CA Automation Suite for Clouds Base Configuration

Service Provider Guide

Release 01.6.00

CA Technologies Product References

This documentation set references the following CA Technologies products and components:

- CA Service Catalog
- CA Process Automation
- CA Embedded Entitlements Manager (CA EEM)
- CA Server Automation
- CA Business Intelligence
- CA IT Client Manager

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction 7

Chapter 2: Administer Users and Profiles 9

User Onboarding 10
Edit Profiles 11
Add Users to Service Groups 12
Request Access to Service Groups 12

Chapter 3: Configure and Provision the Datastore 15

Configure Enhanced Storage Policy Details 16
Configure Storage 17
    Configure Storage Policy Mapping 17
    Configure Storage Charge Back 17
Provision the Datastore 18
Deprovision the Datastore 19

Chapter 4: Configure Network Settings 21

vSwitch Architecture 21
Review the Prerequisites 22
Define Network Address Pools 22
Enable VLANs 23

Chapter 5: Enable Primary Disk Extension Support 25

Review the Prerequisites 26
Import sshremoteexectool.jar Utility 26
Verify LinuxAdmin Parameters in ASC_GlobalDataset for VMware ESX 27
    Update the sudoers File 28

Chapter 6: Access and Run Reports 29

Appendix A: Unsubscribe Users from CA EEM Groups 31

Chapter 1: Introduction

This guide describes the processes for a Service Provider to administer CA Automation Suite for Clouds Base Configuration. Your responsibilities require you to:

- Manage users and their profiles.
- Configure enhanced storage policy and use them in creating new datastores.
- Configure CA Automation Suite for Clouds templates.
- Configure network settings in CA Server Automation.
- Access and run reports.

Chapter 2: Administer Users and Profiles

As a Service Provider, you manage users and their profiles in the system. Before you can manage users and their profiles, you must import users from CA EEM or other external directories. You can use the syncuputil.bat file to import users in bulk. You need to import users only one time.

For more information about running the utility, see the section Specify the Configuration File Properties, in the CA Service Catalog Integration Guide.

After you import users, you can manage the service groups to which the users are assigned. By default, only Service Providers and Approving Managers have rights to edit user profiles (other than their own) and to add users to groups.

The self-service portal allows you to manage users, profiles, and service groups. The portal is accessible from CA Service Catalog with the URL and your credentials.

Use the self-service portal to navigate to User and Access Management.

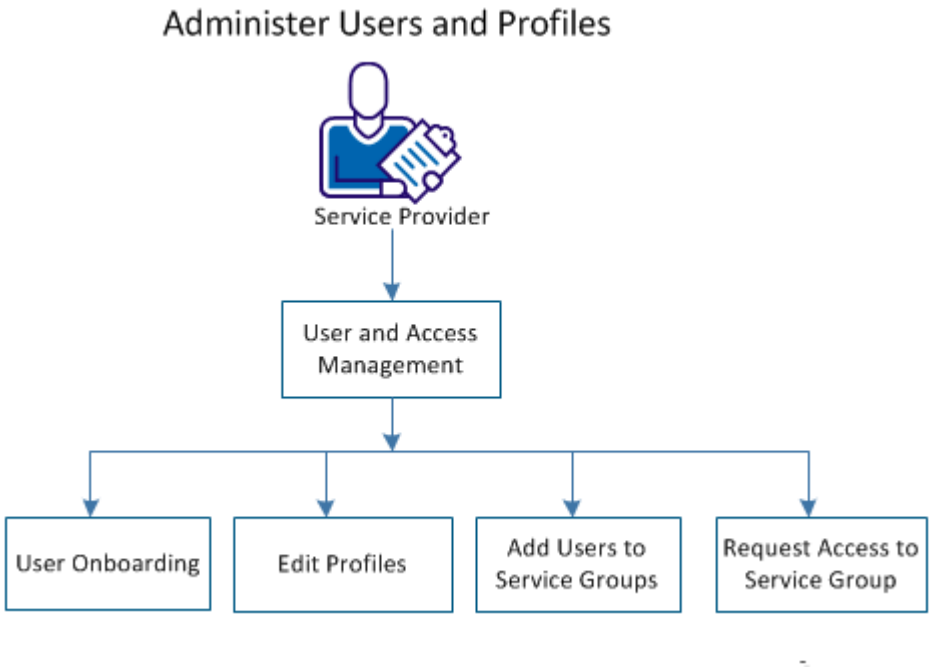
Follow these steps:

1. Log in to CA Service Catalog.
2. Click Requests.

   The available services list opens.
3. Click Foundation Management Services, User and Access Management.

   The User and Access Management page opens.

The following diagram illustrates how a provider can manage users.



Perform the following functions:

- User Onboarding (see page 10)
- Edit Profiles (see page 11)
- Add Users to Service Groups (see page 12)
- Request Access to Service Groups (see page 12)

User Onboarding

You add users to CA Automation Suite for Clouds using the User Onboarding form.

Follow these steps:

1. Access User and Access Management.
2. Click User Onboarding.

   The User Onboarding form opens.
3. Complete the User, Contact, and Organization Details and verify that you completed the required fields at a minimum.

   Note: The Organization that you select determines the templates available to the user.

4. Click Add to Cart and Check Out.

   The Cart Check Out page opens and the reservation cost displays in the My Selections pane.

5. Click the reservation and verify the reservation details before submitting your reservation.

6. Click Save and Submit Cart.

   A confirmation displays indicating that your request was submitted successfully. The My Recent Requests pane updates showing your new and previous reservations. This update can take several seconds.

   This request does not require approval.

Edit Profiles

You can edit the profiles of other users. By default, only Service Providers and Approving Managers have rights to edit user profiles and to add users to groups. You can edit your own profile using the Edit My Profile link.

Follow these steps:

1. Access User and Access Management.
2. Click Edit User Profile.

   The Edit User Profile form opens.

3. Click the magnifying glass icon to search a user and enter the User ID in the Lookup User field.

   A list of users appears.

4. Select a user and click OK.

   The Edit User Profile form updates with the selected user information.

5. Update the fields.

   Note: You cannot edit the First Name, Last Name, User ID, or Organization of the user.

6. Click Add to Cart and Check Out.

   The Cart Check Out page opens and the reservation cost displays in the My Selections pane. Click the reservation and verify the reservation details before submitting your reservation.

7. Click Save and Submit Cart.

   A confirmation displays indicating that your request was submitted successfully. The My Recent Requests pane updates showing your new and previous reservations.

User profile changes do not require approval and your changes take effect immediately.

Add Users to Service Groups

Service groups determine to which services the users in that service group can access.

Refer to the group_service.properties located in %USM_HOME% folder for all offerings to groups mapping.

Follow these steps:

1. Access User and Access Management.
2. Click Add User to Service Group.

   The User to Service Group form opens.
3. (Optional) Select the Starts With or Wildcard option and type the search string in the Select User field. This filters the users that appear in the Select User drop-down list.
4. Select a user from the drop-down list.

   The Subscribed Groups and Subscribe to Group panes populate.
5. Add or remove the user from service groups using the arrows.
6. Click Add to Cart and Check Out.

   The Cart Check Out page opens and the reservation cost displays in the My Selections pane.
7. Click the reservation and verify the reservation details before submitting your reservation.
8. Click Save and Submit Cart.

   A confirmation displays indicating that your request was submitted successfully. The My Recent Requests pane updates showing your new and previous reservations.

   Adding users to service groups does not require approval. Your changes take effect immediately.

Request Access to Service Groups

Service groups determine to which services the users in that service group can access.

Follow these steps:

1. Access User and Access Management.
2. Click Request Access to Service Group.

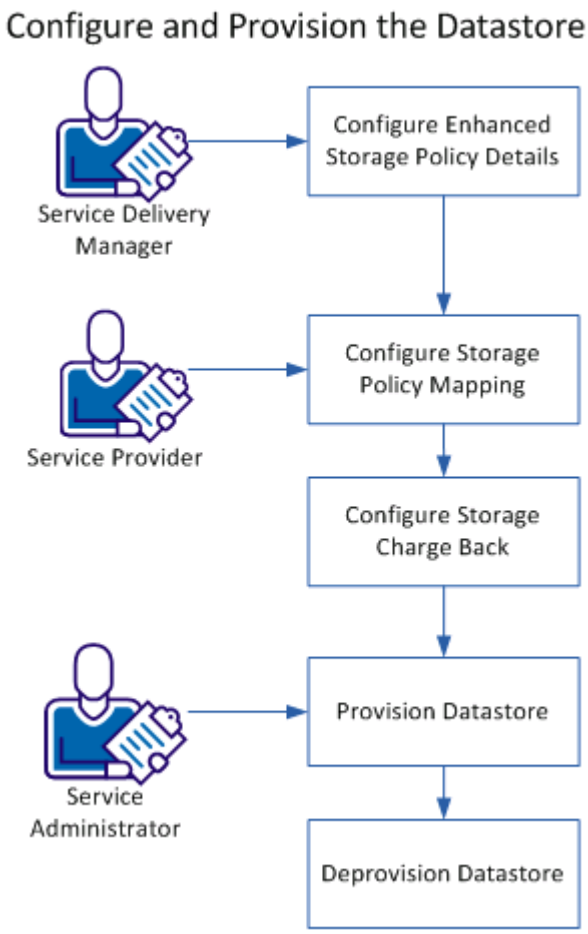
   The Request Access to Service Group page opens with the User ID field populated with your ID. The Belongs to Group(s) field displays the groups that you currently belong to.
3. Add or remove yourself from service groups using the arrows.
4. Click Add to Cart and Check Out.

   The Cart Check Out page opens and the reservation cost displays in the My Selections pane. Click the reservation and verify the reservation details before submitting your reservation.
5. Click Save and Submit Cart.

   A confirmation displays indicating that your request was submitted successfully. The My Recent Requests pane updates showing your new and previous reservations. This update can take several seconds.

Chapter 3: Configure and Provision the Datastore

As a Service Delivery Manager, you configure the enhanced storage policy and enable the Service Provider to use these policies in creating new datastores. The Service Administrator (Tenant Administrator) can later request to provision the new datastore and deprovision the unused datastore in their environment.



Follow these steps:

1. Configure Enhanced Storage Policy Details (see page 16)
2. Configure Storage Policy Mapping (see page 17)
3. Configure Storage Charge Back (see page 17)
4. Provision Datastore (see page 18)
5. Deprovision Datastore (see page 19)

Configure Enhanced Storage Policy Details

As a Service Delivery Manager, you configure the enhanced storage policy details in CA Server Automation to enable the Service Provider to provision the datastore.

Follow these steps:

1. Log in to CA Server Automation as a Service Delivery Manager.
2. Click Resources.
3. From the left-side pane, click Configure, Policies, Storage.
4. Enhanced Storage Policies page opens.
5. Click the plus icon to add a storage policy.

   The Select Policy Type and Name page opens.
6. Complete the following policy details and click Next:
   - Policy Name
   - Description
   - Provisioning Method
   - Protocol
   - NetApp OnCommand Server or EMC SMI-S Server

   The Choose Policy Attributes page opens.
7. Compete the following details and click Next:

   (From the Required Properties section)
   - NetApp or EMC Provisioning Policy
   - Resource Pool

   (From the Provisioning section)
   - Dataset Description
   - Dataset Prefix

- Maximum Allowed Size

The Associate Servers with Policy page opens.

8. Click Finish.

The enhanced storage policy configuration is complete. You have enabled the service provider to proceed with the storage configuration. Verify by creating a data store.

Configure Storage

As a Service Provider, you configure the policies and then add the charge back details for each profile.

Configure Storage Policy Mapping

Follow these steps:

1. Log in to CA Service Catalog as a Service Provider.
2. Click Service Builder, Configuration.
3. From the left-pane menu, click Content Configuration, ASC Storage Policy Mapping.
4. Select the Organization Unit name from the drop-down menu.

   A list of storage policies loads in the table.
5. Select the policies and click Add Policies.

   Newly added policies are listed in the Existing Storage Policies section.

   Note: If you want to remove existing policies, select the policies from the Existing Storage Policies section and click Delete Existing Policies.
6. Repeat steps 4 and 5 for adding policies for other organizational units.
7. Click Save.

Mapping the storage policies to organizations is complete.

Configure Storage Charge Back

Follow these steps:

1. Navigate to the Service Builder menu, click Configuration.
2. From the left-pane menu, click Content Configuration, ASC Storage Charge Back.

3. Select the Organization Unit name from the drop-down menu.
4. Select the Storage Policy name from the drop-down menu.

   The Policy Description, Storage Protocol, and Policy Max Size (GB) information get populated.
5. Enter the values for Hourly Price, Minimum Size (GB), and Maximum Size (GB).
6. Add Default Hourly Price value.

   This value is used if the charge back is not defined for any combination of policy and disk size.

   Note: If you add two or more policy prices within same range for a policy, the system automatically picks the policy with lowest price.
7. Click Save Policy Price.
8. Repeat steps 3 through 7 for each policy and organizational unit and add the charge back details for the profiles.

   Updated policy and price details appear in the table.

   You can select the policies from the table and click Delete Policy Price to remove any existing price configuration.

   Note: If you choose to delete Policy from the ASC Storage Policy Mapping configuration page for the selected organization, all the price configurations are deleted automatically.

The storage configuration is complete. You have enabled the Service Administrator to provision the datastore.

Provision the Datastore

As a service administrator, you can add storage to the available organizational units when you need more storage space in the environment.

Follow these steps:

1. Log in to CA Service Catalog as the service administrator.
2. Click CA Server Automation.
3. Click Infrastructure Management under the VMware ESX Management menu.

   The Infrastructure Management page opens.
4. Click Provision VMware Datastore.

A list of configured VMware Pools for your organization opens.

5. Select a pool that needs more storage, then enter the name and size for the new datastore.
6. Click Fetch Available Storage Policies.

   A list of available policies along with the price details based on the organization of the selected pool appears.
7. Select a policy.
8. Click Add to Cart and Check Out.

   The price of the request is calculated based on the selected policy. A new datastore is created and the status of the request is changed to Pending SSRM Resource Pool Modification. The request is assigned to a Service Administrator (defined in the configuration) and an email is sent to the Service Provider.

   The Service Administrator modifies the pool manually and the status of the request is changed to Completed.

A new datastore is created and attached to the computer resource of the selected pool.

Deprovision the Datastore

You can select one or more datastores and can submit the request to deprovision. If the selected datastore is in use, the deprovisioning request is canceled and you receive an email notification.

Follow these steps:

1. Log in to CA Service Catalog as a Service Administrator (Tenant Administrator).
2. Click Server Automation Services.
3. Click Infrastructure Management under the VMware ESX Management menu.

   The Infrastructure Management page opens.
4. Click Deprovision Datastore.

   A list of datastores that are provisioned to the user opens.
5. Select the datastore that you want to return.
6. Click Add to Cart and Check Out.
7. The status of the request is changed to Pending SSRM Resource Pool Modification. The request gets assigned to the Service Administrator (defined in the configuration), and an email is sent to the Service Provider.

   The Service Administrator modifies the pool manually by removing the datastore from the pool and changes the request status to Datastore detached from Pool.

The request is processed to remove the datastore from the ESX Host or Cluster, and the dataset is deleted from the storage server.

The selected datastore is removed.

Chapter 4: Configure Network Settings

As a Service Provider you configure the network settings in CA Server Automation to enable the network configuration capability for Service Consumers. After you complete the configuration, Service Consumers can configure multiple VLANs depending on the template they chose to reserve the cloud virtual machine.

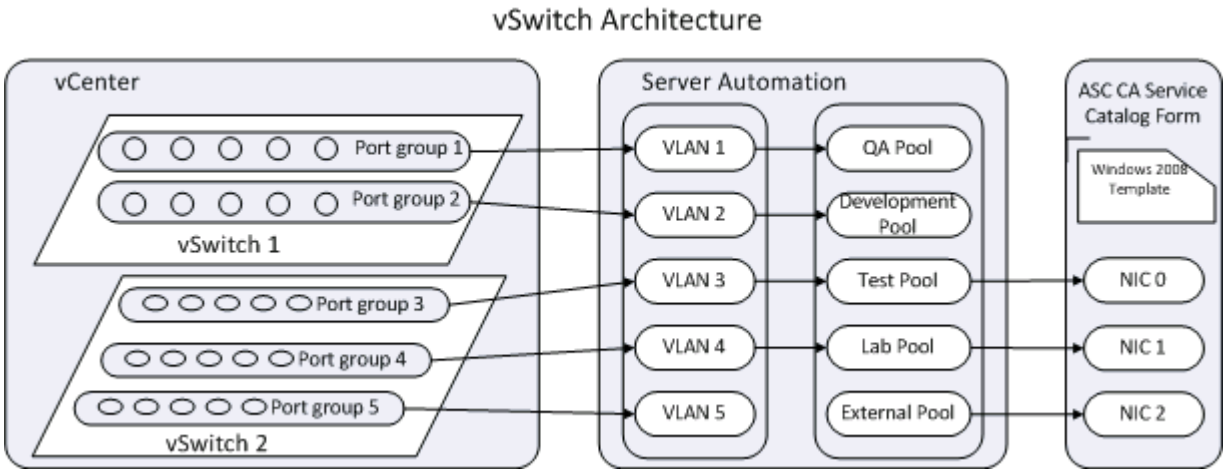
vSwitch Architecture

As a Service Provider the architecture of vSwitch helps you to configure vSwitch.

The VMware vCenter server provides the central point of control for configuring, provisioning, and managing virtualized IT environments.

When multiple vSwitches are present in the vCenter server, you define network pools for each vSwitch by tagging them to different VLAN IDs.

The following diagram illustrates how the components involved interact and enable multiple network support for Service Consumers:



In the vCenter, you configure the vSwitch 1 and vSwitch 2 by creating port groups based on the user requirement. VLAN IDs that are created are then tagged to the port groups.

The Service provider defines the network pools in CA Server Automation. For example, as shown in the vSwitch Architecture diagram network pools like QA Pool, Development Pool, and Test Pool are created in CA Server Automation. Each network pool is then associated and tagged to a VLAN ID with a set of IP addresses (IP Pool).

In the Reserve Virtual Machine form the Service Consumer can select one of the network pools to a Network Interface Card (NIC) associated to the template. This option enables the Service Consumer to choose the network when submitting a request.

Review the Prerequisites

To complete all tasks consider the following items:

- Configure templates. Create custom specifications in the VMware vCenter Server so that the custom specification file consists of equivalent NIC information corresponding to the template. Configure the system image in CA Server Automation by selecting the same custom specification file.
- Contact your network administrator to collect the following details:
  - Virtual LAN (VLAN) IDs tagged to the Port Group of the vSwitch.
  - IP addresses pool configured to VLAN ID, Subnet mask, Gateway address, and DNS name.

Define Network Address Pools

The first step in enabling IP addresses at your site is defining network address pools in the main user interface of the product. Network address pools consist of a range of IP addresses.

Note: Reservation Manager does not permit editing or deleting a network address pool that has been used for reservations. If you want to change something like the IP address range, make a new network address pool. Also, deleting a network that is associated with a VM or logical partition is not allowed.

Follow these steps:

1. Log in to CA Server Automation.
2. Click Resources.
3. Click a data center in the left pane, and select Management, Manage Network Address Pools.

   The Network Address Pools dialog appears.
4. Click + (New), and enter information in the required fields, which are Network Address Pool Name, IP Address, Subnet Mask, and VLAN ID.
5. Click Next.

   A new page for entering network information appears.

6. Enter information in the required fields, which are Default Gateway, Preferred DNS Server, and Domain Name. Click Next.

   A dialog for IP address ranges appears.

7. Enter information in the required fields, and click Add.

   Note: Each address in the pool must have a DNS name entry when the pool is created. When you define network address pools, verify that the static IP address ranges are not assigned to another type of data center.

   The Virtual Hosts pane appears.

8. Select one or more virtual hosts, click Add, and then click Finish.

   Each virtual host must be associated with the network before IP addresses can be assigned to VMs created on the host.

   The network address pool is created and visible on the Reservation Manager page.

Enable VLANs

Network address pools are not accessible for use until you explicitly grant access to users. As a Service Provider you must scope which VLANs are accessible for end user selection. This is done by specifying the network address pools that are accessible to members of each organizational unit.

Follow these steps:

1. Log in to CA Server Automation.
2. Click Select Administer your Reservation Manager, Manage your organizational units.

   Organizational Units page appears.

3. Click to open the organizational unit to which you want to add VLANs.
4. Go to the Network Access tab, and select one or more VLANs.
5. Click OK.

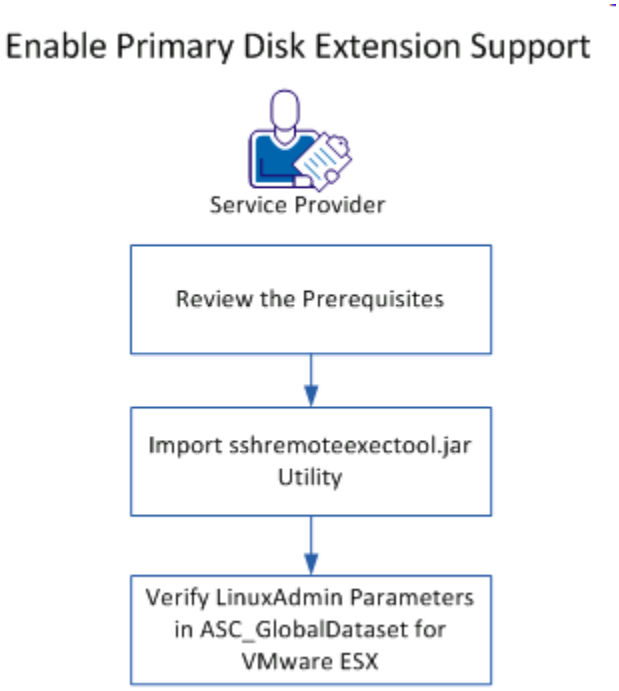
Verify the network configurations. Create a new virtual machine. The name of the network pool that you defined is available in the options.

Chapter 5: Enable Primary Disk Extension Support

As a Service Provider you enable the primary disk extension on the VMware ESX cartridge.

Note: This feature is supported only for CA Server Automation Release 12.7 SP01.

The following diagram illustrates how a Service Provider enables the primary disk extension support:



Follow these steps:

1. Review the Prerequisites (see page 26)
2. Import sshremoteexectool.jar Utility (see page 26)
3. Verify LinuxAdmin Parameters in ASC_GlobalDataset for VMware ESX (see page 27)

Review the Prerequisites

Review the following prerequisites to enable support for the primary disk extension:

- CA Process Automation server must have a network access to provisioned virtual machines.
- **(For Windows)** Enable WMI service. Make sure that WMI service automatically starts on the virtual machines that are provisioned.
- **(For Linux)** Verify that the SSH and SCP services are available and automatically starts on the virtual machines that are provisioned.

Import sshremoteexectool.jar Utility

SSHRemoteexectool utility is used for connecting the provisioned Linux virtual machines through Secure Shell (SSH) protocol. You copy and execute primary disk expansion scripts on the utility.

Follow these steps:

1. Log in to CA Process Automation.
2. Click the Configuration tab.
3. Expand Manage User Resources, Repository, Orchestrator Resources.
4. Click New.

   The new resource page opens.
5. Complete the following details:

   Resource Name

   Specifies the resource name.

   Resource File

   Specifies the resource file.

   Click Browse, navigate to the CA ASC Server Automation - ESX content pack folder, and then open util folder to select the sshremoteexectool.jar file.

   (Optional) Module Name

   Specifies the module name. Select the module name from the drop-down menu.

   (Optional) Resource Description

   Specifies the description for the resource.
6. Click Save.

Verify LinuxAdmin Parameters in ASC_GlobalDataset for VMware ESX

Verify that the LinuxAdmin VM parameters in the ASC_Globaldataset for the VMware ESX cartridge are configured.

Follow these steps:

1. Log in to the CA Process Automation console.
2. Click Library tab.
3. Click the CA ASC folder.
4. Click ASC_GlobalDataset and Check Out.
5. Expand Misc Parameters CHANGE ME and verify the following details:

   LinuxAdmin

   Specifies the Linux VM template parameters.

   For each Linux VM Template, verify the following LinuxAdmin parameters:

   Template

   Specifies the name of the Linux virtual machine template.

   AdminUserName

   Specifies the user name of the virtual machine that accesses the newly provisioned Linux VM using the template.

   Default: root

   AdminPassword

   Specifies the administrator password.

   SSHPort

   Specifies the port where SSH service is listening on the newly provisioned Linux virtual machine with the template.

   Default: 22

   UseSudo

   Specify true if you want to use the sudo user in the Linux environment. For information about configuring the sudo user, see the Update the sudoers File (see page 28) section.
6. Click Save.
7. Click Check In.
8. Click Save and Close.

You have enabled the support for primary disk extension.

Update the sudoers File

Updating the sudoers file lets you issue commands from CA Process Automation using sudo without prompting for the root credentials. If the UseSudo parameter is enabled in the ASC_GlobalDataset, you update the sudoers file.

Follow these steps:

1. Edit the /etc/sudoers file using the visudoers command.
2. Add the following entry:

```
# simple entry for issueing commands if the client does not need granularity

ascuser ALL=NOPASSWD: ALL

# detailed entry for permitting only those commands used by ASC for disk extension

ascuser ALL = NOPASSWD: /sbin/fdisk, /usr/sbin/pvcreate, /usr/sbin/vgdisplay,
/usr/sbin/vgextend, /usr/sbin/lvdisplay, /usr/sbin/lvextend
```

3. Save and close the sudoers file.

Chapter 6: Access and Run Reports

Reports can assist with request approvals by giving you a picture of resource usage and availability. You can also generate service accounting reports and query data within a range to generate reports for stakeholders or verify compliance with Service Level Agreements.

You can run available reports from InfoView directly from CA Service Catalog.

Follow these steps:

1. Log in to CA Service Catalog.
2. Click Reports.
3. Click InfoView.

   The BusinessObjects InfoView page opens.
4. Click Document List and navigate to Public Folders, CA Reports, CA SLCM.

   The CA SLCM folder contains two folders:

   Admin Reports

   Provides reports of interest to Approving Managers and Service Providers.

   User Reports

   Provides reports of interest to service consumers, such as the User Requests report. This report provides details about requests that were opened, approved, or fulfilled within specific time periods.

   Note: Your access to folders and reports depends on your access privileges.
5. Double-click a report.

   The Prompt dialog opens.
6. Type specific parameters to generate the report.
7. Click Run Query.

   The report generates and opens.

Appendix A: Unsubscribe Users from CA EEM Groups

As a Service Provider your responsibility is to unsubscribe users who no longer require to be a part of CA EEM groups.

Follow these steps:

1. Access CA EEM and verify that the Application is set to Service Catalog.
2. Log in using the EiamAdmin account and password.
3. Go to Manage Identities, and select Users.

   The Search Users panel opens.
4. Type the user name in the Value field and click Go.

   Example: spadmin
5. Click the user name from the Users panel.

   The User page opens.
6. From the Application Group Membership section, modify the required user groups.
7. Click Save, and Close.

For more information, see CA EEM documentation.