Cisco Intelligent Automation for Cloud Installation Guide

Release 4.1.1
Published: December 12, 2014

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Text Part Number: OL-29914-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Intelligent Automation for Cloud Installation Guide
© 2014 Cisco Systems, Inc. All rights reserved.

Ensuring Required Prerequisites Are Ready-to-Go

Successful installation of Cisco IAC 4.1.1 requires that certain hardware and software prerequisites be in place before you start the install process.

Cisco IAC Components

The major functional components for deployment of Cisco Intelligent Automation for Cloud 4.1.1 include:

- Cisco Prime Service Catalog (PSC)
- Cisco Process Orchestrator
- Cisco IAC Virtual Appliance

External components include:

- Amazon EC2
- Chef
- Cisco Prime Network Services Controller (PNSC)
- Cisco Prime Performance Manager (PPM)
- Cisco UCS Director
- Cisco UCS Manager
- OpenStack
- Puppet
- VMware vCenter
- VMware vCloud Director

Tip For the complete list of interoperable components and version/release information, see the *Cisco Intelligent Automation for Cloud 4.1.1 Compatibility & Requirements Matrix* located here: http://www.cisco.com/c/en/us/support/cloud-systems-management/intelligent-automation-cloud/tsd-products-support-series-home.html.

Checking Required Prerequisites

Required prerequisite components for Windows installations include but are not limited to:

- Microsoft IIS
- Microsoft .NET framework

Note Be sure to enable Microsoft IIS before installing .NET framework. This will automatically register ASP.NET with Microsoft IIS.

- Oracle and/or Microsoft SQL Server database
- Linux O/S for non-Windows installations
- Java Runtime Environment (JRE)
- JBoss application server
- A web browser: Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, or Apple Safari
- PSExec (version 2.11 or greater) is present on Cisco Process Orchestrator

Note Check that these components are installed, configured, and running in the supported versions (see the*Cisco Intelligent Automation for Cloud 4.1.1 Compatibility & Requirements Matrix* located here: http://www.cisco.com/c/en/us/support/cloud-systems-management/intelligent-automation-cloud/tsd-products-support-series-home.html for details) before you begin the Cisco Intelligent Automation for Cloud installation process.

Tip See Appendix B, “Solution Prerequisites Checklists,” for more details.

Note Refer to the installation guides for each component product for complete information on how to install and configure the associated software; for example, see the *Cisco Process Orchestrator* guides for complete information on Cisco Process Orchestrator.

Note DBAs commonly have a convention or security policy requiring a user-naming scheme. Note that you will most likely not be able to set the username of the service account according to your practices with Cisco IAC 4.1.1.

Note PSExec should be installed on the Cisco Process Orchestrator server for Application Configuration Management. Place PSExec onto your executable path for installing applications on a Windows Server.

Setting Up Your Networks

First, choose a network type to determine how this network can be used:

- User networks are used for deploying virtual machines.
- Management networks are used for management access to cloud servers.
- Infrastructure networks are used for management interfaces of Hypervisor hosts and other infrastructure devices.

Then, prepare your networks to include the following requirements:

- At least one VLAN to use as a destination network for provisioning servers. You can define a destination network as a community, user, or management network when you create the network in Prime Service Catalog.
  - User networks are assigned to specific Virtual Data Centers owned by an organization.
  - Management infrastructure within the cloud system may be used to manage cloud servers, for example, for remote access and monitoring.

Preparing Storage Management

Prepare your storage management system using the following information:

- Install and configure Storage Area Network (SAN) storage or iSCSI storage required for Distributed Resource Scheduler (DRS) clusters. For iSCSI or Network File System (NFS) storage solutions, VMware supports Dynamic Host Configuration Protocol (DHCP.) It is important that any of these solutions use DHCP, otherwise static IP information, wherever it is applicable, will have to be configured manually after the automated process is complete.
- Create the storage volumes that will be used for datastores and datastore clusters.
- Configure Logical Unit Number (LUN) access in your storage management system and assign World Wide Node Name (WWN) pools (see Setting Up Cisco UCS Manager Pools, page 1-4)

vCenter datastores map to or reference specific LUNs. These mappings will replicate to a new host if the host blade has been given the same LUN access as all the other hosts in the cluster. This is accomplished through WWN pools.

LUN configuration can be assigned to any WWN that is within a specific range. For a new host to be assigned WWNs that are within that range, ensure that it is coming from the pre-defined pool. Whenever a service profile is created from a service profile template for a blade, specify that the template generate WWN assignments from a specific pre-defined pool in Cisco UCS Manager. Datastore access should automatically be in sync with all the other hosts in that cluster when the service profile template is used to provision the blade.

Preparing Cisco UCS

Setting Up Cisco UCS Manager

While Cisco UCS Manager is an optional component, should your cloud deployment include this technology, Cisco UCS Manager should be installed and configured before installing Cisco IAC. For instructions on installing and configuring the application, see the Cisco UCS Manager documentation on Cisco.com.

Setting Up Cisco UCS Manager Pools

Cisco UCS Manager utilizes different types of pools to control assignment of unique identifiers (such as UUIDs, MACs and WWNs) to blade servers. These pools must be created and assigned to Service Profiles. You need to create the following pools:

- Universal Unique Identifier (UUID) Suffix Pool—Used to uniquely identify each blade server.
- Media Access Control (MAC) Address Pool—Used to assign a unique MAC address to each vNIC assigned to a blade.
- WWNN (World Wide Node Name) Pool—Assigned to a node in a Fibre Channel fabric, and used to assign unique WWNNs to each blade in a range that will allow appropriate LUN access
- WWPN (World Wide Port Names) Pool—Assigned to specific ports in a Fibre Channel fabric, and used to assign unique WWPNs to each blade in a range that will allow appropriate LUN access

For instructions on creating the pools, see Cisco UCS Manager documentation on Cisco.com.

Preparing VMware Software

vCenter O/S support is shown in Table 1-1.

Table 1-1 OS Customization Support

	vCenter Version		
OS Release	**5**	**5.1**	**5.5**
Windows Server 2012	Yes[2]	Yes[1]	Yes
Windows Server 2008 R2	Yes	Yes	Yes
Red Hat Enterprise Linux 6.x	Yes	Yes	Yes
CentOS 5x	No	Yes[3]	Yes[2]
CentOS 6x	No	Yes[3]	Yes[2]
Ubuntu 12.04 LTS	Yes[2]	Yes[1]	Yes

Key:
No = Not supported
Yes = Supported
Yes[1] = Supported from Update 1
Yes[2] = Supported from Update 2
Yes[3] = Supported from Update 3

Supported Installation Media for ESXi

Provisioning of the ESXi Hypervisor OS always uses the first local drive installed in the blade. Cisco IAC supports installation of ESXi to local disks only (not over a SAN).

VMware Installation Requirements

The following VMware software should be installed:

- vSphere PowerCLI on the Process Orchestrator server to support the activities for adding a new ESXi host to a cluster.

Tip For supported software versions, see the*Cisco Intelligent Automation for Cloud 4.1.1 Compatibility & Requirements Matrix* located here: http://www.cisco.com/c/en/us/support/cloud-systems-management/intelligent-automation-cloud/tsd-products-support-series-home.html.

Prepare your VMware environment for virtual provisioning using the following checklist:

- Install VMware vCenter.
- Configure VMware vCenter:
  - Apply enterprise licensing and enable VMware vSphere Distributed Resource Scheduler (DRS).
  - Determine and create the datacenter, clusters, hosts, datastores, networks, and resource pools to which all commissioned hosts and VMs will be deployed.
- Define at least one VM template with VMware tools using a boot disk.
  - Be sure the template is configured for the exactly the same size and shape VM you want, not including any networks that are not available when the template is cloned.
  - If several different configurations are desired, they should be controlled by supplying a unique template for each configuration.

Provisioned hosts will have evaluation licensing only. You will need to add licensing manually in the vSphere Client.

Tip For information about installing and configuring your VMware environment, see the *ESX and vCenter Server Installation Guide 4.0*.

Note Users must have the ability to create resource pools. In addition, resource pools must be enabled on VMware VCenter.

Tip Forward slashes in vCenter object names break the parsing process. If any of your vCenter object names contain forward slashes, rename the files before you specify a vCenter path.

Installing and Configuring Optional Software

This chapter covers optional software that can be used with Cisco IAC 4.1.1. Note that this chapter provides only product names. For version numbers, see the *Cisco Intelligent Automation for Cloud Product Compatibility Matrix*. Optional software includes but is not limited to:

- Cisco Software, including:
  - Cisco IAC Management Appliance
  - Cisco Prime Network Services Controller
  - Cisco UCS Director
  - Cisco UCS Manager
- VMware, including:
  - vCenter
  - vCloud Director
  - ESXi
  - vSphere
  - vSphere PowerCLI
- Microsoft Active Directory and other LDAP servers
- OpenStack
- Amazon EC2
- Puppet
- Chef

Understanding Cisco Prime Network Services Controller

Cisco Prime Network Services Controller (formerly known as Cisco Virtual Network Management Center, or VNMC) provides centralized multi-device and policy management for Cisco network virtual services. For instructions on installing and configuring Cisco Prime Network Services Controller, see *Cisco Prime Network Services Controller documentation* on Cisco.com.

Understanding Cisco UCS Director

Cisco UCS Director (formerly Cisco Cloupia) delivers unified management for industry-leading converged infrastructure solutions based on Cisco Unified Computing System (UCS) and Cisco Nexus technologies. UCS Director is a higher-level manager over multiple UCS Managers. For instructions on installing and configuring Cisco UCS Director, see *Cisco UCS Director documentation* on Cisco.com.

Understanding Cisco UCS Manager

Cisco Unified Computing System (UCS) Manager provides unified, embedded management of all software and hardware components in the Cisco UCS. It controls multiple chassis and manages resources for thousands of virtual machines. For instructions on installing and configuring Cisco UCS Manager, see *Cisco UCS Manager documentation* on Cisco.com.

Preparing the Directory and Mail Server via LDAP and SMTP

To prepare your directory and e-mail environment, ensure that the following conditions are met:

- LDAP server software, such as Microsoft Active Directory, is installed and configured.
- SMTP server is installed and configured with an account to send and receive e-mails.

Note For information on configuring the STMP server, see the *Cisco Process Orchestrator Installation and Administration Guide* or the *Cisco Cisco Prime Service Catalog Installation Guide*.

Understanding Amazon EC2

Amazon EC2 is a Web-based service that allows business subscribers to run application programs in the Amazon.com computing environment. The EC2 can serve as a practically unlimited set of virtual machines. For more about Amazon EC2, see the Amazon EC2 website at http://aws.amazon.com/ec2/.

Configuring OpenStack

Cisco Intelligent Automation for Cloud 4.1.1 supports the following versions of OpenStack. Note that only the two versions listed below have been implemented and successfully tested here at Cisco. The interoperability of any other version(s) of OpenStack cannot be guaranteed.

- Havana
- IceHouse

Note If you are using Havana or IceHouse, ensure that the Neutron service component has been installed and configured vs. legacy networking (Nova-network).

The following OpenStack services are mandatory for the correct performance of Cisco IAC 4.1.1:

- Block Storage (Cinder)

- Compute (Nova)
- Identity (Keystone)
- Image (Glance)
- Networking (Neutron)
- Prime Performance Manager (Ceiliometer)

also recommended

- Dashboard (Horizon)

OpenStack Configuration Notes

1. If you are using all-in-one deployment or a scenario with only one available compute node make sure that you have set both **allow_resize_to_same_host** and **allow_migrate_to_same_host** to "true" in configuration file at */etc/nova/nova.conf*.

Tip These options allow you to resize the instance on one node.

Set **resize_confrim_window=*x***. By default, this is set to 0, but you need to change this to *x* seconds in order to automatically confirm the resize after *x* seconds.

2. If you are running OpenStack within a virtual machine set, in order to use QEMU you must set the following options in configuration file on your compute host(s) at */etc/nova/nova.conf*:

libvirt_type=qemu

Cinder service=mandatory

Note Configuration changes are applied only after the restart of Nova services.

3. If you would like OpenStack to report debugging information into an *httpd log* file, specify the following parameters in the configuration files found at */etc/openstack-dashboard/local_settings*:

DEBUG=True

TEMPLATE_DEBUG=DEBUG

Note The file may be a significant size; this may negatively affect performance.

4. Check that you have opened all necessary ports in your firewall:

8776 - Block Storage (cinder)

8774 - Compute (nova) endpoints

5000 - Identity service public endpoint

9696- Networking (neutron)

5672 - Message Broker (AMQP traffic)

Tip For the correct steps needed to install the OpenStack solution on your environment, refer to the OpenStack documentation located on the OpenStack website at: http://docs.openstack.org/.

Timesaver You can find a list of the recommended ports here: http://docs.openstack.org/trunk/config-reference/content/firewalls-default-ports.html

Configuring Puppet Labs for Cisco IAC Integration

Puppet Labs software must be licensed and in place for use with Cisco Intelligent Automation for Cloud 4.1.1. Puppet Enterprise 3.0.1 or higher is recommended. The FOSS (Open Source) version is not supported. For POCs, PE is available for free to manage up to 10 nodes.

For Puppet, the following services are included:

- Register Puppet Role
- Update Puppet Infrastructure Item
- Activate Puppet Resource

Note An active Internet connection to the Puppet clients is required to properly install new applications.

Basic Puppet Considerations

To leverage integration with Puppet with Cisco IAC, Puppet modules need to be designed to expose roles and profiles. Node classification is accomplished via Hiera, so the site.pp file for each environment must include the following:

```
node default {
hiera_include('classes')
}
```

Your main hiera.yaml file should look something like the following:

```
---
:backends:
- yaml!

:yaml:
:datadir: /etc/puppetlabs/puppet/environments/%{environment}/hieradata

:hierarchy:
- "nodes/%{fqdn}"
- common
```

Be advised that when you create a Puppet connection from System Setup, it creates two Process Orchestrator targets, a main Web Service target (for future use) and a reference to a Terminal target (for SSH). You should update the terminal target's default maximum number of concurrent sessions to a number greater than one (preferably 100) to avoid bottlenecks when running Puppet on multiple nodes.

Self-service ordering of servers includes the option to apply a single Puppet role from an environment. Although best practice is to assign a single role to a server, this can be extended further to include multiple roles, or add roles later through an add-on service. This is out of scope for Cisco IAC 4.1.1, but is available through stack blueprints using the Application Stack Accelerator Pack (ASAP).

Note With Cisco IAC 4.1.1, you can add multiple puppet applications to a single node (VM).

Puppet is configured via an SSH/PSExec connection to the new node. A well-known root/Administrator (or equivalent) user and password is required for cases where no password is specified in the order. All nodes requiring configuration management should have the same root/Administrator user/password. This can be changed during or post-configuration. Sudo is used for non-root users. The certificate authority for Puppet requires that clocks for master and agent servers be synchronized with a common time source (for example, using the ntpd service).

Note For vCenter, Cisco IAC automatically configures new Puppet nodes to have VMware Tools synchronize the clock with the ESXi host; therefore, the best way to achieve clock synchronization is to ensure that the ESXi hosts and the Puppet Master use the same time authority to set the time.

If the Puppet master requires a private key file to connect, you will need to specify this with the Connect Cloud Infrastructure or Update Cloud Infrastructure service. Check the Additional Options check box to specify this.

If you need to use an alternative repository for the Puppet Enterprise Installer, you can override the default Puppet Labs location with the Connect Cloud Infrastructure or Update Cloud Infrastructure service. Choose the Additional Options check box to specify a different base URL. The installer files must match the Puppet Labs naming conventions exactly.

You can override the location for the hiera node classification files with the Connect Cloud Infrastructure or Update Cloud Infrastructure service. Choose the Additional Options check box to specify an override. You use `$environment` as a placeholder in the path. Be sure your hiera.yaml file is modified accordingly.

Method for Sharing Facts Between Nodes and Stacks

When using Puppet with the Application Stack Accelerator Pack (ASAP), it is often necessary for one node in a stack to be able to reference the facts of another (for example, the IP Address). This is achieved by recording the stack instance name and the role in a stack as external facts for each node that can be used as lookup criteria. To query facts about the other nodes in a stack you need to first have installed the prerequisite *puppetdbquery* module from https://forge.puppetlabs.com/dalen/puppetdbquery.

Facts that Cisco IAC automatically assigns to nodes include:

- `stack_instance`: Name of the Stack Instance (shared by all servers in the same stack)
- *`stack_role`*: Role Name or List of Role Names (comma-separated) for the server
- `iac_organization:` Name of the IAC organization (including tenant prefix) for customer who ordered the stack

In your puppet code, use the following as an example of retrieving facts about another node in the stack.

```
$db_host_ip = query_nodes("stack_instance='$stack_instance' and
stack_role~'(,|^)mysql (,|$)')"
```

The query above returns the IP address for the node that has the role mysql in the same stack as the current node running this code.

Working With Class Parameter Overrides

The IAC integration with Puppet allows class parameter value overrides to be configured and exposed to users ordering servers. This is done through special JSON files that reside in the same location as your profile module's puppet code (under manifests). Class override parameters are always defined in the profile module, and, if present, have the same name as profile or profile subclass followed by ".params.json".

Below is a sample of "webserver.params.json" corresponding to the profile class called "webserver". For each parameter, you provide a friendly name, description, default value, and most importantly, what class parameter you are overriding. You can alternatively define an externally defined fact for a node by specifying 'fact', 'factor' or an empty value for the class_param attribute of the parameter.

If you provide a comma-separated options list, users will have to choose one of the values in the list. Override values are added to the hiera node classification file along with the role that includes the profiles requiring these parameter values. Because class parameter overrides are handled in Hiera node classification, be careful of parameter override precedence. Any values provided in a "class" inclusion block, will take precedence over those values provided by Hiera.

Profile Class Parameter Overrides JSON Example

```
{
    "id": "profile::webserver",
    "parameters": {
    "customer.name": {
        "display_name": "Customer Name",
        "description": "The customer name",
        "help_text": "Please select a valid customer.",  "options": "PuppetLabs,Cisco
        Systems,ACME Bread",
        "data_type": "string",
        "validation": "",  "value": "PuppetLabs",  "required": "yes",
        "class_param": "myapp::custname"
    },
    "customer.greeting": {
        "display_name": "Customer Greeting",
        "description": "Greeting to display to customer.",
        "help_text": "Please select a customer greeting. For example, Hello.",
        "options": "",  "data_type": "string",  "validation": "",  "value": "Hello",
        "required": "yes",
        "class_param": ”facter"
    },
    "http.port": {
        "display_name": "HTTP Port",
        "description": "The HTTP port to use.",
        "help_text": "Please select an HTTP port for the web page. Default is 80.",
        "options": "",  "data_type": "integer",  "validation": "",  "value": "99",
        "required": "no",
        "class_param": "apache::port"
        }
    }




}
```

Proxies for Puppet

To set up your proxies for Puppet, follow the steps below.

Step 1 Navigate to Setup > System Settings > Connections.

Step 2 Select **Connect Cloud Infrastructure** if you are setting up the intitial connection, or select **Update Cloud Infrastructure** if you want to go back into your setup and add or change the proxy settings.

Warning **When you update settings using the Update Cloud Infrastructure, you must re-enter information (such as passwords) into any field that displays as empty. The reason for this is that the system will overwrite the existing data for that field in the database with blanks. Passwords are not displayed for security / cryptographic reasons.**

Step 3 Scroll down and select **Show Additional Options**.

Step 4 Enter the **Installer Package Base** URL as needed.

Step 5 Enter the **Alternate Module Path** information, as needed.

Step 6 Enter the **Hiera Node Classification Path**, as needed.

Step 7 From the **Bootstrap/Proxy info for Operating System**, select either Windows or Linux.

Note You can enter information for both, and Cisco IAC will track it. You can only enter one at a time.

Step 8 Enter the proxy (either **Windows Proxy** or **Linux Proxy**, as is appropriate.) For example, `http://133.133.133.152`. Include the port number, if that is how you have set up your enviroment; for example: `http://133.133.133.152:8080`.

Step 9 In the Proxy Bypass box, enter one or many exceptions. You can enter them as URLs or as IP addresses. They must be separated by semi-colons (;) or the system will not parse them correctly.

Step 10 Enter the **Bootstrap User** name and the **Bootstrap Password**.

Step 11 Enter the **Private Key**, as needed.

Step 12 Click **Submit**.

Note Alternatively, if proxies are used in your environment, you can update the following extended target properties as necessary for your Puppet web target in Process Orchestrator:

```
Puppet.Target.Bootstrap.Linux.Proxy Puppet.Target.Bootstrap.Linux.NoProxy
Puppet.Target.Bootstrap.Windows.Proxy Puppet.Target.Bootstrap.Windows.NoProxy
```

Configuring Chef for Cisco IAC Integration

Chef Labs software must be licensed and in place for use with Cisco Intelligent Automation for Cloud 4.1.1. Hosted or Private Chef 11.4 or higher is required (with appropriate patches). For Chef, the following services are included:

- Register Chef Cookbook
- Register Chef Role

- Update Chef Infrastructure Item
- Activate Chef Resource

Due to Chef recently changing its naming convention for the chef agent installers, we have implemented our own naming conventions for Cisco IAC 4.1.1 for the local repository. This is the template for those files:

```
chef-{version}-{distro}-{arch}.rpm
chef-{version}-{distro}-{arch}.deb
chef-windows-{version}.msi
```

For example:

```
chef-11.12.4-el-5-x86_64.rpm
chef-11.12.4-el-6-x86_64.rpm
chef-11.12.4-ubuntu-x86_64.deb
chef-windows-11.12.4.msi
```

Tip An active Internet connection to the Chef clients is required to properly install new roles.

Tip When registering the Chef master in Cisco IAC 4.1.1, there is the option to configure a proxy server to enable Internet access be used during role installation. If using the proxy settings, make sure to include both the Chef Master and local repository (if applicable) in the proxy bypass. Additional information on proxies is included below.

Basic Chef Considerations

Be advised that when you create a Chef connection from System Setup, it creates two Process Orchestrator targets, a main Web Service target (for future use) with a reference to a Terminal target (for SSH). You should update the terminal target's default maximum number of concurrent sessions to a number greater than one (preferably 100) to avoid bottlenecks when running Chef on multiple nodes.

Self-service ordering of servers includes the option to apply a single Chef role and environment. Although best practice is to assign a single role to a server, this can be extended further to include multiple roles, or add roles/recipes later through an add-on service. This is currently out of scope for this accelerator kit.

For Linux, Chef is configured via an SSH connection to the new node. A well-known root (or equivalent) user and password is required. All Linux templates requiring configuration management should have the same root user and password. This can be changed during or post-configuration. Sudo support will be added in a later release.

You need to set the two extended target properties of the Chef web target in Cisco Process Orchestrator:

```
Chef.Target.Bootstrap.Linux.User
Chef.Target.Bootstrap.Linux.Password
```

Cisco IAC allows users to specify the Administrator user/password, so the above is not required for Windows. The certificate authority for Chef requires that the server and client clocks be synchronized with a common time source (for example, using the ntpd service).

Note The hosts/controller these VM/instances run on should also be synced to the same time source; such as VMware Hosts, Openstack Controller/Compute Node.

Note For vCenter, Cisco IAC automatically configures new Chef nodes to have VMware Tools synchronize the clock with the ESXi host; therefore, the best way to achieve clock synchronization is to ensure that the ESXi hosts and the Chef server use the same time authority to set the time.

If the Chef server/workstation you defined with the Connect Cloud Infrastructure service requires a private key file to connect, you will need to create a new Public-Key Authenticated Admin User runtime user definition in Process Orchestrator and replace the Opscode Chef Terminal (SSH) target's default runtime user.

Tip Connecting via private key is optional, yet recommended.

The integration requires that the cisco-cloud-automation cookbook is uploaded into the Chef repository. The cookbook can be found as a zip file in the kit's Chef folder and should be extracted to a Chef workstation and uploaded to the server. The cookbook is required by the CiscoCM role that also must be uploaded from the included CiscoCM.json file.

During node bootstrapping, the following node attributes are automatically assigned:

- `stack_instance`: Name of the Stack Instance (shared by all servers in the same stack)
- `iac_organization`: Name of the IAC organization (including tenant prefix) for customer who ordered the stack

Working with Role Attributes Overrides

The IAC integration with Chef allows node attribute overrides to be configured and exposed to users ordering servers. Attributes are exposed to IAC via Data Bags. You need to create a Data Bag for each Role that needs attribute overrides with the same name as the corresponding role. In that Data Bag, you must have a Data Bag item, called "default".

Note Use the following JSON sample below as an example.

For each attribute you want to expose, you can provide a friendly name, default, description, help text, and most importantly a Ruby expression that represents the attribute you will override at runtime. If you provide a comma-separated options list, users will have to choose one of the values in the list.

When a node is ordered, a new Data Bag item is created with the name of the node and includes all of the attribute values used for the configured node. These override values are injected by the cisco-cloud-automation cookbook before the recipes in the role are run.

Role Data Bag Sample JSON

```
{
    "id": "default",
    "attributes": {
    "customer.name": {
```

```
        "display_name": "Customer Name",
        "description": "The customer name",
        "help_text": "Please select a valid customer.",  "options": ”Opscode,Cisco
        Systems,ACME Bread",
        "data_type": "string",
        "validation": "",  "value": "Opscode",  "required": "yes",
        "expression": "node.normal[:customer][:name]"
    },
    "customer.greeting": {
        "display_name": "Customer Greeting",
        "description": "Greeting to display to customer.",
        "help_text": "Please select a customer greeting. For example, Hello.",
        "options": "",  "data_type": "string",  "validation": "",  "value": "Hello",
        "required": "yes",
        "expression": "node.normal[:customer][:greeting]"
    },
    "http.port": {
        "display_name": "HTTP Port",
        "description": "The HTTP port to use.",
        "help_text": "Please select an HTTP port for the web page. Default is 80.",
        "options": "",  "data_type": "integer",  "validation": "",  "value": "99",
        "required": "no",
        "expression": "node.force_default[:http][:port]"
        }
    }
}
```

Proxies for Chef

Proxies for Chef are configurable in Connect and update Cloud infrastructure forms. If proxies are used in your environment, you will need to ensure you have the following patches for your Chef server (v11.4-6 provided in Chef folder).

For Linux

```
bootstrap_context.rb (replaces file in <ruby-path-to-chef-gems>/lib/chef/knife/core)
bootstrap.rb (replaces file in <ruby-path-to-chef-gems>/lib/chef/knife)
chef-full.erb (replaces file in <ruby-path-to-chef-gems>/lib/chef/knife/bootstrap)
```

For Windows

`bootstrap_windows_base.rb`
(replaces file in `<ruby-path>/gems/knife-windows-0.5.13/lib/chef/knife/`)

`windows_bootstrap_context.rb`
(replaces file `<ruby-path>/gems/knife-windows-0.5.13/lib/chef/knife/core`)

`windows-chef-client-msi.erb`
(replaces file in `<ruby-path>/gems/knife-windows-0.5.13/lib/chef/knife/bootstrap`)

In your `knife.rb` file, include your proxy information as in the example below

```
bootstrap_proxy = ‘http://64.102.255.40:8080’
bootstrap_no_proxy = ‘192.168.1.*, internal.chef.server’
```

Setting Up Proxies for Chef in Cisco IAC

To set up your proxies for Chef, follow the steps below.

Step 1 Navigate to Setup > System Settings > Connections.

Step 2 Select **Connect Cloud Infrastructure** if you are setting up the initial connection, or select **Update Cloud Infrastructure** if you want to go back into your setup and add or change the proxy settings.

Warning **When you update settings using the Update Cloud Infrastructure, you must re-enter information (such as passwords) into any field that displays as empty. The reason for this is that the system will overwrite the existing data for that field in the database with blanks. Passwords are not displayed for security / cryptographic reasons.**

Step 3 Scroll down and select **Show Additional Options**.

Step 4 Enter the **Installer Package Base** URL as needed.

Step 5 From the **Bootstrap/Proxy info for Operating System**, select either Windows or Linux.

Note You can enter information for both, and Cisco IAC will track it. You can only enter one at a time.

Step 6 Enter the proxy (either **Windows Proxy** or **Linux Proxy**, as is appropriate.) For example, `http://133.133.133.152`. Include the port number, if that is how you have set up your enviroment; for example: `http://133.133.133.152:8080`.

Step 7 In the Proxy Bypass box, enter one or many exceptions. You can enter them as URLs or as IP addresses. They must be separated by semi-colons (;) or the system will not parse them correctly.

Step 8 Enter the **Bootstrap User** name and the **Bootstrap Password**.

Step 9 Click **Submit**.

Installing Cisco IAC PO Automation Packs

In this chapter, you will find instructions for installing the following automation packs:

- Intelligent Automation for Cloud Extension Samples.tap (optional but recommended)
- Intelligent Automation for Cloud Starter.tap
- Intelligent Automation for Cloud.tap
- Intelligent Automation for Compute.tap

Note You first need to install Cisco Process Orchestrator 3.1. For full instructions, refer to the Cisco Process Orchestrator documentation, located here: http://www.cisco.com/c/en/us/support/cloud-systems-management/process-orchestrator/tsd-products-support-series-home.html

Launching the Setup Wizard

Step 1 Download the Cisco IAC 4.1.1 installer. The IAC 4.1.1 PO content files are part of the build file named `IAC 4.1.1.xxxx`.

Note To find the latest file, navigate to http://software.cisco.com. Find the downloads link and look for Cisco Intelligent Automation for Cloud as the software.

Step 2 Un-zip `IAC4.1.1.xxx`.

Step 3 Locate the Cisco IAC 4.1.1 setup.exe file and run it to start the Setup Wizard.

- Click **Next** to proceed to the next step.

Step 4 On the Information page, click **Next** again to continue.

Step 5 On the Confirm Installation page, click **Next** to continue.

Step 6 On the Installation Complete page, check the **Launch automation pack import wizard** now check box.

Step 7 Click **Close** to launch the Automation Pack Import Wizard. The Import Wizard will first configure itself.

Note You will next see the Choose Automation Pack screen, the use of which is explained in "Installing the Core and Common Automation Packs".

Installing the Core and Common Automation Packs

The Choose Automation Packs dialog box displays. This dialog box shows you a list all available automation packs and other services required for Cisco IAC 4.1.1. These include the TAPs you just installed, as well as Core and Common Activities. These are presented in a checklist format, and are pre-checked for your convenience.

Note You must install both the Core and the Common Activities packs. The Cisco IAC packs are dependent on functionality within these packs in order to function properly. In fact, without the Core and Common Activities TAPs, the Cisco IAC TAPs will not import.

Step 1 Click **OK** to continue with chosen options.

Step 2 On the Welcome to the Automation Pack Import Wizard panel, click **Next**.

Step 3 You do not need to enter information on the General Information panel because we are importing the Core and Common Activities. Before you click **Next**, make sure the Core and Common Activities Packs are selected.

- Click **Next**.

Step 4 Enter **Keystore Password** (required for keystore file containing email digital signatures).

Step 5 On the Email Configuration panel, provide the default SMTP server and sender's e-mail address to be used for e-mail activities,

- Click **Next**.

Step 6 The Automation Summary Configuration panel indicates where the automation summary reports that are generated by activities are to be saved and how long the reports are to be retained. The specified file paths will be used to access and view the automation summary reports.

On the Automation Summary Configuration panel, specify the following information.

- Accept the default directory, or enter a different file path for the automation summary directory in the Share Path field. You can also browse to navigate to the file path for the automation summary.
- Enter credentials as needed. (These are not required.)
- In the Virtual directory mapping area you create the share folder that corresponds to a virtual directory in IIS. Note that you may only create the virtual directory in the local IIS.
  - Check the **Enable virtual directory mapping** check box.
  - Click **Create**.

    The Create Virtual Directory dialog box displays, pre-populated with default settings.
  - Click **OK** to accept.

Note Back in the Virtual directory path field, you can edit the string (`http://host:(port)/sharefolder`) if needed.

Step 7 Scroll down and you will see the Automation summary reports grooming settings area. The default deletion period is thirty days, but you can set this to whatever you want, from 1 to 9999. Or, choose the **Delete automation summary reports older than** check box to remove the check and all reports will be saved indefinitely.

- When you are done working with the Automation Summary Configuration panel, click **Next**.

Step 8 On the Data Extraction panel, uncheck all of the data options:

- Business Objects Reports
- Microsoft SCOM Management Packs
- SQL Server Reporting Services Reports

Note Take a note of the folder name where the extracted data will be placed and uncheck the SQL Server Reporting Services Reports if you are not using the MS SQL Reporting solution.

- Click **Next**.

Step 9 The Review Prerequisites panel displays the prerequisites for the automation pack being imported, and will indicate either pass or fail for each prerequisite.

Step 10 After the prerequisite check has completed (and passed), the Importing Objects panel displays:

Step 11 After the objects have been imported, the General Information panel displays:

Installing the Cisco IAC Automation Packs

The four Cisco Automation packs are installed next. These include, in sequence:

- Intelligent Automation for Compute.tap
- Intelligent Automation for Cloud Starter.tap
- Intelligent Automation for Cloud.tap
- Intelligent Automation for Cloud Extension Samples.tap (optional but recommended)

The install process for each Automation Pack is explained next.

Installing the Intelligent Automation for Compute Pack

Step 1 On the General Information panel, review the information there. Note that the **Name** field now displays "Intelligent Automation for Compute." This is the first Cisco IAC automation pack that you will be installing.

- Click **Next**.

Step 2 On the Default Incidents Assignee Setup panel, specify the default user which to assign cloud-related incidents. This is a CPTA (Cloud Provider Technical Administrator) account, or would be within an Active Directory group that was created for all of CPTAs in this Cloud.

- Click **Next**.

Step 3 On the Cisco Process Orchestrator Web Service panel, specify the following data. Check the **Enable non-secure Web Service (HTTP)** check box in the Web Service Settings area. This setting unencrypts the HTTP endpoints.

Tip If or when presented with a security warning message, click **OK**.

- Enter or verify the HTTP Port for the Process Orchestrator web target.
- Choose the appropriate authentication method for the web service:
  - **Basic**—Standard method that provides a username and plaintext password to the authentication mechanism.
  - **Digest**—Method that provides a username and a hashed password to the authentication mechanism.
  - **NTLM**—*Default*. Authentication protocol that is used on networks that include systems running the Windows operating system and on stand-alone systems.

Note The NTLM setting supports both NTLM and NTLMv2. In IIS, NTLM is not enabled by default; you must enable NTLM in IIS if you choose this authentication mechanism. The agents in Prime Service Catalog must also be set to use the same authentication that you specify here.

- When you are done, click **Next** to continue.

Step 4 Enter your credentials:

- On the Default Web Service Credentials panel, specify the credentials for connecting to the Process Orchestrator web service target.
- When done, click **Next** to continue.

Step 5 Enter a password for VMware keystore access.

The VMware keystore password protects the Java keystore file used to keep SSL certificates for all configured VMware targets.

- For new installations, this password can be set to any valid six-character keytool password.

Note If the VMware vSphere PowerCLI has not already been installed in the Process Orchestrator server, the wizard displays an information panel informing you of the situation. You can select **Choose this check box to continue with the import** to proceed. However, if you are using VMware vCenter and you have not yet installed VMware vSphere PowerCLI, the contents of the automation pack may not work correctly, if at all, until PowerCLI has been installed.

- Click **Next**.

Step 6 You will see a process screen display whereby the prerequisites are verified, and then objects are imported.

Step 7 You will then be returned to the General Information panel to install the next Automation Pack.

Installing the Intelligent Automation for Cloud Starter Pack

Step 1 On the General Information panel, review the information about the automation pack. Note that the **Name** field now displays "Intelligent Automation for Cloud Starter."

- Click **Next**.

Step 2 On Configure Process Database Grooming panel, specify the number of days to keep process instances in the database. After the specified number of days, the process instances will be deleted from the database. The default value should be satisfactory.

- Click **Next** to continue.

Step 3 The Data Extraction panel is used to specify the destination where the data is extracted on the Process Orchestrator server. You can simply accept the default location, or browse to specify a different location to extract the files.

Step 4 The Review Prerequisites panel displays briefly and you will see the prerequisites being processed.

Step 5 Next, the Importing Objects panel displays its various progress bars as the data is imported and extracted. This may take some time to complete.

Step 6 When the import is complete, you are automatically returned to the General Information panel.

Step 7 Click **Next**.

Installing the Intelligent Automation for Cloud Extension Samples (Optional)

Step 1 On the General Information panel, review the information about the automation pack. Note that the **Name** field now displays "Intelligent Automation for Cloud Extension Samples."

Step 2 Click **Next**.

- The Review Prerequisites panel displays briefly and you will see the prerequisites being processed.
- Next, the Importing Objects panel displays progress bars as the data is imported and extracted. This may take some time to complete.

When the import is complete, you are automatically returned to the General Information panel.

Step 3 On the General Information panel, click Next to import the Common Activities Automation Pack.

- The Review Prerequisites panel displays briefly and you will see the prerequisites being processed.
- Next, the Importing Objects panel displays progress bars as the data is imported and extracted. This may take some time to complete.
- When the import of the common activities is complete, you are automatically returned to the General Information panel once again.

Step 4 On the General Information panel.

Step 5 Click **Next**.

Step 6 Enter the destination for the extracted data, and choose the data to extract (or un-choose, really, as all of the data has been preselected for you).

Step 7 Click **Next** to continue.

Step 8 Once again, the Review Prerequisites panel displays briefly and you will see the prerequisites being processed.

- As before, the Importing Objects panel displays its various progress bars as the data is imported and extracted. This may take some time to complete.
- When the import process is complete, the Automation Pack Import Wizard panel displays.

Installing the Intelligent Automation for Cloud Pack

Step 1 On the General Information panel, review the information about the automation pack. Note that the **Name** field now displays "Intelligent Automation for Cloud."

- Click **Next**.

Step 2 On Configure Process Database Grooming panel, specify the number of days to keep process instances in the database. After the specified number of days, the process instances will be deleted from the database. The default value should be satisfactory. Click **Next** to continue.

Step 3 The Data Extraction panel is used to specify the destination where the data is extracted on the Process Orchestrator server. You can simply accept the default location, or browse to specify a different location to extract the files, then click **Next**.

Step 4 The Review Prerequisites panel displays briefly and you will see the prerequisites being processed.

Step 5 Next, the Importing Objects panel displays its various progress bars as the data is imported and extracted. This may take some time to complete.

Step 6 When the import is complete, you are automatically returned to the General Information panel.

Completing the Process

After the objects have been imported, the Final Automation Pack Import Wizard Screen displays.

- Review the information below the "Completing the Automation Pack Import Wizard" heading to verify that all is correct.
  - For Cisco IAC, leave the **Refresh Web Server** check box checked.
  - When you are done reviewing the information here, click **Close** to close the wizard.

You have now successfully installed all supporting software for Cisco Process Orchestrator.

Installing Cisco IAC Components for a Fresh Installation

Note Be sure to create a backup of both the Cisco Process Orchestrator database and the Cisco Prime Service Catalog database before you install Cisco IAC 4.1.1.

Note This chapter and the chapters that follow apply to new Cisco Intelligent Automation for Cloud 4.1.1 installations only. If you are upgrading from Cisco IAC 4.1, refer to Chapter A, "Upgrading From Cisco IAC 4.1 to 4.1.1".

Installing Prime Service Catalog Content

The process of installing PSC using the installation packages consists of three steps:

- Importing and Deploying Portal Packages
- Installing the REX Adapter
- Importing and Deploying PSC Catalogs

These steps are outlined in detail below.

Importing and Deploying Portal Packages

Cisco IAC ships with packaged image files and portal pages to provide an easy-to-use portal for ordering services.

Importing IAC Packages on PSC Windows Environments

Importing the IAC packages on Prime Service Catalog Windows environments with IIS requires the following IIS settings changes. IIS 7.5 has a default limit of 30 MB for all upload file. You can change this limit by performing the following steps:

Step 1 Open Server Manager window.

Step 2 In the first (left-most) panel, expand **Server Manager - Roles - Web Server (IIS) - Internet Information Services (IIS) Manager**.

Step 3 In the second (middle) panel, expand **hostname - Sites - Default Web Site**.

Step 4 Click **Default Web Site**.

Step 5 In the third (middle) panel, click **Request Filtering**.

Step 6 In the fourth (right-most) panel, click the link **Edit Feature Settings…**

Step 7 On the **Edit Request Filtering Settings** popup dialog, change the value for **Maximum allowed content length (Bytes)** from 30000000 to a larger number, such as 60000000.

Step 8 Click **OK**.

Step 9 Restart **World Wide Web Publishing Service**.

Copying the Cisco IAC Portlets Package and Extracting Files

Step 1 On the Cisco Process Orchestrator server, navigate to the following folder where `IAC-ServiceCatalog-4.1.1_xxxx.xxx` was extracted. You will see names along the lines of "CS_Services_4-1-1.xml."

Note The file is in a compressed (ZIP) file and will need to be extracted. There is also a ZIP file with the Prime Service Catalog files in it.

Step 2 Extract `IACPortlets-4.1.1_xxxx.xxx` from the compressed (ZIP) file to a temporary location. It will create an `IACPortlets-4.1.1_xxxx.xxx` folder.

Step 3 Stop the JBoss application server by stopping:

- Cisco Prime Service Link, and then
- Cisco Prime Service Catalog

Note For instructions, see "How to Stop/Start the JBoss Server" in the *Cisco Prime Service Catalog 10.x Installation Guide.* The latest version can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog-10-0/model.html#InstallandUpgradeGuides

Step 4 In the `IACPortlets-4.1.1_xxxx.xxx` folder, locate RequestCenter_war.zip.

Step 5 Extract RequestCenter_war.zip to the following directory (for Windows):

```
(JBOSS_DIR)\ServiceCatalogServer\deployments\RequestCenter.war
```

Note Overwrite any existing files, if prompted.

Step 6 Restart the JBoss application server by starting again: Cisco Prime Service Link, and Cisco Prime Service Catalog.

Importing and Deploying Portal Pages

Deploy the Cisco IAC portal page content by importing it from the *PortalPages.xml* portal page file, located in the IACPortlets folder.

Step 1 Choose **Portal Designer** from the module drop-down list to open Portal Designer.

Step 2 In Portal Designer, click the **Portal Pages** tab.

Step 3 In the left navigation pane, click **Actions** and choose **Import** from the drop-down list.

Step 4 On the Import Portal Pages dialog box, click the **Overwrite** radio button in the Conflict Resolution field.

Step 5 In the Import from File field, click **Choose File** to navigate to the IACPortlets folder that you extracted earlier.

- On the Choose File to Upload dialog box, choose the **PortalPages.xml** file and click **Open**.
- On the Import Portal Pages dialog box, click **Import**.

Step 6 Refresh your browser to view the imported portal.

Installing and Configuring the REX Adapter

Note See Appendix F, "Installing (or Reinstalling) the REX Adapter," for details.

Importing and Deploying PSC Catalogs

Complete the following procedure to import and deploy catalogs in Prime Service Catalog. Note that you must be logged into Prime Service Catalog with administrator privileges to perform the procedures.

Installing the Catalogs

Step 1 Open a browser and launch Cisco Prime Service Catalog.

Step 2 Log into the Prime Service Catalog ServiceCatalog web portal as the site administrator

Step 3 Choose **Catalog Deployer** from the module drop-down list.

Step 4 In the Deployment Packages pane, and choose **Action > Import** from the drop-down list.

Step 5 On the Import Package from File dialog box, click **Browse** to navigate to the folder where you saved the Prime Service Catalog files.

Step 6 Choose the **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml** file and click **Import**.

Warning **For new installations, DO NOT import or deploy SC_Common_4-1-1.xml.**

Step 7 When the message *Package Imported Successfully* displays, click **OK**.

The Deployment Packages window refreshes to display the imported package in the Received for Deployment view.

Step 8 Repeat Step 4 through Step 7 again to import **SC_Services_4-1-1.xml.**

Step 9 Repeat Step 4 through Step 7 again to import **SC_Common_4-1-1_Overwrite.xml.**

Deploying the Catalogs

Step 1 In the Deployment Packages pane, choose **Action > Deploy Multiple Packages** from the drop-down list.

Step 2 On the Choose Packages dialog box, choose the check boxes for **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml**, **SC_Services_4-1-1.xml**, and **SC_Common_4-1-1_Overwrite.xml**.

Step 3 Click **Add**.

Step 4 Check the **Chosen Items** check box and ensure that check boxes for **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml**, **SC_Services_4-1-1.xml**, and **SC_Common_4-1-1_Overwrite.xml** are checked.

Step 5 On the Deploy Multiple Package tab, choose **Add Packages to Deploy**.

Step 6 Click **Deploy**.

Step 7 When each package displays *Succeeded* next to it, you will redeploy **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml**

- On the Choose Packages dialog box, choose the check box one more time for **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml**.

Step 8 Click **Add**.

Step 9 Check the **Chosen Items** check box and ensure that check box for **SC_Common_4-1-1_NEW_INSTALL_ONLY.xml** is checked.

Warning **It is important that you deploy SC_Common_4-1-1_NEW_INSTALL_ONLY.xml a second time. This is an easily overlooked step which will result in the installation failing down the road.**

Step 10 On the Deploy Multiple Package tab, choose **Add Packages to Deploy**.

Step 11 Click **Deploy**.

Step 12 Click **Done**.

Deploying Patches

Patch files, if available, are in the same location as theCisco IAC 4.1.1 package files. They are named:

- SC_Services_Patch_4-1-1.xml
- SC_Common_Patch_4-1-1.xml

Note Note that all patches are cumulative. That is, when you deploy the latest patch, it contains all previous patches within it. Therefore, all new and prior patches will all be applied at one time to bring your system fully up to date.

The patch files are deployed like the other package files, and they should be imported/deployed after the main packages. The order is:

- **SC_Common_Patch_4-1-1.xml**
- **SC_Services_Patch_4-1-1.xml**

Step 1 If necessary, choose **Catalog Deployer** from the module drop-down list within Prime Service Catalog.

Step 2 In the Deployment Packages pane, and choose **Action > Import** from the drop-down list.

Step 3 On the Import Package from File dialog box, click **Browse** to navigate to the folder where you saved the Prime Service Catalog files.

Step 4 Choose **SC_Common_Patch_4-1-1.xml**

Step 5 Click **Import**.

Step 6 When the message *Package Imported Successfully* displays, click **OK**.

The Deployment Packages window refreshes to display the imported package in the Received for Deployment view.

Step 7 Repeat Step 4 through Step 6 to import **SC_Services_Patch_4-1-1.xml**.

Step 8 In the Deployment Packages pane, choose **Action > Deploy Multiple Packages** from the drop-down list.

Step 9 On the Choose Packages dialog box, choose the check boxes of packages to deploy, then click **Add**.

Step 10 Check the **Chosen Items** check box and ensure the check boxes for **SC_Common_Patch_4-1-1.xml** and **SC_Services_Patch_4-1-1.xml** are checked.

Step 11 On the Deploy Multiple Package tab, choose **Add Packages to Deploy**.

Step 12 Click **Deploy**.

Step 13 When each package displays *Succeeded* next to it, click **Done**.

CHAPTER 5

Optional Tasks

Setting Up Active Directory Integration (If Applicable)

This section provides examples of setting up optional directory integration in Microsoft Active Directory. Because there are many scenarios for directory integration configuration based on the directory product and settings, it is likely that your environment will vary from what is presented here. However, the required sequence of configuring directory integration would be the same.

Cisco Prime Service Catalog can integrate with directory servers to synchronize user information. This synchronization can be initiated whenever a user logs on or is chosen or during Person Lookup in Prime Service Catalog. Prior to configuring integration in Prime Service Catalog, you must have a directory server installed and populated with corporate data.

Note For instructions on configuring directory integration if your setup varies, see the *Cisco Prime Service Catalog 10.x Integration Guide*. The latest version can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog-10-0/model.html#InstallandUpgradeGuides

Prerequisites

Before configuring directory integration for use with Cisco IAC, you must complete the following tasks:

- Set up organizational unit structure on the LDAP server. If you do not have privileges to perform this task on the LDAP server, seek help from your LDAP server administrator.
- Create the following user accounts in the Users folder on the LDAP server:
  - nsAPI user
  - A user account (any username) with “Read MemberOf” permissions that will be used for performing authentication, directory searches, and user imports into the Prime Service Catalog.

Note Cisco IAC 4.1.1 supports multiple memberships to multiple organizations. However, through Directory Integration these can only be mapped to a *single* organization. After the user has been imported, a CPTA can add the user to additional organizations and assign a Home OU (default organization).

Configuring an LDAP Server

The first step is to add a data source and test the connection in Cisco Prime Service Catalog. The instructions in this section are how one would connect to the LDAP server in the example scenario.

Step 1 Choose **Service Portal** from the module drop-down list, then click the **System Settings** from the **Setup** tab.

Step 2 On the System Setup portal, click the **Connections** tab to open the portlet, then click **Manage Directory Server Connection**.

Step 3 Click **Add** to display the Datasources Configuration pane.

Step 4 In the Add or Edit a Datasource pane, enter the following:

- Enter a name for the datasource. Do not use spaces or special characters.
- Enter a description of the datasource. (*Optional.)*

Step 5 Expand **Choose protocol and server product**, then choose the following:

- The protocol is always **LDAP**.
- Choose **MS Active Directory**. (Other server options are **Sun One** or **IBM Tivoli Directory Server**.)

Step 6 Expand **Connection Information**, then specify the following required datasource information in the definition area. This information includes lookup user that you set up as a prerequisite.

- Choose **Simple** (text username and password) from the Authentication Method drop-down list.
- Choose **Non SSL** from the Mechanism drop-down list.
- Enter the bind-distinguished name (BindDN) value for the lookup user. The BindDN looks like the following example:

  CN=Mehalic Michael,OU=Users,OU=Austin,OU=Texas,OU=USA,
  DC=notexist,DC=local

  Note PSC now supports the use of LAN Manager (down-level logon) formats now. You can still use the BindDN as you have it now but you can also use the format of domainname\username.

- To query the BindDN value, open a command prompt on the Windows server and execute the following command:

  dsquery user -name “[*name*]*”

- Enter the fully qualified hostname or IP address of the LDAP directory server. For example: dc.notexist.local
- Enter the parent folder under which all users will gain access.

  For example, if the User BaseDN is OU=Austin,OU=Texas,OU=USA,DC=notexist,DC=local, then all users in the Austin organization will have access.

- Enter the port number for the LDAP according to either of the following conditions:
  - For a non-SSL connection, the default port number for LDAP is **389**.
  - For an SSL connection, the default port number for LDAP is **636**.
- You can verify the port number for your LDAP server using either by running the command **netstat -an** on the domain controller, or by using the SysInternals tool **TCPView.exe**.

- Enter the password for the user specified as the BindDN.

Step 7 Click **Update**.

Step 8 Check the check box next to the newly added datasource and click **Test Connection**. The Test Status column displays **OK** if the connection is successful.

Configuring Authentication

Configuring authentication requires completing two tasks: configuring mappings and configuring events. The instructions in this section are how one would complete each task in the example scenario.

Configuring Mappings

The first task in configuring authentication is to assign mapping attributes to user data, including first and last name, login ID, and home organization unit. Active Directory has pre-defined mapping attributes, which are used in this example. However, there are data fields that have no specific Active Directory mapping attributes. In such cases (indicated below), you can assign any mapping attribute that you want to the data field.

Step 1 In the **Administration** module, click the **Directories** tab.

Step 2 On the Directory Integration page, click **Mappings** in the menu on the right.

Step 3 In the Mappings pane, click **Add** to display the Mapping Configuration pane.

Step 4 In the "Add or edit a mapping name" pane, specify the following information:

- Enter a name for the mapping. Do not use spaces or special characters.
- *Optional*. Enter a description of the mapping.

Step 5 In the "Configure mapping attributes" area, enter the required information in the text fields. The following table provides examples of datasource mappings for person data. Active Directory mapping attributes are pre-defined and case-sensitive. For information on how to form expressions, see the documentation that shipped with your directory software.

Table 5-1 Person Data and Mapped Attributes

Person Data	Mapped Attribute
First Name	givenName
Last Name	sn
Login ID	sAMAccountName
Personal Identification	sAMAccountName For this data field, there is no corresponding mapping attribute in Active Directory. In this case, you can assign any mapping attribute you want.
e-mail Address	expr:#email#=(.+)?(#email#):NotExist
Home Organization Unit	expr:#department#=(.+)?(#department#):NotExist

Table 5-1 Person Data and Mapped Attributes (continued)

Person Data	Mapped Attribute
Password	sAMAccountName There is no mapping attribute for passwords in Active Directory. Instead, you can map it to another attribute (in this example, sAMAAccountName). You can also map your own expression. For information, see the documentation that shipped with the Active Directory software.
Optional Person Data Mappings	
TimeZone ID	**Example:** expr:#sAMAccountName#=(nsapiuser)?(Etc/Greenwich):America/Tijuana
Role List	**Example:** expr:#memberOf#=(CN=(.*),OU=IAC,OU=Delegation,OU=Groups,OU=Austin,OU=Texas,OU=USA,DC=companyA,DC=local)?($1):

Step 6 Click **Update**.

Step 7 Test the mappings using the Data Test Mapping feature.

Note For instructions on enabling then using the Data Test Mapping feature, see "Testing Mappings" in Chapter 1, "Directory Integration and API," in the *Cisco Prime Service Catalog 10.0 Integration Guide*. The latest version of the technical reference guides can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog/products-technical-reference-list.html

Configure Events

Step 1 Click **Events** in the menu on the right.

Step 2 In the Events pane, click **Edit** next to the Login event to display the Event Configuration pane.

Step 3 Choose **Enabled** from the Event Status drop-down list.

Step 4 In the Event Configuration pane, click **Add step**, then specify the following:

- Choose **External Authentication**.
- Click **Options**, then enter the EUABindDN using the following convention:

  <netbios domain>\#LoginId#

Note You *must* provide the EUABindDN value, which is critical for login events. This value is case-sensitive. This attribute is a pre-defined Active Directory value. The attribute is different for other directories.

Step 5 Click **Update** to add the information as the first step in the event.

Step 6 Click **Add step**.

Step 7 In the Step 2 row, choose **Import Person** from the Operation drop-down list.

Step 8 From the Mapping drop-down list, choose the mapping name you specified when you defined mappings in the previous process.

Step 9 From the Datasource drop-down list, choose the datasource name that you specified in Step 4 of Configuring an LDAP Server, page 5-2.

Step 10 Click **Options**, then specify the following information in the Event Step area:

- Ensure that the Refresh Person Profile check box is checked.
- Leave the Refresh Period (Hours) field blank. If a value populates the field, delete the value.
- Do not create Group/OU:
  - **Organizational Unit—***Check* the check box. Checking this option prevents a user from logging in to the Prime Service Catalog Server unless the user's home organization has been onboarded.
  - **Group—***Uncheck* the check box.

Step 11 Click **Update** to add the information as Step 2 then click **Update** again.

Step 12 In the Events pane, click **Edit** next to the **Person Lookup for Service Form** event to display the Event Configuration pane.

Step 13 Choose **Enabled** from the Event Status drop-down list.

Step 14 In the Event Configuration pane, click **Add step**, then specify the following information in the Options for Event Step1 area:

- Choose **Import Person** as the Operation.
- Click **Options**.
  - Enter 24 in the Refresh Period (Hours) field.
  - Leave all check boxes unchecked.

Step 15 Click **Update** to add the same information as did in Step 1, then click **Update** again.

Creating a Security Group for Each User Role on the LDAP Server

In your directory, create one security group for each user role. The name of each group must exactly match the name of the user role:

- Cloud Provider Technical Administrator
- Cloud Provider Business Administrator
- Tenant Technical Administrator
- Tenant Business Administrator
- Organization Technical Administrator
- Virtual and Physical Server Owner
- Virtual Server Owner
- Solutions Team
- Form Extender

For instructions on creating security groups on your directory server, see the documentation that came with your directory server software.

Note Cisco Intelligent Automation for Cloud 4.1.1 supports an individual's membership to just a *single* organizational unit or membership, not multiple organizations.

Adding the nsAPI User to the Cloud Administration Group

The nsAPI user account that you created on the LDAP server is used to connect Prime Service Catalog to Process Orchestrator. For the nsAPI user account to function properly, you must add it to the Cloud Provider Technical Administrator user group that you created in the directory. For instructions on adding a user to a user role group on your directory server, see the documentation that came with your directory server software.

Configuring User Role Mappings

To map the user roles, you specify the location in the directory that contains the six security groups you created for each role.

Step 1 In Service Catalog, choose **Administration** from the module drop-down list, then click **Directories**.

Step 2 On the Directory Integration page, click **Mappings in the** menu on the right.

Step 3 In the Mappings pane, click **Edit** beside the mapping name you created when you configured mappings (see Configuring Mappings, page 5-3).

Step 4 Expand **Optional Person Data Mappings** at the bottom of the page.

Step 5 In the Role List field at the bottom of the optional mappings list, enter mapping attributes for role list that assigns the user to one of the six Prime Service Catalog user groups that you created in the directory. using the convention used for the example scenario (variables for the example appear in boldface):

```
expr:#memberOf#=(CN=(.*),OU=Groups,OU=Austin,OU=Texas,OU=USA,DC=no
texist,DC=local)?($1):
```

Step 6 Test the mappings using the Data Test Mapping feature.

Note For instructions on enabling and using the Data Test Mapping feature, see "Testing Mappings" in Chapter 1, "Directory Integration and API," in the *Cisco Prime Service Catalog 10.1 Integration Guide.* The latest version of the technical reference guides can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog/products-technical-reference-list.html

Enabling Directory Integration

Before you enable directory integration, be sure you have all user groups configured for use with Cisco IAC. If you do not have all user groups configured before you enable directory integration, you will not be able to log back in to Prime Service Catalog.

Step 1 Choose **Administration** from the module drop-down list, then click **Personalize Your Site**.

Step 2 On the **Customizations** page, scroll down to the Common Settings area and turn the Enable Directory Integration setting **On**.

Step 3 Click the **Update** button at the *bottom* of the page.

Administrative On-boarding of User Accounts

Step 1 The Organization Technical Administrator (OTA) navigates to the User Management page which allows him to add users to the organization.

Step 2 The OTA searches the directory (directory integration for the person search event has previously been configured and tested) for people to assign to his provisioning organization. Once the person is found, he is assigned an appropriate Server Owner role.

Step 3 In **Administration > Directories > Events**, configure a login event. The login event should have one operation: to perform Single Sign-on or External Authentication, as desired.

Step 4 Start a new browser session (if using external authentication) or try a single sign-on entry to the Service Catalog, and try to login as a new user, testing the just configured Login event.

CHAPTER 6

Using the Cisco IAC Virtual Appliance in Management Mode

Timesaver If you do not intend to use Advanced Network Services (VSA 1.0), then connecting a Cisco IAC Management Appliance is not required.

Installing the Virtual Appliance in Management Mode

Install the Cisco IAC 4.1.1 Virtual Appliance via a configuration and install wizard accessed via the vSphere Client window. To deploy the Cisco IAC 4.1.1 Virtual Appliance, follow the steps below:

Step 1 Download the OVA file for the Cisco IAC Virtual Appliance onto the machine where you installed VMware vSphere Client.

Step 2 Launch your VMware vSphere client and connect to a vCenter Server.

Step 3 Choose **File > Deploy OVF Template**.

Step 4 Click **Browse** and navigate to the location where you have saved the OVA file. Choose the OVA file, and then click **Next**.

Step 5 The template details are displayed in the OVF Template Details window. Verify the details, then click **Next**.

Step 6 The End User License Agreement window appears. Read the license agreement, click **Accept**, then click **Next**.

Step 7 In the Name and Location window, specify a name for the virtual machine, and choose the appropriate datacenter and/or folder for the virtual machine. The VM name must be unique within the datacenter and can contain up to 80 characters, excluding the usual special characters owned by the operating system (such as * . / and so on). Click **Next**.

Step 8 The Host or Cluster window may appear depending on your VMware environment. If the Host or Cluster window appears, choose the Cluster or the ESX host where you want the VM to be created.

Step 9 If the Resource Pool window appears, choose a resource pool for the VM.

Step 10 In the Storage window, choose a datastore name that has enough available disk space, then click **Next**. The VM requires up to 40 GB depending on the disk format you will choose in the next step.

Step 11 In the Disk Format window, specify the format for storing the virtual hard disk by clicking the appropriate radio button:

- Thick Provision Lazy Zeroed
- Thick Provision Eager Zeroed
- Thin Provisioning

Step 12 Click **Next.**

Step 13 If the Network Mapping window appears, choose a destination network from the list. Choose a network name has DHCP services available.

Step 14 In the Properties window, enter the following information:

- **Linux Hostname:** Enter a new hostname for this virtual machine. You may enter an unqualified host name (such as “mycomputer”) or a fully-qualified domain name (such as “mycomputer.example.com”). A host name may contain letters, digits, and dashes (-).
- **Linux Root Password:** Enter a new password for the Linux “root” superuser account.
- **Administrator Password:** Enter a password for the IAC Virtual Appliance Administrator. This will also be the password for the operating system's “cisco” user.
- **Administrator Email:** Enter the email address for IAC Service Catalog Appliance Site Administrator. This is used as the sender address for all system-level email notifications.
- **Email Server Hostname:** Enter the hostname or IP address for the SMTP server used for sending email messages.
- **Application Server Password:** Enter a new password for the Application Server administrative user.

  Note This will configure the “admin” user for the Management Appliance’s Tomcat server.

- **Enable SSL Support:** Choose this option to enable SSL support. A self-signed certificate will be generated.

  Note The self-signed SSL certificate can be replaced with a valid SSL certificate after the appliance has been deployed.

- **Time Zone:** Choose a time zone for the server from the list.
- **Enable NTP Support:** Choose this option to enable the NTP client.
- **NTP Server IP/Hostname:** Enter the IP address or host name for your NTP server. Leave this option blank if NTP is not enabled above or a value is supplied by your DHCP server. This value will be overridden by the NTP server supplied by your DHCP server.
- **PostgreSQL System DBA Password:** The Management Appliance's credential manager uses a PostgreSQL database. Enter a password for the database administrative accounts (“postgres”). Enter alphanumeric characters only.
- **Enable Prime Performance Manager:** Choose this option to enable the Prime Performance Manager (PPM) server. The web interface will be available from https://<hostname>/ppm.

  Note You can log into the PPM with the username “cisco” and the administrator password defined above.

- **Process Orchestrator Fully Qualified Domain Name:** Enter the Cisco Process Orchestrator's fully qualified domain name, or IP address. The management Appliance must communicate with a process orchestrator in order to perform network discovery.
- **Process Orchestrator Authentication Type:** Choose the authentication type required to communicate with the Process Orchestrator.
- **Process Orchestrator Port:** (optional) Enter the port that the management appliance will use to communicate with the Process Orchestrator. Default: 61527.
- **Process Orchestrator Username:** Enter the username the management appliance will use to authenticate with the Process Orchestrator.
- **Process Orchestrator Password:** Enter the password the management appliance will use to authenticate with the Process Orchestrator.
- **Process Orchestrator Domain (Windows NTLM):** Enter the Windows domain. Leave blank when basic authentication is chosen as the Process Orchestrator authentication type.
- **Assurance Control Password:** Enter the password required to authenticate with the management appliance's Assurance Control API.

Note This password must also be entered into the "Assurance Control Password" field when setting up the Cisco IAC Management Appliance cloud infrastructure element in the Prime Service Catalog.

Step 15 Click **Next**.

Step 16 In the Ready to Complete window, review the settings.

Step 17 Choose the "**Power on after deployment**" option.

Step 18 Click **Finish**.

Tip Your virtual machine is listed in the left pane of the vSphere Client under the appropriate host or cluster after the OVF Template deployment is complete.

Tip Access the Cisco IAC Virtual Appliance by pointing your web browser to the dynamically-assigned IP address or to the appliance's hostname, if DNS services are available.

Configuring Cisco IAC With the Wizard

The Cisco Intelligent Automation for Cloud 4.1.1 Configuration Wizard guides you through the steps for setting up and configuring the cloud administration and infrastructure.

Accessing the Configuration Wizard

You start the Configuration Wizard to begin the configuration process.

Tip To see field descriptions in the wizard as needed, click the question mark icon.

Step 1 Open a browser and launch Cisco Prime Service Catalog. Be sure to log in as a **Site Administrator**.

Step 2 To access the Cisco Intelligent Automation for Cloud Configuration Wizard:

- Choose **Service Portal from the menu at the top right of the screen.**
- Choose **Setup** from the Cisco IAC 4.1.1 menu
- Choose **Configuration Wizard** from the Setup sub-menu.

Step 3 The Configuration Wizard for Cisco IAC 4.1.1 displays.

The Wizard Welcome Screen

Setting the Custom Styles Directory

Note The Administration page of theCisco Prime Service Catalog works only on specific browsers. See the *Cisco Prime Service Catalog Compatibility Matrix* for more information. The latest version of the documentation can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog-10-0/model.html#InstallandUpgradeGuides

Verify that Cisco IAC is chosen and that Site Administration is associated with this style. To do so, complete these steps.

Step 1 Click the Set Custom Styles Directory link on the Welcome tab for the Cisco IAC 4.1.1 Config Wizard.

Step 2 Click **Custom Styles** in the right menu.

Step 3 Click **Add** to open the Custom Style Properties window.

Step 4 In the Name field, enter **Cisco Intelligent Automation for Cloud 4.1.1**.

Step 5 Check the **Make this Style the default for the entire site** check box.

Step 6 In the Style Directory field, click **Browse**.

Step 7 Click the **IAC** radio button, then click **OK**.

Step 8 Click **Add**.

Step 9 Click **Search** to browse for the organizational units to which to associate the custom style properties.

Configuring Agent Properties

On the **STEP 1** panel of the Cisco Intelligent Automation for Cloud Configuration Wizard, you configure agent properties for all REX agents and HTTP agents.

Timesaver Instructions on how to create the REX Agent and NSAPI accounts also appear elsewhare in this manual. So, if you have already done so, you can skip that step now.

Creating Service Accounts for Both REX Agent and nsAPI Users

Service accounts for the REX adapter and nsAPI are required to connect Cisco Prime Service Catalog to the REX adapter and Process Orchestrator, respectively.

Tip You need to be logged in as a site administrator to complete the steps in this section.

Creating the Service Accounts for REX Agent and nsAPI Users

Step 1 From the Wizard, choose **Create service accounts for both REX Agent and nsAPI users**.

Step 2 On the Organization Designer page, click **Create Person** from the Common Tasks panel (on the left of the screen).

Step 3 On the Create Person form, set up the REX user:

- Enter “REX” as the **First Name** and “User” as the **Last Name**.
- Enter a valid, actively monitored e-mail address. This will be the address where notifications relating to the REX adapter user account will be sent.

Tip Consider using the email address of a CPTA or a distribution list for all CPTAs.

- Choose **(GMT) Greenwich Mean Time** from the drop-down list.

- In the current release, only US English is supported; any language selection you make will be ignored

Note If you are using the Cisco IAC Virtual Appliance, some or all of this information may have been entered for you.

- Browse to choose an Organizational Unit. Click **Search**, click the **Site Administration** radio button, then click **Add**.
- *Optional*. Enter a description or any information pertinent to the user account in the **Notes** field.
- Enter **REXuser** as the **Login**.
- Enter, then enter re-enter (to confirm) the password for the REX user account.

Step 4 Click **Create** to create the new user.

Tip Once the user has been created, the **People** tab contents should automatically display, showing the user information you just entered. If you need to make corrections, make them before proceeding to the next step.

Creating the Service Account for nsAPI User

Note This step is *optional* if you intend to enable Directory Integration.

Step 1 Back on Organization Designer page, choose the **People** tab at the top of the page, if necessary.

Step 2 Click **Copy** (upper right of the screen) to create a copy of the REX user that will be named "nsAPI User".

Note If you are using the Virtual Appliance, this information may have been entered for you.

On the Create Person form:

- Enter "nsAPI" as the **First Name** and "User" as the **Last Name**.
- Enter a valid, actively monitored e-mail address. This will be the address where notifications relating to the nsAPI user account will be sent.

Tip Consider using the email address of a CPTA or a DL for all CPTAs.

- Choose **(GMT) Greenwich Mean Time** from the drop-down list if it is not already filled in.
- As before, only US English is supported; any language selection you make will be ignored.
- Browse to open the Choose an Organizational Unit dialog box.
  - Click **Search**.
  - Click the **Site Administration** radio button
  - Click the **People** tab and then click **Add**.

- Enter **nsAPI** as the **Login**.
- Enter, then confirm password for the nsAPI user account you created earlier.

Step 3 Click **Create** to close the form.

You will be returned to the Organization Designer.

Setting the Calendar for the nsAPI User

Step 1 In Organization Designer, click to access, or ensure that you are on, the **People** tab.

Step 2 In the People pane on the left side of the window, locate the line and click the name nsAPI user record.

Step 3 From the menu on the right side of the page, choose **Calendar**:

Step 4 In the Calendar pane, change all time values in the **To** column to **11:59 PM**.

Step 5 Change times in the **From** column to 12:00 AM if not already done so (as it is for Sunday/Saturday).

Note By default, Monday through Friday start at 9:00 AM, making for a 24-hour calendar.

Step 6 Click **Update**.

Step 7 When your are done, click **Close** in the pop up window.

You will be returned to your location on the wizard.

Setting Username and Password for 'REX Set REX Agent Properties'

Step 1 From the Wizard, choose Set username and password for the 'REX Set REX Agent Properties' agent

Step 2 In the Agents pane on the left, expand **REX Set REX Agent Properties**.

Step 3 Click **Outbound Properties**.

Step 4 In the **REXOutboundAdapter.Username** field, enter the REX login name you created on the Create Person form.

Step 5 In the **REXOutboundAdapter.Password** field, enter the REX password in the Create Person form.

Step 6 Click **Save**.

Step 7 Click **Close**.

You will be returned to your location on the wizard.

Starting the REX Set REX Agent Properties Agent

Step 1 From the Wizard, choose Start 'REX Set REX Agent Properties' agent

Tip If you do not see "REX Set REX Agent Properties" in the list, scroll down or use the pagination at the bottom to navigate to the other pages. Or, sort by agent name by clicking the Name column heading.

Step 2 Click the red icons next to **REX Set REX Agent Properties**.

Step 3 Click the **Start Chosen** button up at the top right corner of the page.

- The red icons turn to green, indicating that they are now sending and receiving.

Note In some cases, you may need to refresh the page before you see the colors change. To do so, click the **Refresh** icon.

Step 4 Close AFC.

Setting REX Agent Configuration

Configure all of the REX agent properties, then verify that the agents are configured correctly.

Step 1 From the Wizard, choose Set REX Agent Configuration

Step 2 On the Set REX Agent Configuration form, enter the REX account login name, then enter and re-enter the REX account password.

Step 3 Enter the URL to the Prime Service Catalog Request Center server in the **Cloud Portal Request Center URL** field.

Tip The URL should include http or https, the hostname and port number, and the pathname to ServiceCatalog. For example, http://localhost:8080/ServiceCatalog.

Step 4 Click **Submit Order** to submit the form and display the Order Confirmation page for the service that you ordered.

Step 5 Click on the number in the **Requisition Number** field to display the details.

Step 6 In the Requisition Details pane, click the requisition number in the **Requisition Number** field to refresh the status.

Tip Repeat this refresh process as many times as needed until the status is **Completed**.

Step 7 Click **Close** to return to the Configuration Wizard.

Starting All REX Agents

You will next start all REX agents; that is, all agents with REX in the name. The current list includes the following eleven REX agents:

1. REX Add Organization Unit
2. REX Add Organization Unit (Tenant)
3. REX Add Person
4. REX Create Queue
5. REX Deactivate OU
6. REX Delete Queue
7. REX Modify Organization Unit
8. REX Set DB Agent Properties
9. REX Set HTTP Agent Properties
10. REX Set NSAPI Agent Properties
11. REX Set REX Agent Properties (already started in a previous step)

Step 1 From the Wizard, choose Start All REX Agents.

Step 2 On the Control Agents Tab of the Service Links portal, click the red symbol next to any and all agents on the page where the outbound adapter is **REX adapter**.

Note Be careful. Clicking the text line for an agent may not actually choose that agent. Instead, it may navigate away from the Control Agents page.

- Click **Start Chosen**.
- Click **Yes**.

  The red icons will turn to green after a bit, indicating that they are now sending and receiving. In some cases, you may need to refresh the page before you see the colors change. To do so, click the **Refresh** icon at the bottom of the page.
- Repeat for all pages.

Tip Where possible, press and HOLD the **Shift** key. Then, click the first REX agent in a long list. Scroll and then (with the **Shift** key still pressed) click the last REX agent visible in the list on the page to quickly choose that group of REX agents. If a vertical scroll bar appears in the list, scroll to choose the last agent on the page.

Tip There may have been additional REX agents in the list that you were not able to see (and therefore, activate). To find them, use the scroll arrow at the bottom of the list. You may need to use the "next page" button at the bottom of the screen, as well, to find all remaining REX agents.

Step 3 Click **Close** to close this form to return to the Configuration Wizard.

Configuring a DB Agent

This step configures the credentials to connect to the database.

Step 1 From the Wizard, choose Configure DB Agent.

Step 2 From the Set Agent Configuration form, complete the following:

- Set Agent Type to DB (should already be set, but be sure to check).
- Enter a username and password.
- Reenter the password to confirm.

Note The username would match the Cisco Prime Service Catalog database information. Normally, this would be "CPSCUSER."

Step 3 Enter the appropriate URL (either MS SQL or Oracle, depending on your setup) into the **JDBC URL** field, for example:

- (MS SQL): `jdbc:sqlserver://localhost:1433;DatabaseName=ServiceCatalog;selectMethod=direct;sendStringParametersAsUnicode=true`
- (Oracle): `jdbc:oracle:thin:@localhost:1521:CPSC`

Note This is the connection to the Cisco Prime Service Catalog database. You will need to change the example provided to replace *localhost* with the address to your actual database server. Only use *localhost* if you are using the built-in Oracle server. (But use the built-in Oracle server only as a test or proof of concept server. Also, ensure the port number being used matches the port number you have set up for your database implementation (the port numbers provided are the defaults as defined by Microsoft or Oracle).

Note Cisco Prime Service Catalog does not allow you to copy text from certain fields. This is why you must type this URL into the JDBC URL field.

Step 4 Enter the appropriate URL (either MS SQL or Oracle, depending on your setup) into the **JDBC Driver Class** field.

Tip Be sure there are no spaces at the beginning or the end of the string.

Step 5 Click **Submit Order**.

Note Monitor this requisition to be sure it completes. Only move on once you are certain that the requisition has completed.

Starting a DB Agent

Follow these steps to enter credentials for connecting to the database.

Step 1 From the Wizard, choose Start DB Agent.

Step 2 Navigate to the page with the agent.

Step 3 On the Control Agents Tab of the Service Links portal, choose **Insert Default Parameters**.

Step 4 Click **Start Chosen**, and then click **Yes** to confirm.

Step 5 Refresh the page and the red light icon next to **Insert Default Parameters** will turn green.

Step 6 Choose **Portal Page Assignment to OU**.

Step 7 Navigate to the page with that agent.

Step 8 Click **Start Chosen**, and then click **Yes** to confirm.

Step 9 Refresh the page until the red light icon next to **Portal Page Assignment to OU** turns green.

Step 10 Click **Close**.

Configuring the nsAPI Agent

To configure the nsAPI agent:

Step 1 From the Wizard, choose Configure NSAPI Agent.

Step 2 On the Set Agent Configuration form, complete the following:

- Set Agent Type to NSAPI (may already be set; be sure to check).
- Choose **Basic** as the Authentication Scheme.

Note This value must be set to "Basic," otherwise nsAPI will not function correctly and you will not be able to properly continue Day 0 setup.

- Enter the nsAPI username and password (as created earlier).
- Reenter the password to confirm.

Step 3 Click **Submit Order**.

Note Monitor this requisition to be sure it completes. Refresh as needed. Only move on once you are certain that the requisition has completed.

Starting the nsAPI Agent

Step 1 From the Wizard, choose Start NSAPI Agent.

Step 2 On the Control Agents Tab of the Service Links portal, choose **Retrieve OU ID on Name**.

Step 3 Navigate to the page (it may be a few pages in).

Step 4 Click **Start Chosen**.

Step 5 Click **Yes** to confirm.

Step 6 Click **Close**.

Setting Up Cloud Administration

Adding a Cloud Administrator Organization

On the **STEP 2** panel of the Cisco IAC Configuration Wizard, you create the home organization for **Cloud Provider Technical Administrators (CPTA)**. CPTAs manage cloud resources and services via the service catalog. They have access to internal network and systems (underlying cloud infrastructure) and onboard/offboard tenants.

Once you have set up the Cloud Organization, you are returned to **STEP 2**. At that time (after the Wizard redisplays), the link for "Add Cloud Administration Organization" has been removed. This is to ensure that you do not inadvertently run that task more than once.

Step 1 From the Wizard, choose Add Cloud Administrator.

Step 2 On the Add Cloud Administration form, enter the following:

- Cloud Admin Organization Name (required)
- Organization Description (optional)
- Company Abbreviation (required; maximum 4 characters)

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Note Monitor and refresh screen as needed. Only move on once you are certain that the process has completed.

Adding Cloud Administrators

Step 1 From the Wizard, choose Add Cloud Administrator(s).

Step 2 On the Add Cloud Administrator form, choose **Create New User** from the drop-down to display the fields for creating a new user as a Cloud Administrator.

Step 3 Provide the following information:

- Enter the first and last name of the new Cloud Provider Technical Administrator.
- Enter a unique login identifier for the Cloud Provider Technical Administrator.
- Enter the new Cloud Administrator's e-mail address.
- From the drop-down list, choose the time zone associated with the new CA's primary address.
- Enter then re-enter the password for the new Cloud Administrator.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Submit Order**.

Step 6 Click **Close** when the status says **Completed**.

Note Monitor and refresh screen as needed. Only move on once you are certain that the process has completed.

Adding Cloud Administrators: Directory Service Users Only

This section applies *only* if you are using a directory service to import user and organization data. Before you proceed, directory integration must be set up. After you set up directory integration, users are automatically imported when they log in, and their Prime Service Catalog roles are automatically assigned based on the user groups to which they were added in the directory.

- User roles are assigned when you define group role mappings during directory integration setup (as shown in "Adding the nsAPI User to the Cloud Administration Group" section on page 5-6).
- You assign the Cloud Administrator role to a user from the directory, rather than from Cisco Prime Service Catalog, by adding the user to the Cloud Administrator user group in the directory.

Making nsAPI a Cloud Provider Technical Administrator

Step 1 From the Wizard, choose Make nsAPI a Cloud Provider Technical Administrator.

Step 2 On the Add Cloud Administrator page, click **Choose an Existing User**.

Step 3 Choose the nsAPI user and then click **Submit Order**. You may see a popup displays the following message: `"The user you have chosen currently belongs to another organization.Assigning the Cloud Administrator role will automatically set user organization to the Cloud Administrator Organization. If you want to assign the role but not modify the Organization. you can do so through Organization Designer"`

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Adding Site Administrator Role to nsAPI User

If you are using a directory service, see the information in the following section, Adding Cloud Administrators, page 7-10.

Step 1 From the Wizard, Step 2, click Add Site Administrator role to nsAPI user.

Step 2 Choose the nsAPI user.

Step 3 Choose **Roles** on the right of the screen.

Step 4 Click **Add** under the list of Roles first to open the search bar.

Step 5 Search for "Site Administrator".

Step 6 Check the **Site Administrator** check box.

Step 7 Click **Add** and click **Close**.

Connecting Cisco Process Orchestrator

Here, you register and connect the various platform elements to be used for the cloud. This setup must be completed before any further setup or usage of the cloud environment can take place.

Step 1 From the Wizard, choose Connect Cisco Process Orchestrator.

Step 2 On the Connect Cloud Infrastructure Screen, choose Cisco Process Orchestrator.

- Enter **Connection Name** (optional)
- Verify the Cloud Portal **Host Name** and **Port Numbers**.
- Ensure Cloud Portal **Connection Encrypted** option is set to False.

Tip The Connection Encrypted is set to "False" by default. Setting to "True" would require SSL being set up and enabled on Cisco Process Orchestrator, which is not required for Cisco IAC 4.1.1.

- Enter the **NSAPI username.**
- Enter the **NSAPI Password**.
- Enter the Process Orchestrator **Connection Name** (optional)
- Enter the Process Orchestrator **Host Name**.
- Verify the Process Orchestrator **Port Number**.
- Enter the Process Orchestrator **Administrator username**.
- Enter the Process Orchestrator **Administrator Domain** (if applicable).
- Ensure Process Orchestrator **Connection Encrypted** option is set to False.

- Choose the Process Orchestrator **Authentication Scheme**.
- Enter the Process Orchestrator **Administrator Password**.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Tip This task of setting the Process Orchestrator values cannot complete until all agents are started, which includes Process Orchestrator. Without the agents running the process can not complete.

Step 5 Enter the Service Link Port for Cisco Cloud Portal.

Step 6 Enter the host name or IP address of the Cisco Cloud Portal

Step 7 Enter the Request Center Port for Cisco Cloud Portal.

Step 8 Click **Close**.

Starting All Other Agents

Finally, you need to start all of the other agents in order to successfully finish this procedure. Wait for at least two minutes before starting this step.

Step 1 From the Wizard, choose Start all other agents.

Step 2 On the Control Agents Tab of the Service Links portal, choose every single agent on every page with a red light icon.

Step 3 Click **Start Chosen**, and then click **Yes** to confirm.

Step 4 The red light icon next to all the remaining agents will turn green. To see if they turn green, click **Refresh** (bottom right corner) to check the new status.

Note There may have been additional agents in the list that you were not able to see (and therefore, activate). To find agents, use the scroll arrow at the bottom of the list or the “next page” button at the bottom of the screen.

Step 5 Click **Close** when completed.

Initializing Cisco IAC Licensing

Step 1 From the Wizard, choose Initialize licensing.

Step 2 Click **Submit Order**.

Step 3 Click on the number in the **Requisition Number** field to display the details.

Step 4 Click **Close** when the status says **Completed**.

Connecting to the Cloud Infrastructure

On the **STEP 3** panel of the Configuration Wizard, you define the connection information for the platform elements that will be used in Cisco IAC. This information will be used by Cisco Process Orchestrator to integrate with the various components involved in the cloud provisioning processes.

Note This step needs to be repeated multiple times for each Platform Element Infrastructure item you intend to connect to.

Step 1 *Log out* of Cisco IAC, close your browser, and then restart it.

Step 2 *Log back in* to Cisco Intelligent Automation for Cloud as the Cloud Provider Technical Administrator (CPTA) you created previously. (See Adding Cloud Administrators, page 7-10.)

Step 3 Once back in, start the Wizard again. Choose Setup > Configuration Wizard.

Step 4 Click **Next**.

You will be returned to **STEP 3** of the Wizard, with two new tasks to complete.

Connecting Cisco IAC Management Appliance (Optional)

Timesaver If you do not intend to use Advanced Network Services (VSA 1.0), then connecting a Cisco IAC Management Appliance is not required.

Step 1 From the Wizard, choose Connect Cisco IAC Management Appliance.

Step 2 On the Connect Cloud Infrastructure form, do the following:

- Choose the **Platform Element Type**.
- Enter a **Connection Name**, **Host Name**, **Description**, and **Port** number.
- Set **Secure Connection** and **Ignore Certificate Error** to either True or False, as needed.
- Enter the **Assurance Control Password** and **User Name.**
- Enter the **Administrator Password** and **User Name**.Reenter the password to confirm. If you are using the Cisco IAC Virtual Appliance, the user is “admin,” and the password is the one you specified earlier.

Note If you are using the Cisco IAC Virtual Appliance, some of this information has been already entered for you.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Connecting Cloud Infrastructure

You can connect to any infrastructure of your choosing, including VMware, UCS Director, Amazon EC2, OpenStack, Chef, Puppet, the Management Appliance, and PNSC, among others.

Note You have to add at least one Cloud Platform Element before you can proceed to Step 4 of the Wizard.

Note Below are the specific instructions for vCenter, but these will be similar for any Platform Element. For more information, see the *Cisco Intelligent Automation for Cloud Administration Guide.*

Step 1 From the Wizard, choose Connect Cloud Infrastructure.

Step 2 On the Connect Cloud Infrastructure form, under Connect VMware vCenter Server, do the following:

- Choose VMware vCenter as the **Platform Element Type**.
- Enter a **Connection Name (Friendly Name)**.
- Enter a **Host Name**, a **Port** number and a **Description**.
- Set the following to either True or False, as needed:
  - **Secure Connection**
  - **Ignore Certificate Error**
  - **Managed by UCS Director**
- Enter **username** and **Password**, the reenter the password to confirm.

Tip You may need to enter the domain name before the username followed by a backslash.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Note Repeat the steps above to add a Prime Network Services Controller (if using ANS), Prime Performance Manager (if you are tracking VM performance), AMQP Server, Chef, or Puppet.

Discovering Cloud Infrastructure (Optional)

Discovering Network Devices (Optional)

The purpose of **STEP 4** is to discover your physical and virtual network appliances.

Note This process can take anywhere from 10 minutes up to an hour.

Timesaver Save for your first Prime NSC, you do not need to pre-provision the virtual devices. Cisco IAC will provision all these devices for you when the first Tenant Organization is onboarded that has elected for Advanced Network Services. If you are not planning on using Advanced Network Services (VSA 1.0), you may skip Step (Tab) 4 and move on to Step (Tab) 5 directly.

Note You do need to have Nexus1000v Virtual Access Switch installed and integrated with VMware as well as a range of VLANs identified in the data up-link. The range of VLANs you intend to specify in your Network PoD should be passed in the data-uplink trunk from N1kv to the ESXi hosts (its VEMs). Cisco IAC does not configure this for you.

Step 1 To discover network devices, from the Wizard choose Discover Network Devices.

Step 2 You are returned to the wizard Step 4 screen.

Step 3 Click **Next** to proceed to Step 5 in the Wizard.

Registering Nexus 1000v Devices (Optional)

Devices which you have discovered and then register are those devices which you want dynamically created VLANs (by Cisco IAC) to be propagated to. So register a device if you want Cisco IAC to go configure the VLAN on it.

Step 1 To register Nexus 1000v devices, from the Wizard choose Register Nexus 1000v.

Step 2 Complete the online process to register Nexus 1000v devices. When you are done, click **Next**.

Note Registration gives the device a “friendly name,” defines the Device Role, and identifies the linkage to the PNSC it is currently integrated with.

Managing PODs

On the **STEP 5** panel of the Wizard, you create PODs and choose the instances that manage its resources. A POD (Point-of-Delivery) contains the platform elements and a data center.

Registering Network PODs

Tip This step is optional. However, it is mandatory if you are using Advanced Network Services. The Network POD is also required for OpenStack as well as Advanced Network Services. Cisco IAC 4.1.1 provides the ability to dynamically provision tenant networks within VDCs.

Use the Register POD service to register an installed POD (Point Of Delivery) and choose the instances that manage its resources, so that you can start using it in the cloud. You must be logged in as a Cloud Provider Technical Administrator to create a network POD in Cisco IAC 4.1.1.

Step 1 From the Wizard, choose Register Network POD.

Step 2 On the Register Network Pod form, define the platform elements:

- Assign a name for this POD.
- Assign a description for this POD.
- *Optional.* Choose the UCS Manager that is to serve this POD.

Note Any physical devices acting as Edge Routers or Layer2 Aggregation Switches should also be selected.

Note The **VLAN Pool** field must have a range of VLANs that Cisco IAC can use to create tenant networks. It is also used in the dynamic creation of Enterprise Transit port-profiles/network when Connection-Type is Enterprise during the process of creating an organization and Load Balancer Networks.

Tip There is a 1-to-1 mapping between UCS Managers and PODs. If the drop-down list is empty, all available UCS Managers have been associated with a POD. For information about defining a new UCS Manager, see Understanding Cisco UCS Manager Service Profile Templates and Policies, page 2-2.

Tip UCS Fabric Inter-connects will also appear in the list for select under the Network POD. The UCS Manager as well as its Fabric Inter-connects should all be selected together.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Note Devices which you have discovered and then register are those devices which you want dynamically created VLANS (by Cisco IAC) to be propagated to. Therefore, register a device if you want Cisco IAC to configure the VLAN on it and choose them when creating the network POD.

Creating Compute PODs

Use the Create POD service to register an installed compute POD (Point Of Delivery) and choose the cloud infrastructure platform elements that manage its resources.

Note There is a 1-to-1 mapping between datacenters and PODs (one between DataCenter and Compute POD; refer to the object model). If the drop-down list is empty, all available datacenters have been associated with a POD.

Note Multiple data centers are supported through multiple Compute PODs. Multiple Compute PODs can reference the same network POD.

Step 1 From the Wizard, choose Create Compute POD.

Step 2 On the Create Compute POD form:

- Enter a new short name and a full description for the Compute POD.
- Choose your Cloud Infrastructure Type, such as VMware vCenter Server.

  Note There are other infrastructure types beyond VMware vCenter Server used in this example.

- Choose the Network POD instance that serves in this POD.
- Choose the vCenter Instance.
- Choose the Datacenter.
- Choose UCS Manager.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Setting System-Wide Services and Provisioning

On the **STEP 6** panel of the Wizard, you choose the system-wide services to offer and enter critical information for provisioning the cloud servers, such as network domain name and default time zone. When you have completed Step 6, click **Next**.

Setting System-Wide Service Options

When a service is disabled, ALL users, including the CTPA, are disallowed from ordering the given service. Although users can see the link to a disabled service, a "disabled" message displays, and "Submit" buttons are hidden on the service forms.

Tip You can re-enable a disabled service at any time. Disabling an option only affects what users can order from the catalog from the time the Set System Wide Service Options service order is fulfilled. It does not affect current services already ordered.

Step 1 From the Wizard, choose Set System-wide Service Options.

Step 2 Choose the proper options based on your hardware inventory.

Step 3 Disable a service by clicking the **No** radio button, or re-enable a disabled service by clicking the **Yes** radio button.

Step 4 Click **Submit Order**.

Step 5 Click on the number in the **Requisition Number** field to display the details.

Step 6 Click **Close** when the status says **Completed**.

Specifying Provisioning Settings

Specify the settings for virtual machine (VM) provisioning, then verify that the VM provisioning settings are configured correctly.

Step 1 From the Wizard, choose Set Provisioning Settings.

Step 2 On the Server Provisioning Settings form, specify the following:

- Enter the period of time allowed, specified in minutes, before a virtual machine deployment operation is determined as failed.
- Enter the amount of time, in whole hours, to suppress duplicate alerts related to cloud automation.
- The amount of time, in whole hours, between consecutive periodical executions of the CloudSync infrastructure discovery service.
- The period of time allowed, specified in minutes, before a CloudSync Discovery operation is determined as failed.
- The amount of time, in minutes, between consecutive periodical executions of platform element connection validation services.
- Enter the name of the Windows domain for commissioned Windows servers to join.
- Enter the username and password for the Windows domain user to join the Windows VM to the Windows domain.
- *Linux only.* Choose the default time zone for the Linux server from the drop-down list. For valid time zone values, see the VMware documentation on VMware.com.
- *Windows only.* Choose the default time zone for the Windows server from the drop-down list. For valid time zone values, see the VMware documentation on VMware.com.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Configuring the E-Mail Notification Templates

Cisco IAC includes a set of default (delivered as part of Prime Service Catalog) e-mail notification templates that you customize for an organization. The cloud system sends the e-mail notifications in response to events such as orders and system errors. Before users can start ordering cloud services, you must configure the e-mail notification templates with the relevant sender and recipient addresses.

Step 1 From the Wizard, choose Set System Email Account.

Step 2 For the editing window, click either the HTML Part or Text Part radio buttons to choose an editor.

Step 3 In the editing panel, modify the default content and add optional content as needed.

Step 4 Click **Update**.

Step 5 Repeat Step 2 through Step 4, above, for the e-mail templates on the Request Center tab.

Assigning From Address for E-Mail Templates

You must assign the From address for the default templates to use for outgoing notification e-mail messages. E-mail cannot be sent without a fully-qualified e-mail address. Follow these steps to assign an e-mail address for the default e-mail templates.

Step 1 Click **Set System Email Account**.

Step 2 Enter the e-mail address you would like to use as the default from address for outgoing notification e-mail messages in the **Sender e-mail Address** field.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Creating Resources for Network Services

On the **STEP 7** panel, you register a datastore, add community and user networks to which users can deploy servers, management networks, and infrastructure networks to be used for creating a Community VDC.

Note Infrastructure networks are also used for management and service interfaces of Virtual Network Devices.

- When you have completed all of the tasks in Step 7, click **Next**.
- If you do not wish to add networks or create a Community VDC, click **Skip**.

Registering a Datastore

Datastores that are discovered automatically during Connect Cloud Infrastructure must be registered before they can be used in the Community VDC community and organization virtual data centers. A single datastore can be used by one or more Virtual Data Centers.

Step 1 From the Wizard, choose Register Datastore.

Step 2 On the Register Datastore form, choose a datastore with a status of "Discovered" to be registered for use.

The form will populate with information specific to the datastore you chosen.

Step 3 Enter a friendly name and description (for example, the type of storage) for the datastore. (Optional)

Step 4 Click **Submit Order**.

Step 5 Click on the number in the **Requisition Number** field to display the details.

Step 6 Click **Close** when the status says **Completed**.

Creating a Service Network

Use the Add Network form to define a VLAN and subnet to use in the cloud system use, for user servers, server management, or for use by the cloud infrastructure.

Tip If you have many hosts, when adding networks, be sure to choose the same port group for each host.

Step 1 From the Wizard, choose Create Service Network.

Step 2 On the Add Network form, from the drop-down choose a **Cloud Infrastructure Type**. Types include:

- Amazon EC2
- Cisco UCS Director
- Openstack Cloud Manager
- VMWare vCenter Server
- VMWare vCloud Director

Note Depending on the cloud infrastructure type you choose, you will then see a selection of different fields populate the screen.

Step 3 Complete the cloud infrastructure fields as required for each type. For example, you may be asked to provide any of the following (as well as other information):

- **Network Name:** Enter a short name for the network that will be shown to users in drop-down selection lists.

- **Subnet Address Specification:** Enter the network for this subnet in CIDR notation. For example, 192.168.20.0/24. Enter only an IPv4 type of IP address. Note: Only networks from /23 through /29 are supported.
- **Community Network:** Choose the network access scope for user networks. A community network is available to users in Community VDCs. Non-community networks require explicit VDC level access to be set before users can deploy servers to it, which is useful for traffic isolation and better security.
- **Public Network:** Specify the duplication policy for this network. Public networks are globally unique, while private networks must only be unique within associated network device contexts.
- **Network Type:** Choose a network type to determine how this network can be used. User networks are used for deploying virtual machines or physical servers. Management networks are used for management access to cloud servers. Infrastructure networks are used for management interfaces of hypervisor hosts and other infrastructure devices.

Note For Advanced Network Services, use "Infrastructure" type for Service, Infrastructure, and Internet Transit. (Theses are the three networks you are asked for when you create a Service Resource Container).

- **Network Source:** Choose how IP addresses management is done in this network. Cisco Prime IPAM, DHCP, Internal, External. Internal is managed by Cisco IAC.
- **Additional:** In addition, you may need to enter any of the following:
  - **Subnet Mask**
  - **Gateway Address**
  - **FHRP1 (First Hop Redundancy Protocol) and FHRP2 Address**
  - **Broadcast Address**
  - **Primary DNS** and **Secondary DNS**

Tip Depending on the cloud infrastructure type you chosen, the form may populate with infrastructure-specific fields which also may be required. Be sure to complete these fields as well. In all cases, the red asterisk will indicate the required field or fields.

Step 4 Click **Submit Order**.

Step 5 Click on the number in the **Requisition Number** field to display the details.

Step 6 Click **Close** when the status says **Completed**.

Creating Infrastructure Networks

From the Wizard, choose Create Infrastructure Network.

Note The steps for this procedure are the same as outlined in the Creating a Service Network, page 7-20.

Creating an Internet Transit Network (Optional)

This is for use in Advanced Network Services to provide Internet Transit Network Connectivity to Organizations. Connectivity from Tenant Org CSRs to the Datacenter/Provider Edge ASRs.

Note The steps for this procedure are the same as outlined in the Creating a Service Network, page 7-20.

Creating the Service Resource Container (Optional)

This is where the Compute POD is associated with the Infrastructure, Service and Internet Transit Networks. In addition, this is also where the target Cluster and Datastore to be used within the Datacenter (identified by the Compute POD) is selected. One place the Service Resource Container is used is during Creation of Organizations to specify the Network an Compute resources to be used by that Organization.

Note The Service Resource Container is *required* for ANS and OpenStack.

Configuring Resources for Network Services (Optional)

From the Wizard, choose Configure Resource for Network Services.

Note The steps for this procedure are the same as outlined in the Creating a Service Network, page 7-20.

Adding a Public Subnet to Network POD (Optional)

Note This is the subnet IPs for Advanced Network Services UnProtected Public Tenant Network and VMs, Floating IPs (Static NAT), and Public VIPs.

Step 1 From the Wizard, choose Add Public Subnet to Network POD.

Step 2 On the Add Public Subnet to Network POD form, enter the following:

- **Subnet Address**. The network address of the subnet.
- **Subnet Bitmask**. The bitmask (numeric) of the subnet you are adding. Do not include the slash.
- **Network POD Name**.
- **Assigned Subnets**. The public subnets that have already been assigned.
- **Unassigned Subnets**. The free public subnets remaining in the pool.

Step 3 Click **Submit Order**.

Step 4 Click on the number in the **Requisition Number** field to display the details.

Step 5 Click **Close** when the status says **Completed**.

Completing the Setup

Now that you have completed all of the required steps in the Configuration Wizard, your cloud environment is ready for ordering. The final phase, is to set or check certain permissions as follows.

Note Most of these permissions will already be set, but problems may arise with the Cisco Intelligent Automation for Cloud 4.1.1 installation if these permissions are not set properly.

Step 1 Access the Organization Designer.

Step 2 Update all CPTA and TTA Roles.

Execute all services:

- **Service Order Service > All**

Access all service items:

- **Service Item Instance data**: Choose **Read all**

Step 3 Update all OTA, TTA, and Server Owner Roles.

- **Service Item Instance** data: Choose **Read all service items** from my BU WebServices
- Add:
  - nsAPI access
  - Requisition Access
  - Requisition System Account

Tip For more information on Organizations, Templates, Users, and so on, see the *Cisco Intelligent Automation for Cloud 4.1.1 Administrator Guide.*

Upgrading From Cisco IAC 4.1 to 4.1.1

Upgrading from Cisco IAC 4.1 to IAC 4.1.1 with Cisco Prime Service Catalog 10.1

The following steps present a simplified and high level view of how to upgrade from Cisco Intelligent Automation for Cloud 4.1 to Cisco IAC 4.1.1. along with Cisco Prime Service Catalog. For more detailed information, see the *Cisco Prime Service Catalog 10.1 Installation Guide* for more information: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog/products-installation-guides-list.html

Note Be sure to create a backup of both the Cisco Process Orchestrator database and the Cisco Prime Service Catalog Request Center database before you upgrade to Cisco IAC 4.1.1.

Step 1 Stop Prime Service Catalog and Cisco Process Orchestrator and backup databases.

Step 2 Upgrade SQL 2008 to SQL Server 2012 SP1 or SP2.

Note Cisco Prime Service Catalog 10.1 requires Microsoft SQL Server 2012, so you will need to move the PSC database to a SQL 2012 Server. Alternatively, you could upgraded the SQL 2008 Server hosting the PSC database to SQL 2012.

Step 3 Change Service Catalog database mode to SQL 2012.

- `SQL Management Studio > Request Center > Options > compatibility level to SQL server 2012 (110)`

Step 4 Install jdk 1.7 in the PSC machine.

- Add the <*path_to_jdk_1.7_java_executable*> to the PATH environment variable. You may have multiple Java installation on your machine. Just make sure that the path to the java executable for JDK 1.7.0_x is first in the path of the PATH environment variable. This is what the PSC 10.1 Installer will use when it is first launched.
  - On Windows: PATH=C:\jdk1.7.0_55\bin\java;%PATH%
  - On Linux: export PATH=/opt/jdk1.7.0_55/bin/java:$PATH

Step 5 Install Java Security files on the PSC machine.

- Copy the unlimited strength policy jar files to <*JDK_1.7_home_dir*>\jre\lib\security directory, overwriting the existing jar files.

Note The unlimited strength policy files are "local_policy.jar" and "US_export_policy.jar", which can be downloaded from the following link: http://www.oracle.com/technetwork/java/javase/downloads/jce-7-download-432124.html

Step 6 Upgrade Prime Service Catalog to 10.1 from cisco.com. Apply all available 10.1 patches as well.

Note Follow the instructions in the *Cisco Prime Service Catalog 10.1 Installation Guide* to upgrade Prime Service Catalog to 10.1: http://www.cisco.com/c/en/us/support/cloud-systems-management/prime-service-catalog/products-installation-guides-list.html

Step 7 Start Prime Service Catalog and make sure you can login.

Step 8 Extract ADK and install the REX adapter.

- Stop Prime Service Catalog
- Extract the adk.zip from the Prime Service Catalog installer to a folder and in that folder replace `kek_new.txt` and kek_old.txt, the KeK files to be taken from your PSC build in this location RequestCenter.war\WEB-INF\classes\config\
- Copy `adapter_REXAdapter.jar` from CiscoPrimeServiceCatalogR2\jboss-as-7.1.1.Final\ServiceLinkServer\deployments\ServiceLink.war\WEB-INF\lib to the new CiscoPrimeServiceCatalog.
- Install the Rex adapter:
  - Open a command window, and cd to the <adk> folder.
  - Set JAVA_HOME to the 1.7 jdk.
  - Run adapter_dbinstaller.cmd (Windows) or adapter_dbinstaller.sh (Linux)
- The following is a sample run for MS SQL Server:
  - c:\adk>adapter_dbinstaller.cmd
  - Please enter the database connection information.
  - Database Type [SQLSERVER]:
  - Database Hostname [localhost]:
  - Database Port [1433]:
  - Database Name [ServiceCatalog]:
  - Username [RCUSER]: RCUser
  - Password:
  - Testing database connection: Success!
  - Adapter Deployment Descriptor File: c:\rex\REXAdapter.xml
- The following is a sample run for Oracle/Linux:
  - c:\adk>./adapter_dbinstaller.sh
  - Please enter the database connection information.
  - Database Type [SQLSERVER]: Oracle
  - Database Hostname [localhost]:

- Database Port [1521]:
- Database Name [ServiceCatalog]:
- Username [CPSCUSER]: CPSCUser
- Password:
- Testing database connection: Success!
- Adapter Deployment Descriptor File: c:\rex\REXAdapter.xml
- Install REX

Step 9 Start Prime Service Catalog.

Upgrading Process Orchestrator

You need to upgrade Cisco Process Orchestrator, as well. For full instructions, refer to the most recent Cisco Process Orchestrator documentation, which can be found here: http://www.cisco.com/c/en/us/support/cloud-systems-management/process-orchestrator/tsd-products-support-series-home.html.

Important Information About Upgrading

- We do not support direct upgrades from Cisco IAC versions earlier than 4.0; for example upgrading from Cisco IAC 3.1 to Cisco IAC 4.1.1. We support only upgrades from 4.1 to Cisco IAC 4.1.1.
- Upgrading may cause certain custom content changes in Cisco Prime Service Catalog to be overwritten. We recommend that you run the upgrade process first in a test environment.
- See the *Cisco Intelligent Automation for Cloud 4.1.1 Compatibility Matrix* for the exact versions of the Cisco (and third-party) software compatible with Cisco IAC 4.1.1.
- Refer to "Post-Upgrade Tasks" section on page A-7 for information on additional post-upgrade tasks you will need to attend to after successfully upgrading to Cisco IAC 4.1.1.

Tip After the upgrade process has finished, be sure to notify all Cisco IAC users to refresh their browser cache. They will continue to see the previous version of Cisco IAC until they do so.

Updating Agents

Tip You need to upgrade agents only when upgrading *manually*. For *new* installations of Cisco Intelligent Automation for Cloud 4.1.1, this task is handled using **Setup > Configuration Wizard** (Day 0).

Step 1 Log into Prime Service Catalog as site administrator.

Step 2 Stop all agents.

Step 3 Choose Service Link > Choose Control Agents.

Step 4 Choose the agent called “REX Set REX Agent Properties.”

Step 5 Choose Outbound Properties.

Step 6 Update the REX username and password.

- Start the agent called “REX Set REX Agent Properties.”
- Open a new browser, log into the service catalog, and go to Service Portal > Setup > System Settings.
- Click Set REX Agent Configuration, enter the username and password for the REX user.
- Click **Submit Order**.

Step 7 Go to the other browser tab to monitor the status of the Set REX Agent Configuration task launched in the previous step.

- Choose Service Link from the drop-down menu.
- Click on the View Transactions tab in the menu bar.
- Click on the External Tasks tab in the main window.
- Wait for the Set REX Agent Configuration task to complete.
- Choose Control Agents and start All REX agents.

Step 8 Go back to Service Portal > Setup > System Settings.

- Choose **Set Agent Configuration**.
- Submit a configuration order for each Agent Type in the drop-down menu (HTTP, NSAPI, DB). See the help text for instructions and examples. Be sure there are no spaces at the beginning or end of the copied help text. Unexpected errors may occur as a result of these spaces. This applies only to DB agent configuration.

Step 9 Go to the other browser tab to monitor the status the NSAPI, HTTP and DB agent configuration tasks launched in the previous step.

- Choose Service Link from the drop-down menu.
- Click on the View Transactions tab and wait for all Set Agent Configuration task to complete. Here are two examples:
  - (MS SQL) `example:jdbc:sqlserver://localhost:1433;DatabaseName=RequestCenter;selectMethod=direct;sendStringParametersAsUnicode=true`
  - (Oracle) `jdbc:oracle:thin:@localhost:1521:XE`

Step 10 Start all agents.

Upgrading and Sub-Interface Support

When upgrading to Cisco IAC 4.1.1 from Cisco IAC 4.*x* with Cloud Services Router (CSR) 3.13 3.13.1S(ED), followed by an upgrade to Cisco Prime Network Services Controller (PNSC) 3.4(x), we only allow sub-interfaces for newly created organizations, preserving the physical interface configuration of existing organizations.

Tip Sub-Interface support on CSR in Cisco IAC 4.1.1 release requires the latest versions of CSR and PNSC. For the complete list of interoperable components and version/release information, see the *Cisco Intelligent Automation for Cloud 4.1.1 Compatibility & Requirements Matrix.*

Upgrading PNSC for Sub-Interface Support

Cisco Intelligent Automation for Cloud 4.1.1 has a new minimum Prime Network Services Controller (PNSC), Cloud Services Router (CSR), Virtual Security Gateway (VSG), Nexus 1000 (N1kv) supported versions, listed below.

Interface	Supported Version
CSR	3.13.1S(ED)
N1kv	5.2.1.SV3.1.1
VSG	Nexus1000v.5.2.1.VSG.2.1.2
PNSC	3.4(x)

Note Upgrading to the latest version of Prime Network Services Controller is mandatory to support Sub-Interface creation on CSR.

Note You should upgrade your IAC Management Appliance or push the new version of Cloud Services Router to your existing appliance repository. Then discover and update set provision settings. The 4.1.1 version of the appliance contains only Cloud Services Router version 3.13.1S(ED).

Tip For more information, see the *Cisco Prime Network Services Controller Upgrade Guide*: http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/network_services_controller/3-2/quick-start-guide/b_Cisco_Prime_Network_Services_Controller_32_Quick_Start_Guide.html#d25e7970a1635

Warning **After the Prime Network Services Controller upgrade, it is required that an "Update Cloud Infrastructure" service order be executed for the PNSC platform element just upgraded, using Cisco Prime Service Catalog. This will update the PNSC version in the PNSC Service Item table.**

Existing Organizations, Before Upgrade

- New networks added to existing Virtual Data Centers (VDCs) as well as new VDCs will use physical interface creation. (Only if upgrading from 4.0 patch 4.)
- Decommissioning of existing VDCs works as expected and is not affected by the upgrade.

Newly-Created Organizations, After Upgrade

- Newly created VDCs, as well as networks added to the new VDCs, will use sub-interface creation.

Note Only new Organizations support sub-interface creation. New VDCs and new networks within these VDCs that belong to new organizations will use the sub-interface creation functionality. New VDCs and their networks created in existing Organizations do *not* support sub-interfaces and will continue to use physical interface creation.

Upgrading CSR and Sub-Interfaces Support

When deploying Cloud Services Routers (CSRs) from version 3.12 to CSR version 3.1.3, we expect the following behavior:

- Existing organizations with CSR 3.12 will not be affected by the Cisco IAC upgrade nor by the CSR upgrade and will continue to use only physical interfaces.

Tip For more information, see the *Cloud Services Router Upgrade Guide*: http://www.cisco.com/c/en/us/td/docs/routers/csr1000/software/configuration/csr1000Vswcfg/swupgradecsr.html

Deploying or Upgrading PNSC

You need to deploy or upgrade Install Cisco Prime Network Services Controller (PNSC) to the latest version (3.4.*x*).

Tip For the complete list of interoperable components and version/release information, see the *Cisco Intelligent Automation for Cloud 4.1.1 Compatibility & Requirements Matrix* located here: http://www.cisco.com/c/en/us/support/cloud-systems-management/intelligent-automation-cloud/tsd-products-support-series-home.html.

Deploying the IAC Management Appliance for CSR

You need to deploy the Cisco IAC Management Appliance to update to the latest compatible version of Cloud Services Router (CSR), which is version 3.13, and to the latest version of Virtual Security Gateway (VSG), which is 2.12.

Post-Upgrade Tasks

Tip After the upgrade process has finished, be sure to notify all Cisco IAC users to refresh their browser cache. They will continue to see the old version of Cisco IAC until they do so.

Adding Permissions

The following permission needs to be added to roles OTA, TTA and VSO using the Organization Designer after upgrade: “Read all Instance Data and Service Item Instance Data-OpenStack Projects.” Also, you will need to add/update portal and portlet permissions.

Deploying New Cisco IAC 4.1.1 Management Appliance

After successfully upgrading to Cisco IAC 4.1.1, you will need to deploy the new Cisco IAC Management appliance. This appliance includes new components such as:

- Prime Performance Manager (PPM)
- Assurance Control
- RabbitMQ
- ACM repository

Note After deploying appliance, update, update the Cisco IAC 4.1.1 management appliance platform element using **System Settings > Connections**.

Setting System-Wide Service Options

Set your system-wide service options after you upgrade using the Set System-wide Service Options form using **Setup > System Settings > System Settings tab**.

Application Configuration Management Support

To use an existing tenant created in an earlier version of Cisco IAC, your CPBA or CPTA will need to create the “ACMTemplate Rate” table manually.

Note For instructions on creating the “ACMTemplate Rate” table manually, see the Cisco Intelligent Automation for Cloud Knowledge Base.

Solution Prerequisites Checklists

Default Ports and Protocols

Table B-1 Requirements—Default Ports and Protocols

Application	Default Port	Protocol	Description	✓
Cisco Prime Service Catalog	8080	TCP	Client web browser connections to the Cisco Prime Service Catalog ServiceCatalog; Process Orchestrator communications to the Cisco Prime Service Catalog request center inbound web service	
	6080	TCP	Process Orchestrator communications to the Cisco Prime Service Catalog service link inbound web service.	
Process Orchestrator	2081	TCP	User Web browser connections to the Process Orchestrator web console	
	61525	TCP	Process Orchestrator Console access to the Process Orchestrator Server	
	61526	TCP	Web Service (API) communication using HTTPS protocol from the Cisco Prime Service Catalog to the Process Orchestrator web service	
	61527	TCP	Web Service (API) communication using HTTP protocol from the Cisco Prime Service Catalog to the Process Orchestrator web service	

Limitations and Scalability

Table B-2 Limitations and Scalability

Entity	Limitations	✓
Cisco UCS Manager	1 instance per delivery (POD). Each POD can contain up to 160 blades/host.	
Cisco Process Orchestrator server	1 Process Orchestrator environment supported by Cisco IAC. Note that multiple servers may be installed in that Process Orchestrator environment	
Registered users	Up to 1,000; up to 200 concurrent users	
Service items (concurrent)	Up to 10,000	
VMware vCenter	1 instance	

Storage Management Requirements

Table B-3 Requirements—Storage Management

Requirement	✓
Create storage and configure as datastores	

Cisco UCS Manager Provisioning Requirements

Table B-4 Requirement—Installing and Configuring UCS Manager

Requirement	✓
UCS Manager is installed and configured before installing Cisco IAC	

Table B-5 Requirements—Creating UCS Manager Pools

Requirement	✓
UUID suffix pool	
MAC address pool	
WWNN pool	
WWPN pool	

Table B-6 Requirements—Creating Cisco UCS Manager Service Profile Templates and Policies

Requirement	✓
A hypervisor service profile template, per cluster, with the same quantity and configuration of vNICs as on other hosts in the same cluster. The native VLAN for the first vNIC should be set to the Management VLAN for that vCenter. **Note** Required only if ESXi Provisioning is enabled.	
At least one service profile template for physical server provisioning. **Note** Required only if Physical Server Ordering is enabled.	
A local boot policy assigned to the physical server service profile template which is set to boot from local disk	
A boot policy named "PXEBoot" which is configured to boot from the network **Note** This name is mandatory	
UCS blades for provisioning VMware ESXi hypervisor hosts have at least one local drive	

VMware Software Requirements

Table B-7 Requirements—VMware Software Installation

Requirement	✓
vCenter object names do not contain forward slashes	
vSphere PowersCLI 5 or later is installed on the Process Orchestrator server	
VMware Enterprise licensing is applied	
VMware vSphere Distributed Resource Scheduler (DRS) is enabled	
VM templates have been created with VMware tools installed to support operating system customizations	

Directory and Mail Server Requirements

Table B-8 Requirements—Directory and Mail Server

Requirement	✓
LDAP server is installed, configured, and deployed	
SMTP server is installed and configured with an account to send and receive e-mails	

Organizations and Users Preparation

Table B-9 Requirements—Organizations and Users

Requirement	✓
Prepare a list of organizations	
Prepare a list of organization users	
Prepare a list of Organization Technical Administrators	

Create a Virtual Datacenter

Table B-10 Requirements—Virtual Datacenter Creation

Requirement	✓
vCenter platform element is registered	
POD is created	
Register Datastores	
Create networks	

Create a Community VDC

Table B-11 Requirements—Community VDC Creation

Requirement	✓
vCenter platform element is registered	
POD is created	
Register Datastores	
Create networks	

Order VM From Template

Table B-12 Requirements—Order VM from Template

Requirement	✓
VM templates created and discovered	
Virtual Data Center or Community VDC is created	
Register Virtual Machine templates	

Order a VM and Install an Operating System

Table B-13 Requirements—Order a VM and Install an Operating System

Requirement	✓
Virtual Data Center or Community VDC created	

Provision ESXi

Table B-14 Requirements—Provision ESXi

Requirement	✓
At least one hypervisor UCS service profile template for each vCenter cluster is created	
Infrastructure Network is created	
Place blades in the Virtual Blade Pool	
Discover and register Cisco UCS service profile templates	

Solution Deployment Checklists

Cloud Infrastructure Setup Checklist

Table C-1 Cloud Infrastructure Setup Checklist

Task	✓
Define the VMware vCenter Server platform element	
Define the Cisco UCS Manager platform element	
Set provisioning settings	
Add infrastructure network	
Add community network	
Create one or more PODs	
Set up the Community VDC	

Cisco Process Orchestrator Setup Checklist

Table C-2 Process Orchestrator Setup Checklist

Task	✓
Import the Core Automation Pack	
Import the Common Activities Automation Pack	
Import the Intelligent Automation for Compute Automation Pack	
Import the Intelligent Automation for Cloud Starter Automation Pack	
Import the Intelligent Automation for Cloud Automation Pack	

REX Adapter Installation Checklist

Table C-3 REX Adapter Installation Checklist

Task	✓
Install the REX Adapter	

Directory Integration Setup Checklist (If Applicable)

Note These tasks are required **only** if external authentication is enabled for your environment. Otherwise, skip to the next checklist.

Table C-4 Directory Integration Setup Checklist

Task	✓
Verify that the prerequisites for directory integration are met	
Configure the LDAP server	
Configure authentication:	
• Configure mappings	
• Configure events	
Configure authorization (Optional):	
• Create a security group for each user role on the LDAP server:	
– Cloud Provider Technical Administrator	
– Organization Technical Administrator	
– Virtual Server Owner	
– Field Extender	
– Service Group	
• Add the nsAPI user to the Cloud Administration Group	
• Configure user role mappings	
Enable directory integration	

Service Catalog Deployment Checklist

Table C-5 Service Catalog Deployment Checklist

Task	✓
Copy service catalog files to Cisco Prime Service Catalog server	
Import and deploy service catalogs	

Portal and Portlet Deployment Checklist

Table C-6 Portal Deployment and Configuration Checklist

Task	✓
Copy portlets folder and extract files	
Configure Cisco Prime Service Catalog stylesheets	
Import and deploy portal pages	
Add portlet access to My Workspace	

Cloud Administration Setup Checklist

Table C-7 Cloud Administration Setup Checklist

Task	✓
Configure and enable approvals	
Set up REX and nsAPI user account	
Set username and password for REX Set REX agent properties	
Start REX Set REX Agent Property agent	
Set REX Agent Configuration and verify that the agent properties are set correctly	
Start REX Set HTTP Agent Property agent	
Set HTTP Agent Configuration and verify that the agent properties are set correctly	
Start all other agents	
Assign e-mail addresses for queue notifications	
Modify the default e-mail notification templates (see Table C-10 on page C-4 for a checklist of all of the templates)	
Create the Cloud Provider Technical Administrator home organization	
Add the new user as a Cloud Administrator (no directory service)	

Directory Integration Setup Checklist (If Applicable)

Note These tasks are required **only** if external authentication is enabled for your environment. Otherwise, skip to the next checklist.

Table C-8 Directory Integration Setup Checklist

Task	✓
Set up directory structure on the LDAP server, with Groups and Users folders.	
Create the nsAPI user account on the LDAP server.	
Create the lookup user account with "Read MemberOf" lookup permissions.	
Configure the LDAP server in Cisco Prime Service Catalog.	
Configure authentication:	
• Configure mappings.	
• Configure events.	
Configure authorization (*Optional*):	
• Create security groups for all six Cisco Prime Service Catalog user roles in each "Groups" folder on the LDAP server.	
• Add the nsAPI user to the CPTA security group.	
• Configure user role mappings.	
Enable directory integration.	

Cisco Intelligent Automation for Cloud Prerequisites

Table C-9 Cisco Intelligent Automation for Cloud Prerequisites Checklist

Task	✓
You have completed the checklists in Appendix B, "Solution Prerequisites Checklists," and have confirmed that all of the Cisco IAC prerequisites are met.	

Email Notification Template Modification Checklist

Table C-10 e-mail Notification Templates Checklist

Email Template	✓
Add Role Completion Notification	
Ad-Hoc Task Started	
Connection Cloud Platform Elements Completed e-mail	
CPO Error Notification Physical Server	
CPO Error Notification VM	
Default Late Activity	
Failure to Create Network	
Failure to Create Target Notification	
Lease Expiration - First Warning	

Table C-10 e-mail Notification Templates Checklist (continued)

Email Template	✓
Lease Expiration - Second Warning	
My Services Departmental Reviews	
My Services Financial and Departmental Authorizations	
My Services Service Group Reviews	
Notification System Error in Service Request	
Order VM from Template Completion Notification	
Process Escalation	
Remove Role Completion Notification	
Service Canceled Notification	
Service Complete Notification	
Service Confirmation Customer Acknowledgement	
Service Link Error on External Task	
Service Rejected Notification	
Service Started e-mail	
Task Fulfillment Escalation Notification	
Task Fulfillment Pending Notification	
Tenant Management Complete Notification	

Organizations and Users Setup Checklist

Table C-11 Organizations and Users Setup Checklist

Task	✓
Create an organization	
Create a new user to add as an Organization Technical Administrator	
Assign Additional Permissions for the Organization Technical Administrator Role	
Assign Additional Permissions for the Server Owner Roles	
Add a Server Owner	

Solution Deployment Worksheets for Cisco Intelligent Automation for Cloud

Hardware Specifications

Table D-1 Hardware Specifications for Platform Elements

Platform Element	Component	Client	Server
Process Orchestrator Server	CPU		
	Memory		
	Disk space		
Cisco Prime Service Catalog	CPU	—	
	Memory	—	
	Disk space	—	
Prime Service CatalogDatabase	CPU	—	
	Memory	—	
	Disk space	—	
UCS	CPU	—	
	Memory	—	
	Blades	—	

Database Connection Settings

Table D-2 Minimum Software Requirements

Component	Server	Version
Application Server Operating System	Process Orchestrator	
	Prime Service Catalog	
Application Server Framework	Process Orchestrator	
	Prime Service Catalog	

Table D-2 Minimum Software Requirements

Component	Server	Version
Application Software	Process Orchestrator	
	Prime Service Catalog	
LDAP Server	Process Orchestrator	
	Prime Service Catalog	
	Note LDAP server requirements apply only if your environment has been enabled for external authentication.	
Web server	Process Orchestrator	
	Prime Service Catalog	
Database	Process Orchestrator	
	Prime Service Catalog	
Web browser	Process Orchestrator	
	Prime Service Catalog	
Virtualization	Hypervisor	
	Hypervisor Manager	
Physical Server Provisioning	Cisco UCS Manager	

Table D-3 Database Connection Settings

Component	Server	Version
Database Specifications	Type (Oracle or Microsoft SQL)	
	Version	
	Host	
	Port	
Process Orchestrator credentials	Database or Windows authentication?	
	Username	
	Password	
	Domain	
ServiceCatalog credentials	Database or Windows authentication?	
	Username	
	Password	
	Domain	

Table D-3 Database Connection Settings

Component	Server	Version
Datamart credentials	Database or Windows authentication?	
	Username	
	Password	
	Domain	
Cisco Prime Service Catalog credentials	Database or Windows authentication?	
	Username	
	Password	
	Domain	

Process Orchestrator Web Service Target Settings

Process Orchestrator web service settings are configured when the Cisco Intelligent Automation for Cloud Compute Automation Pack is imported into Process Orchestrator.

Table D-4 Process Orchestrator Default Web Service Target Settings

Requirement	Setting
HTTP Port of the Process Orchestrator web service target	
HTTPS or HTTP authentication mechanism (NTLM, Digest, or Basic)	
Web service target credentials:	
• Domain of user account that is used to connect to the Process Orchestrator Web service target	
• User account username	
• User account password	

Process Orchestrator-Prime Service Catalog Integration API Connection User Account Credentials

The user credentials for the Prime Service Catalog Integration API Connection to Process Orchestrator are created when the Intelligent Automation for Cloud Starter Automation Pack is imported into Process Orchestrator.This user account is referred to as the *nsAPI user account*.

Table D-5 Process Orchestrator-Prime Service Catalog Integration API Connection User Account Credentials

Requirement	Setting
Username	
Password	

Cisco Prime Service Catalog Request Center and Service Link User Account Credentials

Table D-6 Cisco Prime Service Catalog Request Center and Service Link User Account Credentials

Requirement	Setting
Username	
Password	

REX Adapter Installation Settings

Record the settings using the worksheet provided for your database server.

Table D-7 REX Adapter Installation Settings—SQL Server

Variable	Definition
DBSERVER	
DBPORT	
DBNAME	
DBUSER	
DBPW	

Table D-8 REX Adapter Installation Settings—Oracle® Database (Windows or Linux)

Variable	Definition
DBSERVER	
DBPORT	
SID	
DBUSER	
DBPWD	

Directory Integration Settings (If Applicable)

LDAP Server Configurations

Table D-9 Directory Integration—LDAP Server Settings

Requirement	Setting
Datasource name	
Datasource description *(optional)*	
Protocol	
Server product and version	
BindDN	
Host	
User BaseDN	
Port number	
Password	

Configure Authentication

Configure Mapping

Table D-10 Directory Integration—Mapping Configurations

Requirement	Setting/Mapping Attribute
Mapping name	
Mapping description *(optional)*	
Person data:	
• First Name	
• Last Name	
• Login ID	
• Personal Identification	
• E-mail Address	
• Home Organization Unit	
• Password	

Configure Events

Table D-11 Directory Integration—Event Configurations

Requirement	Setting
EUABindDN	

Mappings Settings

Table D-12 Directory Integration—Mappings Settings

Requirement	Setting
First name	
Last name	
Login ID	
Person identification	
E-mail address	
Home organization unit	
Password	
Role list	

Events Settings

Table D-13 Directory Integration—Events Settings

Requirement	Setting
EUABindDN	

Cloud Administrator and Organization Settings

Table D-14 Cloud Administrator and Organization Settings

Requirement		Setting
nsAPI user credentials:	Username	
	Password	
	Current role assigned	
	Current organization assigned	

Table D-14 Cloud Administrator and Organization Settings (continued)

Requirement		Setting
REX adapter user credentials	Username	
	Password	
	Current role assigned	
	Current organization assigned	
Cloud Administrator—Organization	Organization name	
Cloud Administrator—User credentials	Username	
	Password	
	Current role assigned	
	Current organization assigned	

Agent Properties Settings

REX Set REX Agent Configuration Settings

Table D-15 REX Set REX Agent Properties Settings

Requirement	Setting
REXOutboundAdapter.Username - Username	
REXOutboundAdapter.Password - Password	

REX Agent Configuration Settings

Table D-16 REX Set REX Agent Properties Settings

Requirement	Setting
REX username	
REX password	
Prime Service Catalog Request Center URL	

Set HTTP Properties Configuration Settings

Table D-17 HTTP Agent Settings

Requirement	Setting
Process Orchestrator hostname	
Process Orchestrator Web Service URL	

Table D-17 HTTP Agent Settings (continued)

Requirement	Setting
Authentication Scheme (NTLMv2, NTLM or Basic)	
Process Orchestrator username	
Process Orchestrator password	
Process Orchestrator domain	
Prime Service Catalog hostname	
Prime Service Catalog Service Link URL	

E-mail Addresses for Queue Notifications

Table D-18 E-mail Addresses for Queue Notifications

Queue	E-mail Address(es)
Default Service Delivery	
Cloud Service Cancellation	
Cloud Service Delivery Management	
Cloud Service Lease Administration	
Cloud Service Remediation	

Cloud Platform Connection Settings

VMware vCenter Server Connection Settings

Table D-19 VMware vCenter Server Connection Settings

Platform Element	Requirement	Setting
VMware vCenter Server	Host name	
	Port	
	Secure connection protocol? (T/F)	
	Username	
	Password	

Cisco UCS Manager Connection Settings

Table D-20 Cisco UCS Manager Connection Settings

Platform Element	Requirement	Setting
Cisco UCS Manager	Host name	
	Port	
	Secure connection protocol? (T/F)	
	Ignore certificate error? (T/F)	
	Time zone	
	Username	
	Password	

Provisioning Settings

Table D-21 Provisioning Settings

Requirement	Setting
Cisco SP time zone	
Default virtual server clone timeout	
Cloud duplicate alert suppression time period	
Cloud Domain	
Cloud Domain User	
Cloud Domain Password	
Cloud Default Time Zone Linux	
Cloud Default Time Zone Windows	

System-wide Service Options

Table D-22 System-wide Service Options

Name	Setting
Virtual Machine From Template Ordering	
Virtual Machine and Install OS Ordering	
ESXi Provisioning	
Community VDC Ordering	
Virtual Data Center Ordering	
Advanced Network Services	

Table D-22 System-wide Service Options (continued)

Name	Setting
Multiple Security Zones	
Enhanced VM Security	
High Availability	
Load balancing Services	
Application Configuration Management	
Service Assurance Names	

Network Settings

Table D-23 <network_type> Network Settings

Requirement	Setting
Network name	
Subnet address specification (IP address/ routing prefix)	
Community network	
Public network	
Network type	
NetworksSource	
vCenter portgroup	
UCS VLAN	
Subnet mask	
Gateway address (if other than default)	
FHRP1 address	
FHRP2 address	
Broadcast address (if other than default)	
Primary DNS address	
Secondary DNS address	

POD Settings

Table D-24 Community VDC Settings

Requirement	Setting
Name	
Description	

Table D-24 Community VDC Settings (continued)

Requirement	Setting
VMware vCenter Instance	
VMware Datacenter	
Cisco UCS Manager Instance	

Community VDC Settings

Table D-25 Community VDC Settings

Requirement	Setting
POD	
VMware vCenter Datacenter	

Standards Settings (Optional)

If you have opted not to modify any standards settings for these service options, check the following check box:

☐ **No standard settings have been modified from the default values**.

Lease Term Standards

If you added new lease terms, record the information in Table D-26. If you have not added new lease terms, check the check box below.

☐ **Lease term standards have not been modified from the default values.**

Table D-26 Lease Term Settings

Template	Requirement	Settings
New lease duration	Lease term (for example, 6 months)	
	Runtime (seconds)	
	Storage (seconds)	
	Warning 1 (seconds)	
New lease duration	Lease term (for example, 6 months)	
	Runtime (seconds)	
	Storage (seconds)	
	Warning 1 (seconds)	

Table D-26 Lease Term Settings (continued)

Template	Requirement	Settings
New lease duration	Lease term (for example, 6 months)	
	Runtime (seconds)	
	Storage (seconds)	
	Warning 1 (seconds)	
New lease duration	Lease term (for example, 6 months)	
	Runtime (seconds)	
	Storage (seconds)	
	Warning 1 (seconds)	

Operating Systems Standards

☐ **No operating systems standards have been added or modified.**

Table D-27 Operating System Standards Settings

OS Type (Windows, Linux, ESXi)	OS System
Linux	
Windows	
ESXi	
New operating system standard—OS Type	
New operating system standard—OS Type	
New operating system standard—OS Type	

Server Size Standards

☐ **No server size standards have been added or modified.**

Table D-28 Server Size Standards Settings

Size Label	Component	Setting
Small	CPUs	
	Memory (GB)	
	Storage (GB)	
Medium	CPUs	
	Memory (GB)	
	Storage (GB)	

Table D-28 Server Size Standards Settings (continued)

Size Label	Component	Setting
Large	CPUs	
	Memory (GB)	
	Storage (GB)	
New server size standard (optional)	Size label	
	CPUs	
	Memory (GB)	
	Storage (GB)	
New server size standard (optional)	Size label	
	CPUs	
	Memory (GB)	
	Storage (GB)	
New server size standard (optional)	Size label	
	CPUs	
	Memory (GB)	
	Storage (GB)	

VDC Size Standards

☐ **No VDC size standards have been added or modified.**

Table D-29 VDC Size Standards Settings

Size Label	Component	Setting
Small	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	

Table D-29 VDC Size Standards Settings (continued)

Size Label	Component	Setting
Medium	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	
Large	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	
New VDC size standard (optional)	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	

Table D-29 VDC Size Standards Settings (continued)

Size Label	Component	Setting
New VDC size standard (optional)	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	
New VDC size standard (optional)	Maximum virtual servers	
	Maximum vCPU	
	Maximum memory (GB)	
	Maximum total storage (GB)	
	Maximum physical servers	
	CPU limit (MHz)	
	Resource pool CPU reservation (MHz)	
	Resource pool memory reservation (GB)	
	Number of snapshots	
	VDC	

Required Privileges for vCenter Service Account

This appendix serves as reference for ensuring the service account used for Cisco IAC to connect and manage vCenter Server objects has the required, specific security privileges. To enable these permissions:

Step 1 Connect vSphere Client to vCenter Server.

Step 2 Click **Home**, then click **Roles**.

Step 3 To create a new user role, right-click on a blank area and choose **Add**.

Step 4 Enter a name (for example, "IAC Service Account").

Step 5 Expand each category identified in the list below.

Step 6 Check each privilege identified in the list below.

Step 7 Repeat Steps 5 and 6 for each privilege.

Step 8 Click **OK**.

Note Be sure to add permission for this role to each datacenter to be managed by IAC.

Privilege List

The following privileges are used by Cisco IAC to manage vCenter Servers.

✓	Privilege
	Alarms/Disable alarm action
	Alarms/Modify alarm
	Alarms/Remove alarm
	Alarms/Set alarm status
	AutoDeploy/Host
	AutoDeploy/Image Profile
	AutoDeploy/Rule

✓	Privilege
	AutoDeploy/RuleSet
	Datacenter/Create datacenter
	Datacenter/IP pool configuration
	Datacenter/Move datacenter
	Datacenter/Remove datacenter
	Datacenter/Rename datacenter
	Datastore/Allocate space
	Datastore/Browse datastore
	Datastore/Configure datastore
	Datastore/Low level file operations
	Enumerate Datastores
	vSphere Role Privileges
	Alarms/Acknowledge alarm
	Alarms/Create alarm
	PO VM Activities
	PO Activities Used in 4.0
	Get?Datacenter
	Get?Datastore
	Datastore/Remove datastore
	Datastore/Remove file
	Datastore/Rename datastore
	Datastore/Update virtual machine files
	Datastore cluster/Configure a datastore cluster
	dvPort group/Create
	dvPort group/Delete
	dvPort group/Modify
	dvPort group/Policy operation
	dvPort group/Scope operation
	ESX Agent Manager/Config
	ESX Agent Manager/Modify
	ESX Agent Manager/View
	Extension/Register extention
	Extension/Unregister extension
	Extension/Update extension
	Folder/Create folder
	Folder/Delete folder
	Clone to Datastore Cluster

✓	Privilege
	Add Host Port Group
	Update Host Port Group
	Create Folder
	vSphere Role Privileges
	PO VM Activities
	PO Activities Used in 4.0
	Folder/Move folder
	Folder/Rename folder
	Global/Act as vCenter Server
	Global/Cancel task
	Global/Capacity planning
	Global/Diagnostics
	Global/Disable methods
	Global/Enable methods
	Global/Global tag
	Global/Health
	Global/Licenses
	Global/Log event
	Global/Manage custom attributes
	Global/Proxy
	Global/Script action
	Global/Service managers
	Global/Set custom attribute
	Global/Settings
	Global/System tag

Upgrading Cisco Prime Service Catalog and Installing the REX Adapter

If you are upgrading to Cisco Intelligent Automation for Cloud 4.1.1 from any version of Cisco IAC 4.x version prior to Cisco IAC 4.0.0.4 (specifically, 4.0.0.1, 4.0.0.2, or 4.0.0.3), you will need to upgrade Prime Service Catalog to the latest compatible version and install the REX adapter.

Upgrading Cisco Prime Service Catalog

Warning **Be sure to have a snapshot of your Prime Service Catalog environment and backups of Cisco Prime Service Catalog database and files before upgrading.**

Step 1 For environments with Cisco IAC 4.0 NOT installed on an IAC Virtual Appliance, follow the instructions in the *Cisco Prime Service Catalog Installation Guide* to upgrade Prime Service Catalog.

Step 2 For environments with Cisco IAC 4.0 installed on an IAC Virtual Appliance, use the Cisco Prime Service Catalog Virtual Appliance Upgrade Utility to upgrade the appliance:

http://software.cisco.com/download/release.html?mdfid=285975253&softwareid=284894055&os=VMWare&release=10.0&relind=AVAILABLE&rellifecycle=&reltype=latest&i=!pp

Installing the Latest Prime Service Catalog Patch

Step 1 Install the latest Prime Service Catalog 10.0 R2 patch:

http://software.cisco.com/download/type.html?mdfid=285031811&catid=null

Installing (or Reinstalling) the REX Adapter

Note Before starting the process, we highly recommended that you stop both Cisco Prime Service Catalog and Cisco Prime Service Link services.

Step 1 Copy `Prime Service Catalog/IACAdapters-[release].zip` from the Cisco IAC 4.1.1 download into a temporary directory on the Prime Service Catalog server.

Step 2 Extract `IACAdapters-[release].zip` to a temporary location on the Prime Service Catalog server (hereafter referred to as [rex]).

Step 3 Copy: `\IACAdapters-[release]\deploy\RexAdapter.xml` to `c:\rex\deploy`.

Step 4 Copy `\IACAdapters-[releas]\adapters\adapter_REXAdapter.jar` to `CiscoPrimeServiceCatalog\jboss-as-7.1.1.Final\ServiceLinkServer\deployments\ServiceLink.war\WEB-INF\lib`.

Step 5 Go to the following folder and extract `adk.zip`. (The "adk" folder is part of the Cisco Prime Service Catalog installation files):

`\CiscoPrimeServiceCatalog\jboss-as-7.1.1.Final\ServiceLinkServer\deployments\ServiceLink.war\WEB-INF\CPSC_10.1_win\adk\adk.zip`

Step 6 Copy and replace at destination the "kek" files:

`kek_new.txt and kek_old.txt` from `CiscoPrimeServiceCatalog\jboss-as-7.1.1.Final\ServiceCatalogServer\deployments\RequestCenter.war\WEB-INF\classes\config` to CPSC_10.1.0's `adk` folder.

Step 7 Open a command window, and `cd` to the `<adk>` folder.

Step 8 Run the following command:

- For the Windows operating system: **`adapter_dbinstaller.cmd`**
- For the Linux operating system: **`adapter_dbinstaller.sh`**

The following is a sample run for each database.

Table 6-1 ***Sample Runs***

Database	Sample Run

SQL Server	`c:\adk>adapter_dbinstaller.cmd`
	`found bin\java.exe`
	`Please enter the database connection information.`
	`Database Type [SQLSERVER]:`
	`Database Hostname [localhost]:`
	`Database Port [1433]:`
	`Database Name [ServiceCatalog]:`
	`Username [RCUSER]: CPSCUser`
	`Password:`
	`Testing database connection: Success!`
	`Adapter Deployment Descriptor File: c:\rex\deploy\rexadapter.xml`

Oracle	`c:\adk>adapter_dbinstaller.cmd`
	`found bin\java.exe`
	`Please enter the database connection information.`
	`Database Type [SQLSERVER]: ORACLE`
	`Database Hostname [localhost]:`
	`Database Port [1521]:`
	`Oracle SID [ORCL]:`
	`Username [RCUSER]: CPSCUser`
	`Password:`
	`Testing database connection: Success!`
	`Adapter Deployment Descriptor File: c:\rex\deploy\rexadapter.xml`

Step 9 Restart Cisco Prime Service Catalog.

Step 10 Restart Service Link.

Step 11 Delete all of the contents in the following folders in the Service Catalog Server.

Note Do **not** delete the *actual folders*, only the *contents* within them.

- `CPSC_Install_Dir\jboss-as-7.1.1.Final\RequestCenterServer\tmp\work\*`
- `CPSC_Install_Dir\jboss-as-7.1.1.Final\RequestCenterServer\tmp\vfs\*`
- `CPSC_Install_Dir\jboss-as-7.1.1.Final\ServiceLinkServer\tmp\work\*`
- `CPSC_Install_Dir\jboss-as-7.1.1.Final\ServiceLinkServer\tmp\vfs\*`

Upgrading Cisco PPM to the Full License

The Trial (demo) edition of Prime Performance Manager (PPM) ships with Cisco IAC 3.0.2 Management Appliance. In order to leverage the benefits of the Full (licensed edition) of PPM (1.5.1), you will need to uninstall the demo version and then install the licensed version. How to do so (with an option to save your data, if required) is explained in this section. You must be logged in as a Cloud Provider Technical Administrator (CPTA) to complete this task.

Note You organization will first need to purchase the Full license for Prime Performance Manager 1.5.1. For more information, see your Cisco Sales Representative.

Hardware Requirements for the Demo/Trial/PoC Version of PPM

The maximum number of network elements that can be managed by the small demo / proof of concept hardware is shown in detail below.

Table 7-1 *Network Size (Maximum)*

Number of Devices	200
Number of PWE3 Links	12,400
Number of Interfaces	37,600
Number of Interfaces with Stats	20,900

Table 7-2 Recommended Hardware Configurations

CPU	CPU Type	non-NEBs Compliant Systems	NEBs Compliant Systems
Cisco UCS C22M3	4-core (UCS C22M3)	Xeon E5-2407v2 2.4 GHz	
	4-core (UCS C22M3)	Xeon E5-2407 2.2 GHz	
Cisco UCS C220M3	4-core (UCS C220M3)	Xeon E5-2609v2 2.5 GHz	
	4-core (UCS C220M3)	Xeon E5-2609 2.4 GHz	

Table 7-2 Recommended Hardware Configurations (continued)

CPU	CPU Type	non-NEBs Compliant Systems	NEBs Compliant Systems
Cisco UCS C200M2	4-core (UCS C200M2)	Xeon E5620 2.4 GHz	
Cisco UCS B200M3	4-core (UCS B200M3)	Xeon E5-2609v2 2.5 GHz	
Oracle Netra X3-2 or equivalent	8-core (Oracle X3-2)		Xeon E5-2658 2.1 GHz

Table 7-3 *Recommended Storage*

#	Size and Type	Purpose
1	146GB SAS 15K RPM Drive	OS and PPM
1	300GB SAS 15K RPM Drive	Backups

Table 7-4 *Storage and Performance Requirements*

Type	System	Notes
Linux OS PPM Gateway / Unit Installation	80 GB Used 120 IOPS with about 75% write operations	Driven by devicecache/logs/database/exported reports writes devicecache/ logs/ database /exported reports can be relocated if necessary
First External Partition PPM Gateway / Unit Backups	150 GB Used 250 IOPS with about 45% write operations	Sustained IOPS During Backup Periods Quiet At Other Times

Table 7-5 *Virtual HW and Memory Requirements*

Virtual Hardware Requirements For Vm Environments	Memory And Swap Requirements	Java Virtual Machine Memory Configuration
vCPU Number -- 4 or more - For VM Environments	RAM Size -- 8 GB or greater Swap Space -- 8 GB or greater	Gateway JVM Size -- 2 GB Unit JVM Size -- 4 GB

Upgrading and Saving Previous Data

If you need to preserve the data created during the evaluation (demo) period after upgrading to the Full version of Prime Performance Manager, follow the steps below:

Step 1 Download PPM 1.5 FCS version and the 1.5.1 update from cisco.com.

Step 2 Perform a PPM backup of the PPM 1.5.1 evaluation system by executing the following command:

```
/opt/CSCOppm-gw/bin/ppm backup
```

Step 3 Validate that the backup file(s) were created.

Note The default location of the files is `/opt`.

Examples of files created:

- `ppm15-Unit-hostname.tar`
- `ppm15-Gateway-hostname-backup.tar`

Step 4 Uninstall Prime Performance Manager 1.5.1 evaluation.

- To uninstall a previous build without any questions:

```
/opt/CSCOppm-gw/bin/ppm uninstall -n
```

Step 5 Install 1.5.

- To perform an installation from the directory that contains the PPM installation files:

```
./setup.sh
```

Step 6 After the Gateway and Unit are installed, exit the installation.

Note Do NOT yet start the system.

Step 7 Install upgrade to 1.5.1.

- To perform an installation from the directory that contains the PPM installation files:

```
./setup.sh
```

Step 8 Start the Gateway and Unit after the installation is complete.

Step 9 Validate the system has been updated and the version is 1.5.1:

```
/opt/CSCOppm-gw/bin/ppm version
```

Step 10 Enable SSL and user access after the installation has completed:

- `/opt/CSCOppm-gw/bin/ppm ssl enable`

Step 11 Enable user access after SSL has been installed:

- Execute `/opt/CSCOppm-gw/bin/ppm useraccess enable`
- You will be prompted for additional information, as shown:

  Please choose the type of authentication to use: [local] **linux**

  Enter username: **cisco**

  Enter First Name : **Cisco**

  Enter Last Name : **Administrator**

  Enter access level for user cisco: **5**

Step 12 Perform Prime Performance Manager restore:

```
/opt/CSCOppm-gw/bin/ppm restore both
```

Step 13 After the restore completes for the Gateway and Unit start the system

```
/opt/CSCOppm-gw/bin/ppm start
```

Upgrading Without the Need to Save Data

If you do not need to save your data created with the trial/demo version during the evaluation period, follow the steps below to upgrade to the fully licensed version of Prime Performance Manager.

Step 1 Download Prime Performance Manager (PPM) 1.5 FCS version and the 1.5.1 update from Cisco.com.

Caution You need to back up `/opt/CSCOppm-gw/etc/amqpConfig.xml` before starting. After upgrading, restore the file to the upgraded instance.

Step 2 Uninstall Prime Performance Manager 1.5.1 evaluation version.

- To uninstall a previous build without any questions, execute this command:

```
/opt/CSCOppm-gw/bin/ppm uninstall -n
```

Step 3 Install Prime Performance Manager 1.5 FCS version. To perform an installation from the directory that contains the PPM installation files, do this:

```
./setup.sh
```

Step 4 Install PPM 1.5.1 update.

- To perform an installation from the directory that contains the PPM installation files, type this:

```
./setup.sh
```

Step 5 Start the Gateway and Unit after the installation is complete.

Step 6 Validate the system has been updated and the version is 1.5.1:

```
/opt/CSCOppm-gw/bin/ppm version
```

Step 7 Enable SSL and user access after the installation has completed:

- `/opt/CSCOppm-gw/bin/ppm ssl enable`

Step 8 Enable user access after SSL has been installed:

- Execute `/opt/CSCOppm-gw/bin/ppm useraccess enable`
- You will be prompted for additional information, as shown:

  Please choose the type of authentication to use: [local] **linux**

  Enter username: **cisco**

  Enter First Name : **Cisco**

  Enter Last Name : **Administrator**

  Enter access level for user cisco: **5**

Step 9 After the restore completes for the Gateway and Unit start the system

```
/opt/CSCOppm-gw/bin/ppm start
```