Deploying Avaya Aura® System Manager on Kernel-based Virtual Machine

Release 7.1
Issue 1
August 2017

Notice

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

Documentation disclaimer

“Documentation” means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of 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 or on the express behalf of Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

“Hosted Service” means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. 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 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.

Contents

Chapter 1: Introduction

Purpose

This document describes how to deploy the Avaya Aura® System Manager Kernel-based Virtual Machine (KVM) OVA.

This document is intended for people who install and configure System Manager KVM OVA at a customer site.

Prerequisites

Before deploying the System Manager KVM OVA, ensure that you have the following knowledge, skills and tools.

Knowledge

- KVM hypervisor installation and set up
- Linux® Operating System
- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager

Skills

To administer the KVM hypervisor and Avaya Aura® applications.

Tools

For information about tools and utilities, see “Configuration tools and utilities”.

Chapter 2: Avaya Aura® on Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

You can deploy the following Avaya Aura® applications on KVM:

- Avaya Aura® System Manager Release 7.1.1
- Avaya Aura® Session Manager Release 7.1.1
- Avaya Aura® Communication Manager Release 7.1.1
- Avaya Aura® Utility Services Release 7.1.1

  Note:

  Utility Services 7.1.1 requires the Utility Services 7.1 KVM image.
- Avaya Aura® Application Enablement Services Release 7.1.1
- Avaya Aura® Media Server Release 7.8 SP5 (Software only)
- Avaya Diagnostic Server Release 3.0 (Software only)
- Avaya Session Border Controller for Enterprise Release 7.2

Chapter 3: Planning and preconfiguration

Planning checklist

Ensure that you complete the following before deploying the System Manager on KVM:

No.	Task	Link/Notes	✔
1.	Download the required software.	See “Configuration tools and utilities” and “Release details of System Manager KVM OVA”	
2.	Purchase and obtain the required licenses.	—	
3.	Register for PLDS and activate license entitlements.	Go to the Avaya Product Licensing and Delivery System at https://plds.avaya.com/.	
4.	Prepare the site.	See “Supported hardware” and “Site preparation checklist”	

Supported tools for deploying the KVM OVA

- Virt Manager GUI
- virsh command line interface
- OpenStack
- Nutanix
- Red Hat Enterprise Virtualization administrative tool

Configuration tools and utilities

To deploy the System Manager KVM OVA and to configure the application, you need the following tools and utilities:

- System Manager KVM OVA, see “Release version of System Manager OVAs.”
- A browser for accessing the System Manager Web Console.
- PuTTY, PuTTYgen, and WinSCP.

Release details of System Manager KVM OVA

You can download the following software from the Avaya PLDS website at http://plds.avaya.com/.

Product name	Release version and Service pack	KVM OVA
System Manager	7.1.1	• **Profile 2:** `SMGR-7.1.0.0.1125193-kvm-52.ova` • **Profile 3:** `SMGR-PROFILE3-7.1.0.0.1125193-kvm-52.ova` • **Patch:** `System_Manager_7.1.1.0_r711006931.bin` • **Data Migration Utility:** `datamigration-146.bin`

Supported footprints of System Manager on KVM

Product name	Footprint	Release	CPUs (GHz)	Number of vCPUs	RAM (GB)	HDD (GB)	NICs	Number of users
System Manager	Profile 2	7.1.1	2.29	6	12	105	1	250000
System Manager	Profile 3	7.1.1	2.29	8	18	250	1	250000

Supported hardware

To deploy the Avaya Aura® application KVM OVA on a customer-provided server, the server must be on the Red Hat supported server list for Red Hat Enterprise Linux 7.2.

Site preparation checklist

Use the following checklist to know the set up required to deploy the KVM OVA.

No.	Task	Description	Notes	✔
1	Install the KVM hypervisor.			
2	Install the MobaXterm and Xming softwares on your laptop.	To remotely access the KVM hypervisor, the Virt Manager GUI, and virsh command line interface.		

Unsupported features for System Manager KVM OVA

The System Manager KVM OVA does not support the following features:

- Solution Deployment Manager deployments
- Standalone Avaya WebLM

Chapter 4: Deploying System Manager on Kernel-based Virtual Machine

Extracting KVM OVA

Procedure

1. Create a folder on the KVM host and copy the application KVM OVA in the created folder.
2. Type the command **`tar -xvf`** *<application_KVM.ova>*.

   The system extracts the files from the application KVM OVA.

Deploying System Manager KVM OVA by using Virt Manager

Before you begin

- Access the KVM host remotely.
- Create a folder on the KVM host and copy the System Manager KVM OVA in the created folder.
- Extract the System Manager KVM OVA files.

Procedure

1. On the terminal, run the command: `virt-manager`.
2. On the Virtual Machine Manager window, click **File** > **New Virtual Machine**, and select **Import existing disk image**.
3. On the Create a new virtual machine Step 1 of 4 window, select **Import existing disk image**.
4. Click **Forward**.
5. On the Create a new virtual machine Step 2 of 4 window, perform the following:
   a. In **Provide the existing storage path**, click **Browse**, and select the qcow2 image of System Manager on the KVM host.
   b. In **OS type**, select **Linux**.

c. In **Version**, select **Red Hat Linux Enterprise 7.2**.

d. Click **Forward**.

6. On the Create a new virtual machine Step 3 of 4 window, perform the following:

a. In **Memory (RAM)**, enter the required memory.

b. In **CPU**, enter the number of CPUs for the virtual machine based on the application profile.

c. Click **Forward**.

7. On the Create a new virtual machine Step 4 of 4 window, perform the following:

a. In **Name**, type the name of the virtual machine.

b. Select the **Customize Configuration before Install** check box.

c. Check **Network selection** and verify the required network interface .

d. Click **Finish**.

8. In the left navigation pane, click **Disk 1**. In the **Advanced options** section, perform the following:

a. In **Disk bus**, select **IDE**.

b. In **Storage format**, type `qcow2`.

c. Click **Apply**.

9. In the left navigation pane, click **Boot Options** and perform the following:

a. In **Boot device order**, click **Hard Disk**.

b. Click **Apply**.

10. Click **Begin Installation**.

The system creates a new System Manager virtual machine.

Next steps

On first boot of the virtual machine, provide the System Manager configuration and networking parameters.

Deploying System Manager KVM from CLI by using virsh

Before you begin

- Access the KVM host remotely.
- Create a folder on the KVM host and copy the System Manager KVM OVA in the created folder.
- Extract the System Manager KVM OVA files.

Procedure

1. On the terminal, run the command: `virsh`.
2. On the KVM host CLI, perform the following:
   a. Navigate to the System Manager KVM OVA directory.
   b. Run the System Manager installation utility, type the command: `sh SMGR-installer.sh <System Manager KVM OVA>`.
   c. When the system prompts, select the required System Manager profile.
   d. In **VM name**, type a name of the virtual machine.
   e. In **Drive storage location**, type storage location of the virtual machine.
   f. In **Out of Band Management network**, select the network.
   g. In **Public network**, select the public network.

      The system displays the command to deploy the image.
   h. To continue, type `Y`.

      The system displays the message: `Deploying image`.

Next steps

On first boot of the virtual machine, provide the System Manager configuration and networking parameters.

Deploying System Manager KVM OVA by using OpenStack

Connecting to OpenStack Dashboard

Before you begin

- Create an OpenStack account.
- Acquire adequate permission to upload and deploy the KVM ova.

Procedure

1. In your web browser, type the OpenStack URL.

   For example, http://<openstack.xyz.com>/horizon.
2. In **Domain**, type the domain name.
3. In **User Name**, type the user name.
4. Click **Connect**.

   The system displays the Instance Overview - OpenStack Dashboard page.

Uploading the qcow2 image

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Images**.
3. On the Images page, click **Create Image**.

   The system displays the Create An Image dialog box.
4. In **Name**, type the name of the image.
5. In **Description**, type the description of the image.
6. In **Image Source**, click **Image Location** or **Image File**, and perform one of the following:
   - In **Image Location**, type the exact URL of the qcow2 image.
   - In **Image File**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
7. In **Format**, click **QCOW2 - QEMU Emulator**.
8. Click **Create Image**.

   The system displays the created image on the Images page.

Flavors

Flavors are footprints of an application. The administrator must create flavors for each application.

For information about the footprints, see the profiles and footprints information for the application.

Creating a security group

About this task

Security groups are sets of IP filter rules. Each user must create security groups to specify the network settings for the application.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Access & Security**.
3. On the Access & Security page, click **Create Security Group**.

   The system displays the Create Security Group dialog box.
4. In **Name**, type the name of the security group.

5. In **Description**, type the description of the security group.
6. Click **Create Security Group**.

   The system displays the created security group on the Access & Security page.

Next steps

Add rules to security group.

Related links

Adding rules to a security group on page 16

Adding rules to a security group

Before you begin

Create a security group.

For information about the application-specific ports and protocols, see the port matrix document at http://support.avaya.com/security.

Procedure

1. On the Access & Security page, click **Manage Rules** that is corresponding to the created security group.
2. On the Access & Security / Manage Security Group Rules page, click **Add Rule**.

   The system displays the Add Rule dialog box.
3. In **Rule**, click a rule

   The system displays the fields that are associated with the selected rule.
4. Enter the appropriate values in the fields.
5. Click **Add**.

   The system displays the created rule on the Access & Security / Manage Security Group Rules page.

Related links

Creating a security group on page 15

Deploying application by using OpenStack

Before you begin

- Create flavors.
- Create a security group.

Procedure

1. Connect to OpenStack Dashboard.
2. In the left navigation pane, click **Project** > **Compute** > **Instances**.

3. On the Instance page, click **Launch Instance**.

   The system displays the Launch Instance dialog box.

4. In **Details**, perform the following:
   a. In **Instance Name**, type a name of the instance.
   b. In **Availability zone**, select the availability zone of the instance.
   c. Click **Next**.
5. In **Source**, perform the following:
   a. In the **Available** section, select a check box corresponding to an instance image.

      The system displays the selected image in the **Allocated** section.

   b. Click **Next**.
6. In **Flavors**, perform the following:
   a. In the **Available** section, select a check box corresponding to a flavor name.

      The system displays the selected flavor in the **Allocated** section.

   b. Click **Next**.
7. In **Networks**, perform the following:
   a. In the **Available** section, select a check box corresponding to a network name.

      The system displays the selected network in the **Allocated** section.

   b. Click **Next**.
8. In **Network Ports**, leave the default settings, and click **Next**.
9. In **Security Groups**, perform the following:
   a. In the **Available** section, select a check box corresponding to a security group name.

      The system displays the selected security group in the **Allocated** section.

   b. Click **Next**.
10. In **Key Pair**, leave the default settings, and click **Next**.
11. In **Configuration**, leave the default settings, and click **Next**.
12. In **Metadata**, leave the default settings.
13. Click **Launch Instance**.

    The system displays the created instance on the Instances page. The **Status** column displays: `Spawning`. When the system creates the application instance, the **Status** column displays: `Active`.

    The system displays the static IP Address of the application in the **IP Address** column.

Next steps

Configure the application instance. Use the static IP Address to configure the application instance.

Configuring application instance

Procedure

1. On the Instances page, in the **INSTANCE NAME** column, click the application instance name.
2. On the Instances / <Instance Name> page, click **Console**.
3. On the Instance Console page, go to console, and follow the prompt to configure the application instance.

Deploying System Manager KVM OVA by using Nutanix

Logging on to the Nutanix Web console

Procedure

1. To log on to the Nutanix Web console, in your web browser, type the PRISM URL.

   For example, http://<PRISM_IPAddress>/.
2. In **username**, type the user name.
3. In **password**, type the password.
4. Press **Enter**.

   The system displays the Home page.

Transferring the files by using the WinSCP utility

About this task

Use the following procedure to transfer the files from a remote system to a Nutanix container by using the WinSCP utility.

Procedure

1. Use WinSCP or a similar file transfer utility to connect to the Nutanix container.
2. In **File protocol**, click **SCP**.
3. Enter the credentials to gain access to SCP.
4. Click **Login**.
5. Click **OK** or **Continue** as necessary in the warning dialog boxes.

6. In the WinSCP destination machine pane, browse to `/home/<Container_Name>` as the destination location for the file transfer.
7. Click and drag the `qcow2` image from the WinSCP source window to `/home/<Container_Name>` in the WinSCP destination window.
8. Click the WinSCP **Copy** button to transfer the file.
9. When the copy completes, close the WinSCP window (**x** icon) and click **OK**.

Uploading the qcow2 image

Procedure

1. Log on to the Nutanix Web console.
2. Click **Settings icon ( )** > **Image Configuration**.

   The system displays the Image Configuration dialog box.
3. Click **+ Upload Image**.

   The system displays the Create Image dialog box.
4. In **NAME**, type the name of the image.
5. In **ANNOTATION**, type the description of the image.
6. In **IMAGE TYPE**, click **DISK**.
7. In **STORAGE CONTAINER**, click the storage container of the image.
8. In **IMAGE SOURCE**, perform one of the following:
   - Select **From URL**, type the exact URL of the qcow2 image. For example: `nfs://<127.0.0.1>/<Storage Container Name>/<Image Name>`
   - Select **Upload a file**, click **Browse**. In the Choose File to Upload dialog box, select the qcow2 image from your local system, and click **Open**.
9. Click **Save**.

   The system displays the created image on Image Configuration.

Creating the virtual machine by using Nutanix

Before you begin

- Upload the `qcow2` image.
- Configure the network.

Procedure

1. Log on to the Nutanix Web console.

2. Click **Home** > **VM**.
3. Click **+ Create VM**.

   The system displays the Create VM dialog box.
4. In the General Configuration section, perform the following:
   a. In **NAME**, type the name of the virtual machine.
   b. In **DESCRIPTION**, type the description of the virtual machine.
5. In the Compute Details section, perform the following:
   a. In **VCPU(S)**, type the number of virtual CPUs required for the virtual machine.
   b. In **NUMBER OF CORES PER VCPU**, type the number of core virtual CPUs required for the virtual machine.
   c. In **Memory**, type the memory required for the virtual machine.

      The value must be in GiB.

   You must select the CPU and Memory according to the application footprint profile.
6. In the Disk section, perform the following:
   a. Click **+ Add New Disk**.

      The system displays the Add Disk dialog box.
   b. In **TYPE**, click **DISK**.
   c. In **OPERATION**, click **Clone from Image Service**.
   d. In **IMAGE**, click the application image.
   e. In **BUS TYPE**, click **IDE**.
   f. Click **Add**.

      The system displays the added disk in the **Disk** section.
7. In the Disk section, select a boot device.
8. In the Network Adopters (NIC) section, perform the following:
   a. Click **Add New NIC**.

      The system displays the Create NIC dialog box.
   b. In **VLAN NAME**, click the appropriate NIC.

      The system displays **VLAN ID**, **VLAN UUID**, and **NETWORK ADDRESS / PREFIX** for the selected NIC.
   c. Click **Add**.

      The system displays the added NIC in the Network Adopters (NIC) section.

   You must select the number of NIC according to the application footprint profile.

   If you are configuring Out of Band Management, select one more NIC.

9. In the VM Host Affinity section, perform the following:
   a. Click **Set Affinity**.

      The system displays the Set VM Host Affinity dialog box.
   b. Select one or more host to deploy the virtual machine.
   c. Click **Save**.

      The system displays the added hosts in the VM Host Affinity section.
10. Click **Save**.

    The system displays the message: `Received operation to create VM <name of the VM>`.

    After the operation is successful, the system displays the created virtual machine on the VM page.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.
4. At the bottom of the table, click **Power On**.

   The system starts the virtual machine.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

Configuring the virtual machine

Procedure

1. Click **Home** > **VM**.
2. On the VM page, click **Table**.
3. Select the virtual machine.

4. At the bottom of the table, click **Launch Console**.
5. Follow the prompt to configure the virtual machine.

Deploying application by using Red Hat Virtualization Manager

Logging on to the Red Hat Virtualization Manager Web console

Procedure

1. In your web browser, type the Red Hat Virtualization Manager URL.

   For example, https://<RedHatVirtualizationManager_IPAddress>/ovirt-engine/.
2. To log in, click **Not Logged In** > **Login**.

   The system displays the Red Hat Virtualization Manager Log In page.
3. In **Username**, type the user name.
4. In **Password**, type the password.
5. In **Profile**, click the appropriate profile.
6. Click **Log In**.

   The system displays the Red Hat Virtualization Manager Web Administration page.

Uploading the disk

Before you begin

You must import the `ovirt-engine` certificate into your browser by accessing the `http://<engine_url>/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA` link to get the certificate. Establish the trust for the new Certificate Authority (CA) with the website.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Disks** tab, click **Upload** > **Start**.

   The system displays the Upload Image dialog box.
4. Click **Browse**.

5. In the Choose File to Upload dialog box, select the qcow2 disk image from your local system, and click **Open**.
6. In **Size(GB)**, type the size of the disk.
7. In **Alias**, type the name of the disk.
8. In **Description**, type the description of the disk.
9. In **Data Center**, click the data center to store the disk.
10. In **Storage Domain**, click the storage domain of the disk.
11. In **Disk Profile**, click disk profile.
12. In **Use Host**, click the host of the disk.
13. Click **OK**.

    The system displays the uploaded image on the **Disks** tab. Once the disk image is successfully uploaded, the **Status** column displays `OK`.

Creating the virtual machine by using Red Hat Virtualization Manager

Before you begin

- Upload the `qcow2` disk image.
- Create an instance type.
- Configure the network.

Procedure

1. Log on to the Red Hat Virtualization Manager Web console.
2. In the left navigation pane, click **System**.
3. On the **Virtual Machines** tab, click **New VM**.

   The system displays the New Virtual Machine dialog box.
4. In **Operating System**, click **Linux**.
5. In **Instance Type**, click an instance type.

   You must select the instance type according to the application footprint profile.
6. In **Optimized for**, click **Server**.
7. In **Name**, type the name of the virtual machine.
8. In **Description**, type the description of the virtual machine.
9. In the Instance Images section, perform the following:
   a. Click **Attach**.

      The system displays the Attach Virtual Disks dialog box.

b. In **Interface**, click **IDE**.

c. Click **OK**.

The system displays the added disk in the Instance Images section.

10. In **nic1**, click a vNIC profile.

    If you are configuring Out of Band Management, select one more NIC.

11. Click **OK**.

    After the operation is successful, the system displays the created virtual machine on the **Virtual Machines** tab.

Next steps

Start the virtual machine.

Starting a virtual machine

Before you begin

Create the virtual machine.

Procedure

Right-click the virtual machine and click **Run**.

When the system starts the virtual machine, the system displays a green upward arrow key (▲) corresponding to the virtual machine name.

Next steps

Launch the console. On the first boot of the virtual machine, provide the configuration and networking parameters

Configuring the virtual machine

Before you begin

- Start the virtual machine.
- Install the `virt-viewer` installer to access console.

Procedure

1. Right-click the virtual machine and click **Console**.
2. Follow the prompt to configure the virtual machine.

Configuring the network parameters from console

About this task

When first started, the System Manager virtual machine collects the network parameters. When the system prompts, enter the network parameters.

Before you begin

Deploy the System Manager KVM OVA.

Procedure

1. To provide configuration input, type `y`.
2. Read the End User License Agreement (EULA).
3. To accept the EULA, in **Do you accept the Avaya Software License Terms? (Y)es/(N)o**, type `Y`.
4. At the prompt, enter the management network parameters, public network parameters, virtual FQDN parameters, SMGR CLI User parameters, and SNMPv3 parameters of the System Manager virtual machine.
5. To schedule the remote backup during the System Manager installation, in **Schedule SMGR Backup**, type the backup definition parameters for the System Manager virtual machine.
6. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

   Enable: (Recommended)

   ```
   By enabling Avaya Logins you are granting Avaya access to your
   system.
   This is necessary to maximize the performance and value of your
   Avaya support entitlements, allowing Avaya to resolve product
   issues in a timely manner.
   In addition to enabling the Avaya Logins, this product should be
   registered with Avaya and technically onboarded for remote
   connectivity and alarming. Please see the Avaya support site
   (support.avaya.com/registration) for additional information for
   registering products and establishing remote access and alarming.
   ```

   Disable:

   ```
   By disabling Avaya Logins you are preventing Avaya access to your
   system.
   This is not recommended, as it impacts Avaya’s ability to provide
   support for the product. Unless the customer is well versed in
   managing the product themselves, Avaya Logins should not be
   disabled.
   ```

   a. 1: To enable EASG.

      Avaya recommends to enable EASG.

You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

b. 2: To disable EASG.

7. To confirm the network parameters, type `Y`.

   The system starts the configuration of the network parameters.

   From the time you power on the system, the deployment process takes about 30–40 minutes to complete. Do not reboot the system until the configuration is complete. You can monitor the post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file. Once the configuration is complete, the log file displays the message: `exit status of eject command is 0`.

Next steps

Once the first boot configuration is complete, it is mandatory to deploy the latest patch.

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- On the web browser, type `https://<Fully Qualified Domain Name>SMGR`, and ensure that the system displays the System Manager Log on page.

  The system displays the message: Installation of latest System Manager patch is mandatory.

- On the Command Line Interface, log on to the System Manager console, and verify that the system does not display the message: `Maintenance: SMGR Post installation configuration is In-Progress`.

  It should only display the message: `Installation of latest System Manager patch is mandatory`.

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Related links

Network and configuration field descriptions on page 26

Network and configuration field descriptions

Name	Description
Management IPv4 Address (or Out of Band Management IPv4 Address)	The IPv4 address of the System Manager virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.
Management Netmask	The Out of Band Management subnetwork mask to assign to the System Manager virtual machine.

Table continues…

Name	Description
Management Gateway	The gateway IPv4 address to assign to the System Manager virtual machine.
IP Address of DNS Server	The DNS IP addresses to assign to the primary, secondary, and other System Manager virtual machines. Separate the IP addresses with commas (,).
Management FQDN	The FQDN to assign to the System Manager virtual machine. **Note:** System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
IPv6 Address	The IPv6 address of the System Manager virtual machine for out of band management. The field is optional.
IPv6 Network prefix	The IPv6 subnetwork mask to assign to the System Manager virtual machine. The field is optional.
IPv6 Gateway	The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.
Default Search List	The search list of domain names. The field is optional.
NTP Server IP/FQDN	The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).
Time Zone	The timezone where the System Manager virtual machine is located. A list is available where you select the name of the continent and the name of the country.

Note:

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

Name	Description
Public IP Address	The IPv4 address to enable public access to different interfaces. The field is optional.
Public Netmask	The IPv4 subnetwork mask to assign to System Manager virtual machine. The field is optional.
Public Gateway	The gateway IPv4 address to assign to the System Manager virtual machine. The field is optional.
Public FQDN	The FQDN to assign to the System Manager virtual machine. The field is optional.
Public IPv6 Address	The IPv6 address to enable public access to different interfaces. The field is optional.
Public IPv6 Network Prefix	The IPv6 subnetwork mask to assign to System Manager virtual machine. The field is optional.
Public IPv6 Gateway	The gateway IPv6 address to assign to the System Manager virtual machine. The field is optional.

Name	Description
Virtual Hostname	The virtual hostname of the System Manager virtual machine. **Note:** • The VFQDN value must be unique and different from the FQDN value of System Manager and the elements. • VFQDN is a mandatory field. • Do not add VFQDN entries in the DNS configuration. • Do not add VFQDN in the `/etc/hosts` file on System Manager. Adding VFQDN in the `/etc/hosts` file might cause failures. • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN. • After System Manager installation, if you require to change the System Manager VFQDN value, perform the following: 1. Log in to the System Manager virtual machine with administrator privilege credentials. 2. Run the following command, `changeVFQDN`.
Virtual Domain	The virtual domain name of the System Manager virtual machine.

Name	Description
SNMPv3 User Name Prefix	The prefix for SNMPv3 user.
SNMPv3 User Authentication Protocol Password	The password for SNMPv3 user authentication.
Confirm Password	The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password	The password for SNMPv3 user privacy.
Confirm Password	The password that you must provide to confirm the SNMPv3 user privacy protocol.

Name	Description
SMGR command line user name	The user name of the System Manager CLI user. **Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password	The password for the System Manager CLI user.
Confirm Password	The password that you retype to confirm the System Manager CLI user authentication.

Name	Description
Schedule Backup?	• **Yes**: To schedule the backup jobs during the System Manager installation. • **No**: To schedule the backup jobs later. **Note:** If you select **No**, the system does not display the remaining fields.
Backup Server IP	The IP address of the remote backup server. **Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id	The login ID of the backup server to log in through the command line interface.
Backup Server Login Password	The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password	The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location	The location on the remote backup server.
File Transfer Protocol	The protocol that you can use to create the backup. The values are SCP and SFTP.
Repeat Type	The type of the backup. The possible values are: • `Hourly` • `Daily` • `Weekly` • `Monthly`
Backup Frequency	The frequency of the backup taken for the selected backup type. The system generates an alarm if you do not schedule a System Manager backup every seven days.
Backup Start Year	The year in which the backup must start. The value must be greater than or equal to the current year.
Backup Start Month	The month in which the backup must start. The value must be greater than or equal to the current month.
Backup Start Day	The day on which the backup must start. The value must be greater than or equal to the current day.
Backup Start Hour	The hour in which the backup must start. The value must be six hours later than the current hour.
Backup Start Minutes	The minute when the backup must start. The value must be a valid minute.
Backup Start Seconds	The second when the backup must start. The value must be a valid second.

Name	Description
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG	Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks. The options are: • 1: To enable EASG. • 2: To disable EASG. Avaya recommends to enable EASG. You can also enable EASG after deploying or upgrading the application by using the command: **`EASGManage --enableEASG`**.

Name	Description
Public	The port number that is mapped to public port group. You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.
Out of Band Management	The port number that you must assign to the Out of Band Management port group. The field is mandatory.

Related links

Configuring the network parameters from console on page 25

Installing the System Manager patch from CLI

About this task

From System Manager Release 7.1 and later, you must deploy the patch after the installation is complete.

Before you begin

Download the latest System Manager patch file and save the patch file to the `/swlibrary` location of System Manager.

Procedure

1. Log in to the System Manager command line interface.
2. Run the command: **`SMGRPatchdeploy`** `/swlibrary/<System_Manager_R7.1.1.0_xxxxxxxxx.bin>`.

Next steps

Note:

Modifying the network or management configuration is not recommended before the patch deployment.

Log on to the System Manager web console. At your first log in, change the System Manager web console credentials.

Chapter 5: Upgrading to System Manager Release 7.1.1

Migration path

You can migrate to System Manager Release 7.1.1 on KVM:

- From System Manager Release 7.0.x on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment
- From System Manager Release 6.2.x and 6.3.x on VMware in customer-provided Virtualized Environment
- From System Manager Release 6.x on System Platform

Migrating to System Manager Release 7.1.1 from CLI

About this task

Use the procedure to migrate System Manager from Release 6.x or 7.0.x to System Manager Release 7.1.1 on KVM.

Before you begin

- Ensure that System Manager is running.
- Download the required software files.

Procedure

1. Log on to the old System Manager web console.
2. Record the software version of old System Manager from the **About** link.

   For information, see “Verifying the current software version”.
3. Record the network parameters and system parameters, such as virtual FQDN (vFQDN), IP Address, and Nemask of the old system.
4. Create a backup of System Manager and copy to the remote server by using System Manager web console.

Note:

For upgrades by using data migration utility, use only the backup that you created from the System Manager web console.

5. Log in to the System Manager command line interface of the old system.
6. Shut down the old System Manager.
7. Deploy the System Manager Release 7.1.1 KVM.

   For information, see “Deploying System Manager on Kernel-based Virtual Machine”.

   Important:

   You can use the same network parameters and system parameters that you recorded on the old system or you can use the different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the old system.
8. Log in to the System Manager command line interface of the new system.
9. Copy `datamigration-146.bin`, the Release 7.1.1 bin file, and System Manager backup file to the `/swlibrary` location on System Manager.
10. On System Manager Release 7.1.1, at the prompt, perform the following:
    a. Create a snapshot of the System Manager system.
    b. To run the data migration utility, type the following command:

       ```
       upgradeSMGR /swlibrary/<DMUtility_bin file name>.bin -m -v
       ```

       You must provide the absolute path of the data migration utility.
    c. In **Enter the location of backup file (full path)**, type the absolute path of the backup file.

       ```
       /swlibrary/<backupfile name.*>
       ```

       The system validates the backup file and displays the parameters.
    d. In **Enter the patch file**, type the following command:

       ```
       /swlibrary/<patch file name>.bin
       ```

       For example, `swlibrary/System_Manager_R7.1.0.0.xxxxxxxxx.bin`.

       The system validates the patch file and displays the following message:

       ```
       You are about to run the System Manager Data Migration utility.
       The System Manager will be inaccessible for approximately 60
       minutes, depending on the resources available on the system.
       ```
    e. To continue, type `Y`.

       The system displays the following message:

       ```
       WARNING:- The system is now going down for a halt and will be
       inaccessible for some time.
       Remote broadcast message (Tue Apr 5 21:06:27 2017):
       ```

```
INFO:- System Manager Data Migration would now be executed in
background process. For details, see System Manager Data
Migration logs in the /var/log/Avaya/datamigration/
data_migration.log.
```

11. Log on to System Manager and verify that the upgrade is successful.

    The upgrade takes about 80 to 90 minutes. However, the duration depends on the factors such as the number of users, backup size, hardware used, and the number of resources shared during the upgrade.

    As part of running the data migration utility, the system performs the patch installation in the background that takes about 60–90 minutes.

    You can verify the execution of System Manager:

    - Data Migration Utility from the `/var/log/Avaya/datamigration/data_migration.log` file.
    - Patch from the `/var/log/Avaya/SMGR_Patch.log` file.

12. Verify the software version of the new System Manager.

Next steps

- If the upgrade or patch installation is successful, log off from the system, and remove the snapshot.

  Note:

  Snapshots occupy the system memory and degrades the performance of the virtual application. Therefore, delete the snapshot after you verify the patch installation or the system upgrade.

- If the upgrade or patch installation fails, use the snapshot to restore the system to the original state.

  To collect logs, run the **`collectLogs`** command. The system creates a `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file at `/tmp` directory. Copy the `LogsBackup_xx_xx_xx_xxxxxx.tar.gz` file to remote server and share the file with Avaya Support Team.

Verifying the current software version

Procedure

1. Log on to the System Manager web console.
2. To view the build number, do one of the following:
   - For System Manager Release 6.x, in the upper-right corner of the web console, click the **About** link.
   - For System Manager Release 6.3.19 and later, in the upper-right corner of the web console, click the settings icon (), and then click **About**.

The system displays the About System Manager window with the build details.

3. Verify the version number of System Manager with the highest build number for the release.

Creating a data backup on a remote server

Before you begin

Ensure that the backup server supports the required algorithms for the System Manager remote backup. For more information, see Supported ciphers, key exchange algorithms, and mac algorithms.

System Manager requires password authentication to enable the remote backup servers for successful backup.

Note:

System Manager does not support authentication mechanisms, such as Keyboard-Interactive and public key-based support.

Procedure

1. Perform one of the following:
   - For System Manager 6.1 and later, on System Manager Web Console, click **Services** > **Backup and Restore**.
   - For System Manager 6.0, on System Manager Web Console, click **System Manager Data** > **Backup and Restore**.
   - For System Manager 7.x, on System Manager Web Console, click **Services** > **Backup and Restore**.
2. On the Backup and Restore page, click **Backup**.
3. On the Backup page, click **Remote**.
4. Perform one of the following:
   - Perform the following:
     a. In the **File transfer protocol** field, click `SCP` or `SFTP`.

        Note:

        On System Manager Release 6.3.1 and earlier systems, this option is not available

     b. Enter the remote server IP, remote server port, user name, password, and name and the path of the backup file that you create.
   - Select the **Use Default** check box.

Important:

To use the **Use Default** option, provide the remote server IP, user name, password, and name and path of the backup file, and remote server port on the SMGR Element Manager page. For **Use Default**, on the SMGR Element Manager page, you can click **Services** > **Configurations** and navigate to **Settings** > **SMGR** > **SMGR Element Manager**.

5. Click **Now**.

   If the backup is successful, the Backup and Restore page displays the message: `Backup job submitted successfully. Please check the status detail below!!`

License management

Following are the use cases for managing licenses when a KVM supported application is migrated from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM.

- If the WebLM service is moved from Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, all applications that host licenses on that WebLM must regenerate the licenses as the WebLM service is also moved. In Release 7.1.1, KVM supports the WebLM that is integrated with System Manager.
- If the WebLM service is not moved from existing Appliance Virtualization Platform on Avaya-provided server or from VMware in customer-provided Virtualized Environment to KVM, but only the KVM supported applications move to KVM, then you do not have to regenerate the license for those applications that move to KVM.
- If a customer is using standalone WebLM on Appliance Virtualization Platform on Avaya-provided server or on VMware in customer-provided Virtualized Environment and the customer wants to move the Licensing Services to KVM, then all the licenses need to migrate to the centralized System Manager Release 7.1.1 with integrated WebLM in KVM and the supported KVM applications that move need to regenerate the license files.

Chapter 6: Post-installation tasks

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 7.1.1 and configure System Manager.

Procedure

1. On the web browser, type `https:// <fully qualified domain name of System Manager>`, and ensure that the system displays the System Manager web console.
2. On the upper-right corner, click  and click **About**.

   The system displays the About SMGR window with the build details.
3. Verify the System Manager version number.

Enhanced Access Security Gateway (EASG) overview

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.

Managing EASG from CLI

About this task

After deploying or upgrading an Avaya Aura® application, you can enable, disable, or view the status of EASG.

Before you begin

Log in to the application CLI interface.

Procedure

1. To view the status of EASG, run the command: **`EASGStatus`**.

   The system displays the status of EASG.

2. To enable EASG, do the following:

   a. Run the command: **`EASGManage --enableEASG`**.

      The system displays the following message.

      ```
      By enabling Avaya Services Logins you are granting Avaya access
      to your system. This is required to maximize the performance and
      value of your Avaya support entitlements, allowing Avaya to
      resolve product issues in a timely manner.

      The product must be registered using the Avaya Global
      Registration Tool (GRT, see https://grt.avaya.com) to be
      eligible for Avaya remote connectivity. Please see the Avaya
      support site (https://support.avaya.com/ registration) for
      additional information for registering products and establishing
      remote access and alarming.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is enabled`.

3. To disable EASG, do the following:

   a. Run the command: **`EASGManage --disableEASG`**.

      The system displays the following message.

      ```
      By disabling Avaya Services Logins you are denying Avaya access
      to your system. This is not recommended, as it can impact
      Avaya's ability to provide support for the product. Unless the
      customer is well versed in managing the product themselves,
      Avaya Services Logins should not be disabled.
      ```

   b. When the system prompts, type `yes`.

      The system displays the message: `EASG Access is disabled`.

Viewing the EASG certificate information

Procedure

Log in to the application CLI interface.

EASG site certificate

EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates

Before you begin

1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to /home/*cust* directory, where *cust* is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of *installed_pkcs7_name* in the commands.
4. You must have the following before loading the site certificate:
   - Login ID and password
   - Secure file transfer tool, such as WinSCP
   - Site Authentication Factor

Procedure

1. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.
2. To view information about a particular certificate: run the following command:
   - `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   - `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.
3. To delete the site certificate, run the following command:
   - `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   - `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.

Chapter 7: Resources

Documentation

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips
- Information about service packs
- Access to customer and technical documentation
- Information about training and certification programs
- Links to other pertinent information

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Index

T

U

V