VMware Adapter for SAP Landscape Management Installation Configuration and Administration Guide for VI Administrators

Product version 1.5.1 running on vSphere 6.0

vmware®

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Introduction to VMware Adapter for SAP Landscape Management 1

This chapter introduces you to the VMware Adapter for SAP Landscape Management. The SAP *Landscape Management* product is also called *LaMa*.

This chapter includes the following topics:

About This Guide

VMware Adapter for SAP Landscape Management is a virtual appliance that integrates SAP Landscape Management with VMware management software (VMware vCenter Server and VMware vRealize Automation). This integration of SAP Landscapes with VMware's market-leading SDDC solutions lead to delivering unique automation capabilities, high scalability, improved performance and advanced storage and network management. All this helps to radically simplify the provisioning and management of SAP landscapes.

This procedural guide describes how to install and configure the VMware Adapter for SAP Landscape Management and its dependent software.

Target Audience

This installation guide is primarily written for VMware virtual infrastructure (VI) administrators. Some aspects of the installation may require *LaMa* administrative experience. For VI administrators without *LaMa* experience, consider obtaining their help for completing tasks requiring those skills.

Prerequisites

This installation guide covers installation and configuration of the VMware Adapter for SAP Landscape Management and presumes that the user reading the guide has a functional understanding of LaMa. For documentation related to LaMa or training on LaMa, contact your SAP representative.

Understanding the Organization of this Guide

This installation guide covers an overview, installation and configuration of VMware Adapter for SAP Landscape Management

The guide contains the following chapters:

1 Introduction to VMware Adapter for SAP Landscape Management (this chapter) — About This Guide, target audience, prerequisites, and organization.

2 Overview of VMware Adapter for SAP Landscape Management: Purpose, Benefits, Architecture and Components

3 Performing a Fresh Install / Upgrade of VLA and Configuration

4 Backup and Restore of Configuration

5 Troubleshooting

6 Supplement

Overview of VMware Adapter for SAP Landscape Management: Purpose, Benefits, Architecture and Components

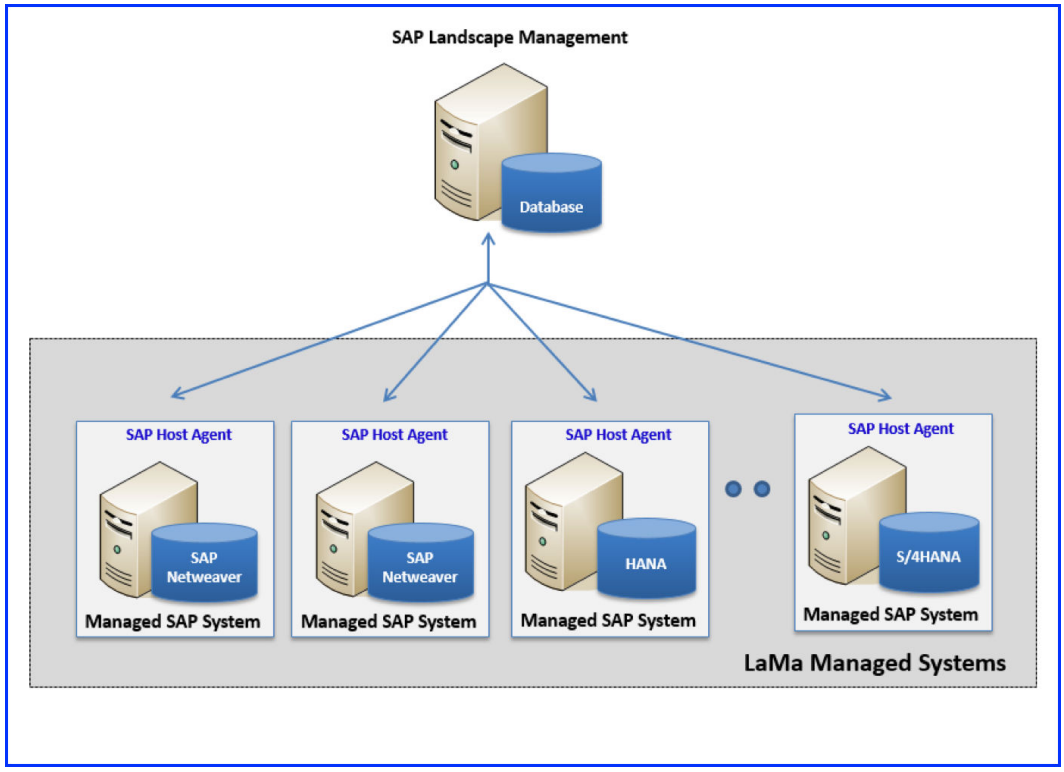
2

This chapter includes the following topics:

Product Overview

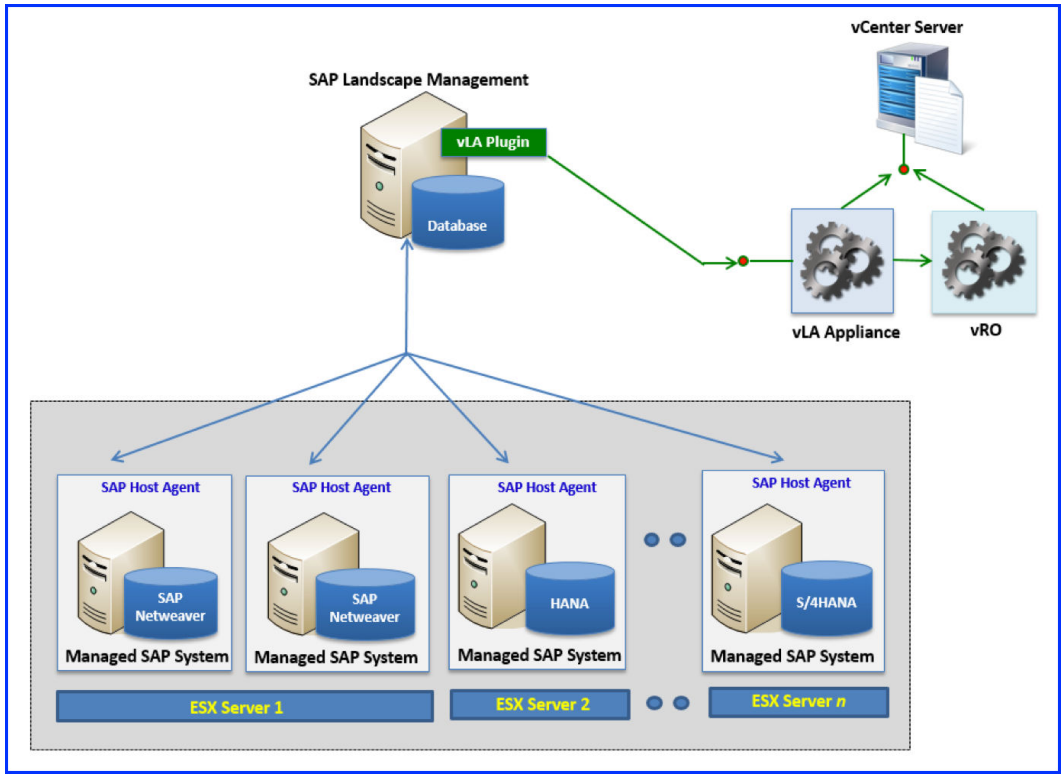
SAP Landscape Management is a solution to centrally manage and provision SAP landscapes running in physical, virtual and cloud infrastructures. It provides a central dashboard for monitoring the hosts (physical servers or virtual machines) and SAP application services in even very complex infrastructures. Additionally, administrators can use the SAP Landscape Management console for performing centralized operations like starting or stopping instances of a SAP service or apply operations simultaneously to complex groups of systems on the entire landscape through predefined single and mass operations. Another aspect of SAP Landscape Management is the ability to support Enterprise Edition SAP System Clone, System Copy or Refresh and System Rename operations. This highly automated and unified IT landscape management capabilities apply not only to SAP Netweaver based applications but also to SAP HANA and SAP S/4HANA systems. All the described features of SAP Landscape Management are based on a communication with the SAP Host Agent of the respective SAP system in the landscape as shown in the following figure:

Figure 2-1. SAP Landscape Management



With virtualized SAP infrastructures on VMware vSphere, the list of use cases can be extended and enhanced with even more features. By using the VMware Adapter for SAP Landscape Management, SAP Landscape Management can now monitor all the virtual machines used for the SAP infrastructure directly out of the VMware vCenter, start or stop VMs, deploy Vms from templates and perform offline or online SAP System Clone, System Copy or Refresh and System Rename operations on VMs. Additionally, live migrations of VMs, networks or datastores for workload balancing, creating a snapshot of a SAP system before a critical change takes place are possible. Thus, combining SAP Landscape Management with the advanced use cases of virtualized infrastructures give SAP customers the highest degree of convenience in terms of automation and control and also significantly saves operational costs. The following figure depicts the SAP Landscape Management along with the components of VMware Adapter for SAP Landscape Management installed:

Figure 2-2. SAP Landscape Management in virtualized environment



As depicted in the preceding figure, VMware Adapter for SAP Landscape Management is a virtual appliance that integrates SAP Landscape Management (LaMa) with VMware's Software Defined Data Center (SDDC) technologies, delivering unique automation capabilities that radically simplify how SAP basis admins and end users provision and manage SAP Landscapes. The results are faster time to market, and reduction in both TCO and operational errors while managing SAP Landscapes.

VMware Adapter for SAP Landscape Management appliance accepts application calls from SAP Landscape Management (LaMa), then uses vRealize Automation or VMware vRealize Orchestrator workflows to execute commands to VMware vCenter Server for VMware related operations, such as starting and stopping a virtual machine.

Features and Benefits

Note Key Features:

VMware Adapter for SAP Landscape Management dramatically simplifies and automates the life-cycle management of SAP landscapes on VMware virtualized infrastructure:

- Provisioning — System Cloning, Copying and System Refresh
  - Automate key SAP Basis provisioning tasks such as system cloning, copying, and system refresh directly in VMware vCenter Server with SAP Landscape Management
  - Leverage SA-API to provision SAP systems from templates in vRealize Automation
- Operations — SAP Hosts, Storage, and Network Migration
  - Migrate VM, switch its data set and network to stand up SAP hosts, move environments, and deploy disaster recovery solutions - all through the SAP Landscape Management interface

- Delivery — Self-Service Through vRealize Automation
  - Enable end users to self-provision SAP Landscapes in vRealize Automation through blueprints created by SA-API

Note Key Benefits:

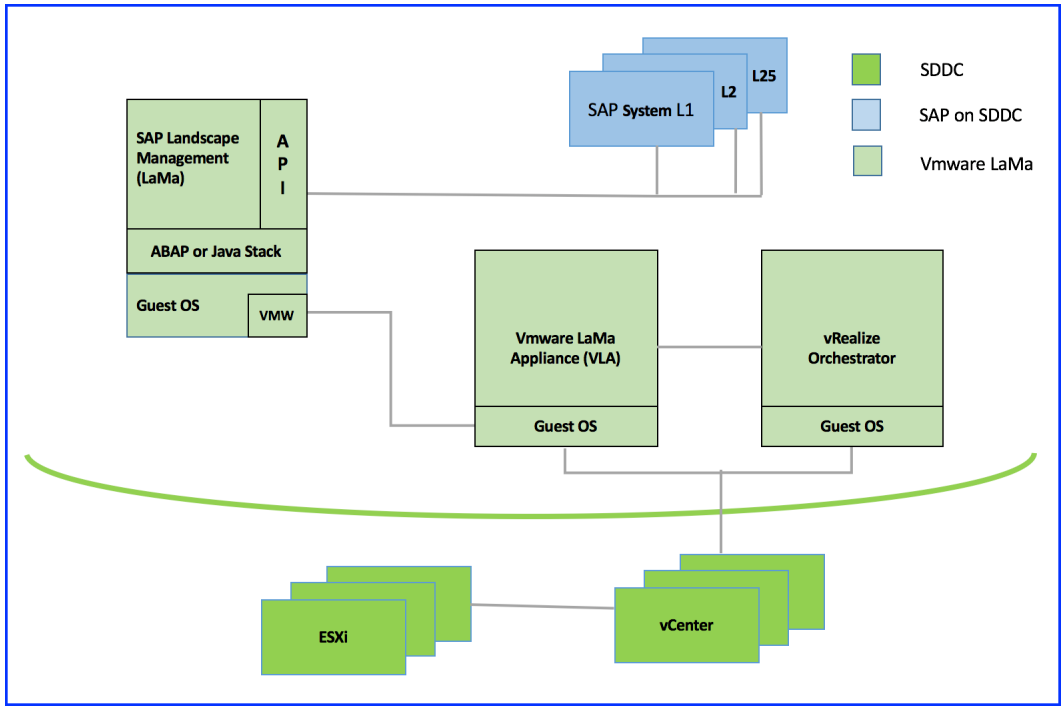
Following are the key benefits of deploying VMware Adapter for SAP Landscape Management:

- Greater operational continuity through centralized management, visibility and control of your entire SAP landscape using a single console
- Increased operational agility by accelerating application life-cycle management operations and faster response to workload fluctuations
- Reduced time, effort and cost to manage and operate your SAP systems through automation of SAP BASIS tasks and leveraging adapter's functions such as VMware vSphere Storage vMotion, network migration and linked online clone and copy
- Increases SAP BASIS and IT admin productivity by automating manual operational tasks and enabling self-service capability
- Lowers total cost of ownership since reduced OpEx leads to increased cost savings

Reference Architecture

The following diagram illustrates the components of a VLA execution environment and their relationship to one another:

Figure 2-3. VLA Execution Environment



The key components in this diagram are :

- SAP Systems (Managed SAP Systems) – Each of these systems consist of software running on one or more machines (bare metal, or in the case of VLA environments, virtual machines [VMs] hosted on VMware vSphere™ products [ESXi systems managed by vCenter Server™]) that perform some business function, such as order processing, accounts payable, general ledger, inventory management,

etc. Each SAP System consists of one or more components like a database service, SAP instance or SAP Host Agent service. When all of the components are up and running, the SAP System is running. When all of the components are stopped, the SAP system is stopped. If some systems are running and some are not, the SAP system is in an intermediate state.

- The *SAP Landscape Management (LaMa)* VM – The SAP Landscape Management (LaMa) application runs on ABAP or Java stack in a Linux based guest OS. It provides a web-based user interface for SAP BASIS administrators to create / destroy / configure / and otherwise operate on and provision SAP Systems and their underlying machinery (bare metal or virtualized).

  The *SAP Landscape Management (LaMa)* has an extensible architecture that allows SAP and third-party vendors, for example VMware, to create plugins to extend certain features.

- The VMware Adapter for SAP Landscape Management — This is a plugin to LaMa that extends how LaMa integrates with the underlying systems virtualized with VMware vSphere (see next bullet), optimizing and extending the functionality for certain operations, such as activating (powering on) and deactivating (powering off), copying and cloning systems, and automation of these copying and cloning operations.

- ESXi and vCenter Server (collectively called vSphere) – ESXi is VMware's premier hypervisor product. VI administrators typically install it on bare-metal server-class computers, with VMs running guest operating systems (OSes) with SAP Systems as applications within the guests. vCenter Server is VMware's premier product for managing environments virtualized with ESXi. Collectively called vSphere, these products provide an enterprise-class environment with features for creating clusters, load balancing VMs between host systems (ESXi instances), fault tolerance, virtual networking, virtual storage, and more. In VLA environments, the VLA appliance (next bullet) runs in a VM on this infrastructure.

  Note It is possible to run ESXi in a nested environment. In this case, VI administrators install ESXi in a VM running in a vSphere environment. For more information on vSphere Templates, see http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.hostclient.doc%2FGUID-F40130B0-0194-4A41-91FA-1A967721924B.html. For more information about vApps, see http://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.powercli.ug.doc%2FGUID-CFCCBEAC-74DD-4259-9D9D-1FCCCB185218.html

  ---

- VMware vRealize Orchestrator™ – This VMware product helps VI administrators automate their environments by creating work flows (essentially scripts) that perform VI administrative actions, including complex actions that may take multiple steps, involve loops, conditions, etc. VMware vRealize Orchestrator workflows can handle exceptions automatically or can pause waiting for a VI administrator to mitigate an issue. See the next bullet for how VLA uses VMware vRealize Orchestrator.

- VMware Landscape Management Appliance (VLA) – This part of the VLA product is a virtual appliance. It maintains connection with one or more vCenters, contains a repository of inventory data and user credentials and executes operations at VMs, ESX hosts, datastores or networks by utilizing VMware vRealize Orchestrator (vRO). Collectively, it consists of one or more web services that accepts commands from (previously discussed) *LaMa* VLA Adapter and take appropriate actions to implement the commands, typically with the help of the (previously discussed) VMware vRealize Orchestrator. For example:

  - When a SAP BASIS administrator activates (powers on) a SAP System via LaMa, the VLA Adapter sends commands to the `vla-service` (discussed later in this topic) to power on the underlying VMs. The `vla-service` in turn invokes a VLA-specific workflow on the VMware vRealize Orchestrator to turn on the VMs in the underlying vSphere infrastructure. An analogous action occurs when a SAP BASIS administrator deactivates (powers off) a SAP System.

- When a SAP BASIS administrator copies a SAP System, the VLA Adapter sends commands to the `vla-service` which in turn invokes a VLA-specific VMware vRealize Orchestrator workflow to create vSphere copies of the VMs on which the SAP Systems reside, configuring the VMs according to the parameters provided by the SAP BASIS administrator in the LaMa web user interface.

The VLA Appliance contains several components, including:

- A purpose-configured and hardened operating system (OS)
- A minimalist set of OS utilities and VLA-specific programs and configuration files required to provide the functionality described here. These include:
  - The `vla-service` — A web service running in `tomcat` that receives and processes commands from the VLA Adapter. It also serves out the VLA dashboard web UI. By default, this server listens on port 8443.
  - Tomcat user database — Database with usernames / passwords used to authenticate access to that instance's services. VI Administrators create an entry in the database for the VLA instance during deployment of the VLA environment using the `vla_user` command as detailed later in this document.
  - A `credentials store` (separate from the username / password database for tomcat access) that contains information needed for the various components of the VLA environment to communicate with one another. Each entry in the credentials store includes a component type (vRealize Orchestrator, *LaMa*, vCenter Server etc), the hostname and port (if configurable) for the component's API, and a username / password used to authenticate to the component's API. You create entries in this database using the `vla_credentials` command as detailed later in this document.

Performing a Fresh Install / Upgrade of VLA and Configuration 3

This chapter includes the following topics:

Performing a Fresh Installation and Configuration

This chapter covers installation and configuration of the components needed to connect *LaMa* to VMware technology. The first half covers deploying and configuring VMware vRealize Orchestrator. The second half discusses deploying and configuring the VMware Landscape Management Appliance (VLA), VMware Adapter for SAP Landscape Management, and the VMware vRealize Orchestrator work flows.

Prerequisites and Planning

During the installation of the solution, you must provide certain information, for example the IP address and fully-qualified domain name (FQDN) of certain hosts, credentials for authenticating to those hosts, options for configuration and more. To expedite your installation, and have it go smoothly, this document provides you with two worksheets to capture the required information.

Gather the information requested in these worksheets, record them, and then use the recorded values during your installation process.

Note For items that ask for a hostname, it is important that you provide the fully-qualified domain names (FQDN) of the hosts, not abbreviated names or IP addresses. For example, for a host whose short name is `foo` and is in the `example.com` domain, use `foo.example.com`, not just foo or foo.example.

Platform/Software/Networking Prerequisites

VLA version 1.5.1 requires, and is only supported on, certain platforms, with certain databases and using certain networking ports. The following sub-sections detail these requirements.

Platforms Supported

- http://www-review.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/adapter-sap-lvm/vmware-adapter-for-sap-landscape-management-release-notes.pdf
- vSphere 6.0 U2

- VMware vRealize Orchestrator

Note VMware changed the name of vCenter Orchestrator to vRealize Orchestrator when they revised the product from version 5.x to version 6.x.

Operating Systems Supported

For details on supported operating systems refer to:
http://www-review.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/adapter-sap-lvm/vmware-adapter-for-sap-landscape-management-release-notes.pdf

Databases Supported

For details on supported databases refer to:
http://www-review.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/adapter-sap-lvm/vmware-adapter-for-sap-landscape-management-release-notes.pdf

VLA System Requirements

- 1vCPU
- 4 GB of Memory
- 9 GB of Disk Space
- 1vNIC
- 1 CD (for updates)

Port Requirements

- vCenter Server ports: 443, 7444
- VLA port: 8443
- VMware vRealize Orchestrator ports: 8281, 8283, 5480

Planning for VMware vRealize Orchestrator Installation

Recall from "Reference Architecture," on page 10 that the VLA environment must include at least one instance of vRealize Orchestrator. Use the following table to plan the deployment of each said instance.

Table 3-1. Table 1 vRealize Orchestrator Deployment Worksheet

vRealize Orchestrator Input Field	Description	Value
Hostname	The FQDN of the host. Needed for deployment. Example : sapi-vco.example.com	
Default Gateway	Needed for deployment. Example : 192.168.1.1	
DNS	Domain Name System Server address. Needed for deployment.	
Network 1 IP Address	Needed for deployment. Example : 192.168.1.110	
Network 1 Netmask	Needed for deployment. Example : 255.255.255.0	

Table 3-1. Table 1 vRealize Orchestrator Deployment Worksheet (Continued)

vRealize Orchestrator Input Field	Description	Value
VMware vRealize Orchestrator configuration interface credentials	Needed for deployment. Username Password	
VMware vRealize Orchestrator group	The group that VMware vRealize Orchestrator administrators belong to. SSO accounts that are members of this group are able to log intoVMware vRealize Orchestrator. Selected when you configure VMware vRealize Orchestrator authentication. See "VMware vRealize Orchestrator Administrators Group," on page 22	
VMware vRealize Orchestrator credentials	A SSO account with administration rights that theVMware vRealize Orchestrator uses to register theVMware vRealize Orchestrator with the Server. Entered when you configure VMware vRealize Orchestrator authentication.	
vCenter Server Administrative Credentials	To setup and create secondary, less privileged accounts on vCenter Server	

Using VLA without DNS Server

NOTE This is NOT the recommended configuration.

The VLA needs the IP address of all hosts with which it communicates, including the LaMa, vRO and vCenter Servers. Most environments use DNS servers to resolve hostnames to IP addresses. If your environment does not use DNS, follow the procedure in the next section to configure host name resolution for the VLA.

Configuring Hosts

If your environment does not have a DNS server, you must list all hosts to which the VLA needs to connect in `/etc/hosts` file on the VLA VM. For each host, enter a line consisting of the IP address, the fully qualified hostname, and the hostname into the file. The IP address must be at the beginning of the line and the entries separated by blanks or tabs. Comments are always preceded by the # sign. For example:

Procedure

- Open the `/etc/hosts` file in the editor of your choice. Make one entry per host on a separate line similar to the following:

```
127.0.0.1 localhost
192.168.0.1 s1.example.com s1 # comment
192.168.0.2 s2.example.com s2 # comment
```

VMware VLA Installation Prerequisites

Recall from "Reference Architecture," on page 10 that the VLA environment must include an instance of the VLA Appliance. Use the following table to plan the deployment of the appliance.

Table 3-2. Table 3 VLA Deployment Worksheet

VLA Input Field	Description	Value
FQDN	Needed for deployment **Note** Fully Qualified Domain Name (FQDN) should resolve to VLA's IP Address	
IP Address	Needed for deployment	
Network Mask	Needed for deployment	
Gateway	Needed for deployment	
DNS Server	Needed for deployment NOTE: If a DNS server is not implemented, see "Using VLA without DNS Server," on page 15	
Console User Name	User name used to login to the VLA. This must not be "root" and must be between 6-32 characters in length.	
Console User Password	Initial password for the console user account. Password must be at least 8 characters in length. You can change the password later by using the "passwd" command on the console, if needed.	
SSH Access	Enable or Disable SSH access on the VLA.	
Timezone	The timezone selection for the VLA.	
VLA Username	Username of VLA application user. The VLA application user is entered to connect *LaMa* to the VLA. Entered when the appliance is configured.	
VLA Password	Password of VLA application user. The VLA application password is entered to connect *LaMa* to the VLA. Entered when the appliance is configured.	
vCenter Server FQDN	FQDN of each vCenter Server that is controlled by the VLA	
vCenter Server User Credentials	The username and password for the Limited Rights service account that the VLA will use to gather inventory from vCenter Server. See section "Creating a Limited-Rights vCenter Server user," on page 30	
VMware vRealize Orchestrator FQDN	Fully Qualified Domain Name of the VMware vRealize Orchestrator Server	
VMware vRealize Orchestrator Credentials	The username and password for a SSO service account that is in the VMware vRealize Orchestrator Admin group	

Table 3-2. Table 3 VLA Deployment Worksheet (Continued)

VLA Input Field	Description	Value
LaMa Credentials	The administrator username and password of the LaMa application	
LaMa SSH Credentials	SSH username and password of LaMa VM	

Virtual Infrastructure Preparation

The VLA appliance runs in a virtual infrastructure (VI) environment similar to the one depicted in section "Reference Architecture," on page 10. The environment includes vCenter Server and VMware vRealize Orchestrator. The following sections (and their sub-sections) provide details on configuring vCenter Server, and deploying / configuring / testing VMware vRealize Orchestrator, so that you can subsequently deploy, configure, and run VLA instance(s) in your virtual infrastructure.

vCenter Server Configuration

There are a number of tasks you must perform on your vCenter Server to prepare for the installation of the VLA. You need to create a group of VMware vRealize Orchestrator administrators, a limited rights vCenter Server user and guest customization specs.

Setting up of accounts needed by the vla-service

The vla-service connects to the VMware vRealize Orchestrator to execute VM commands such as `Start`, `Stop` and `Clone`. The service needs a vCenter Server SSO service account to log into VMware vRealize Orchestrator Server and to run workflows. VMware recommends that you set up an account that has the least amount of privileges needed by the vla-service. To create this account, do the following:

- Create a role for user to execute workflows onVMware vRealize Orchestrator
- Create a VMware vRealize Orchestrator Administrators Group
- Create a VLA user for VMware vRealize Orchestrator
- Set the permission for the VLA user

Create a role for user to execute workflows on VMware vRealize Orchestrator

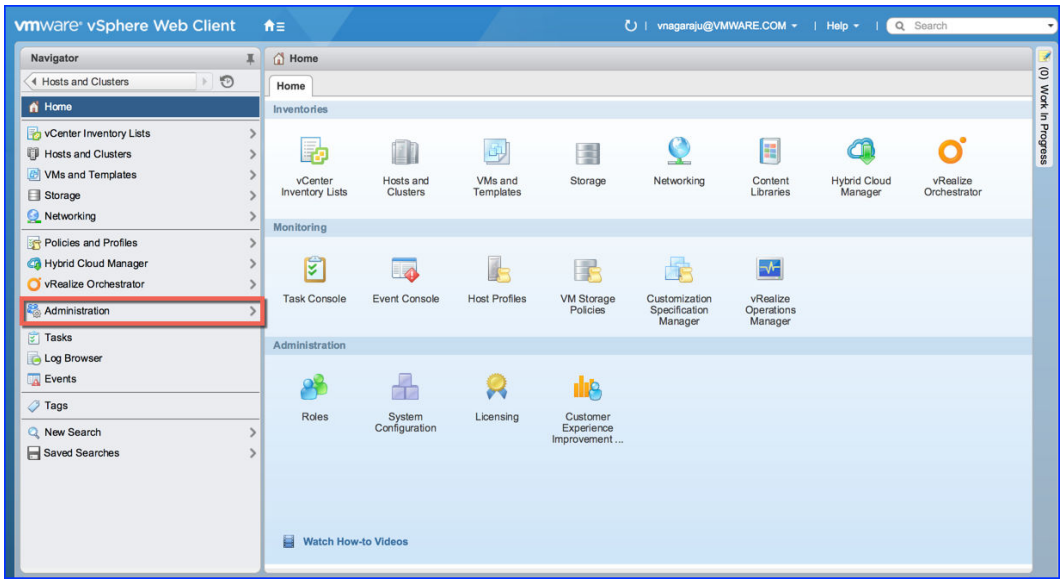
To create a role in vCenter Server for VMware vRealize Orchestrator in order to be able to execute workflows, perform the following steps:

Procedure

1 Log in to VMware vSphere Web Client(VWC) using administrator credentials. Click **Administration** in the Navigator pane.

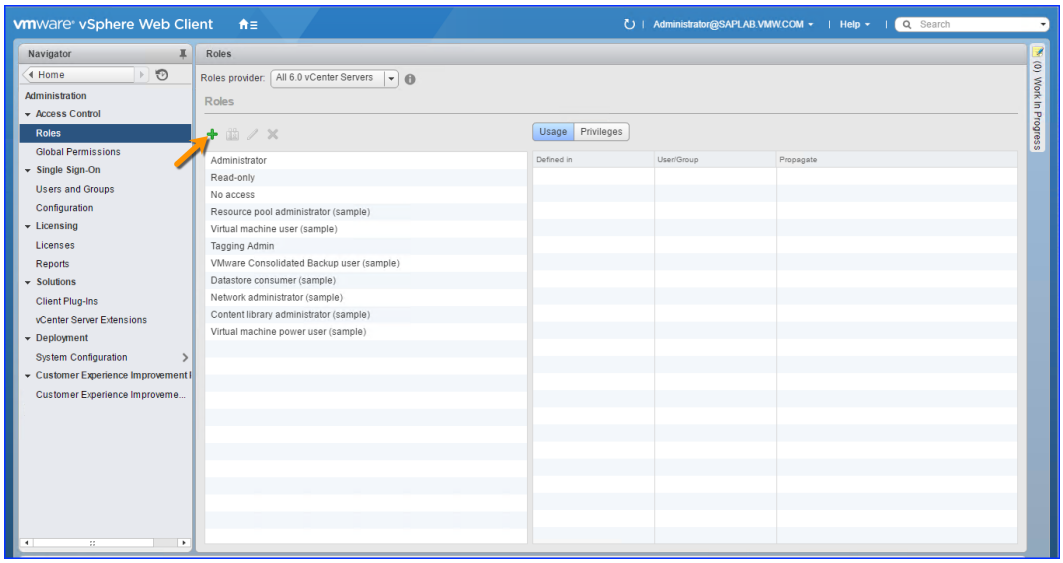
  The browser displays the VWC Home page including a Navigator pane similar to the following. Note that the **Administration** tab is highlighted for emphasis.

Figure 3-1. VWC Home Page



2 Click **Roles** (if not already selected).

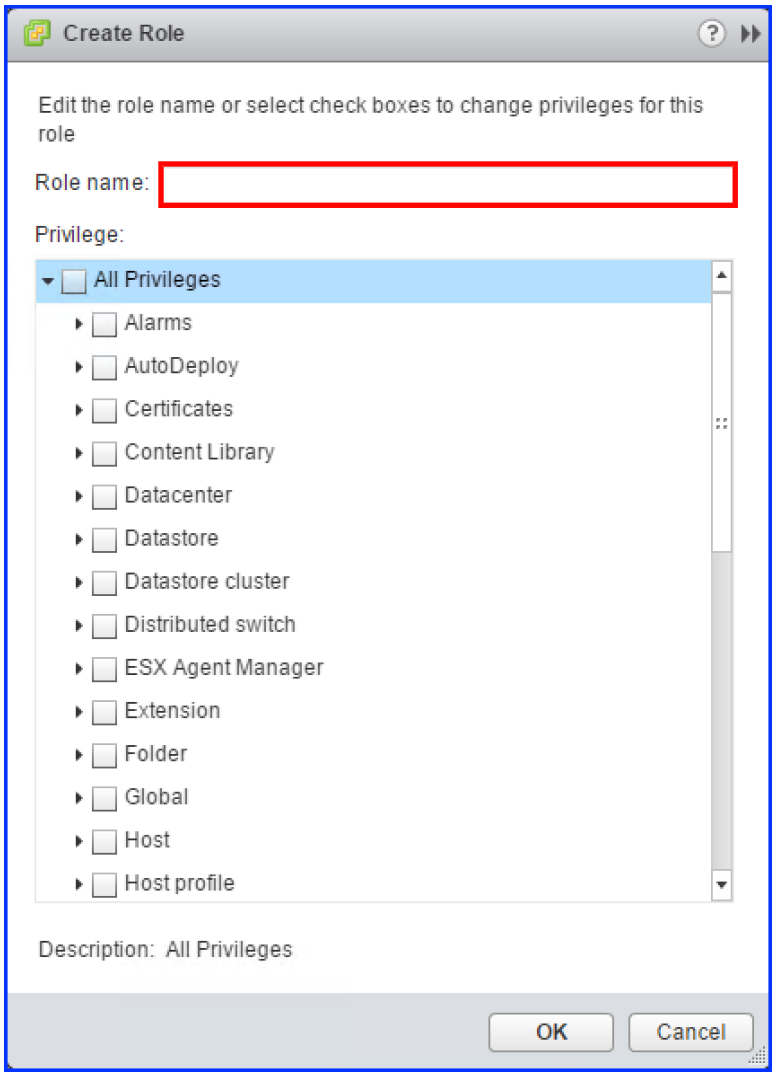
Figure 3-2. VWC - Administration - Roles



3 Click the **Plus sign** in the pane to the right of the Navigator pane (pointed to by the arrow for emphasis).

The browser displays the **Create Role** dialog similar to the following:

Figure 3-3. VWC - Administration - Roles - Create Role



4 In the **Role name** field, type: VLA vRO user

5 In the **Privilege** section, find and check the following privileges for the role:

Table 3-3. Role Privilege Settings

Privilege Settings
Global-> Log event
Virtual Machine-> Interaction-> Power On
Virtual Machine-> Interaction-> Power Off
Virtual Machine-> Interaction-> Suspend
Datastore-> Allocate space
Network-> Assign network
Resource-> Assign virtual machine to resource pool
Resource-> Migrate powered off virtual machine
Resource-> Migrate powered on virtual machine
Virtual Machine-> Configuration-> Settings

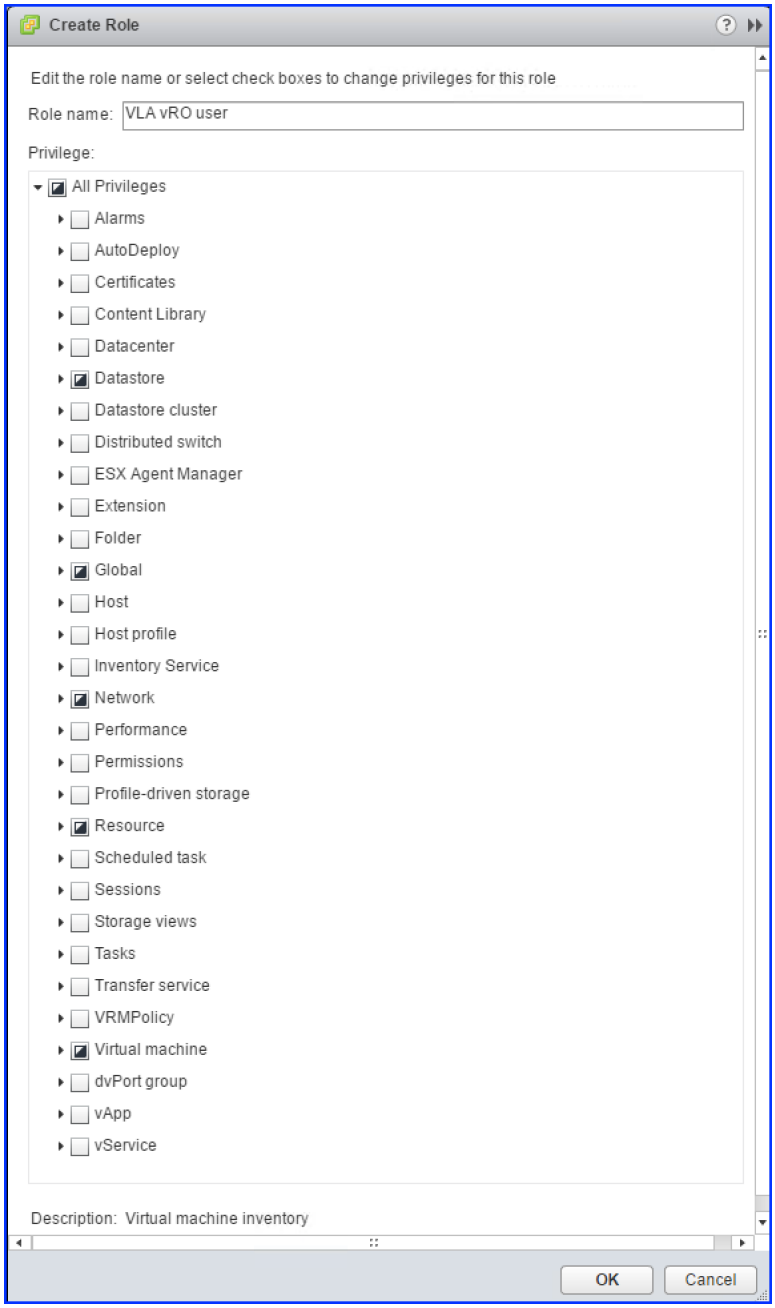
Table 3-3. Role Privilege Settings (Continued)

Privilege Settings
Virtual Machine-> Configuration-> Modify device settings
Virtual Machine-> Inventory-> Create from existing
Virtual Machine-> Provisioning-> Clone virtual machine
Virtual Machine-> Provisioning-> Customize
Virtual Machine-> Provisioning-> Deploy template
Virtual Machine-> Provisioning-> Mark as template
Virtual Machine-> Provisioning-> Mark as virtual machine
Virtual Machine-> Provisioning-> Read customization specifications
Virtual Machine-> Snapshot management-> Create snapshot
Virtual Machine-> Snapshot management-> Remove snapshot
Virtual Machine-> Snapshot management-> Revert to snapshot
Virtual Machine-> Inventory-> Remove

To understand the various LaMa operations and the corresponding privilege settings that you should set when you create a VMware VLA Role in vCenter Server for VMware vRealize Orchestrator, refer to "Role Privilege Settings - VMware VLA Role for VMware vRealize Orchestrator," on page 108

6 Upon completing the previous step, **Privilege** area of the **Create Role** dialog should look similar to the following:

Figure 3-4. VWC - Create Role - Privileges

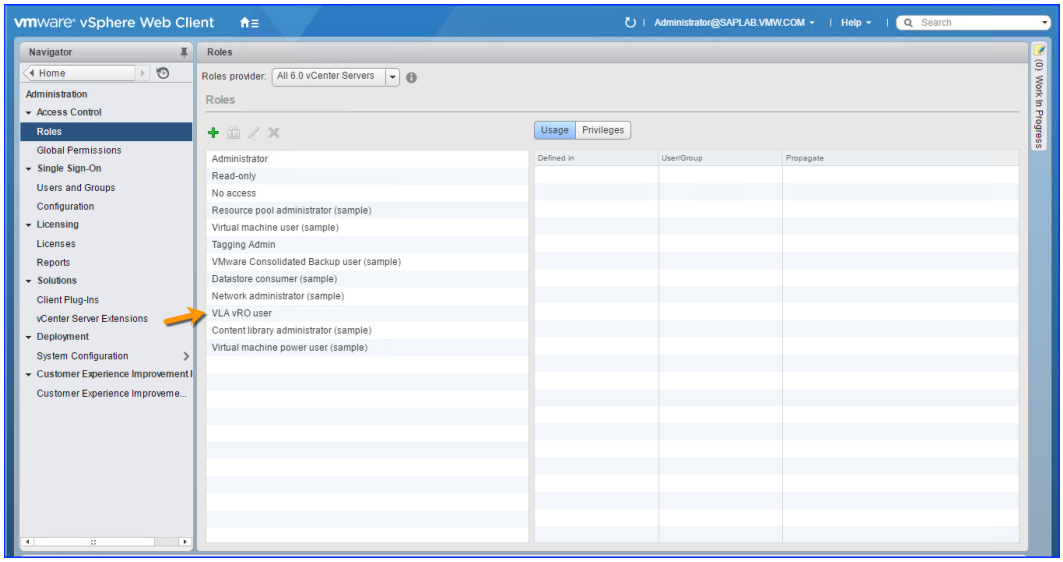


NOTE the half-marked boxes for groups with checked privileges.

7 Click **OK** to create the role.

The browser closes the **Create Role** pop-up. You should now see the new role in the list similar to the following:

Figure 3-5. VWC - Create Role



Note The VLA vRO user role you created is selected for emphasis.

Upon successfully completing the steps mentioned in this section, you next create a role in vCenter Server for VMware vRealize Orchestrator in order to be able to execute workflows.

VMware vRealize Orchestrator Administrators Group

The VMware vRealize Orchestrator Administrators group is a SSO group that is used to grant permission to access the VMware vRealize Orchestrator Server. Any user or group in this group has administrator access to the VMware vRealize Orchestrator Server. Provide this group when configuring the VMware vRealize Orchestrator and VLA user for VMware vRealize Orchestrator. You can use an existing SSO group or create a new one.

Note Make the SSO user referenced in the preceding paragraph a member of the VMware vRealize Orchestrator Administrators Group.

Create a (Limited Rights) VLA user in vCenter Server for VMware vRealize Orchestrator

You need a vCenter Server user to which you assign the role you created in the preceding section. It is recommended calling this user `vlavroadmin`. If your vCenter Server has been associated with an Active Directory Server, create a user in the said Active Directory Service, and then proceed to the next section to assign it the role for vRealize Orchestrator.

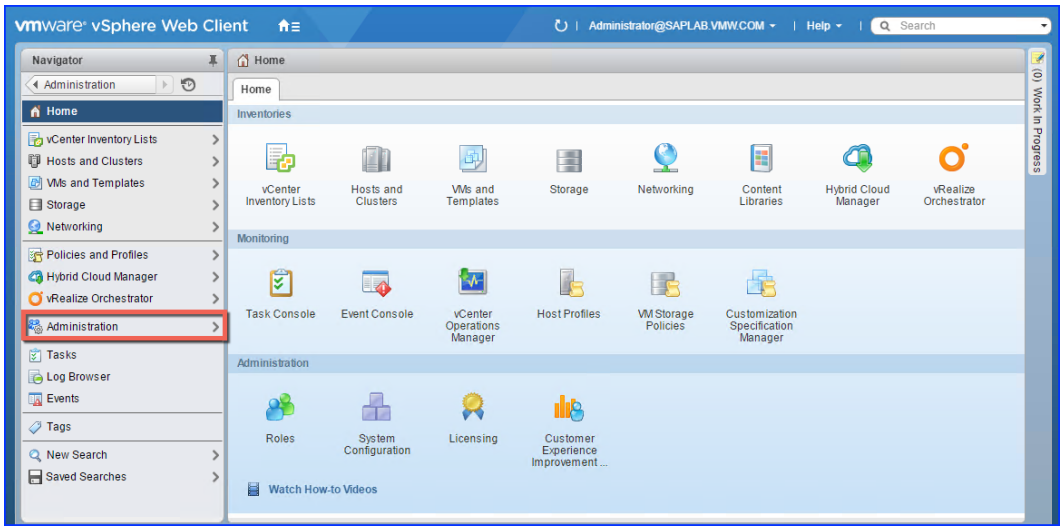
If you are using VMware vCenter Single Sign-On (SSO) Server to maintain your users, follow this procedure to create the `vlavroadmin` user:

Procedure

1 Log in to VMware vSphere Web Client(VWC) using administrator credentials. Click **Administration** in the Navigator pane.

The browser displays the VWC Home page including a Navigator pane similar to the following. Note that the **Administration** tab is highlighted for emphasis.

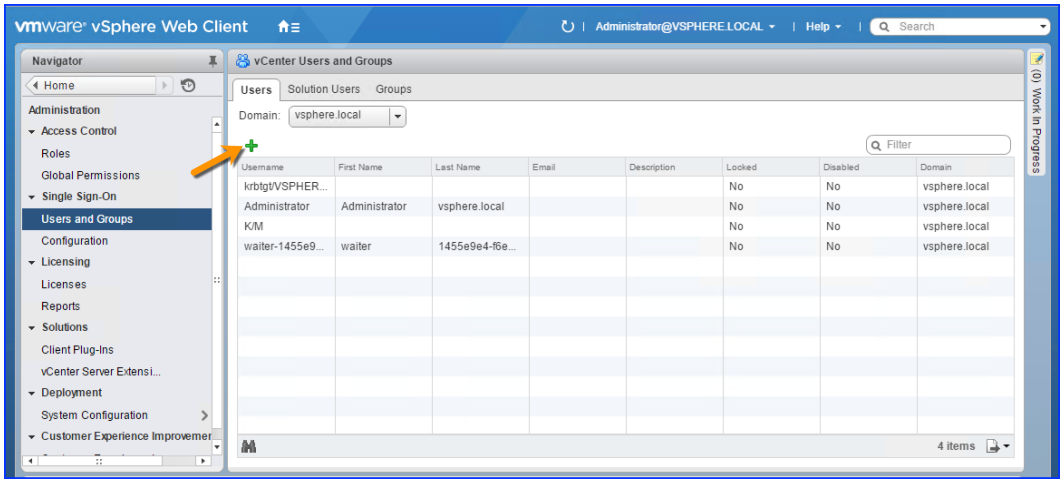
Figure 3-6. VWC Home Page



2 Click **Users and Groups**.

The browser displays a screen similar to the following:

Figure 3-7. VWC - Administration - Users and Groups

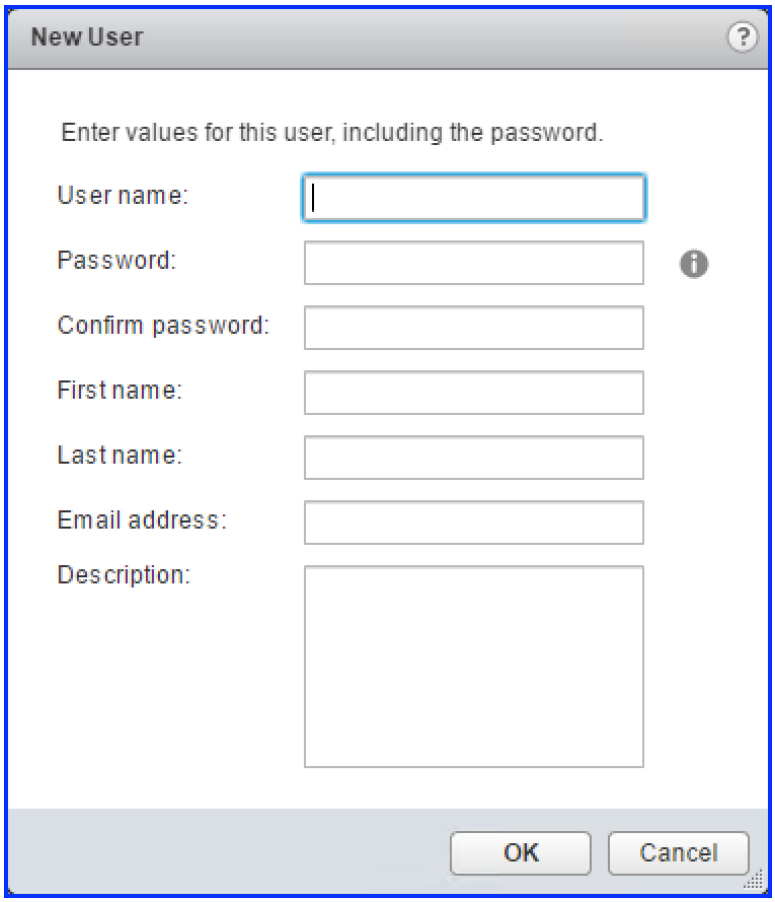


3 Select the SSO domain to which you wish to add the user from the **Domain**

4 Click the **green plus** icon (pointed to by the arrow for emphasis) to add a new user.

The browser displays the New User dialog similar to the following:

Figure 3-8. VWC - New User



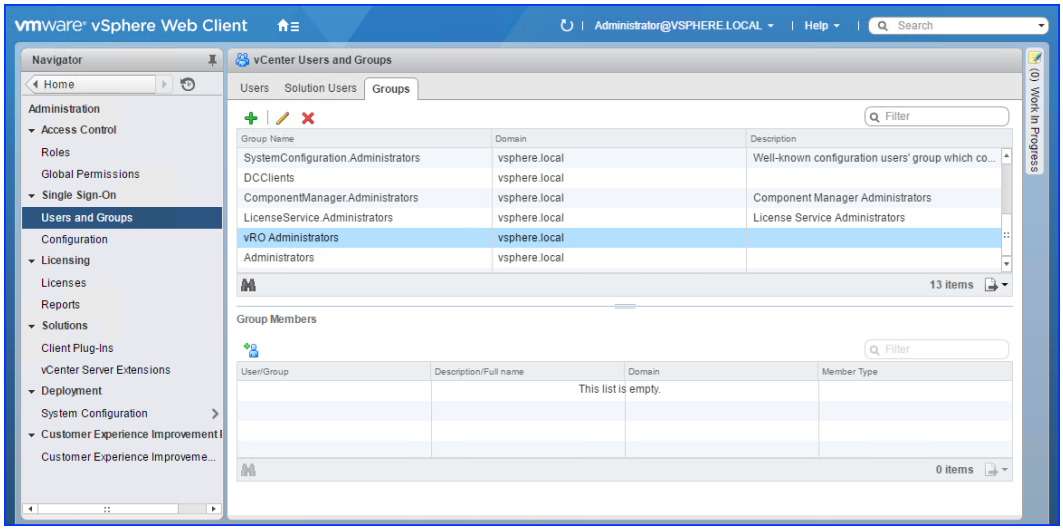
5 Complete the fields in the dialog, giving the user the name vlavroadmin and assigning a conforming password, and then click **OK**.

The browser closes the dialog and displays the Users and Groups page with your new user added.

6 Now Click the **Groups** tab.

Find the vRealize Orchestrator Administrators group in the list of existing groups.

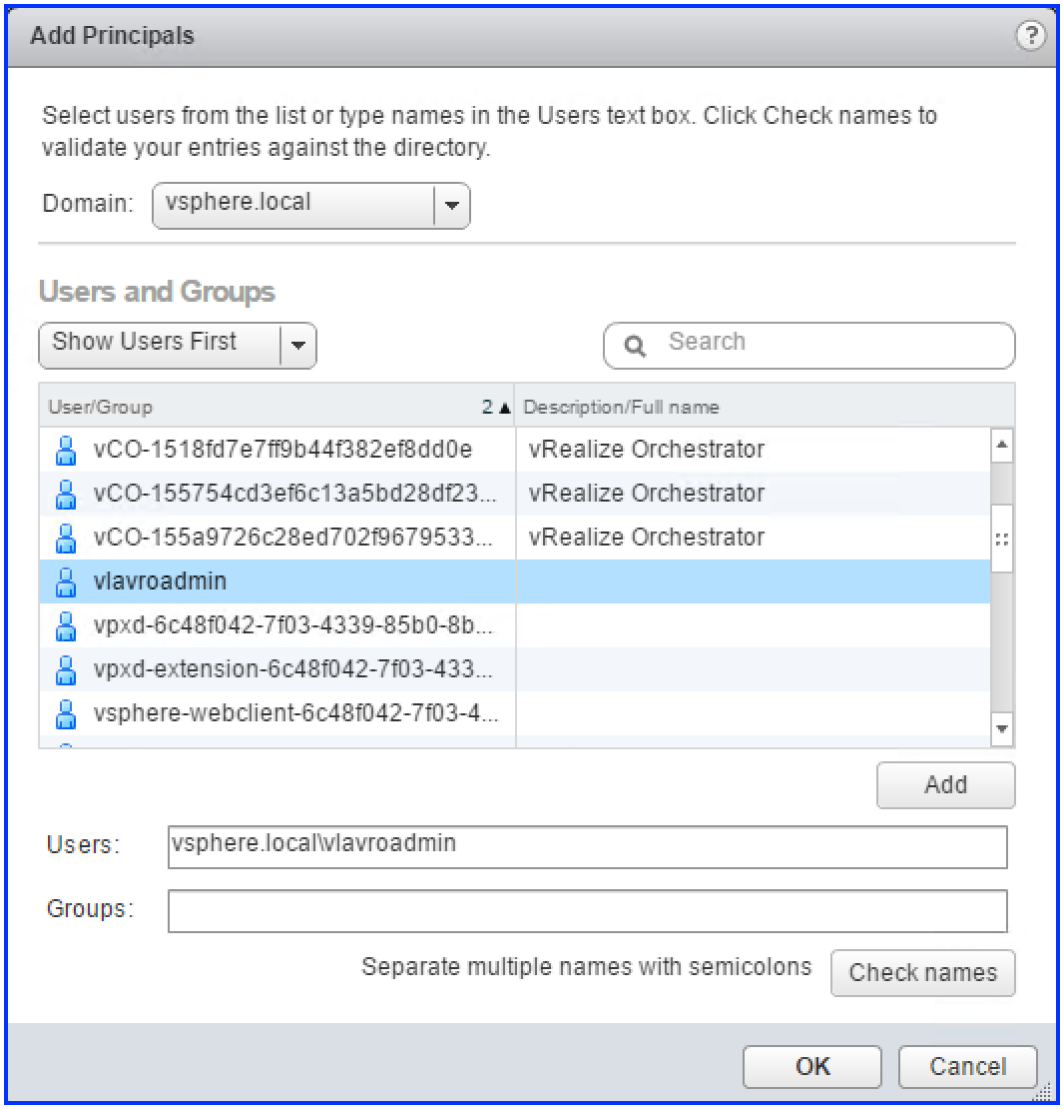
Figure 3-9. VWC - vCenter Users and Groups



7 Click **Add member** (The only icon under Group Members)

The browser displays the **Add principals** dialog similar to the following:

Figure 3-10. VWC - Add Member - Add principals



8 Find vlavroadmin in the **User/Group** list and then Click **Add** and **OK**.

The browser closes the dialog and displays the Groups tab with your new user added to the vRealize Orchestrator Administrators group.

You have successfully created a VLA user in vCenter Server for VMware vRealize Orchestrator

Setting Permissions for the (Limited Rights) VLA user in vCenter Server for VMware vRealize Orchestrator

Procedure

1 Log into the vSphere Web Client (VWC) with administrator credentials.

2 Click **Hosts and Clusters**.

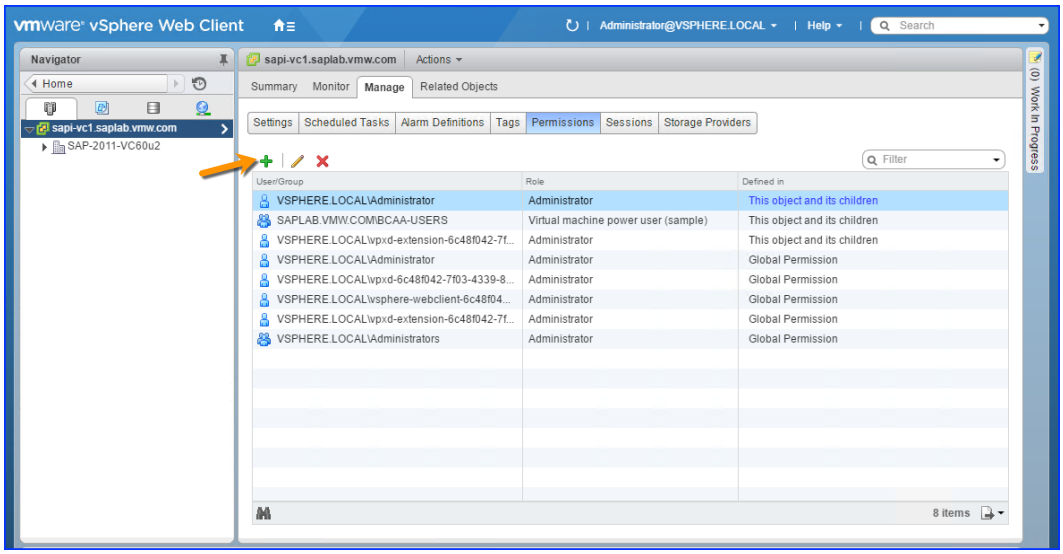
3 Click on the vCenter Server you want the VLA to manage.

4 Click **Manage**.

Click on **Permissions**.

The browser displays a screen similar to the following:

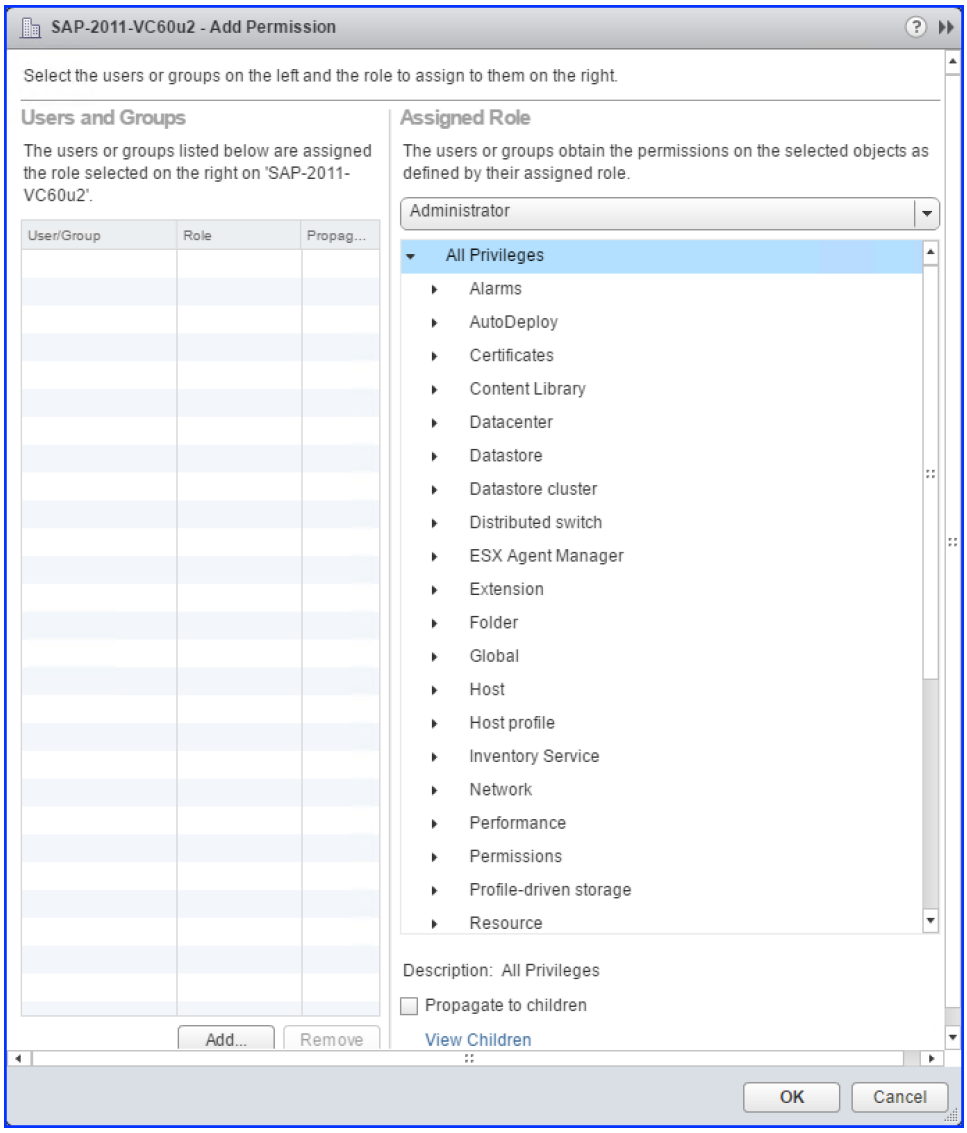
Figure 3-11. VWC-Hosts and Clusters-Manage-Permissions



5 Click the **green plus** icon to add permission.

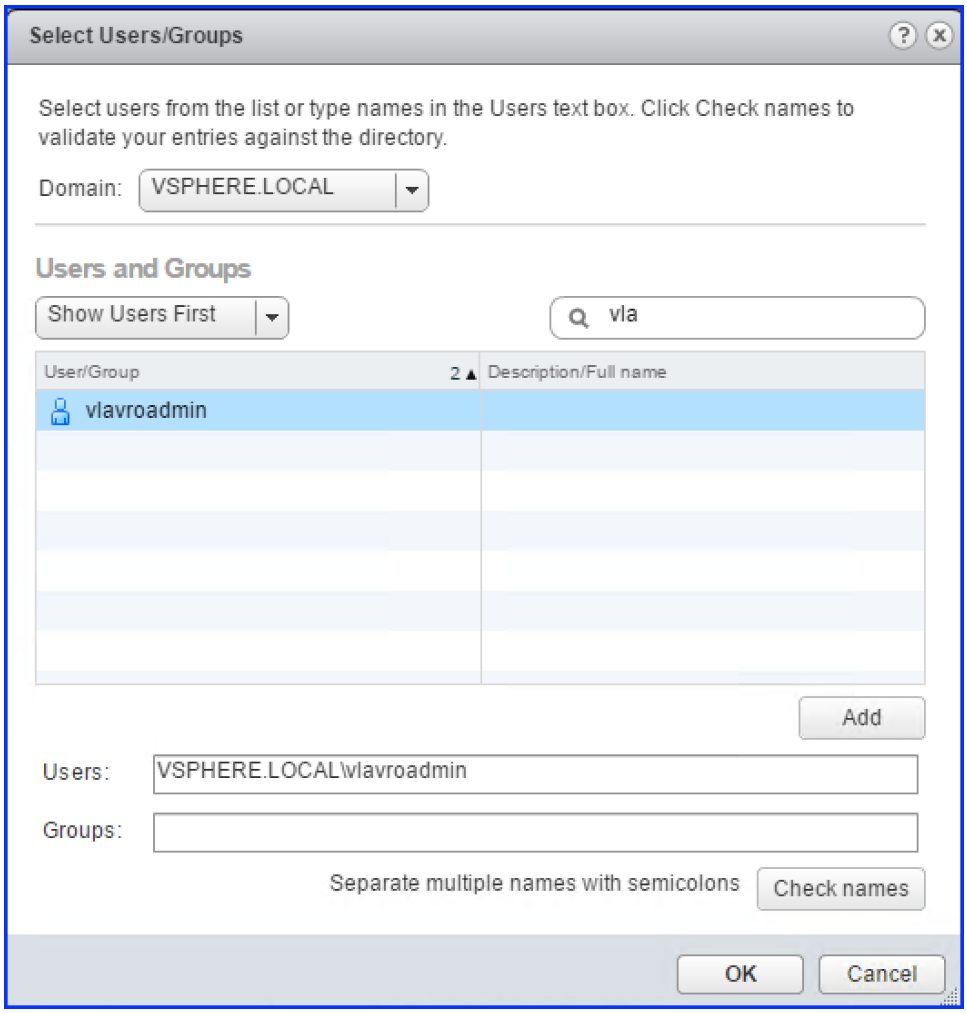
The browser displays a screen similar to the following:

Figure 3-12. VWC-Add Permission



6 Click **Add** ...

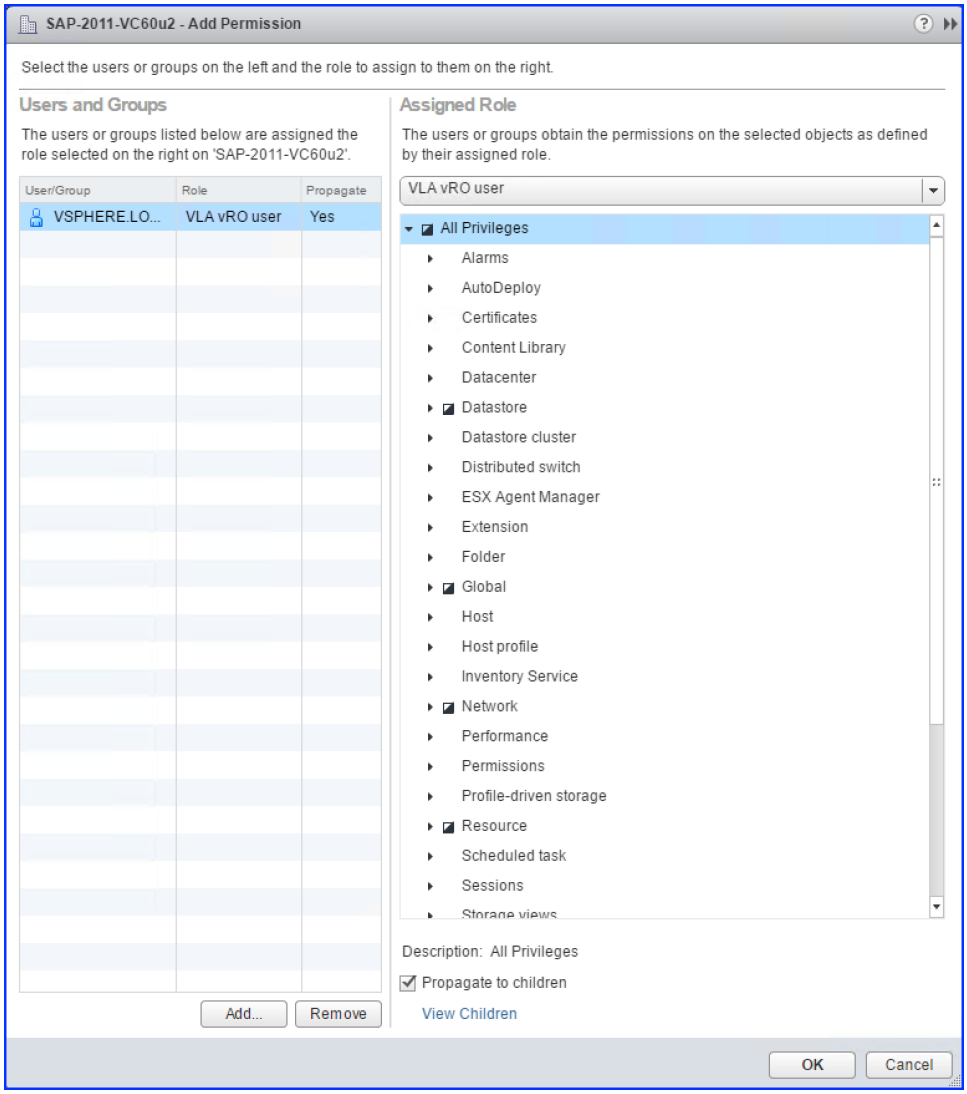
Figure 3-13. VWC-Select User's Groups



7 Choose your SSO domain, and select the user vlavroadmin. Click **Ok**.

8 In the **Assigned Role** List box, select role VLA vRO user.

Figure 3-14. VWC - Add Permission



9 Make sure the **Propagate to children** check box is checked.

Note If the **Propagate to children** option is not checked for vCenter Server intentionally in order to adjust access rights for the user more accurately, then granting permissions to the following inventory objects should be taken into account:

- vCenter Server (The **Hosts and Clusters** view)
- Datacenters and Folders for Datacenters (The **Hosts and Clusters** view)
- Clusters and ESXi hosts within the Clusters, and Hosts and Clusters Folders (The **Hosts and Clusters** view)
- Resource Pools and vApps (The **Hosts and Clusters** view)
- Virtual Machines, VM Templates and Folders for Virtual Machines (The **VMs and Templates** view)
- Datastores and Folders for Datastores (The **Storages** pane)
- Networks and Distributed Switches (The **Networking** view)

  Setting access permissions per inventory object can be done in the same manner as it's demonstrated for the vCenter Server: The user vlavroadmin needs assigning to the VLA vRO user role for an inventory object on the **Manage - Permissions** tab of this object.

  A lack of permissions for some of the aforementioned objects may result in execution errors of LaMa operations.

10 Click **OK**. This saves the permission.

You have successfully set required permissions for the VLA user in vCenter Server for VMware vRealize Orchestrator

Creating a Limited-Rights vCenter Server user

The vla-service connects to vCenter Server(s) to gather inventory and statistics. The service needs a vCenter Server SSO service account to log into vCenter Server. VMware recommends that you set up an account that has the least amount of privileges needed by the vla-Service. To create this account:

1 Create a VMware VLA role

2 If you are using VMware SSO, Create a VMware VLA user

3 Set the permission for the Appliance User

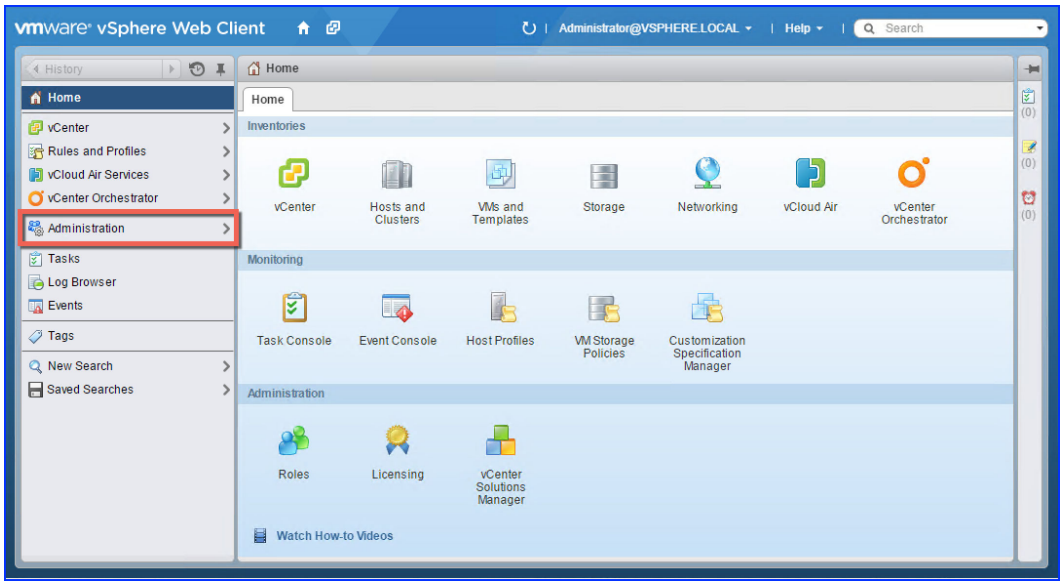
Create a VMware VLA Role

Procedure

1 Log in to the VMware vSphere Web Client(VWC) using administrator credentials.

  The Browser displays the VWC Home page including a Navigator pane similar to the following:

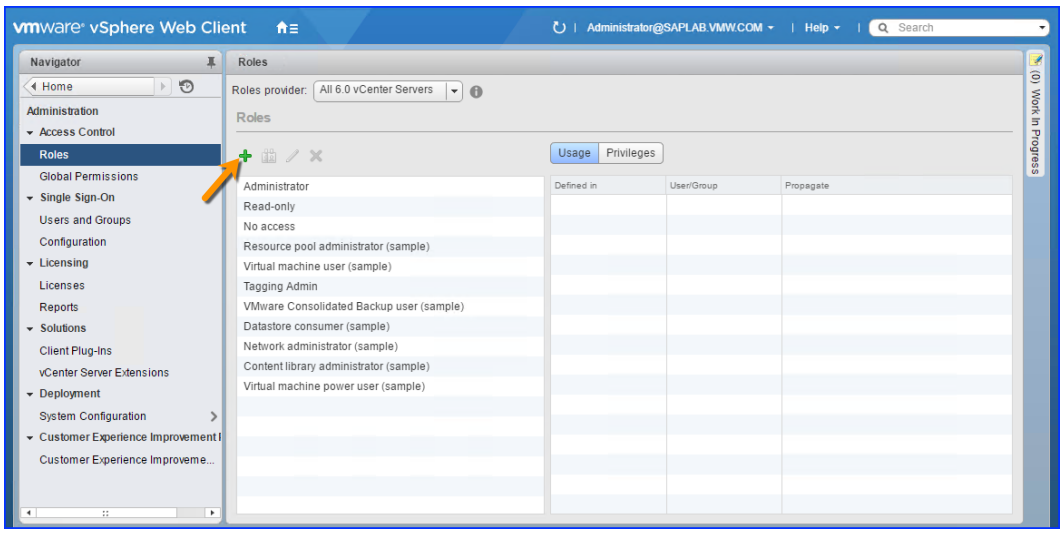
Figure 3-15. VWC - Administration



2 Click **Administration** (highlighted for emphasis).

The Browser displays a page similar to the following:

Figure 3-16. VWC - Administration - Roles

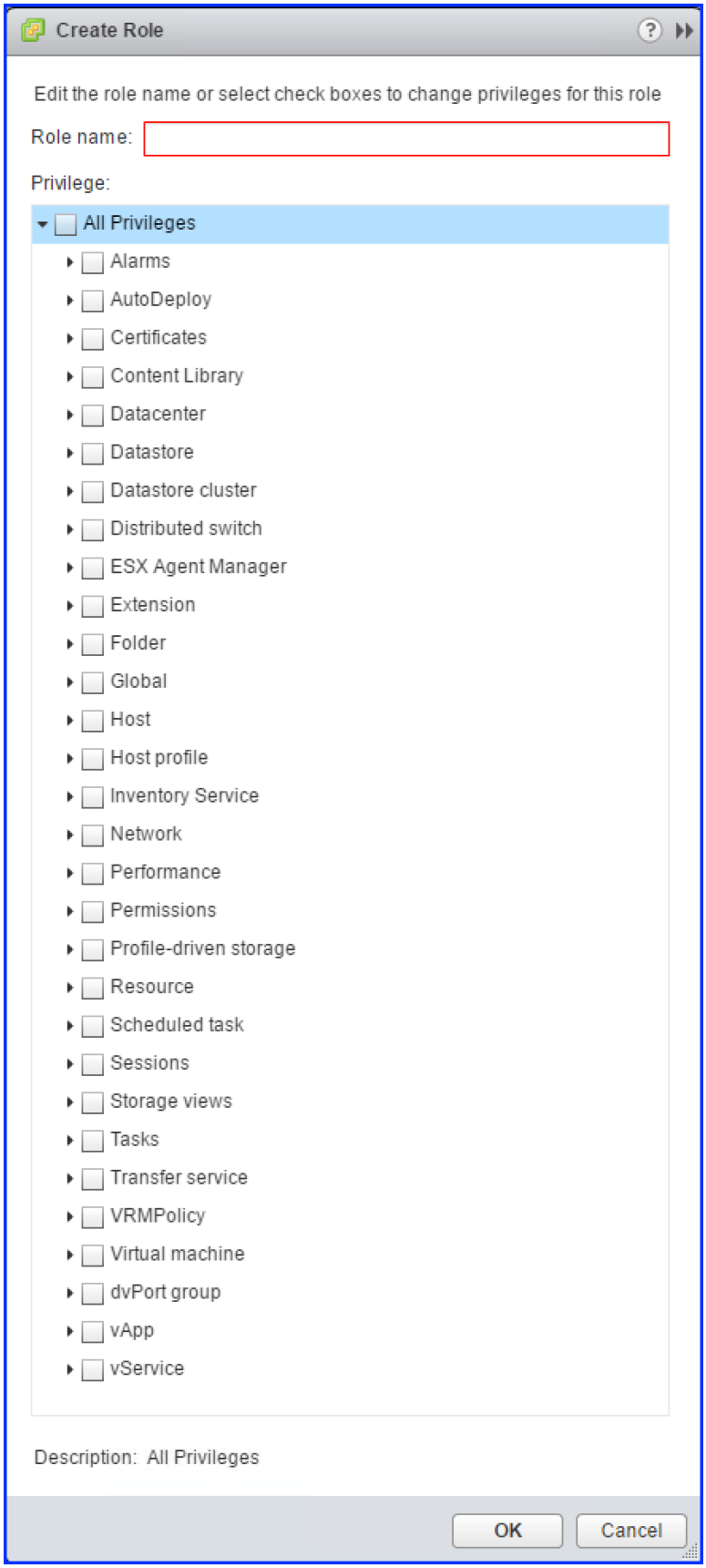


3 Click **Roles** (if it is not already selected).

4 Click the **Plus sign** in the pane to the right of the Navigator pane (pointed to by the arrow for emphasis).

The browser displays the Create Role dialog similar to the following:

Figure 3-17. VWC - Create Role



5 In the Role name field, type : **VMware LaMa Appliance**.

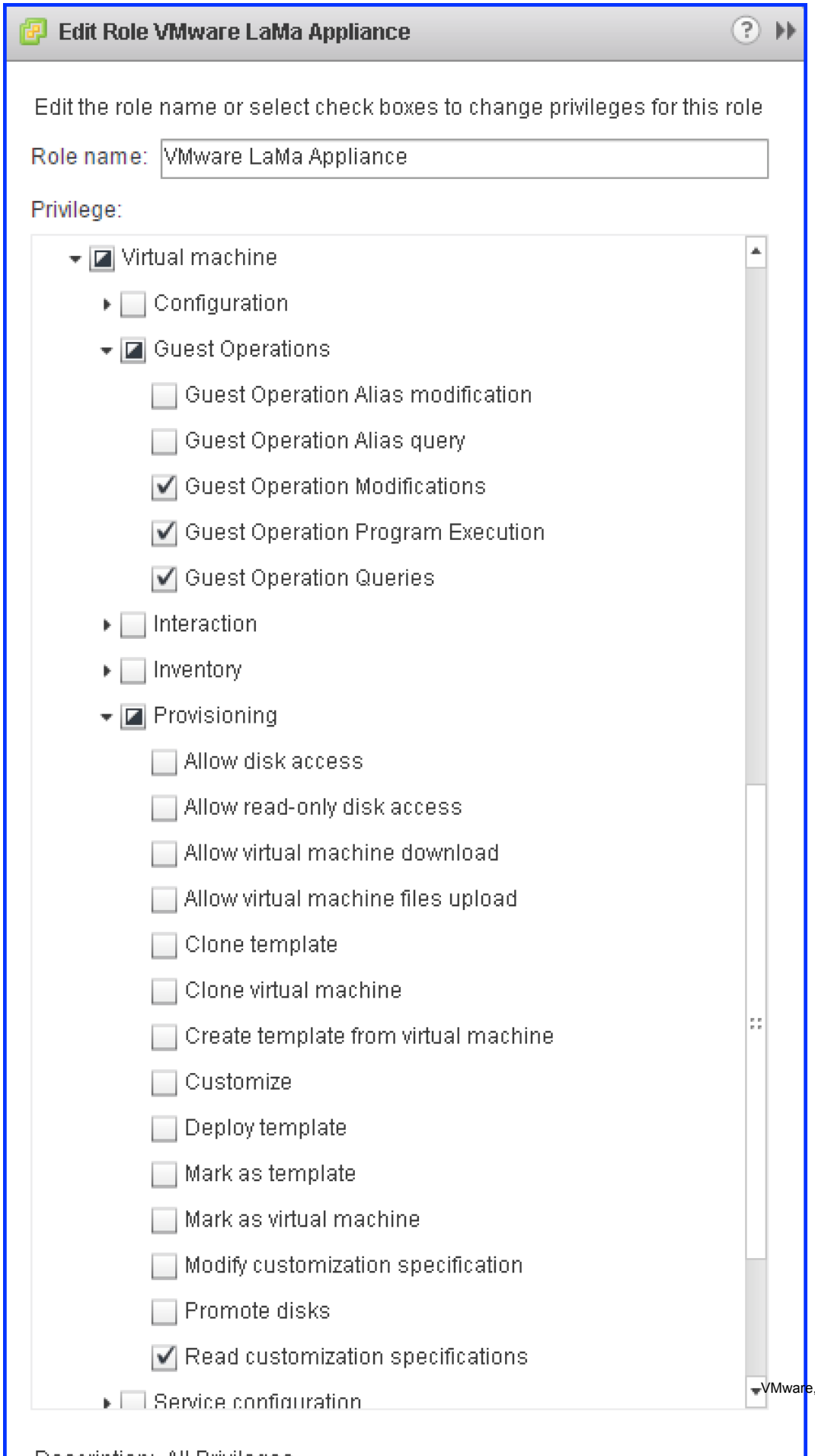
6 In the **Privilege** section find and check the following privileges for the role:

Table 3-4. Role Privileges

Privilege List
Virtual Machine -> Provisioning -> Read Customization Specification
Virtual Machine -> Guest Operations -> Guest Operation Modifications
Virtual Machine -> Guest Operations -> Guest Operation Program Execution
Virtual Machine -> Guest Operations -> Guest Operation Queries

The Privilege area of the Create Role dialog should look similar to the following:

Figure 3-18. VWC - Create Role

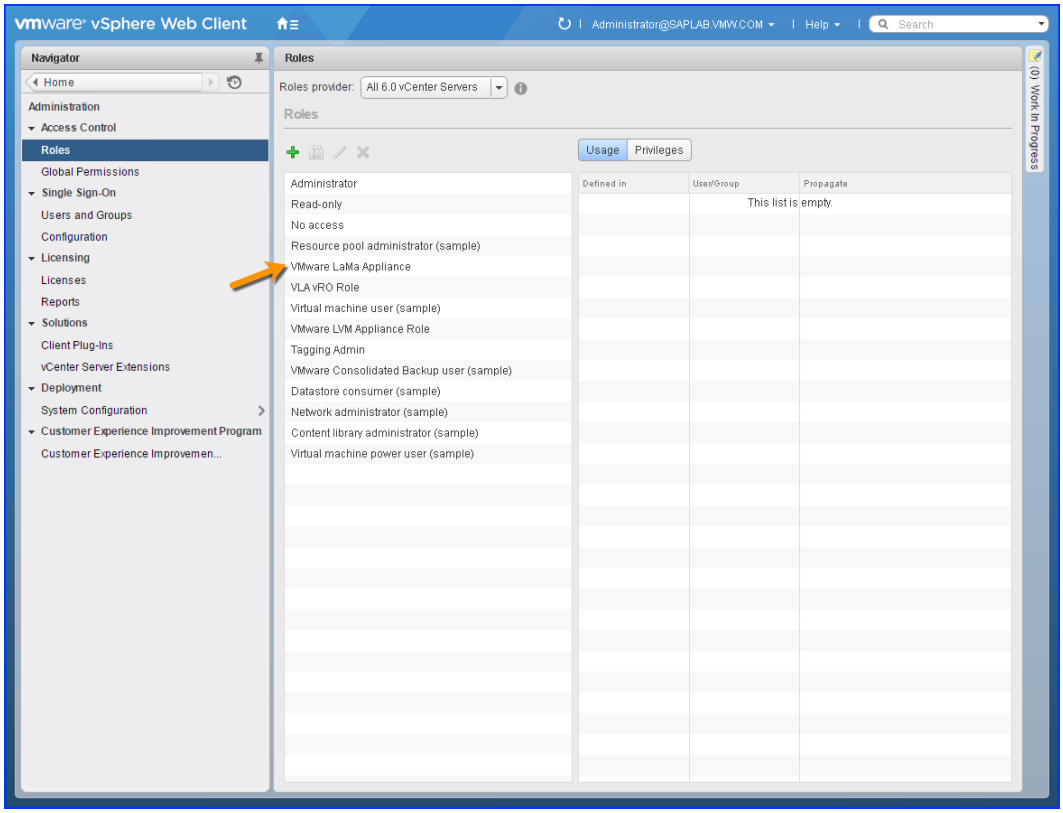


Note All the boxes, **Provisioning** and **Guest Operations** under **Virtual machine** should be half checked upon checking the privileges mentioned in the **Role Privileges** table above.

7 Click **OK** to create the role.

The browser closes the Create Role pop-up. You should now see the new role in the list similar to the following:

Figure 3-19. VWC - Roles



Note The **VMware LaMa Appliance** role selected for emphasis.

You successfully created a VMware VLA Role.

Create a (Limited Rights) VLA user

You need a vCenter Server user to which you assign the role you created in the preceding section. You may want to use a meaningful name, say **vla_appliance_user**. If your vCenter Server has been associated with an Active Directory Server, create a user in said Active Directory Service, and then proceed to the next section to assign it the VMware VLA role.

If you are using VMware Single Sign On Server (SSO) to maintain your users, follow this procedure to create the user by name **vla_appliance_user**:

Procedure

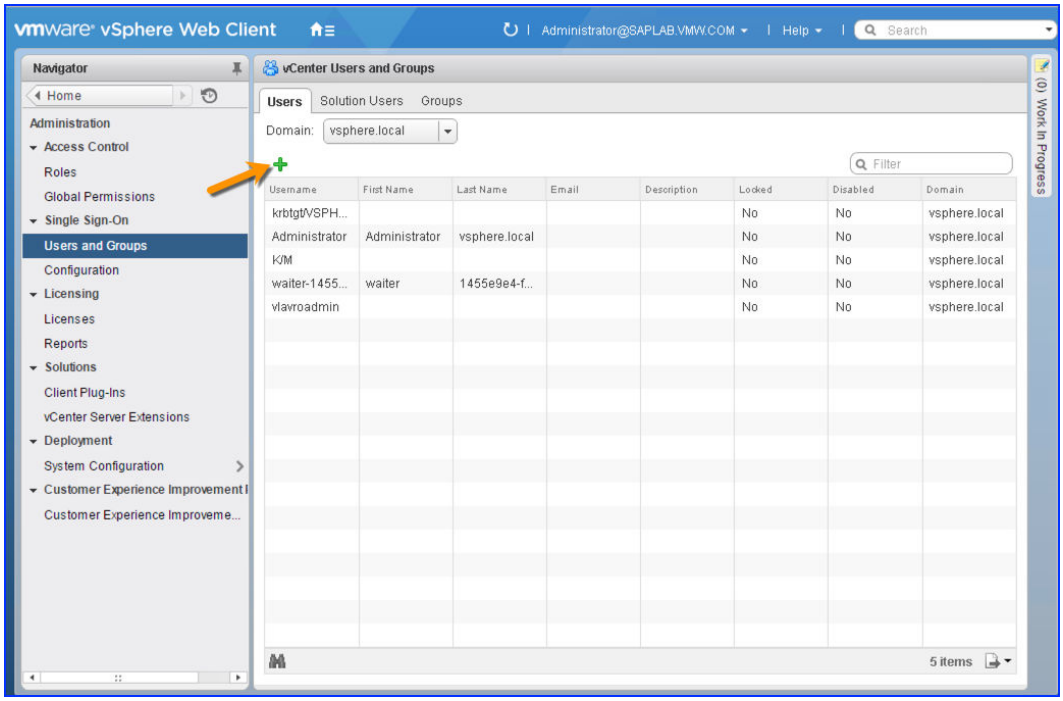
1 Log in to the VMware vSphere Web Client(VWC) using administrator credentials.

2 Click **Administration** in the left panel of the VMware vSphere Web Client.

3 Click **Users and Groups**.

The browser displays a screen similar to the following:

Figure 3-20. VWC - Users and Groups

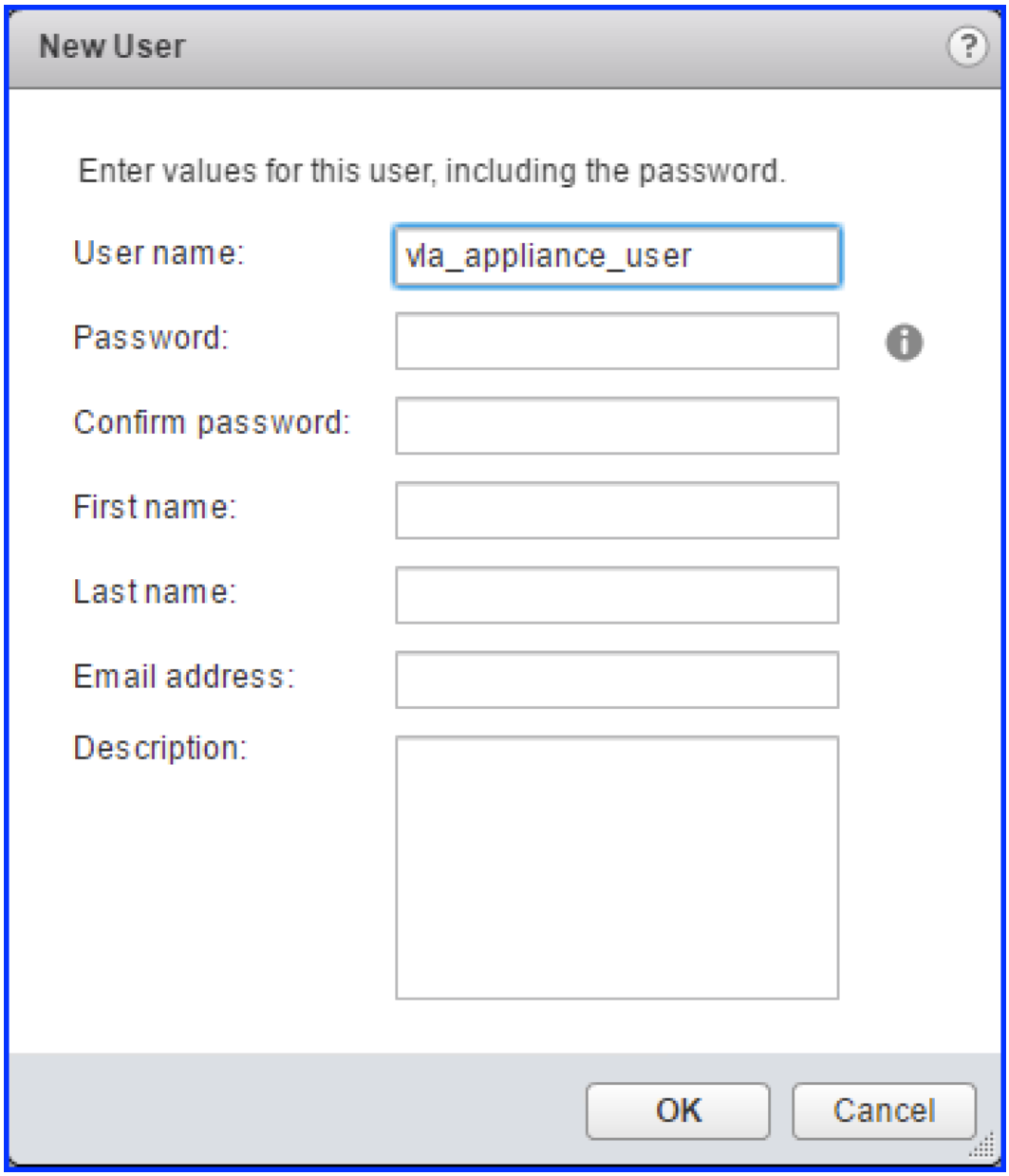


4 Select the SSO domain to which you wish to add the user from the **Domain** dropdown (for example **vsphere.local**)

5 Click the **green plus** icon to add a user.

The browser displays the New User dialog similar to the following:

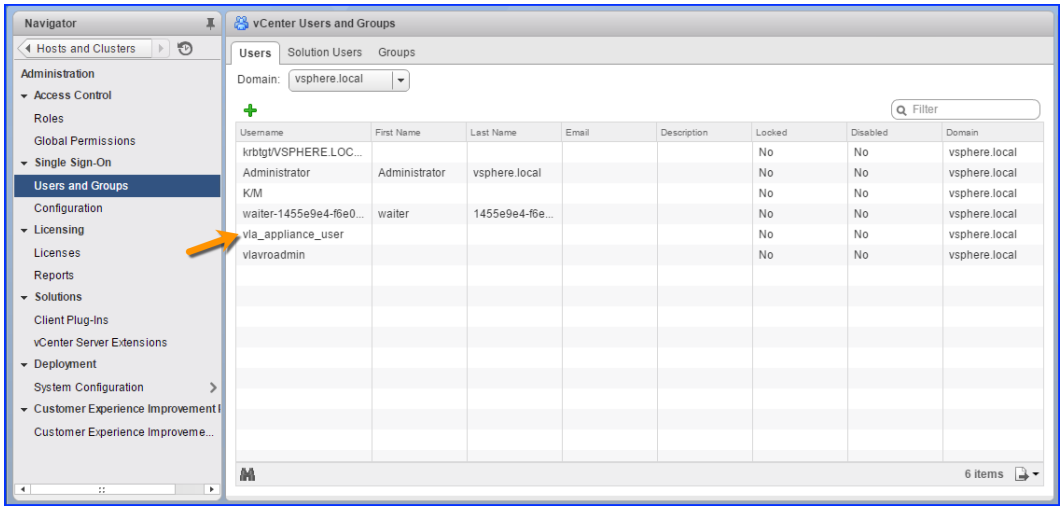
Figure 3-21. VWC - New User



6 Complete the fields in the dialog, giving the user the name **vla_appliance_user** and assigning a conforming password, and then Click **OK**.

The browser closes the dialog and displays the Users and Groups page with your new user added, similar to the following:

Figure 3-22. VWC - vCenter Users and Groups



NOTE The list now includes the **vla_appliance_user** user, selected for emphasis.

You successfully created a new user for the VLA.

Setting Permission For the (Limited Rights) VLA user

Procedure

1 Log into the VMware vSphere Web Client(VWC) with administrator credentials

2 Click **Hosts and Clusters**.

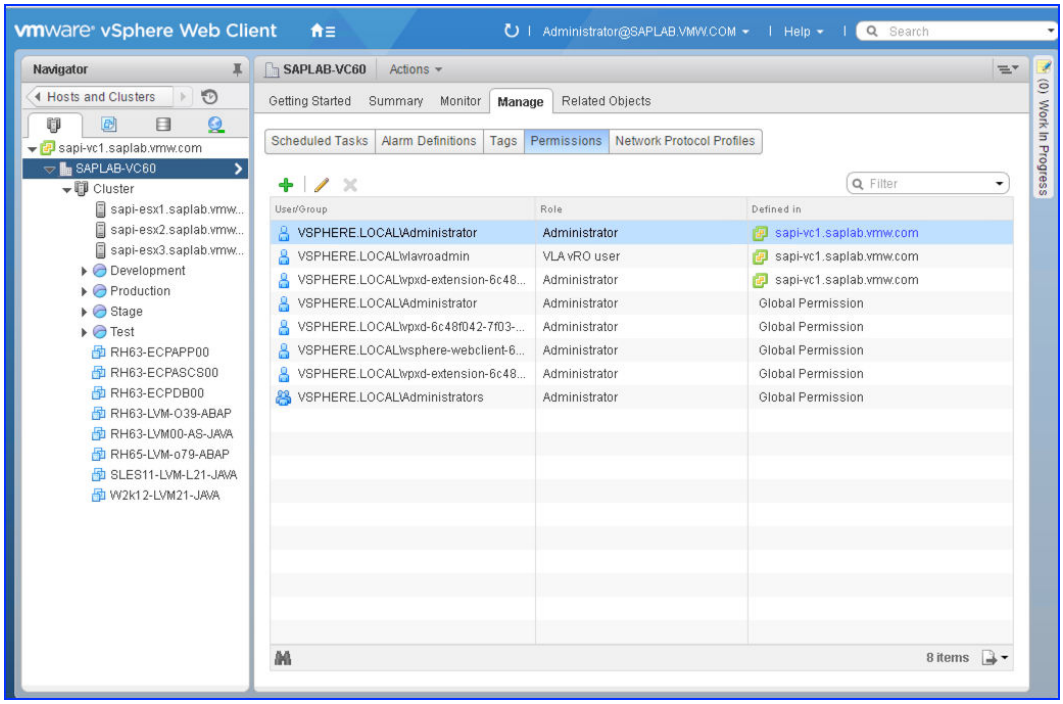
3 Click on the vCenter Server you want the VMware VLA to manage.

4 Click **Manage**

Click **Permissions**.

Your browser displays a page similar to the following:

Figure 3-23. VWC-Hosts and Clusters-Manage-Permissions

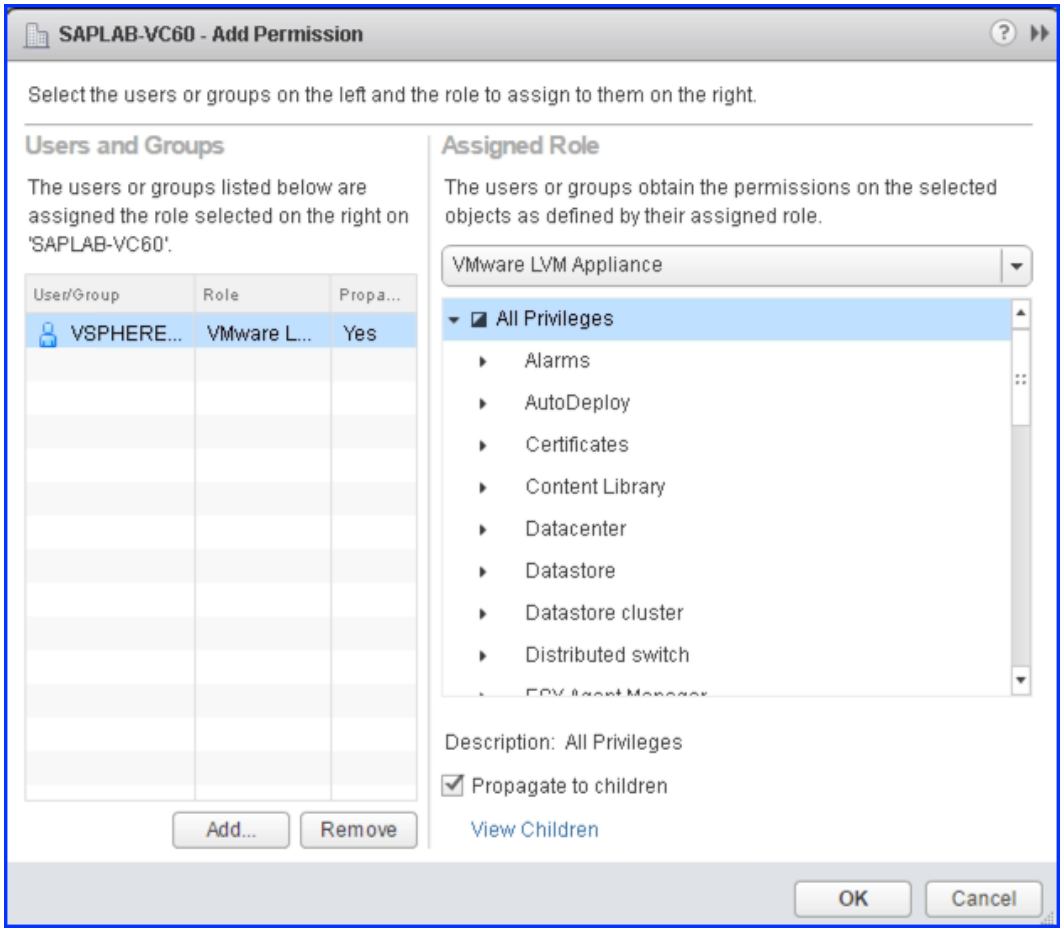


5 Click the **green plus** icon to add permission.

6 Click **Add**….

Your browser displays a page similar to the following:

Figure 3-24. Add Permission



7 Choose your SSO domain, and select the user **vla_appliance_user**.

8 Click **OK**

9 In the **Assigned Role** List box, select **VMware LaMa Appliance**.

10 Make sure the **Propagate to children** check box is checked.

Note if the **Propagate to children** option is not checked for vCenter Server intentionally in order to adjust access rights for the user more accurately, then granting permissions to the following inventory objects should be taken into account:

- vCenter Server (The **Hosts and Clusters** view)
- Datacenters and Folders for Datacenters (The **Hosts and Clusters** view)
- Clusters and ESXi hosts within the Clusters, and Hosts and Clusters Folders (The **Hosts and Clusters** view)
- Resource Pools and vApps (The **Hosts and Clusters** view)
- Virtual Machines, VM Templates and Folders for Virtual Machines (The **VMs and Templates** view)
- Datastores and Folders for Datastores (The **Storages** pane)
- Networks and Distributed Switches (The **Networking** view)

Sttting access permissions per inventory object can be done in the same manner as it's demonstrated for the vCenter Server: the user **vlaadmin** needs assigning to the VMware VLA role for an inventory object on the **Manage - Permissions** tab of this object.

11 Click **OK**.

This saves the permission. A lack of permissions for some of the aforementioned objects may result in absence of the objects in LaMa Virtualization Landscape.

You have successfully set required permissions for the VLA user.

Guest Customization Specification

When you clone a virtual machine, vSphere allows you to customize the guest operating system of the virtual machine, including the hostname, network settings, licensing and more. These customizations allow for license compliance and help prevent conflicts of certain configurations, including IP addresses and host names.

When vSphere performs the clone operation with customizations, it must have a `guest customization specification` that matches key configuration aspects of the virtual machine being cloned, including the guest operating system type and number of virtual network interfaces (vNICs). For example, when cloning a virtual machine with a Windows guest operating system and 2 vNICs, vSphere looks for a guest customization specification for Windows virtual machine with 2 vNICs.

VMware Adapter for SAP Landscape Management requires the use of guest customization specification to perform **copy** and **clone** operations in the *LaMa*, with or without templates.

The next two sub-sections discuss how to use the VMware vSphere Web Client(VWC) to create guest customization specification for Linux and Windows virtual machines, each with a single virtual network interface (vNIC). You must use the applicable procedure to create guest customization specification that match each of the configurations (guest operating system type and number of vNICs) for the virtual machine in which you run your SAP Systems. For example, if you have some SAP system running on Linux virtual machine with one vNIC, another with two vNICs, and a third one with Windows guest operating system and 2 vNICs, you need three separate guest customization specifications matching these configurations.

Create a Customization Specification for Linux

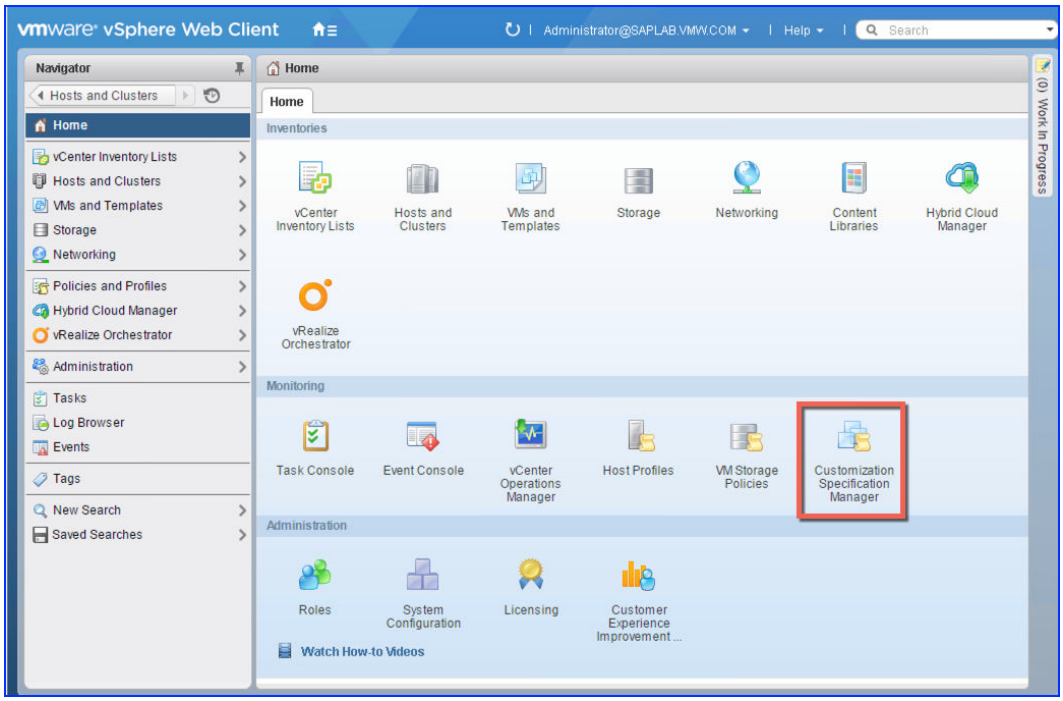
Use the Guest Customization wizard to save guest operating system settings in a specification that you can apply when cloning virtual machines or deploying from templates.

Procedure

1 Log in to the VMware vSphere Web Client(VWC) as someone with administrative privileges.

The browser displays a page similar to the following:

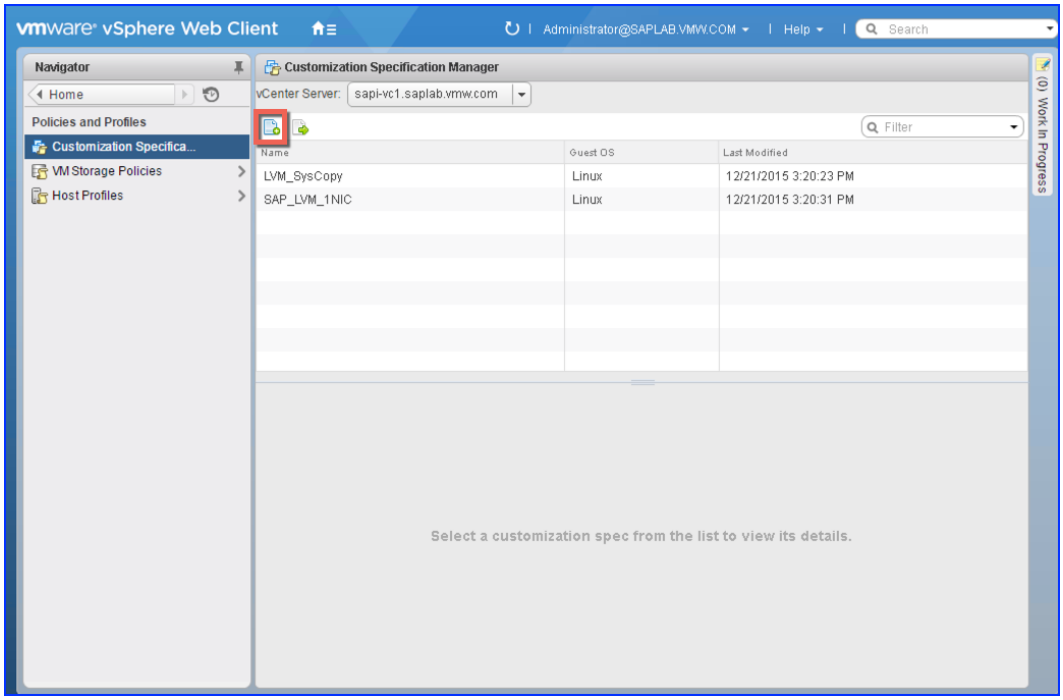
Figure 3-25. VWC-Administration-Customization Specification Manager



2 From the Object Navigator column (right pane), either Click on **Customization Specification Manager** tab under **Monitoring** section (highlighted in the preceding figure for emphasis) OR select **Policies and Profiles** > **Customization Specification Manager** .

The browser displays a page with the Customization Specification Manager, similar to the following:

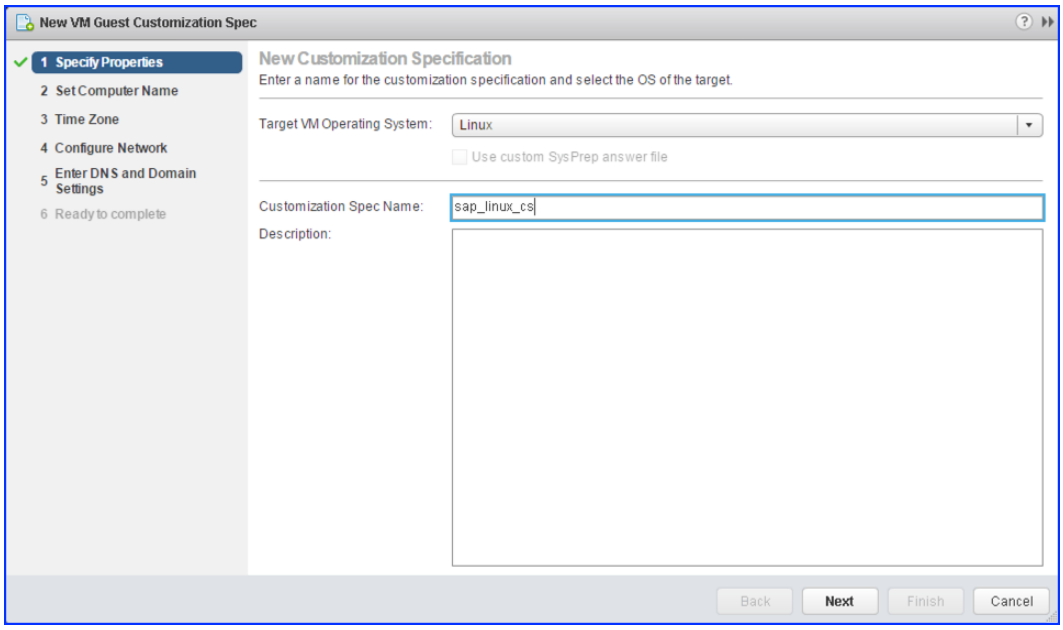
Figure 3-26. VWC-Customization Specification Manager



3 Click the Create a New specification icon (highlighted in the preceding figure for emphasis).

The browser displays the **New VM Guest Customization Spec** Wizard similar to the following:

Figure 3-27. VWC-New VM Guest Customization Spec



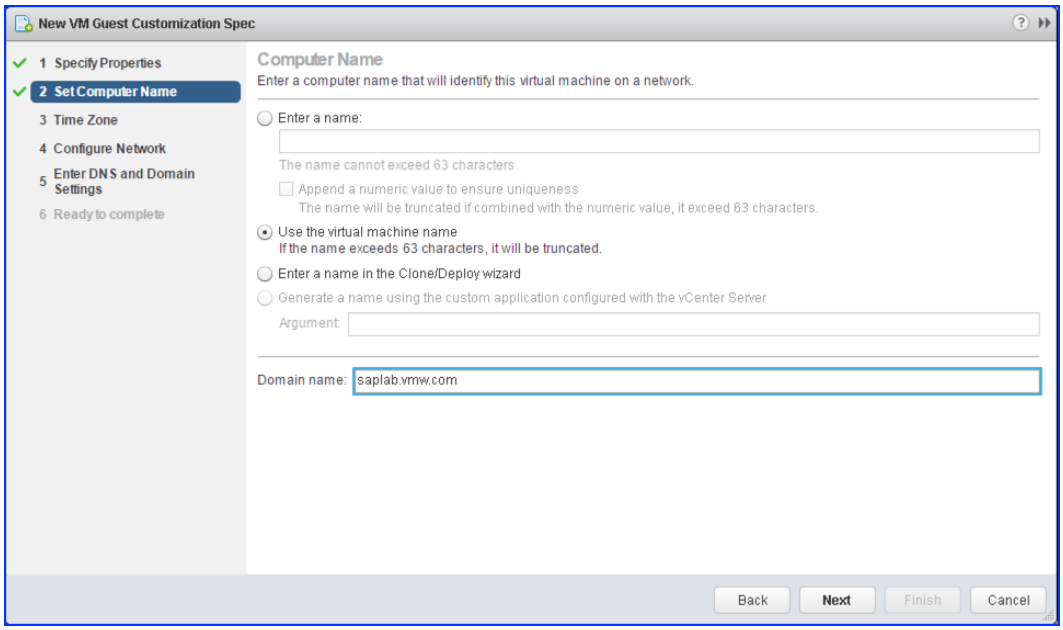
4 Select Linux as the Target virtual machine operating system.

5 Enter a name for the customization specification in the **Customization Spec Name** field. VMware suggests choosing a Customization Spec Name that makes it easy for the LaMa Administrator to identify the contents of the customization specification. The **Description** field should contain a brief description of the customization specification.

6 Click **Next**.

The browser displays the **Set Computer Name** dialog of the wizard similar to the following:

Figure 3-28. VWC-New VM Guest Customization Spec-Set Computer Name



7 Select **Use the virtual machine name** radio button.

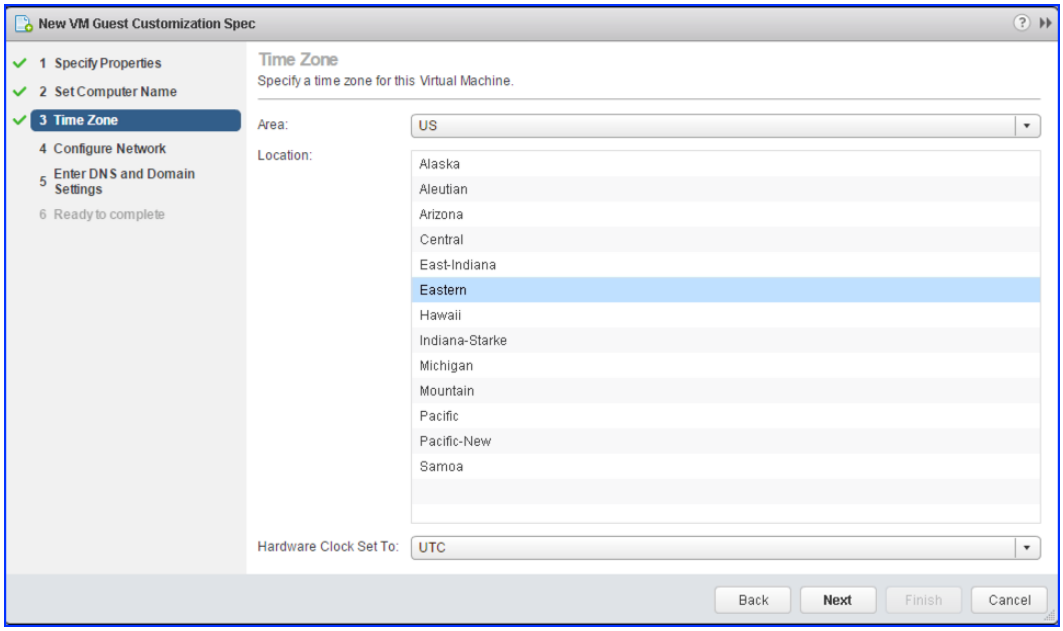
8 Enter the DNS domain to which the virtual machine belongs to in the **Domain Name** field, and then Click **Next**.

The browser displays the **Time Zone** dialog of the wizard.

9 Here you select the **Area** and **Location** of the virtual machine so that it has the proper time zone.

10 Specify the time zone to which you want to **Set the Hardware Clock**, and Click **Next**.

Figure 3-29. VWC-New VM Guest Customization Spec-Time Zone & Location



The browser now displays the **Configure Network** dialog of the wizard:

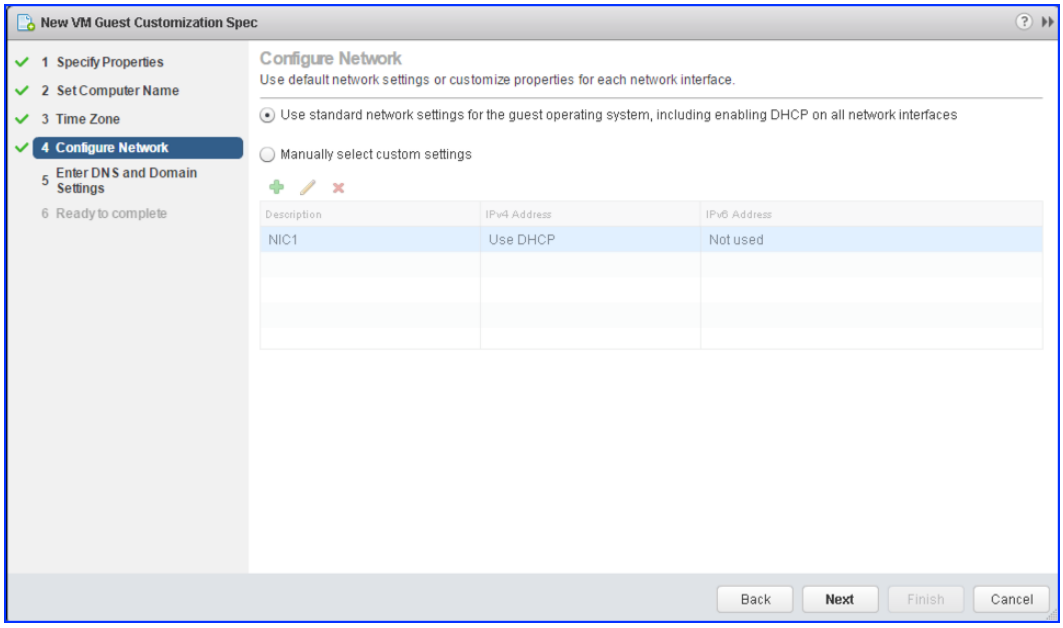
11 The **Configure Network** section of the wizard allows you to configure every network interface of the customization specification.

In this dialog, you can:

- Add a network interface by Clicking the plus icon
- Edit an existing defined network interface, including IP parameters, by:
  - Selecting the interface to edit
  - Clicking the pencil (edit) icon
- Delete network interfaces by:
  - Selecting the interface to delete
  - Clicking the X icon

As shown, by default, a new virtual machine Guest Customization Spec defines one network interface, called **NIC1**, that use DHCP to get IP parameters. VMware recommends creating Guest Customization Specs for each of the permutations of number of NICs and the IP configuration (DHCP, Static IP, and Prompt for IP) that may be needed for your production / test / development environments.

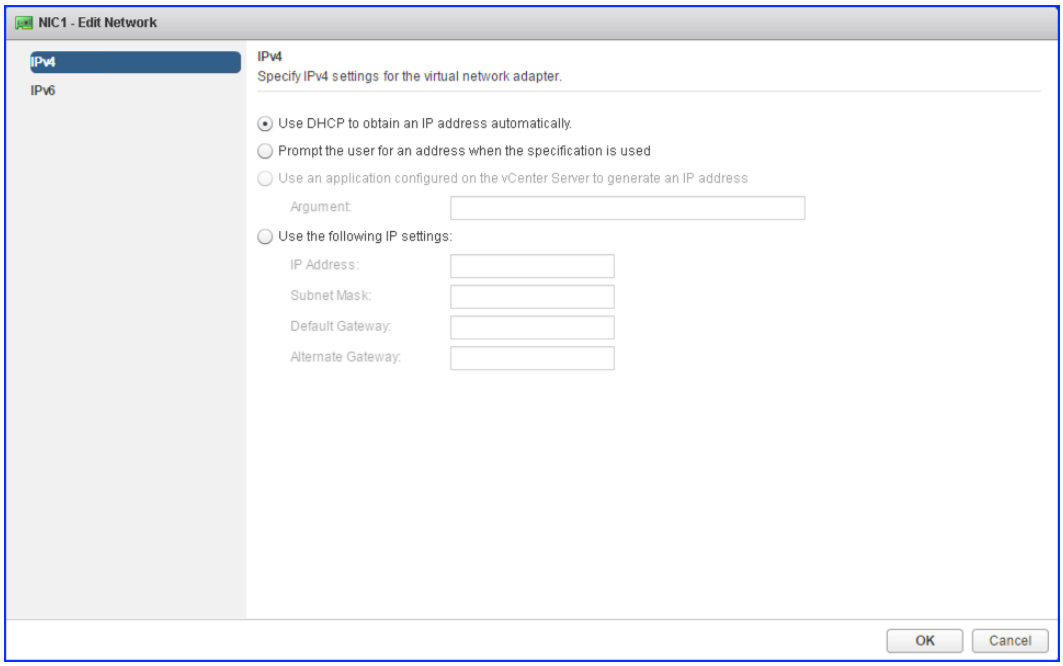
Figure 3-30. VWC-New VM Guest Customization Spec-Configure Network



12 If you want to modify a network interface's configuration, do the following :

- Select **Manually select custom settings** radio button.
- Select the network interface to edit.
- Click the **Edit**(pencil) icon. The Wizard browser displays the Edit Network page, similar to the following:

Figure 3-31. Edit Network



- Choose the method vCenter Server uses to assign the IP address to this network interface (one of the following):

  1 **Use DHCP to obtain an IP address**

2 **Prompt the user for an address when the specification is used**

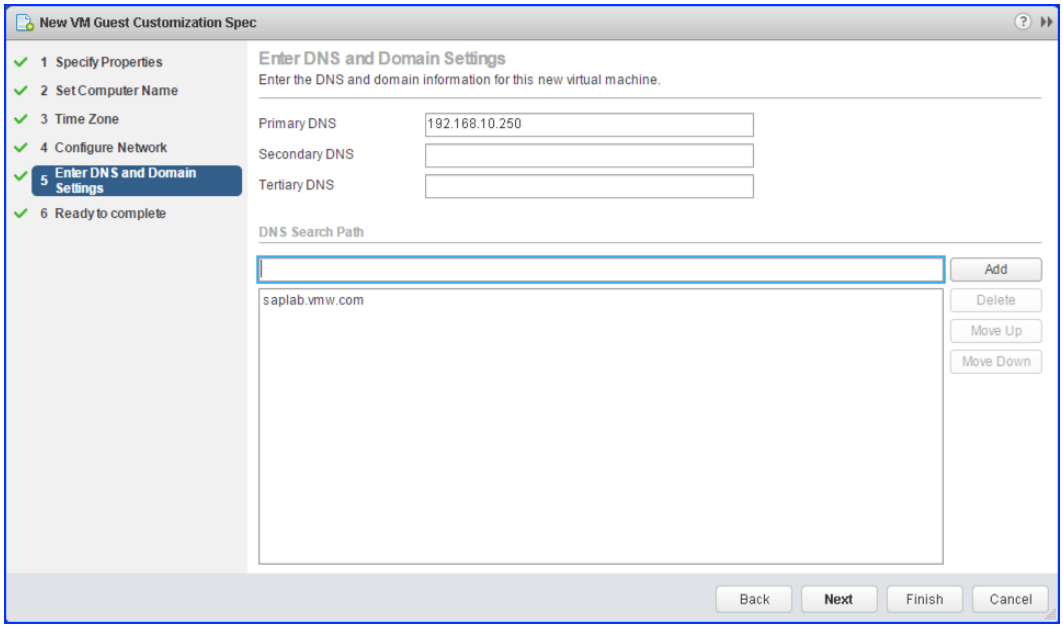
3 **Use the following IP Settings** - Static IP settings. Enter appropriate values.

- Click **OK**. The browser returns to the New VM Custom Spec wizard, on the **Configure Network** dialog shown previously in this procedure.

13 Add as many network interfaces as you need for this customization specification, using the Step 11 to configure each of the network interfaces, and then Click **Next**.

The browser now displays the **Enter DNS and Domain Settings** dialog of the wizard, similar to the following:

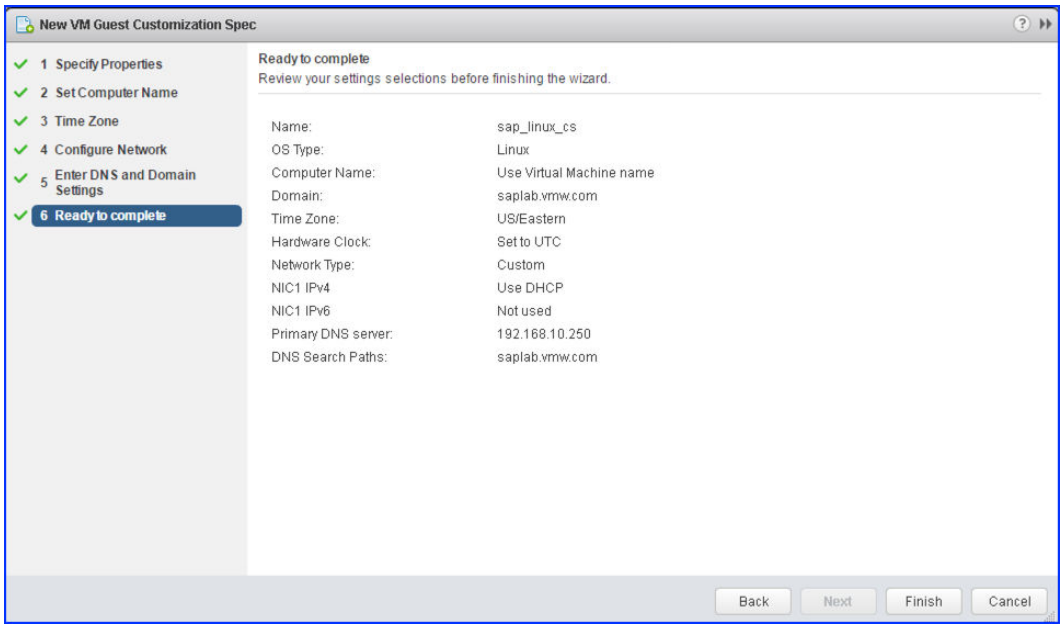
Figure 3-32. VWC-New VM Guest Customization Spec-DNS



14 Enter the DNS servers that the virtual machine uses in the **Enter DNS and Domain Settings** section of the wizard. You can also manage the DNS search path. To add a domain, type the domain name in the field under DNS Search Path and Click **Add**. Then Click **Next**.

The browser displays the **Ready to complete** dialog of the wizard, similar to the following:

Figure 3-33. Ready to complete



15 Click **Finish** to create the customization specification.

The new customization specification that you created is now listed in the Customization Specification Manager list.

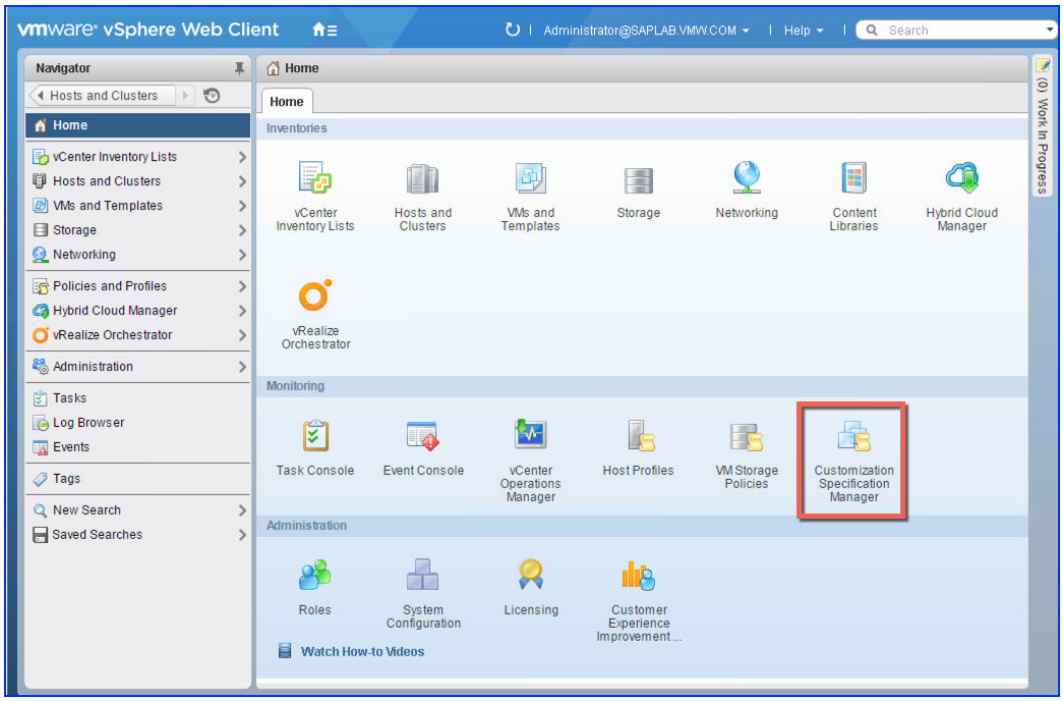
You can now use this customization specification to perform a clone or copy operations of a virtual machine.

Create a Customization Specification for Windows in the vSphere Web Client

Procedure

1 From the VMware vSphere Web Client(VWC) Home inventory page, select **Rules and Profiles** > **Customization Specification Manager** OR **Click** on **Customization Specification Manager** tab under **Monitoring** section as seen in the following screenshot:

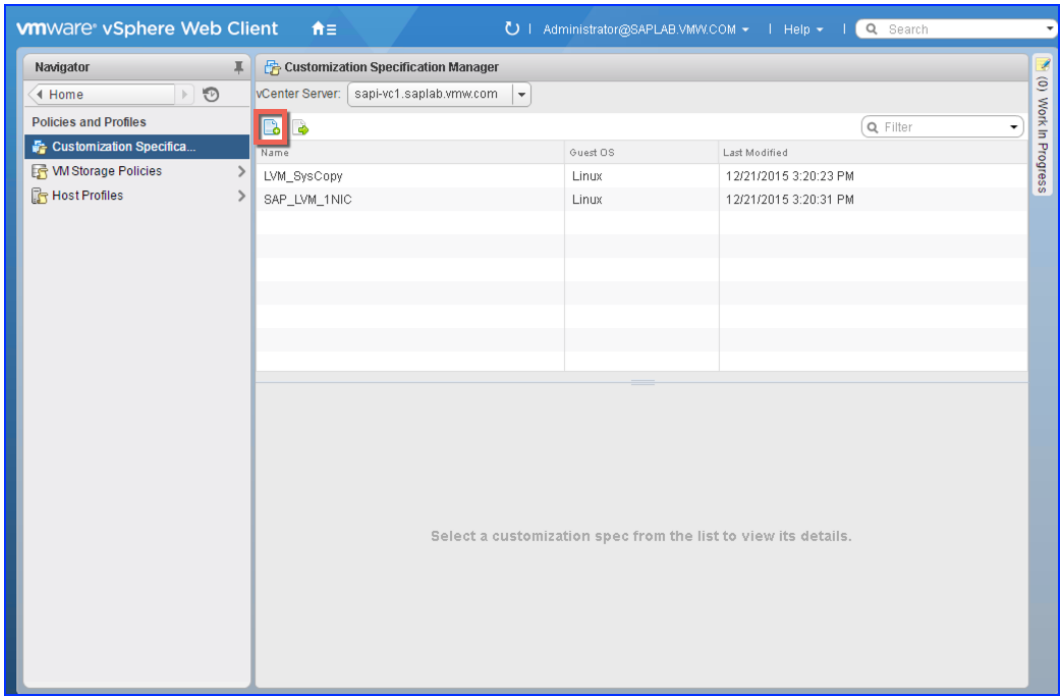
Figure 3-34. VWC-Customization Specification Manager



2 Click the Create a New specification icon highlighted in the following screenshot.

This opens up the New VM **Guest Customization Specification** wizard.

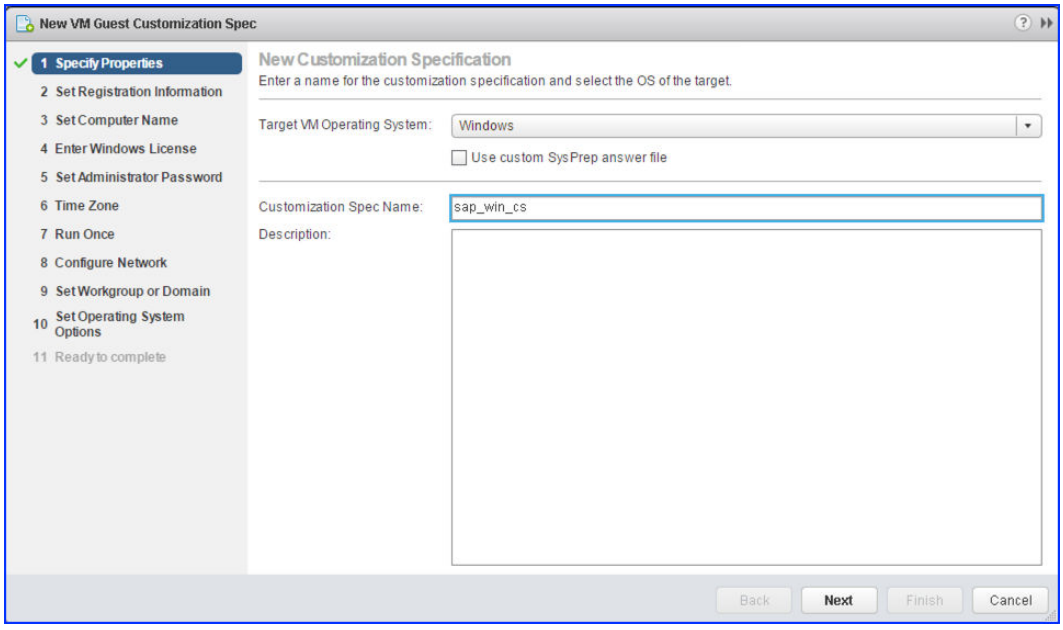
Figure 3-35. VWC-Guest Customization Spec Wizard



3 Select Windows as the **Target VM Operating System**. Enter a name for the customization specification in the **Customization Spec Name** field. We suggest you provide a **Customization Spec Name** that makes it easy for the LaMa Administrator to identify the contents of the customization specification. The **Description** field should contain a brief description of the Customization Specification. Click **Next**.

Your browser window looks similar to the following:

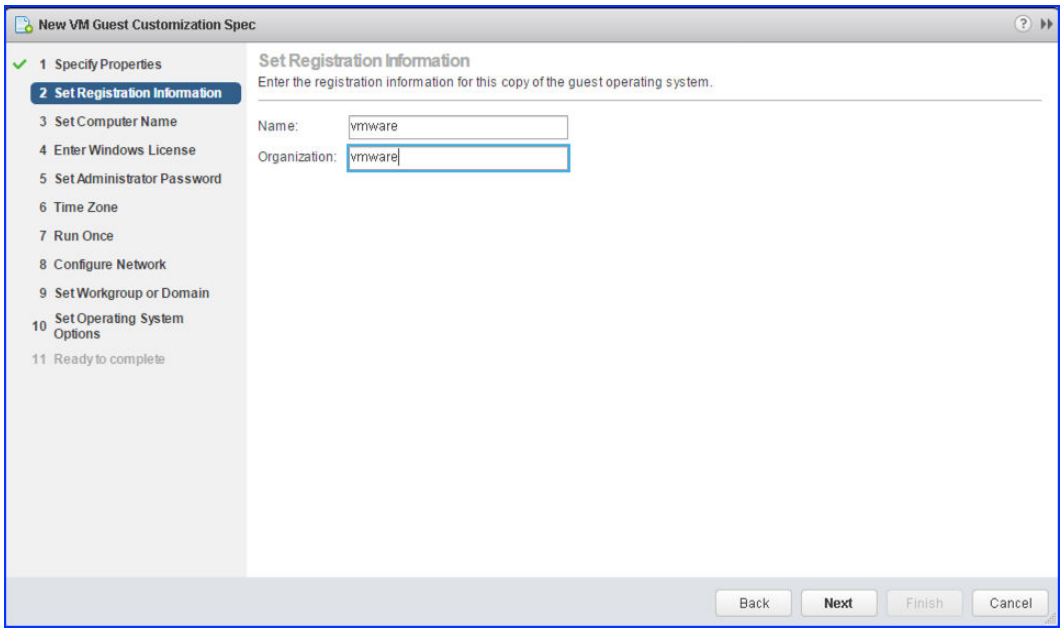
Figure 3-36. VWC-New Customization Specification



4 Type the virtual machine owner's **name** and organization in the **Set Registration Information** section of the wizard. Then Click **Next**.

Your browser window looks similar to the following:

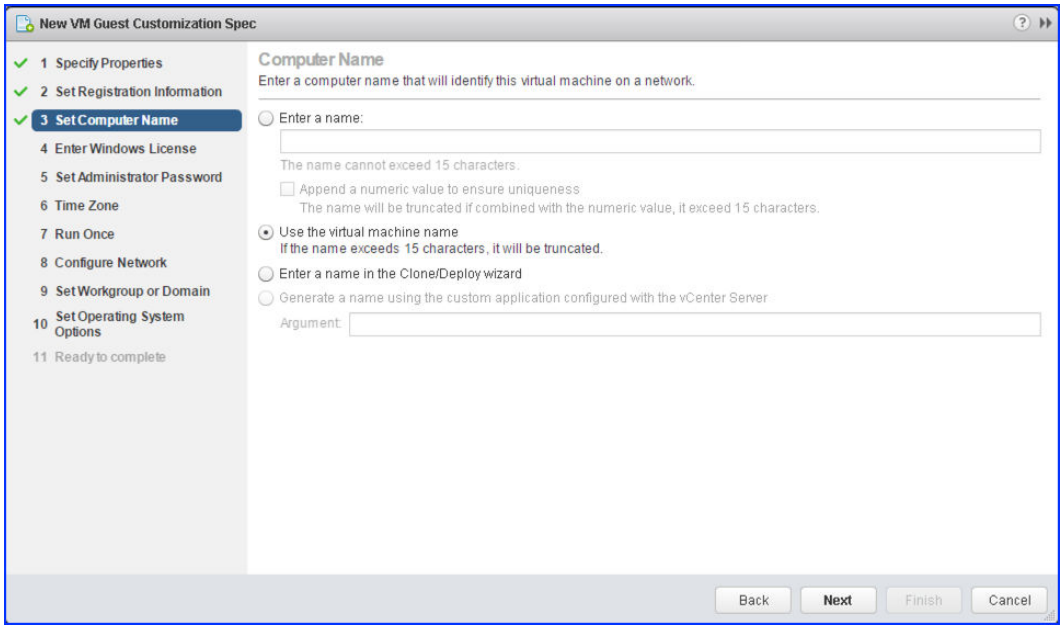
Figure 3-37. VWC-Set Registration Information



5 In the **Set Computer Name** section of the wizard, Choose **Use the virtual machine name**, enter the **Domain Name** for the virtual machine and Click **Next**.

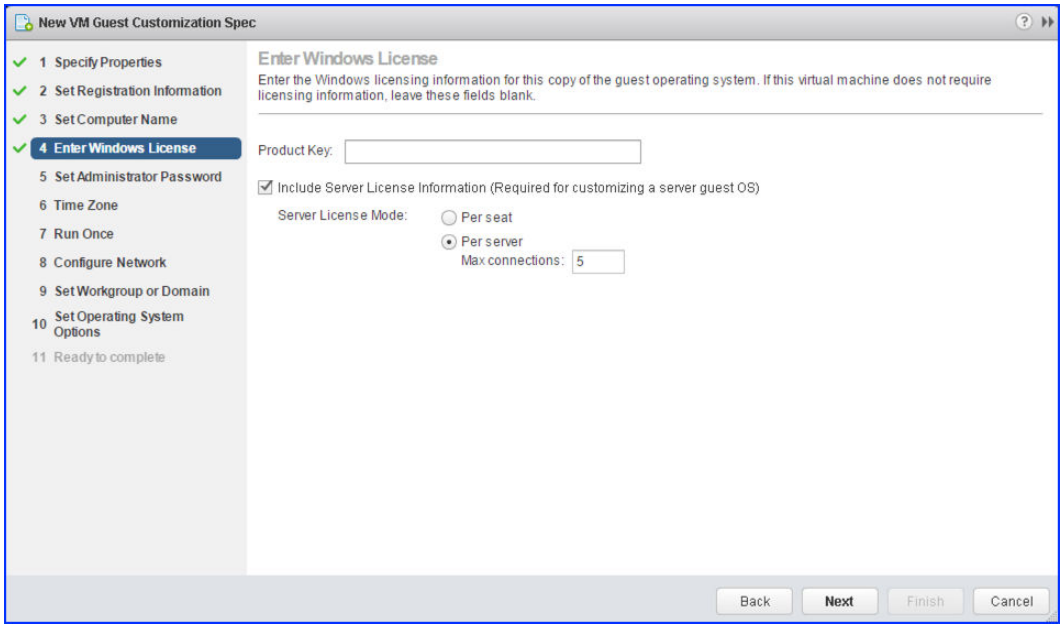
Your browser window looks similar to the following:

Figure 3-38. VWC-New VM Guest Customization Spec-Computer Name



6 Provide licensing information for the Windows Operating System and Click **Next**.

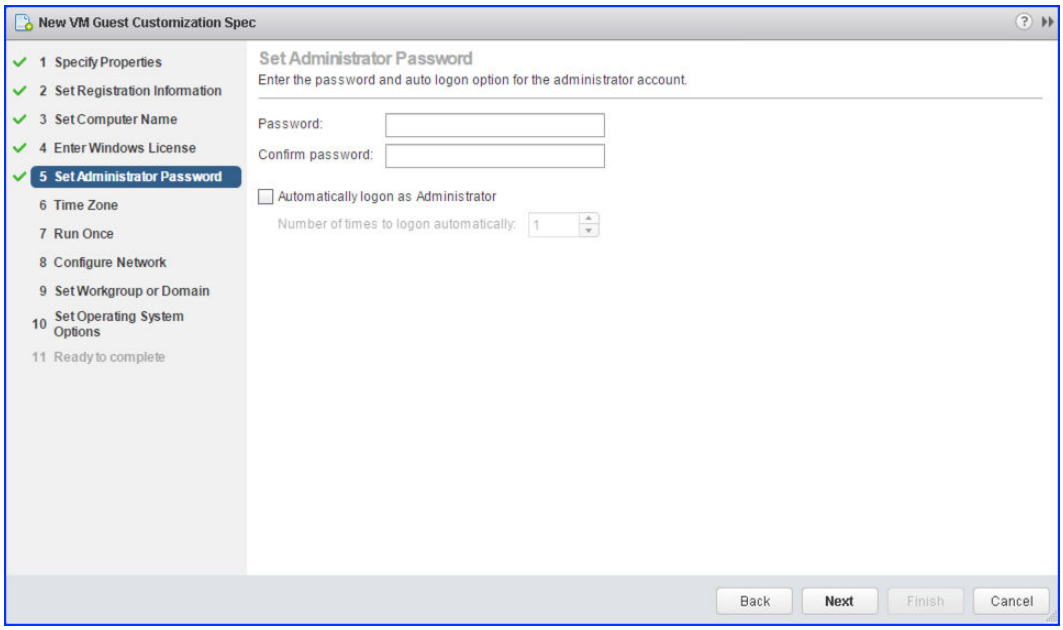
Figure 3-39. VWC-New VM Guest Customization Spec-Enter Windows License



7 Configure the administrator password for the virtual machine. You confirm the password and then Click **Next**.

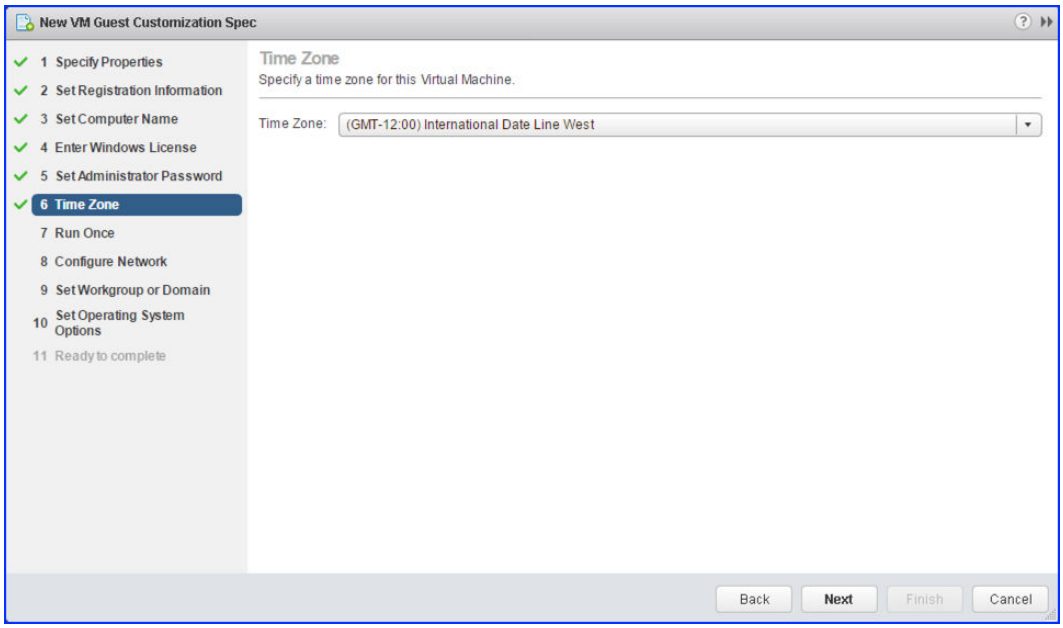
Your browser window looks similar to the following:

Figure 3-40. VWC-New VM Guest Customization Spec-Set Administrator Password



8 Select the time zone for the virtual machine and Click **Next**.

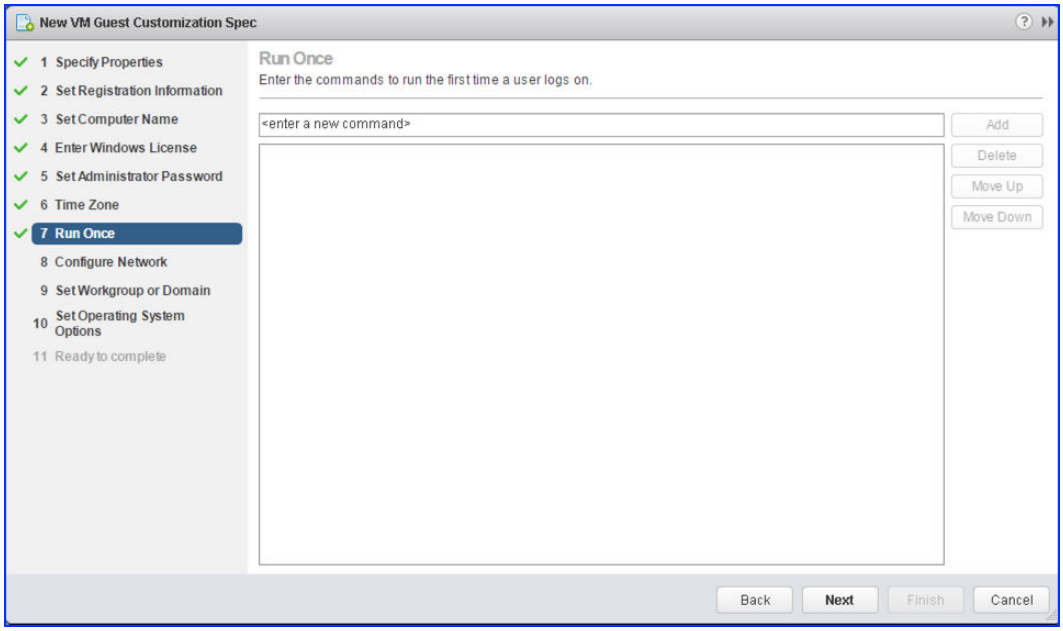
Figure 3-41. VWC-New VM Guest Customization Spec-Time Zone



9 (Optional) On the Run Once page, specify commands to run the first time a user logs into the guest operating system and Click **Next**. See the Microsoft Sysprep documentation for information about `RunOnce` commands

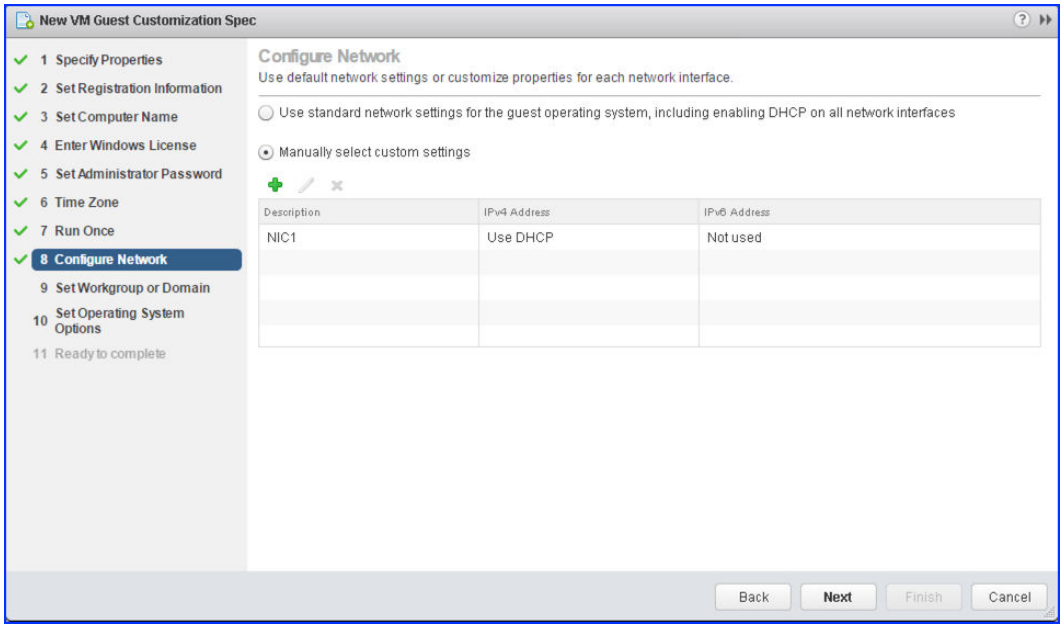
Your browser window looks similar to the following:

Figure 3-42. VWC-New VM Guest Customization Spec-Run Once



10 In the Configure Network section of the wizard, select **Manually select custom settings**. This section allows you to configure every network interface of the Customization Specification. You can add a network interface by Clicking the **plus** icon. If you want to change the IP settings of any network interface, Click the **edit** button (the pencil icon). By default, there is one network interface defined called NIC1. It is configured to use DHCP.

Figure 3-43. VWC-New VM Guest Customization Spec-Configure Network



11 When you Click the **edit** button the **Edit Network** dialog is displayed. If you want to configure the network interface to use DHCP select **Use DHCP to obtain an ip address** and Click **OK**. If you want the network interface to use a static ip address, select **Prompt the user for an address when the specification is used**. Enter the netmask and gateway address and then Click **OK**.

Your browser window looks similar to the following:

Figure 3-44. VWC-New VM Guest Customization Spec-IPv4

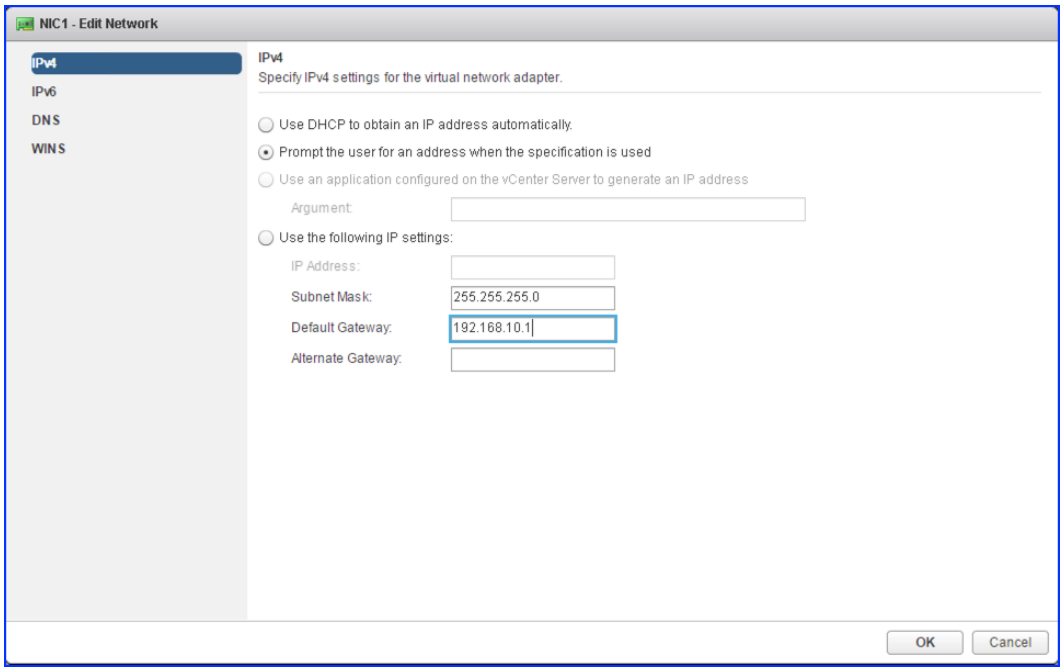
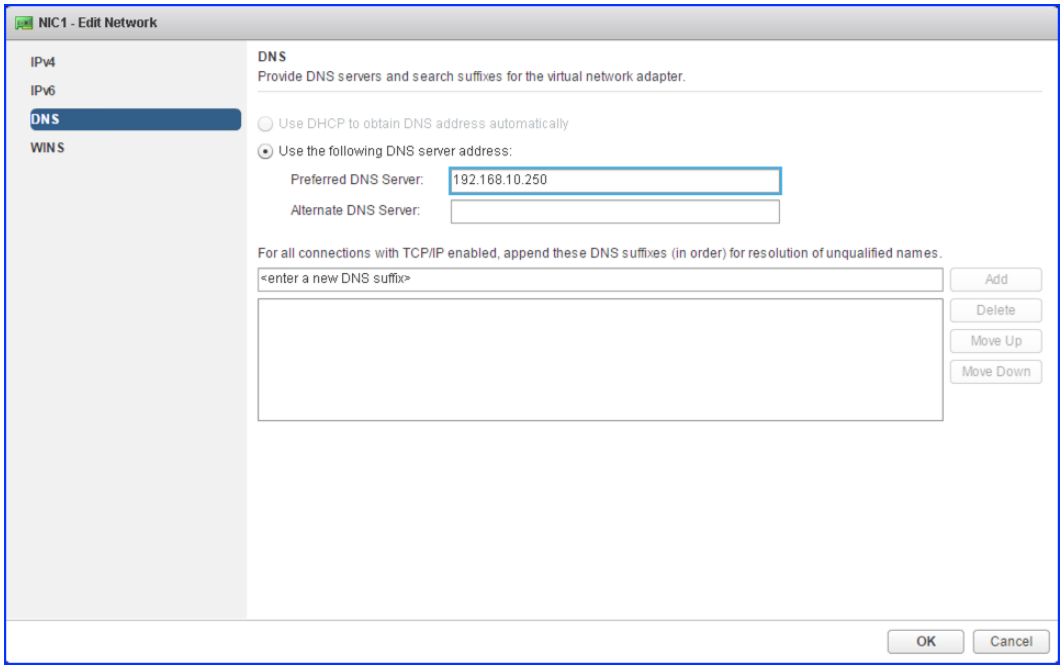
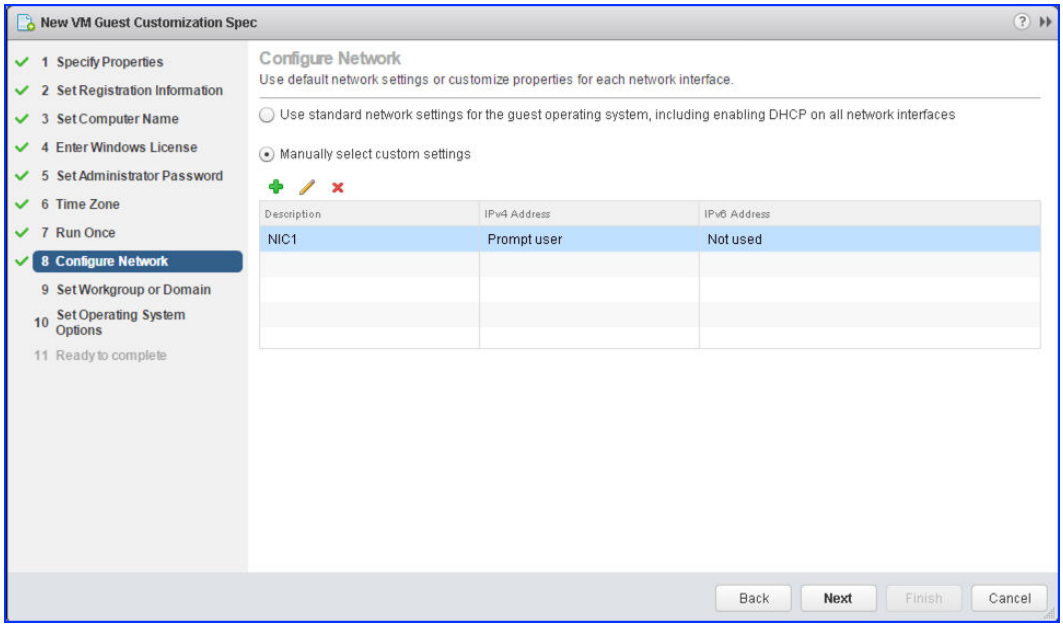


Figure 3-45. VWC-New VM Guest Customization Spec-DNS



12 Add and configure as many networks interfaces as needed for your Customization Specification. When all of your network interfaces are added and configured, Click **Next**.

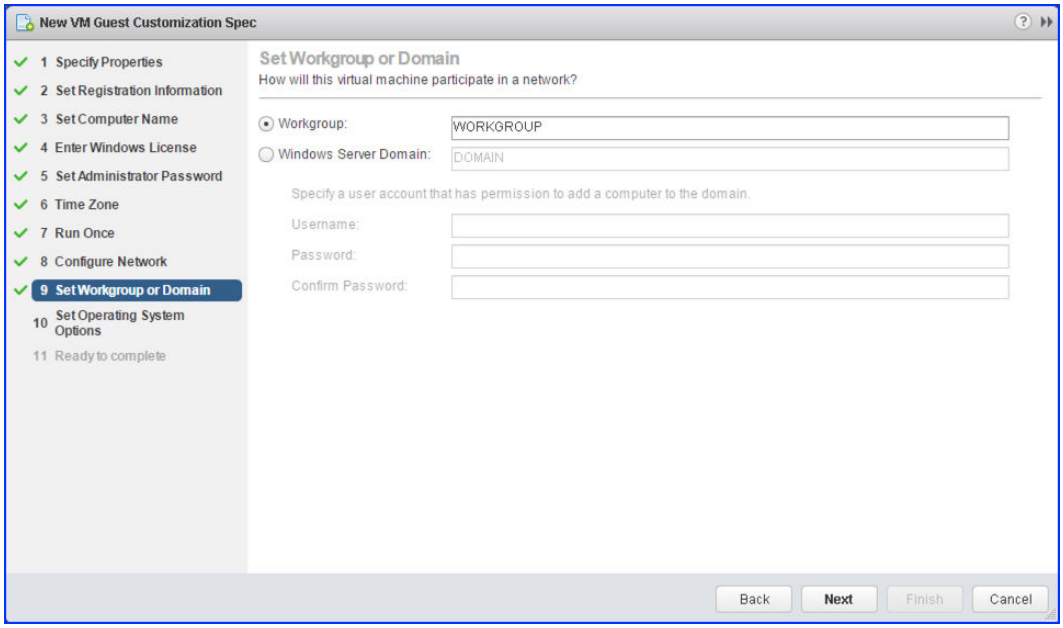
Figure 3-46. VWC-New VM Guest Customization Spec-Add/Configure Additional network Interfaces



13 You now enter the Workgroup or Domain for the virtual machine.

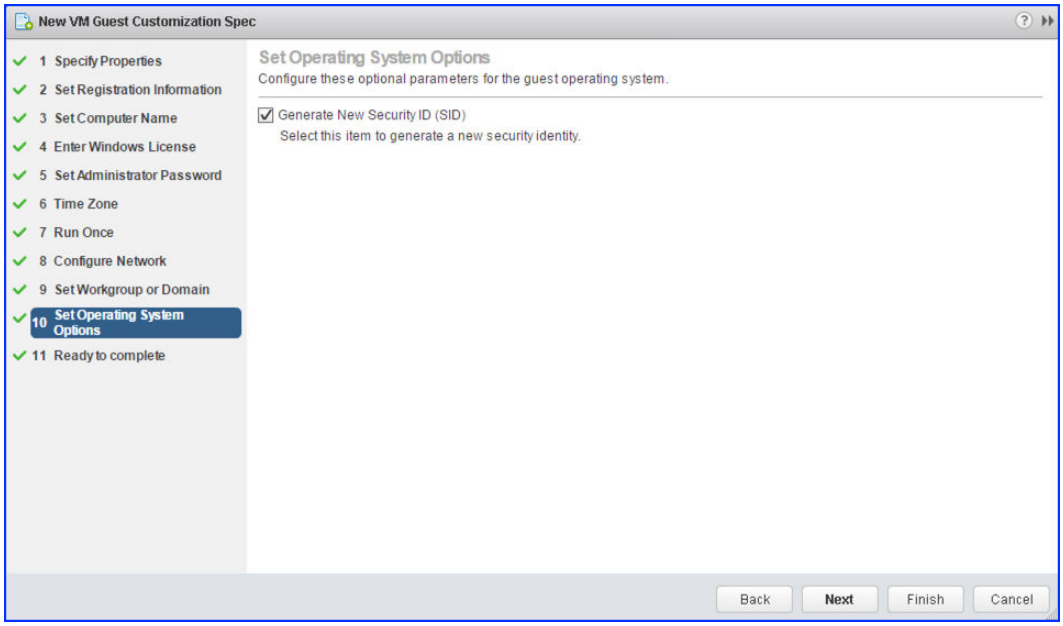
Your browser window looks similar to the following:

Figure 3-47. VWC-New VM Guest Customization Spec-Set Workgroup or Domain



14 In the **Set Operating System Options** section you can choose whether you want to create a new Security ID for the VM. A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template from which it was cloned or deployed. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

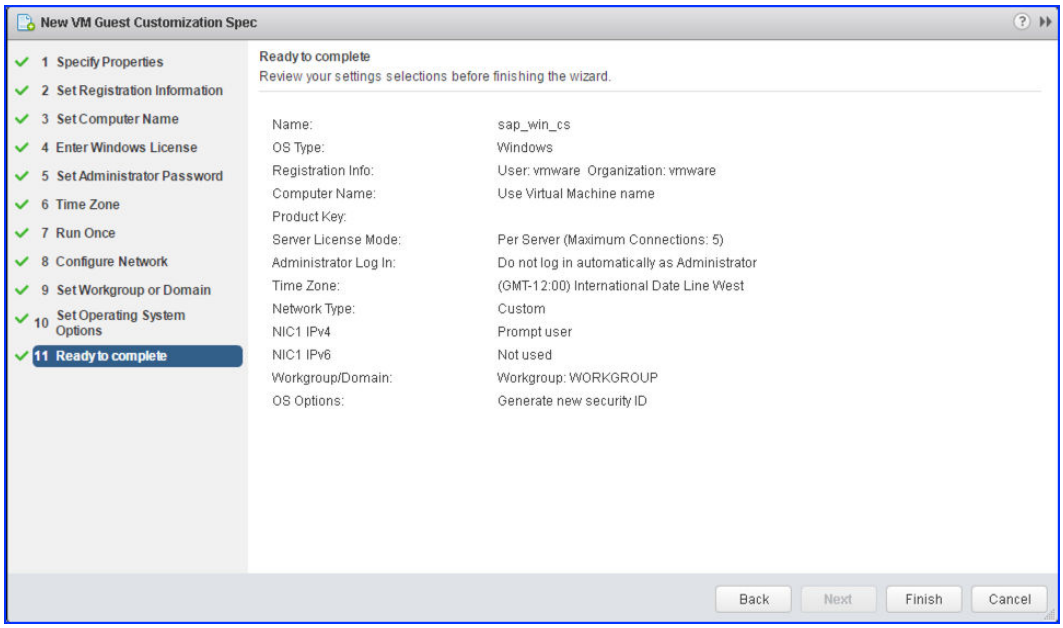
Figure 3-48. VWC-New VM Guest Customization Spec-Set OS Options



15 Click **Finish** to create the customization specification.

It is now listed in the Customization Specification Manager.

Figure 3-49. VWC-New VM Guest Customization Spec-Ready to Complete



You can now use this customization specification to customize virtual machine guest operating systems.

Source SAP system virtual machines configuration notes

MAC Address

In order to successfully complete any copy / clone operation for a SAP system hosted on virtual machines, a virtual infrastructure administrator should make sure that all virtual machines of the SAP system in vSphere are configured to use an automatic MAC address configuration. This option affects a target VM because it might become unavailable via a network if the network has multiple VMs with the same MAC address. To avoid this situation the target SAP system VMs should obtain a new MAC address and it can be provided by setting the source VM MAC Address settings to "Automatic".

These settings can be changed using a native vCenter client or a web-interface.

Deploy and Configure VMware VLA

The VMWare VLA is the central application for the VMware Adapter for SAP Landscape Management. The VLA contains:

- VMware LaMa Application
- VMware Adapter for SAP Landscape Management
- VMware vRealize Orchestrator workflows that you install on the VMware vRealize Orchestrator

The appliance is lightweight and easy to deploy and configure. Follow the detailed steps below to install the VLA, adapter and VMware vRealize Orchestrator workflows.

Downloading the VLA OVA file for VLA deployment

You download the OVA file for VLA deployment ("Deploy VLA," on page 59) as described in this section.

Prerequisites

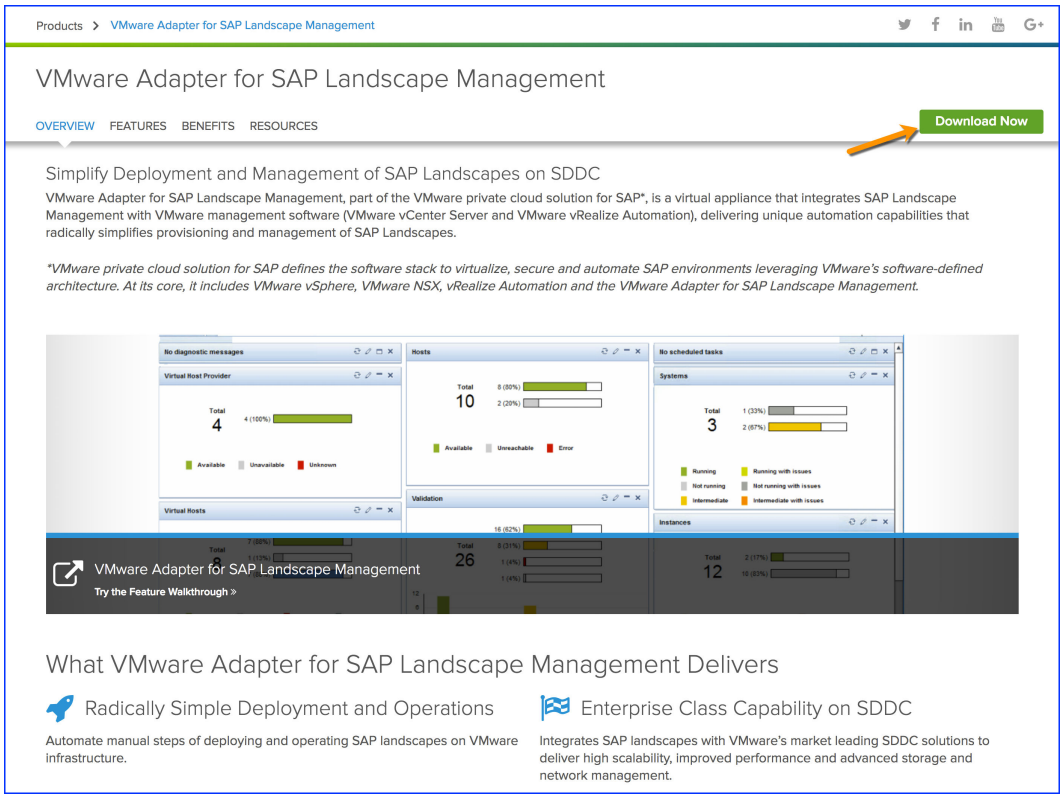
In order to download the VLA OVA file, you need an account at `my.vmware.com`, which is free.

Procedure

1 Browse to http://www.vmware.com/products/adapter-sap-lvm.html

The browser displays the a page similar to the following:

Figure 3-50. VMware Adapter for SAP Landscape Management Home



2 Click **Download Now** (pointed to in the preceding figure).

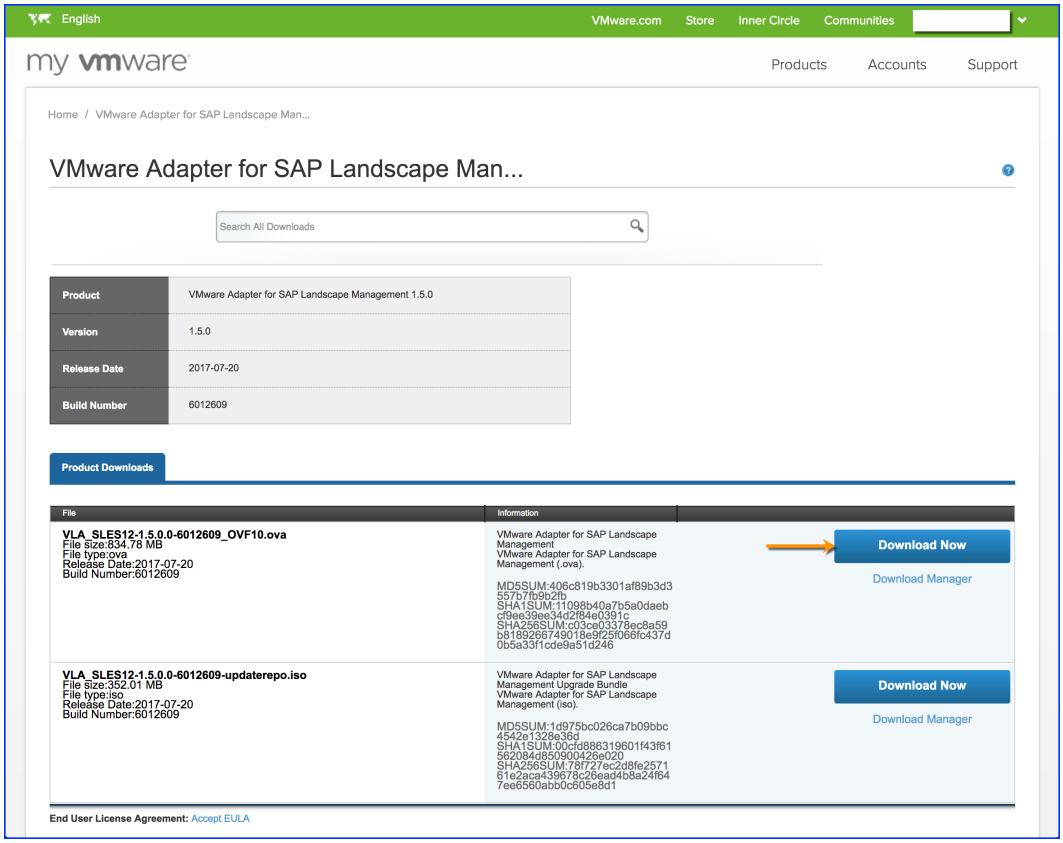
The **Download Now** tab redirects the browser to the login page at `my.vmware.com`, causing the browser to display a page similar to following:

Figure 3-51. my vmware login

3 Enter your login credentials and Click **Log In** (pointed to in the preceding figure for emphasis)

The browser displays the product download page similar to the following:

Figure 3-52. VLA OVA Download



4 Click **Download Now** (pointed to in the preceding figure for emphasis), to download the VLA OVA file.

You have downloaded the VLA OVA file for VLA deployment (Refer "Deploy VLA," on page 59)

Deploy VLA

VMware ships the VMware VLA as an OVA File, which you use to create, deploy the VLA Appliance, as follows:

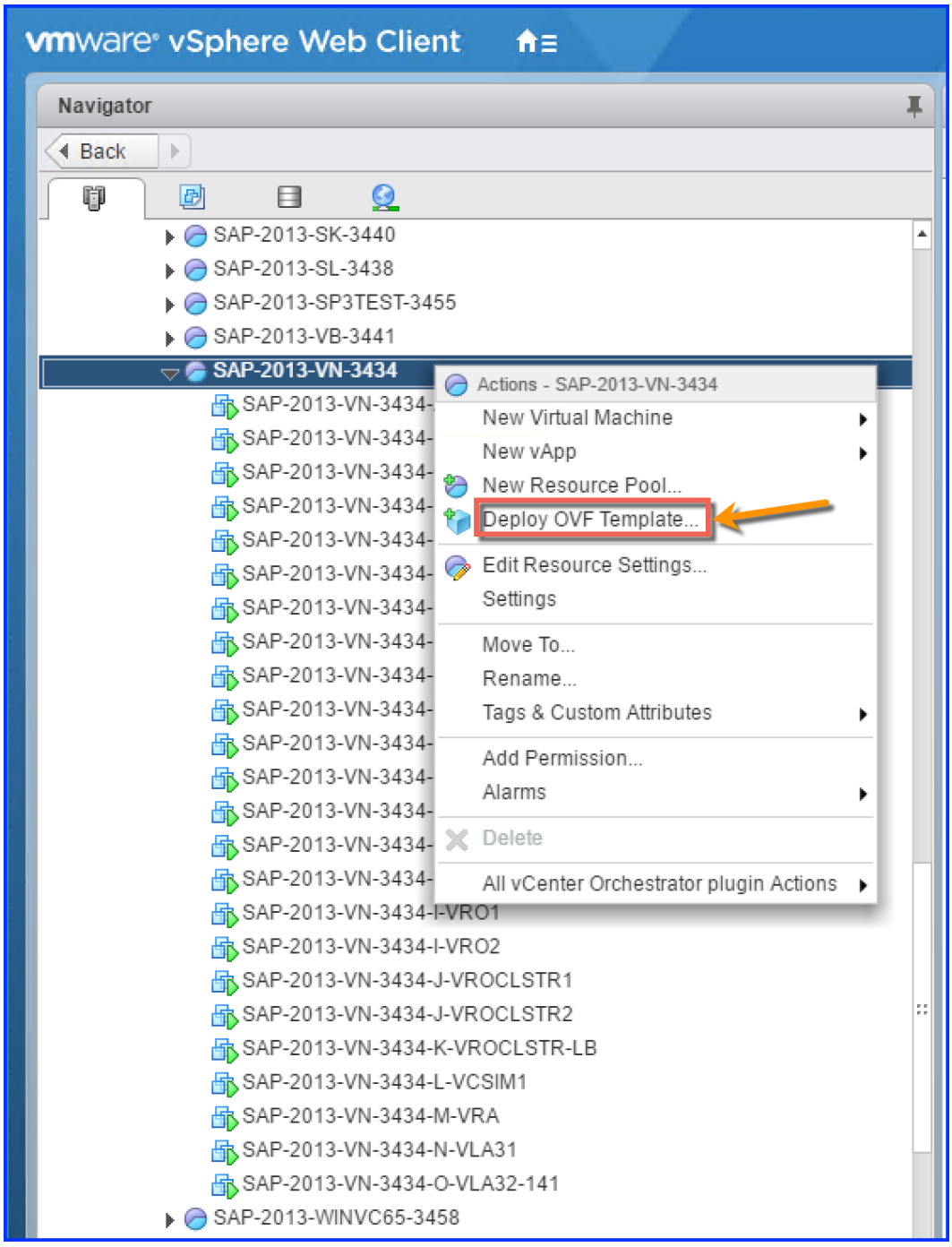
Procedure

1 Have the VLA OVA file downloaded to your workstation or staged for delivery via a web server on your network.

2 Login to the VMware vSphere Web Client (VWC) as a user with rights to deploy a virtual machine.

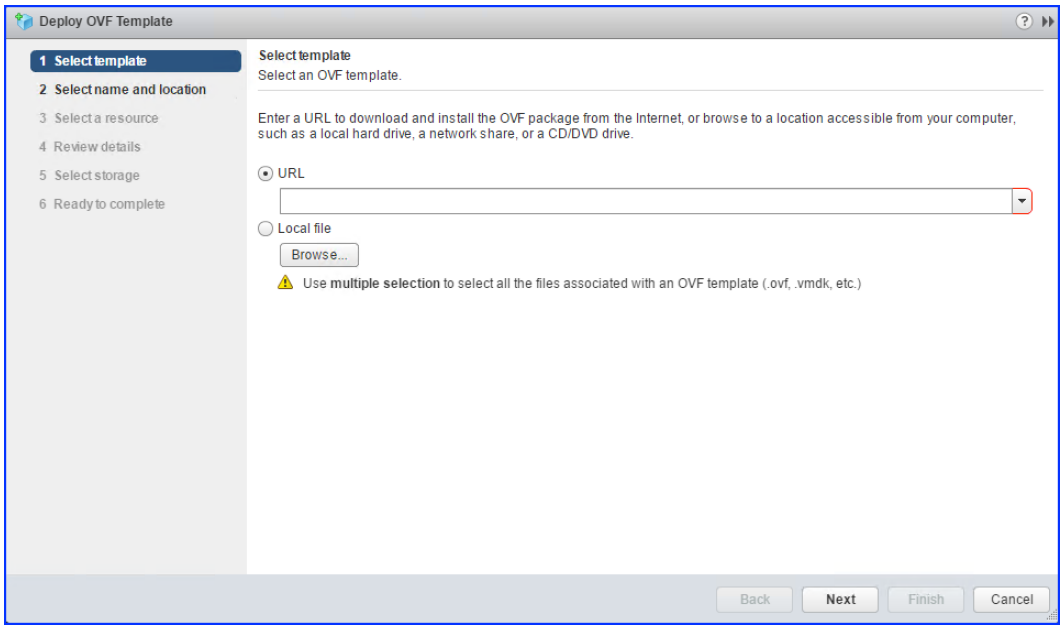
3 Right Click on the organization object such as a **data center**, **host**, **cluster**, or **resource pool** to which you wish to deploy the VLA, and then Click **Deploy OVF Template** from the resulting fly-out menu as depicted in the following figure:

Figure 3-53. VWC-Deploy OVF Template



The browser displays the **Deploy OVF Template** wizard similar to the following:

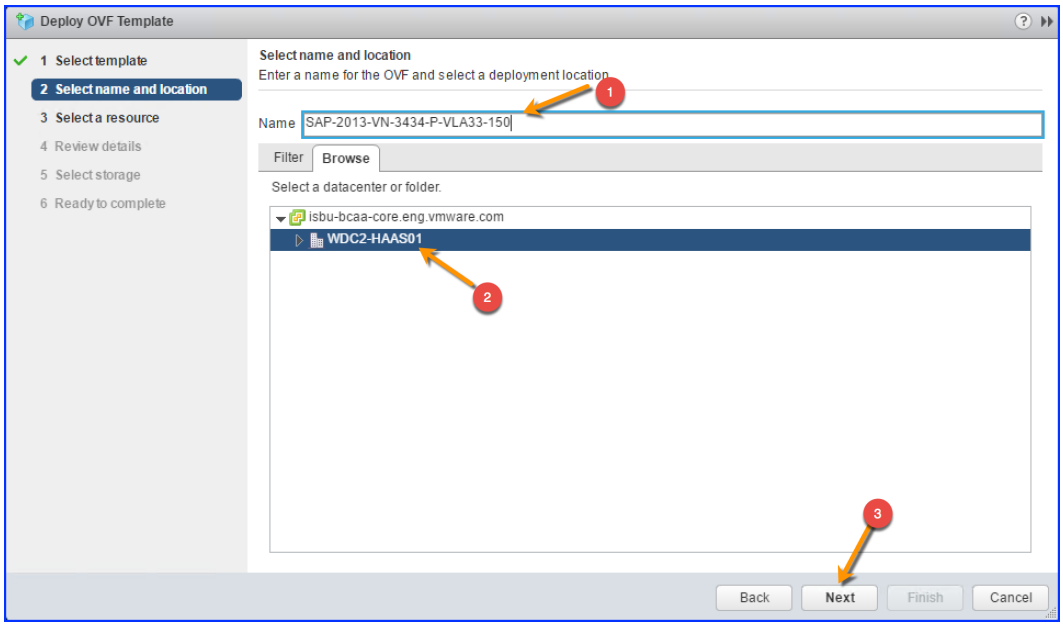
Figure 3-54. Deploy OVF template-Select source



4 In the first step **Select template**, you either select the radio button **URL** where you have staged the VLA OVA file, if you wish to deploy VLA via a web server on your network. Else, if you wish to deploy VLA with a previously downloaded VLA OVF file, select the radio botton **Local file**. Click on **Browse** button and locate the specific VLA OVF file that you will use to deploy the VLA. Then Click **Next**.

The wizard displays the **Select name and location** page similar to the following:

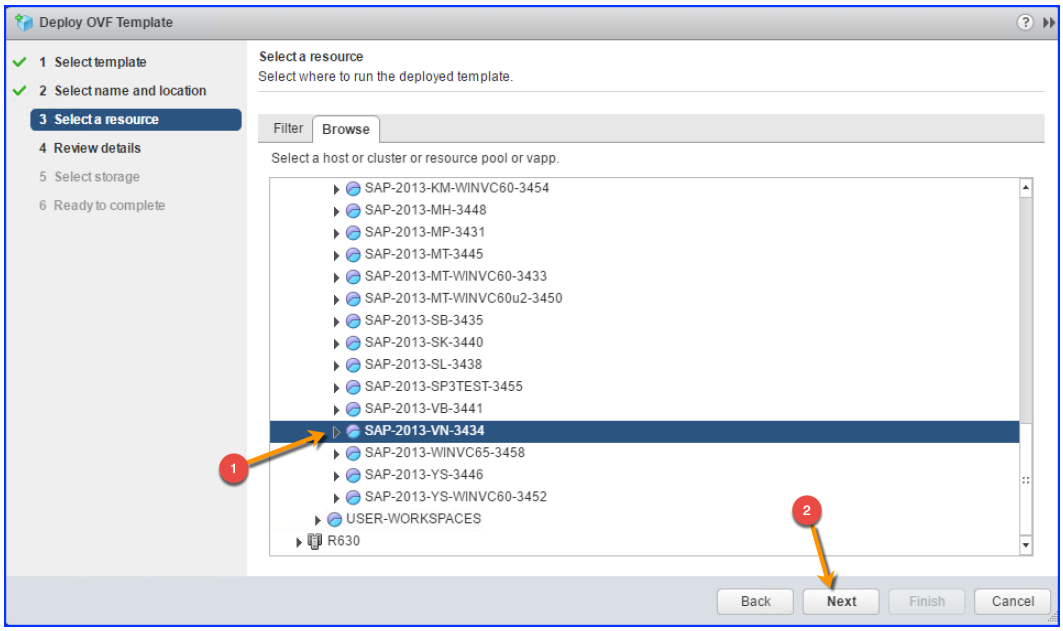
Figure 3-55. Select name and location



5 Enter a name for the VLA Appliance that allows you to easily identify it. Also, select a datacenter or folder where you wish to deploy the VLA. Then, Click **Next**.

The wizard displays **Select a resource** page similar to the following:

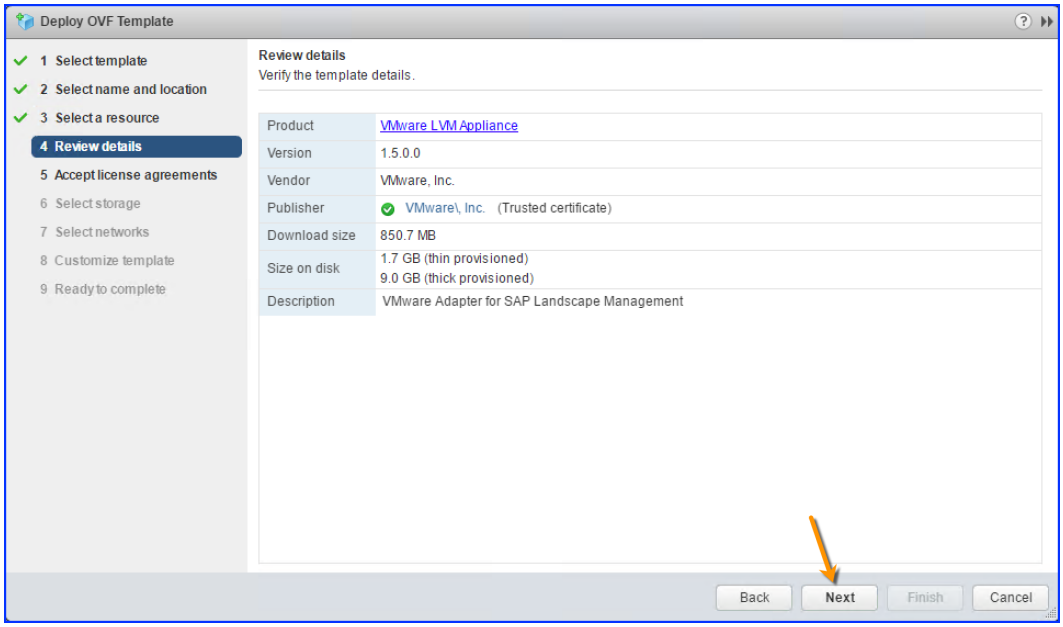
Figure 3-56. Select a resource



6 Select a host or cluster or resource pool or vapp (as appropriate), where you will be running your VLA virtual machine. Then, Click **Next**.

The wizard displays the **Review details** page similar to the following:

Figure 3-57. Review details



7 Verify the information displayed on the **Review details** page of the wizard. Click on **Next** to proceed.

The wizard now displays the **Accept license agreements** page.

8 Read through each license agreement and accept it by Clicking on the **Accept** tab. Click on **Next** to proceed.

Note There are two license agreements that you will have to accept as depicted in the following figures:

Figure 3-58. Accept license agreements 1 of 2

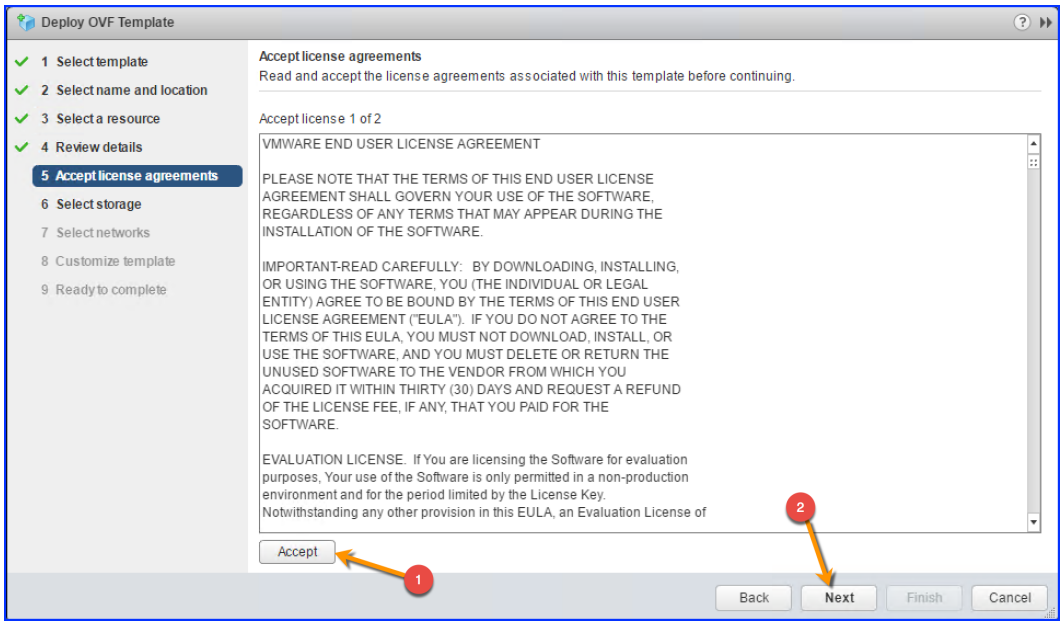
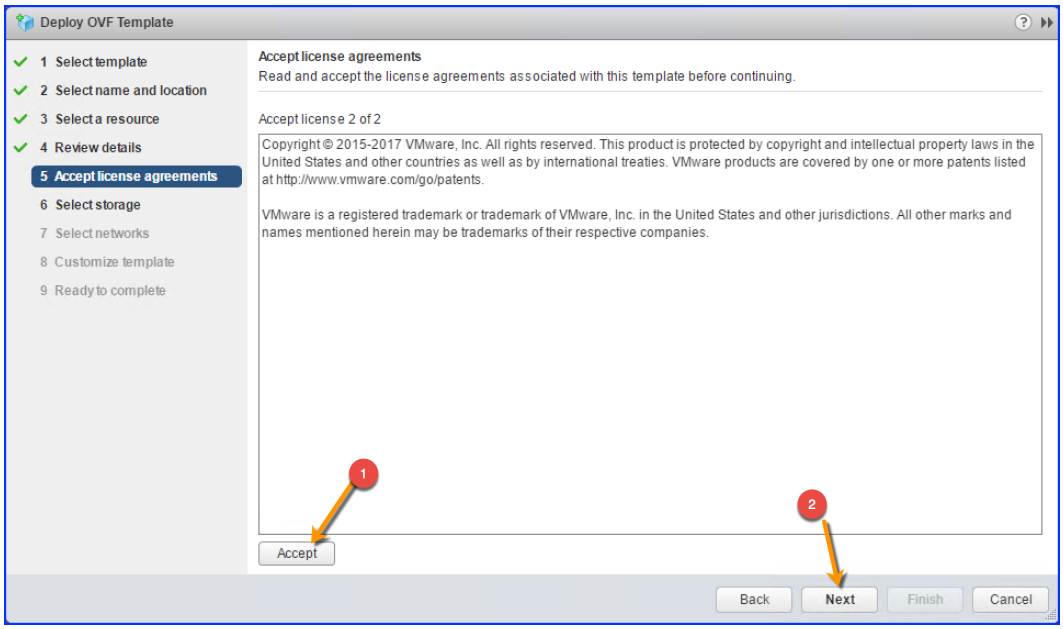


Figure 3-59. Accept license agreements 2 of 2

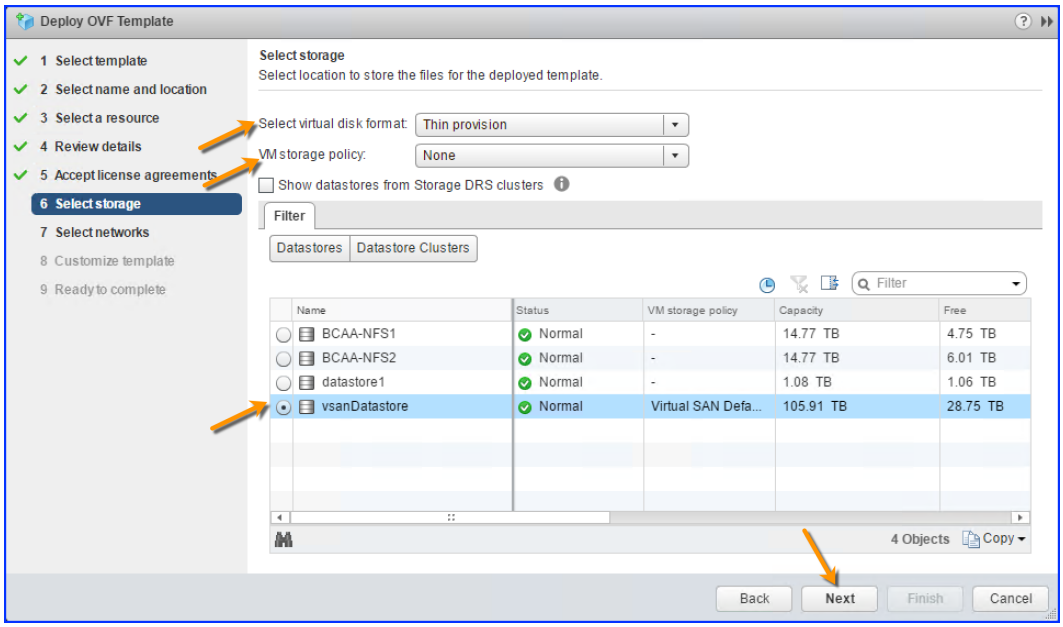


At the completion of this step, the wizard takes you to the **Select storage** page.

9 Select the datastore on which to write the VLA's virtual disks. If appropriate, select the virtual disk format (some datastore types do not allow you to choose format), select the storage policy (if one is available), and then Click **Next**.

The **Select storage** page of the wizard looks similar to the following:

Figure 3-60. Select storage

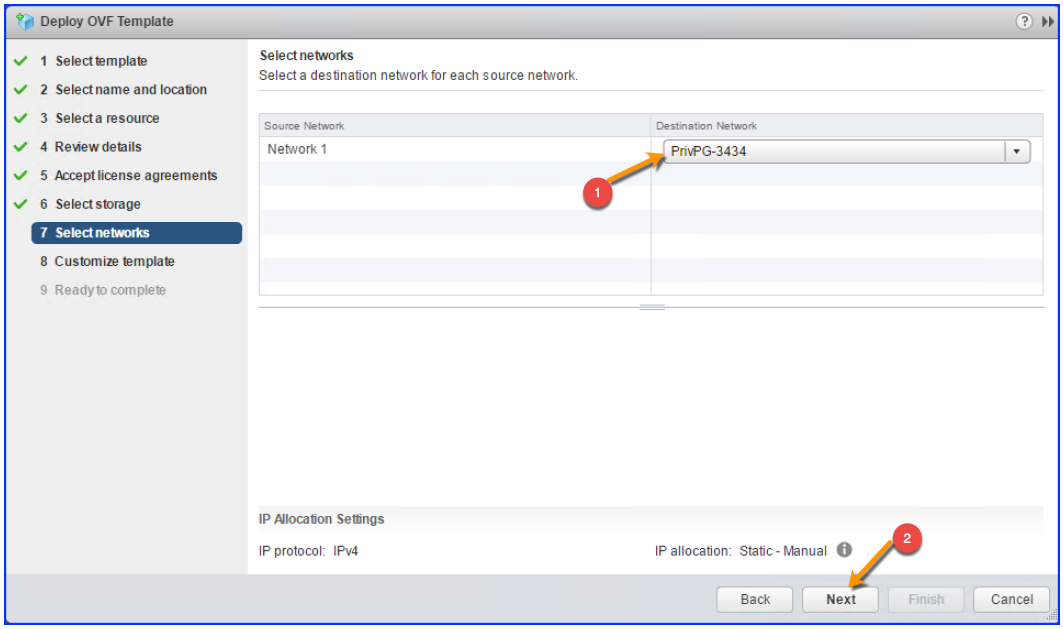


The wizard now displays **Select networks** page.

10 Select the Destination Network for each Source Network. Click **Next** to proceed.

The Select networks page looks similar to the following figure:

Figure 3-61. Select networks



The wizard now displays the **Customize template** page similar to the following:

Figure 3-62. Customize template

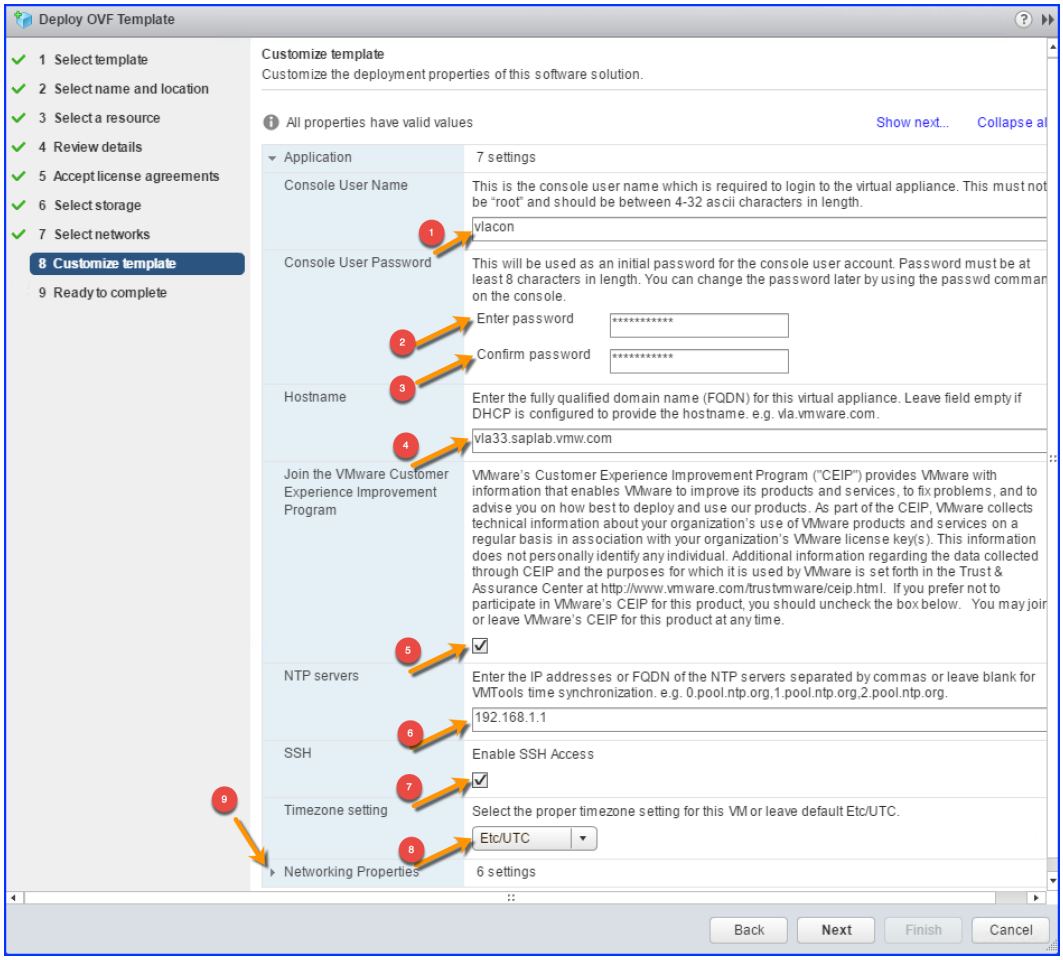
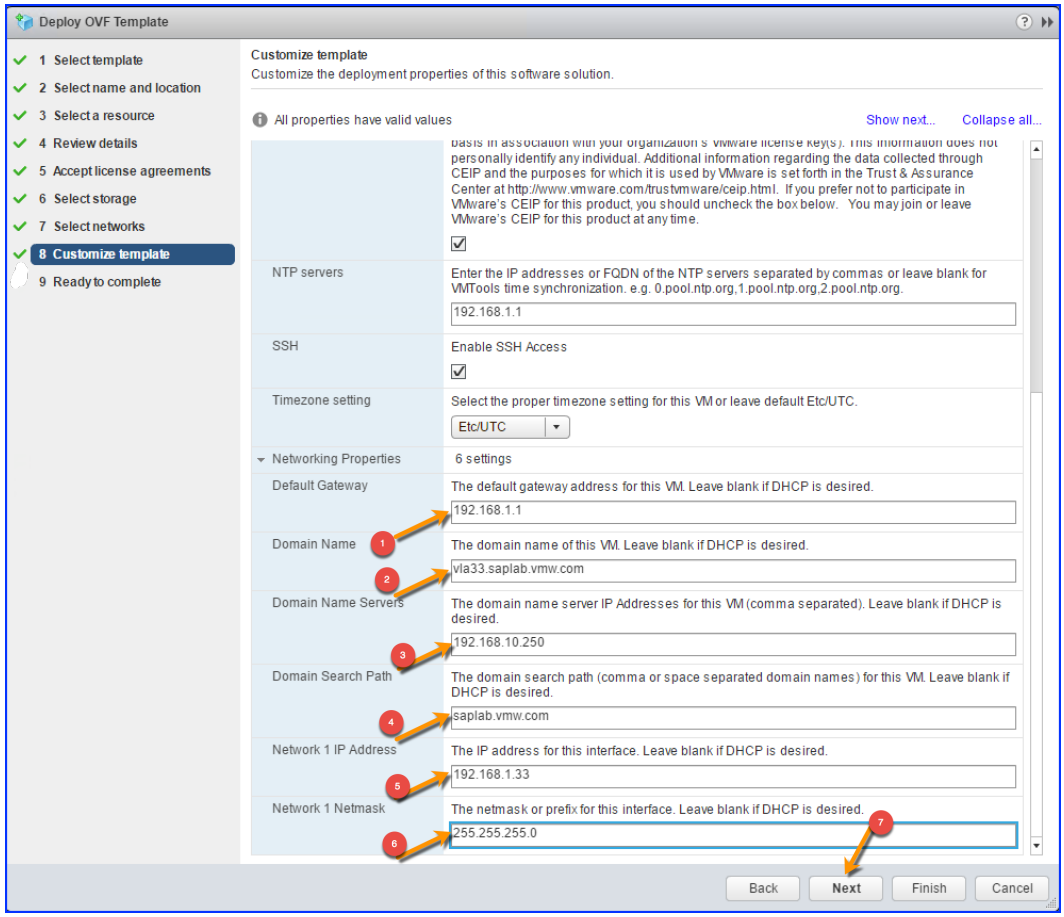


Figure 3-63. Customize template Contd. (Networking Properties)



11 In the **Customize template** dialog —

NOTE Provide values as appropriate to your environment/setup.

a Enter the Console User Name and Password. You need to enter the password twice for confirmation.

NOTE The console password that you enter in this step has an expiry of 60 days.

b Enter a FQDN (Fully Qualified Domain Name) for the new VLA virtual machine to use. FQDN should be resolvable to appliance IP Address by DNS server configured during deployment. VLA will always get a DHCP acquired IP Address.

c Enter the IP address or FQDN of the NTP server.

d Uncheck the check box you wish to Leave the VMware Customer Experience Improvement program (CEIP). Refer "Customer Experience Improvement Program," on page 78 for details.

NOTE The check box to enable you to Join the CEIP is checked by default

e Type in the IP address or the FQDN of the NTP servers, separated by commas.

f If you want to enable SSH select the **Enable SSH Access** checkbox

g Set the Time zone appropriately

h Scroll down to the expand **Networking Properties** section.

i Use the fields in this section to enter the static IP information for the VLA, including:

1 Default gateway IP address

2 FQDN of your VLA Appliance

3 DNS Server IP address

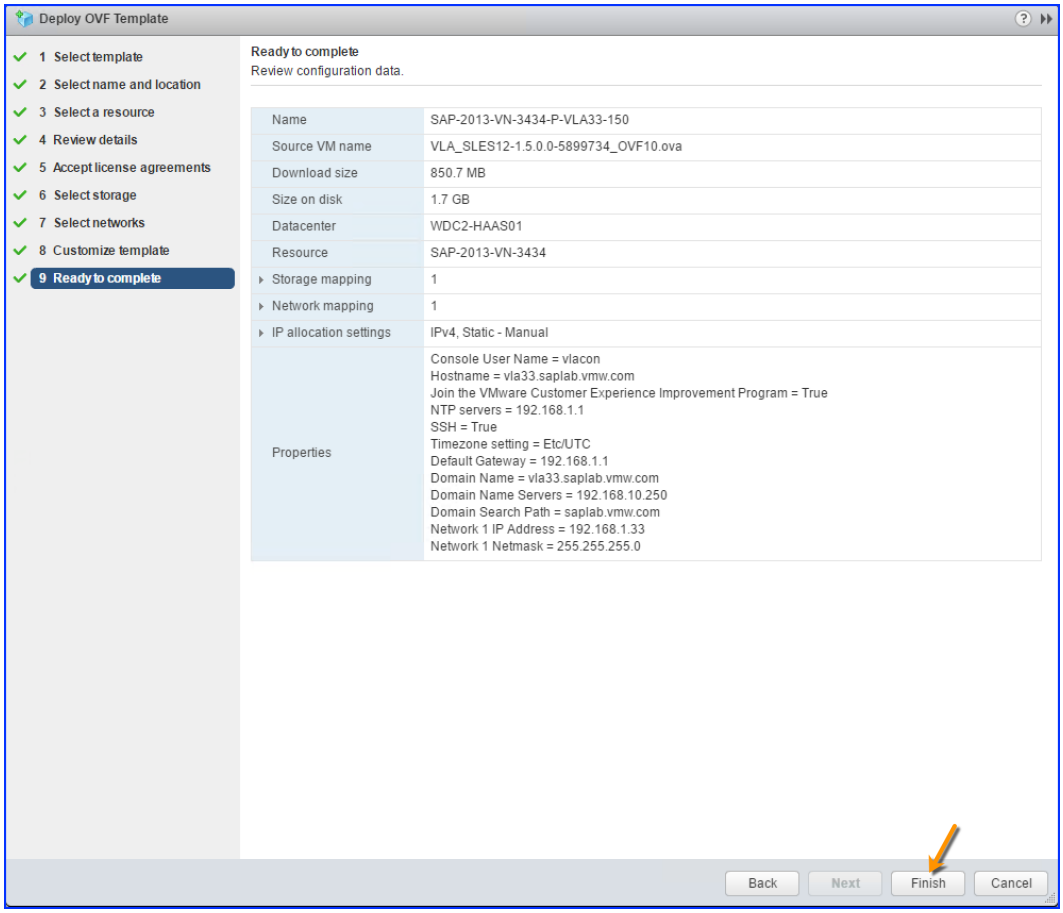
4 Domain search path

5 IP Address of the VLA. If you leave this field blank VLA will get a DHCP acquired IP address.

6 Network Mask for the interface

After configuring these options, Click **Next**. The Wizard now displays the **Ready to complete** dialog depicted as follows:

Figure 3-64. Ready to complete



12 Review all the configurations made so far. Click on **Finish** to start the VLA virtual machine deployment process. To monitor the progress of VLA deployment, you can watch the **Recent Tasks** pane in the VMware vSphere Web Client (VWC).

By executing the preceding steps you should be able to successfully deploy a VLA appliance in your environment.

Configure the VMware VLA

The next step is to configure the VMware VLA. You will:

- Configure the vla-service

- Install the VMware Adapter for SAP Landscape Management

vla-service Configuration

The following sections provide procedures for configuring the vla-service.

Create VLA Service user and password

The VMware Adapter for SAP Landscape Management uses the VLA Service user to connect to the VMware VLA Service. The VLA Service user and password are required to configure the VMware adapter in the LaMa web interface. There is only one VLA Service user per appliance. If you reset the VLA Service user and password, you will have to update the changes in the Configuration section of the VLA web interface.

The VLA Service password must be greater than 8 characters and contain a letter, number and symbol.

To set the LaMa Service user and password:

1 Go to the VLA console window.

2 You execute the `sudo` command to get administrative access. This is needed to be able to execute the subsequent steps. You are prompted for the password. Enter the console user password that you provided when deploying the VLA (See "Deploy VLA," on page 59)

```
sudo –s
```

3 Type the following command to create a user that you subsequently use to authenticate to the VLA appliance's web user interface:

vla_user -S LOCAL_USER –a vla-server -u <vla-service-user-name>

where <vla-service-user-name> is the name of the user you wish to create for the VLA server.

For example:

```
# vla_user –S LOCAL_USER –a vla–server –u vla
```

Note The **Tomcat** server for the VLA Appliance also uses this user to authenticate access to the `VLA REST API` used by the VLA Adapter running in the LaMa system.

---

4 When prompted, enter the password. You are required to enter the password twice.

5 Open a new browser window or tab.

6 Type the URL of the VLA Server Dashboard on the **Tomcat** instance

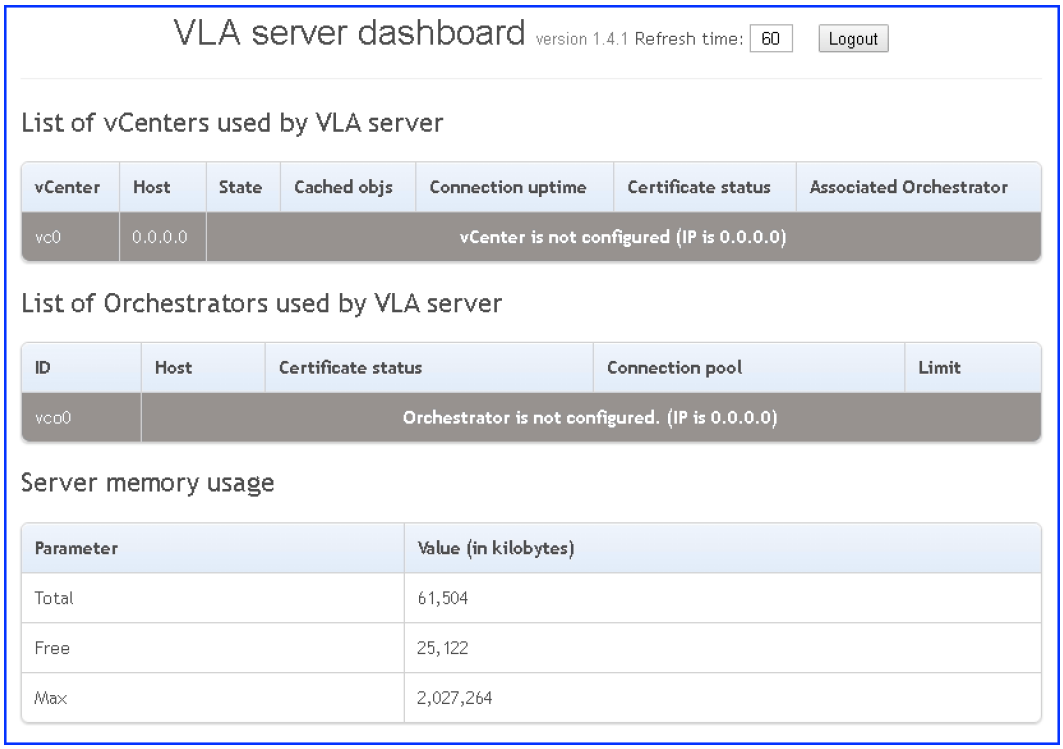
https://<vla_hostname_or_IP>:8443/vla/dashboard, where `<vla_hostname_or IP>` is the FQDN of the VLA or its IP address — for example

```
https://vla–host:8443/vla/dashboard
```

7 If there is a prompt with a certificate warning, accept the warning.

8 You are required to authenticate. Enter the VLA Service username and password combination that use used in step 3. The browser displays a page similar to the following:

Figure 3-65. VLA Server Dashboard



9 Do not close the window for the dashboard. It displays the status and some basic statistics of the VMware VLA service which you use to confirm the health of the VLA service in later steps.

10 Validate that the credentials command worked by entering the following command:

```
vla_credentials –l
```

In the next set of steps, you connect the VLA Service to the VMware vRealize Orchestrator and vCenter Server.

Connecting to VMware vRealize Orchestrator

Prerequisites

The VMware VLA Service connects to the VMware vRealize Orchestrator Server. The VMware VLA Service uses VMware vRealize Orchestrator to execute commands such as Start, Stop, and Clone. You use the `vla_credentials` command to manage VMware vRealize Orchestrator connection(s), using flags to add, modify, remove, and Test credentials entries.

When the `vla_credentials` command runs, it not only creates entries in the credentials database on the VLA server, but also performs several checks. When invoked for creating connections to VMware vRealize Orchestrator, this command checks the following:

- That the credentials supplied with the command (described in the following procedure) work. It tests this by trying to authenticate to the VMware vRealize Orchestrator system with the supplied credentials.
- That the VMware vRealize Orchestrator can reach each vCenter Server that has been registered to it.

You must run the `vla_credentials` command as an administrator on the VLA appliance. Since the VLA appliance does not have a root user enabled, you gain administrative access from your VLA login account using the `sudo` command with the `-s` flag.

Procedure

1 Go to the VLA console (or SSH) window and enter the following commands from the shell.

2 Execute the `sudo` command to get administrative access.

```
sudo –s
```

3 Create a credentials for the VMware vRealize Orchestrator by entering the following command:

`vla_credentials` -a -s vco -n <hostname> -u <vcoUsername>

where:

a <hostname> is the FQDN of the VMware vRealize Orchestrator Server

b <vcoUsername> is the name of the limited-rights vCenter Server user for VMware vRealize Orchestrator (see Section "Create a (Limited Rights) VLA user," on page 35) , in the format user@domain. For example:

```
# vla_credentials –a –s vco –n sapi–vco.example.com –u administrator@vsphere.local
```

4 When prompted, enter the password for the user specified with the –u flag.

5 Look for a success message. If a failure message mentions a certificate checker error, you can override the certificate checker as discussed in the section "Certificate Checker: Check is completed with errors," on page 103

6 Refresh the VLA Server Dashboard browser window and look for the VMware vRealize Orchestrator Server in the dashboard. You should see a VCO configuration similar to the following:

Figure 3-66. VLA Dashboard

ID	Host	Certificate status	Connection pool	Limit
▶ vco0	sapi-vco.saplab.vmw.com	OK	Total: 50, In use: 0	1

7 Type the following command to list the credentials currently configured. You should see an output similar to the following.

Figure 3-67. Credentials Configured

```
vla_credentials -l
ID      Schema & port    Hostname                    User                          Server Type     Associated servers
vc0     https:443        sapi-vc1.saplab.vmw.com     administrator@vsphere.local   vcenter         vco1
vco1    https:8281       sapi-vco.saplab.vmw.com     administrator@vsphere.local   vco             vc0
```

Install / Update Workflows in the VMware vRealize Orchestrator Server

1 Go to the VLA console window.

2 You execute the `sudo` command to get administrative access. This is needed to be able to execute the subsequent steps. You are prompted for the password. Enter the console user password that you provided when deploying the VLA (See "Deploy VLA," on page 59)

```
sudo –s
```

3 Type the following command at the prompt to install the VMware vRealize Orchestrator workflows

```
vla_vco_package_install –i
```

4 Refresh the browser window, find the orchestrator and expand it by Clicking the arrow in the ID column in the orchestrator list. The browser displays orchestrator workflow list similar to the following:

Figure 3-68. Orchestrator Workflows

ID	Host	Certificate status	Connection pool	Limit
▼ vco1	vro1.saplab.vmw.com	OK	Total: 50, In use: 0	1

List of loaded Orchestrator workflows

Operation	Workflow	Description	Version
suspend	LVM suspend virtual machine and wait workflow	Suspends a virtual machine and waits for the task to complete.	1.41.1
onError	On-error	This workflow is meant to be implemented by end-user This is a part of VMware Adapter for SAP Landscape Management suite, don't execute it manually. Phase parameter that is passed to workflow must be one of the following: - PRE_CREATE During pre-create workflow - DEPLOYMENT During instantiation after pre-create workflow - POST_CREATE During post-create workflow - FINALIZATION After post-create workflow (e.g. while setting status or something similar)	1.41.1
convertVmToTemplate	Convert VM to template	Convert virtual machine to template This is a part of VMware Adapter for SAP Landscape Management suite, don't execute it manually!	1.41.1
customizeVM	Customize VM	The workflow used to apply customization specification to the VM This is a part of VMware Adapter for SAP Landscape Management suite, don't execute it manually!	1.41.1
createVMFromTemplate	LVM provisioning, create vm from template/snapshot	This workflow is a part of Landscape Management provision operation it creates a clone of a virtual machine or provision new vm from template. This is a part of VMware Adapter for SAP Landscape Management suite, don't execute it manually.	1.41.1
getVcoLogs	LVM send troubleshooting information (scripting.logs, workflow executions, vSphere versions) to emai	This workflow collects logs VMware vCO, version of the VMware vCenter and all the connected ESXi hosts. This information is sent to the your email or put vco logs zip file in out var "mime_zip_file" and VMware Env version in out var "vmware_version". This workflow for technical support and helps it to gather information about the environment customers. This is a part of VMware Adapter for SAP Landscape Management suite, don't execute it manually.	1.41.1

Note If you open the VLA Server Dashboard in Internet Explorer 11 and Click the arrow in the orchestrator ID column (under the **List of Orchestrators used by VLA Server**) you do not see the expanded list of workflows as seen in the preceding figure. However, this functionality works fine in other browsers like Google Chrome, Microsoft Edge and Firefox.

Connecting to vCenter Server

To register or add a new vCenter Server connection, do the following steps:

Prerequisites

The VLA Service connects to one or more vCenter Servers to gather inventory and metrics. The VLA Service can hence connect to one or more vCenter Servers. You can use commands to register (or add), modify, remove, test, and list vCenter Server connections. You must add at least one vCenter Server connection. When you add a vCenter Server connection, you associate a VMware vRealize Orchestrator with the vCenter Server that you are adding. This lets the LaMa service know which VMware vRealize Orchestrator to use to process actions on the vCenter Server objects.

Procedure

1 Go to the VLA console window.

2 Execute the `sudo` command to get administrative access and enter the console user password that you provided when deploying the VLA (Step 9 of "Deploy VLA," on page 59)

```
sudo –s
```

3 Add an entry to the credentials database for the vCenter Server. To do this, enter the following command at the prompt:

```
vla_credentials –a –s vcenter –n <vcenter–fqdn> –u <vcenter–user> –A <vco–id>
```

where:

- `<vcenter–fqdn>` is the fully-qualified domain name of the vCenter Server you wish to connect to the VLA
- `<vcenter–user>` is the name of the limited-rights vCenter Server user you previously created ("Create a (Limited Rights) VLA user," on page 35)
- `<vco–id>` is the ID for the VMware vRealize Orchestrator server you added in section ("Connecting to VMware vRealize Orchestrator," on page 69). If you don't know the ID of the VMware vRealize Orchestrator Server, use the command `vla_credentials –l`, which returns output similar to the following:

Figure 3-69. VLA Credentials

```
ID      Schema & port    Hostname                 User                          Server Type     Associated servers
-------------------------------------------------------------------------------------------------------------------
vco0    https:8281       sapi-vco.saplab.vmw.com  administrator@example.com     vco             vc1
vc1     https:443        sapi-vc1.saplab.vmw.com  administrator@example.com     vcenter         vco0
```

For example:

```
# vla_credentials –a –s vco –n sapi–vco.example.com –u administrator@vsphere.local –A
vco0
```

when prompted, enter the password for the user you specified.

4 Look for a success message. If a failure message mentions a certificate checker error, you can override the certificate checker (See "Certificate Checker: Check is completed with errors," on page 103)

5 Refresh the browser window and look for the server in the VLA Server Dashboard. You should see an entry to the vCenter Server that you connected to in step 3 above.

6 You can also type the following command at the prompt on the VLA console.

```
vla_credentials –l
```

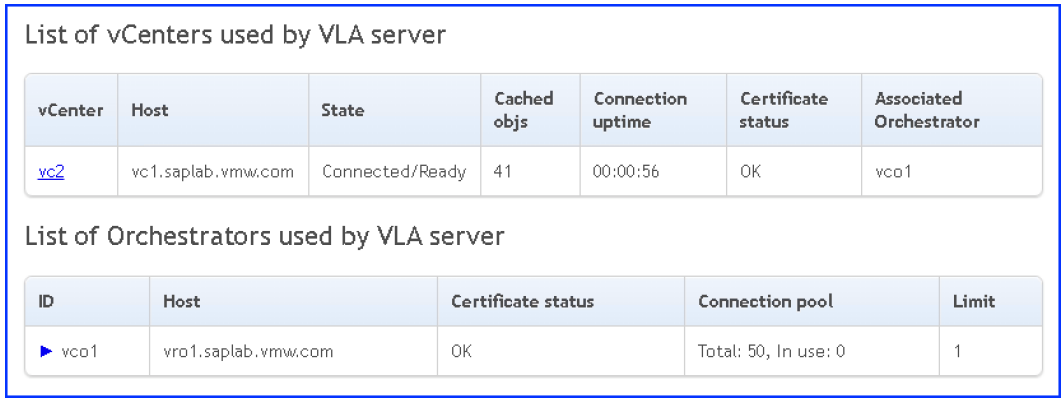
Figure 3-70.

```
vla_credentials -l
ID      Schema & port    Hostname                 User                          Server Type     Associated servers
-------------------------------------------------------------------------------------------------------------------
vc0     https:443        sapi-vc1.saplab.vmw.com  administrator@vsphere.local   vcenter         vco1
vco1    https:8281       sapi-vco.saplab.vmw.com  administrator@vsphere.local   vco             vc0
```

7 For each additional vCenter Server repeat steps 3 through 6 in this section.

Confirm Connection Status

Figure 3-71. VLA Server Dashboard - Association



The next step is to confirm the health of the vCenter Server and VMware vRealize Orchestrator Connections. Go to the browser window that has the VLA Server Dashboard. Reload the VLA Service dashboard to view all your vCenter Server , their connection state and associations. The VLA Server Dashboard also shows the VMware vRealize Orchestrator connection and the VMware vRealize Orchestrator workflows if installed on the VMware vRealize Orchestrator Server.

Install the VMware LaMa Adapter

To complete your installation, the VMware Adapter for SAP Landscape Management needs to be installed on the LaMa VM. There are different installation instructions for Microsoft Windows and Linux operating systems. If you are using Linux as your LaMa OS, you can install the VMware Adapter using the command line.

Install the VMware LaMa Adapter on Microsoft Windows

To install, the adapter LaMa VM should be running Windows Server. Before you perform the installation, ensure that the LaMa is running. The installation of the adapter is done in 2 phases:

1 Download the adapter file to the LaMa VM from the dashboard

2 Install the adapter with the `deploy` command

Download the Adapter

1 Log into the LaMa VM and launch a browser window.

2 Enter the URL for the LaMa Service Dashboard, for example:

https://<vla hostname>:8443/vla/dashboard, where `<vla_hostname>` is the FQDN or IP address of VLA.

3 You may be prompted with a certificate warning, just accept the warning and proceed to the dashboard-landing page.

4 The dashboard should be displayed after you enter the LaMa Service username and password.

5 Scroll to the bottom of the dashboard page

6 Click VMware Adapter for LaMa.

a if prompted for a directory for the download, specify

```
C:\usr\sap\<SID>\J<Instance>\j2ee\deployment\scripts
```

b If you are not for a directory for the download, after downloading the file, move it to the directory

```
C:\usr\sap\<SID>\J<Instance>\j2ee\deployment\scripts
```

7 Verify that the adapter file **VMwareLVM.ear** file is in the scripts directory

Install the Adapter

1 Right click on the Windows start icon and open a command prompt with administrative rights.

2 At the C: prompt change directory to `C:\usr\sap\<SID>\J<Instance>\j2ee\deployment\scripts`

3 Run the following command:

```
make_SDA.bat VMwareLVM.ear
```

4 Use the `deploy` command to deploy the adapter to LaMa - for example,

```
deploy <user>:<password>@localhost:50004 ..\SDA\VMwareLVM.ear
```

```
Usage: deploy <user>:<password>@<host>:<port> <ear file> [-no_start]
Parameters:
<user>    User with administrators' rights.
<password>    Password for this user.
<host>    Target AS Java host.
<port>    Target LaMa telnet port is 5000N
<ear file>    Path to archive.
[-no_start]    Deployed modules are not started.
```

Install the VMware Adapter for SAP Landscape Management on Linux (SUSE or Redhat)

Recall from the product architecture discussion (See "Reference Architecture," on page 10) that in addition to the VLA Appliance and VCO workflows that this document discussed installing in previous sections, the VLA product includes a VMware Adapter for SAP LaMa system. This section, and its sub-sections, discuss how to install said VMware Adapter for SAP LaMa where said system is running on a supported SUSE or Redhat Linux operating system.

Before you can deploy said adapter, ensure that the LaMa system is running, that you can SSH to it and logon to its Netweaver web user interface.

VMware currently supports two methods for deploying the VLA Adapter to the LaMa system:

- Using the `vla_adapter` command, discussed in the next sub-section (See "Deploying the VMware Adapter for SAP Landscape Management via the vla_adapter command," on page 74)
- Issuing a series of shell commands as discussed in section "Deploying the VMware Adapter for SAP Landscape Management via Several Shell Commands," on page 75

The next two sub-sections provide details for each of these options.

Deploying the VMware Adapter for SAP Landscape Management via the `vla_adapter` command

To install the adapter to the LaMa system via the `vla_adapter` command:

1 Login to the VLA system as the user you created when you deployed your VLA system.

2 Gain administrative access via the following command:

```
sudo –s
```

Enter the console user password that you provided when deploying the VLA (Step 9 of "Deploy VLA," on page 59)

3 Deploy the LaMa component of the VLA product to the LaMa system by entering the following command:

```
vla_adapter -a -f <ipaddress> -u <lama-shell-admin> –x <lama-web-admin>
```

where:

- ipaddress — is the IP address or FQDN of the LaMa system
- <lama-shell-admin> — is the name of a user that can login to the Linux shell (via SSH) on the LaMa Linux system and has Linux administrative privileges, for example **root**.
- <lama-web-admin> — is the name of a user that can login to the LaMa web user interface and has LaMa administrative privileges, for example **Administrator**.

This command prompts you for passwords for both the shell login (SSH) and LaMa web user interface accounts. Provide those passwords when prompted.

The following is an example of running `vla_adapter` command against a LaMa at IP address 192.168.10.21 with the lama-shell-admin set to **root** and the lama-web-admin set to **Administrator**, including the password prompts and output from the command showing progress and success:

```
# vla_adapter –a –f 192.168.10.21 –u root –x Administrator
Enter SSH password:
Enter LaMa administrator password:
VLA: vla_adapter [INFO]: Start installing the adapter to LaMa server
VLA: vla_adapter [INFO]: Adapter installation successful
#
```

Deploying the VMware Adapter for SAP Landscape Management via Several Shell Commands

This section discusses the steps you must take to deploy the VMware Adapter for SAP Landscape Management system without using the `vla_adapter` command. It consists of a series of shell commands that you run on the LaMa system from a shell, that provides analogous behavior to the LaMa system. You typically only use this method if the LaMa system does not allow SSH access from the VLA appliance (because this alternative method is longer, manually driven, and thus more error-prone).

Follow these steps to deploy the VLA Adapter manually:

1 Copy the adapter and deploy script from the VLA to the LaMa system:

   a Start a shell session on the LaMa system as **root**.

   b Copy the deploy script to the `/tmp` directory via `scp`:

   ```
   scp root@<vla FQDN>:/opt/vmware/vla/lvm/vlvma_manage/arch/deploy /tmp
   ```

   c Copy the adapter to the `/tmp` directory via `scp`:

   ```
   scp root@<vla FQDN>:/opt/vmware/vla/lvm/vlvma_manage/arch/VMwareLVM.ear /tmp
   ```

2 Install the adapter using the deploy script.

   a Log into the LaMa VM.

   b Change directory to `/tmp`.

   c Type `deploy`. The script will prompt you for the following items:

      1 LaMa IP Address — Usually should be set to 127.0.0.1

      2 LaMa Port Address — for instance 00, the port should be 50008

      3 LaMa User ID — a LaMa user with administrative rights

      4 LaMa User Password — password of the LaMa user.

      5 Adapter EAR file Absolute Path — the absolute path to the VMwareLVM.ear file.

      6 LaMa Instance directory — the directory that has the LaMa instance, usually `/usr/sap`. If you are unsure, the deploy script will search for it if you leave this parameter blank.

Configure LaMa to use the VMware Adapter for SAP Landscape Management

The VMware Adapter for SAP Landscape Management receives LaMa commands and forwards them to the VLA for execution. The next setup step is to configure an adapter instance to connect the adapter to the VLA server. Once the connection is established, the LaMa manages the hosts and instances that reside on the SDDC.

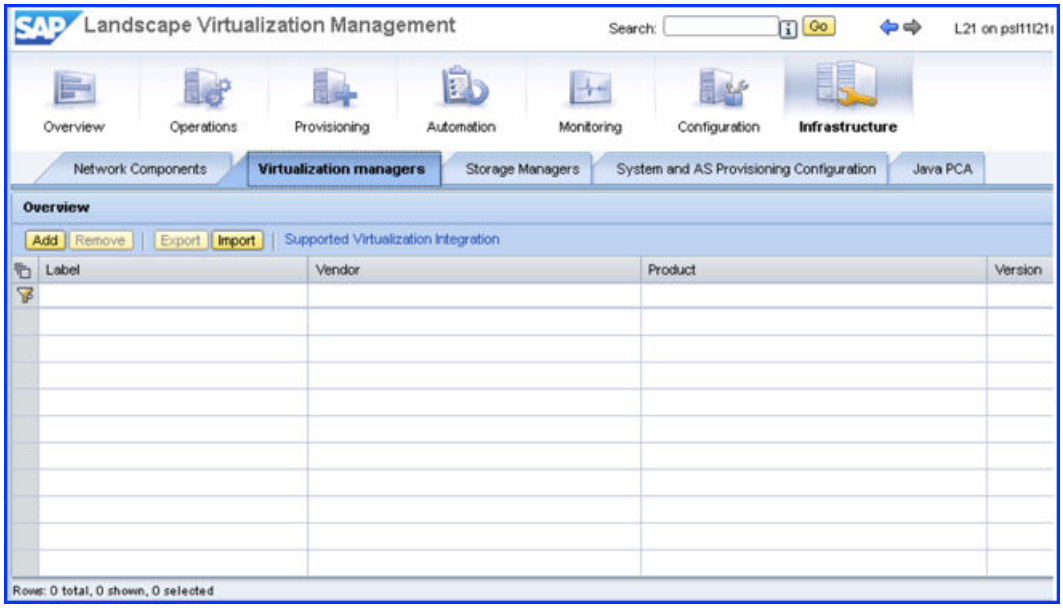
Procedure

1 Login to LaMa web user interface with credentials that have administrator rights.

2 Click **infrastructure**, and click **Virtualization managers**.

The browser displays a page similar to the following:

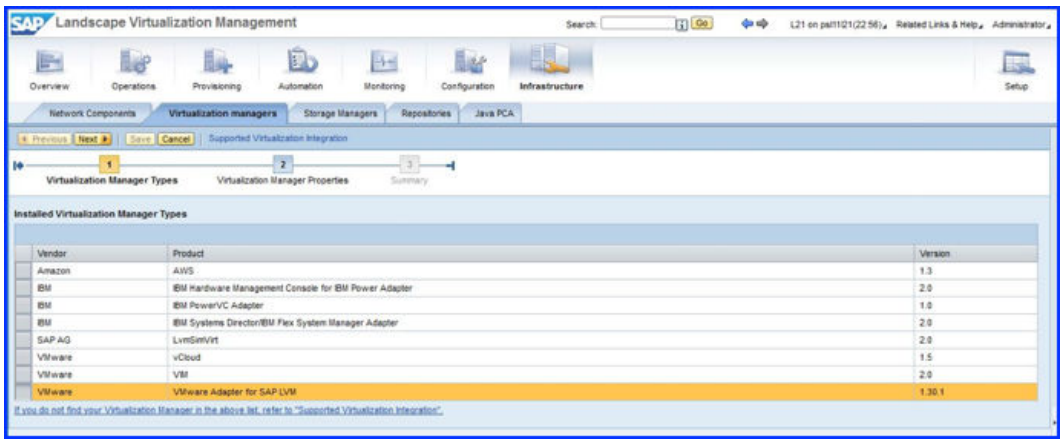
Figure 3-72. LaMa-Virtualization managers



3 Click **Add**.

The browser displays a wizard to configure a new Virtualization Manager, starting with the **Virtualization Manager Types** page similar to the following:

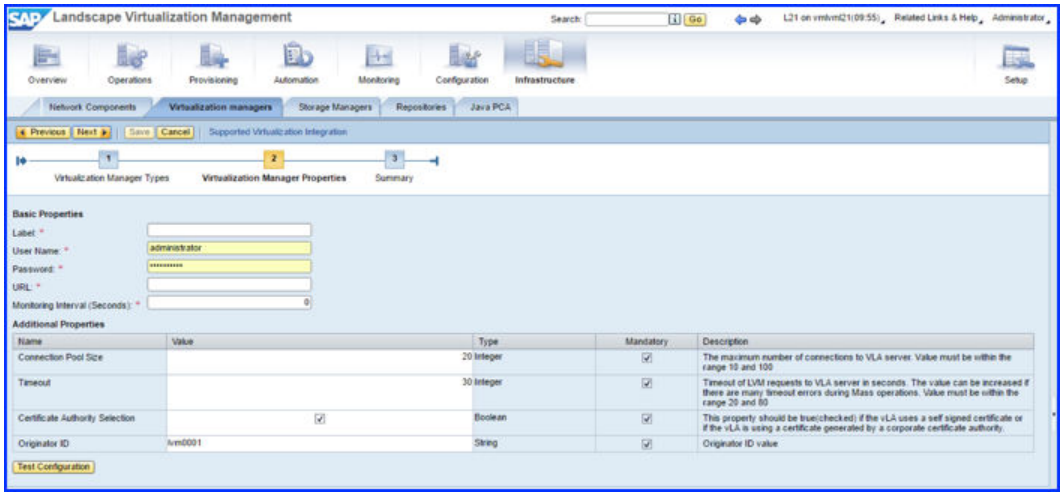
Figure 3-73. LaMa-Add-Virtualization Manager Types



4 Select the entry (highlighted above for emphasis) with VMware Adapter for SAP Landscape Management in the Product column and version of the VLA Adapter you deployed in the version column and then click **Next**.

The browser displays the **Virtualization Manager Properties** page similar to the following:

Figure 3-74. LaMa- VMware Adapter for SAP Landscape Management



5 Enter a name for this instance of the VLA Adapter in the **Label** field.

6 Enter the User Name and Password of the VLA user.

7 Enter the URL for the VLA. This should be https://<hostname_or_IP_address>:8443/vla, where `<hostname_or_IP_address>` is the FQDN or IP address of VLA.

8 Enter a Monitoring Interval between 30 and 60 seconds. This is, how often the adapter gathers inventory updates from the VLA.

9 There are four **Additional Properties**:

a **Connection pool size** sets the maximum connection between the adapter and the VLA.

b Timeout sets the timeout duration (in seconds) between the adapter and the VLA

c A checkbox for **Certificate Authority Selection**. Select this if the VLA contains a self-signed certificate or a certificate that is generated by a corporate certificate authority.

d Originator ID – Unique Id used for transaction logging. This ID is a string and will identify this instance of the adapter in the system logs. We recommend you use LaMa-001 for the first instance in your enterprise, LaMa-002 for your second, etc.

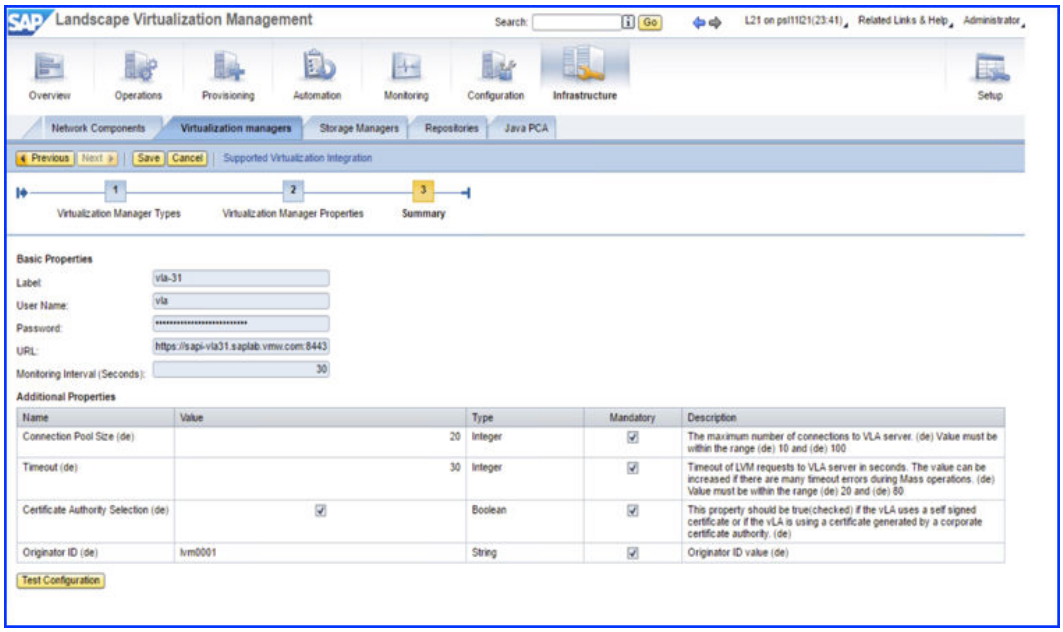
10 After all properties are entered, click **Test Configuration**. If the test succeeds, the configuration is correct (the VLA Adapter was able to communicate with the VLA Appliance)

The browser displays Connection Successful in the status bar.

11 Click **Next**.

The browser displays the Summary step of the wizard, similar to the following:

Figure 3-75. LaMa-Test Configuration



12 Click **Save**.

This saves the configuration of the adapter.

The VMware Adapter for SAP Landscape Management should now appear as configured in the LaMa web user interface.

Customer Experience Improvement Program

This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at `http://www.vmware.com/trustvmware/ceip.html`. To join or leave the CEIP for this product, please refer to the following topics:

- To join or leave during deployment, see "Deploy VLA," on page 59.
- To join or leave during update of the VLA, see "Join or Leave CEIP during VLA Upgrade," on page 94
- To join or leave at any time after deployment or update, using the VLA's web UI, see "Change Participation Preference to CEIP (GUI Method)," on page 111
- To join or leave at any time after deployment or update, using the VLA's CLI, see "Change Participation Preference CEIP (CLI Method)," on page 109

You have an option to select your participation preference to either **Join** or **Leave** CEIP for VLA product, at the time of deploying the VLA virtual appliance VM (see "Deploy VLA," on page 59). However, if you wish to change your participation preference at any later point in time following VLA deployment, you can do so either from the command line or from the GUI.

Perform an Upgrade of the VLA

If you have an older version of VLA system, you can upgrade it to a later version instead of performing a fresh VLA installation. This section provides an overview of the upgrade process and the steps for upgrading the VLA system.

Understanding the Upgrade Process

While the details and steps of each upgrade are slightly different, they have much in common and follow the same basic steps. This section describes the overall update flow. Its sub-sections describe the specific steps for the different upgrade scenarios. The following table shows the possible versions from which you can upgrade and the versions to which they can be upgraded:

Table 3-5. VLA Software Updates

Version	Can be Upgraded to
1.3.1	1.4.1
1.4.0	1.4.1
1.4.1	1.5.0
1.5.0	1.5.1

Caution Before performing any update, you should snapshot your VLA VM. In case the update does not produce a working environment, you can revert, from snapshot, to your current working system. The upgrade program will prompt you to ensure you have taken the snapshot before it allows you to proceed.

Note If you have already installed a VMware Adapter for Landscape Management on your LaMa system, you should first uninstall the adapter (Refer "Uninstall the VMware Adapter for SAP Landscape Management," on page 101) before proceeding with the following VLA upgrade steps.

Upgrading the VLA involves the following high level events:

1 Download an ISO file that contains the new version of the VLA to a specific directory on your existing VLA system.

2 Run the `upgrade` program on your existing VLA, from the specific directory, providing the name of the file you downloaded in Step 1.

   This step mounts the ISO file and installs new and updates existing RPM files in your existing VLA's filesystem.

3 Reboot the VLA

   Note During the first boot after running `upgrade`, the 1.4.1 software does the following, depending on your previous version of the VLA:

   - From 1.3.1, it creates a new database used by the SA-API server (for vRA integration). 1.3.1 did not contain the SA-API server (for vRA integration). It was added in 1.4.
   - From 1.4, it updates the database used by the SA-API server (for vRA integration).

4 Manually update the workflows in the VMware vRealize Orchestrator with versions installed on the VLA as part of Step 2.

   The VLA server and SA-API server (for vRA integration) leverage these workflows for some of its work. Each version of the VLA has its own set of said workflows.

Downloading the VLA ISO (Update) file

If you are to upgrade your VLA from a previous version to a later version, you first need to download the ISO file for later version of VLA as described in this section.

Prerequisites

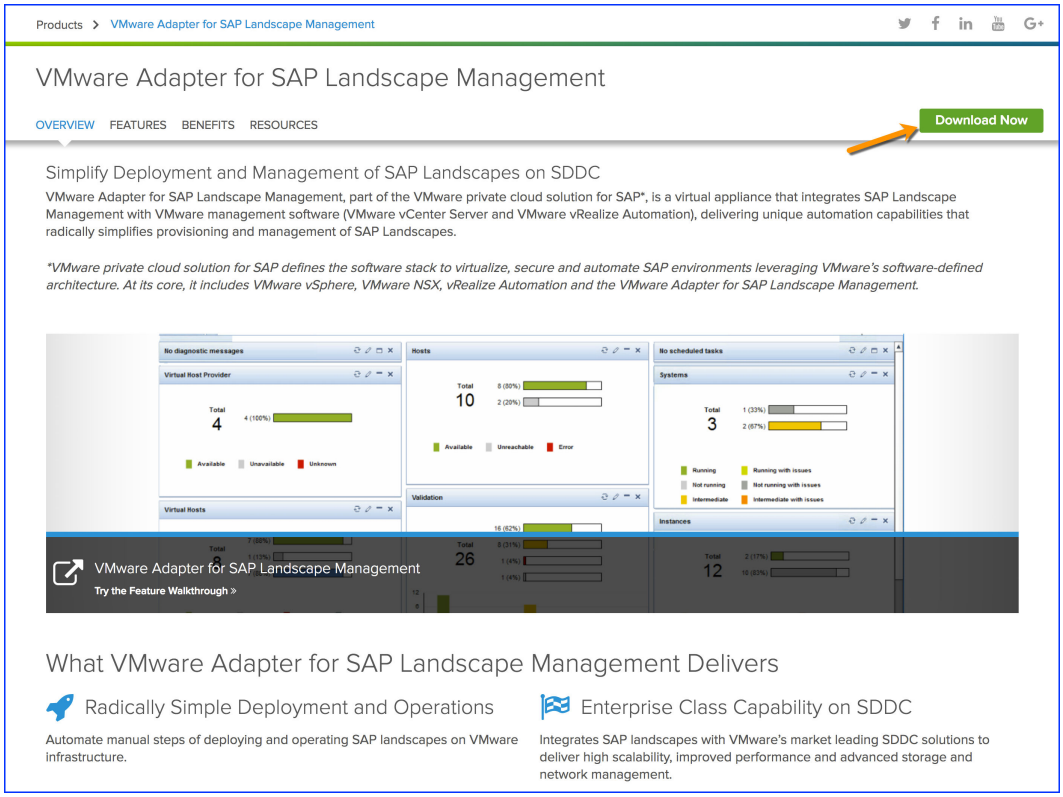
In order to download the VLA ISO file, you need an account at `my.vmware.com`, which is free.

Procedure

1 Browse to http://www.vmware.com/products/adapter-sap-lvm.html

The browser displays the a page similar to the following:

Figure 3-76. VMware Adapter for SAP Landscape Management Home



2 Click **Download Now** (pointed to in the preceding figure).

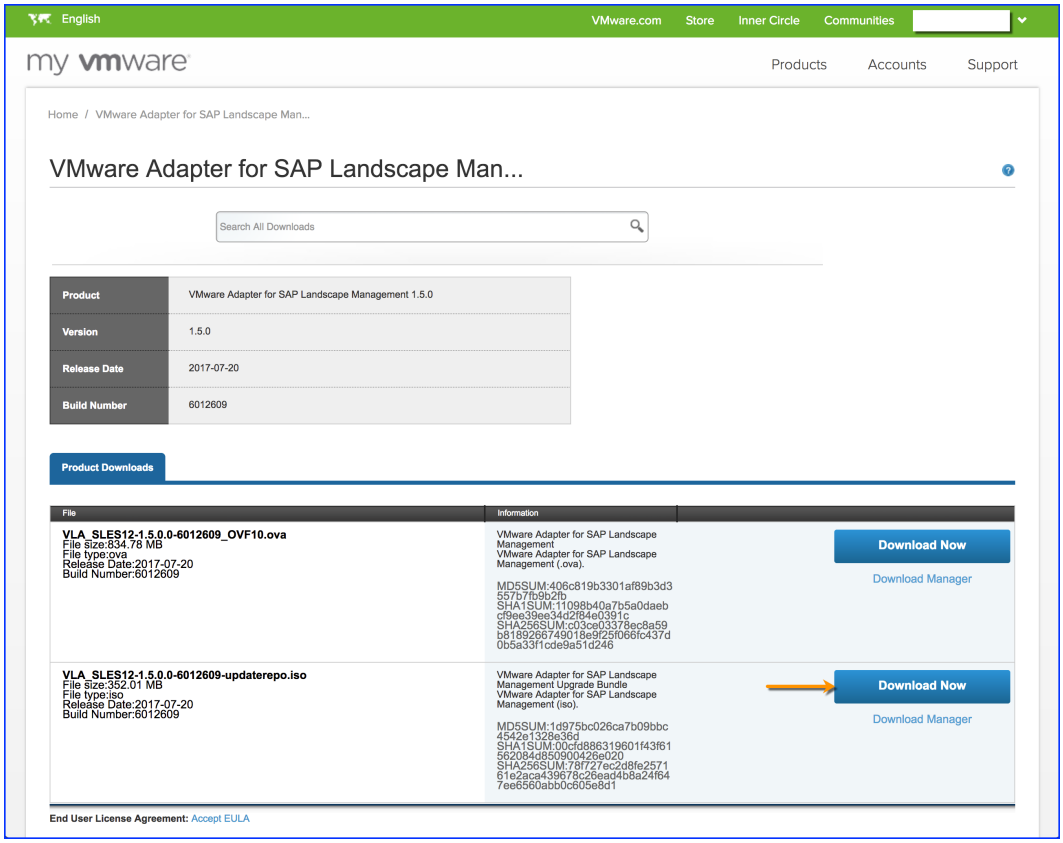
The **Download Now** tab redirects the browser to the login page at `my.vmware.com`, causing the browser to display a page similar to following:

Figure 3-77. my vmware login

3 Enter your login credentials and Click **Log In** (pointed to in the preceding figure for emphasis)

The browser displays the product download page similar to the following (This page shows the details for VLA version 1.5.0. The details for other versions will be slightly different):

Figure 3-78. VLA ISO Download



4 Click **Download Now** (pointed to in the preceding figure for emphasis), to download the VLA ISO file.

You have downloaded the VLA ISO file needed for upgrade. You can now perform the upgrade steps on your VLA.

Upgrading from 1.3.1 to 1.4.1

Note Take a snapshot of the VLA before proceeding with the upgrade

Once you have taken the snapshot of the VLA, execute the following steps to do the VLA upgrade:

Prerequisites

You are running version 1.3.1 VLA and have decided to upgrade it to version 1.4.1 VLA.

Procedure

1 SSH into the VLA as **root**.

Note If you are unsuccessful and see a "**Network error:Connection refused**" message, you may have to first start the SSH service on the VLA. To start the `SSH` service on the VLA, login as **root** from the vCenter VLA console. Enter the **root** password. You may then be asked to change the password for **root** account. Type in the new password twice. You then start the `SSH` service on the VLA using the `sys_ssh` command as depicted in the following figure:

Figure 3-79. Start SSH Service on VLA

```
vla33 login: root
Password:
You are required to change your password immediately (root enforced)
Changing password for root.
(current) UNIX password:
New password:
Retype new password:
Last login: Fri Feb 10 03:33:47 UTC 2017
Last login: Fri Feb 10 03:33:47 on tty1
vla33:~ # sys_ssh -s START
VLA: sys_ssh [INFO]: SSH service has been started by root user
vla33:~ #
```

You should now be able to SSH into the VLA successfully

2 Change directory to `/system2` on the VLA

3 Copy the VLA ISO file that you will use to upgrade your existing VLA from http://www.vmware.com/products/adapter-sap-lvm.html into the `/system2` directory.

Note Use any tool of your choice like `wget`, `WinSCP`, `scp` etc.

4 Execute the `sys_software_update` script to initiate the upgrade process. Specify the ISO file that you copied into the `/system2` directory that will be used for upgrade of the VLA as depicted in the following figure:

Figure 3-80. VLA Upgrade -1

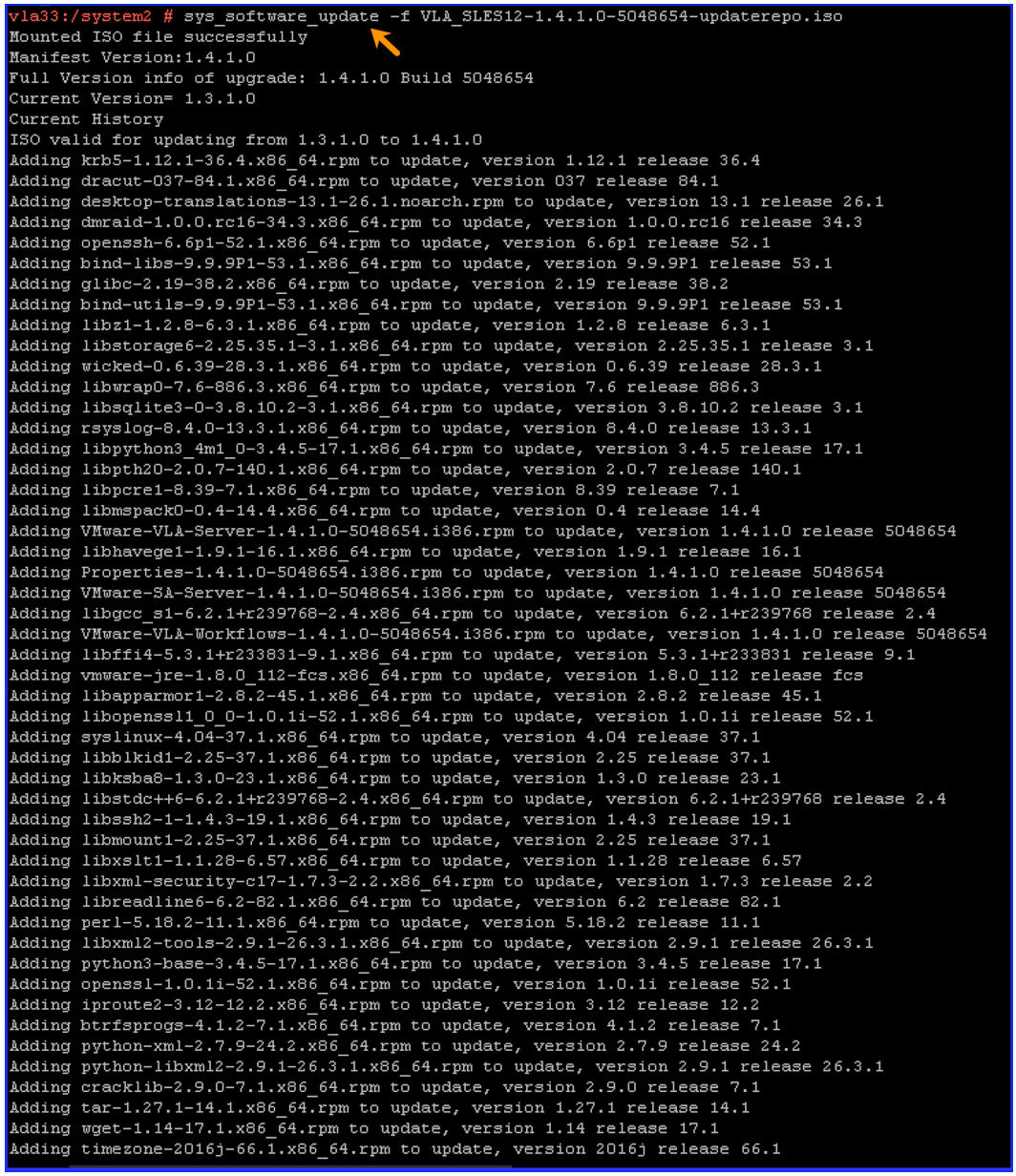


Figure 3-81. VLA Upgrade - 2

```
Adding rpm-4.11.2-15.1.x86_64.rpm to update, version 4.11.2 release 15.1
Adding perl-Bootloader-0.844-1.1.x86_64.rpm to update, version 0.844 release 1.1
Adding device-mapper-1.02.97-74.1.x86_64.rpm to update, version 1.02.97 release 74.1
Adding expect-5.45-18.56.x86_64.rpm to update, version 5.45 release 18.56
Adding kmod-17-8.1.x86_64.rpm to update, version 17 release 8.1
Adding perl-Bootloader-YAML-0.844-1.1.x86_64.rpm to update, version 0.844 release 1.1
Adding libparted0-3.1-19.3.1.x86_64.rpm to update, version 3.1 release 19.3.1
Adding kpartx-0.5.0-55.1.x86_64.rpm to update, version 0.5.0 release 55.1
Adding libvmtools0-10.0.5-3.1.x86_64.rpm to update, version 10.0.5 release 3.1
Adding sudo-1.8.10p3-2.6.1.x86_64.rpm to update, version 1.8.10p3 release 2.6.1
Adding util-linux-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding shadow-4.1.5.1-19.5.1.x86_64.rpm to update, version 4.1.5.1 release 19.5.1
Adding systemd-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding systemd-presets-branding-SLE-12.1-5.1.noarch.rpm to update, version 12.1 release 5.1
Adding systemd-sysvinit-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding dbus-1-1.8.22-22.2.x86_64.rpm to update, version 1.8.22 release 22.2
Adding procps-3.3.9-7.1.x86_64.rpm to update, version 3.3.9 release 7.1
Adding ntp-4.2.8p9-55.1.x86_64.rpm to update, version 4.2.8p9 release 55.1
Adding haveged-1.9.1-16.1.x86_64.rpm to update, version 1.9.1 release 16.1
Adding dnsmasq-2.71-13.1.x86_64.rpm to update, version 2.71 release 13.1
Adding insserv-compat-0.1-13.1.noarch.rpm to update, version 0.1 release 13.1
Adding sysconfig-0.83.9-10.1.x86_64.rpm to update, version 0.83.9 release 10.1
Adding libcurl4-7.37.0-31.1.x86_64.rpm to update, version 7.37.0 release 31.1
Adding suse-module-tools-12.3-21.1.x86_64.rpm to update, version 12.3 release 21.1
Adding sles-release-DVD-12.1-1.331.x86_64.rpm to update, version 12.1 release 1.331
Adding wicked-service-0.6.39-28.3.1.x86_64.rpm to update, version 0.6.39 release 28.3.1
Adding curl-7.37.0-31.1.x86_64.rpm to update, version 7.37.0 release 31.1
Adding update-alternatives-1.16.10-12.3.1.x86_64.rpm to update, version 1.16.10 release 12.3.1
Adding parted-3.1-19.3.1.x86_64.rpm to update, version 3.1 release 19.3.1
Adding kernel-default-3.12.67-60.64.24.1.x86_64.rpm to update, version 3.12.67 release 60.64.24.1
Adding perl-base-5.18.2-11.1.x86_64.rpm to update, version 5.18.2 release 11.1
Adding sysconfig-netconfig-0.83.9-10.1.x86_64.rpm to update, version 0.83.9 release 10.1
Adding grub2-2.02~beta2-89.1.x86_64.rpm to update, version 2.02~beta2 release 89.1
Adding libx86emu1-1.5-1.2.x86_64.rpm to update, version 1.5 release 1.2
Adding libuuid1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libudev1-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding grub2-i386-pc-2.02~beta2-89.1.x86_64.rpm to update, version 2.02~beta2 release 89.1
Adding libsmartcols1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libpython2_7-1_0-2.7.9-24.2.x86_64.rpm to update, version 2.7.9 release 24.2
Adding libprocps3-3.3.9-7.1.x86_64.rpm to update, version 3.3.9 release 7.1
Adding libnettle4-2.7.1-9.1.x86_64.rpm to update, version 2.7.1 release 9.1
Adding libkmod2-17-8.1.x86_64.rpm to update, version 17 release 8.1
Adding Apache-Tomcat-8.5.9-5048654.i386.rpm to update, version 8.5.9 release 5048654
Adding libidn11-1.28-4.1.x86_64.rpm to update, version 1.28 release 4.1
Adding Credentials-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding VMware-LVM-Adapter-1.41.1-5048654.i386.rpm to update, version 1.41.1 release 5048654
Adding VMware-VLA-VcoLogCollector-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding libexpat1-2.1.0-17.1.x86_64.rpm to update, version 2.1.0 release 17.1
Adding libdbus-1-3-1.8.22-22.2.x86_64.rpm to update, version 1.8.22 release 22.2
Adding libcap2-2.22-13.1.x86_64.rpm to update, version 2.22 release 13.1
Adding libbz2-1-1.0.6-29.2.x86_64.rpm to update, version 1.0.6 release 29.2
Adding libpci3-3.2.1-10.1.x86_64.rpm to update, version 3.2.1 release 10.1
Adding libxml2-2-2.9.1-26.3.1.x86_64.rpm to update, version 2.9.1 release 26.3.1
Adding libgcrypt20-1.6.1-16.33.1.x86_64.rpm to update, version 1.6.1 release 16.33.1
Adding libhogweed2-2.7.1-9.1.x86_64.rpm to update, version 2.7.1 release 9.1
Adding expat-2.1.0-17.1.x86_64.rpm to update, version 2.1.0 release 17.1
Adding openslp-2.0.0-17.1.x86_64.rpm to update, version 2.0.0 release 17.1
Adding libldap-2_4-2-2.4.41-18.22.1.x86_64.rpm to update, version 2.4.41 release 18.22.1
Adding libaugeas0-1.2.0-10.1.x86_64.rpm to update, version 1.2.0 release 10.1
```

Figure 3-82. VLA Upgrade - 3

```
Adding libxerces-c-3_1-3.1.1-12.3.x86_64.rpm to update, version 3.1.1 release 12.3
Adding bash-4.2-82.1.x86_64.rpm to update, version 4.2 release 82.1
Adding sles-release-12.1-1.331.x86_64.rpm to update, version 12.1 release 1.331
Adding python-base-2.7.9-24.2.x86_64.rpm to update, version 2.7.9 release 24.2
Adding libwicked-0-6-0.6.39-28.3.1.x86_64.rpm to update, version 0.6.39 release 28.3.1
Adding libcrack2-2.9.0-7.1.x86_64.rpm to update, version 2.9.0 release 7.1
Adding hwinfo-21.38-10.3.1.x86_64.rpm to update, version 21.38 release 10.3.1
Adding bzip2-1.0.6-29.2.x86_64.rpm to update, version 1.0.6 release 29.2
Adding python3-3.4.5-17.1.x86_64.rpm to update, version 3.4.5 release 17.1
Adding python-lxml-3.2.3-4.55.x86_64.rpm to update, version 3.2.3 release 4.55
Adding python-2.7.9-24.1.x86_64.rpm to update, version 2.7.9 release 24.1
Adding findutils-4.5.12-7.1.x86_64.rpm to update, version 4.5.12 release 7.1
Adding dirmngr-1.1.1-7.1.x86_64.rpm to update, version 1.1.1 release 7.1
Adding lsof-4.84-22.1.x86_64.rpm to update, version 4.84 release 22.1
Adding vim-7.4.326-7.1.x86_64.rpm to update, version 7.4.326 release 7.1
Adding permissions-2015.09.28.1626-13.1.x86_64.rpm to update, version 2015.09.28.1626 release 13.1
Adding kbd-1.15.5-8.7.1.x86_64.rpm to update, version 1.15.5 release 8.7.1
Adding glibc-locale-2.19-38.2.x86_64.rpm to update, version 2.19 release 38.2
Adding pciutils-ids-2016.04.04-11.1.noarch.rpm to update, version 2016.04.04 release 11.1
Adding libsolv-tools-0.6.23-2.34.1.x86_64.rpm to update, version 0.6.23 release 2.34.1
Adding kexec-tools-2.0.5-17.2.x86_64.rpm to update, version 2.0.5 release 17.2
Adding pciutils-3.2.1-10.1.x86_64.rpm to update, version 3.2.1 release 10.1
Adding kmod-compat-17-8.1.x86_64.rpm to update, version 17 release 8.1
Adding aaa_base-13.2+git20140911.61c1681-25.1.x86_64.rpm to update, version 13.2+git20140911.61c1681 release 25.1
Adding netcfg-11.5-27.1.noarch.rpm to update, version 11.5 release 27.1
Adding udev-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding util-linux-systemd-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding open-vm-tools-10.0.5-3.1.x86_64.rpm to update, version 10.0.5 release 3.1
Adding lvm2-2.02.120-74.1.x86_64.rpm to update, version 2.02.120 release 74.1
Validated all sha1 sums of the various RPMs
Shutting down system services to install update
shutdown system services was successful

Updating, this may take some time
Update successful
Post script run was successful
Software update was successful.
Reboot the system, then update the vCO/vRO workflows.
```

5 Execute the `reboot` command.

NOTE Connection to the host will get closed due to the reboot. Once the VLA is up, SSH to the VLA as **root**. If you are unable to connect to the VLA via SSH, maybe the SSH service need to be started on the VLA. Follow the procedure in step 1 of this section to start the SSH service on the VLA. You will then be able to successfully SSH into the VLA.

---

6 Update the orchestrator workflows following the reboot of the VLA by executing the following command:

```
vla_vco_package_install –i
```

7 Update the VMware Adapter for SAP Landscape Management on the SAP Landscape ManagementVM (Refer "Deploying the VMware Adapter for SAP Landscape Management via the vla_adapter command," on page 74

NOTE The older VMware Adapter for SAP Landscape Management that may have been installed on the SAP Landscape Management VM using the version 1.3.1 VLA will stop working following an upgrade to version 1.4.1 VLA.

---

8 Recreate the *Tomcat* user if required. ("Create VLA Service user and password," on page 68)

NOTE Following the upgrade and reboot if you discover that the *Tomcat* vla-server is not available, based on the message on the console when you SSH to the VLA, the user password may have got cleared due to the upgrade process. Hence you will have to recreate the *Tomcat* user

---

Upon successfully completing the previous steps, you should have upgraded the VLA from version 1.3.1 to version 1.4.1

Upgrading from 1.4.0 to 1.4.1

Note Take a snapshot of the VLA before proceeding with the upgrade.

Once you have taken the snapshot of the VLA, execute the following steps to do the VLA upgrade:

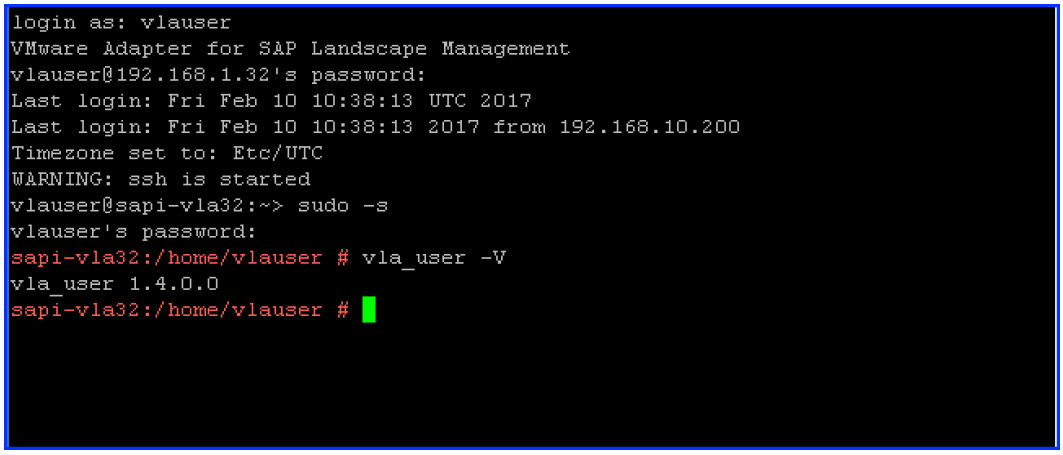
Prerequisites

You are running a stable VLA system (version 1.4.0) and have decide to upgrade it to version 1.4.1

Procedure

1 SSH to VLA system using appropriate credentials and verify the current version of the VLA using the `vla_user` command as depicted in the following figure:

Figure 3-83. SSH to VLA



2 Change directory to `/system2` on the VLA.

3 Copy the VLA ISO file that you will use to upgrade your existing VLA from http://www.vmware.com/products/adapter-sap-lvm.html into the `/system2` directory.

Note Use any tool of your choice like `wget`, `WinSCP`, `scp` etc.

4 Execute the `sys_software_update` script to initiate the upgrade process. Specify the ISO file that you copied into the `/system2` directory that will be used for upgrade of the VLA as depicted in the following figure:

Figure 3-84. VLA Upgrade - 1

```
sapi-vla32:/system2 # sys_software_update -f ./VLA_SLES12-1.4.1.0-5048654-updaterepo.iso
Mounted ISO file successfully
Manifest Version:1.4.1.0
Full Version info of upgrade: 1.4.1.0 Build 5048654
Current Version= 1.4.0.0
Current Version Full 1.4.0.0 Build 4747622
Current History
Update history:
1.4.0.0 Build 4747622 Fri Feb 10 10:53:51 UTC 2017

ISO valid for updating from 1.4.0.0 to 1.4.1.0
Adding dracut-037-84.1.x86_64.rpm to update, version 037 release 84.1
Adding bind-libs-9.9.9P1-53.1.x86_64.rpm to update, version 9.9.9P1 release 53.1
Adding bind-utils-9.9.9P1-53.1.x86_64.rpm to update, version 9.9.9P1 release 53.1
Adding libz1-1.2.8-6.3.1.x86_64.rpm to update, version 1.2.8 release 6.3.1
Adding wicked-0.6.39-28.3.1.x86_64.rpm to update, version 0.6.39 release 28.3.1
Adding rsyslog-8.4.0-13.3.1.x86_64.rpm to update, version 8.4.0 release 13.3.1
Adding libpth20-2.0.7-140.1.x86_64.rpm to update, version 2.0.7 release 140.1
Adding libpcre1-8.39-7.1.x86_64.rpm to update, version 8.39 release 7.1
Adding VMware-VLA-Server-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding Properties-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding VMware-SA-Server-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding VMware-VLA-Workflows-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding libblkid1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libmount1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libreadline6-6.2-82.1.x86_64.rpm to update, version 6.2 release 82.1
Adding tar-1.27.1-14.1.x86_64.rpm to update, version 1.27.1 release 14.1
Adding wget-1.14-17.1.x86_64.rpm to update, version 1.14 release 17.1
Adding timezone-2016j-66.1.x86_64.rpm to update, version 2016j release 66.1
Adding kmod-17-8.1.x86_64.rpm to update, version 17 release 8.1
Adding libparted0-3.1-19.3.1.x86_64.rpm to update, version 3.1 release 19.3.1
Adding sudo-1.8.10p3-2.6.1.x86_64.rpm to update, version 1.8.10p3 release 2.6.1
Adding util-linux-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding systemd-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding systemd-sysvinit-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding ntp-4.2.8p9-55.1.x86_64.rpm to update, version 4.2.8p9 release 55.1
Adding dnsmasq-2.71-13.1.x86_64.rpm to update, version 2.71 release 13.1
Adding wicked-service-0.6.39-28.3.1.x86_64.rpm to update, version 0.6.39 release 28.3.1
Adding update-alternatives-1.16.10-12.3.1.x86_64.rpm to update, version 1.16.10 release 12.3.1
Adding parted-3.1-19.3.1.x86_64.rpm to update, version 3.1 release 19.3.1
Adding kernel-default-3.12.67-60.64.24.1.x86_64.rpm to update, version 3.12.67 release 60.64.24.1
Adding libuuid1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libudev1-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding libsmartcols1-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Adding libkmod2-17-8.1.x86_64.rpm to update, version 17 release 8.1
```

Figure 3-85. VLA Upgrade -2

```
Adding Credentials-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding VMware-LVM-Adapter-1.41.1-5048654.i386.rpm to update, version 1.41.1 release 5048654
Adding VMware-VLA-VcoLogCollector-1.4.1.0-5048654.i386.rpm to update, version 1.4.1.0 release 5048654
Adding libpci3-3.2.1-10.1.x86_64.rpm to update, version 3.2.1 release 10.1
Adding bash-4.2-82.1.x86_64.rpm to update, version 4.2 release 82.1
Adding libwicked-0-6-0.6.39-28.3.1.x86_64.rpm to update, version 0.6.39 release 28.3.1
Adding hwinfo-21.38-10.3.1.x86_64.rpm to update, version 21.38 release 10.3.1
Adding dirmngr-1.1.1-7.1.x86_64.rpm to update, version 1.1.1 release 7.1
Adding vim-7.4.326-7.1.x86_64.rpm to update, version 7.4.326 release 7.1
Adding pciutils-3.2.1-10.1.x86_64.rpm to update, version 3.2.1 release 10.1
Adding kmod-compat-17-8.1.x86_64.rpm to update, version 17 release 8.1
Adding udev-210-116.3.3.x86_64.rpm to update, version 210 release 116.3.3
Adding util-linux-systemd-2.25-37.1.x86_64.rpm to update, version 2.25 release 37.1
Validated all sha1 sums of the various RPMs
Shutting down system services to install update
shutdown system services was successful

Updating, this may take some time
Update successful
Post script run was successful
Software update was successful.
Reboot the system, then update the vCO/vRO workflows.
sapi-vla32:/system2 #
```

5 Execute the `reboot` command.

Note Connection to the host will get closed due to the reboot. Once the VLA is up, try to SSH to it using the credentials you used previously in this section in step 1.

Figure 3-86. Verify the Upgrade and Reboot the VLA

6 Update the orchestrator workflows following the reboot of the VLA as follows:

```
vla_vco_package_install –i
```

Upon successfully completing the previous steps, you should have upgraded the VLA from version 1.4.0 to version 1.4.1

Upgrading from 1.4.1 to 1.5.0

Note Take a snapshot of the VLA before proceeding with the upgrade.

Once you have taken the snapshot of the VLA, execute the following steps to do the VLA upgrade:

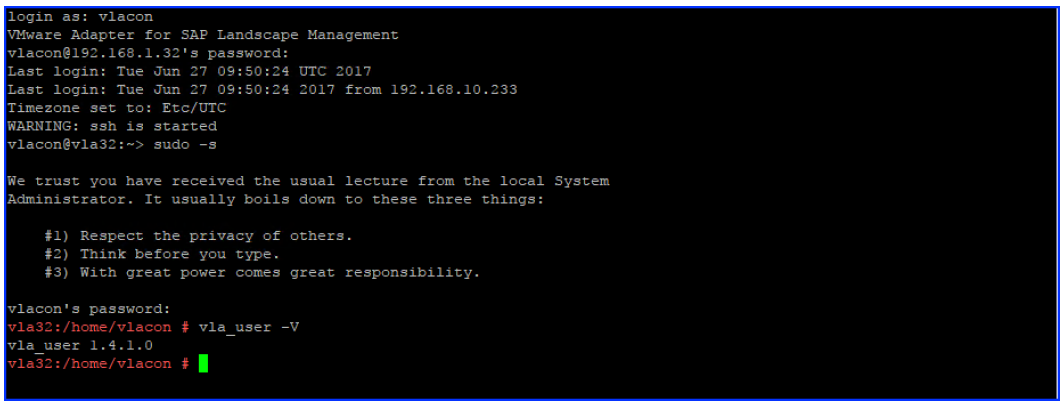
Prerequisites

You are running a stable VLA system (version 1.4.1) and have decide to upgrade it to version 1.5.0

Procedure

1 SSH to VLA system using appropriate credentials and verify the current version of the VLA using the `vla_user` command as depicted in the following figure:

Figure 3-87. SSH to VLA



2 Change directory to`/system2` on the VLA.

3 Copy the VLA ISO file that you will use to upgrade your existing VLA from http://www.vmware.com/products/adapter-sap-lvm.html into the `/system2` directory.

Note Use any tool of your choice like `wget`, `WinSCP`, `scp` etc.

4 Execute the `sys_software_update` script to initiate the upgrade process. Specify the ISO file that you copied into the `/system2` directory that will be used for upgrade of the VLA as depicted in the following figure:

Figure 3-88. VLA Upgrade - 1

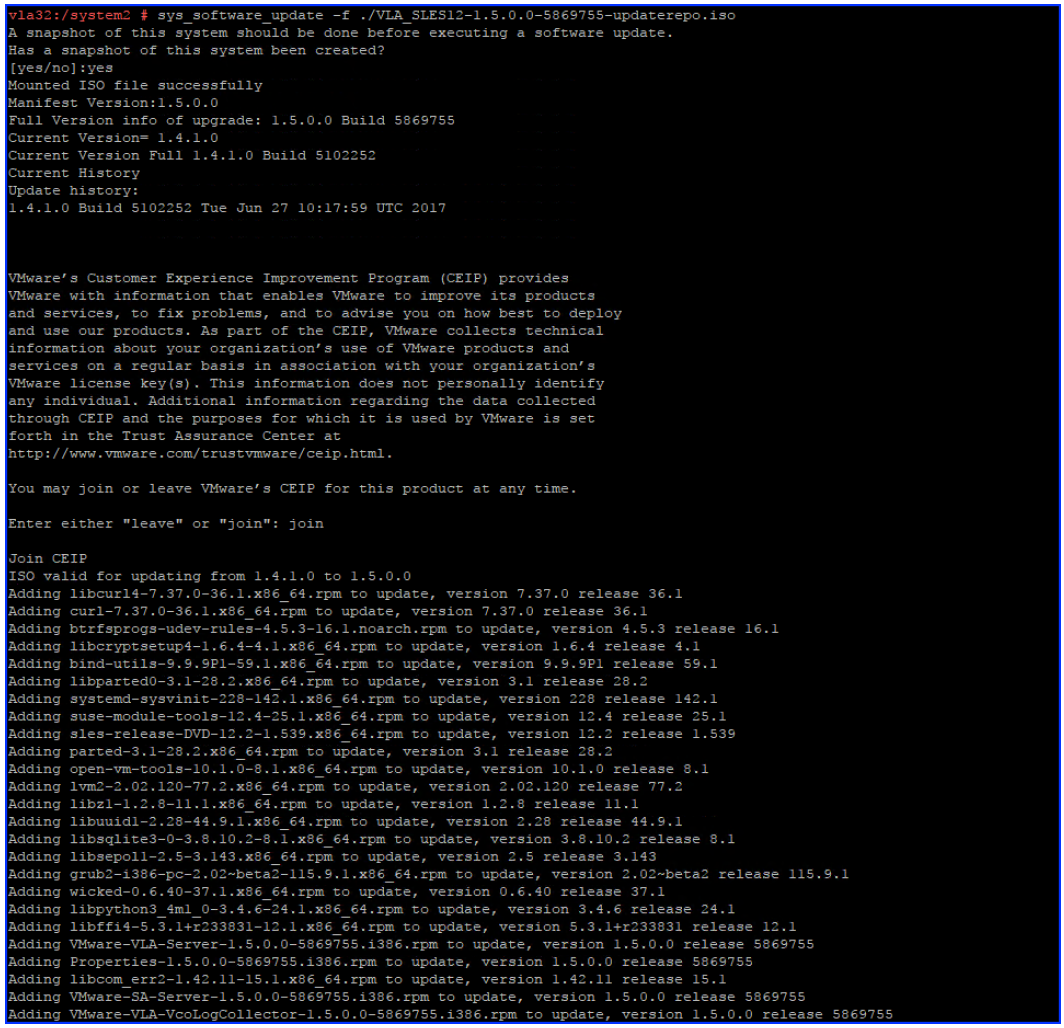


Figure 3-89. VLA Upgrade -2

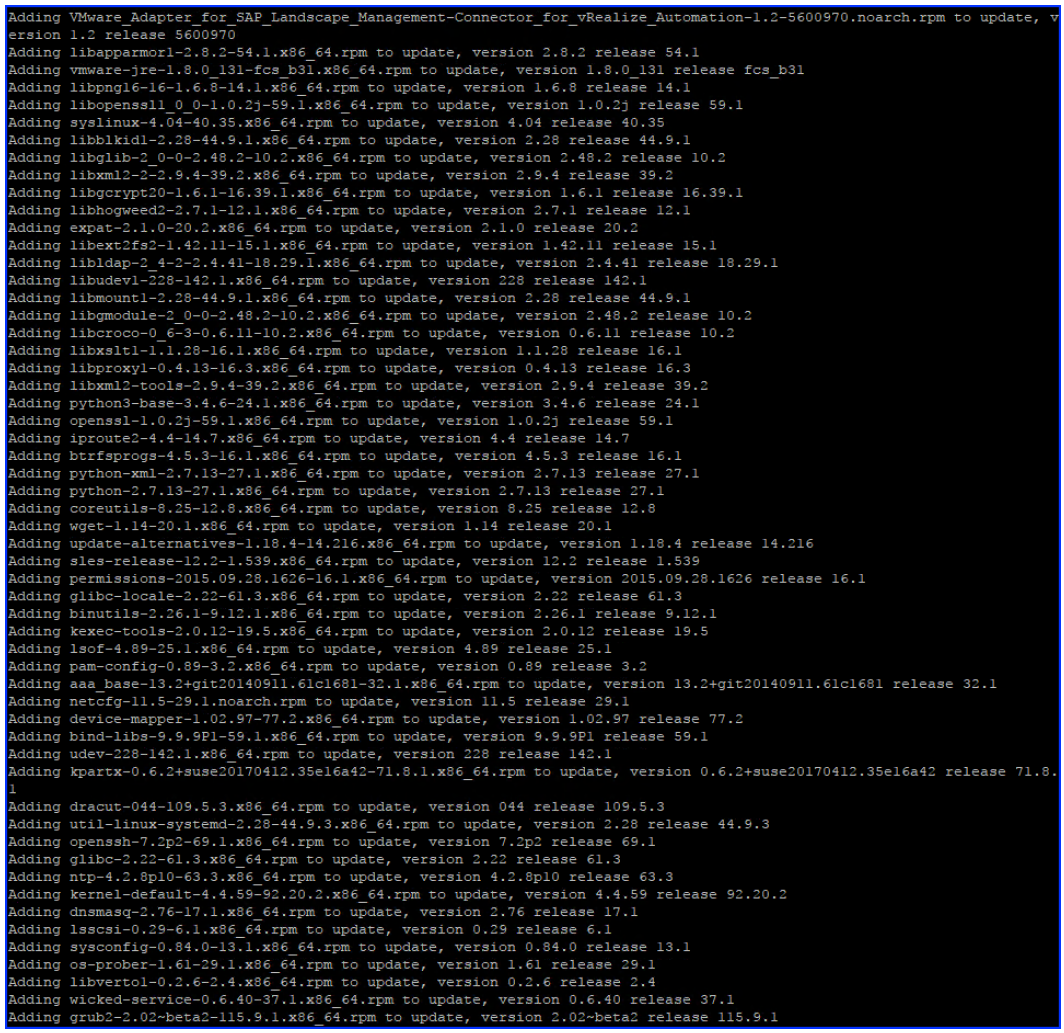
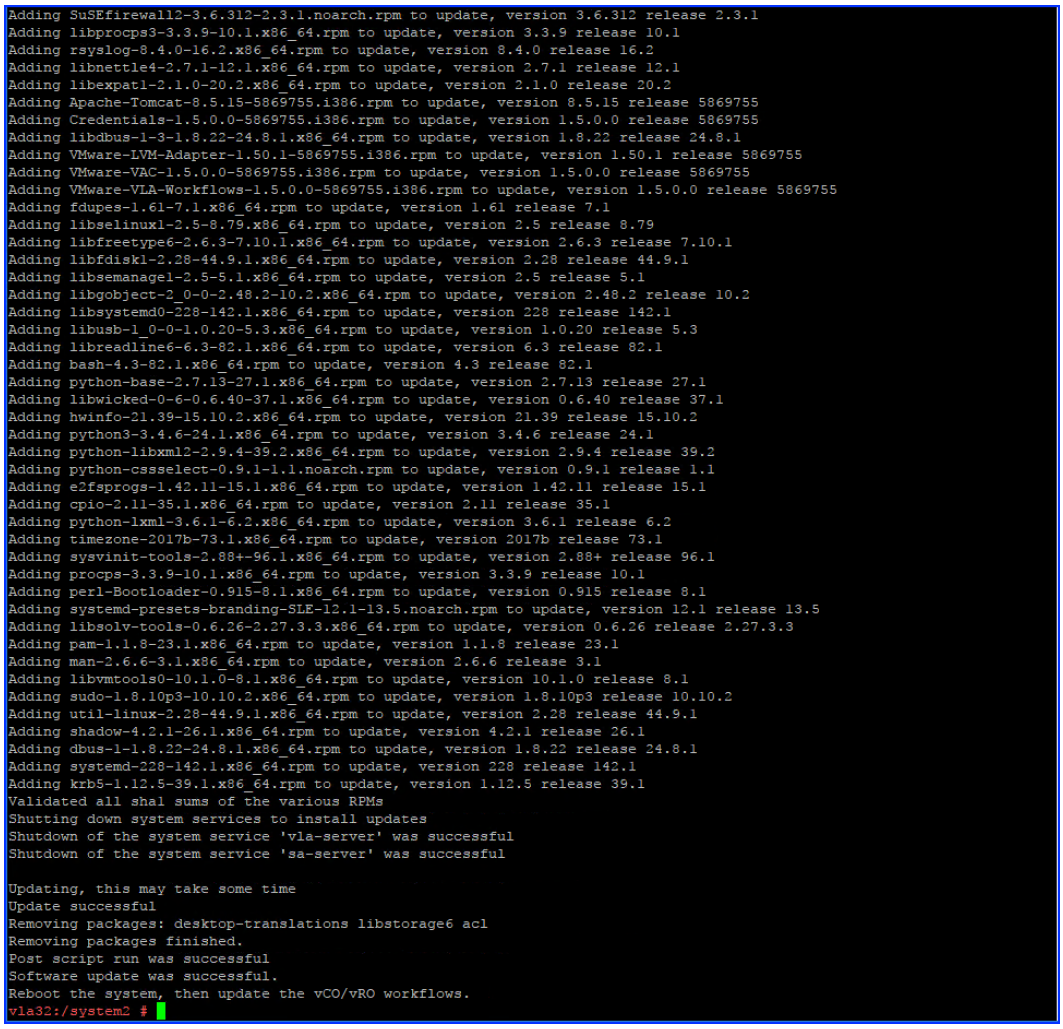


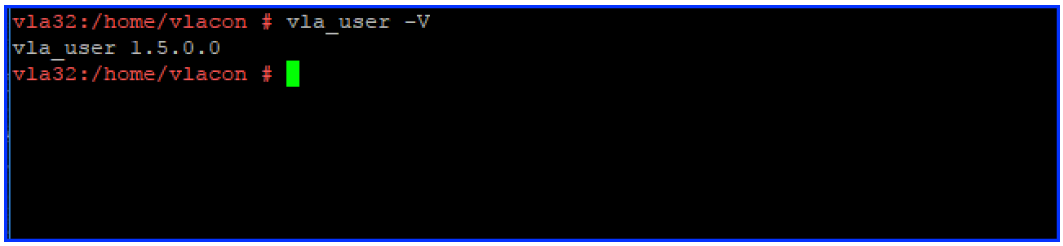
Figure 3-90. VLA Upgrade-3



5 Execute the `reboot` command.

Note Connection to the host will get closed due to the reboot. Once the VLA is up, try to SSH to it using the credentials you used previously in this section in step 1.

Figure 3-91. Verify the Upgrade and Reboot the VLA



6 Update the orchestrator workflows following the reboot of the VLA as follows:

```
vla_vco_package_install -i
```

Upon successfully completing the previous steps, you should have upgraded the VLA from version 1.4.1 to version 1.5.0

Upgrading from 1.5.0 to 1.5.1

Note Take a snapshot of the VLA before proceeding with the upgrade.

Once you have taken the snapshot of the VLA, execute the following steps to do the VLA upgrade:

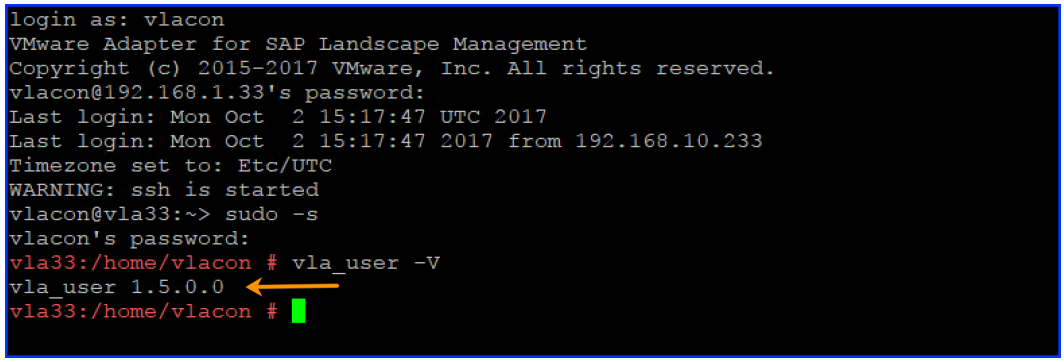
Prerequisites

You are running a stable VLA system (version 1.5.0) and have decide to upgrade it to version 1.5.1

Procedure

1 SSH to VLA system using appropriate credentials and verify the current version of the VLA using the `vla_user` command as depicted in the following figure:

Figure 3-92. SSH to VLA



2 Change directory to `/system2` on the VLA.

3 Copy the VLA ISO file that you will use to upgrade your existing VLA from http://www.vmware.com/products/adapter-sap-lvm.html into the `/system2` directory.

Note Use any tool of your choice like `wget`, `WinSCP`, `scp` etc.

4 Execute the `sys_software_update` script to initiate the upgrade process. Specify the ISO file that you copied into the `/system2` directory that will be used for upgrade of the VLA as depicted in the following figure (the exact update and version number may be slightly different from what is depicted in the screenshot):

Figure 3-93. VLA Upgrade - 1

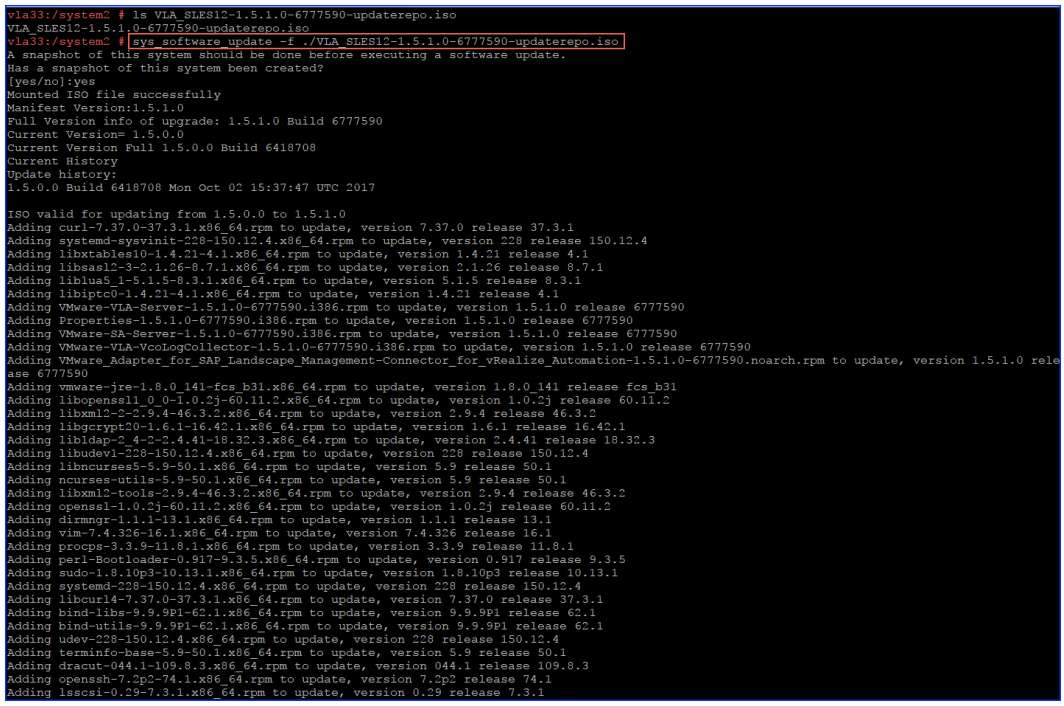
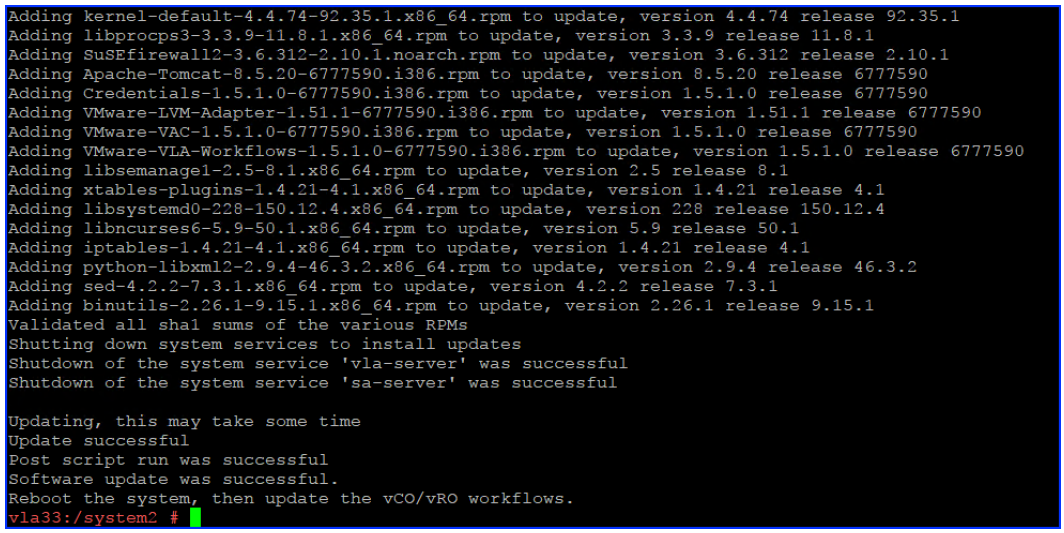


Figure 3-94.



5 Execute the `reboot` command.

NOTE Connection to the host will get closed due to the reboot. Once the VLA is up, try to SSH to it using the credentials you used previously in this section in step 1.

Figure 3-95. Verify the Upgrade and Reboot the VLA

6 Update the orchestrator workflows following the reboot of the VLA as follows:

```
vla_vco_package_install -i
```

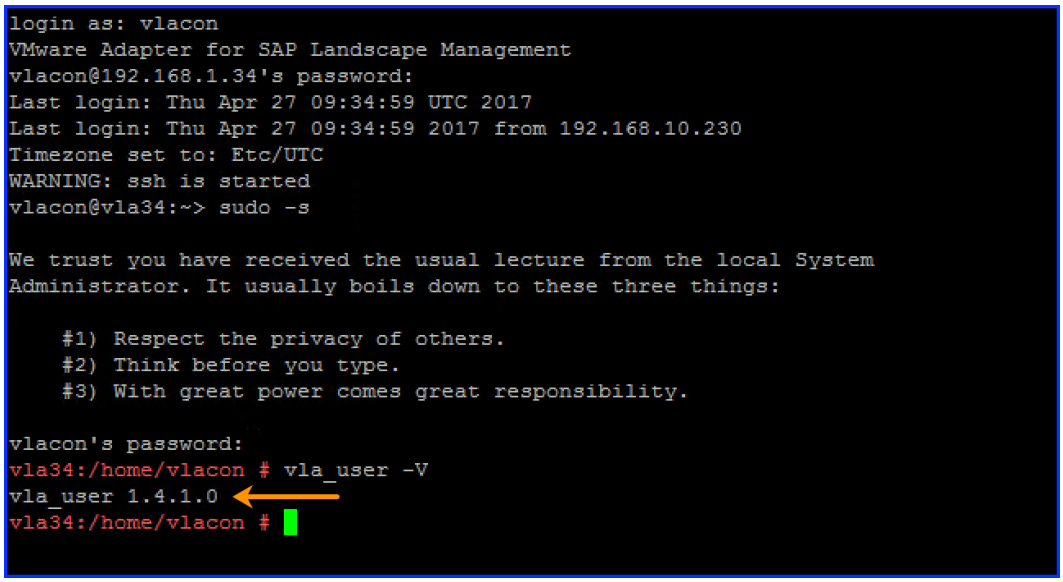
Upon successfully completing the previous steps, you should have upgraded the VLA from version 1.5.0 to version 1.5.1

Join or Leave CEIP during VLA Upgrade

Procedure

1 SSH to the VLA system using appropriate credentials and verify the current version of the VLA using the `vla_user` command as depicted in the following figure:

Figure 3-96. SSH to VLA



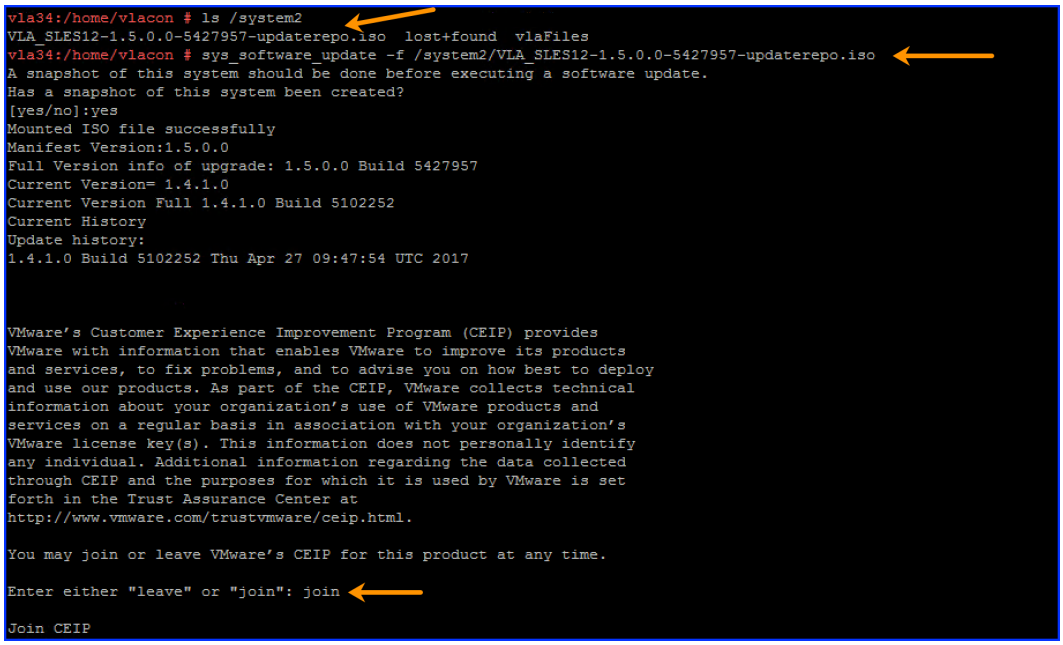
2 Change directory to `/system2` on the VLA.

3 Copy the VLA ISO file that you will use to upgrade your existing VLA from http://www.vmware.com/products/adapter-sap-lvm.html into the `/system2` directory.

NOTE Use any tool of your choice like `wget`, `WinSCP`, `scp` etc.

4 Execute the `sys_software_update` script to initiate the upgrade process. Specify the ISO file that you copied into the `/system2` directory that will be used for upgrade of the VLA as depicted in the following figure:

Figure 3-97. VLA Upgrade-1



NOTE The build number of the ISO file that you will be using for upgrade will be different than the one demonstrated in the preceding figure

5 Choose whether to participate in the VMware CEIP or not by typing in **join** or **leave** respectively as part of upgrade, as depicted in the preceding figure.

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your organization's VMware license key(s). This information does not personally identify any individual.

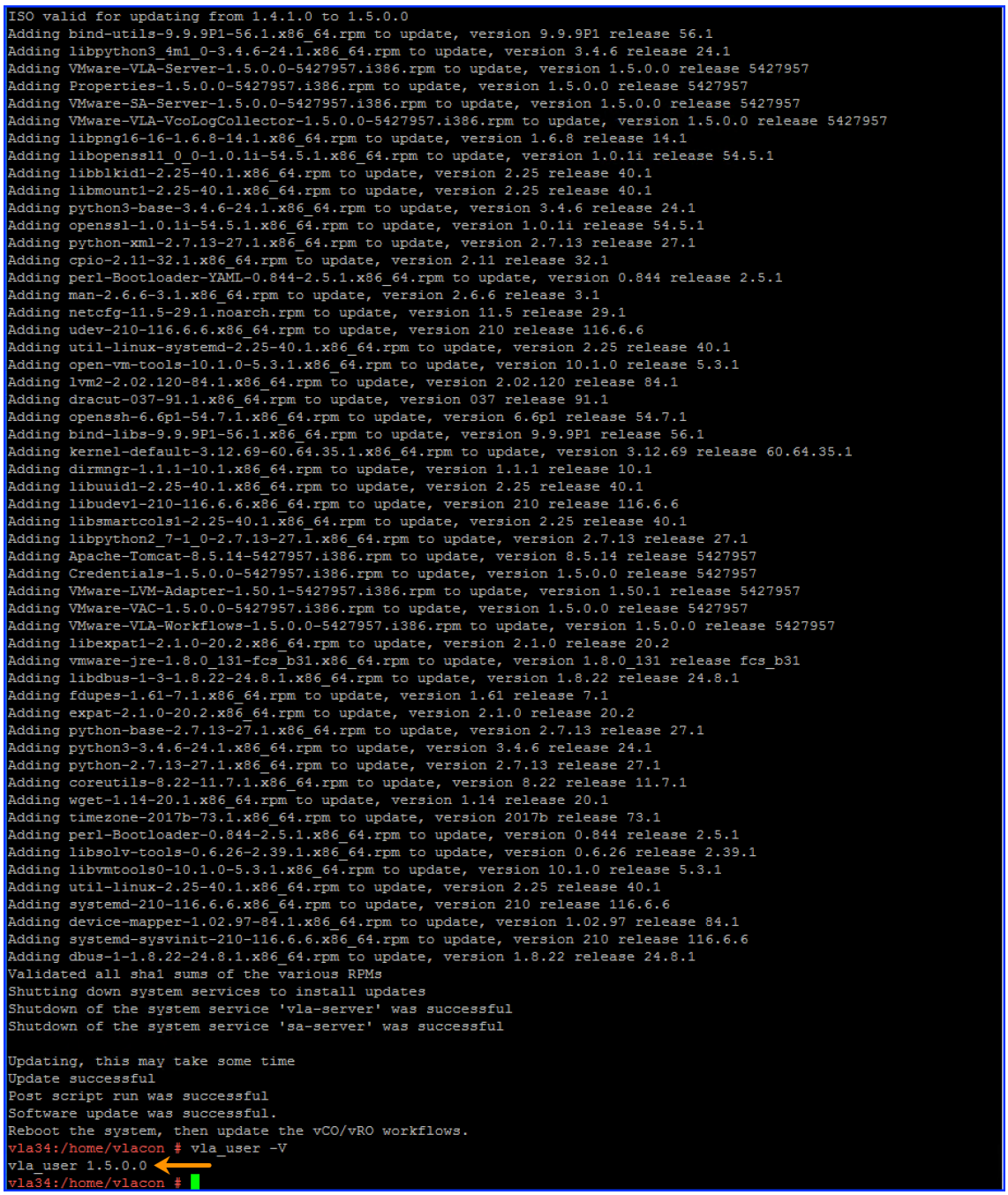
Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at `http://www.vmware.com/trustvmware/ceip.html`.

- If you prefer not to participate in VMware's CEIP for this product, you should type **leave**.
- If you wish to participate in VMware's CEIP for this product, you should type **join**.

You may **join** or **leave** VMware's CEIP for this product at any time.

6 Verify the upgraded version of the VLA upon successful completion of the upgrade process using the `vla_user` command as depicted in the following figure:

Figure 3-98. VLA Upgrade-2



Backup and Restore of Configuration 4

The VLA configuration and settings can be stored in a file for backup purposes. This file can be used to restore VLA configuration and settings. The VLA backup file includes:

- LaMa service settings - web server configuration, credentials database, key store, LaMa User account.
- System Settings - network settings, OS accounts and server certificate.

This chapter includes the following topics:

Backup the Configuration

The LaMa Service Dashboard allows you to make a backup of the VLA configuration:

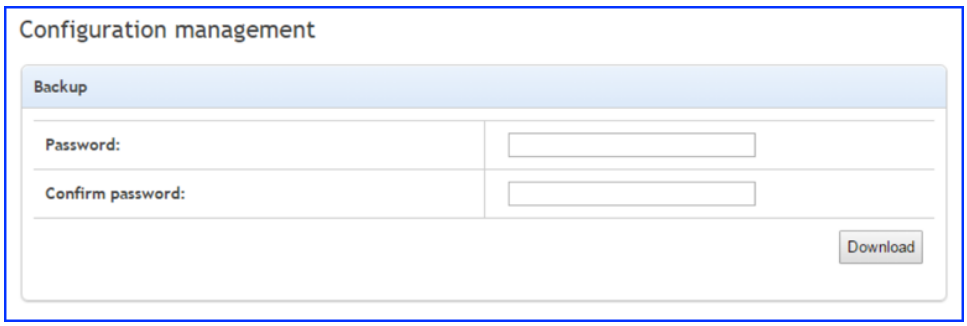
Procedure

1 In a new browser window or tab enter the URL for the LaMa Service Dashboard page on the Tomcat instance, for example: https://vla_hostname_or_IP:8443/vla/dashboard, where `<vla_hostname_or_IP>` is the FQDN or IP address of VLA.

2 You may be prompted with a certificate warning. Accept the warning and proceed to the dashboard landing page.

3 Scroll to the Backup heading of the Configuration management section.

Figure 4-1. Configuration Management

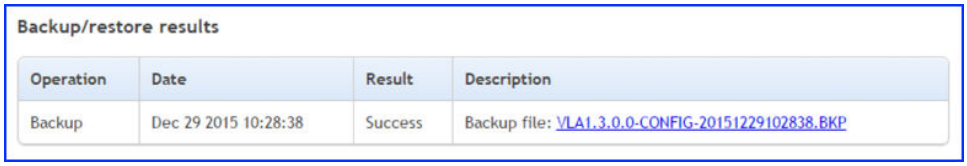


4 Enter password for the backup file. The password must be at least 8 characters long and must contain at least: an upper case letter, a lower case letter, a number, a special character. Click **Download**.

5 Verify that the backup file VLA<version>-CONFIG-<date and time>. BKP is successfully downloaded.

6 In addition, you can see the results in the Backup/restore results section of the dashboard page.

Figure 4-2. Backup/Restore Results



Restore the Configuration using the LaMa Service Dashboard

The LaMa Service Dashboard allows you to Restore VLA configuration:

Prerequisites

To restore the VLA configuration, you will need to provide a VLA backup file. The backup file contains configuration and settings of the VLA.

Procedure

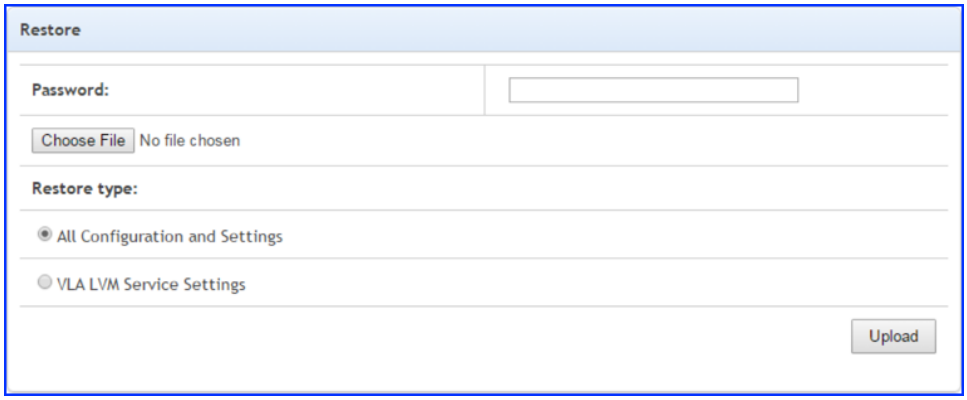
1 In a new browser window or tab enter the URL for the LaMa Service Dashboard page on the Tomcat instance, for example: https://<vla_hostname_or_IP>:8443/vla/dashboard , where `<vla_hostname_or_IP>` is the FQDN or IP address of VLA.

2 You may be prompted with a certificate warning. Accept the warning and proceed to the dashboard landing page.

3 Enter the LaMa Service username and password. This opens the dashboard.

4 Scroll to the Restore heading of the Configuration Management section.

Figure 4-3. Restore



5 Click **Choose File** and select the backup file.

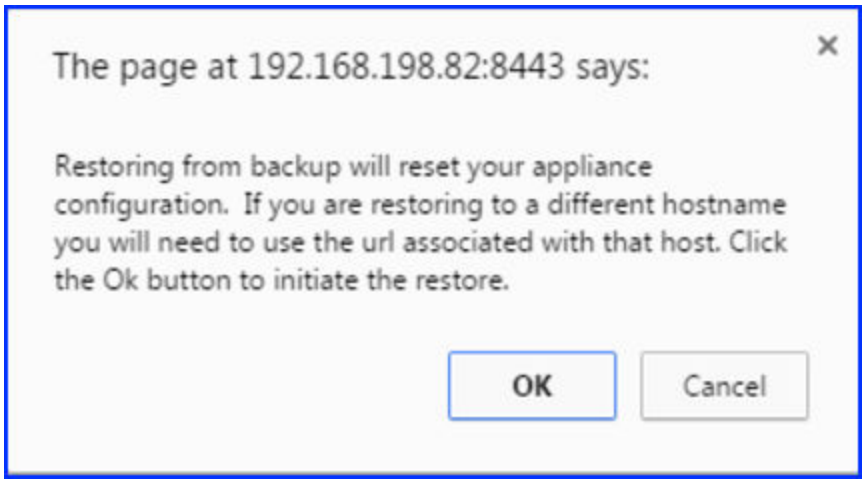
6 Enter the password for the backup file.

7 Select the Restore type:

- **All Configuration and Settings** includes the VLA LaMa Service Settings along with the system settings, network settings, accounts and server certificate.
- VLA LaMa Service Settings includes web server configuration, credentials database, the key store and LaMa user account.

8 Click Upload to start the restore process.

Figure 4-4. Restore Process



9 The browser now displays a confirmation dialog. Click **OK** if you want to restore the settings.

10 You can see the results in the Backup/restore results section of the dashboard page.

Figure 4-5. Backup / Restore Results

Backup VLA using Snapshot

When you use the Backup functionality of the VLA from the *LaMa Service Dashboard* page, only a few mutable files get saved. Suppose you take a backup of the VM (say VLA) using the said method. Subsequently, some of these mutable files and a few other config files happen to change. Now when you use the Restore functionality of the VLA from the *LaMa Service Dashboard* page, note that only the mutable files that was backed up previously will get restored. You may discover that the VLA is unable to run following the restore. You can avoid this situation by taking a backup of the VLA using snapshots. For details on using snapshots to manage a virtual machine refer to https://pubs.vmware.com/vsphere-55/index.jsp?topic=%2Fcom.vmware.vsphere.html.hostclient.doc%2FGUID-CA948C69-7F58-4519-AEB1-739545EA94E5.html.

Troubleshooting 5

This chapter includes the following topics:

Log Locations

```
VLA application log : /var/log/apache-tomcat/vla.log
Tomcat server log   : /var/log/apache-tomcat/catalina.vla-server.out
Tomcat access log   : /var/log/apache-tomcat/access.vla-server.log
```

Permanently enable SSH

If you want to permanently enable the SSH service, type the following commands at a prompt:

```
$ sudo -s
# sys_ssh -s START
```

To permanently disable the SSH:

```
$ sudo -s
# sys_ssh -s STOP
```

Uninstall the VMware Adapter for SAP Landscape Management

To uninstall a previous version of the VMware Adapter for SAP Landscape Management installed on your LaMa server:

1 Verify that LaMa is up and running.

2 Log into the LaMa server.

3 Log in to SAP NetWeaver Java Server using the Telnet to port 5000N where N = instance number of the Telnet for the Java Server. For example:

```
# telnet localhost 50008
```

4 Enter the administrator username and password.

5 Run the following command to see if adapter is already installed:

```
> list_app | grep VMwareLVM
```

6 If the adapter appears in the list, then it has been installed.

7 Run the following command to uninstall the adapter:

```
> undeploy name=VMwareLVM vendor=JavaEE on_undeploy_error=stop
```

8 Run the following command to verify that the adapter is uninstalled:

```
> list_app | grep VMware
```

9 If the adapter does not appear in the list, then it has been uninstalled.

10 Exit from `telnet`.

Service Cipher Suites

VM Service has two sets of cipher suites: "**Strong**" and "**Weak**". Strong suites are enabled by default.

Table 5-1.

Strong	Weak
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_3DES_EDE_CBC_SHA	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_ECDSA_WITH_RC4_128_SHA, TLS_ECDH_ECDSA_WITH_RC4_128_SHA, TLS_ECDHE_RSA_WITH_RC4_128_SHA, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDH_RSA_WITH_RC4_128_SHA, SSL_RSA_WITH_RC4_128_SHA

To change the cipher suites, use the following commands:

1 `vla_tomcat_cipher` -s STRONG to set "Strong" cipher suites

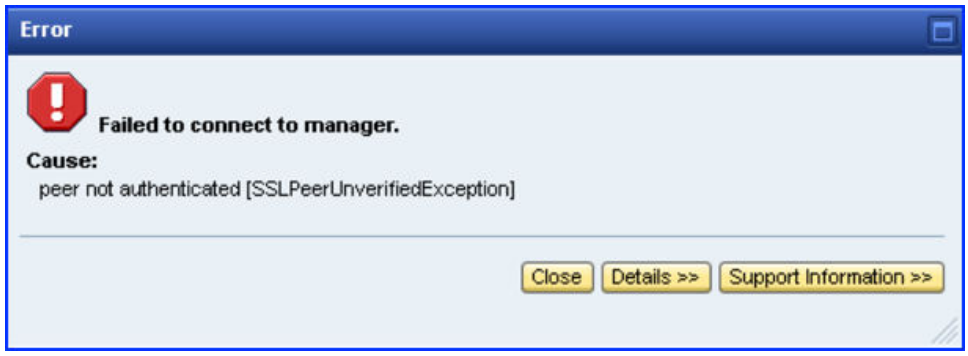
2 `vla_tomcat_cipher` -s WEAK to set "Weak" cipher suites

3 `vla_tomcat_cipher` -g to see the enabled set of cipher suites

Issues and Errors

Peer not authenticated [SSLPeerUnverifiedException]

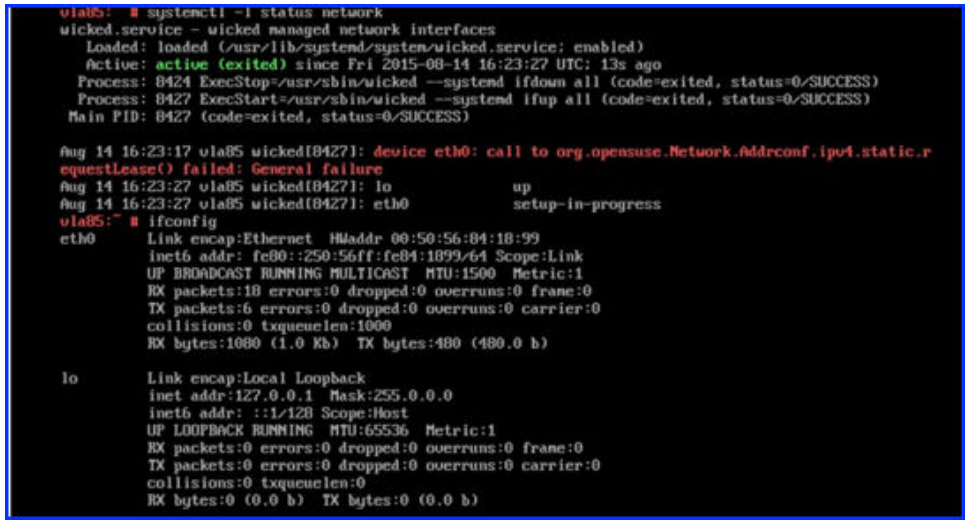
This error could happen during connection test or infrastructure retrieval.



Possible reasons are invalid VLA Server Certificate. Make sure 'Certificate Authority Selection' check box is enabled.

Wicked fails during network configuration

This error can happen during network configuration.



Possible reason: invalid IP address.

Certificate Checker: Check is completed with errors

This error occurs when adding/modifying VMware vRealize Orchestrator or vCenter Server connection

Possible reason: The Certificate Checker checks the server's certificate. If it finds an error, it will prevent the addition of the VMware vRealize Orchestrator or vCenter Server connection to the appliance.

The most common reason for this error is that the VMware vRealize Orchestrator or vCenter Server is using its default certificate. To change this default use, you have the option of regenerating the server certificate and trying to add the server to the appliance.

- For regenerating the vCenter Server certificate, refer to these knowledge base articles:
  - vCenter 5.5: Deploying and using the SSL Certificate Automation Tool 5.5
  - vCenter 6.0: Regenerating the vSphere 6.0 certificates using a new self-signed VMware Certificate Authority certificate

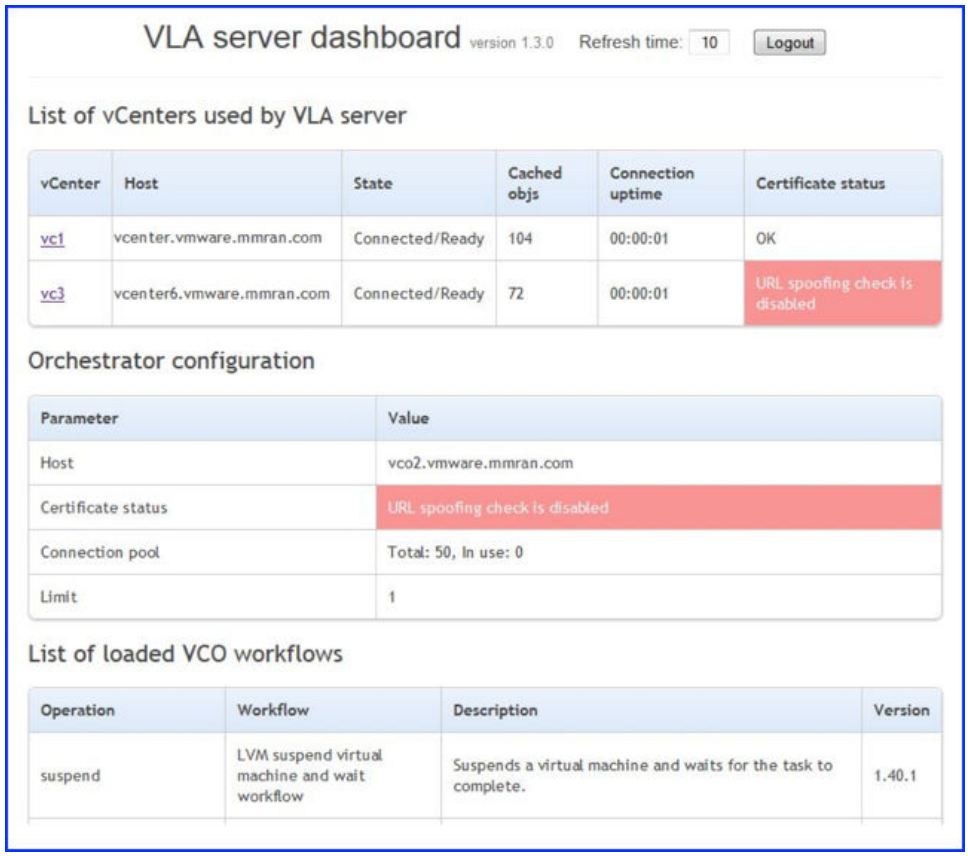
You also have the option to override the Certificate Checker by using the -f flag of the `vla_credentials` script. To add a VMware vRealize Orchestrator or vCenter Server connection at the command line, use this command, where `ServerType` is `vco` or `vcenter`:

```
vla_credentials –a –f -s ServerType –u Username –n FQDN_of_server
```

For example, this command would be for a VMware vRealize Orchestrator connection:

```
# vla_credentials -a -f -s vco -u administrator@vsphere.local –n sapi–vco.example.com
```

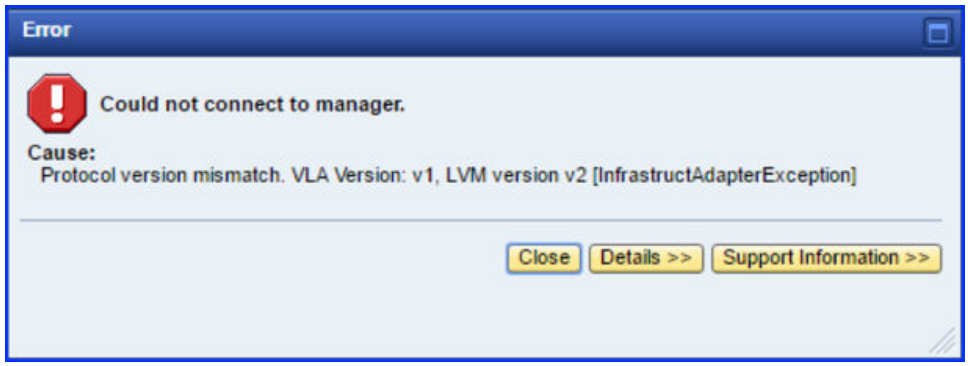
URL spoofing check is disabled in certificate status



Possible reason: VMware vRealize Orchestrator or vCenter Server connection is added to VLA Server by using the -f option of the `vla_credentials` script. For more information, run the command `vla_credentials –h`.

Protocol version mismatch

Error message: Could not connect to manager. Cause: Protocol version mismatch.



This error occurs when the LaMa adapter is incompatible with the VLA server. To fix this issue you need to upgrade the VLA server.

Supplement 6

This chapter includes the following topics:

Add a new Admin user to VLA

The first step is to log into the VLA Appliance via the console. Since SSH is disabled by default, you must use the console. The root login for VLA has been removed. You add a new admin user (non root user with sudo privileges) using the steps mentioned below :

1 Select the new VLA Appliance object in thevSphere Web Client, switch to the summary tab, and select **Launch Remote Console**.

2 A new browser window or tab should open. The VLA console should be available. Login using the console username and password that you provided when you deployed the VLA.

```
Welcome to VMware LaMa Appliance for SAP
sapi-vla31 login:
Password:
```

3 Execute the "sudo –s" command to enable yourself to run programs with security privileges of the root or superuser. You are prompted to enter your password.

```
# sudo –s
```

4 Use the useradd command to add a new non-root user with sudo privileges. Choose an appropriate username for the new user you are trying to add.

```
useradd -m -d /home/<username> –s /bin/bash -c "<description of user account>" -G
users,wheel <username>
```

5 Set a password for the new user you just added using the `passwd` command. You need to enter the password twice following which you get the "Password Changed" prompt.

```
# passwd <username>
# New password:
# Retype new password:
```

Setting up a strong password for VLA Admin user

You are recommended to setup a strong password for the VLA admin user account. Password could be at least 8 characters in length comprising of letters (uppercase/lowercase), numbers and symbols. The steps to change the password at any time is mentioned below :

1 Login using the VLA console using your username and password.

```
Welcome to VMware LaMa Appliance for SAP
sapi-vla31 login:
Password:
```

2 Execute the "`sudo` –s" command to enable yourself to run programs with security privileges of the root or superuser. You are prompted to enter your password.

```
# sudo –s
```

3 Enter the passwd command to configure a new password.

```
# passwd <admin_username>
```

4 You are required to type in the new password twice. The recommendation is to choose strong and meaningful passwords .

5 Enter the exit command to come out of the privileged mode.

```
# exit
```

To check the version of the build that you are currently running

Execute this command from the VLA Appliance console

```
sapi-vla31:/home/username # sudo sys_software_update -g
Current Version = 1.4.0.0 Build <build_number>
```

Role Privilege Settings - VMware VLA Role for VMware vRealize Orchestrator

This section defines the various privilege the you must set for different LaMa operations, when you create a VMware VLA Role in vCenter Server for VMware vRealize Orchestrator

Table 6-1. Role Privileges

LaMa Operation	Privileges
Activate VM	Global-> Log event Virtual Machine-> Interaction-> Power On
Deactivate VM	Global-> Log event Virtual Machine-> Interaction-> Power Off
Suspend VM	Global-> Log event Virtual Machine-> Interaction-> Suspend

Table 6-1. Role Privileges (Continued)

LaMa Operation	Privileges
Migrate	Datastore-> Allocate space Global-> Log event Network-> Assign network Resource-> Assign VM to resource pool Resource-> Migrate powered off VM Resource-> Migrate powered on VM Virtual Machine-> Configuration-> Settings
Provision Virtual Host	Datastore-> Allocate space Global-> Log event Network-> Assign network Resource-> Assign VM to resource pool Virtual Machine-> Configuration-> Modify device settings Virtual Machine-> Interaction-> Power On Virtual Machine-> Inventory-> Create from existing Virtual Machine-> Provisioning-> Clone VM Virtual Machine-> Provisioning-> Customize Virtual Machine-> Provisioning-> Deploy template Virtual Machine-> Provisioning-> Mark as template Virtual Machine-> Provisioning-> Mark as VM Virtual Machine-> Provisioning-> Read customization specifications Virtual Machine-> Snapshot management-> Create snapshot Virtual Machine-> Snapshot management-> Remove snapshot
Provision SAP system	Datastore-> Allocate space Global-> Log event Network-> Assign network Resource-> Assign VM to resource pool Virtual Machine-> Configuration-> Modify device settings Virtual Machine-> Interaction-> Power On Virtual Machine-> Inventory-> Create from existing Virtual Machine-> Provisioning-> Clone VM Virtual Machine-> Provisioning-> Customize Virtual Machine-> Provisioning-> Read customization specifications Virtual Machine-> Snapshot management-> Create snapshot Virtual Machine-> Snapshot management-> Remove snapshot Virtual Machine-> Snapshot management-> Revert to snapshot
Destroy SAP System	Global-> Log event Virtual Machine-> Interaction-> Power Off Virtual Machine-> Inventory-> Remove

Change Participation Preference CEIP (CLI Method)

You can change the participation preference to CEIP from the command line using the `vla_user_property` command.

Procedure

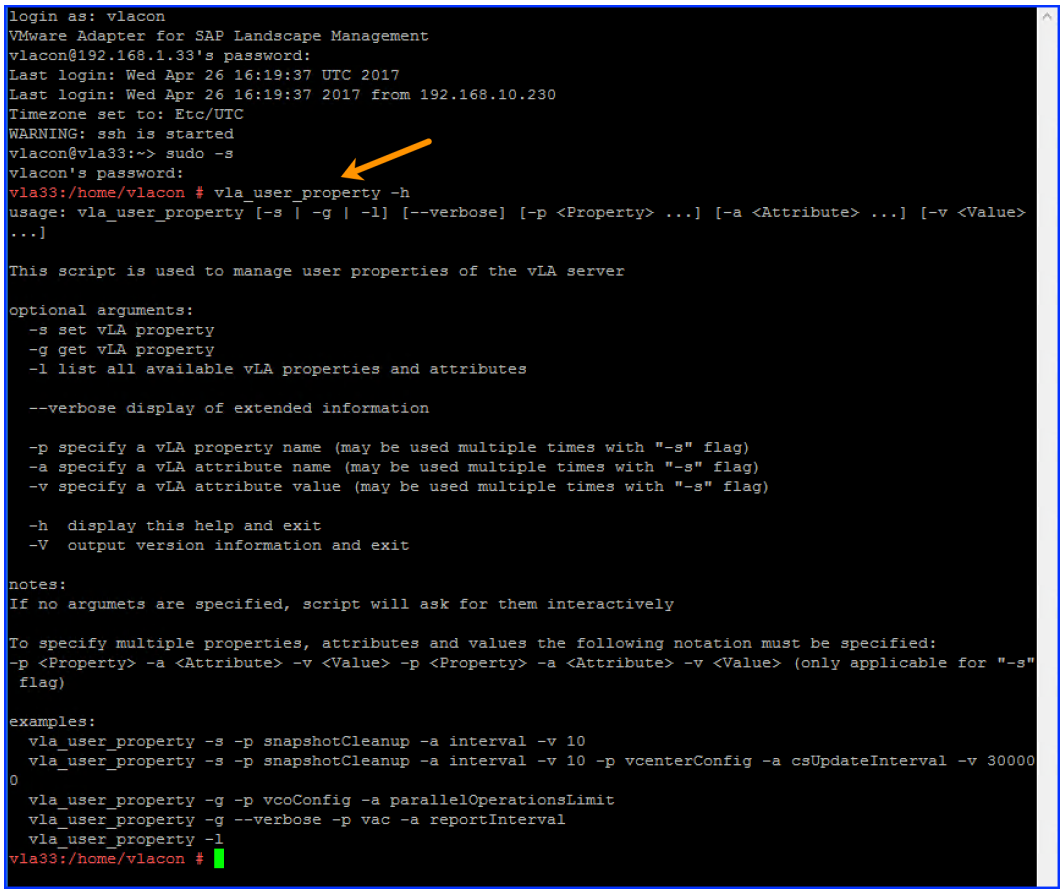
1 Go to the VLA console window using appropriate credentials

2 Execute the `sudo` command to get administrative access. This is needed to be able to execute the subsequent steps. You are prompted for the password. Enter the console user password that you provided when deploying the VLA

```
sudo –s
```

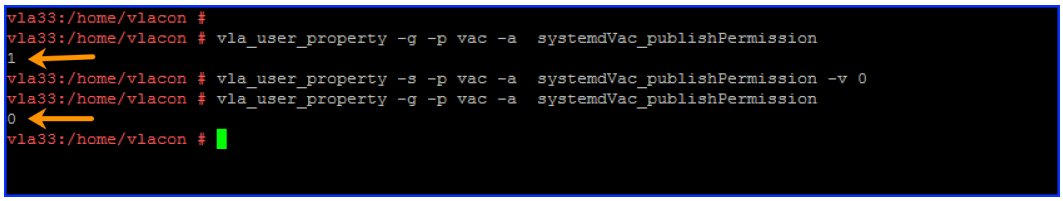
3 Explore the help available for the `vla_user_property` command that you use to change your CEIP participation preference, as depicted in the following figure:

Figure 6-1. VLA Console Login



4 Use the `vla_user_property` command with **-g** (get) option to get your current participation preference to CEIP. Use the **-s** (set) option to change your participation preference to CEIP as shown in the following figure:

Figure 6-2. Changing the CEIP Participation Preference



NOTE

- An output of **1** for the `vla_user_property` command with **-g** (get) option indicates that the current participation preference to CEIP is **Join**.
- An output of **0** for the `vla_user_property` command with **-g** (get) option indicated that the current participation preference to CEIP is **Leave**.
- Use the -l (list) option to list out all available VLA properties and attributes

You are able to successfully change your participation preference to CEIP from the command line.

Change Participation Preference to CEIP (GUI Method)

Procedure

1 Power on your VLA appliance, if it is not already **ON**

2 Create a user that you subsequently use to authenticate to the VLA appliance's web interface, the **VLA server dashboard**.

a Execute steps 1, 2, 3 and 4 from section "Create VLA Service user and password," on page 68

3 Login to the VLA server dashboard

a Open a new browser window or tab

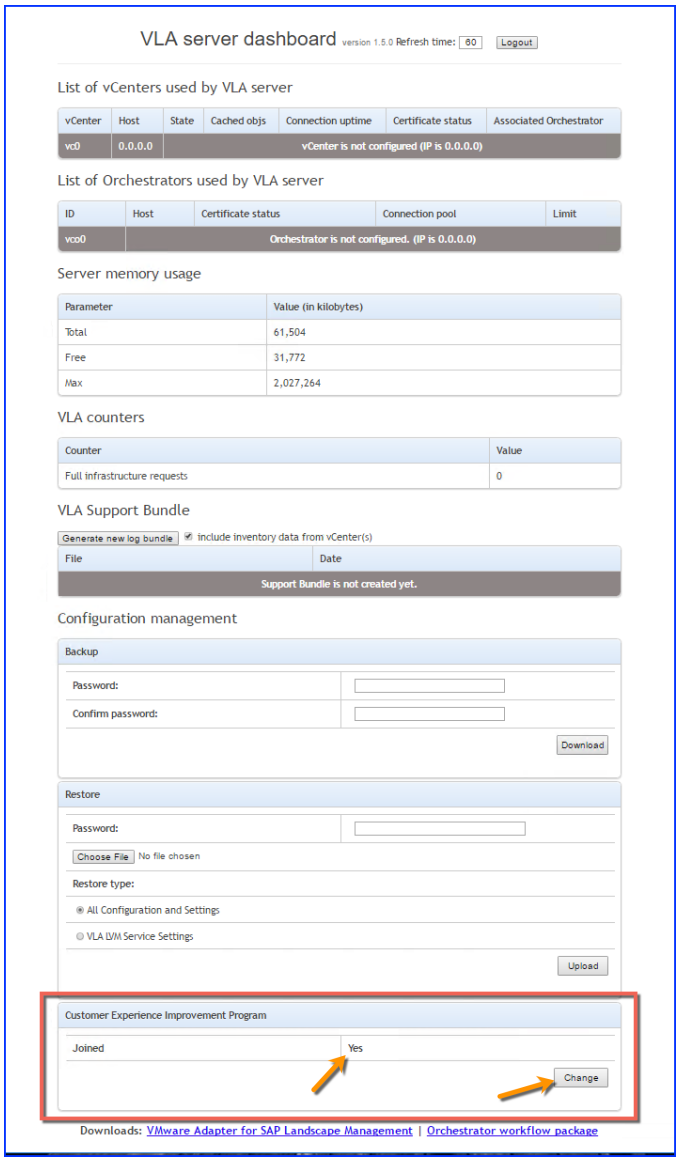
b Type the URL of the VLA server dashboard on the Tomcat instance:

```
https://<vla_hostname or IP>:8443/vla/dashboard ,
using either the FQDN vla_hostname or the IPv4 address of the VLA
```

c Accept the certificate warning, if prompted

d Type in your VLA service username and password that you set in step 2 in this section. The browser displays a page similar to the following:

Figure 6-3. VLA server dashboard



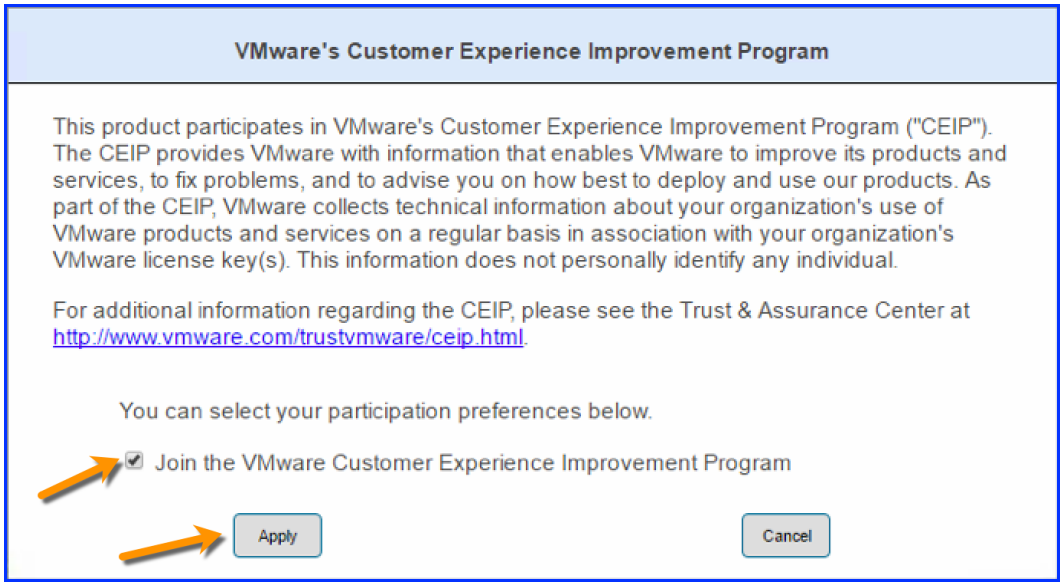
The CEIP section on the VLA server dashboard (highlighted for reference in the preceding figure) depicts the current status of the participation preference of this user to CEIP as **Joined**

4 Execute the following steps to change the participation preference to CEIP of this product:

a Click on **Change** (highlighted with arrow for reference in the preceding figure) to change the participation preference

The browser opens a window similar to the following where you can either **Check** or **Uncheck** your participation to either **Join** or **Leave** CEIP, respectively.

Figure 6-4. Select CEIP participation preference



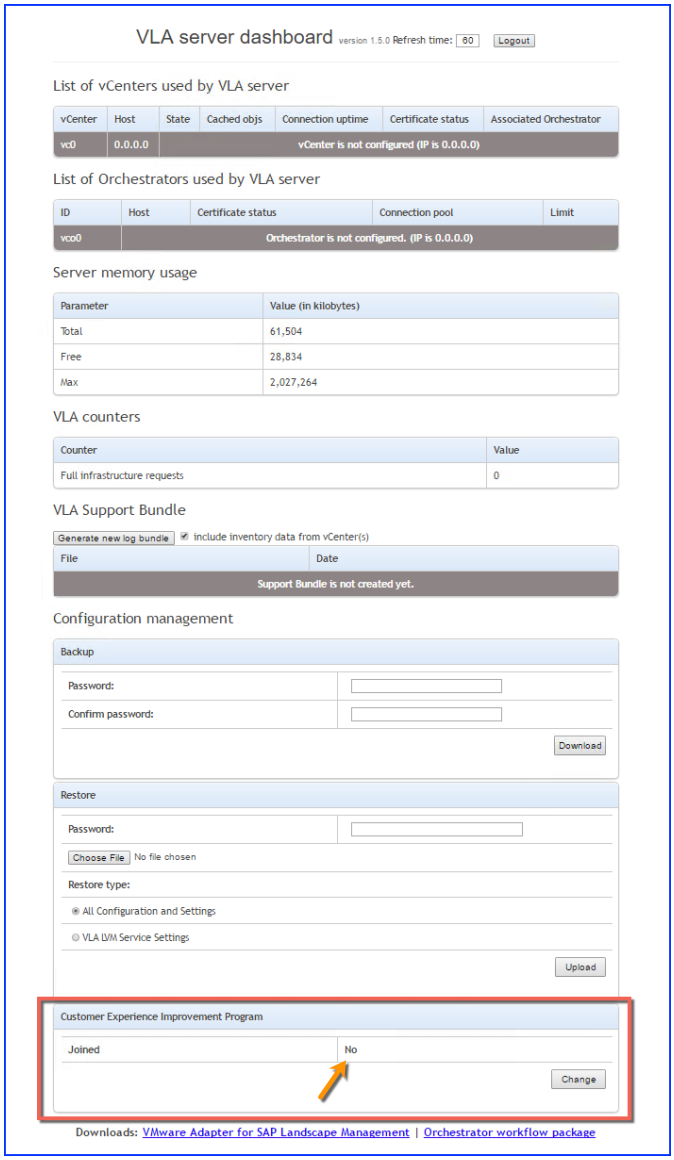
b Click on the Check box against **Join the VMware Customer Experience Improvement Program** to Leave the CEIP of this product.

For example, your CEIP Joined status currently showed as **Yes** as per step 3 in this section. You should see the Check box as **Checked** in the preceding figure, initially. You can then change your participation preference in order to **Leave** the CEIP by **Unchecking** the Check box (highlighted with arrow in the preceding figure).

c Click on **Apply** to confirm the change

The VLA server dashboard now depicts the CEIP Joined status as **No** (highlighted for reference) as shown in the following figure:

Figure 6-5. CEIP Participation Preference Changes



This means that you have chosen to Leave the CEIP for this product, as of now.

You have viewed your current CEIP participation preference on the VLA server dashboard and understand the steps to execute to change it.

Consistent Network Device Naming (CNDN)

Modern server platforms support an increasing number of network interface ports on the motherboard (Lan-on-Motherboard or LOM) in addition to numerous add-in (single and multiport) adapters. Traditionally, network interfaces are enumerated as eth[012...], but these names do not necessarily correspond to the actual labels as seen on the chassis. This new naming convention assigns names to network interfaces based on their physical location, whether embedded or in PCI slots. By converting to this naming convention, system administrators will no longer have to guess at the physical location of a network port, or modify each system to rename them into some consistent order.

In this classic naming scheme for network interfaces, the kernel simply assigns the names beginning with "eth0, "eth1", ... to all the interfaces as they are probed by the device drivers during the system boot process. As the driver probing is generally not predictable, in a multi network interfaces setup, a given network interface that for example, got a name assignment "eth0" in the first boot may end up with a different name on the next boot. This is undesirable and can have serious security implications, for example in firewall rules which are coded for certain naming schemes and which are hence very sensitive to unpredictable changing names. Also, this naming scheme gives no clue whatsoever of the interface's physical location on the system (for example, whether it is on the system's motherboard or if it is on an add-in card or if it is on an add-in card with multiple ports and which port on the card it is located). Hence you need a consistent device naming scheme that can provide the following benefits:

- Stable network interface names across reboots
- Stable network interface names when you add or remove hardware
- Stable network interface names when you update/change the kernel or device drivers
- Stable network interface names when you replace a broken/defective ethernet card for example, with a new one
- The network interface names automatically get determined without user configuration and they just work
- The network interface names are predictable

During SAP workload provisioning operations, like cloning a VM, it is essential to keep the same network interface names on the target clone system as is available on the source system. In order to do this, you need to enable *Consistent Network Device Naming* in the source operating system. The next 3 sub-sections describe the specific steps to enable *Consistent Network Device Naming* on SLES, RHEL and Windows operating systems respectively.

SLES 11 and SLES 12 - *Consistent Network Device Naming*

On SLES based systems you can use the `biosdevname` program that inturn uses information from the system's BIOS to enable *Consistent Network Device Naming* on the target system as is on the source system. Execute the following steps to enable *Consistent Network Device Naming* on the source operating system.

Procedure

1 `SSH` to the source system as **root**.

Figure 6-6. SSH as **root**

2 Install the `biosdevname` utility. You can use any available package manager. The following figure depicts installing `biosdevname` using `rpm`:

Figure 6-7. Install `biosdevname`

```
vm-s11o12-a4:~ # ls biosdevname-0.2.4-67.1.x86_64.rpm
biosdevname-0.2.4-67.1.x86_64.rpm
vm-s11o12-a4:~ # rpm -i ./biosdevname-0.2.4-67.1.x86_64.rpm
warning: ./biosdevname-0.2.4-67.1.x86_64.rpm: Header V3 RSA/SHA256 signature: NOKEY, key ID 3dbdc284
Scanning scripts ...
Resolve dependencies ...
Install symlinks in /lib/mkinitrd/setup ...
Install symlinks in /lib/mkinitrd/boot ...
vm-s11o12-a4:~ #
```

3 Verify your `biosdevname` installation done in the previous step and also list out information about the current system network adapters.

Figure 6-8. List all available network adapter information

```
vm-s11o12-a4:~ # /sbin/biosdevname -d
BIOS device: eth0
Kernel name: eth0
Permanant MAC: 00:50:56:8C:1E:D9
Assigned MAC : 00:50:56:8C:1E:D9
Driver: vmxnet3
Driver version: 1.4.2.0-k-NAPI
Firmware version: N/A
Bus Info: 0000:03:00.0
PCI name      : 0000:03:00.0
PCI Slot      : 7

BIOS device: eth1
Kernel name: eth1
Permanant MAC: 00:50:56:8C:FD:50
Assigned MAC : 00:50:56:8C:FD:50
Driver: vmxnet3
Driver version: 1.4.2.0-k-NAPI
Firmware version: N/A
Bus Info: 0000:0b:00.0
PCI name      : 0000:0b:00.0
PCI Slot      : 8

vm-s11o12-a4:~ #
```

4 Remove the **70-persistent-net-rules** file from the `/etc/udev/rules.d` directory, if it already in there.

5 Reboot the operating system as depicted in the following figure:

Figure 6-9. Reboot the OS

```
vm-s11o12-a4:~ # cd /etc/udev/rules.d
vm-s11o12-a4:/etc/udev/rules.d # ls
40-alsa.rules                70-kpartx.rules          77-network.rules        85-usb_autosuspend_devices.rules  99-vmware-scsi-udev.rules
50-iscsi-firmware-login.rules  70-persistent-cd.rules  79-yast2-drivers.rules  85-usb_elotouch_wakeup.rules
51-packagekit-firmware.rules   70-persistent-net.rules  81-mount.rules          99-iwlwifi-led.rules
70-kdump.rules               71-biosdevname.rules     81-mptctl.rules         99-pcsc_lite.rules
vm-s11o12-a4:/etc/udev/rules.d # rm 70-persistent-net.rules
vm-s11o12-a4:/etc/udev/rules.d # reboot

Broadcast message from root (pts/0) (Thu Jun  8 03:02:03 2017):

The system is going down for reboot NOW!
vm-s11o12-a4:/etc/udev/rules.d #
```

After rebooting the operating system all the current network interfaces on the system will be renamed according to the *Consistent Network Device Naming* scheme.

RHEL 7 and RHEL 6 - *Consistent Network Device Naming*

RHEL based systems receive new network device interfaces with new IP settings applied along with incremented indexes in the interface names. For example, if the source system has two network interfaces eth0 and eth1, then the target system will obtain the network interface names as eth2 and eth3 respectively.

RHEL 7 — In RHEL 7, *Consistent Network Device Naming* is enabled by default. Thus no additional actions are required from a user/administrator perspective.

RHEL 6 — The `biosdevname` utility does not work in operating system hosted on virtual machine. Hence you are required to execute the following workaround:

Note This option requires that the system is not using NetworkManager (i.e **NM_CONTROLLED=no** in `ifcfg-*` files) (Source: https://access.redhat.com/solutions/112643)

Procedure

1 `SSH` to the source system as **root**.

2 Identify the PCI address of your Ethernet interfaces with `lspci` command as depicted in the following figure:

Figure 6-10. Login as root and execute `lspci`

```
login as: root
root@192.168.10.231's password:
Last login: Thu Jun  8 23:33:31 2017 from 192.168.10.230
[root@vm-r65o11-a4 ~]# lspci -D | grep Ethernet
0000:0b:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
0000:13:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
[root@vm-r65o11-a4 ~]#
```

3 Create the `/etc/udev/rules.d/60-persistent-net.rules` file and fill it with the following type of network device NAME mapping, highlighted for reference as depicted in the following figure:

Figure 6-11. Create `60-persistent-net.rules` file

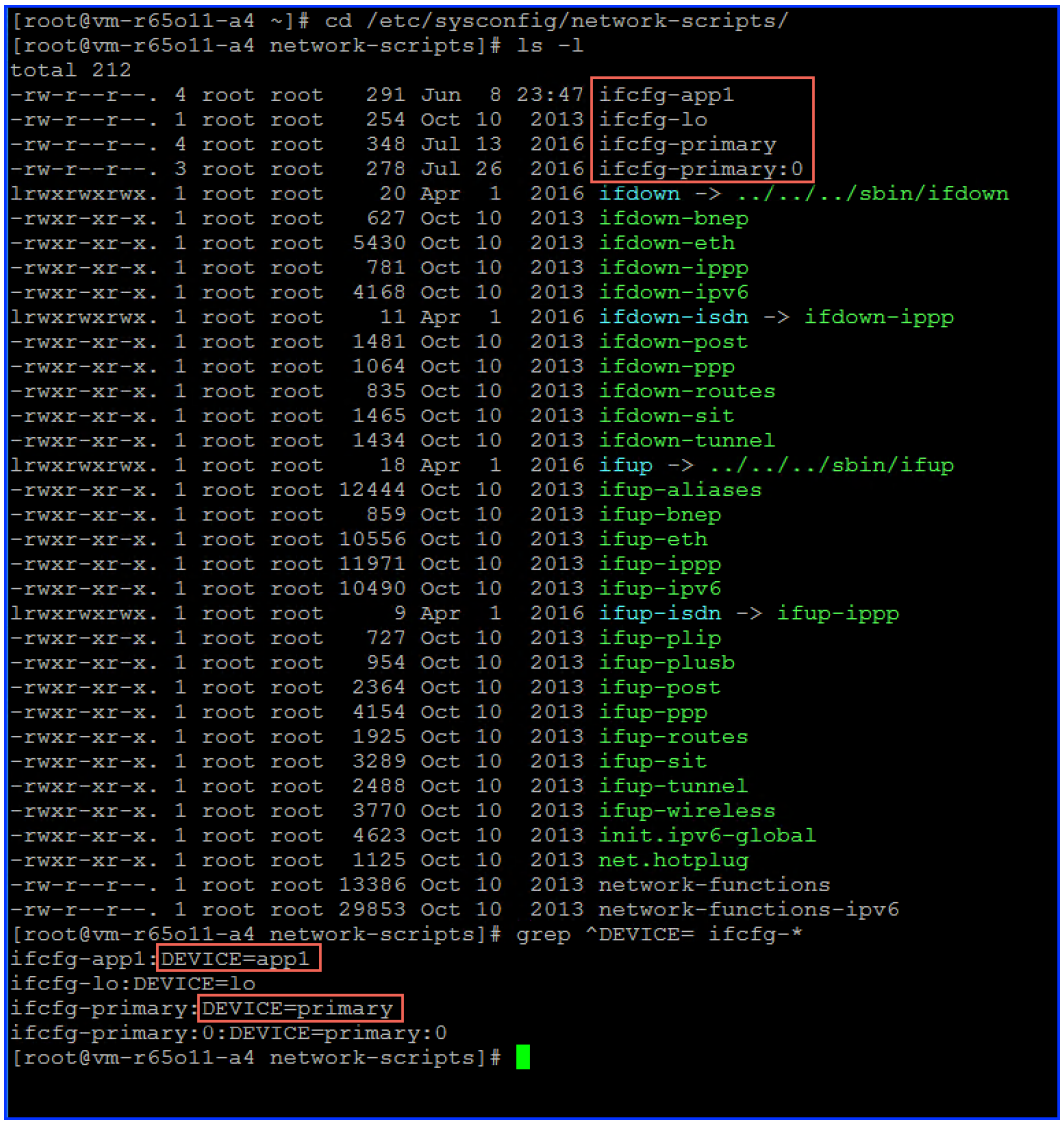
```
[root@vm-r65o11-a4 ~]# cd /etc/udev/rules.d
[root@vm-r65o11-a4 rules.d]# ls -l
total 52
-rw-r--r--. 1 root root 1652 Aug 25  2010 60-fprint-autosuspend.rules
-rw-r--r--. 1 root root  153 Feb  1  2013 60-ipath.rules
-rw-r--r--. 1 root root 1060 Jun 29  2010 60-pcmcia.rules
-rw-r--r--. 1 root root  318 Apr  6  2016 60-persistent-net.rules
-rw-r--r--. 1 root root  316 Aug  6  2013 60-raw.rules
-rw-r--r--. 1 root root  789 Apr  1  2016 70-persistent-cd.rules
-rw-r--r--. 1 root root  256 Jun 28  2016 70-persistent-net.rules
-rw-r--r--. 1 root root  320 Sep 12  2012 90-alsa.rules
-rw-r--r--. 1 root root   83 Apr  1  2011 90-hal.rules
-rw-r--r--. 1 root root 2486 Jun 30  2010 97-bluetooth-serial.rules
-rw-r--r--. 1 root root  308 Oct 21  2013 98-kexec.rules
-rw-r--r--. 1 root root   54 Nov  3  2011 99-fuse.rules
-rw-r--r--. 1 root root  341 Apr  4  2016 99-vmware-scsi-udev.rules
[root@vm-r65o11-a4 rules.d]# cat 60-persistent-net.rules
# 0000:0b:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01) was eth0
ACTION=="add", SUBSYSTEM=="net", KERNELS=="0000:0b:00.0", NAME:="primary"

# 0000:13:00.0 Ethernet controller: VMware VMXNET3 Ethernet Controller (rev 01)
ACTION=="add", SUBSYSTEM=="net", KERNELS=="0000:13:00.0", NAME:="app1"

[root@vm-r65o11-a4 rules.d]#
```

4 Rename and modify (using any editor of your choice), `/etc/sysconfig/network-scripts/ifcfg-*` files to use the new names in the **DEVICE=value** fields. The following figure depicts the DEVICE values after modifying the corresponding `ifcfg-*` files (highlighted for reference).

Figure 6-12.



5 Ensure that you have console access in case there are some network connectivity issues. Reboot the system by executing the `reboot` command.

After rebooting the operating system all the current network interfaces on the system will be renamed according to the *Consistent Network Device Naming* scheme.

Windows - *Consistent Network Device Naming*

Windows based systems running either Windows 2008 R2 or Windows 7 guest operating system configured with the VMXNET3 virtual network device in vCenter Server have one known issue. When a provisioning operation is done like cloning a VM, the target system gets new device and interface names (this name is the original name as is on the source system but with an incremented index suffix, like **`Local Area Connection #2`** instead of just **`Local Area Connection`**. In order to prevent such issues and keep the original device and interface names as is, following the provisioning operation, you need to apply the Microsoft hot fixes for the specific operating system type that you are using.

1 For Windows 2008 R2 or Windows 7 versions prior to Service Pack 1, Install the hot fix described in the Microsoft Knowledge Base article 2344941 (https://support.microsoft.com/en-us/help/2344941/-0x0000007b-stop-error-when-you-replace-an-iscsi-or-pci-express-network-adapter-or-a-motherboard-with-an-identical-device-on-a-windows-server-2008-r2-based-or-windows-7-based-computer), before deploying the template.

2 For Windows 2008 R2 or Windows 7 versions post Service Pack 1, Install the hot fix described in the Microsoft Knowledge Base article 2550978 (https://support.microsoft.com/en-in/help/2550978/-0x0000007b-stop-error-after-you-replace-an-identical-iscsi-network-adapter-in-windows-server-2008-r2-sp1-or-in-windows-7-sp1) before deploying the template.

Command Line Interface Reference

VMware vCenter Server Connections

The LaMa Service connects to vCenter Server to gather inventory and metrics. The LaMa Service can connect to one or more vCenter Server. The CLI command `vla_credentials` manage vCenter Server connections via Add, Modify, Remove, Test, List and associate with VMware vRealize Orchestrator.

List all vCenter Server Connections

You can display all the vCenter Server connections that are configured by running the command:

```
# sudo vla_credentials -l
```

Add a vCenter Server Connection

To add a new vCenter Server onto the vla-service, run the command:

```
# sudo vla_credentials -a -s vcenter -n <FQDN> –u <user> [–A <vCO_id>][–f]

Parameters:
  <FQDN> – vCenter server FQDN.
  <user> - Administrator user for vCenter.
  <vCO_id> - vCenter Orhestration ID on VMware LaMa Service.
  [–f] - Using force mode, for ignore validation certificate.
```

Note To get help on the command use the -h option:

```
# sudo vla_credentials –h
```

Some examples:

```
# sudo vla_credentials –a –s vcenter –n vcenter.example.local –u 'DOMAIN_ALIAS\user' –A vco1 –P
https:443
# sudo vla_credentials –a –s vcenter –n vcenter.example.local –u 'example.org\user' –A vco1 –P
https:443
# sudo vla_credentials –a –s vcenter –n vcenter.example.local –u user@example.org –A vco1 –P
https:443
# sudo vla_credentials –a –s vcenter –n vcenter.example.local –u user –A vco1 –P https:443
# sudo vla_credentials –a –s vco –n vco.example.local –u user –P https:8281
```

Modify a vCenter Server Connection

To modify a configured vCenter Server on vla-service, run the command:

```
# sudo vla_credentials -m -s vcenter -n <FQDN> –u <user> [–A <vCO_id>][–f]

Parameters:
  <FQDN> – vCenter server FQDN configured on VMware LaMa Service.
  <user> – Administrator user for vCenter.
  <vCO_id> - vCenter Orhestration ID on VMware LaMa Service.
  [–f] - Using force mode, for ignore validation certificate.
```

Delete a vCenter Server Connection

To delete a configured vCenter Server on vla-service, run the command:

```
# sudo vla_credentials -d -n <FQDN>

Parameters:
  <FQDN> – vCenter server FQDN configured on VMware LaMa Service.
```

Test vCenter Server Connection

To test connection to a configured vCenter Server, run the command:

```
# sudo vla_credentials -t -n <FQDN>

Parameters:
  <FQDN> – vCenter server FQDN configured on VMware LaMa Service.
```

Test vCenter Server Certificate

To validate the vCenter Server Certificate run the command:

```
# sudo vla_credentials -c -s vcenter -n <FQDN>
```

```
Parameters:
  <FQDN> – vCenter server FQDN.
```

VMware vRealize Orchestrator

The VMware LaMa Service connects to the VMware vRealize Orchestrator Server. The VMware LaMa Service uses the VMware vRealize Orchestrator to execute commands such as Start, Stop, and Clone. Currently the VMware LaMa service can connect to one VMware vRealize Orchestrator Server. The CLI command `vla_credentials` manages the VMware vRealize Orchestrator connection via Add, Modify, Remove, and Test functions.

List VMware vRealize Orchestrator Connection

To display the VMware vRealize Orchestrator connection that is configured run the command:

```
# sudo vla_credentials –l
```

Add VMware vRealize Orchestrator Connection

To add a new VMware vRealize Orchestrator connection onto the VMware LaMa (Landscape Management) Service, run the command:

```
# sudo vla_credentials -a -s vco -n <FQDN> –u <user> [–f]
```

```
Parameters:
  <FQDN> – VMware
                vRealize Orchestrator server FQDN.
  <user> - Administrator user for VMware
                vRealize Orchestrator.
 [–f] - Using force mode, for ignore validation certificate.
```

Modify a VMware vRealize Orchestrator Connection

To modify a configured VMware vRealize Orchestrator Server on vla-service, run the command:

```
# sudo vla_credentials -m -s vco -n <FQDN> –u <user> [–f]
```

```
Parameters:
  <FQDN> – VMware
                vRealize Orchestrator server FQDN configured on VMware LaMa Service.
  <user> – Administrator user for VMware
                vRealize Orchestrator.
  [–f] - Using force mode, for ignore validation certificate.
```

Delete a VMware vRealize Orchestrator Connection

To delete a configured VMware vRealize Orchestrator Server on vla-service, run the command:

```
# sudo vla_credentials -d -n <FQDN>

Parameters:
  <FQDN> – VMware
                vRealize Orchestrator server FQDN configured on VMware LaMa Service.
```

Test VMware vRealize Orchestrator Server Connection

To test connection to a configured VMware vRealize Orchestrator server, run the command:

```
# sudo vla_credentials -t -n <FQDN>

Parameters:
  <FQDN> – vCenter server FQDN configured on the Lama Service.
```

Test VMware vRealize Orchestrator Server Certificate

To validate VMware vRealize Orchestrator Server Certificate, run the command:

```
# sudo vla_credentials -c -s vco -n <FQDN>

Parameters:
  <FQDN> – VMware
                vRealize Orchestrator server FQDN.
```

Binding Service to a Port / IP Address

Use the `sys_service_configuration` command to do the following:

- Bind a service to a particular port
- Reset and associate the service back to a default port
- Bind a service to a particular IP address
- Allow all IP addresses to access a service

```
Usage: sys_service_configuration [–h] [–l] [–s] [–V] [–S [SERVICE]] [–p [PORT]] [–i [IPV4]] [–d]
[–v] [–t]
```

To bind a service to a particular port and IP address execute the following steps:

1. Execute the `sys_service_configuration` command with -l (list) option, to list out the available service names, assigned ports or default ports and the associated IPv4 binding.

   ```
   # sys_service_configuration –l
   ```

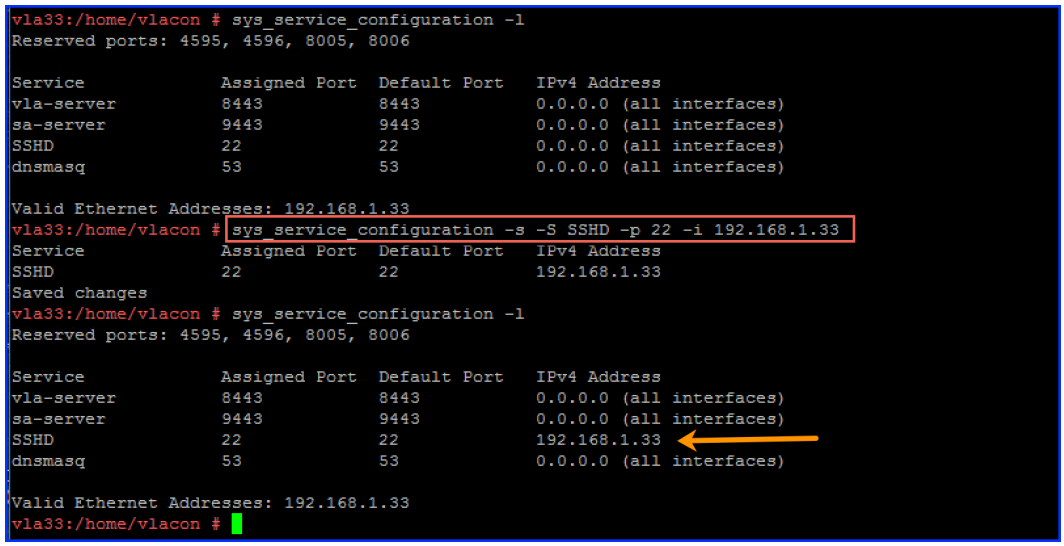
2. Bind the identified service listed in the preceding step to a particular port / IP address as follows:

   ```
   # sys_service_configuration –s –S SSHD –p 22 –i 192.168.1.33
   ```

3. Verify if the service did bind to the specified port / IP address by executing step 1 again.

The following figure depicts the preceding three steps:

Figure 6-13. Binding a service to a particular port / IP address



Note

1 If you configure the same service multiple times on the command line, the `sys_service_configuration` command accepts only the last full set, as depicted in the following figure:

Figure 6-14. Configuring same service multiple times

```
vla33:/home/vlacon # sys_service_configuration -l
Reserved ports: 4595, 4596, 8005, 8006

Service             Assigned Port  Default Port   IPv4 Address
vla-server          8443           8443           0.0.0.0 (all interfaces)
sa-server           9443           9443           0.0.0.0 (all interfaces)
SSHD                22             22             0.0.0.0 (all interfaces)
dnsmasq             53             53             0.0.0.0 (all interfaces)

Valid Ethernet Addresses: 192.168.1.33
vla33:/home/vlacon # sys_service_configuration -s -S SSHD -p 22 -i 192.168.1.32 -s -S SSHD -p 22 -i 192.168.1.33
Service             Assigned Port  Default Port   IPv4 Address
SSHD                22             22             192.168.1.33
Saved changes
vla33:/home/vlacon # sys_service_configuration -l
Reserved ports: 4595, 4596, 8005, 8006

Service             Assigned Port  Default Port   IPv4 Address
vla-server          8443           8443           0.0.0.0 (all interfaces)
sa-server           9443           9443           0.0.0.0 (all interfaces)
SSHD                22             22             192.168.1.33
dnsmasq             53             53             0.0.0.0 (all interfaces)

Valid Ethernet Addresses: 192.168.1.33
vla33:/home/vlacon #
```

2 If you enter duplicate values for parameters on the command line, the `sys_service_configuration` command causes a warning as depicted in the following figure:

Figure 6-15. Configuring with duplicate parameter values

```
vla33:/home/vlacon # sys_service_configuration -l
Reserved ports: 4595, 4596, 8005, 8006

Service             Assigned Port  Default Port   IPv4 Address
vla-server          8443           8443           0.0.0.0 (all interfaces)
sa-server           9443           9443           0.0.0.0 (all interfaces)
SSHD                22             22             192.168.1.33
dnsmasq             53             53             0.0.0.0 (all interfaces)

Valid Ethernet Addresses: 192.168.1.33
vla33:/home/vlacon # sys_service_configuration -s -S SSHD -p 22 -i 192.168.1.33
No change in SSHD for port=22 and IPv4:192.168.1.33
warning, no update
vla33:/home/vlacon #
```

Create custom tomcat instance certificate for alternative hostname

When you deploy a VLA, the appliance contains a single vNIC to which you apply a single IP address and, ideally, FQDN (as part of the deployment). On first boot, the VLA creates a self-signed certificate using the FQDN (or IP address if no FQDN is present).

After deployment, you or other administrators may configure one or more additional vNIC(s) on the appliance, for example for network isolation, multi-homing, etc. In order for traffic through these additional vNIC(s) to be secure, the VLA needs a change to its certificate configuration. You can either:

- Create and Deploy a wild-card certificate that works for all the FQDNs associated with the appliance's vNICs

- Create and Deploy one additional certificate for each of the additional FQDNs associated with the additional vNIC(s)

Note Further discussion of creating and deploying certificates is beyond the scope of this document.

```
# sudo vla_cert –c –i <service–name > –f –H <Alternative_FQDN>
```

For Example:

```
# sudo vla_cert –c –i vla–server –f –H vla–managed.example.com
```

Manage LaMa Adapter

Use the `vla_adapter` command to install / uninstall the VMware LaMa adapter or create an installation archive. When you install / uninstall the adapter, the `vla_adapter` command prompts you for the LaMa administrator user password. You should enable the SSH and have root access to the vla-service to use the `vla_adapter` command.

```
# vla_adapter (–a|–d|–c) –f LAMA_HOST –u SSH_USER –x LAMA_ADMIN_USERNAME
 –a flag for installation
 –d flag for uninstallation
 –c flag for manual deployment archive creation (for debug purposes)
```

Note When you uninstall the VMware LaMa adapter using the `vla_adapter` command with -d option, you notice that the VMware LaMa adapter does not appear in the list under **Provisioning -> Virtualization Adapters** in your browser. However, you observe that the VMware LaMa adapter still shows up in the list under **infrastructure -> Virtualization Managers** in your browser. This is a known issue and VMware is working on a solution to fix it. The fix will be available in future releases.

Index