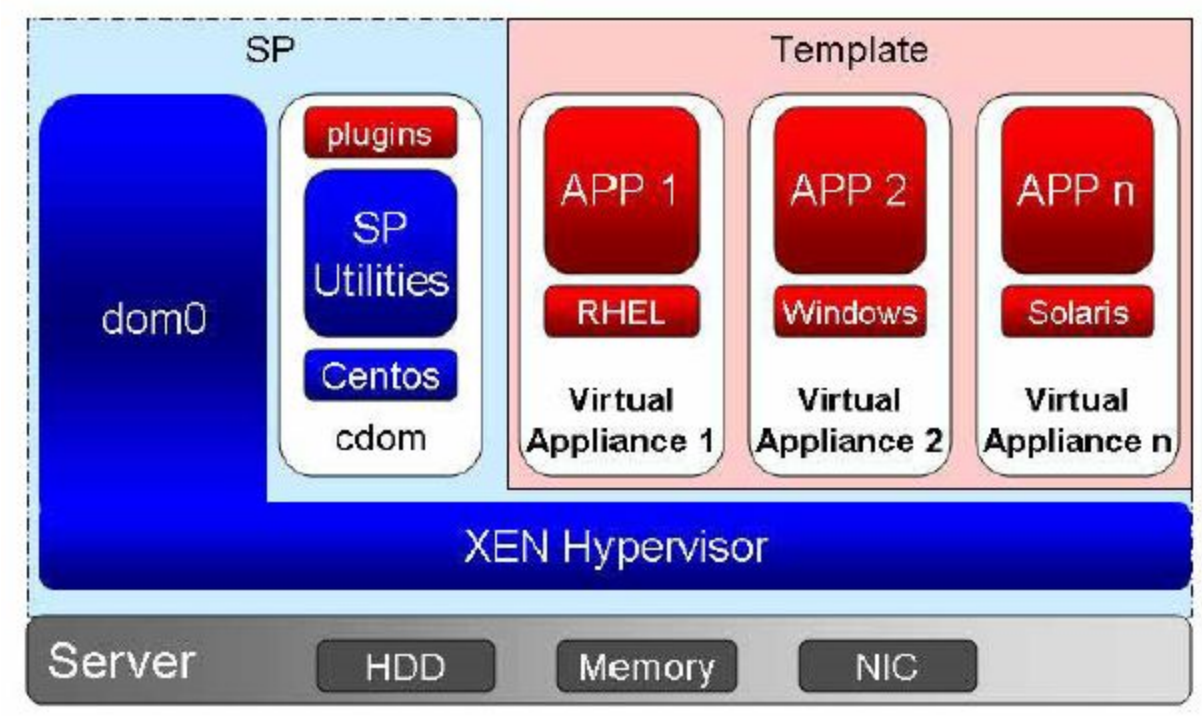
Chapter 1: System Platform overview

Avaya Aura® System Platform technology delivers simplified deployment of Unified Communications and Contact Center applications. This framework leverages virtualization technology, predefined templates, common installation, licensing, and support infrastructure.

System Platform:

- is a software platform running CentOS plus Xen open source hypervisor for virtual machine monitoring and management
- hosts one or more Avaya products, each running on its own virtual server (virtual machine), all running on a single physical server platform
- provides a set of utilities commonly required for Avaya products, including installation, upgrade, backup/restore, licensing server, hardware monitoring and alarming, and remote access

The following figure shows an abstraction of the System Platform virtualized environment:



Avaya deploys System Platform through a *virtual appliance* model. The model includes:

- An Avaya-defined common server platform
- An Operating System (O/S) for allocating and managing server hardware resources (CPU, memory, disk storage, and network interfaces) among virtual machine instances running on the server platform

- System Platform
- An Avaya solution template containing a bundled suite of pre-integrated Avaya software applications
- A Secure Access Gateway, supporting a Secure Access Link (SAL) for remote diagnosis by Avaya or an Avaya Partner.

The advantages of System Platform include:

- Consolidation of servers
- Simpler maintenance
- Faster disaster recovery
- Easy installation of any Avaya Aura® solution template (bundled applications suite) on a single server platform
- Simpler and faster deployment of applications and solutions
- Efficient licensing of applications and solutions
- Security
- Portability of applications
- Reduction of operating costs
- Avaya common look-and-feel Web Console (Web Graphical User Interface) for server, virtual machine, application, and overall solution management.
- Remote access and automated alarm reporting for Network Management Systems monitored by Avaya Services and Avaya Partners personnel
- High Availability option for failover using active and standby servers
- Coordinated backup and restore
- Coordinated software upgrades

Installation

Avaya provides an installation wizard program for System Platform software on Avaya-defined common server platforms.

Following System Platform installation, you install Avaya Aura® solution templates on the same server. Template installation significantly streamlines solution deployment across your organization. Installation wizard software installs a solution template in less time than if you installed multiple applications individually. The installation process is simple and requires only personnel with basic software installation skills. System Platform also supports remote installation of Avaya Aura® solution templates.

Virtual machines

System Platform interacts with the following virtual machines:

- System domain (`dom0`) virtual machine
- Console domain (`cdom`) virtual machine
- Services domain (`services_vm`) virtual machine
- Template virtual machines

System domain virtual machine:

In addition to exporting virtualized instances of CPU, memory, network and block devices, the system exposes a control interface to manage how these resources are shared between the running domains. Access to the control interface is restricted to one specially-privileged virtual machine, known as domain 0 or System Domain.

Console domain virtual machine:

The Console Domain virtual machine is a part of System Platform and contains many platform elements, including the System Platform Web Console.

The Console Domain is capable of deploying and running the following plug-ins:

- Virtual Appliance (VA) plug-ins, which interact with virtual appliances for operations such as backing up and restoring data, providing sanity heartbeats, and getting version information
- Preinstallation plug-ins, which accept parameters that are configured by the user at the time of installation
- Post-installation plug-ins
- Backup plug-in
- Restore plug-in
- Patch plug-ins, which install or uninstall patches in the system

In the System Platform Web Console, the Console Domain displays as **cdom**.

In its virtual machine command line, the Console Domain displays as **udom**.

Services domain virtual machine:

The Services virtual machine (Services_vm) hosts embedded SAL operations for remote monitoring and diagnosis.

Template virtual machines:

During template installation, System Platform creates one or more template virtual machines, where each virtual machine provides an independent virtual server environment for one Avaya Aura® applications. All of the applications running on the various template virtual machines together deploy an Avaya Aura® solution.

Solution templates

A solution template is a set of one or more Avaya applications pre-integrated for easy installation on System Platform. Installation personnel must download these templates using the Product Licensing and Delivery System (PLDS) (http://plds.avaya.com). PLDS allows Avaya customers, Avaya Partners, and associates to manage software licensing and to download software for various Avaya products.

System Platform provides an installation wizard for the template. The installation wizard enables you to configure template-specific parameters, including network and server details, or to upload a preconfigured Electronic Preinstallation Worksheet (EPW) created in a stand-alone version of the installation wizard.

Note:

You must install System Platform before installing solution template software on a single server. Some solutions offer a server with System Platform and an Avaya Aura solution template pre-installed.

Networking

System Platform uses software bridging to support networking for virtual machines. Software bridging works like a network switch inside the system. During installation, System Platform creates two software bridges: *avpublic* and *avprivate*.

The avpublic bridge connects to a physical interface and serves as the default connection to your LAN. Most virtual machines have a virtual interface on the avpublic bridge to connect to your network. You can reach avpublic IP addresses by using PING over your network.

The avprivate bridge does not connect to any physical interface, but instead provides internal communication among the virtual machine instances running on a single server hardware platform. You cannot reach avprivate IP addresses by using PING over your network.

Some templates require additional connections to your network. In some cases, System Platform creates another software bridge for this purpose. This bridge contains the name specified by the template, and the name is visible during template installation or in the Network Configuration page.

If a virtual machine has high or real time traffic requirements, it can be assigned a dedicated network interface card (NIC) in the template file. This means that the virtual machine is assigned another physical NIC on the system and does not use avpublic. For example, in the Solution for Midsize Enterprise, Application Enablement Services uses eth3. See related solution template documentation for more information.

If a virtual machine in the installed template requires a dedicated NIC, it must have a separate cable connection to your network. Both the avpublic interface and the dedicated NIC must be connected to the network for those machines to communicate in the same way as if they were separate physical machines. For example, in the Solution for Midsize Enterprise, the Console Domain is on the avpublic bridge and Application Enablement Services has a dedicated NIC (eth 3). In this case you must connect eth0 and eth3 to the network before attempting to ping the Application Enablement Services virtual machine from the Console Domain.

High Availability

System Platform applications can have high availability through a redundant hardware and software setup. The primary node continuously updates the secondary node with any changes in system configuration or runtime data. When the primary server fails, the secondary server uses that data to restore all functionality to the system. For more information, see the System Platform High Availability introduction in your solution template documentation.

Note:

System Platform High Availability is available only with supporting solution templates. (Some templates implement a different, solution-specific, High Availability configuration independent ofSystem Platform High Availability.)

Remote serviceability

Avaya or Avaya Partner support personnel can access and service System Platform from a remote location so that a site service call becomes unnecessary.

System Platform uses Secure Access Link (SAL), which is an Avaya serviceability solution for support and remote management. SAL provides remote access and alarm reporting capabilities for Avaya and Avaya Partners.

SAL uses your existing Internet connectivity to facilitate remote support. All communication outbound from your environment uses encapsulated Hypertext Transfer Protocol Secure (HTTPS). This is just one of many security features used by SAL to support secure remote access.

Avaya Partners without a SAL Concentrator must provide their own IP-based connectivity (for example, B2B VPN connection) to deliver remote services.

Important:

The SAL Gateway in the Services Virtual Machine or on a stand-alone server supports System Platform and Avaya Aura® solution templates. Avaya Partners and customers must register SAL, the solution template, and System Platform with Avaya during installation, and must configure SAL for remote support. Avaya support will be delayed or circumvented if SAL is improperly implemented or inoperative. System Platform and SAL do not support modem connections.

Chapter 2: What's new in System Platform Release 6.2

Avaya Aura® System Platform 6.2 builds upon the previous release (6.0.*x*) and offers the following features:

- Enhanced High Availability (solution-dependent)
- SAL deployment on Services Virtual Machine
- SNMP MIB-2 support
- Customer provided hardware (solution-dependent)
- Kernel and RPM patching and rollback

Important:

Some features exist only if explicitly supported by your Avaya Aura® solution template. Features unsupported by your solution template will be absent from the System Platform Web Console GUI. For more information, refer to feature topics in your Avaya Aura® solution documentation.

For more information about these features beyond the brief descriptions provided here, refer to System Platform administrative topics in your Avaya Aura solution documentation.

Enhanced High Availability

System Platform supports multiple modes of High Availability operation, facilitating efficient failover from a primary node to a secondary node with little or no interruption in system services. The modes are:

- Fast Reboot High Availability (FRHA)
- Machine Preserving High Availability (MPHA)
- Live Migration High Availability (LMHA, used only with MPHA))

System Platform FRHA mode was available prior to System Platform version 6.2. The two new HA modes (MPHA/LMHA) implement a new Virtual Server Synchronization Technology (VSST) offering on System Platform.

Note:

Your Avaya Aura® solution template must specifically support MPHA mode for it to be configurable in pages of the System Platform Web Console.

Note:

Avaya Aura System Platform High Availability does not support:

- IPv6 and cannot be configured with IPv6 addresses.
- Customer provided servers.

For more information about specific HA mode support, refer to your Avaya solution template documentation, available from http://support.avaya.com.

SAL deployment on Services Virtual Machine

Beginning with System Platform release 6.2, the Secure Access Link Gateway (SAL gateway) no longer runs on the System Platform Console Domain (cdom) virtual machine. Instead, SAL 2.1 runs on an independent Services Virtual Machine (services_vm domain) on your Avaya Aura® solution server. As with the prior implementation of the SAL gateway running on the cdom virtual machine, this new configuration supports secure remote access to local server resources, and forwards alarms (SNMPv2 or v3 traps) from your local solution server to a remote Network Management System (NMS).

SNMP MIB-2 support

By default, this feature enables SNMPv2 management systems to automatically discover any System Platform server in an Avaya Aura®-based network, including retrieval of server status and vital statistics. This is useful, for example, when using System Manager to view the entire inventory of System Platform servers across multiple Avaya Aura® enterprise solutions at a glance. This feature eliminates the tedious and error-prone task of manually adding a large number of System Platform servers to an SNMP management system, where that system typically requires three or more IP addresses for each System Platform server instance. SNMP management systems can also query any recognized System Platform server for its logical configuration.

Customer provided hardware

System Platform can run on customer-provided server platforms that meet Avaya-specified hardware requirements for the System Platform itself, for a specific Avaya Aura® solution template, and for any configuration options you require in your system.

Since each Avaya Aura® solution template has different requirements for server resources, configuration, capacity, and performance, refer to your Avaya Aura® solution template documentation, available from http://support.avaya.com.

Kernel and RPM patching and rollback

Using **Patch Management** features of the Web Console, you can install, commit, roll back (undo), or remove kernel patches. (These are patches applied to the CentOS kernel for System Platform.) The manual rollback feature allows you to test a patch before committing it to the system. The automatic rollback feature enables the system to autonomously recover from problems resulting from patch installation, or from an administrative lockout after installing a patch remotely over the Secure Access Link.

Index

C

Customer provided server hardware 15

H

High Availability 13
- Live Migration HA (LMHA) 13
- Machine Preserving HA (MPHA) 13
- System Platform 13

K

Kernel 15
- patching and rollback 15

L

legal notices 2

M

MIB-2 support 14

N

notices, legal 2

O

overview 7
- System Platform 7

P

Patching and rollback 15
- kernel and RPM 15

S

SAL 14
- deployment on Services VM 14

Servers 15
- customer provided 15

Services VM 14
- SAL deployment on 14

SNMP 14
- MIB-2 support 14

System Platform 7, 13
- High Availability 13
- overview 7
- what's new in 13