Cloud Administrator Guide

NetIQ Cloud Manager 2.1.3

September 28, 2012

Legal Notice

Contents

About This Guide

This guide provides instructions for administering a NetIQ Cloud Manager system. It includes the following sections:

Intended Audience

This information is intended for anyone who is assigned the Cloud Administrator role for a NetIQ Cloud Manager system. Consumers of this information should be experienced Linux and Windows system administrators who are familiar with virtual machine technology and datacenter operations.

Additional Documentation

For other NetIQ Cloud Manager 2.1.3 documentation, see the NetIQ Cloud Manager 2.*x* documentation site (https://www.netiq.com/documentation/cloudmanager2/).

Formatting Conventions

Cloud Manager product documentation uses consistent formatting conventions to help you recognize and differentiate items throughout the documentation. The following table summarizes these conventions.

Convention	Use
Italics	◆ Titles or menu items from the user interface ◆ Book and CD-ROM titles ◆ Variable names and values ◆ Emphasized words
`Fixed Font`	◆ File and folder names ◆ Commands and code examples ◆ Text you must type ◆ Text (output) displayed in the command-line interface
Brackets, such as *[value]*	◆ Optional parameters of a command
Braces, such as *{value}*	◆ Required parameters of a command
Logical OR, such as *value1*|*value2*	◆ Exclusive parameters. Choose one parameter.

About NetIQ Corporation

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

For questions about products, pricing, and capabilities, please contact your local partner. If you cannot contact your partner, please contact our Sales Support team

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, please contact our Technical Support team.

Worldwide:	www.netiq.com/Support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. We want to hear your comments and suggestions about this manual and the other documentation included with this product.

- Please use the *User Comments* feature at the bottom of each page of the online documentation to provide specific feedback about the content on that page. A documentation representative will contact you via e-mail with a resolution to the documentation problem within five business days.
- If you have more general suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, please visit http://community.netiq.com.

Cloud Setup

The following sections provide information to help you set up your Cloud environment. The sections follow the same process and include the same information as the *Getting Started* view in the Cloud Manager console:

1 Creating a Zone

A Cloud Manager zone is single Cloud Manager Orchestration Server and its managed resources (VM hosts, storage repositories, networks, and so forth). You create a zone by defining a connection from the Cloud Manager Application Server to the Cloud Manager Orchestration Server. After you create the zone, its resources become part of the Cloud environment that you can use to service your customers.

1. On the main navigation bar, click *Getting Started*, then click *Create Zones* (in the *Set Up Your Cloud Environment* list).

   or

   On the main navigation bar, click *Configuration*, click the *Zones* tab, then click *Create*.

2. Provide the following information:

   Name: Provide a unique name for the zone. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Description: If desired, add more information to further identify the zone. The description is displayed in the Cloud Manager console to all users.

   Enabled: Do not change this setting. The zone should be enabled.

   Server Address: Specify the DNS name or IP address of the Orchestration Server.

   Server Port: Specify the port used by the Orchestration Server Web Service.

   Username: Specify the Administrator user name that enables login to the Orchestration Server.

   Password: Specify and confirm the password for the Administrator username.

   Secure Connection: Select this option if the Cloud Manager Application Server is configured for an SSL connection to the Orchestration Server.

3. Click *OK* to create the zone and add it to the list.

For more information about zones, see Chapter 8, “Managing Zones,” on page 39.

2 Creating Resource Groups Within the Zone

A resource group defines a set of VM hosts that an organization can use for its business services. In addition to the VM hosts, the resource group includes one or more service levels that define the cost of the host resources (vCPUs, memory, storage, and networks) and the service objectives (availability, support response time, and so forth).

2.1 Resource Group Requirements

All VM hosts that you include in a resource group must reside in the same Cloud Manager zone. Additionally, the hosts should be identical in terms of hypervisor technology, operating system version, network configuration, storage repository configuration, and hardware capabilities. This ensures a consistent environment for business services regardless of the host. It also ensures that the resource group’s service levels apply to all hosts.

As an example, you might create a Business Critical resource group that consists of high-performance hosts intended for mission-critical applications and services. You assign the resource group a Platinum service level with costs that reflect the more expensive hardware and service contract. Any business service that is provisioned to the resource group also inherits the resource and service costs.

Or, you might create a Lab resource group that consists of standard-performance hosts intended for software testing. You assign the resource group a Bronze service level with costs that reflect the less expensive hardware and service contract.

2.2 Shared and Dedicated Resource Groups

A resource group can be shared among multiple organizations, which means that each organization’s business services utilize the same resources, or a resource group can be assigned to only one organization, in which case only that organization’s business services consume the resources.

2.3 Creating a Resource Group

1 On the main navigation bar, click *Getting Started*, then click *Create Resource Groups* (in the *Set Up Your Cloud Environment* list).

or

On the main navigation bar, click *Resources*, click the *Resource Groups* tab, then click *Create*.

2 If your Cloud Manager system has multiple zones, the Select Zone dialog box is displayed. Select the zone that contains the resources you are grouping, then click *OK* to display the Create Resource Group dialog box.

3 In the *General* fields, provide the following information for the resource group:

Name: Specify a unique name for the group. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

Zone: Displays the zone whose hosts you can add to the group. You cannot change this setting.

Hypervisor: Select the hypervisor technology for the group's hosts. You can add only those hosts that meet the hypervisor criteria.

Workload Repository: The *Default* setting causes a provisioned workload to be stored in the same repository as the VM template used to create it. If you want workloads provisioned to this resource group to be stored in a different shared repository, you must add hosts to the group (see Step 4), then come back and select the shared repository for the workloads. The Workload Repository list is populated only after you add hosts to the resource group.

Group Type: This applies only if VMware vSphere is the selected hypervisor. Select *Host* if you want the resource group to use hosts and host clusters. Select *Resource Pool* if you want the resource group to use a resource pool.

Resource Pool: If you specified *Resource Pool* as the group type, select the resource pool to include in the group.

Description: Provide any additional information for the resource group.

4 If the group type is *Host*, add hosts to the group:

4a Under *Associations*, click the *Hosts* tab.

4b Click *Add* to display the Add Hosts dialog box.

The list displays all available hosts and host clusters in the zone that meet the selected hypervisor criteria. Hosts that are already assigned to another resource group are not displayed.

4c Select the hosts.

You can Shift-click and Ctrl-click to select multiple hosts.

4d Click *OK* to add the selected hosts to the *Hosts* list.

5 Ignore the *Service Levels* tab.

At this point, there are no service levels to assign to the resource group. The next task is to create service levels (see Chapter 3, "Creating Service Levels for Resource Groups," on page 19). You assign service levels to resource groups at that time.

6 Ignore the *Networks* tab.

The *Networks* tab shows the networks associated with the hosts you added to the group. The list is view-only so you can't make any changes. However, the list is not generated until you save the resource group. If you want to see the networks at this time, click *Save*, double-click the resource group to open it again, then click the *Networks* tab.

7 Ignore the *Organizations* tab.

At this point, there are no organizations to assign the resource group to. You create organizations and assign resource groups to them later (see Chapter 5, "Creating an Organization," on page 25).

8 Click *Save* to add the resource group to the list.

For more information about resource groups, see .Part VI, "Resource Management," on page 121.

3 Creating Service Levels for Resource Groups

A resource group has no costs associated with it until you create a service level and assign it to the resource group. The service level defines the cost of the host resources (vCPUs, memory, storage, and networks) and the cost of the service objectives (availability, support response time, and so forth).

You can use the same service level for multiple resource groups. For example, you might have two identical resource groups that require the same service level.

You can also assign multiple service levels to a single resource group. For example, you might create two service levels with the same resource costs but with different service support levels—the first with 24x7x365 support and the second with 12x5x365 support. The user, when requesting a business service, could select the desired service level.

1. On the main navigation bar, click *Getting Started*, then click *Create Service Levels* (in the *Set Up Your Cloud Environment* list).

   or

   On the main navigation bar, click *Resources*, click *Service Levels*, then click *Create*.

2. In the *General* section, provide the following details for the service level:

   Name: Specify a unique name for the service level. This name is displayed in business service workloads.

   You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Creation Date: Displays the current date.

   Description: Provide any additional information for the service level.

3. In the *Monthly Resource Costs* fields, define the cost (per month) to use the host resources:

   vCPU: Specify the cost per virtual CPU.

   Memory: Specify the cost per megabyte (MB) of memory.

   Disk: Specify the cost per gigabyte (GB) of disk space.

   Network: Specify the cost per network interface card.

4. Assign the service level to the appropriate resource groups:

   4a Under *Associations*, click the *Resource Groups* tab.

   4b Click *Add* to display the Add Resource Groups dialog box.

   4c Select the groups to add.

   You can Shift-click and Ctrl-click to select multiple groups.

   4d Click *OK*.

5 If you don't want to add service level objectives, click *Save*, then continue with the next task, "Creating Workload Templates" on page 21.

or

If you want to add service level objectives, you must create them first. Click *Save* to save the service level, then do the following:

5a Click the *Service Level Objectives* link.

5b Click *Create* to display the Create Service Level Objective dialog box.

5c Provide the following information:

Name: Specify a name for the objective. This name is displayed in all business service workloads.

You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

Monthly Cost: Specify the cost associated with the objective. If the objective does not have a cost, leave the field empty.

Description: Provide optional text to further identify the service level objective.

Creation Date: Displays the current date.

Objective Type: If this objective represents workload availability, select *Availability*. Otherwise, select *General*.

Value: If the objective type is *Availability*, specify the target availability as a percentage (for example, 99.9). If the objective type is *General*, specify an appropriate objective value.

5d Click *Save*.

6 Add objectives to the service level:

6a Click the *Service Levels* link, select the service level, then click *Edit*.

6b Under *Associations*, click the *Service Level Objectives* tab.

6c Click *Add* to display the Add Service Level Objectives dialog box.

6d Select the objectives to add.

You can Shift-click and Ctrl-click to select multiple objectives.

6e Click *OK* to add the selected objectives to the *Service Level Objectives* list.

6f Click *Save*.

You can include the same objective in more than one service level.

4 Creating Workload Templates

Business service workloads are created from workload templates. Each workload template identifies a VM template and the customizations (such as increased CPUs or decreased memory) that you want applied when creating a workload from the template.

The VM templates you can use come from your Cloud Manager zones. A single VM template can be used in multiple workload templates.

1 On the main navigation bar, click *Getting Started*, then click *Create Workload Templates* (in the *Set Up Your Cloud Environment* list).

or

On the main navigation bar, click *Catalog*, click the *Workload Templates* tab, then click *Create*.

2 If your Cloud Manager system has multiple zones, the Select Zone dialog box is displayed. Select the zone that contains the VM template you want, then click *OK* to display the Create Workload Template dialog box.

3 In the *General* section, provide the following information for the workload template:

Name: Specify a unique name for the workload template. Users see this name (along with the description, zone, and operating system) when selecting the workload template they use to create their business service workload.

You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

Setup Cost: Specify the cost associated with setting up the workload. This is a one-time fee.

License Cost: Specify the license costs associated with the workload's software. This cost is per month.

Zone: Displays the zone you selected for the workload template. You cannot change this setting.

Creation Date: Displays the current date. You cannot change this setting.

Description: Provide any additional information to identify the workload template. Users see this description (along with the name, zone, and operating system) when selecting the workload template from which to create business service workload.

4 In the *Virtual Machine Settings* section:

4a In the *VM Template* list, select a VM template.

After you select a VM template, the template's operating system and hypervisor information is displayed. You cannot change these settings.

The VM template's resource information (CPUs, memory, network interface cards, and disks) is also displayed. You can customize this information as necessary.

4b Customize the settings to increase or decrease the workload resources:

Number of CPUs: Select the number of CPUs for the workload. Some hypervisor technologies do not support more than 8 CPUs per workload, so the maximum number allowed is 8.

Memory: Select the megabytes (MB) of RAM to allocate to the workload.

Number of NICs: Select the number of network interface cards (NICs) to allocate to the workload.

Disks Summary: Displays the size of the mandatory workload disks and the number of optional workload disks defined in the template, Mandatory workload disks are always created. They are inherited from the VM template or manually defined on the *Disks* tab. Optional workload disks are available to the user but are created only if the user specifies sizes for the disks.

You add disks on the Disks page (see Step 5 below) and the disk information is then displayed in these fields.

4c By default, each resource setting is unlocked, which means that users can change it when creating workloads from the template. If you want to prevent users from changing a setting, select the check box.

5 If you want to add disks to the workload template, or if you want to specify whether or not the current disks should be included when calculating the cost of the workload:

5a Click the *Disks* tab.

The template can include up to 10 additional disks.

5b Click *Add* to add a disk to the list.

5c Make sure the disk is selected in the list, then specify a size (in the *Size* field below the list) to make the disk mandatory.

or

Leave the size set to 0 to make the disk optional.

The maximum size per disk is 1024 GB (1 TB). If you specify the size when adding a disk, the disk becomes mandatory. Users cannot remove or change a mandatory disk. If you add a disk with the size set to 0, the disk becomes optional. Users can leave the size at 0, in which case the disk is not created with the workload, or they can specify a size and create the disk.

5d In the *Cost* field, select the check box if you want to include the cost of the disk in the workload's total cost.

If you don't enable the *Cost* option, the disk becomes a free disk and is not included when calculating the cost of the workload.

6 If the template is a Windows-based template and you want to pre-populate some of the Windows settings, click *Windows Settings*, then complete the following steps.

You might not want to pre-populate some settings, such as *Computer Name*, if the template will be used to create multiple workloads. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the user) or when performing the pre-build configuration (by an administrator).

6a Configure the *Domain Settings*:

Computer Name: Specify the computer name for the virtual machine.

Domain or Workgroup: Select *Domain* or *Workgroup*, then specify the name of the domain or workgroup to which you want the virtual machine added.

Domain Administrator User ID: This applies only if you are adding the virtual machine to a domain. Specify a domain administrator user ID that can be used to add the virtual machine to the domain specified in the *Domain* field.

6b Modify the *Installation Settings*:

Run Once Commands: Specify any Windows RunOnce commands that you want run during the first log in to the virtual machine. For information about Windows RunOnce commands, see the Microsoft Windows documentation.

7 If the template is a Windows-based template and you want to pre-populate some of the Windows licensing information, click *Windows Licensing* and fill in the fields., then click *OK* to create the workload template and add it to the list.

Windows Product Key: Specify the product key for the workload's Windows operating system.

If you pre-populate this field in the template, the data is masked from users and cannot be copied.

Registered to Name: Specify an individual, department, company or so forth to whom the Windows operating system software is registered.

You might not want to pre-populate some settings, such as *Windows Product Key*, if the template will be used to create multiple workloads and the key does not cover multiple installations. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the user) or when performing the pre-build configuration (by an administrator).

8 If the template is a Linux-based template and you want to pre-populate some of the Linux settings, click *Linux Settings* and fill in the fields, then click *OK* to create the workload template and add it to the list.

Hostname: Specify the host name for the workload

Domain Name: Specify the domain for the workload (for example, netiq.com or provo.netiq.com).

You might not want to pre-populate some settings, such as *Hostname*, if the template will be used to create multiple workloads. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the user) or when performing the pre-build configuration (by an administrator).

9 (Optional) If you have already created organizations and resource groups that support workload templates, you can associate the workload template with the organizations and business groups of your choice, but you must choose an organization whose resource groups support the type of hypervisor (and VM template) compatible with the workload template.

9a Click *Associations*, then select either the *Organizations* tab or the *Business Groups* tab to open a list.

9b Select (that is, click) the organization or business group you want to associate with this workload template, then click *OK*.

or

Select (that is, Ctrl+click) the organizations or business groups you want to associate with this workload template, then click *OK*.

NOTE: The Workload Templates list displays only the workload templates from the organization where your business group resides. You must assign workload templates at the organization level before they become available for selection at the business group level.

For more information about workload templates, see Part IV, "Catalog Management," on page 87.

5 Creating an Organization

An organization represents a tenant to which you are offering Cloud services. Through the organization, you make resource group assignments that dictate the hosts, service levels, repositories, and networks available to the organization, and make workload template assignments that determine the types of business service workloads available to the organization.

After you create an organization, you can define the organization's membership and assign roles such as Business Service Owner, Business Group Sponsor, and Organization Manager to those members. Membership and role assignments are covered in the next task, "Creating Users and Groups" on page 29.

1. On the main navigation bar, click *Getting Started*, then click *Create Organizations* (in the *Set Up Your Cloud Environment* list).

   or

   On the main navigation bar, click *Organizations*, click the *Organizations* tab, then click *Create*.

2. Provide the following details to define the organization:

   Name: Specify a unique name for the organization. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Description: Provide any additional information to identify the organization.

   Domains: If you want to enable users to self-register in this organization, specify the e-mail domains associated with the organization.

   Self-registration occurs when a valid LDAP user who does not have a Cloud Manager account first logs in. The user's e-mail domain is compared to the e-mail domains defined for the organization. If it matches one of the e-mail domains, the user is added to organization's Members list.

   You can associate one or more e-mail domains with the organization. To specify multiple e-mail domains, separate the names with commas (for example, `netiq.com,novell.com,attachmate.com`).

   Discount %: If you want a discount applied to all business services created by members of this organization, specify the discount percentage.

   Auto Approval: When a user creates a business service request, the request goes through an approval workflow that includes both a Sponsor and an Administrator. The Sponsor is a member of the organization who provides the financial approval for the business service. The Administrator is a System user (such as yourself, another Cloud Administrator, or a Zone Administrator) who provides the resource capacity approval for the business service. You can use Auto Approval to bypass one or both of the approvals.

   The organization inherits the Auto Approval settings from the Cloud Manager system settings (accessed through *Configuration* on the main navigation bar). To change the settings for the organization, click *Override*, then configure the settings as desired.

Logo: You can upload a logo file for the organization. Three formats are supported: PNG, JPG, and GIF. Any size is acceptable. Cloud Manager resizes the logo to a maximum of 216x216 pixels, maintaining the width-to-height proportions. For example, a 432x200 image would be resized to 216x100. The logo file is stored on the Cloud Manager Application Server.

To upload a file, mouse over *No Image*, then click *Upload New Image*. Browse for and select the image, then click *OK* to upload it to the Cloud Manager Application Server.

3 Add the resource groups that you want the organization to have access to:

3a Under *Membership and Access*, click the *Resource Groups* tab.

3b Click *Add* to display the Add Resource Groups dialog box.

3c Select the resource groups you want to add.

You can Shift-click and Ctrl-click to select multiple groups.

3d Click *OK* to add the selected resource groups to the *Resource Groups* list.

4 Add the workload templates that you want the organization to have access to:

4a Under *Membership and Access*, click the *Workload Templates* tab.

4b Click *Add* to display the Add Workload Templates dialog box.

4c Select the workload templates.

You can Shift-click and Ctrl-click to select multiple workload templates.

4d Click *OK* to add the selected workload templates to the *Workload Templates* list.

5 Add the networks that you want the organization to have access to.

The available networks are determined by the VM hosts included in the resources group. However, to enable you to provide isolated networks for organizations that share the same resource group, the networks from a resource group are not automatically assigned to an organization when you add the resource group. Instead, you must separately add the networks you want assigned to the organization.

5a Under *Membership and Access*, click the *Networks* tab.

5b Click *Add* to display the Add Networks dialog box.

5c Select the networks.

You can Shift-click and Ctrl-click to select multiple workload templates.

5d Click *OK* to add the selected networks to the *Networks* list.

6 Ignore the *Users* tab and the *Business Groups* tab at this time.

The *Users* tab lets you add members to the organization and assign them roles within the organization. The *Business Groups* tab lets you view the sub-units that have been created for the organization. Creating business groups is covered in the next task, "Creating an Organization's Business Groups" on page 27. Creating users is covered in Chapter 7, "Creating Users and Groups," on page 29.

7 Click *Save* to create the organization and add it to the list.

For more information about organizations, see Part V, "Organization Management," on page 103.

6 Creating an Organization's Business Groups

An organization includes one or more business groups. A business group represents a unit within the organization, such as a department or cost center, for which business services can be deployed.

A business group can be assigned access to all of an organization's resources or only some of the resources. When a business service is created for a business group, it uses only the assigned resources. Multiple business groups can be assigned the same resources, which means that the resources become shared resources.

1 On the main navigation bar, click *Getting Started*, then click *Create Business Groups* (in the *Set Up Your Cloud Environment* list).

or

On the main navigation bar, click *Organizations*, click the *Business Groups* tab, then click *Create*.

2 Provide the following details to define the business group:

Name: Specify a unique name for the group. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

Organization: Select the organization where you want to add the business group.

Description: Provide any additional information to identify the business group.

Auto Approval: Business service requests require approval from both the group's Sponsor and an administrator. The *Auto Approval* settings let you bypass one or both of the approvers.

The business group inherits the *Auto Approval* settings from its organization. To change the settings for the business group, click *Override*, then configure the settings as desired.

Costs: The business group inherits the *Costs* setting from its organization. To change the setting for the business group, click *Override*, then configure the setting as desired. The *Show* setting allows group members to see cost information for workloads. The *Hide* setting prevents group members from seeing cost information.

3 Add the resource groups that you want the business group to have access to:

3a Under *Membership and Access*, click the *Resource Groups* tab.

3b Click *Add* to display the Add Resource Groups dialog box.

The list displays the organization's resource groups. A business group is limited to the resource groups assigned to its organization.

3c Select the resource groups you want to add.

You can Shift-click and Ctrl-click to select multiple groups.

3d Click *OK* to add the selected resource groups to the *Resource Groups* list.

4 Add the workload templates that you want the business group to have access to:

4a Under *Membership and Access*, click the *Workload Templates* tab.

4b Click *Add* to display the Add Workload Templates dialog box.

The list displays the organization's workload templates. A business group is limited to the workload templates assigned to its organization.

4c Select the workload templates.

You can Shift-click and Ctrl-click to select multiple workload templates.

4d Click *OK* to add the selected workload templates to the *Workload Templates* list.

5 Add the networks that you want the business group to have access to.

The available networks are determined by the VM hosts included in the resources groups you added in Step 3. However, to enable you to provide isolated networks for business groups that share the same resource group, the networks from a resource group are not automatically assigned to a business group when you add the resource group. Instead, you must separately add the networks you want assigned to the business group.

5a Under *Membership and Access*, click the *Networks* tab.

5b Click *Add* to display the Add Networks dialog box.

The list displays the organization's networks. A business group is limited to the networks assigned to its organization.

5c Select the networks.

You can Shift-click and Ctrl-click to select multiple networks.

5d Click *OK* to add the selected networks to the *Networks* list.

6 Ignore the *Users* tab and the *Business Services* tab at this time.

The *Users* tab lets you add members to the business group and assign them roles within the business group. The *Business Services* tab lets you view the business services that are currently deployed for the business unit. Creating users for the business group is covered in the next task, "Creating Users and Groups" on page 29.

7 Click *Save* to create the business group and add it to the list.

For more information about business groups, see Part V, "Organization Management," on page 103.

7 Creating Users and Groups

Access to Cloud Manager requires a Cloud Manager user account. Through the account, a user receives rights to perform various roles in the Cloud Manager system, in an organization, or in both. Rights can also be assigned to user groups to enable all members of the group to perform specific roles.

You can create users and groups by manually entering information or by importing information from your LDAP authentication source.

7.1 Manually Creating Users

1. On the main navigation bar, click *Getting Started*, then click *Create Users and Groups* (in the *Set Up Your Cloud Environment* list).

   or

   On the main navigation bar, click *Organizations*, then click the *Users* tab.
2. On the *Users* tab, click *Create* to display the Create User dialog box.
3. Provide the following details to define the user:

   Full Name: Specify the user’s full name as you want it to appear in NetIQ Cloud Manager.

   E-Mail Address: Specify the user’s e-mail address as defined in their LDAP authentication account. If necessary, you can specify more than one address; use commas to separate addresses.

   The e-mail address enables the Cloud Manager system to send messages (tasks, notifications, and so forth) to the user as needed.

   Phone Number: This field is optional. Specify a contact number if desired.
4. Select the user’s scope:

   Organization: An organization scope enables the user to perform roles within a specific organization. The roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

   To give the user an organization scope, select *Organization*, then select the organization in which to place the user.

   System: A system scope enables the user to administer the Cloud Manager system. The roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. In addition, a System user can be given any of the organization roles.
5. (Organization user only) If you want the user to always be able to view business service costs regardless of the *Costs* setting for a business group, select *Always show costs*.

An organization's or business group's *Costs* setting can be set to *Show* or *Hide*. The purpose of the *Always show costs* setting is to ensure that business service costs are always visible to the user even if the *Costs* setting is set to *Hide*.

For example, you might want to select this option for users who are Sponsors. This ensures that the users can always see costs even if the organization or business group is set to hide costs.

6 (System user only) Assign system-level roles to the user.

The system-level roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. These roles can be assigned only to System users.

6a To assign the Approver, Build Administrator, Catalog Manager, or Cloud Administrator role, click the *System* tab, click *Add*, select the desired roles, then click *OK*.

6b To assign the Zone Administrator role, click the *Zone* tab, click *Add*, select the desired zone, then click *OK*.

7 Assign organization-level roles to the user.

The organization-level roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor. The Approver and Build Administrator roles can be assigned only to System users. The other roles can be assigned to both System users and Organization users.

Several of the roles can be assigned at the organization, business group, or business service level. For example, you can make a user a Sponsor for a business group, in which case the user can approve requests for business services from that business group only. Or, you can make the user a Sponsor for the organization, in which case the user can approve requests for all business services in the organization.

7a Click the *Organization* tab to add a role at the organization level, click the *Business Group* tab to add a role at the business group level, or click the *Business Service* tab to add a role at the business service level.

7b Click the role that you want to assign

For example, if you selected the *Business Group* tab and you want to enable the user to create business services for the business group, click *Business Service Owner*.

7c Click *Add*, select the object (organization, business group, or business service) to which you want the role to apply, then click *OK* to add it to the list.

8 Ignore the *Membership* tab at this time.

The *Membership* tab lets you add users to groups. You must create the groups first. This task is discussed in "Manually Creating User Groups" on page 31 and "Importing User Groups from LDAP" on page 34

9 When you have finished assigning roles to the user, click *Save*.

For more information about users and roles, see Part III, "User Management," on page 59.

7.2 Manually Creating User Groups

Rather than assign roles to individual users, you can create user groups and assign roles to the user groups. Users (and other user groups) that are added to a group inherit the group's roles.

User group roles are cumulative. If you add a user to a group, the user retains its directly assigned roles and also gains the roles inherited from the group.

1. On the main navigation bar, click *Getting Started*, then click *Create Users and Groups* (in the *Set Up Your Cloud Environment* list).

   or

   On the main navigation bar, click *Organizations*.
2. Click the *User Groups* tab, then click *Create* to display the Create User Group dialog box.
3. Provide the following details to define the user group:

   Full Name: Specify the group's full name as you want it to appear in NetIQ Cloud Manager.

   E-Mail Address: This field is optional. If you enter an e-mail address, any messages generated for the group's roles are sent to the e-mail address. If you don't enter an e-mail address, the messages are sent to the group members' addresses.
4. Select the group's scope:

   Organization: An organization scope enables the group to be assigned roles within a specific organization. The roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

   To give the group an organization scope, select *Organization*, then select the organization in which to place the group.

   System: A system scope enables the group to be assigned roles for the Cloud Manager system. The roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. In addition, a System group can be given any of the organization roles.
5. (System user groups only) Assign system-level roles to the group.

   The system-level roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. These roles can be assigned only to System user groups.

   5a To assign the Approver, Build Administrator, Catalog Manager, or Cloud Administrator role, click the *System* tab, click *Add*, select the desired roles, then click *OK*.

   5b To assign the Zone Administrator role, click the *Zone* tab, click *Add*, select the desired zone, then click *OK*.
6. Assign organization-level roles to the group.

   The organization-level roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor. The Approver and Build Administrator roles can be assigned only to System user groups. The other roles can be assigned to both System and Organization user groups.

Several of the roles can be assigned at the organization, business group, or business service level. For example, you can make a user group a Sponsor for a business group, in which case the group members can approve requests for business services from that business group only. Or, you can make the user group a Sponsor for the organization, in which case the group members can approve requests for all business services in the organization.

6a Click the *Organization* tab to add a role at the organization level, click the *Business Group* tab to add a role at the business group level, or click the *Business Service* tab to add a role at the business service level.

6b Click the role that you want to assign.

For example, if you selected the *Business Group* tab and you want to enable the user group to create business services for the business group, click *Business Service Owner*.

6c Click *Add*, select the object (organization, business group, or business service) to which you want the role to apply, then click *OK* to add it to the list.

7 Add members to the group:

7a Click the *Membership* tab.

7b Click *Members*, then click *Add* to display the Add Members dialog box.

7c Select the users and user groups you want to add to the group.

You can Shift-click and Ctrl-click to select multiple users and groups.

7d Click *OK* to add the users and user groups to the Members list.

8 When you have finished assigning roles and adding members, click *Save*.

For more information about user groups and roles, see Part III, "User Management," on page 59.

7.3 Importing Users from LDAP

You can create users by importing information from your LDAP authentication source. You can import users as System or Organization users. After you import a user, you can assign roles to the user.

1 On the main navigation bar, click *Getting Started*, then click *Create Users and Groups* (in the *Set Up Your Cloud Environment* list).

or

On the main navigation bar, click *Organizations*.

2 If you want to import Organization users, click the *Organizations* tab, select the target organization for the import, click *Edit* to display the Edit Organization dialog box, then click *Import* (located above the *Members* list on the *Users* tab).

or

If you want to import System users, click *Configuration* (on the main navigation bar) to display the System Configuration dialog box, click the *Users* tab, click the *Members* tab, then click *Import*.

3 Authenticate to the LDAP directory:

3a Click the *LDAP* tab.

3b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

3c In the *Search Bind Account* section, fill in the following fields:

DN: Specify an account that has search rights to the directory location from which you want to import users. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Password Confirm: Confirm the password for the account.

3d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information and try again.

4 Import users:

4a Click the *Import* tab.

4b Click *Add*.

When you click *Add*, an new import entry is added to the list. You use the fields below the list to define the entry.

4c In the DN field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all users located within the container are imported. If you only want to import one user, specify the DN of the user object.

4d If you specified a container for import, select *Users*.

4e If you specified a container for import, select *Scan Tree* if you want to import users located in its subcontainers.

4f Click *Import*.

The imported users are added to the *Members* list. Users are identified by the  icon.

5 When you have finished importing users, click *OK* or *Save* to close the dialog box.

6 Assign roles to the users:

6a On the main navigation bar, click *Organizations*.

6b Click the *Users* tab, select the user to whom you want to assign roles, then click *Edit*.

6c (System user only) Assign system-level roles.

The system-level roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. These roles can be assigned only to System users.

6c1 To assign the Approver, Build Administrator, Catalog Manager, or Cloud Administrator role, click the *System* tab, click *Add*, select the desired roles, then click *OK*.

6c2 To assign the Zone Administrator role, click the *Zone* tab, click *Add*, select the desired zone, then click *OK*.

6d Assign organization-level roles.

The organization-level roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor. The Approver and Build Administrator roles can be assigned only to System users. The other roles can be assigned to both System users and Organization users.

Several of the roles can be assigned at the organization, business group, or business service level. For example, you can make a user a Sponsor for a business group, in which case the user can approve requests for business services from that business group only. Or, you can make the user a Sponsor for the organization, in which case the user can approve requests for all business services in the organization.

6d1 Click the *Organization* tab to add a role at the organization level, click the *Business Group* tab to add a role at the business group level, or click the *Business Service* tab to add a role at the business service level.

6d2 Click the role that you want to assign

For example, if you selected the *Business Group* tab and you want to enable the user to create business services for the business group, click *Business Service Owner*.

6d3 Click *Add*, select the object (organization, business group, or business service) to which you want the role to apply, then click *OK* to add it to the list.

6e When you have finished assigning roles to the user, click *Save*.

For more information about users and roles, see Part III, "User Management," on page 59.

7.4 Importing User Groups from LDAP

You can create user groups by importing them from your LDAP authentication source. After you import a group, you can assign roles to the group.

An imported user group's membership is maintained in the LDAP authentication source. Any users who are members of the user group in the LDAP source receive the roles that are assigned to the user group in Cloud Manager.

An imported user group's members are not imported and do not display in the group's *Members* list. In addition, you cannot manually add users or user groups to an imported group.

1 On the main navigation bar, click *Getting Started*, then click *Create Users and Groups* (in the *Set Up Your Cloud Environment* list).

or

On the main navigation bar, click *Organizations*.

2 If you want to import Organization user groups, click the *Organizations* tab, select the target organization for the import, click *Edit* to display the Edit Organization dialog box, then click *Import* (located above the *Members* list on the *Users* tab).

or

If you want to import System user groups, click *Configuration* (on the main navigation bar) to display the System Configuration dialog box, click the *Users* tab, click the *Members* tab, then click *Import*.

3 Authenticate to the LDAP directory:

3a Click the *LDAP* tab.

3b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

3c In the *Search Bind Account* section, fill in the following fields:

User DN: Specify an account that has read rights to the directory location from which you want to import users. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Password Confirm: Confirm the password for the account.

3d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information try again.

4 Import user groups:

4a Click the *Import* tab.

4b Click *Add*.

When you click *Add*, an new import entry is added to the list. You use the fields below the list to define the entry.

4c In the DN field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all user groups located within the container are imported. If you only want to import one user group, specify the DN of the user group object.

4d If you specified a container for import, select *Groups*.

4e If you specified a container for import, select *Scan Tree* if you want to import user groups located in its subcontainers.

4f Click *Import*.

The imported user groups are added to the *Members* list. User groups are identified by the  icon.

5 When you have finished importing user groups, click *OK* or *Save* to close the dialog box.

6 Assign roles to the groups:

6a On the main navigation bar, click  *Organizations*.

6b Click the *Users* tab, select the user group to which you want to assign roles, then click *Edit*.

6c (System user groups only) Assign system-level roles.

The system-level roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. These roles can be assigned only to System user groups.

6c1 To assign the Approver, Build Administrator, Catalog Manager, or Cloud Administrator role, click the *System* tab, click *Add*, select the desired roles, then click *OK*.

6c2 To assign the Zone Administrator role, click the *Zone* tab, click *Add*, select the desired zone, then click *OK*.

6d Assign organization-level roles.

The organization-level roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor. The Approver and Build Administrator roles can be assigned only to System user groups. The other roles can be assigned to both System and Organization user groups.

Several of the roles can be assigned at the organization, business group, or business service level. For example, you can make a user group a Sponsor for a business group, in which case the group members can approve requests for business services from that business group only. Or, you can make the user group a Sponsor for the organization, in which case the group members can approve requests for all business services in the organization.

6d1 Click the *Organization* tab to add a role at the organization level, click the *Business Group* tab to add a role at the business group level, or click the *Business Service* tab to add a role at the business service level.

6d2 Click the role that you want to assign

For example, if you selected the *Business Group* tab and you want to enable the user group to create business services for the business group, click *Business Service Owner*.

6d3 Click *Add*, select the object (organization, business group, or business service) to which you want the role to apply, then click *OK* to add it to the list.

6e When you have finished assigning roles to the user group, click *Save*.

For more information about user groups and roles, see Part III, "User Management," on page 59.

System Management

The following sections provide information to help configure and manage your Cloud Manager system:

8 Managing Zones

A Cloud Manager zone is single Cloud Manager Orchestration Server and its managed resources (VM hosts, storage repositories, networks, and so forth). The following sections provide instructions to help you manage your zones:

8.1 Creating Zones

Roles that Can Perform This Task: Cloud Administrator

A Cloud Manager zone is a single Cloud Manager Orchestration Server and its managed resources (VM hosts, storage repositories, networks, and so forth). You create a zone by defining a connection to the Orchestration Server. After you create the zone, its resources become part of the Cloud environment that you can use to service your customers.

1. On the main navigation bar, click *Configuration*, click the *Zones* tab, then click *Create*.
2. Provide the following information:

   Name: Provide a unique name for the zone. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Description: If desired, add more information to further identify the zone. The description is displayed in Cloud Manager to administrators only.

   Enabled: Leave this setting selected.

   Server Address: Specify the DNS name or IP address of the Orchestration Server.

   Server Port: Specify the port used by the Orchestration Server Web Service.

   Username: Specify the Administrator user name that enables login to the Orchestration Server.

   Password: Specify and confirm the password for the user name you supplied.

   Secure Connection: Select this option if the Cloud Manager Application Server is configured for an SSL connection to the Orchestration Server.
3. Click *OK* to create the zone and add it to the list.
4. When you have finished creating zones, click *OK* to close the System Configuration dialog box.

8.2 Disabling Zones

Roles that Can Perform This Task: Cloud Administrator

The primary purpose for disabling a zone is to perform maintenance tasks on the Cloud Manager Orchestration Server without receiving error messages and exceptions in the Cloud Manager console because the server is down. While the zone is disabled, the following occurs:

- Any objects (hosts, VM templates, and so forth) provided by the zone's Orchestration Server are no longer displayed in the Cloud Manager console. However, Cloud Manager objects (resource groups, service levels, workload templates, and so forth) are still displayed. A user receives a "Zone Disabled" error when adding, editing, or deleting any Cloud Manager object that includes an Orchestration Server object.
- Any workloads deployed in the zone continue in their current state (unless an issue with the zone causes them to be stopped). In the Cloud Manager console, a workload's state displays as "Unknown" and the owner cannot cycle the workload.

To disable a zone:

1. On the main navigation bar, click *Configuration*, then click the *Zones* tab.
2. Select the zone to disable, then click *Edit*.
3. Deselect the *Enabled* check box.
4. Click *OK* to disable the zone.

8.3 Enabling Zones

Roles that Can Perform This Task: Cloud Administrator

To enable a zone:

1. On the main navigation bar, click *Configuration*, then click the *Zones* tab.
2. Select the zone to enable, then click *Edit*.
3. Select the *Enabled* check box.
4. Provide the Administration password for the Cloud Manager Orchestration Server.
5. Click *OK* to enable the zone.

8.4 Removing Zones

Roles that Can Perform This Task: Cloud Administrator

You cannot remove a zone that has 1) business service workloads running in the zone, 2) business service requests in process, or 3) resource groups, service levels, and workload templates associated with the zone.

To remove a zone:

1. On the main navigation bar, click  *Configuration*, then click the *Zones* tab.
2. Select the zone to remove, then click *Remove*.

   If the *Remove* action is not available, the zone has workload templates or resource groups associated with it.
3. Click *Yes* to confirm removal of the zone.

9 Customizing the Capacity Thresholds and Data Refresh Interval

Roles that Can Perform This Task: Cloud Administrator

The Capacity view provides resource capacity and usage information for the organizations and zones in your system.

The Capacity view has two settings you can customize: *Thresholds* and *Data Refresh Interval*. *Thresholds* lets you set the Warning threshold and Problem threshold for used resource capacity. *Data Refresh Interval* lets you determine how often capacity data is collected.

1. On the main navigation bar, click *Configuration*, then click the *Capacity* tab.
2. Under *Thresholds*, select the Warning and Problem thresholds you want for each resource (Memory, CPU, and Storage).

   The Capacity view displays resource usage as a percentage of the total capacity. Visually, this is displayed as a horizontal bar ranging from 0 percent to 100 percent.

   The Warning and Problem thresholds help you quickly see when resource usage is approaching your resource capacity. Up to the Warning threshold, usage is displayed as a green bar. When the Warning threshold is reached, usage is displayed as a yellow bar. When the Problem threshold is reached, usage is displayed as a red bar.
3. Under *Data Refresh Interval*, specify a frequency for collecting capacity data from your system.
   - **3a** (Optional) Select *No Refresh* if you choose not to periodically refresh the data. This option keeps the original capacity data for display on the Capacity dashboard.
   - **3b** (Optional) Select *Interval* to specify how frequently you want to initiate capacity data collection.

     Keep in mind that data collection can be an intensive process. The frequency of data collection and the duration of data collection (which is dependent on the size of your system) could affect your system's performance. You should specify an interval that balances the need for up-to-date information against the potential impact to system performance while the Capacity engine is running.

     The system must update the capacity data at least once before you can accurately estimate the interval. You can base your estimate on the data displayed in the Capacity Update dialog box when you select *Update* in the Capacity view.
   - **3c** (Optional) Select *Daily Time* to specify the time each day (based on the Cloud Manager Application Server's clock and time zone) when you want Cloud Manager to collect capacity data.
4. Click *OK* to save your change.

10 Managing System Users, User Groups, and Roles

Roles that Can Perform This Task: Cloud Administrator

You can add users and user groups to the system and then assign roles to the users and groups so that they can perform specific functions within the system or within organizations.

Users, user groups, and roles are covered in Part III, “User Management,” on page 59.

11 Configuring E-Mail Notifications

Roles that Can Perform This Task: Cloud Administrator

Cloud Manager can send e-mail messages to remind task owners about tasks that need to be completed and to notify Business Service Owners of business services that are about to expire or that have expired. For Cloud Manager to do this, you must provide the connection information for an SMTP server to route the messages. You can also customize the schedule for the message notifications.

1. On the main navigation bar, click *Configuration*, then click the *Notification* tab.
2. Configure the SMTP server connection:

   Host: Specify the IP address or DNS name of the host running the SMTP server.

   Server Port: Specify the port on which the SMTP server listens for incoming messages.

   Use Authentication: If the SMTP server requires an authentication user name and password, select this option, then specify the user name and password.
3. If desired, customize the schedule for task notifications:

   Number of days allocated to complete a task: Select how long a task owner has to complete a task before it becomes overdue. The default is 5 days.

   Number of days before first reminder notification: Select when a task owner receives the first reminder notification about the due date. The default is 3 days before the task due date.

   Number of days between notifications: Select how often, after the first reminder notification, a task owner receives follow-up notifications about the due date. The default is every day.
4. If desired, customize the schedule for business service expiration notifications:

   Number of days before first expiration notification: Select when a Business Service Owner receives the first e-mail that the business service is about to expire. The default is 7 days before the expiration date.

   Number of days between notifications: Select how often, after the initial notification, a Business Service Owner receives follow-up e-mails about the expiration date. The default is every day.
5. Click *OK*.

12 Configuring Remote Console Access to Workloads

The Cloud Manager console provides remote console access to business service workloads via an embedded Flash VNC application. The application can connect to workloads either directly or through a VNC repeater (proxy).

By default, the Cloud Manager console is configured to use the VNC repeater included with the Cloud Manager Application Server. Alternately, you can set up an external VNC repeater or configure the VNC application to connect directly to workloads. Each solution has advantages and disadvantages

Solution	Advantages	Disadvantages
Built-In Repeater	◆ Minimal setup ◆ Supports NAT and firewalls ◆ If used with NAT or a firewall, use can be limited to Cloud Manager users	◆ VNC traffic flows through Cloud Manager Application Server, increasing workload on a single server
External Repeater	◆ Supports NAT and firewalls ◆ Offloads VNC traffic from the Cloud Manager Application Server ◆ Scalable by clustering the repeater	◆ Increased setup ◆ VNC requests are not authenticated through Cloud Manager
Direct Connection	◆ Most scalable	◆ Each workload must include a VNC server ◆ No support for NAT or firewalls ◆ VNC requests are not authenticated through Cloud Manager

The following sections provide instructions for configuring each of the remote console access solutions:

12.1 Disabling Remote Console Access

Roles that Can Perform This Task: Cloud Administrator

If you don't want users to be able to access workloads through the Cloud Manager console, you can disable remote console access. This disables remote console access to all workloads through the Cloud Manager console only. It does not disable VNC on the host or the workload.

1. On the main navigation bar, click *Configuration*, then click the *Remote Console* tab.
2. In the *Connection* field, select *Disable*.
3. Click *OK*.

12.2 Setting Up the Built-In VNC Repeater

Roles that Can Perform This Task: Cloud Administrator

To have the Cloud Manager console use the built-in VNC repeater:

1. On the main navigation bar, click *Configuration*, then click the *Remote Console* tab.
2. In the *Connection* field, select *Use built-in VNC repeater*.
3. If the VNC repeater requires a static port for reasons such as firewall support, specify the port in the *Repeater Port* field. Otherwise, leave the field blank so that the VNC repeater dynamically selects an available port when it starts.
4. Click *OK*.

12.3 Setting Up an External VNC Repeater

Roles that Can Perform This Task: Cloud Administrator

To have the Cloud Manager console use an external VNC repeater:

1. Install the VNC repeater by using the product's documentation.
2. Configure the repeater to respond to both Flash policy requests and VNC proxy requests.
3. In the Cloud Manager console, configure the remote console to use the external repeater:
   - **3a** On the main navigation bar, click *Configuration*, then click the *Remote Console* tab.
   - **3b** In the *Connection* field, select *Use external VNC repeater*.
   - **3c** In the *Repeater Address* field, specify the DNS or IP address of the VNC repeater's server.
   - **3d** In the *Repeater Port* field, specify the port assigned to the repeater.
   - **3e** Click *OK*.

12.4 Setting Up Direct Connections

Roles that Can Perform This Task: Cloud Administrator

To have the Cloud Manager console connect directly to workloads:

1. Make sure that each VM host or VM is configured with a VNC Server.

   Depending on the hypervisor, the VM host might handle the VNC requests for the VM or the VM might handle the requests. Refer to your hypervisor documentation for information about how your hypervisor handles VNC requests to VMs.
2. Configure the VNC Server to respond to Flash policy requests.
3. In the Cloud Manager console, configure the remote console to use a direct connection:
   - **3a** On the main navigation bar, click *Configuration*, then click the *Remote Console* tab.
   - **3b** In the *Connection* field, select *Connect directly*.
   - **3c** Click *OK*.

12.5 Enabling Repeater SSL Encryption

Roles that Can Perform This Task: Cloud Administrator

To enable SSL encryption of VNC traffic between your browser and the VNC repeater (making it difficult for an outside entity to intercept and analyze activity between your browser and the repeater):

1. On the main navigation bar, click *Configuration*, then click the *Remote Console* tab.
2. Select the *Enable Repeater SSL Encryption* check box.
3. In the *Repeater Keystore* field, enter the path to a Java keystore where the SSL key to the VNC Repeater is stored.

   By default, this field is populated from the original Cloud Manager SSL configuration (if that option was chosen).
4. In the *Keystore Password* field, enter the password to the Java keystore where the SSL key to the VNC Repeater is stored.

   By default, this field is populated from the original Cloud Manager SSL configuration (if that option was chosen).
5. (Conditional) If you select the built-in repeater, specify the path to the repeater keystore and passwords. The first password (required) opens the keystore file. The second password (optional) retrieves the private key within the file. The need for the second password depends on the settings you used when you generated the keystore.

   NOTE: The fields on this page validate the keystore and passwords as you make changes: if you enter an incorrect password, the field displays a red asterisk.
6. Click *OK*.

13 Configuring Auto Approval for Business Service Requests

Roles that Can Perform This Task: Cloud Administrator

When a business service request is submitted, the request goes through an approval workflow that requires both a Sponsor approval and an Administrator approval. The Sponsor approval is intended to be a financial check and the Administrator approval is intended to be a resource capacity check.

You can enable automatic Sponsor approval, Administrator approval, or both for your system. This eliminates the need to assign users as Sponsors and Approvers for organizations or business group. If you don't want the system settings to apply to an organization or a business group, you can override the settings at the organization or business group.

To configure the system Auto Approval settings:

1. On the main navigation bar, click *Configuration*, then click the *Tasks* tab.
2. Select *Sponsor* to enable automatic Sponsor approval.
3. Select *Administrator* to enable automatic Administrator approval.
4. Click *OK* to save the changes.

14 Customizing the Workload Update Schedule

Roles that Can Perform This Task: Cloud Administrator

When a business service is deployed, Cloud Manager takes a snapshot of the business service's workloads. This snapshot maintains a record of the service levels, resource allocations, and costs associated with the workloads at deployment time.

For business services with an expiration date, the snapshot is updated only if the business service is changed and redeployed. At that time, Cloud Manager takes a new snapshot that reflects any changes to the service levels, resource allocations, and costs associated with the workloads. For example, if the cost of the resources has increased since the first deployment, the second deployment reflects the cost increase.

For business services without an expiration date, you can determine when workload snapshots are updated so that non-expiring business services accurately reflect changes in the service levels, resource allocations, and costs associated with their workloads. You can update workloads either weekly or monthly. The update occurs on the last day of the selected period. You can also force an immediate update.

1. On the main navigation bar, click *Configuration*, then click the *Workload Updates* tab.
2. Select *Weekly* or *Monthly* for the update frequency.
3. If you want to force an update immediately, click *Update Now.*
4. Click *OK.*

15 Customizing the Cloud Manager Console Interface

Roles that Can Perform This Task: Cloud Administrator

The Cloud Manager console has two interface settings that you can customize: *Currency* and *Workload Dialog*. *Currency* determines the display symbol that is used in Cloud Manager currency fields. *Workload Dialog* determines which tabs (*Windows Settings*, *Windows Licensing*, *Linux Settings*, and *Networks*) are displayed when creating and managing business service workloads.

1. On the main navigation bar, click *Configuration*, then click the *User Interface* tab.
2. Under *Currency*, select the currency symbol you want to use.

   This setting affects only the display symbol. It does not affect the format of the currency fields. All fields are formatted as 00.00 regardless of the currency symbol. In addition, changing the currency symbol does not perform any currency conversion on existing costs (workloads, workload templates, resources, and so on). For example, if you change from United States Dollar (USD) to Euro (EUR), $50.00 simply becomes €50.00.

   Any users who log in after the change see the new currency symbol. For you to see the change, you must log out and then log in again.
3. Under *Workload Dialog*, select the workload tabs you want hidden.

   A workload contains *Windows Settings, Windows Licensing*, *Linux Settings*, and *Networks* tabs that must be configured when requesting a business service. By default, these are displayed so that the user can fill in the required information.

   If you don't want to require the user to provide this information, you can hide any or all of the tabs. The Build Administrator or a Cloud Administrator must then provide the information when completing the pre-build configuration task for the requested business service.

   All organizations inherit this setting; however, you can override the inherited setting at each organization.
4. Under *Workload Dialog*, specify whether the entering the virtual machine name is to be mandatory for pre-configuration.
5. Click *OK* to save your change.

III User Management

The following sections provide information to help you manage the users and user groups in your Cloud environment:

16 User Concepts

Users must have a Cloud Manager account in order to perform activities within the Cloud Manager system. The following sections provide information you should understand as you create and manage user accounts and user groups:

16.1 Organization Scope versus System Scope

When you create a Cloud Manager account for a user, you can give the user an Organization scope or a System scope. The scope determines what roles can be assigned to the user.

A user with the Organization scope (referred to as an *Organization user* or *Organization member*) is assigned membership in a specific organization and can hold Organization roles. These roles provide rights to perform activities within the user’s organization, such as creating business groups, allocating organization resources to the business groups, and deploying business services.

A user with the System scope (referred to as a *System user*) is not assigned membership in an organization and can hold System roles. These roles provide rights to perform system-level activities, such as configuring the Cloud Manager system, creating zones, creating organizations, creating groups of resources for use by organizations, and monitoring zone and organization resource capacity. In addition, System users can be assigned Organization roles for any organization in the system.

Organization and System scopes also apply to user groups, meaning that there are *System user groups* and *Organization user groups*. Users groups are discussed in “Cloud Manager User Groups versus LDAP User Groups” on page 67.

Both System roles and Organization roles are discussed in detail in “Cloud Manager Roles” on page 61.

16.2 Cloud Manager Roles

A user must have one or more Cloud Manager roles in order to do anything in Cloud Manager. There are nine Cloud Manager roles. All nine roles can be given to System users, while only four of the roles can be given to Organization members. Each role carries its own set of rights and responsibilities for the Cloud Manager system or for an organization within the system.

16.2.1 Descriptions

The following five roles are System roles. Only System users can be assigned these roles.

- **Cloud Administrator:** Has full rights to the Cloud Manager system. Can perform all tasks in the system
- **Zone Administrator:** Has rights to manage the resources for one or more assigned zones. Only System users can be Zone Administrators.
- **Catalog Manager:** Has rights to create, modify, and delete workload templates. Workload templates must be assigned to organizations by the Cloud Administrator.
- **Build Administrator:** Has rights to complete pre-build and post-build configuration for workloads in requested business services.
- **Approver:** Has rights to approve or deny a business service request based on available zone and organization resource capacity.

The following four roles are Organization roles. Both Organization users and System users can be assigned these roles.

- **Organization Manager:** Has rights to manage users, role assignments, resource assignments, and business services within an assigned organization. System users can be assigned as Organization Managers in multiple organizations. Organization users can be assigned as Organization Managers only in their own organization.
- **Sponsor:** Has rights to approve or deny a business service request based on financial reasons.
- **Business Service Owner:** Has rights to create, modify, and delete business services for an organization or for specific business groups within an organization.
- **Business Group Viewer:** Has rights to view business services for a business group.

16.2.2 Rights

System Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
USERS									
Create System user accounts and user groups, either manually or by importing from an LDAP directory	■								
Modify System user and user group properties (e-mail, phone number, and so forth)	■								
ROLES									
Assign Cloud Administrator role	■								
Assign Zone Administrator role	■								
Assign Catalog Manager role	■								

System Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Assign Build Administrator role	■								
Assign Approver role	■								
CAPACITY & REPORTS									
View resource capacity for system	■								
Generate resource capacity reports for system	■								

Zone Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Assign Zone Administrator role	■								
Create, modify, and delete zones	■								
Create, modify, and delete resource groups for zones	■	■							
View resource capacity for zones	■	■							
Generate resource capacity reports for zones	■	■							

Organization Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
USERS									
Create Organization user accounts and user groups, either manually or by importing from an LDAP directory	■					■			

Organization Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Modify Organization user and user group properties (e-mail, phone number, and so forth)	■					■			
ROLES									
Assign Organization Manager role	■					■			
Assign Sponsor role	■					■			
Assign Business Group View role	■					■			
Assign Business Service Owner role	■					■			
ORGANIZATIONS									
Create modify, and delete organizations	■								
Assign a cost factor (discount or markup) to organizations	■					✔ *			
Assign resource groups to organizations	■								
Assign workload templates to organizations	■								
Assign networks to organizations	■								
BUSINESS GROUPS									
Create modify, and delete business groups	■					■			
Assign workload templates from an organization to its business groups	■					■			
Assign resource groups from an organization to its business groups	■					■			
Assign networks from an organization to its business groups	■					■			
View information and business services for a business group								■	
CAPACITY & REPORTS									
View resource capacity for organizations	■				■				

Organization Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Generate resource capacity reports for organizations	■					■			

* Applies only to an Organization Manager who is a System user. An Organization Manager who is a member of the organization cannot change the cost factor for the organization.

Resource Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
RESOURCE GROUPS									
Create, modify, and delete resource groups	■	■							
Assign resource groups to organizations	■								
Assign resource groups to an organization's business groups	■					■			
SERVICE LEVELS									
Create modify, and delete service levels	■								
Create modify, and delete service level objectives	■								
Assign resource costs to service levels	■								
Assign service levels to resource groups	■								
CAPACITY & REPORTS									
View resource capacity for organization	■				■				
View resource capacity for zone	■	■							
View resource capacity for system	■								
Generate resource capacity reports for organizations	■					■			

Resource Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Generate resource capacity reports for zones	■	■							
Generate resource capacity reports for the system	■								

Catalog Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Assign Catalog Managers	■								
Create, modify, and delete workload templates	■		■						
Assign workload templates to organizations	■								

Business Service Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Import existing VMs as business services	■								
Request new business services	■					■			■
Request changes to existing business services	■					■			■
Provide Administrator approval or rejection of business service requests (new and change)	■				■				
Provide Sponsor approval or rejection of business service requests (new and change)	■						■		

Business Service Management Rights	Cloud Administrator	Zone Administrator	Catalog Manager	Build Administrator	Approver	Organization Manager	Sponsor	Business Group Viewer	Business Service Owner
Complete pre-build and post-build workload configuration tasks for business service requests (new and change)	■			■					
Delegate business service ownership to other users	■					■			
Cycle (start, suspend, stop) business service workloads	■					■			■
Remotely access business service workloads	■					■			■
View business services								■	
Delete business services	■					■			■

16.3 Cloud Manager User Groups versus LDAP User Groups

Rather than assign roles to individual users, you can create user groups and assign roles to the user groups. Users who are added to a group inherit the group's roles.

There are two types of user groups:

- **Cloud Manager:** These groups are created in Cloud Manager. The group's membership is maintained in Cloud Manager. You can add both users and other groups (including LDAP user groups) to the group.
- **LDAP:** These groups are imported from your LDAP authentication source. The group's membership is maintained in the LDAP source. You cannot add users or other groups to the group in Cloud Manager.

16.4 Roles That Can Create User Accounts and User Groups

The following roles have rights to create users and user groups. This includes manually entering information to create users or groups and importing users or groups from the LDAP authentication source.

- **Cloud Administrator:** Can create both System and Organization users and groups.
- **Organization Manager:** Can create Organization users and groups for assigned organizations. For example, a System user who is an Organization Manager for multiple organizations can create users in each of the assigned organizations. An Organization user who is an Organization Manager for his or her organization can create users only for that organization.

17 Creating User Accounts

Access to Cloud Manager requires a Cloud Manager user account. Through the account, a user receives rights to perform various roles in the Cloud Manager system, in an organization, or in both.

There are two types of user accounts: System and Organization. A System account enables a user to be assigned system-level roles (Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator) and organization-level roles (Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor). You can also create accounts for Organization users. Organization users can be assigned organization-level roles only.

You can create users by manually entering information or by importing information from your LDAP authentication source.

17.1 Manually Creating System and Organization Users

Roles that Can Perform This Task: Cloud Administrator, Organization Manager (Organization users only)

The following steps explain how to create users by manually entering their information. For information about creating users by importing their information from your LDAP authentication source, see "Importing System Users from LDAP" on page 70 and Section 17.3, "Importing Organization Users from LDAP," on page 71.

1. On the main navigation bar, click *Organizations*.
2. Click the *Users* tab, then click *Create* to display the Create User dialog box.
3. Provide the following details to define the user:

   Full Name: Specify the user's full name as you want it to appear in Cloud Manager.

   E-Mail Address: Specify the user's e-mail address as defined in their LDAP authentication account. If necessary, you can specify more than one address; use commas to separate addresses.

   The e-mail address enables the Cloud Manager system to send messages (tasks, notifications, and so forth) to the user as needed.

   If LDAP is being used for authentication (without Access Manager or Cloud Security Services), the e-mail address is also used for login.

   Phone Number: This field is optional. Specify a contact number if desired.
4. Select the user's scope:

Organization: An organization scope enables the user to perform roles within a specific organization. The roles are Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

To give the user an organization scope, select *Organization*, then select the organization in which to place the user.

System: A system scope enables the user to administer the Cloud Manager system. The roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. In addition, a System user can be given any of the organization roles.

5 Add the user to user groups.

When you add a user to a group, the user inherits the roles assigned to the group.

5a Click the *Membership* tab.

5b Click *Add*, select the desired user groups, then click *OK*.

You can Shift-click and Ctrl-click to select multiple groups.

6 Click *Save* to add the user to the *Users* list.

7 To assign roles to the user, see Assigning Roles to Users and Groups.

17.2 Importing System Users from LDAP

Roles that Can Perform This Task: Cloud Administrator

The following steps explain how to create System users by importing information from your LDAP authentication source. For information about creating System users by manually entering information, see "Manually Creating System and Organization Users" on page 69.

1 On the main navigation bar, click *Configuration*.

2 Click the *Users* tab, click *Members*, then click *Import*.

3 Authenticate to the LDAP directory:

3a Click the *LDAP* tab.

3b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

3c In the *Search Bind Account* section, fill in the following fields:

DN: Specify the distinguished name of an account that has search rights to the directory location from which you want to import users. For example,
`cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Confirm Password: Confirm the password for the account.

3d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information and try again.

4 Import users:

4a Click the *Import* tab.

4b Click *Add*.

When you click *Add*, a new import entry is added to the list. You use the fields below the list to define the entry.

4c In the *DN* field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all users located within the container are imported. If you only want to import one user, specify the DN of the user object.

4d If you specified a container for import, select *Users*.

4e If you specified a container for import, select *Scan Tree* if you want to import users located in its subcontainers.

4f Click *Import*.

The imported users are added to the *Members* list. Users are identified by the  icon.

5 Click *OK* to close the System Configuration dialog box.

6 To assign roles to a user, see Assigning Roles to Users and Groups.

17.3 Importing Organization Users from LDAP

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

The following steps explain how to create Organization users by importing information from your LDAP authentication source. For information about creating Organization users by manually entering information, see "Manually Creating System and Organization Users" on page 69.

1 On the main navigation bar, click  *Organizations*.

2 Click the *Organizations* tab, select the target organization for the import, click *Edit* to display the Edit Organization dialog box.

3 On the *Users* tab, click *Members*, then click *Import*.

4 Authenticate to the LDAP directory:

4a Click the *LDAP* tab.

4b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

4c In the *Search Bind Account* section, fill in the following fields:

DN: Specify the distinguished name of an account that has search rights to the directory location from which you want to import users. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Confirm Password: Confirm the password for the account.

4d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information and try again.

5 Import users:

5a Click the *Import* tab.

5b Click *Add*.

When you click *Add*, a new import entry is added to the list. You use the fields below the list to define the entry.

5c In the *DN* field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all users located within the container are imported. If you only want to import one user, specify the DN of the user object.

5d If you specified a container for import, select *Users*.

5e If you specified a container for import, select *Scan Tree* if you want to import users located in its subcontainers.

5f Click *Import*.

The imported users are added to the *Members* list. Users are identified by the  icon.

6 Assign roles to a user.

An Organization user can be assigned roles at the organization level, business group level, or business service level. If you want to assign an imported user a role at the organization level, continue with the following steps. If you want to assign roles at the other two levels, exit the dialog box and see Assigning Roles to Users and Groups.

Users must be given roles in order to do anything in the organization. There are six roles that apply at the organization level: Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

Role assignments at the organization level are inherited by the organization's business groups. For example, if you give a user the Business Service Owner role for an organization, the user can create business services for any business group in the organization. If you want to limit the user to a role in specific business group, you must make the role assignment in the business group.

6a Click the role (*Approver*, *Build Administrator*, *Business Group Viewer*, *Business Service Owner*, *Organization Manager*, or *Sponsor*) that you want to assign to a user.

6b Click *Add*.

Depending on the role that you are adding, the selection dialog box can contain two lists: *Members* and *System Users*. The *Members* list includes all members of the organization and the *System Users* list includes all Cloud Manager System users.

6c Select the users you want to add, then click *OK*.

You can Shift-click and Ctrl-click to select multiple users.

7 Click *Save* to close the Edit Organization dialog box.

18 Providing Self Registration for Users

You can enable user accounts to be created automatically the first time valid LDAP users log in to the Cloud Manager Application Console. This process, referred to as self registration, requires you to associate users' domain names with the Cloud Manager system (for registering System users) or with organizations (for registering Organization users). For example, if you associated the `netiq.com` domain name with your system, any user who logged in with `netiq.com` in their e-mail address would be made a System user.

The following sections explain how to set up self registration and how to automate role assignments for self-registering users:

18.1 Setting Up Self Registration for System Users

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click  *Configuration*.
2. Click the *Users* tab.
3. In the *Domains* field, specify the e-mail domains that you want registered to the system.

   For example, if you want all users who log in with e-mail addresses that include the `netiq.com` or `novell.com` domain names, specify `netiq.com,novell.com`. Use a comma to separate domain names.
4. Click *OK* to save your changes.

18.2 Setting Up Self Registration for Organization Users

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click  *Organizations*.
2. On the *Organizations* tab, select the organization for which you want to set up self registration, then click *Edit*.
3. In the *Domains* field, specify the e-mail domains that you want registered to the organization.

For example, if you want all users who log in with e-mail addresses that include the `suse.com` domain name, specify `suse.com`. If you specify multiple domains, use a comma to separate domain names.

4 Click *OK* to save your changes.

18.3 Automating Role Assignments to Self-Registered Users

Roles that Can Perform This Task: Cloud Administrator

When a user self registers, his or her user account is created without any role assignments. You can manually assign roles to the user after the account is created, but this negates much of the administrative benefit gained by allowing the user to self register.

To receive the maximum benefit of self registration, you can assign roles to users through the use of LDAP user groups. By assigning roles to LDAP user groups, you can ensure that LDAP users who are members of those groups automatically inherit those roles when they self register.

To automate role assignments for self-registered users:

1 In your LDAP source, create the LDAP user groups you want.

For example, in the LDAP directory used for authenticating System users, you could create an LDAP user group for Cloud Administrators, another for Zone Administrators, and another for Build Administrators. In the LDAP directory used for authenticating an organization's users, you could create LDAP user groups for Organization Managers and Business Service Owners.

2 Add the appropriate LDAP users to each LDAP user group.

For example, if you created a Business Service Owners group, add the users who are Business Service Owners for the organization.

3 Add the LDAP user groups to Cloud Manager using one of the following methods:

- Import the user group information from LDAP. For instructions, see "Importing System User Groups from LDAP" on page 76 and "Importing Organization User Groups from LDAP" on page 77.
- Create the user groups by manually adding group information, including the distinguished name of the user group in LDAP. For instructions, see "Manually Creating System and Organization User Groups" on page 75.

4 Assign roles to the user groups. For instructions, see "Assigning Roles to Users and Groups" on page 81.

19 Creating User Groups

Rather than assign roles to individual users, you can create user groups and assign roles to the user groups. Users who are added to a group inherit the group's roles.

User group roles are cumulative. If you add a user to a group, the user retains its directly assigned roles and also gains the roles inherited from the group.

As with users, there are two types of user groups: System and Organization. A System group can be assigned system-level roles (Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator) and organization-level roles (Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor). An Organization user group can be assigned organization-level roles only.

You can create user groups by manually entering information or by importing information from your LDAP authentication source.

19.1 Manually Creating System and Organization User Groups

Roles that Can Perform This Task: Cloud Administrator, Organization Manager (Organization users only)

The following steps explain how to create user groups by manually entering information. For information about creating user groups by importing information from your LDAP authentication source, see "Importing System User Groups from LDAP" on page 76 and Section 17.3, "Importing Organization Users from LDAP," on page 71.

1. On the main navigation bar, click *Organizations*.
2. Click the *User Groups* tab, then click *Create* to display the Create User Group dialog box.
3. Provide the following details to define the user group:

   Full Name: Specify the group's full name as you want it to appear in Cloud Manager.

   E-Mail Address: This field is optional. If you enter an e-mail address, any messages generated for the group's roles are sent to the e-mail address. If you don't enter an e-mail address, the messages are sent to the group members' addresses.
4. In the *Scope* field, select *System*.
5. In the *Type* field, select the group's type:
   - **LDAP DN:** Select this option to specify an LDAP group. The group's membership is maintained in the LDAP source. You cannot add users to the group in Cloud Manager.

Use standard LDAP notation to specify the distinguished name of the user group in the LDAP source (for example, `cn=orgmanagers,dc=provo,dc=netiq,dc=com`).

- **Cloud Manager:** Select this option to create a user group that exists only in Cloud Manager. You maintain the group membership in Cloud Manager. The group can include both users and other groups (including LDAP user groups).

6 Add members to the group:

6a Click the *Membership* tab.

6b Click *Members*, then click *Add* to display the Add Members dialog box.

6c Select the users and user groups you want to add to the group.

You can Shift-click and Ctrl-click to select multiple users and groups.

6d Click *OK* to add the users and user groups to the Members list.

7 Click *Save*.

8 To assign roles to the user, see Assigning Roles to Users and Groups.

19.2 Importing System User Groups from LDAP

Roles that Can Perform This Task: Cloud Administrator

The following steps explain how to create System user groups by importing information from your LDAP authentication source. For information about creating Organization user groups by manually entering information, see "Manually Creating System and Organization User Groups" on page 75.

An imported user group's membership is maintained in the LDAP authentication source. Any users who are members of the user group in the LDAP source receive the roles that are assigned to the user group in Cloud Manager.

An LDAP user group's members are not imported to Cloud Manager and do not display in the group's *Members* list. In addition, you cannot manually add users or user groups to an imported group.

1 On the main navigation bar, click *Configuration*.

2 Click the *Users* tab, click *Members*, then click *Import*.

3 Authenticate to the LDAP directory:

3a Click the *LDAP* tab.

3b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

3c In the *Search Bind Account* section, fill in the following fields:

User DN: Specify an account that has read rights to the directory location from which you want to import users. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Password Confirm: Confirm the password for the account.

3d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information and try again.

4 Import user groups:

4a Click the *Import* tab.

4b Click *Add*.

When you click *Add*, a new import entry is added to the list. You use the fields below the list to define the entry.

4c In the DN field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all user groups located within the container are imported. If you only want to import one user group, specify the DN of the user group object.

4d If you specified a container for import, select *Groups*.

4e If you specified a container for import, select *Scan Tree* if you want to import user groups located in its subcontainers.

4f Click *Import*.

The imported user groups are added to the *Members* list. User groups are identified by the  icon.

5 Click *Save* to close the System Configuration dialog box.

6 To assign roles to a user group, see Assigning Roles to Users and Groups.

19.3 Importing Organization User Groups from LDAP

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

The following steps explain how to create Organization user groups by importing information from your LDAP authentication source. For information about creating Organization user groups by manually entering information, see "Manually Creating System and Organization Users" on page 69.

An imported user group's membership is maintained in the LDAP authentication source. Any users who are members of the user group in the LDAP source receive the roles that are assigned to the user group in Cloud Manager.

An LDAP user group's members are not imported to Cloud Manager and do not display in the group's *Members* list. In addition, you cannot manually add users or user groups to an imported group.

1 On the main navigation bar, click  *Organizations*.

2 Click the *Organizations* tab, select the target organization for the import, click *Edit* to display the Edit Organization dialog box.

3 On the *Users* tab, click *Members*, then click *Import*.

4 Authenticate to the LDAP directory:

4a Click the *LDAP* tab.

4b In the *LDAP Location* section, fill in the following fields:

Host: Specify the FQDN (fully qualified domain name) or IP address of the host machine running the LDAP server. For example, `ldap.mycompany.com` or `123.45.67.8`.

Port: Specify the TCP port (on the host machine) where the LDAP server is listening for LDAP connections. The standard port for non-SSL connections is 389. The standard port for SSL connections is 636.

Use SSL: If the Cloud Manager Application Server is configured for an SSL connection to the LDAP server, select this option to enable the secure connection.

4c In the *Search Bind Account* section, fill in the following fields:

DN: Specify the distinguished name of an account that has search rights to the directory location from which you want to import users. For example, `cn=Administrator,cn=Users,dc=MyCompany,dc=com`

Password: Specify the password for the account.

Confirm Password: Confirm the password for the account.

4d Click *Test Connection*.

If the connection is successful, the Test Status is displayed as *Passed*. If the connection is not successful, validate the connection information and try again.

5 Import user groups:

5a Click the *Import* tab.

5b Click *Add*.

When you click *Add*, an new import entry is added to the list. You use the fields below the list to define the entry.

5c In the *DN* field, use standard LDAP notation (`ou=provo,dc=netiq,dc=com`) to specify the distinguished name for the target container or object, then click *Validate*.

If you specify a container, all user groups located within the container are imported. If you only want to import one user group, specify the DN of the user group object.

5d If you specified a container for import, select *Groups*.

5e If you specified a container for import, select *Scan Tree* if you want to import users located in its subcontainers.

5f Click *Import*.

The imported user groups are added to the *Members* list. User groups are identified by the  icon.

6 Assign roles to a user group.

An Organization user group can be assigned roles at the organization level, business group level, or business service level. If you want to assign an imported user group a role at the organization level, continue with the following steps. If you want to assign roles at the other two levels, exit the dialog box and see Assigning Roles to Users and Groups.

User groups must be given roles in order for group members to do anything in the organization. There are six roles that apply at the organization level: Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

Role assignments at the organization level are inherited by the organization's business groups. For example, if you give a group the Business Service Owner role for an organization, the group members can create business services for any business group in the organization. If you want to limit the user group to a role in specific business group, you must make the role assignment in the business group.

6a Click the role (*Approver*, *Build Administrator*, *Business Group Viewer*, *Business Service Owner, Organization Manager*, or *Sponsor*) that you want to assign to a user group.

6b Click *Add*.

Depending on the role that you are adding, the selection dialog box can contain two lists: *Members* and *System Users*. The *Members* list includes all members of the organization and the *System Users* list includes all Cloud Manager System users.

6c Select the user groups you want to add, then click *OK*.

You can Shift-click and Ctrl-click to select multiple groups.

7 Click *Save* to close the Edit Organization dialog box.

20 Assigning Roles to Users and Groups

Roles that Can Perform This Task: Cloud Administrator, Organization Manager (Organization users only)

System users and user groups can be assigned both system-level roles (Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator) and organization-level roles (Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor). Organization users can be assigned organization-level roles only.

For role descriptions, see Section 16.2, "Cloud Manager Roles," on page 61.

1. On the main navigation bar, click *Organizations*.
2. To assign a role to a user, click the *Users* tab, select the user, then click *Edit* to display the Edit User dialog box.

   or

   To assign a role to a user group, click the *User Groups* tab, select the user group, then click *Edit* to display the Edit User Group dialog box.
3. (System user or group only) Assign system-level roles.

   The system-level roles are Approver, Build Administrator, Catalog Manager, Cloud Administrator, and Zone Administrator. These roles can be assigned only to System users or groups.

   3a To assign the Approver, Build Administrator, Catalog Manager, or Cloud Administrator role, click the *System* tab, click *Add*, select the desired roles, then click *OK*.

   3b To assign the Zone Administrator role, click the *Zone* tab, click *Add*, select the desired zone, then click *OK*.
4. Assign organization-level roles.

   The organization-level roles are Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor. The Approver and Build Administrator roles can be assigned only to System users and groups. The other roles can be assigned to both System and Organization users and groups.

   Several of the roles can be assigned at the organization, business group, or business service level. For example, you can make a user a Sponsor for a business group, in which case the user can approve requests for business services from that business group only. Or, you can make the user a Sponsor for the organization, in which case the user can approve requests for all business services in the organization.

   4a Click the *Organization* tab to add a role at the organization level, click the *Business Group* tab to add a role at the business group level, or click the *Business Service* tab to add a role at the business service level.

   4b Click the role that you want to assign.

For example, if you selected the *Business Group* tab and you want to enable the user or group to create business services for the business group, click *Business Service Owner*.

4c Click *Add*, select the object (organization, business group, or business service) to which you want the role to apply, then click *OK* to add it to the list.

5 When you have finished assigning roles, click *Save* to save the role changes.

21 Deleting Users

Roles that Can Perform This Task: Cloud Administrator, Organization Manager (Organization users only)

When you delete a user, be aware of the following:

- The user's deployed business services remain deployed. Other users (Cloud Administrators, Business Service Owners, and so forth) who had access to the business services continue to have access. If the user was the sole owner of a business service, you can assign other users as owners of the business service, either before or after the user is deleted.
- The user's business service requests remain in progress. As with deployed business services, other users (Cloud Administrators, Business Service Owners, and so forth) who had access to the requests continue to have access. If the user was the sole owner of a business service request, you can assign other users as owners of the business service, either before or after the user is deleted.
- The user's claimed tasks must be released (unclaimed) or claimed by another user, either a Cloud Administrator or another user who has the same role as the deleted user. The tasks can be claimed before or after the user is deleted.

To delete a user:

1. On the main navigation bar, click *Organizations*.
2. Click the *Users* tab, select the user to delete, then click *Delete*.
3. Click *Yes* to confirm the deletion.

22 Deleting User Groups

Roles that Can Perform This Task: Cloud Administrator, Organization Manager (Organization user groups only)

When you delete a user group, the group members are not deleted, but they lose any roles that they inherited through membership in the group.

1. On the main navigation bar, click *Organizations*.
2. Click the *User Groups* tab, select the user group to delete, then click *Delete*.
3. Click *Yes* to confirm the deletion.

IV Catalog Management

The following sections provide information to help you manage the catalog of workload templates in your Cloud environment:

23 Workload Template Concepts

Workload templates are used to create the workloads for business services. The following sections provide information you should understand as you create and manage workload templates:

23.1 Workload Template Components

A workload template consists of the following:

- **Template name:** This is the display name that Business Service Owners see when selecting from the list of workload templates. You should use a naming scheme that makes sense to the users who will consume the template.
- **Costs:** You can add one-time setup costs and monthly software license costs to the template. The costs are applied to all workloads created from the template.
- **VM template:** This is the VM template that is used to create the workloads. It is located in one of the Cloud Manager Orchestration repositories.
- **Custom VM template settings:** The VM template includes default resource settings for CPUs, memory, networks (NICs), and disk space. You can increase or decrease the settings to customize the workload template. For example, if the VM template is configured with one CPU, you can increase the CPU setting to two CPUs. When a workload is created from the workload template, the resulting VM is configured with two CPUs rather than one.
- **Windows or Linux settings:** If the VM template’s operating system is Windows, the template includes Windows settings. If the operating system is Linux, the template includes Linux settings. You can pre-populate any settings that you want to be the same for all workloads created from the template. For example, if you want all workloads to use the same password for the local Administrator account, you could pre-populate that setting. See the next section, “Pre-Populated Template Settings” on page 90.
- **Associations:** (Optional) After they are created, you can associate the workload template with one or more business groups or organizations.

23.2 Pre-Populated Template Settings

When a Windows-based workload is created from a template, certain Windows settings, such as the computer name, the domain or workgroup, and the Windows product key, must be supplied. Likewise, when a Linux-based workload is created from a template, certain Linux settings, such as the host name, must be supplied.

If there are settings that will be the same for all workloads created from a template, you can pre-populate those settings. For example, if you want all Windows workloads to use the same password for the local Administrator account, you can provide that password in the template.

Any settings that you do not pre-populate must be filled in when requesting a new business service (by the Business Service Owner) or when performing the pre-build configuration (by a Cloud Administrator or a Build Administrator).

23.3 Workload Template Changes

You can change workload template settings at any time, even if the template has been used to create workloads. The only restriction is that you cannot specify a different VM template if the workload template is in use by a requested or deployed workload.

Changing a workload template has no immediate effect on deployed workloads. However, if a change is requested for a deployed workload, the workload settings are validated against the new workload template settings. This might require the Business Service Owner to change settings that he or she did not plan to change. For example, suppose that you create a workload template that allocates 4 CPUs. A Business Service Owner creates a workload (with 4 CPUs) from the workload template. You then change the workload template's CPU allocation from 4 to 2. After the change, the Business Service Owner requests a change to the workload's number of disks. When creating the change request, the Business Service Owner must also change the CPUs from 4 to 2 because 4 CPUs are no longer supported by the new workload template.

23.4 VM Template Changes

VM templates are managed (created, changed, and deleted) through the Cloud Manager Orchestration Server console. If you change a VM template that is referenced by a workload template, the change is not recognized for the workload template unless you open the workload template in Edit mode and then save it again. You do not need to change any workload template settings, you only need to save the template again.

23.5 Workload Template Deletions

You can delete a workload template unless it is currently being used to build a workload. As soon as the workload is built and deployed, you can delete the workload template.

Deleting a workload template has no effect on deployed workloads, even if the Business Service Owner of one of the workloads requests a change to it.

23.6 Catalog Manager Role

As a Cloud Administrator, you have full rights to the Cloud Manager system. This includes creating, editing, and deleting workload templates. However, you might decide that you want the person who creates your VM templates on the Cloud Manager Orchestration Server or in the hypervisor tools to also be the person who creates your Cloud Manager workload templates.

To facilitate the delegation of workload template responsibilities, Cloud Manager includes a System role called Catalog Manager. A Catalog Manager has rights only to create, modify, and delete workload templates. The Catalog Manager can't see anything else (organizations, business services, resources, reports, and so forth) in the Cloud Manager console. Because of this, you (or other Cloud Administrators) must assign workload templates to organizations; the Catalog Manager cannot make template assignments.

24 Creating Workload Templates

Roles that Can Perform This Task: Cloud Administrator, Catalog Manager

Workload templates are used to create the workloads for requested business services.

1. On the main navigation bar, click *Catalog*.
2. On the *Workload Templates* tab, click *Create*.
3. If your Cloud Manager system has multiple zones, the Select Zone dialog box is displayed. Select the zone that contains the VM template you want, then click *OK* to display the Create Workload Template dialog box.
4. In the *General* section, provide the following information for the workload template:

   Name: Specify a unique name for the workload template. Business Services owners see this name when selecting the workload templates they use to create their business services.

   You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Setup Cost: Specify the cost associated with setting up the workload. This is a one-time fee.

   License Cost: Specify the license costs associated with the workload's software. This cost is per month.

   Zone: Displays the zone you selected for the workload template. You cannot change this setting.

   Creation Date: Displays the current date. You cannot change this setting.

   Description: Provide any additional information to identify the workload template.
5. In the *Virtual Machine Settings* section:

   5a In the *VM Template* list, select a VM template.

   After you select a VM template, the template's operating system and hypervisor information is displayed. You cannot change these settings.

   The VM template's resource information (CPUs, memory, network interface cards, and disks) is also displayed. You can customize this information as necessary.

   5b Customize the settings to increase or decrease the workload resources:

   Number of CPUs: Select the number of CPUs for the workload. Some hypervisor technologies do not support more than 8 CPUs per workload, so the maximum number allowed is 8.

   Memory: Select the megabytes (MB) of RAM to allocate to the workload.

   Number of NICs: Select the number of network interface cards (NICs) to allocate to the workload.

Disks Summary: Displays the size of the mandatory workload disks and the number of optional workload disks defined in the template, Mandatory workload disks are always created. They are inherited from the VM template or manually defined on the *Disks* tab. Optional workload disks are available to the user but are created only if the user specifies sizes for the disks.

You add disks on the Disks page (see Step 6 below) and the disk information is then displayed in these fields.

5c By default, each resource setting is unlocked, which means that a business service requestor can change it when creating a workload from the template. If you want to prevent a user from changing a setting, select the  check box.

6 If you want to add disks to the workload template, or if you want to specify whether or not the current disks should be included when calculating the cost of the workload:

6a Click the *Disks* tab.

The template can include up to 10 additional disks.

6b Click *Add* to add a disk to the list.

6c Make sure the disk is selected in the list, then specify a size (in the *Size* field below the list) to make the disk mandatory.

or

Leave the capacity set to 0 to make the disk optional.

The maximum size per disk is 1024 GB (1 TB). If you specify the size when adding a disk, the disk becomes mandatory. Users cannot remove or change a mandatory disk. If you add a disk with size set to 0, the disk becomes optional. Users can leave the size at 0, in which case the disk is not created with the workload, or they can specify a size and create the disk.

6d In the *Cost* field, select the check box if you want to include the cost of the disk in the workload's total cost.

If you don't enable the Cost option, the disk becomes a free disk and is not included when calculating the cost of the workload.

7 If the template is a Windows-based template and you want to pre-populate some of the Windows settings, click *Windows Settings*, then complete the following steps.

You might not want to pre-populate some settings, such as *Computer Name*, if the template will be used to create multiple workloads. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the Business Service Owner) or when performing the pre-build configuration (by an administrator).

7a Configure the *Domain Settings*:

Computer Name: Specify the computer name for the virtual machine.

Domain or Workgroup: Select *Domain* or *Workgroup*, then specify the name of the domain or workgroup to which you want the virtual machine added.

Domain Administrator User ID: This applies only if you are adding the virtual machine to a domain. Specify a domain administrator user ID that can be used to add the virtual machine to the domain specified in the *Domain* field.

7b Modify the *Installation Settings*:

Run Once Commands: Specify any Windows RunOnce commands that you want run during the first log in to the virtual machine. For information about Windows RunOnce commands, see the Microsoft Windows documentation.

8 If the template is a Windows-based template and you want to pre-populate some of the Windows licensing information, click *Windows Licensing* and fill in the fields., then click *OK*.

Windows Product Key: Specify the product key for the workload's Windows operating system.

If you pre-populate this field in the template, the data is masked from users and cannot be copied.

Registered to Name: Specify an individual, department, company or so forth to whom the Windows operating system software is registered.

You might not want to pre-populate some settings, such as *Windows Product Key*, if the template will be used to create multiple workloads and the key does not cover multiple installations. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the Business Service Owner) or when performing the pre-build configuration (by an administrator).

9 If the template is a Linux-based template and you want to pre-populate some of the Linux settings, click *Linux Settings* and fill in the fields., then click *OK*.

Hostname: Specify the host name for the workload

Domain Name: Specify the domain for the workload (for example, netiq.com or provo.netiq.com).

You might not want to pre-populate some settings, such as *Hostname*, if the template will be used to create multiple workloads. Any settings that you do not pre-populate must be filled in when requesting a new business service (by the Business Service Owner) or when performing the pre-build configuration (by an administrator).

10 (Optional) If you have already created organizations and resource groups that support workload templates, you can associate the workload template with the organizations and business groups of your choice, but you must choose an organization whose resource groups support the type of hypervisor (and VM template) compatible with the workload template.

10a Click *Associations*, then select either the *Organizations* tab or the *Business Groups* tab to open a list.

10b Select (that is, click) the organization or business group you want to associate with this workload template, then click *OK*.

or

Select (that is, Ctrl+click) the organizations or business groups you want to associate with this workload template, then click *OK*.

NOTE: The Workload Templates list displays only the workload templates from the organization where your business group resides. You must assign workload templates at the organization level before they become available for selection at the business group level.

---

25 Assigning Workload Templates to Organizations and Business Groups

The workload template catalog is not directly available to organizations. Any workload templates you want available to an organization must be assigned to the organization. After a workload template is assigned to an organization, you can then make it available for use in all or some of the organization's business groups.

25.1 Assigning Workload Templates to an Organization

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Organizations*.
2. In the *Organizations* list, select the target organization, then click *Edit*.
3. Click the *Workload Templates* tab.
4. Click *Add* to display the Add Workload Templates dialog box, select the workload templates to be added, then click *OK*.

   You can Shift-click or Ctrl-click to select multiple workload templates.
5. When you have finished adding templates, click *Save* to save the changes to the organization.

25.2 Assigning Workload Templates to a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

A business group does not automatically inherit the workload templates assigned to its organization. Any of the organization's workload templates that you want available to the business group must be assigned to it.

1. On the main navigation bar, click *Organizations*, then click the *Business Groups* tab.
2. In the *Business Groups* list, select the target business group, then click *Edit*.
3. Click the *Workload Templates* tab.

4 Click *Add* to display the Add Workload Templates dialog box, select the workload templates to be added, then click *OK*.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished adding templates, click *Save* to save the changes to the business group.

25.3 Removing Workload Template Assignments from an Organization

Roles that Can Perform This Task: Cloud Administrator

You can remove a workload template from an organization unless it is currently being used to build a workload for one of the organization's business groups. As soon as the workload is built and deployed, you can remove the workload template.

Removing a workload template assignment from an organization also removes any assignments from its business groups.

1 On the main navigation bar, click *Organizations*.

2 In the *Organizations* list, select the organization from which you want to remove the workload template assignment, then click *Edit*.

3 Click the *Workload Templates* tab.

4 Select the workload template to be removed, click *Remove*, then click *Yes* to confirm the template removal.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished removing templates, click *Save* to save the changes to the organization.

25.4 Removing Workload Template Assignments from a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

You can remove a workload template from a business group unless it is currently being used to build a workload for the business group. As soon as the workload is built and deployed, you can remove the workload template.

1 On the main navigation bar, click *Organizations*.

2 Click the *Business Groups* tab, select the business group from which you want to remove the workload template assignment, then click *Edit*.

3 Click the *Workload Templates* tab.

4 Select the workload template to be removed, click *Remove*, then click *Yes* to confirm the template removal.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished removing templates, click *Save* to save the changes to the business group.

26 Modifying Workload Templates

Roles that Can Perform This Task: Cloud Administrator, Catalog Manager

You can change workload template settings at any time, even if the template has been used to create workloads. The only restriction is that you cannot specify a different VM template if the workload template is in use by a requested or deployed business service.

Changing a workload template has no immediate effect on deployed workloads. However, if a change is requested for a deployed workload, the workload settings are validated against the new workload template settings. This might require the Business Service Owner to change settings that he or she did not plan to change. For example, suppose that you create a workload template that allocates 4 CPUs. A Business Service Owner creates a workload (with 4 CPUs) from the workload template. You then change the workload template's CPU allocation from 4 to 2. After the change, the Business Service Owner requests a change to the workload's number of disks. When creating the change request, the Business Service Owner is also required to change the CPUs from 4 to 2 because 4 CPUs are no longer supported by the new workload template.

1. On the main navigation bar, click *Catalog*.
2. On the *Workload Templates* tab, select the template to modify, then click *Edit*.
3. Make the desired changes to the template, then click *OK* to save the changes.

   For a description of the workload template settings, see "Creating Workload Templates" on page 93 or click the icon in the Edit Workload Template dialog box.

27 Deleting Workload Templates

Roles that Can Perform This Task: Cloud Administrator, Catalog Manager

You can delete a workload template unless it is currently being used to build a workload. As soon as the workload is built and deployed, you can delete the workload template.

Deleting a workload template has no effect on deployed workloads, even if the Business Service Owner of one of the workloads requests a change to it.

1. On the main navigation bar, click  *Catalog.*
2. On the *Workload Templates* tab, select the template to delete, then click *Delete*.
3. Confirm the deletion.

V Organization Management

The following sections provide information to help you manage the organizations in your Cloud environment:

28 Creating Organizations

Roles that Can Perform This Task: Cloud Administrator

An organization represents a tenant to which you are offering Cloud services. Through the organization, you make resource group assignments that dictate the hosts, service levels, repositories, and networks available to the organization, and make workload template assignments that determine the types of business service workloads available to the organization.

After you create an organization, you (or an Organization Manager) can define the organization's membership and assign roles such as Business Service Owner, Business Group Sponsor, and Organization Manager to those members. Membership and role assignments are covered in the next task, *Create Users and Groups*.

1. On the main navigation bar, click *Organizations,* click the *Organizations* tab, then click *Create*.
2. Provide the following details to define the organization:

   Name: Specify a unique name for the organization. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Description: Provide any additional information to identify the organization.

   Domains: If you want to enable users to self-register in this organization, specify the e-mail domains associated with the organization.

   Self-registration occurs when a valid LDAP user who does not have a Cloud Manager account first logs in. The user's e-mail domain is compared to the e-mail domains defined for the organization. If it matches one of the e-mail domains, the user is added to organization's Members list.

   You can associate one or more e-mail domains with the organization. To specify multiple e-mail domains, separate the names with commas (for example, `netiq.com,novell.com,attachmate.com`).

   Discount %: If you want a discount applied to all business services created by members of this organization, specify the discount percentage.

   Auto Approval: When a user creates a business service request, the request goes through an approval workflow that includes both a Sponsor and an Administrator. The Sponsor is a member of the organization who provides the financial approval for the business service. The Administrator is a System user (such as yourself, another Cloud Administrator, or a Zone Administrator) who provides the resource capacity approval for the business service. You can use Auto Approval to bypass one or both of the approvals.

   The organization inherits the Auto Approval settings from the Cloud Manager system settings (accessed through *Configuration* on the main navigation bar). To change the settings for the organization, click *Override*, then configure the settings as desired.

Logo: You can upload a logo file for the organization. Three formats are supported: PNG, JPG, and GIF. Any size is acceptable. Cloud Manager resizes the logo to a maximum of 216x216 pixels, maintaining the width-to-height proportions. For example, a 432x200 image would be resized to 216x100. The logo file is stored on the Cloud Manager Application Server.

To upload a file, mouse over *No Image*, then click *Upload New Image*. Browse for and select the image, then click *OK* to upload it to the Cloud Manager Application Server.

3 Add the workload templates that you want the organization to have access to.

You do not need to assign workload templates to the organization at this time. If you want to do it later, see Section 25.1, "Assigning Workload Templates to an Organization," on page 97 when you are ready.

3a Under *Membership and Access*, click the *Workload Templates* tab.

3b Click *Add* to display the Add Workload Templates dialog box.

3c Select the workload templates.

You can Shift-click and Ctrl-click to select multiple workload templates.

3d Click *OK* to add the selected workload templates to the *Workload Templates* list.

4 Add the resource groups that you want the organization to have access to.

You do not need to assign resource groups to the organization at this time. If you want to do it later, see Section 38.1, "Assigning Resource Groups to an Organization," on page 137 when you are ready.

4a Under *Membership and Access*, click the *Resource Groups* tab.

4b Click *Add* to display the Add Resource Groups dialog box.

4c Select the resource groups you want to add.

You can Shift-click and Ctrl-click to select multiple groups.

4d Click *OK* to add the selected resource groups to the *Resource Groups* list.

5 Add the networks that you want the organization to have access to.

The available networks are determined by the VM hosts included in the resources groups. However, to enable you to provide isolated networks for two or more organizations that share the same resource group, the networks from a resource group are not automatically assigned to an organization when you add the resource group. Instead, you must separately add the networks you want assigned to the organization.

5a Under *Membership and Access*, click the *Networks* tab.

5b Click *Add* to display the Add Networks dialog box.

5c Select the networks.

You can Shift-click and Ctrl-click to select multiple networks.

5d Click *OK* to add the selected networks to the *Networks* list.

6 Add organization members.

6a Click *Save* to create the organization.

You can only add users after the organization has been saved.

6b Refer to "Manually Creating System and Organization Users" on page 69 for details about creating users and adding them to an organization. Or refer to "Importing Organization Users from LDAP" on page 71 for details about importing users from an LDAP source into the organization.

7 Assign roles for the organization.

Users must be given roles in order to do anything in the organization. There are six roles that apply to an organization: Approver, Build Administrator, Business Group Viewer, Business Service Owner, Organization Manager, and Sponsor.

Role assignments at the organization level are inherited by the organization's business groups. For example, if you give a user the Business Service Owner role for an organization, the user can create business services for any business group in the organization. If you want to limit the user to a role in specific business group, you must make the role assignment in the business group.

7a Click the *Users* tab, then click the role (*Approver*, *Build Administrator*, *Business Group Viewer*, *Business Service Owner*, *Organization Manager*, or *Sponsor*) that you want to assign to a user.

7b Click *Add*.

Depending on the role that you are adding, the selection dialog box can contain two lists: *Members* and *System Users*. The *Members* list includes all members of the organization and the *System Users* list includes all Cloud Manager System users.

7c Select the users you want to add, then click *OK*.

You can Shift-click and Ctrl-click to select multiple users.

8 Click *Save* to add the organization to the *Organizations* list.

29 Customizing Organization Configuration Settings

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

The Organization Configuration settings determine if organization members can see all workload costs and settings when creating and managing business services.

To customize the settings:

1. On the main navigation bar, click *Organizations*.
2. On the *Organizations* tab, select the target organization, then click *Edit*.
3. In the upper-right corner of the dialog box, click the icon to display the Organization Configuration dialog box.
4. Configure the following settings:

   Organization Costs: Select whether the organization's business service costs are hidden from or shown to the organization's members. This applies to all Organization members regardless of their assigned roles.

   You can override this setting on a business group. For example, if you show business service costs for the organization, you can hide costs for a specific business groups. Organization users can see the costs associated with all of the organization's business services with the exception of business services created by the one business group.

   In some cases, you might want to hide costs from some users but not from others. To achieve this, you can hide the costs at the organization or business group level, but then enable the *Always show costs* option on the individual user accounts.

   Workload Dialog: A workload contains *Windows Settings*, *Windows Licensing*, *Linux Settings*, and *Networks* tabs that must be configured when requesting a business service. These tabs can be hidden, in which case a Build Administrator or Cloud Administrator must provide the information when completing the pre-build configuration tasks for the business service.

   The organization inherits the Workload Dialog settings configured at the system level. If you want to override the system settings to apply different settings for the organization, select *Override System Setting*, then enable or disable the tabs as desired.

   To revert the settings to the system settings, deselect *Override System Setting*.
5. Click *OK*.

30 Creating Business Groups

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

A business group represents a unit within an organization, such as a department or cost center, with which business services are associated. An organization can have one or more business groups.

A business group can be assigned all of an organization's resources or only some of the resources. When a business service is created for a business group, it uses only the assigned resources. Multiple business groups can be assigned the same resources, which means that the resources become shared resources.

1. On the main navigation bar, click *Organizations*.
2. Click the *Business Groups* tab, then click *Create*.
3. Provide the following details to define the business group:

   Name: Specify a name for the group. The name should be different than any other business group name.

   Organization: Select the organization for the business group. The organization assignment cannot be changed after the business group is created.

   Description: Provide any additional information to identify the business group.

   Auto Approval: Business service requests require both a Sponsor approval and an Administrator approval. The Sponsor approval is a financial check, while the Administrator approval is a resource capacity check. You can use Auto Approval to bypass one or both of the approvals.

   Sponsor is selected by default. If you don't want automatic Sponsor approval, you must add sponsors to the group (see Step 4).

   Select *Administrator* to automatically grant Administrator approval for the group's business services.

   Costs: The business group inherits the *Costs* setting from its organization. To change the setting for the business group, click *Override*, then configure the setting as desired. *Show* allows group members to see cost information for workloads. *Hide* to prevent group members from seeing cost information.
4. Assign roles for the business group.

   There are three roles that apply to a business group: Business Group Viewer, Business Service Owner, and Sponsor. By default, users assigned these roles at the organization also have these same roles in the business group.

   4a Click the *Users* tab, then click the role (*Business Group Viewer*, *Business Service Owner,* or *Sponsor*) that you want to assign to a user.

   4b Click *Add*.

Depending on the role that you are adding, the selection dialog box can contain two lists: *Members* and *System Users*. The *Members* list includes all members of the organization and the *System Users* list includes all Cloud Manager System users.

4c Select the users you want to add, then click *OK*.

You can Shift-click and Ctrl-click to select multiple users.

5 Add the workload templates that you want the business group to have access to.

You do not need to assign workload templates to the business group at this time. If you want to do it later, see Section 25.2, "Assigning Workload Templates to a Business Group," on page 97 when you are ready.

5a Under *Membership and Access*, click the *Workload Templates* tab.

5b Click *Add* to display the Add Workload Templates dialog box.

The list displays the organization's workload templates. A business group is limited to the workload templates assigned to its organization.

5c Select the workload templates.

You can Shift-click and Ctrl-click to select multiple workload templates.

5d Click *OK* to add the selected workload templates to the *Workload Templates* list.

6 Add the resource groups you want the business group to have access to.

You do not need to assign resource groups to the organization at this time. If you want to do it later, see Section 38.2, "Assigning Resource Groups to a Business Group," on page 138 when you are ready.

6a Under *Membership and Access*, click the *Resource Groups* tab.

6b Click *Add* to display the Add Resource Groups dialog box.

The list displays the organization's resource groups. A business group is limited to the resource groups assigned to its organization.

6c Select the resource groups you want to add.

You can Shift-click and Ctrl-click to select multiple resource groups.

6d Click *OK* to add the selected resource groups to the *Resource Groups* list.

7 Add the networks that you want the business group to have access to.

The available networks are determined by the VM hosts included in the resource groups. However, to enable you to provide isolated networks for business groups that share the same resource group, the networks from a resource group are not automatically assigned to a business group when you add the resource group. Instead, you must separately add the networks you want assigned to the business group.

7a Under *Membership and Access*, click the *Networks* tab.

7b Click *Add* to display the Add Networks dialog box.

7c Select the networks.

You can Shift-click and Ctrl-click to select multiple networks.

7d Click *OK* to add the selected networks to the *Networks* list.

8 Click *Save*.

31 Assigning Resource Groups to Organizations and Business Groups

Resource groups must be assigned to an organization in order for the organization's business services to use those resources. After you assign resource groups to an organization, you or the Organization Manager can make them available to business groups within the organization.

The following steps assume that the resource groups you want to assign already exist. If they do not, see "Creating, Modifying, and Deleting Resource Groups" on page 125.

31.1 Assigning Resource Groups to an Organization

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Organizations*.
2. On the *Organizations* tab, select the target organization, then click *Edit*.
3. Add the resource groups you want the organization to have access to:
   - **3a** Under *Membership and Access*, click the *Resource Groups* tab.
   - **3b** Click *Add* to display the Add Resource Groups dialog box.
   - **3c** Select the resource groups to add.

     You can Shift-click and Ctrl-click to select multiple groups.
   - **3d** Click *OK* to add the selected resource groups to the *Resource Groups* list.
4. Add the networks that you want the organization to have access to.

   The resource group's networks are determined by its VM hosts. To enable you to provide isolated networks for organizations that share the same resource group, the networks are not automatically added when you add the resource group. You must explicitly add the networks you want assigned to the organization.
   - **4a** Under *Membership and Access*, click the *Networks* tab.
   - **4b** Click *Add* to display the Add Networks dialog box.
   - **4c** Select the networks to add.

You can Shift-click and Ctrl-click to select multiple networks.

4d Click *OK* to add the selected networks to the *Networks* list.

5 When you have finished adding resource groups, click *Save* to save the changes.

31.2 Assigning Resource Groups to a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

A business group does not automatically inherit the resource groups assigned to its organization. Any of the organization's resource groups that you want to be available to the business group must be assigned to it.

1 On the main navigation bar, click *Organizations*, then click the *Business Groups* tab.

2 In the *Business Groups* list, select the target business group, then click *Edit*.

3 Add the resource groups you want the business group to have access to:

3a Under *Membership and Access*, click the *Resource Groups* tab.

3b Click *Add* to display the Add Resource Groups dialog box.

3c Select the resource groups to add.

You can Shift-click and Ctrl-click to select multiple groups.

3d Click *OK* to add the selected resource groups to the *Resource Groups* list.

4 Add the networks that you want the business group to have access to.

The resource group's networks are determined by its VM hosts. To enable you to provide isolated networks for business groups that share the same resource group, the networks are not automatically added when you add the resource group. You must explicitly add the networks you want assigned to the business group.

4a Under *Membership and Access*, click the *Networks* tab.

4b Click *Add* to display the Add Networks dialog box.

4c Select the networks to add.

You can Shift-click and Ctrl-click to select multiple networks.

4d Click *OK* to add the selected networks to the *Networks* list.

5 When you have finished adding resource groups, click *Save* to save the changes to the business group.

31.3 Removing Resource Group Assignments from an Organization

Roles that Can Perform This Task: Cloud Administrator

You can remove a resource group from an organization only if the resource group is not hosting any deployed business services from the organization's business groups.

Removing a resource group assignment from an organization also removes any assignments from its business groups.

1. On the main navigation bar, click *Organizations*.
2. In the *Organizations* list, select the organization from which you want to remove the resource group assignment, then click *Edit*.
3. Click the *Resource Groups* tab.
4. Select the resource group to be removed, click *Remove*, then click *Yes* to confirm the removal.

   You can Shift-click or Ctrl-click to select multiple resource groups.
5. When you have finished removing resource groups, click *Save* to save the changes to the organization.

31.4 Removing Resource Group Assignments from a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

You can remove a resource group from a business group only if the resource group is not hosting any of the business group's deployed business services.

1. On the main navigation bar, click *Organizations*.
2. Click the *Business Groups* tab, select the business group from which you want to remove the resource group assignment, then click *Edit*.
3. Click the *Resource Groups* tab.
4. Select the resource group to be removed, click *Remove*, then click *Yes* to confirm the removal.

   You can Shift-click or Ctrl-click to select multiple resource groups.
5. When you have finished removing resource groups, click *Save* to save the changes to the business group.

32 Assigning Workload Templates to Organizations and Business Groups

The workload template catalog is not directly available to organizations. Any workload templates you want to be available to an organization must be assigned to the organization. After a workload template is assigned to an organization, you can then make it available for use in all or some of the organization's business groups.

32.1 Assigning Workload Templates to an Organization

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Organizations*.
2. In the *Organizations* list, select the target organization, then click *Edit*.
3. Click the *Workload Templates* tab.
4. Click *Add* to display the Add Workload Templates dialog box, select the workload templates to be added, then click *OK*.

   You can Shift-click or Ctrl-click to select multiple workload templates.
5. When you have finished adding templates, click *Save* to save the changes to the organization.

32.2 Assigning Workload Templates to a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

A business group does not automatically inherit the workload templates assigned to its organization. Any of the organization's workload templates that you want to be available to the business group must be assigned to it.

1. On the main navigation bar, click *Organizations*, then click the *Business Groups* tab.
2. In the *Business Groups* list, select the target business group, then click *Edit*.
3. Click the *Workload Templates* tab.

4 Click *Add* to display the Add Workload Templates dialog box, select the workload templates to be added, then click *OK*.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished adding templates, click *Save* to save the changes to the business group.

32.3 Removing Workload Template Assignments from an Organization

Roles that Can Perform This Task: Cloud Administrator

You can remove a workload template from an organization unless it is currently being used to build a workload for one of the organization's business groups. As soon as the workload is built and deployed, you can remove the workload template.

Removing a workload template assignment from an organization also removes any assignments from its business groups.

1 On the main navigation bar, click *Organizations*.

2 In the *Organizations* list, select the organization from which you want to remove the workload template assignment, then click *Edit*.

3 Click the *Workload Templates* tab.

4 Select the workload template to be removed, click *Remove*, then click *Yes* to confirm the template removal.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished removing templates, click *Save* to save the changes to the organization.

32.4 Removing Workload Template Assignments from a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

You can remove a workload template from a business group unless it is currently being used to build a workload for the business group. As soon as the workload is built and deployed, you can remove the workload template.

1 On the main navigation bar, click *Organizations*.

2 Click the *Business Groups* tab, select the business group from which you want to remove the workload template assignment, then click *Edit*.

3 Click the *Workload Templates* tab.

4 Select the workload template to be removed, click *Remove*, then click *Yes* to confirm the template removal.

   You can Shift-click or Ctrl-click to select multiple workload templates.

5 When you have finished removing templates, click *Save* to save the changes to the business group.

33 Managing Organization Users, User Groups, and Roles

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

You can add users and user groups to an organization and then assign roles to the users and groups so that they can perform specific functions within the organization.

Users, user groups, and roles are covered in Part III, “User Management,” on page 59.

VI Resource Management

The following sections provide information to help you manage the resources in your Cloud environment:

34 Resource Group Concepts

A resource group defines a set of VM hosts that an organization can use for its business services. In addition to the VM hosts, the resource group includes one or more service levels that define the cost of the host resources (vCPUs, memory, storage, and networks) and the service objectives (availability, support response time, and so forth).

34.1 VM Host Recommendations

All VM hosts that you include in a resource group should be identical in terms of hypervisor technology, operating system version, network configuration, storage repository configuration, and hardware capabilities. This ensures a consistent environment for business services regardless of the host. It also ensures that the resource group’s service levels apply to all hosts.

34.2 Shared and Dedicated Resource Groups

A resource group can be shared among multiple organizations, which means that each organization’s business services utilize the same resources, or a resource group can be assigned to only one organization, in which case only that organization’s business services consume the resources.

34.3 Service Levels

A resource group identifies a collection of VM hosts to which workloads can be deployed. However, a resource group does not includes any costs associated with running workloads on the hosts. A resource group also does not include any service objectives for the workloads (such as host availability or support response time). The resource costs and service objectives are applied to resource groups through the use of service levels.

A service level defines the monthly cost for each type of host resource (vCPUs, memory, storage, and networks). For example, you might set the cost of one vCPU at $25 per month. If a workload requires two vCPUs, $50 is added to the monthly cost of the workload.

A service level can also include service objectives. Objectives typically define measurable behaviors such as host availability (uptime) or support response time and have a cost associated with them. Any service objective costs are added to the monthly cost of a workload that is deployed in the resource group.

A service level can be assigned to multiple resource groups. For example, two identical resource groups might require the same service level.

Multiple service levels can also be assigned to a single resource group. For example, two service levels might have the same host resource costs but different service support levels - the first with 24x7x365 support and the second with 12x5x365 support. The user, when requesting a business service, could select the service level with the desired support level.

34.4 Examples

As an example, you might create a Business Critical resource group that consists of high-performance hosts intended for mission critical applications and services. You assign the resource group a Platinum service level with costs that reflect the more expensive hardware and service contract. Any business service that is provisioned to the resource group's hosts automatically inherits the resource and service costs.

Or, you might create a Lab resource group that consists of standard-performance hosts intended for software testing. You assign the resource group a Bronze service level with costs that reflect the less expensive hardware and service contract.

35 Creating, Modifying, and Deleting Resource Groups

A resource group defines a set of VM hosts that an organization can use for its business services. In addition to the VM hosts, the resource group includes one or more service levels that define the cost of the host resources (vCPUs, memory, storage, and networks) and the service objectives (availability, support response time, and so forth).

35.1 Creating Resource Groups

Roles that Can Perform This Task: Cloud Administrator, Zone Administrator (create resource groups and add hosts only; cannot add service levels or assign resource groups to organizations)

1. On the main navigation bar, click  *Resources*.
2. Click the *Resource Groups* tab, then click *Create*.
3. If you are the Zone Administrator for multiple zones, the Select Zone dialog box is displayed. Select the zone that contains the resources you are grouping, then click *OK* to display the Create Resource Group dialog box.
4. In the *General* fields, provide the following information for the resource group:

   Name: Specify a unique name for the group. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Zone: Displays the zone whose hosts you can add to the group. You cannot change this setting.

   Hypervisor: Select the hypervisor technology for the group’s hosts. You can add only those hosts that meet the hypervisor criteria.

   Workload Repository: The *Default* setting causes a provisioned workload to be stored in the same repository as the VM template used to create it. If you want workloads provisioned to this resource group to be stored in a different shared repository, you must add hosts to the group (see Step 5), then come back and select the shared repository for the workloads. The *Workload Repository* list is populated only after you add hosts to the resource group.

   Group Type: This applies only if VMware vSphere is the selected hypervisor. Select *Host* if you want the resource group to use hosts and host clusters. Select *Resource Pool* if you want the resource group to use a resource pool.

   Resource Pool: If you specified *Resource Pool* as the group type, select the resource pool to include in the group.

Description: Provide any additional information for the resource group.

5 If the group type is *Host*, add hosts to the group:

5a Under *Associations*, click the *Hosts* tab.

5b Click *Add* to display the Add Hosts dialog box.

The list displays all available hosts and host clusters in the zone that meet the selected hypervisor criteria. Hosts that are already assigned to another resource group are not displayed.

5c Select the hosts.

You can Shift-click and Ctrl-click to select multiple hosts.

5d Click *OK* to add the selected hosts to the *Hosts* list.

6 Add service levels to the group:

6a Under *Associations*, click the *Service Level* tab.

6b Click *Add* to display the Add Service Levels dialog box.

6c Select the service levels.

You can Shift-click and Ctrl-click to select multiple service levels.

6d Click *OK* to add the selected service levels to the *Service Levels* list.

7 Ignore the *Networks* tab.

The *Networks* tab shows the networks associated with the hosts you added to the group. The list is view-only so you can't make any changes. However, the list is not generated until you save the resource group. If you want to see the networks at this time, click *Save*, double-click the resource group to open it again, then click the *Networks* tab.

8 Specify the organizations that can use the resource group:

8a Under *Associations*, click the *Organizations* tab.

8b Click *Add* to display the Add Organizations dialog box.

8c Select the organizations to which you want to assign the resource group.

You can Shift-click and Ctrl-click to select multiple hosts.

8d Click *OK* to add the selected organizations to the *Organizations* list.

IMPORTANT: The resource group is added to the organization, but its networks are not made available to the organization. To make the networks available, edit the organization and add the resource group's networks to the *Networks* list.

9 Click *Save*.

35.2 Modifying Resource Groups

Roles that Can Perform This Task: Cloud Administrator, Zone Administrator (add and remove hosts only)

You can modify a resource group to add or remove hosts, to add or remove service levels, and to change the organization assignments.

Be aware of the following when you remove hosts and service levels from a resource group and a resource group from an organization:

- You can remove a host at any time. Any business service workloads running on the host continue to run until they are cycled (stopped, then started) in the Cloud Manager console. At that point, they are moved to another host in the resource group.
- You cannot remove a service level if it is associated with a business service that is deployed to the resource group.
- You cannot remove a resource group assignment from an organization if the organization has business services deployed to the resource group. In addition, removing a resource group assignment from an organization also removes any assignments from its business groups.

To modify a resource group:

1. On the main navigation bar, click  *Resources*.
2. Click the *Resource Groups* tab, select the resource group you want to modify, then click *Edit*.
3. Make the desired changes to the resource group, then click *OK* to save the changes.

   For a description of the resource group settings, see "Creating, Modifying, and Deleting Resource Groups" on page 125 or click the  icon in the Edit Resource Group dialog box.

35.3 Deleting Resource Groups

Roles that Can Perform This Task: Cloud Administrator, Zone Administrator

You can delete a resource group only if the resource group is not hosting any deployed business services.

1. On the main navigation bar, click  *Resources*.
2. On the *Resource Groups* tab, select the resource group to delete, then click *Delete*.

   If the *Delete* action is not available, the resource group is hosting deployed business services and cannot be deleted.
3. Click *Yes* to confirm the deletion.

36 Creating, Modifying, and Deleting Service Levels

A service level defines the monthly cost for each type of host resource (vCPUs, memory, storage, and networks). For example, you might set the cost of one vCPU at $25 per month. If a workload requires two vCPUs, $50 is added to the monthly cost of the workload.

A service level can also include service objectives. Objectives typically define measurable behaviors such as host availability (uptime) or support response time and have a cost associated with them. Any service objective costs are added to the monthly cost of a workload that is deployed in the resource group.

The following sections provide instructions for managing service levels and service level objectives:

36.1 Creating Service Levels

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Resources*.
2. Click the *Service Levels* tab, then click *Create*.
3. In the *General* section, provide the following details for the service level:

   Name: Specify a unique name for the service level. This name is displayed in business service workloads.

   You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

   Creation Date: Displays the current date.

   Description: Provide any additional information for the service level.
4. In the *Monthly Resource Costs* fields, define the cost (per month) to use the host resources:

   vCPU: Specify the cost per virtual CPU.

   Memory: Specify the cost per megabyte (MB) of memory.

   Disk: Specify the cost per gigabyte (GB) of disk space.

Network: Specify the cost per network interface card.

5 (Optional) Add objectives to the service level.

5a Under *Associations*, click the *Service Level Objectives* tab.

5b Click *Add* to display the Add Service Level Objectives dialog box.

5c Select the objectives to add.

You can Shift-click and Ctrl-click to select multiple objectives.

If you have not yet created the objectives you want, see "Creating Service Level Objectives" on page 131

5d Click *OK* to add the selected objectives to the *Service Level Objectives* list.

6 Assign the service level to the appropriate resource groups:

6a Under *Associations*, click the *Resource Groups* tab.

6b Click *Add* to display the Add Resource Groups dialog box.

6c Select the groups to add.

You can Shift-click and Ctrl-click to select multiple groups.

6d Click *OK*.

7 Click *Save*.

36.2 Modifying Service Levels

Roles that Can Perform This Task: Cloud Administrator

You can modify a service level to change the resource costs and objectives. Changing a service level can impact the cost of business services currently using the service level.

1 On the main navigation bar, click *Resources*, then click the *Service Levels* tab.

2 Select the service level you want to modify, then click *Edit*.

3 In the *General* section, modify the details for the service level:

Name: Specify a unique name for the service level. This name is displayed in business service workloads.

You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The maximum length is 110 characters.

Creation Date: Displays the current date.

Description: Provide any additional information for the service level.

4 In the *Monthly Resource Costs* fields, define the cost (per month) to use the host resources:

vCPU: Specify the cost per virtual CPU.

Memory: Specify the cost per megabyte (MB) of memory.

Disk: Specify the cost per gigabyte (GB) of disk space.

Network: Specify the cost per network interface card.

5 Add objectives to the service level:

5a Under *Associations*, click the *Service Level Objectives* tab.

5b Click *Add* to display the Add Service Level Objectives dialog box.

5c Select the objectives to add.

You can Shift-click and Ctrl-click to select multiple objectives.

If you have not yet created the objectives you want, see "Creating Service Level Objectives" on page 131

5d Click *OK* to add the selected objectives to the *Service Level Objectives* list.

6 Remove objectives from the service level:

6a Under *Associations*, click the *Service Level Objectives* tab.

6b In the *Service Level Objectives* list, select the objectives you want to remove.

You can Shift-click and Ctrl-click to select multiple objectives.

6c Click *Remove*.

7 Assign the service level to resource groups:

7a Under *Associations*, click the *Resource Groups* tab.

7b Click *Add* to display the Add Resource Groups dialog box.

7c Select the groups to add.

You can Shift-click and Ctrl-click to select multiple groups.

7d Click *OK*.

8 Remove the service level from resource groups:

8a Under *Associations*, click the *Resource Groups* tab.

8b Select the resource groups from which to remove the service level.

You can Shift-click and Ctrl-click to select multiple groups.

8c Click *Remove*.

9 Click *Save* to save your changes to the service level.

36.3 Deleting Service Levels

Roles that Can Perform This Task: Cloud Administrator

If a service level is associated with a business service, you cannot delete the service level.

1 On the main navigation bar, click *Resources*, then click the *Service Levels* tab.

2 Select the service level you want to delete, then click *Delete*.

3 Click *Yes* to confirm the deletion.

If the service level is associated with a workload, you receive a message informing you that the service level cannot be deleted.

36.4 Creating Service Level Objectives

Roles that Can Perform This Task: Cloud Administrator

Service level objectives define measurable characteristics such as availability, throughput, frequency, response time, and quality. Each of these characteristics typically has multiple objectives that identify a different level of service.

For example, you might define three availability objectives (97%, 98%, and 99%) and associate them with different service levels (Silver, Gold, and Platinum). By associating different costs with the objectives, you can establish the desired cost structure for your service levels.

1. On the main navigation bar, click *Resources*.
2. Click the *Service Levels* tab, click *Service Level Objectives*, then click *Create* to display the Create Service Level Objective dialog box.
3. Provide the following details:

   Name: Specify a name for the service level objective. The name should be different than any other objective name.This name not only appears to administrators but also to business service requestors when they configure workloads with service levels that include the objective.

   Monthly Cost: Specify the cost associated with the objective. If the objective does not have a cost, leave the field empty.

   Description: Provide optional text to further identify the service level objective.

   Creation Date: Displays the current date.

   Objective Type: If this objective represents workload availability, select *Availability*. Otherwise, select *General*.

   Value: If the objective type is *Availability*, specify the target availability as a percentage (for example, 99.9). If the objective type is *General*, specify an appropriate objective value.
4. Click *Save*.

36.5 Modifying Service Level Objectives

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Resources*.
2. Click the *Service Levels* tab, then click *Service Level Objectives*.
3. Select the objective you want to modify, then click *Edit*.
4. Modify the following details:

   Name: Specify a name for the service level objective. The name should be different than any other objective name.This name not only appears to administrators but also to business service requestors when they configure workloads with service levels that include the objective.

   Monthly Cost: Specify the cost associated with the objective. If the objective does not have a cost, leave the field empty.

   Description: Provide optional text to further identify the service level objective.

   Creation Date: Displays the current date.

   Objective Type: If this objective represents workload availability, select *Availability*. Otherwise, select *General*.

   Value: If the objective type is *Availability*, specify the target availability as a percentage (for example, 99.9). If the objective type is *General*, specify an appropriate objective value.
5. Click *Save*.

36.6 Deleting Service Level Objectives

Roles that Can Perform This Task: Cloud Administrator

You cannot delete a service level objective that is associated with a service level. Remove the objective from any service levels before deleting it.

1. On the main navigation bar, click *Resources*.
2. Click the *Service Levels* tab, then click *Service Level Objectives*.
3. Select the service level you want to delete, then click *Delete*.
4. Click *Yes* to confirm the deletion.

   If the objective is associated with a service level, you receive a message informing you of the association.

37 Assigning Service Levels to Resource Groups

A resource group identifies a collection of VM hosts to which workloads can be deployed. However, a resource group does not includes any costs associated with running workloads on the hosts. A resource group also does not include any service objectives for the workloads (such as host availability or support response time). The resource costs and service objectives are applied to resource groups through the assignment of service levels.

37.1 Assigning Service Levels

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click  *Resources*.
2. Click the *Resource Groups* tab, select the resource group to which you want to assign a service level, then click *Edit*.
3. Under *Associations*, click the *Service Level* tab.
4. Click *Add* to display the Add Service Levels dialog box.
5. Select the service level.

   You can Shift-click and Ctrl-click to select multiple service levels.
6. Click *OK* to add the selected service level to the *Service Levels* list.
7. Click *Save* to save the changes to the resource group.

37.2 Removing Service Levels

Roles that Can Perform This Task: Cloud Administrator

You cannot remove service levels that are associated with business services deployed in the resource group.

1. On the main navigation bar, click  *Resources*.
2. Click the *Resource Groups* tab, select the resource group from which you want to remove the service level, then click *Edit*.
3. Under *Associations*, click the *Service Level* tab.

4 Select the service level to remove.

   You can Shift-click and Ctrl-click to select multiple service levels.

5 Click *Remove* to remove the selected service level from the *Service Levels* list.

6 Click *Save* to save the changes to the resource group.

   If the service level is associated with a business service that is deployed in the resource group, you receive a message stating that the service level cannot be removed.

38 Assigning Resource Groups to Organizations and Business Groups

Resource groups must be assigned to an organization in order for the organization's business services to use those resources. After you assign resource groups to an organization, you or the Organization Manager can make them available to business groups within the organization.

The following steps assume that the resource groups you want to assign already exist. If they do not, see "Creating, Modifying, and Deleting Resource Groups" on page 125.

38.1 Assigning Resource Groups to an Organization

Roles that Can Perform This Task: Cloud Administrator

1. On the main navigation bar, click *Organizations*.
2. On the *Organizations* tab, select the target organization, then click *Edit*.
3. Add the resource groups you want the organization to have access to:
   - **3a** Under *Membership and Access*, click the *Resource Groups* tab.
   - **3b** Click *Add* to display the Add Resource Groups dialog box.
   - **3c** Select the resource groups to add.

     You can Shift-click and Ctrl-click to select multiple groups.
   - **3d** Click *OK* to add the selected resource groups to the *Resource Groups* list.
4. Add the networks that you want the organization to have access to.

   The resource group's networks are determined by its VM hosts. To enable you to provide isolated networks for organizations that share the same resource group, the networks are not automatically added when you add the resource group. You must explicitly add the networks that you want assigned to the organization.
   - **4a** Under *Membership and Access*, click the *Networks* tab.
   - **4b** Click *Add* to display the Add Networks dialog box.
   - **4c** Select the networks to add.

You can Shift-click and Ctrl-click to select multiple networks.

4d Click *OK* to add the selected networks to the *Networks* list.

5 When you have finished adding resource groups, click *Save* to save the changes.

38.2 Assigning Resource Groups to a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

A business group does not automatically inherit the resource groups assigned to its organization. Any of the organization's resource groups that you want to be available to the business group must be assigned to it.

1 On the main navigation bar, click *Organizations*, then click the *Business Groups* tab.

2 In the *Business Groups* list, select the target business group, then click *Edit*.

3 Add the resource groups you want the business group to have access to:

3a Under *Membership and Access*, click the *Resource Groups* tab.

3b Click *Add* to display the Add Resource Groups dialog box.

3c Select the resource groups to add.

You can Shift-click and Ctrl-click to select multiple groups.

3d Click *OK* to add the selected resource groups to the *Resource Groups* list.

4 Add the networks that you want the business group to have access to.

The resource group's networks are determined by its VM hosts. To enable you to provide isolated networks for business groups that share the same resource group, the networks are not automatically added when you add the resource group. You must explicitly add the networks you want assigned to the business group.

4a Under *Membership and Access*, click the *Networks* tab.

4b Click *Add* to display the Add Networks dialog box.

4c Select the networks to add.

You can Shift-click and Ctrl-click to select multiple networks.

4d Click *OK* to add the selected networks to the *Networks* list.

5 When you have finished adding resource groups, click *Save* to save the changes to the business group.

38.3 Removing Resource Group Assignments from an Organization

Roles that Can Perform This Task: Cloud Administrator

You can remove a resource group from an organization only if the resource group is not hosting any deployed business services from the organization's business groups.

Removing a resource group assignment from an organization also removes any assignments from its business groups.

1. On the main navigation bar, click *Organizations*.
2. In the *Organizations* list, select the organization from which you want to remove the resource group assignment, then click *Edit*.
3. Click the *Resource Groups* tab.
4. Select the resource group to be removed, click *Remove*, then click *Yes* to confirm the removal.

   You can Shift-click or Ctrl-click to select multiple resource groups.
5. When you have finished removing resource group, click *Save* to save the changes to the organization.

38.4 Removing Resource Group Assignments from a Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

You can remove a resource group from a business group only if the resource group is not hosting any of the business group's deployed business services.

1. On the main navigation bar, click *Organizations*.
2. Click the *Business Groups* tab, select the business group from which you want to remove the resource group assignment, then click *Edit*.
3. Click the *Resource Groups* tab.
4. Select the resource group to be removed, click *Remove*, then click *Yes* to confirm the removal.

   You can Shift-click or Ctrl-click to select multiple resource groups.
5. When you have finished removing resource group, click *Save* to save the changes to the business group.

39 Monitoring Resource Capacity

Roles that Can Perform This Task: Cloud Administrator, Zone Administrator (zone only), Approver (organization only)

The Capacity view provides information about used, reserved, and allocated resource capacity for organizations and zones.

39.1 Accessing the Capacity View

To open the Capacity view:

1 On the main navigation bar, click  *Capacity*.

39.2 Understanding the Capacity View

The Capacity view includes three main sections:

39.2.1 Capacity Summary Bar

The Capacity Summary bar provides a summary for the total resources within your management scope.

For example, if you are a Cloud Administrator, you see a summary for all of the resources in your Cloud. If you are a Zone Administrator, you see a summary of all of the resources in the zones you manage. If you are an Approver, you see a summary of all of the resources in your assigned organizations and zones.

Each resource (Memory, CPU, and Storage) has its own capacity indicator. The indicator displays the used and reserved capacity as a percentage of the total available capacity.

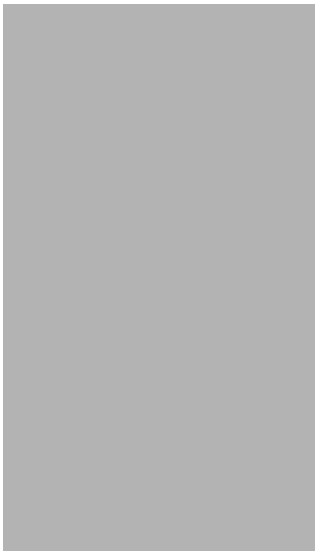
The color of the indicator is determined by the Warning and Problem thresholds set for the Cloud environment. Green indicates that no thresholds have been reached, yellow indicates that the Warning threshold has been reached, and red indicates that the Problem threshold has been reached.

The Issues section of the Capacity Summary bar shows the following:

- No resource issues.
- The number of resources that have reached the Warning threshold.
- The number of resources that have reached the Problem threshold.

39.2.2 Organizations or Zones List

The Organizations or Zones list displays the organizations or zones for which you can view resource capacity.



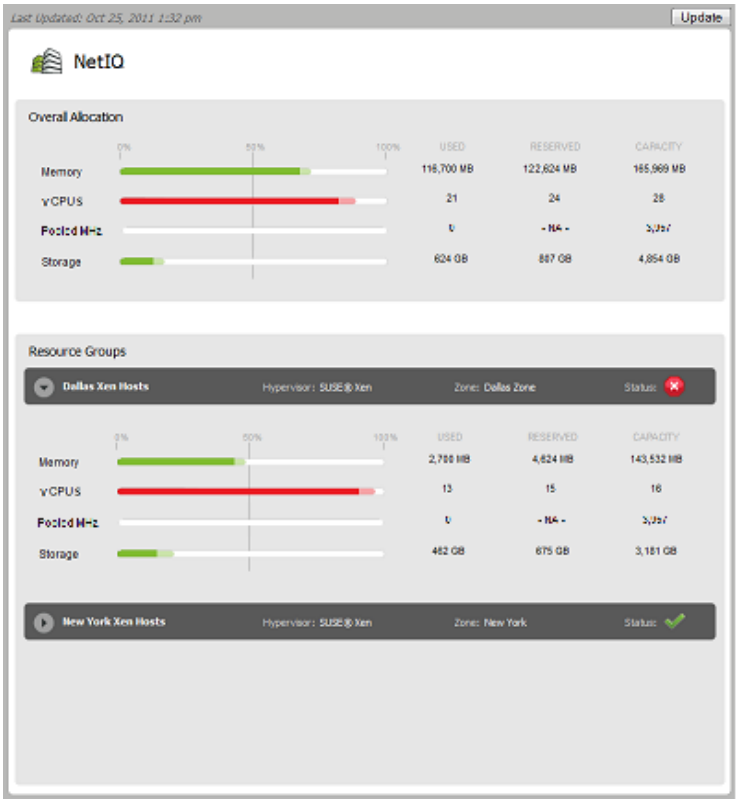
Depending on your role, you might be able to see either organizations or zones but not both.

The icon next to each organization or zone indicates the current status of the resources for that item. The statuses correspond to the statuses that can be listed in the Capacity Summary bar:

- No resource issues.
- One or more resources for the organization or zone have reached the Warning threshold.
- One or more resources for the organization or zone have reached the Problem threshold.

39.2.3 Organizations or Zones Details

The Organizations or Zones Details panel displays the resource capacity information for the organization or zone that is selected in the list.



The *Overall Allocation* section provides a summary of the used, reserved, and available capacity for the entire organization or zone. The *Resource Groups* section shows the same type of information for the each resource group in the organization or zone.

- **Memory:** The memory (RAM) resources.
- **vCPUs:** The host and cluster virtual CPU resources, represented in number of CPUs. This resource is displayed only if a resource group contains hosts or clusters.
- **Pooled MHz:** The resource pool CPU resources, represented in MHz of CPU. This resource is displayed only if a resource group contains vSphere resource pools.
- **Storage:** The shared storage resources. This includes SAN (Storage Area Network) and NAS (Network-attached Storage). Local storage is not included.

For each resource, the following information is displayed:

- **Used:** The amount of the resource that is actually being consumed by deployed workloads. For example, a workload might be allocated 4 GB of memory but only be using 2 GB.
- **Reserved:** The amount of the resource that is reserved for deployed workloads. For example, if a workload is allocated 4 GB of memory, all 4 GB are reserved.
- **Capacity:** The total amount of the resource that is available for deployed workloads. For memory from hosts and clusters, the *Capacity* field reflects the total physical memory of the hosts, not just the memory that is available for workloads. For example, a host's physical memory might be 16252 MB, with the actual memory available for workloads being 10695 MB.

Because the *Capacity* field uses the physical memory amount (16252 MB), you might not have as much memory capacity as appears. For memory from resource pools, the *Capacity* field reflects the actual memory pool size.

The *Resource Groups* sections provide capacity details for each resource group assigned to the organization or zone. The status of each resource group is also displayed.

The *Last Updated* field displays the last time the capacity data was updated. The *Update* button lets you update the data.

39.3 Updating the Capacity Data

The Capacity engine collects capacity data on a regular interval specified in System Configuration. The collected data is cached on the Cloud Manager Application Server.

The Capacity data is static, meaning that the Capacity view displays the same data until you update from the cached data on the Cloud Manager Application Server.

To update the data:

1. Click *Update*.

   If the cached data is newer than the current data, the Capacity view is updated with the cached data.
2. Click *Yes* to confirm that you to continue with the manual update.

   The Capacity engine collects the new data from the system. As soon as the data is collected, the Capacity view automatically updates to the new data.

39.4 Debugging Capacity Collection Issues

As a Cloud Manager administrator, you might occasionally encounter capacity collection issues in the Cloud Manager system. You can enable the debugging for capacity collection logging on your production level Cloud Manager Application Server to help you or NetIQ Support troubleshoot these issues.

The Cloud Manager Application Server uses a custom properties file, `/etc/cmplanner.logging.properties`, to enable logging. Its contents, including the `DEBUG` setting, look like this:

```
# Set root logger level to DEBUG and its only appender to A1.
log4j.rootLogger=WARN, CMFILE, CMOUT

# Planner is set to be a ConsoleAppender.
log4j.appender.CMOUT=org.apache.log4j.ConsoleAppender
log4j.appender.CMOUT.layout=org.apache.log4j.PatternLayout
log4j.appender.CMOUT.layout.ConversionPattern=%-4r [%t] %-5p %c %x - %m%n

# File appender
log4j.appender.CMFILE=org.apache.log4j.RollingFileAppender
log4j.appender.CMFILE.layout=org.apache.log4j.PatternLayout
log4j.appender.CMFILEt.layout.ConversionPattern=[%d{dd MMM yyyy HH:MM:ss}] %-5.5p
| %-16.16t | %-32.32c{1} | %X{bundle.id} - %X{bundle.name} - %X{bundle.version} |
%m%n
log4j.appender.CMFILE.file=${karaf.base}/logs/cloudmanager_server.log
log4j.appender.CMFILE.append=true
log4j.appender.CMFILE.maxFileSize=10MB
log4j.appender.CMFILE.maxBackupIndex=10


# Logging category modifications for novell-esb
log4j.logger.org.quartz=DEBUG
log4j.logger.com.netiq.rest.planner.CmPlanner=DEBUG
log4j.logger.com.netiq.service.planner.capacitybot.CapacityBot=DEBUG
```

To enable debug logging,

1. Edit the properties file, changing any `WARN` value to a `DEBUG` value (see example, above).
2. In the Karaf console, run an update on the AppServices bundle.

   The update process requires that you enter a module ID. You can find this ID using a `list` command and then browsing the list of modules and their accompanying IDs.

VII Business Service Management

The following sections provide information to help you deploy business services, manage deployed business services, and change deployed business services:

40 Requesting Business Services

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

A deployed business service starts as a request. The request defines the business service, including its name, contract period, and workloads. As soon as you submit the request, it goes through an approval and build process that you can track until the business service is deployed.

1. On the main navigation bar, click *Business Services*, then click the *Requests* tab.
2. Click *Create* to display the Create Business Service Request dialog box.
3. Provide the following details for the business service:

   Service Name: Specify a name that is different than any other business service names for the business group. You can use letters, numbers, and the following special characters: space, hyphen, underscore, apostrophe, percent, ampersand, and period. The name must begin with a letter or number and have a maximum length of 110 characters.

   Start Date: Click to select the date you want the business service to be available.

   Expiration Date: Click to select the date you want the business service to no longer be available. If you don't want the business service to expire, delete the date from the field.

   Contract Length: If an expiration date is selected, this field displays the total number of months for the contract.

   Organization: Select the organization for which you are creating the business service. You can select the business group before the organization, in which case the correct organization is automatically selected.

   Business Group: Select the business group for which you are creating the business service.

   Creator: Displays your user name.

   Business Purpose: Provide details that explain the purpose or justification for the business service. This information is visible to the business service's approvers during the request approval process.
4. Add a workload to the business service:
   - **4a** Click *Add* to display the Select Workload Template dialog box.

     The dialog box displays a list of workload templates. A template provides the base settings and costs for the workload.
   - **4b** Select the workload template from which to create the workload, then click *OK* to display the Configure Workload dialog box.
   - **4c** On the *Resources* tab, specify a name for the workload, select a service level, and customize the resources allocated to the workload.

     You cannot customize the resources if they are locked. For additional information about the *Resources* settings, click the button.
   - **4d** Click the *Disks* tab to configure the workload's disks.

The workload's mandatory disks are listed. The mandatory disks are created with the workload and cannot be customized.

If the *Add* action, located above the list, is available, there are optional disks you can create for the workload. Click *Add*, then specify the size for the disk.

For additional information about the *Disks* settings, click the button.

4e Click the *Networks* tab (if it is displayed), select a network interface card, then assign the network and configure the network address and name servers.

For additional information about the *Networks* settings, click the button.

4f (Optional) Click the *Windows Settings* tab (if it is displayed), then provide an Administrator account password, computer name, and workgroup or domain information.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide during pre-build configuration of the workloads. For additional information about the *Windows Settings* settings, click the button.

4g (Optional) Click the *Windows Licensing* tab (if it is displayed), then provide a Windows product key, and registration name.

If the Cloud Administrator has pre-populated the Windows Product Key field, the data is masked. You cannot copy this data.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide during pre-build configuration of the workloads. For additional information about the *Windows Licensing* settings, click the button.

4h (Optional) Click the *Linux Settings* tab (if it is displayed), then provide a host name and domain name.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide during pre-build configuration of the workloads. For additional information about the *Linux Settings* settings, click the button.

4i (Optional) Click the *Console Access* tab, then set the password for VNC access to the workload.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide during pre-build configuration of the workloads. For additional information about the *Console Access* settings, click the button.

4j Click *OK* to save the workload and add it to the *Workloads* list.

5 Add any additional workloads to the business service.

You can add additional workloads by repeating Step 4 or by copying an existing workload and then modifying it as necessary. To copy a workload:

5a Select the workload to copy, then click *Copy*.

5b Select the number of copies to create, and provide a unique name for each copy.

5c Click *OK*.

The new workloads are added to the *Workloads* list.

5d Edit each new workload to provide any missing information.

Each new workload contains as much of the original information as possible, but information such as network addresses, Windows computer names, and Linux host names are not copied because they need to be unique for each workload.

6 (Optional) Give other users ownership rights to the business service.

The Users list lets you see any users who have been explicitly assigned ownership rights to the business service. It does not show users who inherit ownership rights to the business service through their roles.

6a Click the *Users* tab, then click *Add*.

6b Select users from the two lists.

The *Members* list displays all users who are members of the business service's organization. The *System Users* list displays users who are not members of the organization.

You can Shift-click and Ctrl-click to select multiple users (or user groups).

6c Click *OK*.

The users are added to the list.

7 Click *Save* to add the request to the *Requested Services* list without submitting it.

or

Click *Submit* to add the request and submit it for approval.

41 Managing Business Service Requests

After you request a business service, a business service request is added to your *Requests* list. You can complete any of the following tasks to manage the request.

41.1 Submitting a Request

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

The following steps assume that you have a saved business service request that you want to submit. If you have not yet created the request, see Requesting Business Services.

1. On the main navigation bar, click *Business Services*, then click *Requests*.
2. Select the request, then click *Submit*.

41.2 Editing a Request

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

You can edit only unsubmitted requests. If you want to change a submitted request, you must withdraw it, change it, and then resubmit it. For information about withdrawing a request, see Withdrawing a Request.

1. On the main navigation bar, click *Business Services*, then click the *Requests* tab.
2. Select the request, then click *Edit*.

   or

   Double-click the request.
3. Modify the request as desired.

   For a description of the settings, click the button.
4. Click *Save* to save your changes without submitting the request.

   or

   Click *Submit* to save your changes and submit the request.

41.3 Withdrawing a Request

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

Withdrawing a request stops the provisioning process. You can withdraw a submitted request until it reaches a certain phase in the *Building* process. At that point, the *Withdraw* action is no longer available.

After you withdraw a request, you can make changes to it and resubmit it, or you can delete it.

1. On the main navigation bar, click *Business Services*, then click the *Requests* tab.
2. Select the request, then click *Withdraw*.

41.4 Deleting a Request

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

You can delete non-submitted requests. To delete a submitted request, you must first withdraw it so that it becomes a non-submitted request. For information about withdrawing a request, see Withdrawing a Request.

1. On the main navigation bar, click *Business Services*, then click the *Requests* tab.
2. Select the request, then click *Delete*.
3. Click *Yes* to confirm the deletion.

42 Importing Existing Virtual Machines

If you have an existing virtual machine that is not part of the Cloud Manager system, you can import it as new business service or you can import it into a deployed business service. Because the virtual machine is already provisioned, the request and provisioning processes are skipped and the virtual machine is imported directly as a deployed workload.

In order to import a virtual machine, it must reside on a host associated with a resource group. The virtual machine can be running, shut down, or suspended.

42.1 Importing a Virtual Machine into a New Business Service

Roles that Can Perform This Task: Cloud Administrator

The following steps explain how to import a virtual machine as a new business service. To import a virtual machine into an existing business service, see Section 42.2, "Importing a Virtual Machine into a Deployed Business Service," on page 156.

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Click *Import* to display the Import Business Service dialog box.
3. Provide the following details for the business service:

   Service Name: Specify a name for the business service. The name should be unique among other business services you have created.

   Start Date: Defaults to the current date. You cannot change the start date.

   Expiration Date: Click to select the date you want the business service to no longer be available. If you don't want the business service to expire, leave the field empty.

   Contract Length: If an expiration date is selected, this field displays the total number of months for the contract.

   Organization: Select the organization for which you are importing the business service.

   Business Group: Select the business group for which you are importing the business service.

   Creator: Displays your name. You cannot change the creator.

   Business Purpose: Provide details that explain the purpose or justification for the business service.
4. Import a virtual machine:

   4a On the *Workloads* tab, click *Import* to display the Select Virtual Machine dialog box.

   The dialog box displays a list of virtual machines that can be imported into the selected business group.

4b Select the virtual machine to import, then click *OK* to display the Configure Imported Workload dialog box.

4c On the *Resources* tab, configure the following:

Workload Name: By default, the workload inherits the virtual machine name. Make sure the name is different from other workloads included in the business service.

License Costs: Specify the monthly cost for licenses associated with the workload.

Service Level: Select the service level for the workload.

4d (Optional) On the *Disks* tab, select a disk, then enable the *Cost* check box to include the disk's cost in the business service cost or disable the check box to exclude the disk from the business service cost.

4e Click *OK* to save the configuration and add the workload to the business service.

5 Assign users as owners of the business service:

5a On the *Users* tab, click *Add* to display the Add Business Service Owner dialog box.

5b Select the users to add as owners.

You can add members of the organization or System users. Shift-click and Ctrl-click to select multiple users.

5c Click *OK*.

6 Click *Import* to add the business service to the list of deployed business services.

At this point, you can change the imported workload's resources if necessary. This is a change to the business service and requires a change request to go through the approval process and the imported workload to be rebuilt. See Chapter 44, "Changing Deployed Business Services," on page 161.

42.2 Importing a Virtual Machine into a Deployed Business Service

Roles that Can Perform This Task: Cloud Administrator

The following steps explain how to import a virtual machine into an existing deployed business service. To import a virtual machine as a new business service, see Section 42.1, "Importing a Virtual Machine into a New Business Service," on page 155.

1 On the main navigation bar, click *Business Services*, then click *Deployed*.

2 Select the business service to which you want to import the virtual machine, then click *Manage*.

or

Double-click the business service.

3 On the *Workloads* tab, click *Import* to display the Select Virtual Machine dialog box.

The dialog box displays a list of virtual machines that can be imported into the selected business group.

4 Select the virtual machine to import, then click *OK* to display the Configure Imported Workload dialog box.

5 On the *Resources* tab, configure the following:

Workload Name: By default, the workload inherits the virtual machine name. Make sure the name is different from other workloads included in the business service.

License Costs: Specify the monthly cost for licenses associated with the workload.

Service Level: Select the service level for the business service.

6. (Optional) On the *Disks* tab, select a disk, then enable the *Cost* check box to include the disk's cost in the business service cost or disable the check box to exclude the disk from the business service cost.
7. Click *OK* to save the configuration and add the workload to the business service.
8. Click *Save* to save the business service.

43 Managing Deployed Business Services

You can cycle (start, suspend, stop) a deployed business service's workloads, open a remote console to a workload, and give other users access to the business service.

43.1 Starting, Suspending, or Shutting Down a Workload

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service with the workload you want to cycle, then click *Manage*.
3. In the *Workloads* list, select the workload.
4. Click one of the following controls:

   Start the workload.

   Suspend the workload.

   Shut down the workload.
5. Click *Close*.

43.2 Opening a Workload Console

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

Cloud Manager provides remote access to workloads via a VNC console.

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service with the workload you want to access, then click *Manage*.
3. In the *Workloads* list, select the workload, then click *Console*.
   - The *Console* action opens a new browser window that provides VNC access to the selected workload's desktop. The *Console* action is enabled even when a workload is shut down, which gives users the opportunity to enter a password before restarting the virtual machine.

- If the VNC session does not require a password, the user can press Enter. If the user enters a password incorrectly when the VNC session is established, he or she can enter the password again.
- The *Console* action is not enabled for imported workloads that have not yet been configured for VNC access.

4 Specify the console password to log in.

After you log in, Cloud Manager opens a remote console session to the workload. Most functions of the remote console work the same as the local console. However, if you need to use special key sequences such as Ctrl+Alt+Del, you must select them from the *Send Special Key Sequence* menu located at the top of the console.

NOTE: In this version of Cloud Manager, the VNC console is rendered using HTML 5. If you use Internet Explorer 9 as the browser to view the Cloud Manager Web Console, you need to make sure that either the Adobe (Shockwave) Flash add-on is enabled or that the Google Chrome Frame add-on is enabled. Both of these add-ons are available for free download.

5 When you have finished, close the browser window to end the session.

43.3 Delegating Ownership of a Business Service

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

By default, the following users have ownership rights to a business service:

- The creator of the business service
- All Business Service Owners for the business group that the business service belongs to
- All Business Service Owners for the organization
- All Organization Managers

If necessary, you can delegate ownership to other users. When you do so, the user receives rights to view, manage, and change the business service.

1 On the main navigation bar, click *Business Services*, then click *Deployed*.

2 Select the business service to which you want to give another user access, then click *Manage*.

3 Click the *Users* tab to display the *Business Service Owner* list.

4 Click *Add*, select the users or user groups you want to give access to the business service, then click *OK*.

You can Shift-click and Ctrl-click to select multiple users and user groups.

If the *Add* action is not available, you do not have rights to give access to other users.

44 Changing Deployed Business Services

You can change a business service's details (expiration date and business purpose) and workloads. Any change (including changing the expiration date and business purpose) generates a change request that must be approved before the changed business service can be redeployed.

44.1 Changing a Business Service's Details

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service, then click *Change*.
3. Modify the details for the business service:

   Expiration Date: Specify the date you want the business service to no longer be available.

   Business Purpose: Provide details that explain the purpose or justification for the change to the business service.
4. Click *Submit* to submit your business service change request.

   or

   If you don't want to submit the change request at this time, click *Save* to save the change request.

   A change icon is added next to the business service name in the *Deployed* list to indicate that a change request has been generated and added to the *Requests* list. If you saved the change request rather than submitting it, you must go to the *Requests* list to edit the request or submit it.

44.2 Reassigning a Business Service to a Different Business Group

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

You can reassign a business service to a different business group if 1) you have rights to the other business group and 2) the business group's resources (hypervisor, service levels, and so forth) support the business service's workloads.

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service, then click *Change*.
3. In the *Business Group* list, select the target business group.
4. Click *Submit* to submit your business service change request.

   or

   If you don't want to submit the change request at this time, click *Save* to save the change request.

   A change icon is added next to the business service name in the *Deployed* list to indicate that a change request has been generated and added to the *Requests* list. If you saved the change request rather than submitting it, you must go to the *Requests* list to edit the request or submit it.

44.3 Adding a Workload

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service to which you want to add a workload, then click *Change*.
3. On the *Workloads* tab, click *Add* to display the Select Workload Template dialog box.

   The dialog box displays a list of workload templates. A template is the basis for a workload, providing basic workload settings and costs.
4. Select the workload template from which to create the workload, then click *OK* to display the Configure Workload dialog box.
5. On the *Resources* tab, specify a name for the workload, select a service level, and customize the resources allocated to the workload.

   If the resources are locked, you cannot customize them. For additional information about the *Resources* settings, click the button.
6. Click the *Disks* tab to configure the workload's disks.

   The workload's mandatory disks are listed. The mandatory disks are created with the workload and cannot be customized.

   If the *Add* action, located above the list, is available, there are optional disks you can create for the workload. Click *Add*, then specify the size for the disk

   For additional information about the *Disks* settings, click the button.
7. Click the *Networks* tab (if it is displayed), select a network interface card, then assign the network and configure the network address and name servers.

   For additional information about the *Networks* settings, click the button.
8. (Optional) Click the *Windows Settings* tab (if it is displayed), then provide an Administrator account password, computer name, and workgroup or domain information.

   If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide it during pre-build configuration of the workloads. For additional information about the *Windows Settings* settings, click the button.

9 (Optional) Click the *Windows Licensing* tab (if it is displayed), then provide a Windows product key, and registration name.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide it during pre-build configuration of the workloads. For additional information about the *Windows Licensing* settings, click the button.

If the Cloud Administrator has pre-populated the Windows Product Key field, the data is masked. You cannot copy this data.

10 (Optional) Click the *Linux Settings* tab (if it is displayed), then provide a host name and domain name.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide it during pre-build configuration of the workloads. For additional information about the *Linux Settings* settings, click the button.

11 (Optional) Click the *Console Access* tab, then set the password for VNC access to the workload.

If you do not provide this information at this time, a Build Administrator or Cloud Administrator must provide it during pre-build configuration of the workloads. For additional information about the *Console Access* settings, click the button.

12 Click *OK* to save the workload and add it to the *Workloads* list.

13 Click *Submit* to submit your business service change request.

or

If you don't want to submit the change request at this time, click *Save* to save the change request.

A change icon is added next to the business service name in the *Deployed* list to indicate that a change request has been generated and added to the *Requests* list. If you saved the change request rather than submitting it, you must go to the *Requests* list to edit the request or submit it.

44.4 Modifying a Workload

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

1 On the main navigation bar, click *Business Services*, then click *Deployed*.

2 Select the business service with the workload you want to modify, then click *Change*.

3 On the *Workloads* tab, select the workload to modify, then click *Edit*.

4 Modify the workload settings as desired.

For information about the workload settings, click the button.

IMPORTANT: The *Service Level* field and *Resource Group* field (if it is available) determine which resource group hosts the workload. If you use either of these fields to change the workload's resource group, you need to stop and then start the workload after it is rebuilt. The workload is not moved to the new resource group until it is manually restarted.

5 Click *OK* to save the workload changes.

6 Click *Submit* to submit your business service change request.

or

If you don't want to submit the change request at this time, click *Save* to save the change request.

44.5 Removing a Workload

Roles that Can Perform This Task: Cloud Administrator, Organization Manager, Business Service Owner

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service with the workload you want to remove, then click *Change*.
3. On the *Workloads* tab, select the workload, then click *Remove*.
4. Click *Yes* to confirm the action.
5. Click *Submit* to submit your business service change request.

   or

   If you don't want to submit the change request at this time, click *Save* to save the change request.

45 Extending Business Service Expiration Dates

Roles that Can Perform This Task: Cloud Manager, Organization Manager, Business Service Owner

To extend the expiration date for a business service, you must submit a business service change request. The request goes through the standard approval and configuration workflow for a business service.

1. On the main navigation bar, click *Business Services*, then click *Deployed*.
2. Select the business service, then click *Change*.
3. Change the expiration date to the desired date.
4. Click *Submit* to submit your business service change request.

   or

   If you don't want to submit the change request at this time, click *Save* to save the change request.

   A change icon is added next to the business service name in the *Deployed* list to indicate that a change request has been generated and added to the *Requests* list. If you saved the change request rather than submitting it, you must go to the *Requests* list to edit the request or submit it.

46 Displaying or Hiding Business Service Costs

The Cloud Manager console displays business service costs in places such as the business service lists, the individual business service dialog boxes, and business service cost reports. System users always see the business service costs. However, you can choose whether or not to display costs to Organization members.

There are three levels at which you can configure the *Costs* setting:

- **Organization:** This setting applies to all Organization members. For example, if the *Costs* setting is set to *Hide*, no Organization members can see business service costs.
- **Business Group:** This setting overrides the organization setting for the business group. For example, if the organization *Costs* setting is set to *Hide*, but the business group *Costs* setting is set to *Show*, Organization members can see the costs for that business group's business services.
- **User:** Each user account has an *Always show costs* setting that overrides the organization and business group *Costs* setting.

46.1 Configuring an Organization's Costs Setting

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

1. On the main navigation bar, click *Organizations*.
2. On the *Organizations* tab, select the target organization, then click *Edit*.
3. In the upper-right corner of the dialog box, click the icon to display the Organization Configuration dialog box.
4. Under *Organizations Costs*, select *Show* or *Hide*.

   The setting applies to all Organization members unless it is overridden for a business group or individual user.
5. Click *OK* to save your changes.

46.2 Configuring a Business Group's Costs Setting

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

1. On the main navigation bar, click *Organizations*.
2. Click the *Business Groups* tab, select the target business group, then click *Edit*.

3 In the *Costs* field, select *Override* to override the setting inherited from the organization, then select *Show* or *Hide*.

   The setting applies to all business services created for the business group. If the costs are hidden, no Organization members can see the costs unless you enable the *Always show costs* setting for individual users.

4 Click *Save* to save your changes.

46.3 Configuring a User's Costs Setting

Roles that Can Perform This Task: Cloud Administrator, Organization Manager

1 On the main navigation bar, click *Organizations.*

2 Click the *Users* tab, select the target user, then click *Edit*.

3 In the *Cost Visibility* field, select *Always show costs* to enable the user to see business service costs regardless of the organization and business group *Costs* settings.

   The setting is disabled for System users. System users can always see business service costs.

4 Click *Save* to save your changes.

VIII Tasks Management

The following sections provide information to help you manage the tasks that are created when requesting, changing, or deleting a business service:

47 Displaying Administrator or Sponsor Tasks

Roles that Can Perform This Task: Cloud Administrator, Sponsor

In the *Unclaimed Tasks* list and the *All Tasks* list, tasks are categorized as Administrator tasks or Sponsor tasks. The Administrator tasks are the two configuration tasks (pre-build configuration and post-build configuration) and the Administrator approval task. The Sponsor task is the Sponsor approval task.

You can filter the two lists to show only Administrator tasks, only Sponsor tasks, or all tasks.

1. On the main navigation bar, click *Tasks*.
2. Click the list you want (*Unclaimed* or *All Tasks*).
3. In the select box at the top of the list, select the tasks you want to display (*All Tasks*, *Administrator Tasks*, or *Sponsor Tasks*).

48 Tasks Concepts

Business services can be created, changed, and deleted. Each of these actions results in a *creation* request, a *change* request, or a *deletion* request. Each request must go through a workflow process in order for the request to be approved (or denied) and the resulting business service workloads to be configured if necessary.

During the workflow process for a request, tasks are generated. These tasks must be completed for the business service to be created, changed, or deleted. The following sections provide information you should understand in order to successfully manage the tasks generated for you and other roles in your system:

48.1 Types of Tasks

There are two types of tasks generated during the workflow process:

- **Approval Tasks:** Approval tasks require the task owner to either approve or deny the business service request. There are two approval tasks generated during the workflow process: an Administrator approval task and a Sponsor approval task.

  The Administrator approval task is generated for an administrator (Approver or Cloud Administrator) to provide IT approval. If the administrator approves the request, a Sponsor approval task is then generated for the Sponsor to provide financial approval.
- **Configuration Tasks:** Configuration tasks require the task owner to complete the configuration of business service workloads. There are two configuration tasks generated during the workflow process: a pre-build configuration task and a post-build configuration task.

  The pre-build configuration task occurs before the requested business service's workloads are built, and a post-build configuration task occurs after the workloads are built. The tasks are generated for Build Administrators and Cloud Administrators.
- **Trigger Tasks:** Trigger tasks require user input before performing an action, for example, a user can choose to immediately reboot a virtual machine as part of a change request, which could potentially lose data. Alternatively, a trigger task can be scheduled, allowing the user to delay a task to complete at a later time. For example, a user could schedule a VM reboot for midnight on a Saturday.

  When a change request is made for a business service, the reboot trigger task occurs after the pre-build configuration task, and before the changes are applied to the workloads in the system build step. The trigger task is generated for the Business Service Owner and for Build Administrators and Cloud Administrators.

48.2 Task Order in the Workflow Process

During the workflow process, tasks are generated sequentially as needed so that the process flows correctly. The following table shows the workflow process and where the approval and configuration tasks occur in the process. The table also indicates the roles that can perform each task.

Workflow Process	Performed by
Create a request	Business Service Owner Organization Manager Cloud Administrator
Administrator approval task	Approver Cloud Administrator
Sponsor approval task	Sponsor Cloud Administrator
Pre-build configuration task	Build Administrator Cloud Administrator
 Reboot trigger task (at Change Request)	Business Service Owner Organization Manager Cloud Administrator
Build the workloads	System
Post-build configuration tasks	Build Administrator Cloud Administrator
Deploy the business service	System

The workflow process shown above is for requests for new or changed business services. Requests for deleted business services go through the two approval stages only. No configuration tasks are required and the business service is deleted after the Sponsor approval.

48.3 Task Assignments and Owners

Tasks are assigned to roles and not specific individuals. For example, the Sponsor approval task is assigned to all users who have the Sponsor role for the organization or business group that requested the business service. Likewise, the configuration tasks are assigned to all users who are Build Administrators for the organization or the business group that requested the business service. The Reboot trigger task is assigned to users who are Business Service Owners or administrators for the organization or business group that requested a change in the business service.

Individual users can claim a task to become the *task owner*. No other users can work on the task while it is owned by the user. If necessary, owned tasks can be released by the owner or claimed by another user.

49 Claiming Tasks

Roles that Can Perform This Task: Cloud Administrator, Approver (Administrator approval tasks only), Sponsor (Sponsor approval tasks only), Build Administrator (configuration tasks only)

You can claim an unclaimed task or a task that is owned by another user. When you claim a task, you become the task owner. No one else can work on the task unless you release (unclaim) the task or the other user claims it from you.

You cannot assign a task to another user. The task must be claimed by the other user.

1. On the main navigation bar, click *Tasks*.
2. To claim an unclaimed task, click the *Unclaimed* tab.

   or

   To claim a task owned by another user, click the *All Tasks* tab.
3. Select the task to claim, then click *Claim*.

   The task is added to your *My Tasks* list. It also remains in the *All Tasks* list but you are added as the task owner.

50 Approving and Denying Requests

Roles that Can Perform This Task: Cloud Administrator, Approver (Administrator approval tasks only), Sponsor (Sponsor approval tasks only)

As a Cloud Administrator, you can complete both Administrator approval tasks and Sponsor approval tasks.

1. On the main navigation bar, click *Tasks*, then click the *Unclaimed* tab.
2. Select the task for the business service request, then click one of the following options:
   - *Review*: Lets you review the business service before approving or denying the request.
   - *Approve*: Approves the request.
   - *Deny*: Denies the request. You must specify the reason for the denial. The user receives an e-mail with the reason and can modify the business service and resubmit the request.
   - *Claim*: Assigns the task to you and moves it to your *My Tasks* list. No other user can access the task. This is useful if you want to make sure that you own the task but want to complete it at a later time.
3. If you clicked *Review*, review or change the business service details, including the workload details. When you are finished, select one of the following:
   - *Approve*: Approves the request.
   - *Deny*: Denies the request. You must specify the reason for the denial. The user receives an e-mail with the reason and can modify the business service and resubmit the request.
   - *Claim*: Assigns the task to you and moves it to your *My Tasks* list.
   - *Close*: Closes the task without approving or denying it.

51 Completing Configuration Tasks

As a Cloud Administrator, you can complete both pre-build configuration and post-build configuration tasks.

51.1 Completing Pre-Build Configuration Tasks

Roles that Can Perform This Task: Cloud Administrator, Build Administrator

The pre-build configuration task pauses the workflow process to give you an opportunity to perform any configuration required before the business service workloads are built. This might be configuration that you complete in the Cloud Manager console, such as configuring the Windows settings (Administrator account password, computer name, product license key, and registered name) or remote console password for one of the workloads. Or, it might be a task that you need to perform at the Cloud Manager Orchestration Server or in your hypervisor tools.

1. On the main navigation bar, click *Tasks*, then click the *Unclaimed* tab.
2. Select the task (the subject is *Pre-build configuration of a new Business Service* or *Pre-build configuration of a changed Business Service*).

   If there is configuration that must be completed for the business service in the Cloud Manager console, the *Complete* action is not available and an asterisk (*) appears next to it. You can mouse over the asterisk to view the remaining configuration requirements.
3. If you want to claim the task so that others cannot work on it, click *Claim*.

   Claimed tasks are moved to your *My Tasks* list.
4. Complete any configuration required for the workloads:
   - **Cloud Manager console tasks:** Select the configuration task, then click the *Review* action to display the task. Select a workload that needs to be configured, then click *Edit*. Configure the required settings and save the workload.
   - **External tasks:** Complete the tasks.
5. Mark the task as complete:
   - If you claimed the task, it is your *My Tasks* list. Select the task, then click *Complete*.
   - If you did not claim the task, it is in the *Unclaimed* list. Select the task, then click *Complete*.

51.2 Completing Post-Build Configuration Tasks

Roles that Can Perform This Task: Cloud Administrator, Build Administrator

The post-build configuration task pauses the provisioning workflow to give you an opportunity to perform any post-build configuration for the business service workloads. You must complete the configuration (if any) and then mark the task as completed to continue the workflow process.

1. On the main navigation bar, click *Tasks*, then click the *Unclaimed* tab.
2. If you want to claim the task so that no others can work on it, select the task, then click *Claim*.

   Claimed tasks are moved to your *My Tasks* list.
3. If you want to review the business service request, select the task (the subject is *Post-build configuration of a new Business Service* or *Post-build configuration of a changed Business Service*), then click *Review*.
4. Complete any configuration required for the workloads.
5. Mark the task as complete:
   - If you claimed the task, it is your *My Tasks* list. Select the task, then click *Complete*.
   - If you did not claim the task, it is in the *Unclaimed* list. Select the task, then click *Complete*.

52 Completing Trigger Tasks

As a Cloud Administrator, you can complete or schedule a reboot trigger task.

52.1 Completing Reboot Trigger Tasks

Roles that Can Perform This Task: Business Service Owner, Cloud Administrator, Build Administrator

As a Cloud Administrator, you can complete any workload reboot trigger task. The trigger task pauses the provisioning change request workflow between the pre-build configuration task and before the changes are applied tot he workloads in the system build. This gives you an opportunity to immediately reboot or to schedule the reboot of a business service workload at a later time.

The reboot trigger task stops progress of the workflow, pending user interaction. The task blocks an unintentional reboot of a workload from occurring at an inopportune time. The *Reboot Now* feature in the task lets you decide when the system is in a state to accommodate a reboot, and then to take the appropriate action to reboot immediately.

The reboot scheduling feature accommodates situations when you want the workload to change significantly and these changes will result in the service being taken offline for a significant amount of time. Scheduling an off-hours, weekend, or vacation reboot can make the downtime less impactful to your business.

1. On the main navigation bar, click *Tasks*, then click the *Unclaimed* tab.
2. Select the task for the business service change request (it should be tagged with a “needs reboot” message), then click one of the following options:
   - *Review*: Lets you review the business service change request before immediately rebooting or scheduling a reboot of the workload.
   - *Reboot Now*: Reboots the workload when the option is selected.
   - *Schedule Reboot*: Lets you specify the date and time when you want the workload reboot to occur.
   - *Claim*: Assigns the task to you and moves it to your *My Tasks* list. No other user can access the task. This is useful if you want to make sure that you own the task but want to complete it at a later time.
   - *Unclaim*: Releases the task and returns it to the *Unclaimed* list.
3. If you clicked *Review*, you can review or change the business service details, including the workload details using one of these options:
   - *Add*: Opens a list of workload templates where you can select an additional template to add and configure for the business service request.
   - *Edit*: Lets you edit the configuration details of the selected workload.

- *Remove*: Deletes the selected workload from the business service change request.
- *Copy*: Lets you create copies of the selected workload.

You can also select *Claim*, *Reboot Now*, or *Schedule Reboot* from this Review Task dialog box, as explained in Step 2.

IX Reports

The following sections provide information to help you generate reports:

53 Report Descriptions

Cloud Manager provides nine reports that provide information about business service costs, resource usage, organizations, and zones.

As a Cloud Administrator, you can generate all nine reports with an unlimited scope (all organizations, zones, business services, and so forth). Other roles can generate specific reports, as indicated in the following table, with a limited scope as determined by their roles.

For example, you can generate a Business Service Cost Details report for any organization, while an Organization Manager can generate the same report but only for his or her organization.

Report Name	Description
Business Service Cost Details	The cost details for each business service in an organization, organized by business group. Can be generated by: Cloud Administrator, Organization Manager, Sponsor, Business Service Owner, Business Group Viewer
Business Service Cost History	The history of all cost changes for each business service in an organization, organized by business group. Can be generated by: Cloud Administrator, Organization Manager, Sponsor, Business Service Owner, Business Group Viewer
Business Service Cost Summary	A summary of the setup, monthly, annual, and contract costs for all business services in an organization, organized by business group. Can be generated by: Cloud Administrator, Organization Manager, Sponsor, Business Service Owner, Business Group Viewer
Cloud Business Service Cost Details	The cost details for each business service in every organization, organized by organization and then business group. Can be generated by: Cloud Administrator
Organization Overview	A summary of the number of users, business groups, resource groups, business services, and workloads in the organization, along with the monthly and annual business service costs. Can be generated by: Cloud Administrator
Resource Group Details	A summary of the resource groups in a zone. Can be generated by: Cloud Administrator, Zone Administrator
Shared Storage Details	The details (such as capacity, used and free space, and stored VMs and templates) for all shared storage devices in a zone. Can be generated by: Cloud Administrator, Zone Administrator

Report Name	Description
Shared Storage Summary	A summary of the shared storage devices in a zone. Can be generated by: Cloud Administrator, Zone Administrator
Zone Overview	A summary of the number of resource groups, hosts, clusters, workloads, workload templates, networks, and storage devices in a zone. Can be generated by: Cloud Administrator, Zone Administrator

54 Generating Reports

Roles that Can Perform This Task: Cloud Administrator, Zone Administrator, Organization Manager, Sponsor, Business Service Owner, Business Group Viewer

You can generate reports in PDF, CSV, and XLS format. Generated reports are saved in your *My Reports* list until you delete them. For descriptions of the reports, see Chapter 53, "Report Descriptions," on page 185.

To generate a report:

1. On the main navigation bar, click  *Reports*.
2. Click *Generate* to display the Reports dialog box.
3. In the *Report Templates* list, select the report you want to generate and the format you want, then click *Next*.
4. In the Report Parameters dialog box, select the organization or zone for which to generate the report, then click *Generate*.

   A report window appears. Depending on the amount of data to be collected, the report might be completed quickly or it might take a while. As soon as the report is completed, it is displayed in the report window, saved to your computer, opened in an associated application, or you are prompted about which action you want to take (depending on your browser configuration).

   If the report is taking a while, you can close the report window and the report continues to generate. If you close the report, its status is shown in the *My Reports* list. As soon as it is complete, you can view it.

A Setting Up Cloud Manager to Log to a Sentinel Collector

NetIQ has created a Sentinel Collector to provide data capture capabilities for NetIQ Cloud Manager Application Server . Sentinel must be installed and operational before attempting to use this Collector.

The Collector parses, normalizes, and enhances records received from a data source (known as an Observer). Other Event Source Management (ESM) components like Connectors and Collector Managers perform functions such as remote protocol connections and data mapping. To learn more about Sentinel and its components, see the NetIQ Sentinel product page (http://www.netiq.com/products/sentinel/index.asp) or the NetIQ Sentinel product documentation (https://www.netiq.com/documentation/sentinel70/).

You can download a custom-built Sentinel Collector plug-in for Cloud Manager at the Sentinel Plug-ins Web site (http://support.novell.com/products/sentinel/secure/sentinelplugins.html). The site also has a link to download documentation for the Cloud Manager Collector.

If you choose to use this Collector, you need to configure Cloud Manager to send its syslog information to the Collector. Use the following steps to set up Cloud Manager.

1 At the Cloud Manager Application Server, modify the file: `/opt/netiq/cloudmanager/etc/cmauditlogger.properties`.

1a In the properties file, change the following line

```
log4j.appender.CMSYSLOG.layout.ConversionPattern=%m\n
```

to look like this:

```
log4j.appender.CMSYSLOG.layout.ConversionPattern=NQ_CloudManager: %m\n
```

1b In the properties file, change the current audit location line

```
log4j.category.com.novell.cm.audit.api.impl.AuditLogger=INFO, CMFILE
```

to look like this:

```
log4j.category.com.novell.cm.audit.api.impl.AuditLogger=INFO, CMFILE,
CMSYSLOG
```

1c (Optional) If you don't want the local audit file, change the current audit location line

```
log4j.category.com.novell.cm.audit.api.impl.AuditLogger=INFO, CMFILE
```

to look like this:

```
og4j.category.com.novell.cm.audit.api.impl.AuditLogger=INFO, CMSYSLOG
```

1d Save the properties file and restart the Application Server.

2 At the Cloud Manager Application Server, configure syslog to receive messages from the Application Server and then send it to the Sentinel server. To do this, modify the file: `/etc/syslog-ng/syslog-ng.conf`.

2a In the syslog file, add a new source. For example:

```
source r_src { udp(ip("localhost") port(514)); };
```

2b (Conditional) If other services are already logging locally over UDP, you can add a filter line in the syslog file. For example:

```
filter f_ncm        { facility(syslog) and match('NQ_CloudManager:'); };
```

NOTE: The `syslog` value shown for the facility in the line above should match the value for the facility specified in the `cmauditlogger.properties` file. The default is `syslog`.

2c In the syslog file, create a destination and log entry for syslog. For example:

```
destination sentinel { tcp("###.###.###.##" port(1468)); };
log { source(r_src); filter(f_ncm); destination(sentinel); };
```

NOTE: The port number shown in the first line above must match the port for the Syslog TCP listener on the Sentinel server.

2d Save the file and restart syslog on the Application Server. On SUSE Linux Enterprise Server 11, the syslog restart command looks like this:

```
/etc/init.d/syslog-ng restart
```

3 Ensure that the Sentinel Collector for NetIQ Cloud Manager Collector is added to Sentinel and that the Syslog TCP connector in Sentinel is configured and running.

B Enabling Rebranding on the Mobile Cloud Manager Clients

If you want users of the iPhone and iPad Cloud Manager clients to see proprietary branding of Cloud Manager, customized for their organization, you need to configure the Cloud Manager Application Server to enable this "rebranding" feature.

B.1 Automatic Rebranding Setup

The Cloud Manager 2.1.1 installation configuration automatically configures the Cloud Manager Application Server to serve up files from `/var/opt/netiq/cloudmanager/webres` and `/var/opt/netiq/cloudmanager/webres/mobile`.

B.1.1 New Installation

Use the following steps to finish the setup of the rebranding feature after the initial Cloud Manager Application Server installation:

1. Copy the proprietary images you want to use to rebrand the mobile clients to `/var/opt/netiq/cloudmanager/webres/mobile`.
2. Restart Cloud Manager services (making sure to clear the cache) using the following command:

   ```
   /etc/init.d/netiq-cloudmanager reload
   ```
3. Make sure you can access one of the rebranded files via a Web browser. For example, `login.png`:

   ```
   https://<server>:8183/resources/mobile/login.png
   ```

NOTE: When you reference Cloud Manager files from a browser or from a mobile client, the files must be referenced explicitly. For example, if you have a file called `acme.jpg` in a `webres/mobile` folder (`/var/opt/netiq/cloudmanager/webres/mobile/acme.jpg`), you cannot browse to it directly. You must browse to it using an explicit URL, similar to one of the following:

- `http://<server_name>:<port>/resources`
- `http://<server_name>:<port>/resources/mobile`

B.1.2 Upgrade

If you are upgrading from Cloud Manager 2.0 or 2.1 to Cloud Manager 2.1.1, the resource path for rebranding is the same path used in the earlier configuration.

B.2 Rebranding the Image Resources

The NetIQ Cloud Manager documentation Web site has some templates of image resources (https://www.netiq.com/documentation/cloudmanager2/resources.zip) that you can download and use to customize your own rebranded images. You need to ensure the following:

- When a graphic designer creates the new brand images, the image size, format, and filename must remain the same. The image resources can help the designer maintain these criteria.

  A subfolder in the `.zip` download includes screen examples that show the images in context.
- When you are finished customizing the images to match your own branding, upload them to the Cloud Manager Application Server.

The mobile device automatically detects the presence of the new images and rebrands itself on launch.