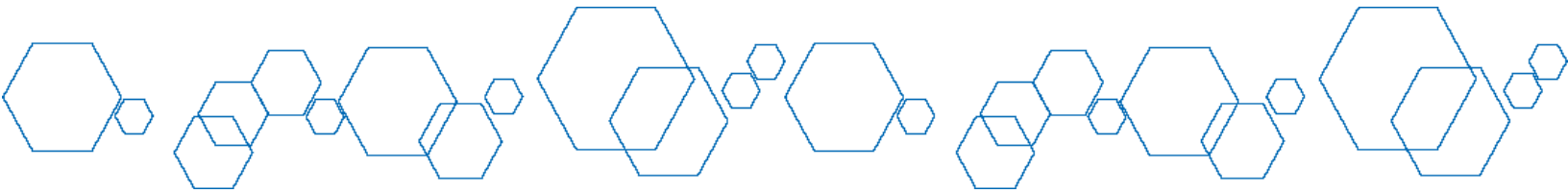
Administration Guide for HyTrust CloudControl®



Version 6.3

January 2021

Copyright and Legal Notice

HyTrust CloudControl® v 6.3

U.S. Patent information: http://www.hytrust.com/patents.

HyTrust, Inc.
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040 U.S.A.
Phone (650) 681-8100

Email: info@hytrust.com
Website: http://www.hytrust.com/
https://twitter.com/HyTrust

Contents

What's New

The following tables provide an overview of the significant changes to this guide for the current release. The tables do not provide an exhaustive list of all changes made to the documentation or of the new features in the release.

What's New in CloudControl, Version 6.3

Feature	Description	Where Documented
Support for Multi-Factor Authentication	Multi-factor authentication is now supported in CloudControl. You can also create a whitelist for multi-factor authentication, allowing you to connect to vCenter through CloudControl without being prompted for multi-factor authentication.	See About Multi-Factor Authentication on page 123.
System Jobs improvements	The Job Monitoring page has been renamed to the System Jobs page. You can view system jobs, and on some jobs can edit the scheduling, run them immediately, and terminate jobs that have frozen.	See Viewing the System Jobs Page on page 128.
Config Hardening improvements	For vSphere environments, you can now choose either ComputeCollection (VMFolder) or VirtualMachine as a resource constraint, and select resources for a configuration hardening policy at a parent resource level.	See Creating a Configuration Hardening Policy on page 84.

Chapter 1. Introduction

HyTrust CloudControl is a cloud security policy framework (CloudSPF) which provides unified visibility and controls to manage access, standardize and control configuration, and protect various types of workloads running across differing cloud platforms. CloudControl enables automated protection and compliance while minimizing time and resources associated with security and compliance. Seamlessly deployed as a virtual appliance, CloudControl is designed to fit easily within the configuration and architecture of most data centers.

With CloudControl, you can achieve the following:

- Unified Visibility
  - Protects your full technology stack from the underlying cloud infrastructure (AWS or vSphere) to the Kubernetes cluster.
  - Provides unified management dashboards which allow you to see an all-in-one view of your organization's security posture across the full stack and management systems.
  - Helps you understand where your workloads are located with a centralized view of workload inventory across private cloud (vCenter, ESXi, VMs, and datastores) and public cloud (EC2 and S3).
- Unified Policy
  - Consistently enforces security controls in your AWS, vSphere and Kubernetes environment.
  - Allows you to segment your workloads into different security and compliance zones with a patented tagging mechanism.
  - Detects security vulnerabilities and configuration issues to prevent cyber attacks.
- Continuous Compliance
  - Automates configuration hardening and continuously monitors your cloud environments to increase ROI and reduce the costs associated with maintaining compliance.
  - Saves time with comprehensive audit-quality logs and reports of all administrative access to meet regulatory environments, that are displayed on user-friendly dashboards.
  - Provides compliance template models for standards such as PCI-DSS, DISA STIG, NIST 800-53, HIPAA, and GDPR. You can use the templates as is, or create custom templates to align more closely with your unique security and operational requirements.

Chapter 2. Managing Users and Groups

CloudControl supports the following:

- Local Authentication Mode
- Active Directory Authentication

Managing Local Users

CloudControl allows you to use Local Authentication Mode instead of Active Directory Authentication. The local user account gives you full access to CloudControl, but with limited group permissions. At installation, we will create one predefined user/role and three predefined groups, with a password set during configuration.

User	Group
ASC_SuperAdminRole	ASC_SuperAdminGroup
ASC_CloudAdminRole	ASC_CloudAdminGroup
ASC_CloudSecurityAdminRole	ASC_CloudSecurityAdminGroup

Note: You can add or modify the users in a group, but you cannot delete the groups.

Viewing Local Users

From the **Home** tab, select **System > Authentication** to view the Authentication page for Local Authentication Mode. The following information is displayed:

Field	Description
User ID	The ID of the user.
First Name	The first name of the user.
Last Name	The last name of the user.
Groups	The group to which the user belongs.
Last Login Time	The last time the user was logged in to CloudControl.

Adding a Local User

1. From the **Home** tab, select **System > Authentication**.
2. Click the **Add** button.
3. In the Add Local User window, complete the following:

Field	Description
First Name	Enter the first name of the user for this account.
Last Name	Enter the last name of the user for this account.
User Name	Enter the ID name for the local user. The ID must be at least 6 characters long, and can only contain letters, digits and the following special characters: "-","_", "." and "@".
Password	Enter the password for this account. The password must be at least 8 characters and contain at least one lower case letter, one upper case letter, one number, and one special character.
Re-enter Password	Enter the password again.
Groups	Select the group for the user.

4. Click **Add**.

Active Directory Authentication

CloudControl allows you to use Active Directory (AD) for your authentication. Before you can configure AD, you need to create a service account. After it is configured, you can modify your users and groups.

Active Directory Service Account Requirements

CloudControl uses a service account to integrate with Active Directory (AD). The service account has read-only access to the AD server to discover and collect information about the users and their group memberships that operate in the environment protected by CloudControl. This account is used for authorization purposes, and to ensure that the CloudControl instance operates against the proper AD domains.

The CloudControl service account uses the following attributes:

- RootDSE
  - ldapServiceName
  - configurationNamingContext
  - rootDomainNamingContext

    - defaultNamingContext
- Configuration Naming Context
    - nETBIOSName
    - dnsRoot
- Domain
    - canonicalName
    - msDS-PrincipalName
- User
    - cn
    - distinguishedName
    - sAMAccountName
    - mail
    - memberOf
    - userPrincipalName
- Group
    - cn
    - distinguishedName
    - sAMAccountName
    - mail
    - member
- Site
    - cn
    - distinguishedName
    - siteObjectBL
- SiteLink
    - cn
    - distinguishedName
    - siteObjectBL

If needed, work with your AD administrator to configure these permissions for the CloudControl service account. We recommend setting the 'Protect object from accidental deletion' option in the CloudControl service account properties.

Creating the Active Directory Service Account

1. Log in to the Windows host machine running your AD server using credentials that have sufficient privileges to create new accounts.
2. In AD, add a new user to serve as the CloudControl service account, for example htaServiceAccount.

   Important: You must create a unique service account. Do not use a built-in Administrator account as a service account. The service account may be located in any container or organizational unit. For example, you could use htaServiceAccount as the Service OU, place users in the Users OU, and place CloudControl groups in the Groups OU.
3. Click **Next**.
4. When you are asked to assign the password to the new service account, perform the following:
   - Enter the password in the Password and Confirm password fields.
   - Deselect the User must change password at next logon checkbox.
   - Select the Password never expires checkbox.
5. Click **Next**.

Configuring Active Directory

Before you configure CloudControl to use Active Directory, you must add a CloudControl service account and grant it the proper privileges. If you have already enabled Local Authentication, then it will be disabled when you configure Active Directory.

1. From the **Home** tab, select **System > Primary Authentication**.
2. Click **Configure Active Directory Now** to start the Configure Active Directory wizard.
3. In the confirmation box, click **OK**.
4. On the Details page of the Configure Active Directory wizard, enter the following:

Field	Value
Configuration Method	Choose whether to use Automatic or Manual configuration.
Domain Name	Enter the default domain name to use with Active Directory.
Security	Choose whether to use SSL or no security. This is for automatic configuration only.
Account	Enter the name of the service account that you created.
Password	Enter the password for the service account.

5. Click **Continue**.

6. If you selected Automatic configuration, do the following:
   a. On the Domains page of the Configure Active Directory wizard, verify the domain that you want to use. The default domain is displayed with a star icon.

      Important: CloudControl automatically adds all of the discovered domain controllers and global catalogs, starting with the closest. If you have a large number, then this will be done in the background. If the domain that you want to use is not visible, and you do not want to wait, then we recommend that you complete the configuration process, then edit your AD configuration later.

   b. Optionally edit the domain controllers and global catalog.

   c. Click **Continue** and proceed to step 8.

7. If you selected Manual configuration, do the following:
   a. On the Details page of the Configure Active Directory wizard, click **Add a Domain Controller Now** or the **Create** button and complete the following:

      Important: The same domain controller must be entered as both a Domain Controller and as a Global Catalog.

Field	Value
Name	Enter the domain controller name.
Security	Select whether you want to use no security or SSL.
Port	Enter the port for the domain controller or global catalog.
User Search Context (Base DN)	Enter the Base DN to use for searching users.
Group Search Context (Base DN)	Enter the BASE DN to use for searching groups.

      Note: The Add a Domain Controller Now link is only available the first time you add a domain controller or global catalog.

   b. Click **Add**.

   c. Click the **Create** button to create an additional domain controller, or click **Continue**.

   d. On the Global Catalogs page, click **Add a Global Catalog Now** or the **Create** button and complete the following:

      Important: The same domain controller must be entered as both a Domain Controller and as a Global Catalog.

Field	Value
Name	Enter the domain controller name.
Security	Select whether you want to use no security or SSL.
Port	Enter the port for the domain controller or global catalog.
User Search Context (Base DN)	Enter the Base DN to use for searching users.
Group Search Context (Base DN)	Enter the BASE DN to use for searching groups.

   e. Click **Add**.

   f. Click the **Create** button to create an additional global domain, or click **Continue**.

   g. On the **Add Additional Domains** pop-up, choose one of the following:
      - Click Add Additional Domains if you want to add one or more domains in addition to the default domain.

        On the Additional Domains page, click **Add a Domain Now** or the **Create** button, enter the domain information, and click **Continue**.
      - Click **Skip**.

   h. Click **Close** and proceed to step 8.

8. On the ASC_SuperAdmin Role Mapping page, enter the group name for the ASC_SuperAdmin user.

   The group name is the Active Directory security group name. Select the AD group name that you want to associate with the default role. The group names are automatically populated by CloudControl.

9. Click **Continue**.
10. On the Summary page, review your changes, then click **Apply**.
11. Click **Apply AD settings and Log Out** in the confirmation window.
12. Click **OK** to confirm.

Once the process is complete, you are logged out of CloudControl GUI. You must use your AD credentials to log back in to CloudControl.

Configuring a Second Active Directory Account

Beginning with release 6.2.1, CloudControl now supports two Active Directory accounts.

Before You Begin

Create an Active Directory service account that will be used to authenticate users from the new Active Directory server. For more information, see Active Directory Service Account Requirements on page 14 and Creating the Active Directory Service Account on page 16.

Procedure

1. From the **Home** tab, select **System > Primary Authentication**.
2. On the Authentication page, select Actions > **Add Active Directory**.
3. In the confirmation box, click **Configure Active Directory**.
4. On the Details page of the Configure Active Directory wizard, enter the following:

Field	Value
Configuration Method	Choose whether to use Automatic or Manual configuration.
Set as Default Identify Source	Check the checkbox if you want this Active Directory to be the primary used for lookups. If you do not, then the first Active Directory that was configured in CloudControl will be the primary.
Domain Name	Enter the root domain name to use with Active Directory.
Security	Choose whether to use SSL or no security. This is for automatic configuration only.
Account	Enter the name of the service account that you created for this Active Directory.
Password	Enter the password for the service account.

5. Click **Continue**.

6. If you selected Automatic configuration, do the following:
   a. On the Domains page of the Configure Active Directory wizard, verify the domain that you want to use. The default domain is displayed with a star icon.

      Important: CloudControl automatically adds all of the discovered domain controllers and global catalogs, starting with the closest. If you have a large number, then this will be done in the background. If the domain that you want to use is not visible, and you do not want to wait, then we recommend that you complete the configuration process, then edit your AD configuration later.

   b. Optionally edit the domain controllers and global catalog.

   c. Click **Continue** and proceed to step 8.

7. If you selected Manual configuration, do the following:
   a. On the Details page of the Configure Active Directory wizard, click **Add a Domain Controller Now** or the **Create** button and complete the following:

      Important: The same domain controller must be entered as both a Domain Controller and as a Global Catalog.

Field	Value
Name	Enter the domain controller name.
Security	Select whether you want to use no security or SSL.
Port	Enter the port for the domain controller or global catalog.
User Search Context (Base DN)	Enter the Base DN to use for searching users.
Group Search Context (Base DN)	Enter the BASE DN to use for searching groups.

      Note: The Add a Domain Controller Now link is only available the first time you add a domain controller or global catalog.

   b. Click **Add**.
   c. Click the **Create** button to create an additional domain controller, or click **Continue**.
   d. On the Global Catalogs page, click **Add a Global Catalog Now** or the **Create** button and complete the following:

      Important: The same domain controller must be entered as both a Domain Controller and as a Global Catalog.

Field	Value
Name	Enter the domain controller name.
Security	Select whether you want to use no security or SSL.
Port	Enter the port for the domain controller or global catalog.
User Search Context (Base DN)	Enter the Base DN to use for searching users.
Group Search Context (Base DN)	Enter the BASE DN to use for searching groups.

   e. Click **Add**.
   f. Click the **Create** button to create an additional global domain, or click **Continue**.
   g. On the **Add Additional Domains** pop-up, choose one of the following:
      - Click Add Additional Domains if you want to add one or more domains in addition to the default domain.

        On the Additional Domains page, click **Add a Domain Now** or the **Create** button, enter the domain information, and click **Continue**.
      - Click **Skip**.
   h. Click **Close** and proceed to step 8.
8. On the Summary page, review your changes, then click **Apply**.

The new Active Directory is added, and you can now choose between them by using the Active Directory drop-down at the top right of the Authentication page.

Viewing your Active Directory Settings

The Authentication page displays all the information for your Active Directory configuration. All of the information can be modified.

Note: If you have configured two Active Directories, only one is shown at a time. Use the Active Directory drop-down at the top right to select the Active Directory that you want to view. The Active Directory with a star is the default identify source.

All user names are normalized in the format **<name>@<domain>** before they are displayed in the CloudControl GUI.

Note: If you modify any information on a tab, you must click **Apply** to save your changes before you view a different tab. Otherwise CloudControl will prompt you to save or discard your changes, or cancel changing tabs.

Service Account tab

Displays the current service account used to integrate with Active Directory.

To modify, enter the new service account and the password, reconfirm the password, and click **Apply**.

Domains tab

Displays the domain, the domain controllers, and the global catalogs used to find the users and groups for authentication purposes.

- To modify your existing settings, click the domain link, or select the domain and click the **Edit** button.
- To add a new domain, domain controller and global catalog, click the **Add** button.

When finished making changes, click **Apply**.

ASC_SuperAdmin Role Mapping tab

Displays the information for the ASC-SuperAdmin role. To update the role mapping, you must update the Root trust manifest. See About Access Control Policies on page 60.

Advanced tab

Displays the following:

- User-To-Group Map Cache Timeout (minutes)—Configures how long CloudControl will cache the mapping of group memberships for a user before freshly discovering the mappings from the directory service. Valid entries are from 1 minute to 1440 minutes.

  We recommend that you use the default value of 5 minutes.

- Enable Nested Group Search—When disabled, CloudControl discovers only direct group memberships. When enabled, CloudControl builds a list of both direct and nested group memberships by searching recursively within any nested groups that are used in any existing Rules.

  The default setting is enabled. Leave set to enabled if you have nested groups in your Directory Service or in any existing Rules and require recursive searching.

  If recursive searching of nested groups is not required, you can disable this to improve query efficiency.

  Select **Refresh > Refresh User-to-Group Map Cache** to force change updates in between your scheduled User-to-Group Map Cache Timeout. This allows you to set a longer cache period and manually refresh when needed.

- Nested Group Map Cache Timeout (minutes)—If Enable Nested Group Search is enabled, this configures how long CloudControl will cache recursive group memberships (groups that are contained within other groups) that are used in existing Rules before freshly discovering the mappings from the directory service. Valid entries are from 10 minutes to 1440 minutes, and the default value is 60 minutes.

  Select **Refresh > Refresh Nested Group Map Cache** to immediately refresh the nested group map cache.

- Domain Controllers Status Refresh Interval (minutes)—Configures how long CloudControl will cache the domain controller status before freshly discovering the status from the directory service. Valid entries are from 1 minute to 525600 minutes, and the default is 1440 minutes.

  Select **Refresh > Run Domain Controller Status Refresh** to immediately refresh the domain controller status.

- Discovery Service Refresh (minutes)—For Automated Discovery only, specify the time interval in minutes at which Active Directory settings will be re-discovered. Valid entries are from 30 minutes to 525600 minutes, and the default is 1440 minutes.

- Select **Refresh > AD Configuration Refresh** to force the system to search for new domain controllers and global catalogs for existing domains.

Actions menu

On the Actions menu, you can select one of the following:

- **Actions > Change to Manual Mode**—If you are in Automated Discovery mode, allows you to change to manual mode.
- **Actions > Change to AD Mode**—If you are in manual mode, allows you to change to Automated Discovery mode.
- **Actions > Reconfigure Active Directory**—Allows you to completely change your AD settings.
- **Actions > Add Active Directory**—Allows you to configure a second Active Directory. The limit is 2.
- **Actions > Remove Active Directory**—If you have two Active Directories, you can remove one of them. The current Active Directory shown in the Authentication window is the one that will be removed.

Chapter 3. Managing vSphere

About vSphere

When you add vSphere to CloudControl, you can protect your vCenters and ESXi hosts. CloudControl has organized your vSphere inventory into the following categories to help you find your information:

- Management: vCenters
- Compute (hosts, datacenters, clusters, virtual machines, and folders)
- Network (switches, network, port groups, and folders)
- Storage (datastores and folders)

Adding vCenters to CloudControl

CloudControl learns about your vSphere environment when you add a vCenter.

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, select **Actions > Add vCenter**.

   Note: If there are no vCenters in your system, you can also click the **Add vCenter** link on the **vSphere** page.

3. On the About page, specify the following:

Field	Value
IP/FQDN	Enter the vCenter IP address or FQDN.
Port	Enter the port used for the vCenter, or accept the default.
Service Account	The vCenter service account to be used for CloudControl. The same account must be used across all vCenter Servers, and it must have administrator privileges.
Service Account Password	The password for the vCenter service account.

4. On the Configure page, view and approve the certificates for the Platform Services Controller (PSC) and all vCenters that were discovered. The Approve checkbox must be checked for all certificates before you can add the vCenter.
   - Certificates from a trusted source have the Approve checkbox checked automatically.
   - Click the **Certificate** link to view the certificate details. Click **Approve** to populate the approve checkbox for the certificate, or click the **x** icon to close the window.
   - Certificates without a certificate authority are displayed with a warning icon. Click the link in the tool tip to add a CA. For more information, see Installing a Certificate Authority on page 115. You can manually approve these certificates by checking the Approve checkbox.
   - Certificates that are invalid or expired are displayed with an error icon. These certificates cannot be approved.

   All vCenter and PSC certificates are displayed on the Certificate Authorities tab on the Certificates page.
5. Determine if you want to use a single Published IP for each vCenter or a Published IP Range to be used for all current and future vCenters in this ELM.

   Important: If you plan to use Access Control, you must have a Published IP address or range.
   - For a Published IP, click the **Configure** link in the Published IP column of the vCenter table, enter the Published IP Address and Netmask, and click **Apply**.
   - For a Published IP Range, enter the Published IP Address and Netmask in the Published IP Range section.
6. When all certificates are approved, click **Continue**.

   Note: You cannot click **Continue** until all of the Approve checkboxes are checked.
7. On the **Details** page, you can monitor the process as all of your vSphere information is collected.
8. Click **Continue**.
9. On the Onboard Hosts page, you can view the hosts that were discovered, remove hosts, or add additional hosts to be added to CloudControl. Select the hosts that you want to add and click **Onboard Hosts**.

   You must add hosts before you can run Configuration Hardening policies (assessment and remediation) against your hosts.

10. On the Hosts Credentials page, you can add or import the credentials for your ESXi hosts.
    - To add credentials:
      a. Select one or more ESXi hosts that share the same credentials and click **Add Credentials**.
      b. In the Add Host Credentials window, enter the User Name and Password for the ESXi hosts and click **Apply**.

      The Credentials column for each host displays the status. This can be one of the following:
      - Missing
      - Valid
      - Invalid
    - To import credentials, you will need to upload a CSV file in the following format:
      `ESXINAME, PASSWORD, USERNAME`
      a. Select one or more ESXi hosts that share the same credentials and click **Import Credentials**.
      b. Select the file that you want to import and click **Continue**.
      c. Review the summary on the Discovered page.
      d. Click **Apply**.

    Important: If you do not add the credentials, then you cannot run Configuration Hardening policies (assessment and remediation) against your hosts.
11. After you have added the credentials, you can enable Global PIP. Global PIP is disabled by default. For more information, see Enabling and Disabling Global PIP on page 29.
12. Click **Continue**.
13. Click **Done** to view the dashboard for the newly added vCenters.

What to Do Next

- Review your vSphere inventory (See Viewing vSphere Inventory below)
- View the Certificate Authorities that have been imported (See Viewing Certificate Details on page 111)

Viewing vSphere Inventory

From the **Home** tab, select **Inventory > vSphere** to view the vSphere page. From here, you can view in depth information of all vSphere resources, as well as any tags or policies related to those resources. This information is displayed in a dashboard or a resource page.

Note: You need to add a vCenter before you can view any information. See Adding vCenters to CloudControl on page 24.

Dashboard Pages

Dashboard pages are a visual overview of your resources and their security postures. For vSphere, you can view the global dashboard, and dashboards for each vCenter, virtual machine, and host.

The dashboard pages display the following information:

- An overview of all vSphere resources discovered by CloudControl.
- Current configuration hardening status in a pie chart.
- Recent history of your configuration hardening activities. You can view either assessment or remediation results. Clicking on the different links shows you the following information:
  - Click the date and time link to see the assessment that was completed at that time.
  - Click the template name link to view the details of the particular template.
  - Click the policy name link to view details about the policy.
  - Click the ESXi host name to view details about that host.
- Trending information about your configuration hardening posture.

Click the expander icon in each tile to open the Views page with detailed information. You can also click the options under the **Views** menu. From the Views page, you can click the **x** icon to return to the original location.

Resource Pages

Each resource page displays a list of the resources for each type, along with other important information per resource, such as details and tags. You can also use the **Actions** menu to assign and unassign tags to a selected resource.

Most of the table cells have links that you can click to view additional information. Depending on the type of resource, it will either open a new tab (for example, clicking a name in the Name column of a vCenter), or it will open a pop-up window on the same page (for example, clicking on the links in the DataCenters column).

The following vSphere resources have their own resource pages and sub pages:

- Management: vCenters
- Compute (hosts, datacenters, clusters, virtual machines, and folders)

  Note: The hosts resource page also displays the following:
  - For configuration hardening, CloudControl displays an icon that immediately lets you see the configuration hardening of the host. If the host has not been assessed, the icon is grey. If the configuration hardening templates run against the host are above the global compliance threshold, then the icon is green. If the configuration hardening templates run against the host are below the global compliance threshold, then the icon is red.
  - For trust attestation, CloudControl displays a green check for hosts that are trusted, and a red x for hosts that are not trusted.
- Network (switches, network, port groups, and folders)
- Storage (datastores and folders)

Editing or Importing Credentials for ESXi Hosts

You can edit the credentials for one or more ESXi hosts at a time.

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Compute** link, and then click the **Hosts** link.
3. Select the ESXi host or hosts to which you want to add or import credentials.
   - To edit credentials:
     a. Select one or more ESXi hosts that share the same credentials and click **Edit Credentials**.
     b. In the Edit Host Credentials window, enter the User Name and Password for the ESXi hosts and click **Apply**.

        The Credentials column for each host displays the status. This can be one of the following:
        - Missing
        - Valid
        - Invalid
   - To import credentials, you will need to upload a CSV file in the following format:
     `ESXINAME, PASSWORD, USERNAME`
     a. Select one or more ESXi hosts that share the same credentials and click **Import Credentials**.
     b. Select the file that you want to import and click **Continue**.
     c. Review the summary on the Discovered page.
     d. Click **Apply**.

Sync vSphere Inventory

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the vSphere page, click the vCenters link.
3. Select the vCenter or vCenters that you want to sync.
4. Select **Actions > Sync Inventory**.
5. Click **OK** to refresh vCenter inventory.

Navigating vSphere Inventory Pages

The Views pages allow you to view in depth information on your inventory.

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the vSphere page, click **Views** and select one of the following:
   - **Resources** to view all resources under the specified object.
   - **Current Configuration Hardening** to view the current configuration hardening activities.
   - **Configuration Hardening Activity** to view all configuration hardening activities.
   - **Configuration Hardening Policies** to view all configuration hardening policies.
3. Click the **x** icon to return to your original location.

Global Published IP Address

You can now use a Global published IP address (Global PIP) to access your protected ESXi hosts when using the CloudControl proxy. With Global PIP, instead of individual IP addresses, one IP address is created for all of your ESXi hosts to use when you proxy SSH access to ESXi and ESXi Web GUI. Once the hosts are added to CloudControl with valid credentials, Global PIP ports are allocated for each host.

Each host is allocated four ports to distinguish them from other hosts. The ports are used for the following:

- HTTP traffic
- HTTPS traffic
- SSH traffic
- Open VM Console

The range of ports to be used is from 49152 to 65535. The unused ports are stored in a port pool. We recommend that you do not manually close any of the ports in this range and that you do not use the ports for any other purpose.

You can enable Global PIP when you originally add vSphere and your ESXi hosts to CloudControl, or at a later time. Once Global PIP is enabled, it is enforced for all ESXi hosts that have been added to CloudControl. If you add additional hosts to the vCenter, if they have valid credentials they will automatically be allocated ports. If a host does not have valid credentials, then the Global PIP ports are not allocated and you cannot access the proxy.

Important: You cannot use the VMware Remote Console (VMRC) to access the virtual machine's remote consoles using the ESXi UI with a Global PIP. Use the web browser instead.

Enabling and Disabling Global PIP

You can enable or disable Global PIP from the vSphere Inventory page.

Enabling Global PIP

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Compute** link.
3. On the Compute tab, click the Hosts link.

4. On the Hosts page, next to the Actions button, click the Global PIP **Disabled** link.
   Alternatively, you can select one or more hosts and select **Actions > Manage Global PIP**.
5. In the Manage Global PIP window, do the following:
   a. Set the Status to **Enabled**.
   b. In the Global PIP / FQDN field, enter the IP address or FQDN to use for the Global PIP.
   c. Enter the Netmask.
   d. Check the confirmation checkbox.
   e. Click **Apply**.

   Global PIP is now enabled for all hosts that have been added to CloudControl. Click **Download CSV** to download a CSV file that contains the details of all assigned ports.

Disabling Global PIP

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Compute** link.
3. On the Compute tab, click the Hosts link.
4. On the Hosts page, next to the Actions button, click the Global PIP **Enabled** link.
   Alternatively, you can select one or more hosts and select **Actions > Manage Global PIP**.
5. In the Manage Global PIP window, do the following:
   a. Set the Status to **Disabled**.
   b. Check the confirmation checkbox.
   c. Click **Apply**.

Viewing Assigned Ports for Global PIP

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Compute** link.
3. On the Compute tab, click the Hosts link.
4. On the Hosts page, click on the host that you want to view.
5. On the host dashboard, in the Details section, locate the following section:

Field	Description
Global PIP	Displays the Global PIP status. This can be either Enabled or Disabled.
Proxy Access Ports	If the Global PIP status is Enabled and the host credentials are valid, displays the number of proxy ports for the host. Click the number to view the port assignments.

Connecting to an Individual Host Through Global PIP

You can connect to one of your individual protected ESXi hosts through Global PIP using the following methods:

Accessing the Host using the Web Browser

If you have the Global Published IP address and the HTTPS port number, you can directly connect to an individual protected ESXi host using a web browser.

Important: To access the hostmenu, you must have the Compute.VirtualMachine.Manage_ConsoleInteract, Compute.VirtualMachine.View, and Management.Administration.Edit permissions. Add these permissions to the user role in a new access control rule in the trust manifest that is assigned to Appliance Root.

1. Retrieve the Global PIP and the HTTPS port for the ESXi host to which you want to connect. See Viewing Assigned Ports for Global PIP on the previous page.
2. Enter the URL in your browser. The URL uses the following format: https://<Global-PIP>:<HTTPS-port>.
3. Log in using your proxy credentials used to connect to an ESXi host without Global PIP.

Accessing the Hostmenu using the Web Browser

If you have the Global Published IP address, but do not know the HTTPS port number, you can directly connect to the hostmenu and then navigate to the specific host.

Important: To access the hostmenu, you must have the Management.CloudPlatform.Login and CloudControl.Inventory.View_GPIP permissions. Add these permissions to the user role in a new access control rule in the trust manifest that is assigned to Appliance Root.

1. Retrieve the Global PIP for your ESXi hosts.
2. Enter the URL in your browser using the following format: https://<Global-PIP>/hostmenu.
3. Log in using your proxy credentials used to connect to an ESXi host without Global PIP.

Accessing the Host Directly using SSH

If you have the Global Published IP address and the SSH port number, you can directly connect to an individual protected ESXi host using SSH.

1. Retrieve the Global PIP and the SSH port for the ESXi host to which you want to connect. See Viewing Assigned Ports for Global PIP on the previous page.
2. Open your SSH client.
3. Connect to the Global PIP assigned to the host to which you want to connect, using the specific port number for that host.

   For example, SSH to <Global-PIP>:<SSH-port>
4. Log in using your proxy credentials used to connect to an ESXi host without Global PIP.

Accessing the Host using the CLI Host Menu

If you do not have the SSH port number, you can establish an SSH connection and then use the command line menu to navigate to the desired host. You must have the Management.CloudPlatform.Login privilege to connect to the ESXi hosts.

1. Open your SSH client.
2. Connect to the Global PIP assigned to the host to which you want to connect, using the standard port 22.
3. Log in using the following credentials:
   - Username—**sshuser**
   - Password—**hytrust**

   Important: These credentials only establish the SSH connection. They do not provide shell access to your ESXi hosts.
4. At the CLI prompt, enter the proxy credentials used to connect to an ESXi host without Global PIP.
5. In the SSH Menu, navigate to the host that you want to access.

   The path should be similar to the following:

   SSO Domains > <*SSO_Domain_name*> > <*PSC_name*> > <*vCenter_name*> > <*Host_name*>
6. Enter your text at the command line prompt.

Refreshing Trust Status of your TPM Hosts

You can manually refresh the trust status of your TPM hosts.

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the vSphere page, click the vCenters link.
3. On the Compute tab, click the Hosts link.
4. On the Hosts page, click on a TPM host.
5. On the host dashboard, select **Actions > Refresh Trust Status**.

The trust status will automatically refresh.

Chapter 4. Managing NSX-T

About NSX-T

VMware NSX-T Data Center is a network virtualization platform that provides an agile software-defined infrastructure to build cloud-native application environments. NSX-T Data Center is focused on providing networking, security, automation, and operational simplicity for emerging application frameworks and architectures that have heterogeneous endpoint environments and technology stacks.

CloudControl has organized your NSX-T inventory into the following categories to help you find your information:

- NSX-T Data Centers
- System (NSX managers, compute managers, clusters, nodes, transport zones)
- Networking (switches, load balancers, DHCP servers, VPN servers)
- Distributed Firewalls
- Gateway Services (routers and gateways, gateway firewall)
- Groups (security groups, IP sets, MAC sets, IP pools)

Adding an NSX-T Data Center to CloudControl

CloudControl learns about your NSX-T environment when you add a NSX-T Data Center.

1. From the **Home** tab, select **Inventory > NSX-T**.
2. On the **NSX-T** page, select **Actions > Add NSX-T Data Center**.

   Note: If there are no NSX-T Data Centers in your system, you can also click the **Add NSX-T Data Center** link on the **NSX-T** page.

3. On the About page, specify the following:

Field	Value
IP/FQDN	Enter the NSX-T Data Center address or FQDN.
Port	Enter the port used for the NSX-T Data Center, or accept the default.
Service Account	The NSX-T Manager service account to be used for CloudControl. The account must be used across all NSX-T Managers, and it must have enterprise administrator privileges.
Service Account Password	The password for the NSX-T Manager service account.
Proxy - Published IP/FQDN	The IP address or FQDN to use to route all traffic to this NSX-T Data Center.
Proxy - Published Netmask	The subnet mask to use to route all traffic to this NSX-T Data Center.

4. Click **Continue**.
5. Review the Certificate Details and click **Approve**.
6. On the **Details** page, you can monitor the process as all of your NSX-T information is collected.
7. Click **Continue** to view the dashboard for the newly added vCenters.

What to Do Next

- Review your NSX-T inventory (See Viewing NSX-T Inventory below)

Viewing NSX-T Inventory

From the **Home** tab, select **Inventory > NSX-T** to view the NSX-T page. From here, you can view in depth information of all NSX-T resources, as well as any tags or policies related to those resources.

Note: You need to add NSX-T before you can view any information. See Adding an NSX-T Data Center to CloudControl on the previous page.

Dashboard Pages

Dashboard pages are a visual overview of your resources and their security postures. For NSX-T, you can view the global dashboard for all of your NSX-T Data Centers.

The dashboard pages display the following information:

- An overview of all NSX-T resources discovered by CloudControl.
- Current configuration hardening status in a pie chart.

- Recent history of your configuration hardening activities. You can view either assessment or remediation results. Clicking on the different links shows you the following information:
  - Click the date and time link to see the assessment that was completed at that time.
  - Click the template name link to view the details of the particular template.
  - Click the policy name link to view details about the policy.
  - Click the ESXi host name to view details about that host.
- Trending information about your configuration hardening posture.

Each page displays a list of the resources for each type, along with other important information per resource, such as details and tags. You can also use the **Actions** menu to assign and unassign tags to a selected resource.

The following NSX-T resources have their own resource pages and sub pages:

- NSX-T Data Centers
- System (NSX managers, compute managers, clusters, nodes, transport zones)
- Networking (switches, load balancers, DHCP servers, VPN servers)
- Distributed Firewalls
- Gateway Services (routers and gateways, gateway firewall)
- Groups (security groups, IP sets, MAC sets, IP pools)

Editing an NSX-T Data Center

1. From the **Home** tab, select **Inventory > NSX-T**.
2. On the **NSX-T** page, select the NSX-T Data Center that you want to edit.
3. Select **Actions > Edit NSX-T Data Center**.
4. On the Edit NSX-T Data Center page, you can modify the following:

Field	Value
Friendly	The Friendly Name for the NSX-T Data Center
Service Account	The NSX-T Manager service account to be used for CloudControl. The account must be used across all NSX-T Managers, and it must have enterprise administrator privileges.
Service Account Password	The password for the NSX-T Manager service account.
Proxy - Published IP/FQDN	The IP address or FQDN to use to route all traffic to this NSX-T Data Center.
Proxy - Published Netmask	The subnet mask to use to route all traffic to this NSX-T Data Center.

5. Click **Apply**.

What to Do Next

- Review your NSX-T inventory (See Viewing NSX-T Inventory on page 34)

Sync NSX-T Inventory

1. From the **Home** tab, select **Inventory > NSX-T**.
2. On the **NSX-T** page, select the NSX-T Data Center that you want to sync.
3. Select **Actions > Sync Inventory**.
4. Click **OK** to refresh the inventory.

Removing an NSX-T Data Center from CloudControl

1. From the **Home** tab, select **Inventory > NSX-T**.
2. On the **NSX-T** page, select the NSX-T Data Center that you want to remove.
3. Select **Actions > Remove NSX-T Data Center**.
4. In the confirmation box, check the 'Are you sure you want to remove <NSX-T_IP>?' checkbox and click **Remove**.

Chapter 5. Managing Kubernetes and OpenShift Clusters

About Kubernetes Clusters

A cluster is a set of machines, called nodes, that run containerized applications managed by a container orchestration platform, such as Kubernetes. CloudControl protects the following objects for each Kubernetes cluster:

- Nodes—Worker machines in Kubernetes. Each node represents a single machine, for example, a physical machine in a datacenter, or a virtual machine hosted on a cloud provider.
- Namespaces—A virtual cluster backed by the same physical cluster. Resource names must be unique within a namespace, but not across multiple namespaces.
  - Deployments—Define how to create and update application instances, and monitors the application after it has been created.
  - Pods—A group of one or more containers with shared storage, a network IP, and specific rules that govern how a container should run. Pods should be run as a single instance, and can be replicated to run multiple instances.
    - Containers—The lowest level of a micro-service which holds the running application, the libraries and their dependencies.
  - Services—Define a logical set of pods and a policy by which to access them.

This is the same whether you are using kubeadm, kops, or Red Hat OpenShift to manage Kubernetes.

Kubernetes Prerequisites

- CloudControl uses a service account to integrate with Kubernetes. Each cluster requires its own service account with full admin privileges on most Kubernetes resources.

  We recommend that you create a service account with the cluster-admin role, which allows super-user access to perform any action on any resource.
- If your Kubernetes clusters are running on-premises, the root account must be enabled on the master (API server) node, so that CloudControl can configure a webhook.
- If your Kubernetes clusters are running on the cloud (as an EC2 on AWS) and CloudControl is also running on AWS (deployed from an AMI), you must do the following:
  - The root account must be enabled on the master (API server) node, so that CloudControl can configure a webhook.
  - Security Groups (both in-bound & out-bound) rules must be configured between Kubernetes master (or load balancer) and CloudControl for the following ports: API, SDK, and SSH.
- CloudControl supports Kubernetes versions 1.17 and above in a single master mode.
- The Kubernetes master must be able to ping the CloudControl IP with port 443.
  - When CloudControl is running as a Virtual Appliance for OVA, the IP is the node IP for a standalone node, or the VIP for a cluster.
  - When CloudControl is running as an AWS Cloud Appliance, use the private IP found on the Description tab for the CloudControl EC2 instance.
- The Kubernetes master (API server) must be running. For a systemd-based setup, this will be a service. For a containerized setup (KOPS or KUBEADM), this will be a kube-apiserver pod.
- The master node must be visible in CloudControl to use a tag-based configuration hardening policy. Ensure that the 'kubectl get nodes' command shows the master node with the label 'master'.
- Using deployment control requires the following:
  - For a KOPS or Kubeadm cluster, the "ValidatingAdmissionWebhook" must be enabled before you add the cluster. This is not required for systemd.
  - For all clusters, your DNS must be configured to allow two-way communication between the cluster and CloudControl before you add the cluster.

OpenShift Prerequisites

- CloudControl supports OpenShift version 3.11.
- The OpenShift master (API server) must be running as a k8s_apiserver pod.
- The OCR (OpenShift Container Registry) is automatically added or removed with your OpenShift clusters. You cannot add an OCR using the same process as you would an image registry. OCRs can only be added as a part of their corresponding OpenShift cluster.

- Before you add an OpenShift cluster, your DNS must be configured so that CloudControl can connect to the corresponding OCR using the OpenShift route for the OCR. The format should be **`docker-registry-default.<domain.com>`**.
- OpenShift users must have the following privileges for CloudControl to fetch OpenShift cluster inventory and the OCR:
  - oc adm policy add-role-to-user system:registry <username>
  - oc adm policy add-role-to-user admin <username>
  - oc adm policy add-role-to-user system:image-builder <username>
  - oc adm policy add-cluster-role-to-user system:registry <username>
  - oc adm policy add-cluster-role-to-user admin <username>
  - oc adm policy add-cluster-role-to-user system:image-builder <username>
  - oc adm policy add-cluster-role-to-user cluster-admin <username>

  Where <username> is the OpenShift user name to be used when adding an OpenShift cluster.
- Using deployment control with OpenShift requires the following:
  - The "ValidatingAdmissionWebhook" must be enabled before you add the cluster.
  - Your DNS must be configured to allow two-way communication between the cluster and CloudControl before you add the cluster.

Adding a Kubernetes Cluster

CloudControl learns about the container environment when you add Kubernetes clusters.

1. From the **Home** tab, select **Inventory > Kubernetes**.
2. On the **Clusters** page, select **Actions > Add Kubernetes Cluster**.

   Note: If there are no clusters in your system, you can also click the **Add Kubernetes Cluster** link on the **Kubernetes Clusters** page.
3. On the Import page, choose one of the following:
   a. Select the **Import File** radio button, then click **Browse** and choose the kubeconfig file that you want to import.
   b. Select the **Enter Text** radio button, then paste the contents of the kubeconfig file in plain text.

   Note: A kubeconfig file is a configuration file written in YAML that describes the cluster that you want to add.
4. Click **Continue**.
5. On the Clusters page, select the cluster that you want to add and click **Continue**.

   Note: You can only select one cluster.
6. If you have more than one user in the kubeconfig file, select the user that you want to use and click **Continue**.

   CloudControl uses the user name to discover the type of cluster to be added.

7. On the About page, choose your vendor type:
   - For Kubernetes, complete the following:

Field	Value
Friendly Name	Enter the friendly name for the cluster.
SSH Port	Enter the SSH port for the cluster.
Root Access Credentials	Select one of the following radio buttons and enter the required information: • **User Name/Password**—Enter the User Name and Password. • **SSH Key**—Enter the User Name and an SSH key that is not encrypted. **Note:** The user name root is predefined and cannot be modified.

   - For OpenShift, complete the following:

Field	Value
Friendly Name	Enter the friendly name for the cluster.
User	Enter the OpenShift user name.
Password	Enter the OpenShift password.

8. Click **Continue**.
9. On the **Details** page, you can monitor the process.
10. Click **Continue** to view the dashboard for the newly added cluster.

What to Do Next

- View your inventory (See Viewing Kubernetes Inventory below)
- For Kubernetes, add an image registry (See Adding an Image Registry on page 53)

  Note: The OpenShift Container Registry (OCR) is automatically added with your cluster. If you remove the cluster, the OCR is automatically removed as well.
- View your image registries (See Viewing Image Registries on page 53)

Viewing Kubernetes Inventory

From the **Home** page, select **Inventory > Kubernetes** to view the Kubernetes Clusters page. From here, you can view in depth information of all of the objects in that cluster, as well as any tags or policies related to those objects. This information is displayed in a dashboard or a resource page.

Note: You need to add a cluster before you can view any information. See Adding a Kubernetes Cluster on the previous page.

Dashboard Pages

Dashboard pages are a visual overview of your resources and their security postures. For Kubernetes, you can view the global dashboard or a dashboard for each cluster.

The dashboard pages display the following information:

- An overview of all Kubernetes objects globally or for the cluster.
- Current and trending configuration hardening information.
- Recent and trending runtime violations.
- Deployment control overview.
- Cluster details (for cluster-level dashboards). This includes the Platform field which indicates if the Kubernetes cluster is being hosted by another platform. You can click the resource name to view the dashboard for that resource.

Click the expander icon in each tile to open the Views page with detailed information. You can also click the options under the **Views** menu. From the Views page, you can click the **x** icon to return to the original location.

Resource Pages

Each resource page displays a list of the resources for each type, along with other important information per resource, such as details and tags. You can also use the **Actions** menu to assign and unassign tags to a selected resource.

Most of the table cells have links that you can click to view additional information. Depending on the type of resource, it will either open a new tab (for example, clicking a name in the Name column of a Kubernetes cluster), or it will open a pop-up window on the same page (for example, clicking on the links in the Configuration Hardening column).

If the cluster is hosted by another platform, an icon with hover text will be displayed indicating the platform that the cluster resides on, for example, OpenShift or AWS.

Navigating Kubernetes Inventory View Pages

The Views pages allow you to view in depth information on your inventory.

1. From the **Home** tab, select **Inventory > Kubernetes**.
2. On the Kubernetes Clusters page, click **Views** and select one of the following:
   - **Resources** to view all resources under the specified object.
   - **Deployment Control** to view all deployment policies related to the resources.
   - **Container Runtime Violations** to view all container runtime violations related to the resources.
   - **Current Configuration Hardening** to view the current configuration hardening activities.
   - **Configuration Hardening Activity** to view all configuration hardening activities.
     Configuration Hardening Policies to view all configuration hardening policies.
3. Click the **x** icon to return to your original location.

Updating Cluster Configuration

1. From the **Home** tab, select **Inventory > Kubernetes**.
2. On the **Kubernetes Clusters** page, click the Clusters link.
3. Select the cluster for which you want to update the configuration.
4. Select **Actions > Update Configuration**.
5. On the Import page, choose one of the following:
   a. Select the **Import File** radio button, then click **Browse** and choose the kubeconfig file that you want to import.
   b. Select the **Enter Text** radio button, then paste the contents of the kubeconfig file in plain text.
6. Click **Continue**.
7. Select the Kubernetes cluster that you want to add.
8. Click **Continue**.
9. On the About page, specify the following:

Field	Value
Friendly Name	Enter the friendly name for the cluster.
SSH Port	Enter the SSH port for the cluster.
User	Select the user from the drop-down list. If there is only one user in the kubeconfig file, then that value is selected by default.
Root Access Credentials	Select one of the following radio buttons and enter the required information: • **User Name/Password**—Enter the User Name and Password. • **SSH Key**—Enter the User Name and an SSH key that is not encrypted. **Note:** The user name root is predefined and cannot be modified.

10. Click **Continue**.
11. On the Proxy page, select **ON** if you want to configure a proxy, and specify the following:

Field	Value
Proxy URL	Required. Enter the HTPPS URL for the proxy.
Proxy User Name	Enter the user name to use for the proxy.
Proxy Password	Enter the password to use for the user name.

12. Click **Continue**.

Sync Cluster Inventory

1. From the **Home** tab, select **Inventory > Kubernetes**.
2. On the **Kubernetes Clusters** page, click the Clusters link.
3. Select the cluster that you want to sync.
4. Select **Actions > Sync Inventory**.
5. Click **OK** to refresh the cluster inventory.

Remove Cluster

1. From the **Home** tab, select **Inventory > Kubernetes**.
2. On the **Kubernetes Clusters** page, click the Clusters link.
3. Select the cluster that you want to remove.
4. Select **Actions > Remove Cluster**.
5. Click **OK** in the confirmation window.

Chapter 6. Managing AWS Accounts

About AWS Accounts

Amazon Web Services (AWS) is a secure cloud services platform, managed by AWS accounts. Each account can have compute power, database storage, content delivery and other functionality. CloudControl protects the following AWS functionality:

- AWS Account—An Amazon.com account that is enabled to use AWS products.
- Compute—AWS products used for compute, such as Amazon Elastic Compute Cloud (EC2) or Amazon Elastic Container Service (ECS).
- Network—AWS products used for networking, such as Amazon VPC.
- Storage—AWS used for database storage, such as Amazon Simple Storage Service (S3).

AWS Account Prerequisites

Before you can add an AWS Account, you must have the following:

- An IAM user with 'Programmatic access' enabled that has the appropriate privileges to be a CloudControl service user. See AWS Service Account Requirements on the next page.
- The access key ID and secret access key for the account to be added.

- CloudTrail that is configured with a trail that:
  - is enabled.
  - writes all API calls from all regions into a single bucket.

  For more information, see Creating a CloudTrail on page 47.

AWS Service Account Requirements

CloudControl uses a service account in the form of an IAM user to integrate with AWS. This service account is used to discover and collect information about the AWS Account protected by CloudControl.

Note: Each IAM user can only be associated with one AWS Account. If you plan to protect multiple AWS Accounts, you will need an AWS service account for each one.

To create an AWS service account, you must do the following:

1. Create a new IAM user using the name that you want for your service account, for example, htcc-service-user.

   The IAM user must have programmatic access, but do not add any permissions at this time.

   Important: Once created, the Access Key ID and the Secret Access Key are displayed. You must note them now, as the secret key is not displayed anywhere else in AWS. These two keys are required when you add an AWS account to CloudControl.

2. Create a customer-managed policy, and paste the following text under the JSON tab to add the permissions.

   Important: All values must be exactly as shown.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "config:DescribeConfigurationRecorders",
                "config:DescribeConfigurationRecorderStatus",
                "cloudtrail:DescribeTrails",
                "cloudtrail:GetEventSelectors",
                "cloudtrail:GetTrailStatus",
                "cloudtrail:StartLogging",
                "cloudtrail:UpdateTrail",
                "cloudwatch:DescribeAlarmsForMetric",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateFlowLogs",
                "ec2:CreateSecurityGroup",
                "ec2:CreateVpc",
                "ec2:DeleteFlowLogs",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteVpc",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeAddresses",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeFlowLogs",
                "ec2:DescribeHostReservationOfferings",
```

```
"ec2:DescribeHostReservations",
"ec2:DescribeHosts",
"ec2:DescribeImages",
"ec2:DescribeInstances",
"ec2:DescribeInstanceStatus",
"ec2:DescribeMovingAddresses",
"ec2:DescribeNetworkInterfacePermissions",
"ec2:DescribeNetworkInterfaces",
"ec2:DescribeRegions",
"ec2:DescribeReservedInstances",
"ec2:DescribeReservedInstancesListings",
"ec2:DescribeReservedInstancesModifications",
"ec2:DescribeReservedInstancesOfferings",
"ec2:DescribeSecurityGroupReferences",
"ec2:DescribeSecurityGroups",
"ec2:DescribeStaleSecurityGroups",
"ec2:DescribeSubnets",
"ec2:DescribeVpcAttribute",
"ec2:DescribeVpcClassicLink",
"ec2:DescribeVpcClassicLinkDnsSupport",
"ec2:DescribeVpcEndpointConnectionNotifications",
"ec2:DescribeVpcEndpointConnections",
"ec2:DescribeVpcEndpoints",
"ec2:DescribeVpcEndpointServices",
"ec2:DescribeVpcEndpointServiceConfigurations",
"ec2:DescribeVpcEndpointServicePermissions",
"ec2:DescribeVpcPeeringConnections",
"ec2:DescribeVpcs",
"ec2:DescribeVpnGateways",
"ec2:RevokeSecurityGroupEgress",
"ec2:RevokeSecurityGroupIngress",
"ecr:BatchCheckLayerAvailability",
"ecr:BatchGetImage",
"ecr:DescribeImages",
"ecr:DescribeRepositories",
"ecr:GetAuthorizationToken",
"ecr:GetDownloadUrlForLayer",
"ecr:ListImages",
"iam:ChangePassword",
"iam:CreateRole",
"iam:CreateVirtualMFADevice",
"iam:EnableMFADevice",
"iam:GenerateCredentialReport",
"iam:GetAccountPasswordPolicy",
"iam:GetAccountSummary",
"iam:GetCredentialReport",
"iam:GetGroup",
"iam:GetGroupPolicy",
"iam:GetPolicy",
"iam:GetPolicyVersion",
"iam:GetRole",
"iam:GetRolePolicy",
"iam:GetUser",
"iam:GetUserPolicy",
```

```
                "iam:ListAccountAliases",
                "iam:ListAttachedGroupPolicies",
                "iam:ListAttachedRolePolicies",
                "iam:ListAttachedUserPolicies",
                "iam:ListEntitiesForPolicy",
                "iam:ListGroupPolicies",
                "iam:ListGroups",
                "iam:ListGroupsForUser",
                "iam:ListPolicies",
                "iam:ListPoliciesGrantingServiceAccess",
                "iam:ListPolicyVersions",
                "iam:ListRolePolicies",
                "iam:ListRoles",
                "iam:ListUserPolicies",
                "iam:ListUsers",
                "iam:ListVirtualMFADevices",
                "iam:UpdateAccountPasswordPolicy",
                "iam:UpdateRole",
                "kms:DescribeKey",
                "kms:ListKeys",
                "kms:GetKeyRotationStatus",
                "logs:CreateLogDelivery",
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeMetricFilters",
                "logs:PutMetricFilter",
                "logs:UpdateLogDelivery",
                "s3:GetBucketAcl",
                "s3:GetBucketLocation",
                "s3:GetBucketLogging",
                "s3:GetBucketPolicy",
                "s3:GetBucketTagging",
                "s3:GetEncryptionConfiguration",
                "s3:ListAllMyBuckets",
                "s3:ListBucketByTags",
                "s3:PutBucketLogging",
                "s3:PutObject",
                "sns:ListSubscriptionsByTopic"
            ],
            "Resource": "*"
        }
    ]
}
```

3. After you create the policy, attach the policy to the IAM user that you created.

Creating a CloudTrail

This procedure describes how to create a CloudTrail as required for CloudControl. You may set other preferences as needed for your environment.

1. Login to your AWS Management Console.
2. Select **Services > Management & Governance > CloudTrail**.
3. Click **View Trails** and then click **Create Trail**.

4. Complete the following fields:
   a. Enter the name for your CloudTrail.
   b. Under Storage Location, select an existing S3 bucket or create new one.
   c. Determine if you need to enable Log File SSE-KMS encryption. If so, fill in the appropriate fields.
      Determine if you need to enable Log file validation. If so, enable it.
   d. Set 'Management Events' to All.
   e. Set 'Management Events, API activity' to read and write.
5. Click **Create**.

Adding an AWS Account

CloudControl learns about the AWS environment when you add an account.

Note: If you do not have a service account with the correct privileges set, you will not be able to add an AWS account to CloudControl. See the AWS Service Account Requirements section of the Installation Guide for HyTrust CloudControl.

1. From the Home tab, select **Inventory** > **AWS Accounts**.
2. On the **AWS Accounts** page, select **Actions > Add AWS Account**.
   Note: If there are no AWS accounts in your system, you can also click the **Add AWS Account** link on the **AWS Accounts** page.
3. On the About page in the Add AWS Account wizard, enter the Access Key ID and the Secret Access Key for the account.
4. Click **Continue**.
   If the AWS account is found with no errors, click **Continue** in the validation window to proceed.
   If there is an error, perform one of the following:
   - If the credentials are incorrect, AWS account is not found, click **OK** to close the window. Enter the correct credentials, and then click **Retry** on the About page.
   - If the AWS account is found but you are missing privileges, click **OK** to close the window. Assign the appropriate privileges to the Service User in the AWS management console, and then click **Retry** on the About page.
   - If the AWS account is found but the CloudTrail is disabled, click **OK** to close the window. Configure the CloudTrail bucket in the AWS management console, and then click **Retry** on the About page.
5. On the CloudTrail page, select the CloudTrail Bucket that you want to use.
6. Click **Continue**.
7. On the **Details** page, you can monitor the process.
8. Click **Continue** to view the dashboard for the newly added AWS account.

Viewing AWS Inventory

From the **Home** page, select **Inventory > AWS Accounts** to view the AWS Accounts page. From here, you can view in depth information of all of the compute, network, and storage resources in an AWS account, as well as any tags or policies related to those resources. This information is displayed in a dashboard or a resource page.

> **Note:** You need to add an account before you can view any information. See Adding an AWS Account on the previous page.

Dashboard Pages

Dashboard pages are a visual overview of your resources in various tiles. For AWS, you can view the global dashboard or a dashboard for each AWS account.

The dashboard pages display the following information:

- An overview of all AWS account resources globally or for the specific account.
- Current, recent, and trending configuration hardening information.
- Account details (for account-level dashboards). This includes the Hosted Systems field that indicates if any other platforms are being hosted. You can click the resource name to view the dashboard for that resource.

Click the expander icon in each tile to open the Views page with detailed information. You can also click the options under the **Views** menu. From the Views page, you can click the **x** icon to return to the original location.

Resource Pages

Each resource page displays a list of the resources for each type, along with other important information per resource, such as details and tags. You can also use the **Actions** menu to assign and unassign tags to a selected resource. For each account, the resource page displays the following tabs:

- Compute—Compute resources, instances, dedicated hosts, such as EC2 .
- Network—Networking and content delivery resources, such as VCP.
- Storage—Storage collection buckets such as S3.

You can click the links to view a pop-up window with more details.

Navigating AWS Account Inventory Views Pages

The Views pages allow you to view in depth information on your inventory.

1. From the Home tab, select **Inventory** > **AWS Accounts**.
2. On the AWS Accounts page, click **Views** and select one of the following:
   - **Resources**—to view all resources under the specified object.
   - **Current Configuration Hardening**—to view the current configuration hardening activities.
   - **Configuration Hardening Activity**—to view all configuration hardening activities.
   - **Configuration Hardening Policies**—to view all configuration hardening policies.
3. Click the **x** icon to return to your original location.

Sync AWS Account Inventory

1. From the Home tab, select **Inventory** > **AWS Accounts**.
2. On the **AWS Accounts** page, click the Accounts link.
3. Select the AWS account that you want to sync.
4. Select **Actions > Sync Inventory**.
5. Click **OK** to refresh the inventory.

Updating AWS Account Configuration

1. From the Home tab, select **Inventory** > **AWS Accounts**.
2. On the AWS Accounts page, click the Account link.
3. Select the AWS account for which you want to update the configuration.
4. Select **Actions > Update Configuration**.
5. Enter the Access Key ID and the Secret Access Key for the account.
6. Click **Continue**.
7. On the confirmation page, click **Continue**.
8. On the CloudTrail page, select the CloudTrail that you want to use.
9. Click **Continue**.

Remove AWS Account

1. From the Home tab, select **Inventory** > **AWS Accounts**.
2. On the **AWS Accounts** page, click the Accounts link.
3. Select the AWS account that you want to remove.

4. Select **Actions > Remove Account**.
5. Click **OK** in the confirmation window.

Chapter 7. Managing Image Registries

About Image Registries

An image registry is a service that stores your repositories and images. Each repository contains one or more version of the same image. All images in a repository must have the same name, and are differentiated by tags. The tag name corresponds to the version of the image. The most recent image is also tagged as 'latest'.

In the following image, all images in a repository have the same name, but the version number is different.

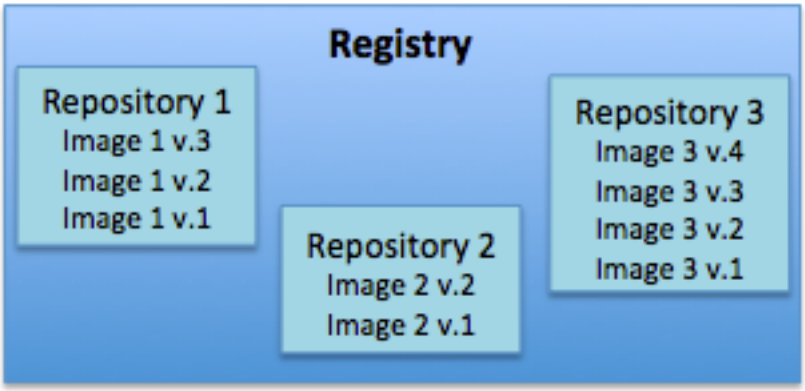


Image registries are not protected by CloudControl, but adding a registry allows CloudControl to discover valuable information about the registry, such as the number of images and their specific vulnerabilities.

Select **Inventory > Image Registries** to view the registries that you have added to CloudControl.

Adding an Image Registry

CloudControl learns about the current state of your image repositories when you add a registry.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the **Image Registries** tab, select **Actions > Add Registry**.

   Note: If there are no registries in your system, you can also click the **Add Registry** link on the **Image Registries** page.
3. On the About page, specify the following:

Field	Value
Name	Enter the name that you want to use for the registry.
IP/FQDN	Enter the IP Address or FQDN for the registry.
Port	Enter the registry port used in configuration of the local registry.
Authorization Schema	Choose one of the following to use for authorization: • BASIC • OAUTH
User	Enter the user name for the registry.
Password	Enter the password for this user.
Description	Enter an optional description.

4. Click **Continue**.
5. If you did not already add a certificate authority, you will be prompted to add one.
   a. In the Missing Certificate Authority window, click **Install Certificate Authority Now**.
   b. On the Install Certificates page, do one of the following:
      - Select Import and then click the **Browse** button to locate the certificate file.
      - Select Enter Text and then paste the contents of the certificate into the Certificate Data field.
   c. Click **Continue**.
6. On the **Details** page, you can monitor the process.
7. Click **Continue** to view the dashboard for the newly added registry.

Viewing Image Registries

From the **Home** tab, select **Inventory > Image Registries** to view the Manage Image Registries page.

Note: Although you can only manually add Docker Image Registries, you can also view any AWS Elastic Container Registries (ECRs) or OpenShift Container Registries (OCRs) that are added automatically.

The Registries tab displays all of the image registries that have been added to CloudControl and the following details:

- Name—The name that you assigned to the registry. Click the link in the Name column to view a detailed registry page that lists the registry details, tags, and all of the images in that registry.
- IP address—The IP address of to the registry. Registries with the same IP address can be differentiated by port number and name.
- Hostname—The hostname of the registry.
- Port—The port assigned to the registry.
- Platform—The registry platform name for ECRs and OCRs.
- Region—The region associated with the registry.
- Description—The optional description assigned to the registry.
- Images—The number of images in the registry. Click the link in the Images column to view a detailed registry page that lists the registry details, tags, and all of the images in that registry.
- Tags—Any tags assigned to the registry. Click the link in the Tags column to view the Manage Tags page, which lets you add or remove existing tags from the image registry. If you need to create a tag, see Creating Tags on page 105.

The Images tab displays all of the images that were added with the image registries and the following details:

- Name—The name assigned to the image. Click the link in the Name column to view a pop-up with tabs displaying the Details, Vulnerabilities, Containers, and Tags for that image.
- Image ID—The ID in SHA-256 hash format.
- Version—The version of the image. The most recent version is always called the latest.
- Image Tag—The image tag assigned to the registry.
- Registry—The registry that the image belongs to.
- Vulnerabilities—The number of vulnerabilities and the type. Click a link in the Vulnerabilities column to view a pop-up with tabs displaying the Details, Vulnerabilities, Containers, and Tags for that image. The vulnerabilities tab lists each vulnerability with their CVE, severity, and description. Click the CVE link to view details about the CVE.
- Signature—Displays true if the image is signed, and false if the image is not signed.
- Containers—The number of containers associated with the image registry. Click the link in the Containers column to view a pop-up with tabs displaying the Details, Vulnerabilities, Containers, and Tags for that image. The containers tab lists the name of each container, and the cluster and namespace to which the container belongs.
- Create Time—The date and time that the image was created.
- Tags—Any tags assigned to the image. Click the link in the Tags column to view the Manage Tags page, which lets you add or remove existing tags from the image. If you need to create a tag, see Creating Tags on page 105.

  Note: You need to add an image registry before you can view any information. See Adding an Image Registry on the previous page.

Updating Image Registry Configuration

Updating the image registry configuration re-adds your existing registry to CloudControl with different configuration information.

Note: All tag associations created in CloudControl are retained.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry that you want to modify.
3. Select **Actions > Update Configure**.
4. On the Configure Registry page, modify the following information as needed:

Field	Value
Name	Enter the name that you want to use for the registry.
IP/FQDN	Enter the IP Address or FQDN for the registry.
Port	Enter the SSH port for the registry.
Authorization Schema	Choose one of the following to use for authorization: • BASIC • OAUTH
User	Enter the user name for the registry.
Password	Enter the password for this user.
Description	Enter an optional description.

5. Click **Continue** to save your changes.

Refreshing your Image Registry Inventory

Refreshing your image registry pulls the latest information from the online Docker registry into CloudControl.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry that you want to refresh.
3. Select **Actions > Sync Inventory**.
4. Click **OK** on the confirmation page.

Assessing Image Registry Vulnerabilities

CloudControl assesses any changes in the vulnerabilities in your image registry every two hours. You can perform this task manually if you want to view results more often.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry where you want to assess vulnerabilities.

   If you are on the Registry page for a specific registry, you do not need to specify.
3. Select **Actions > Assess Vulnerabilities**.
4. Click **OK** on the confirmation page.

   A message displays stating that the assessment has been queued.
5. To verify the job, from the **Home** tab, select **System > System Settings**.

   If the job is still running, you will see it on the Recent Jobs section, with the prefix 'vulnerability-collector' added to the job name. If the job has completed, click the expander icon to view it on the Job Monitoring page.

Assigning a Tag to a Registry

Note: You must have created CloudControl tags before you can assign them to a registry. For more information, see Creating Tags on page 105.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry where you want to assign a tag.
3. Select **Actions > Assign Tags**.
4. On the Manage Tags page, click the **Assign Tag** button.

   Note: If there are no tags assigned to the registry, you can also click the **Assign Tags Now** link.
5. On the Select Tag page of the Assign Tags wizard, select the tag that you want to assign.
6. Click **Continue**.
7. On the Values page, select the values that you want to assign.
8. Click **Assign**.
9. On the Manage Tags page, verify the tags and values, and click **Close**.

Assigning a Tag to a Registry Image

Note: You must have created CloudControl tags before you can assign them. For more information, see Creating Tags on page 105.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, click the Images tab.
3. Select the image where you want to assign a tag.
4. Select **Actions > Assign Tags**.

5. On the Manage Tags page, click the **Assign Tag** button.
   Note: If there are no tags assigned to the resource, you can also click the **Assign Tags Now** link.
6. On the Select Tag page of the Assign Tags wizard, select the tag that you want to assign.
7. Click **Continue**.
8. On the Values page, select the values that you want to assign.
9. Click **Assign**.
10. On the Manage Tags page, verify the tags and values, and click **Close**.

Unassigning a Tag from a Registry

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry where you want to assign a tag.
3. Select **Actions > Unassign Tags**.
4. On the Manage Tags page, select the tag that you want to unassign.
5. Click **Close**.

Deleting an Image Registry

Deleting an image registry removes the registry and permanently deletes any tag associations made in CloudControl.

1. From the **Home** tab, select **Inventory > Image Registries**.
2. On the Manage Image Registries page, select the registry that you want to delete.
3. Select **Actions > Remove Registry**.
4. Click **OK** on the confirmation page.

Chapter 8. Trust Manifests

About Trust Manifests

Trust manifests are the security component of CloudControl. You can manage your trust manifests on the Manage Trust Manifests page. From the **Home** tab, select **Security > Trust Manifests**.

CloudControl supports the following types of trust manifests:

- Access Control—Provides security by limiting access to your vSphere and NSX-T environments.
- Boundary Control—Allows you to use rules and constraints to authenticate and authorize delivery of encryption keys to the data encrypted and managed by HyTrust DataControl/KeyControl.
- Deployment Control—Provides security when deploying Kubernetes and OpenShift clusters.
- Exception Control—Allows you to define rules to allow certain vSphere URL patterns and route them to either vCenter or the proxy.

  Important: Do not use exception control policies unless instructed by HyTrust.
- Secondary Approval—Provides security by requiring additional approvals before users can perform certain disruptive operations on your vSphere and NSX-T environments.
- Trust Attestation—Allows you to define rules to ensure selected resources match the trust attestation requirements.

When you create a trust manifest, you add a security policy to it. Both the trust manifest and the security policy must be the same type, for example, an access control trust manifest requires an access control policy. After the trust manifest has been reviewed, you can publish it. Once published, you can assign a resource to the trust manifest.

Trust manifests can be assigned to one or more resources:

- For Deployment Control, you can assign resources at the cluster and namespace level.
- For Access Control and Secondary Approval, you can assign resources at the vCenter, Data Center, and VM folder level.
- For Boundary Control, you can only assign resources at the Appliance Root level.
- For Trust Attestation, you can assign resources at the Appliance Root, vCenter, Data Center, Cluster, and ESXi Host level.

  Note: Each resource can only be associated with one trust manifest of a given type.

Global Trust Manifests

Global Trust Manifests are created by default and assigned to Appliance Root at installation. This allows you to install CloudControl without disrupting your existing environment.

Global Trust Manifests cannot be modified, but can be assigned to additional resources besides Appliance Root. If you create a new trust manifest that you apply to Appliance Root, then the global trust manifest will no longer be assigned to the Appliance Root resource.

Note: You cannot delete a cloned or custom trust manifest that is assigned to Appliance Root. You must first assign Appliance Root to a different trust manifest, and then you can delete it. Global trust manifests cannot be deleted.

To view where appliance root is assigned, from the Manage Trust Manifests page select **Actions > Manage Root Trust Manifests**.

The following Global Trust Manifests are created:

- HyTrust Global Trust Manifest for Access Control—Created for the local authentication mode. Supports a subset of the default roles.
- HyTrust Global Trust Manifest for Access Control_AD—When you switch to Active Directory mode, this trust manifest is created. If you have a custom access control trust manifest assigned to Root, then will be called <Custom_Trust_Manifest_Name>_AD. By default, this only supports the ASC_SuperAdmin role. You must add more rules to fully protect your environment.
- HyTrust Global Trust Manifest for Boundary Control—Created with no rules. You can add rules when you decide to use boundary control.
- HyTrust Global Trust Manifest for Deployment Control—Created with no rules enabled. You must enable rules to protect your environment.
- HyTrust Global Trust Manifest for Exception Control—Created with no rules. You can add rules if you decide to use exception control.

  Important: We recommend that you contact HyTrust support before using exception control.
- HyTrust Global Trust Manifest for Secondary Approval—Created with no rules. You can add rules when you decide to use secondary approval.
- HyTrust Global Trust Manifest for Trust Attestation—Created with no rules. You can add rules when you decide to use trust attestation.

About Access Control Policies

The access control policy, as part of a trust manifest, allows you to determine who can access what in your environment. Each rule links a role to a user or group, and when published in a trust manifest, they can be associated to a resource. Access control policies are also used to configure view hiding. For more information, see About View Hiding on page 101.

CloudControl access control policies are comprised of one or more rules containing the following:

Field	Description
Name	The name of the rule.
Description	The optional description of the rule.
Role	The role to be assigned to the rule. See Viewing Roles on page 96.
Subjects	The user or group to be assigned to the role.
Constraints	
Resource Tag	Provides additional selection criteria based on tags that are applied to a resource.
Subject	Provides the following selection criteria for the user allowed to perform the action: • Access Location—Limits the IP address or range that can be used. • Access Method—Limits the type of method that can be used, for example, vSphere SDK or REST. • Access Time—Limits the times when the user can perform the action.

Note: The default ASC_SuperAdmin rule is created by default when you enable AD. You can modify the rule or delete it.

Creating an Access Control Trust Manifest from the CloudControl GUI

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Access Control in the Policy Type field.

5. In the Access Control Policy section, complete the following:

Field	Description
Name	Enter the name of the rule.
Description	Enter the optional description of the rule.
Role	Select the role to be assigned to the rule. See Viewing Roles on page 96.
Subjects	Enter the user or group to be assigned to the role. The AD domain is displayed automatically. Type to search for the group or user that you want to use.
Constraints	**Constraints**
Resource Tag	Enter the additional selection criteria based on tags that are applied to a resource. a. Select the tag information and a resource. If you select Equals, then the rule will be applied only to resources of the specified type with the specified tag and tag value. b. Select where the tag originated. We suggested you use Appliance Console as it can apply to all types of resources across platforms in CloudControl. c. Click Add.
Subject	Select the type of access for the user allowed to perform the action: • Access Location—Enter the IP address or range that can be used for access. • Access Method—Enter the type of method that can be used, for example, vSphere SDK or REST. • Access Time—Enter the times when the user can perform the action.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Creating an Access Control Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.

4. Enter a YAML file in the following format:

```
metadata:
    name: Trust Manifest for Access Control policy
    description: Outlines Access Control policy
policies:
    accessControlPolicy:
    accessControlRules:
     -
     name: Access Control Rule for administrators
     description: Grant SuperAdmin privileges to administrators on VMs tagged blue.
     role: ASC_SuperAdmin
                action: Permit
                subjects:
                    - 'local::user:SuperAdminUser'
                resourceConstraints:
                    tags:
                     -
                       operator: Equals
                       name: Tenant
                       value: Blue
                       origin: Appliance Console
                       resourceType: VirtualMachine
                subjectConstraints:
                    accessLocation:
                        ipRanges:
                            operator: NotBetween
                            range:
                                startIp: 10.222.81.131
                                endIp: 10.222.81.136
                        ipAddresses:
                            operator: Equals
                            ip:
                                - 10.222.81.137
                    accessMethod:
                        operator: Equals
                        methods:
                            - RESTAPI
                            - vSphereWebClient
                    accessTime:
                        frequency: weekly
                        startTime: '09:00:00'
                        endTime: '21:00:00'
                        daysOfTheWeek:
                            - Wednesday
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

About Boundary Control Policies

Boundary control trust manifest policies allow you to set the rules for what resources are included in the boundary. Trust manifest rules are defined based on the following:

- Tags on the VM
- Tags on the host
- Trust status of the host

Note: You can also use the default global boundary control trust manifest to use all vCenters and ESXi hosts that have been added to CloudControl as the boundary.

Creating a Boundary Control Trust Manifest from the CloudControl GUI

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Boundary Control in the Policy Type field.

5. In the Boundary Control Rules section, complete the following:

Field	Description
Name	Enter the name of the rule.
Description	Enter the optional description of the rule.
Virtual Machine Constraints	
Virtual Machine Tag	Enter the additional selection criteria based on tags that are applied to a virtual machine. a. Select the operator. • If you select Equals, then the rule will be applied only to virtual machines that match the criteria. • If you select Not Equals, virtual machines that match the criteria are excluded. b. Optionally select where the tag originated. If you do not want to specify, you can leave it set to All Tag Origins. c. Select the tag name that is associated with the virtual machine. You can specify a specific tag value, or leave it set to All Tag Values. d. Click **Add**.
Host Constraints	
Trust Attestation status is trusted	Check the checkbox if you want only trusted hosts to be allowed in this boundary. For more information, see About Trust Attestation on page 120.
Host Tag	Enter the additional selection criteria based on tags that are applied to a host. a. Select the operator. • If you select Equals, then the rule will be applied only to virtual machines that match the criteria. • If you select Not Equals, virtual machines that match the criteria are excluded. b. Optionally select where the tag originated. If you do not want to specify, you can leave it set to All Tag Origins. c. Select the tag name that is associated with the host. You can specify a specific tag value, or leave it set to All Tag Values. d. Click **Add**.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Creating a Boundary Control Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.
4. Enter a YAML file in the following format:

```
metadata:
  name: Trust Manifest for Boundary Control policy
  description: Outlines Boundary Control policy
policies:
  boundaryControlPolicy:
    boundaryControlRules:
      - name: Boundary Control Rule for blue boundary
        description: Boundary for blue VMs must be any Trusted host labeled Blue in France
        hostConstraints:
          requireTrustedHost: true
          tags:
            - operator: Equals
              name: Tenant
              value: Blue
              origin: Appliance Console
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

About Deployment Control Policies

The deployment control policy, as part of a trust manifest, allows you to determine what images from a registry are safe to be added to your protected clusters. CloudControl enforces image security using deployment policies, which are comprised of one or more deployment rules:

- Private Registry Rules
  - Private Registries—Allows you to enter a list of private registries, either onboarded or not, that you want to evaluate with the trust manifest. Only the images from registries listed in the Allowed Registries section are evaluated to see if they can be deployed. Images from all other registries will be denied.

  - Signature Rule—Allows you to deny images that do not have an associated digital signature.
  - Attributes Rule—Allows you to deny or deploy images based on their image ID or image name.
  - Vulnerabilities Rule—Allows you to deny or deploy images based on CVSS scores or specific CVEs.
- Public Registry Rules
  - Public Registry Rule—Allows images from public registries to be deployed in your environment without any evaluation.

    Important: We strongly recommend that you do leave the public registry rule set to ENABLED and do not allow public registries to be deployed. If you must use a public registry, then you can leave the rule set to ENABLED and enter that specific registry into the Allowed Registries field. This will allow only that specific registry image to be deployed, and will prevent all other public registry images from deployment.

Rules can either have a True or False value, and can also include a 'stop processing' clause. Deployment rules in a policy are evaluated in the following order:

- If False, the image will not be deployed and no further rules are evaluated.
- If True, AND there is a 'stop processing' clause, the image is allowed to be deployed and no further rules are evaluated.
- If True, the next rule in the policy is evaluated. If this is the only rule, then the image is allowed to be deployed.
- If all rules are True, then the image is allowed to be deployed.

Important: We recommend that you always use the image SHA as it is a unique identifier for your images. Pods can be created by using either an image name with tag, or an image name with SHA, and in many cases images with the same SHA could have been tagged with different tags. For example, you could have a single image named TestImage with different tags like TestImage:3, TestImage:4, and TestImage:5, but all these images will have the same SHA as the underlying image is the same for all three of them.

When you create any Deployment Control Policy rules, you should use the image name with SHA to ensure that the intended image is evaluated no matter what tags are there. If you use an image name with tag, such as TestImage:3, then only the image that matches that specific tag will be selected. The other images, TestImage:4 and testImage:5 will not be evaluated.

Creating a Deployment Control Trust Manifest from the CloudControl GUI

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Deployment Control in the Policy Type field.

5. In the Deployment Control Rules section, complete the following information:
   a. In the Private Registries section, in the Allowed Registries field, enter the registries that you want to allow. The registries can be existing onboarded registries or registries that you plan to onboard. Registries that have not been onboarded are depicted with a yellow warning icon.
   b. In the Rules section, in the Signature Rule field, select Enabled or Disabled to determine whether or not to deny images when no signature is present.
   c. In the Attribute Rule field, select Enabled or Disabled to determine whether or not to evaluate using attributes, and then complete the following:

Field	Description
Name	Enter the name of the rule. The name cannot contain any special characters.
Step 1. Exemption List Deploy on Match	Select ENABLED or DISABLED to determine whether or not to use this criteria when evaluating. If yes, use the + and - symbols to add the following criteria: • Image ID—Enter the image ID in SHA format to match. • Image Name—Enter the Name and Tag Regex to match. If there is a match, the image will immediately be deployed, and no other deployment policy rules will be evaluated. If there is no match, continue to the next enabled step. If there are no other steps, continue to the next rule in the deployment policy.
Step 2. Whitelist Deny on No Match	Select ENABLED or DISABLED to determine whether or not to use this criteria when evaluating. If yes, use the + and - symbols to add the following criteria: • Image ID—Enter the image ID in SHA format to match. • Image Name—Enter the Name and Tag Regex to match. If there is no match, the image will immediately be denied, and no other deployment policy rules will be evaluated. If there is a match, continue to the next enabled step. If there are no other steps, continue to the next rule in the deployment policy.
Step 3. Blacklist Deny on Match	Select ENABLED or DISABLED to determine whether or not to use this criteria when evaluating. If yes, use the + and - symbols to add the following criteria: • Image ID—Enter the image ID in SHA format to match. • Image Name—Enter the Name and Tag Regex to match. If there is a match, the image will immediately be denied, and no other deployment policy rules will be evaluated. If there is no match, continue to the next rule in the deployment policy.

c. In the Vulnerabilities Rule field, select Enabled or Disabled to determine whether or not to evaluate using vulnerabilities, and then complete the following:

Field	Description
Name	Enter the name of the rule. The name cannot contain any special characters.
Deny deployment if thresholds are exceeded:	Enter the number of high, medium, and low vulnerabilities that you are willing to allow in your deployment. Deployment is denied if the number of vulnerabilities exceeds your selected limit.
Whitelist Ignore thresholds for the following vulnerabilities:	Use the drop-down list to select the vulnerabilities that you want to exclude from the threshold limit. You can search by any part of the vulnerability name, such as CVE or 2018.
Blacklist Always deny images with the following vulnerabilities:	Use the drop-down list to select the vulnerabilities that will always cause deployment to be denied. You can search by any part of the vulnerability name, such as CVE or 2018.

d. Optional. In the Public Registries selection, you can add public registries to be deployed without any evaluation. We recommend that you leave this section enabled, and do not enter any values in the Allowed Registries field.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Publish**—Publish the trust manifest.

   Or click the **Cancel** link to close the trust manifest without saving.

Creating a Deployment Control Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.

4. Enter a YAML file in the following format:

```
metadata:
  name: Trust Manifest for Deployment Control policy
  description: Outlines Deployment Control policy
policies:
  deploymentControlPolicy:
    deploymentControlRules:
      -
        privateRegistriesOriginRestriction:
          acceptablePrivateRegistries:
            - registry1.test.hytrust.com
          enabled: true
      -
        publicRegistriesOriginRestriction:
          acceptablePublicRegistries:
            - hub.docker.com
          enabled: true
          publicRegistriesEnabled: true
      -
        containerNotarization:
          enabled: false
      -
        containerImageAttributeRestriction:
          name: "Image Attribute Rule"
          blacklistEnabled: true
          blacklistedImages:
            -
              containerImage:
                imageNameRegex: nginx
                imageTagRegex: 1\.3
                type: BLACKLIST
          enabled: true
          exemptedImages:
            -
              containerImage:
                imageNameRegex: nginx
                imageTagRegex: 1\.7.*
                type: EXEMPTIONLIST
          exemptionlistEnabled: true
          whitelistEnabled: true
          whitelistedImages:
            -
              containerImage:
                imageNameRegex: nginx
                imageTagRegex: 1\.6
                type: WHITELIST
      -
        cveRestriction:
          blacklistEnabled: true
          cveCountsEnabled: true
          name: "Vulnerabilities Rule"
          enabled: false
          threshold:
            HIGH: 0
```

```
    LOW: 100
    MEDIUM: 0
    CRITICAL: 0
  whitelistEnabled: true
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

About Exception Control Policies

Important: Do not use exception control policies unless instructed by HyTrust.

The exception control policy, as part of a trust manifest, allows you to define rules to allow certain vSphere URL patterns and route them to either vCenter or the proxy. For future security you can use a location-based constraint to further restrict

CloudControl only allows the vSphere URL Patterns exception control rule.

Creating an Exception Control Trust Manifest from the CloudControl GUI

Important: Do not use exception control policies unless instructed by HyTrust.

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Exception Control in the Policy Type field.

5. In the Exception Control Rules section, complete the following:

Field	Description
Name	Enter the name of the rule.
Description	Enter the optional description of the rule.
Rule Type	Select the rule to use. Currently CloudControl only supports vSphere URL Patterns.
Authorization Effect	Select one of the following: • Allow—Send the request directly to vCenter and bypass the CloudControl proxy. • Forward—Forward the request to the CloudControl proxy for processing.
Constraints	
URL Patterns	Specify the URL pattern to be processed as a valid regular expression.
Access Location	Enter the IP address or range that can be used for access.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Note: It takes about 10 minutes for newly created exception control policies to be enforced.

Creating an Exception Control Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.

4. Enter a YAML file in the following format:

```
metadata:
  name: Trust Manifest for Exception Control policy
  description: Outlines Exception Control policy
policies:
  exceptionControlPolicy:
    exceptionControlRules:
      - ruleType: VSPHERE_URL_PATTERNS
        effect: FORWARD
        name: Exception Control Rule for vSphere URL patterns
        description: Exception Control Rule for forwarding operations with certain URL to the
proxy for evaluation
          patterns.
        urlPatterns:
          - "*/folder"
        accessLocation:
          ipRanges:
            operator: NotBetween
            range:
              startIp: 10.222.81.131
              endIp: 10.222.81.136
          ipAddresses:
            operator: Equals
            ip:
              - 10.222.81.137
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

About Secondary Approval Policies

Use Secondary Approval to configure CloudControl to require additional approval before users can perform selected disruptive operations on a resource. For example, you can require secondary approval before deleting or powering off a virtual machine or vApp, editing a firewall, or creating an edge gateway service.

When a user attempts to perform a vSphere or NSX-t operation that requires secondary approval, the operation fails with a notification that secondary approval is required, and that a request was generated.

> **Note:** If you have SMTP configured, and the users or groups have an email address in AD, then email messages are generated.

You can approve or deny a request on the Secondary Approval Requests page. See Approve or Deny Secondary Approval Requests on page 76.

> **Important:** Users cannot approve their own requests, even if they are in the approval group. A different user must approve the request.

Creating a Secondary Approval Trust Manifest from the CloudControl GUI

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Secondary Approval in the Policy Type field.

5. In the Secondary Approval Policy section, complete the following:

Field	Description
Name	Enter the name of the rule.
Description	Enter the optional description of the rule.
Subjects	Enter the user or group that needs secondary approval to perform the operations. The AD domain is displayed automatically. Type to search for the group or user that you want to use.
Approvers	Enter the user or group that approves secondary approval for the requesting users to perform the operations. The AD domain is displayed automatically. Type to search for the group or user that you want to use.
Operations	Add the operations that must be approved in order to perform. You can type to search for the operations, or click the plus icon to view all operations.
Approval Duration	Select the number of minutes or hours that the requester can perform the operation. The default is 120 minutes.
Max Allowed Operations	Select the maximum number of allowed operations that requester can perform. Leave blank for unlimited.
Constraints	
Resource Tag	Enter the additional selection criteria based on tags that are applied to a resource. a. Select the tag information and a resource. If you select Equals, then the rule will be applied only to resources of the specified type with the specified tag and tag value. b. Select where the tag originated. We suggested you use Appliance Console as it can apply to all types of resources across platforms in CloudControl. c. Click Add.
Subject	Select the type of access for the user allowed to perform the action: • Access Location—Enter the IP address or range that can be used for access. • Access Method—Enter the type of method that can be used, for example, vSphere SDK or REST. • Access Time—Enter the times when the user can perform the action.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Creating a Secondary Approval Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.
4. Enter a YAML file in the following format:

```
metadata:
    name: Trust Manifest for Secondary Approval policy
    description: ''
policies:
    secondaryApprovalPolicy:
        secondaryApprovalRules:
         -
          name: Secondary Approval Rule for administrators
          description: Require Secondary Approval for Delete VM operation on VMs tagged blue.
          action: Permit
          subjects:
              - 'local::group:ASC_NetworkEngineer'
          approvers:
              - 'local::group:ASC_SuperAdmin'
          operations:
              - Compute.VirtualMachine.Delete
          approvalDuration: 120
          resourceConstraints:
              tags:
                -
                  operator: Equals
                  name: Tenant
                  value: Blue
                  origin: Appliance Console
                  resourceType: VirtualMachine
          subjectConstraints:
              accessTime:
                  frequency: monthly
                  daysOfTheMonth:
                      - 3
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Approve or Deny Secondary Approval Requests

1. From the **Home** tab, select **Security > Secondary Approval Requests**.
2. On the Secondary Approval Requests page, you can do the following:

- Click the tabs to view Pending or All requests.
- Approve a pending request by selecting the request and clicking the **Approve** button.
- Deny a pending request by selecting the request and clicking the **Deny** button.

About Trust Attestation Policies

The trust attestation policy, as part of a trust manifest, allows you to use the trust attestation fingerprints that were captured to evaluate hosts. You can use either the platform or the OS fingerprint that was captured, or both. You can also use specific constraints to limit the hosts that are trusted.

Creating a Trust Attestation Trust Manifest from the CloudControl GUI

When names are required, you can use alphanumeric characters and spaces, but no special characters except _ (underscore), - (hyphen), and . (period).

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. On the Details tab of the Create Trust Manifest page, enter the name and optional description for the trust manifest.
4. Select Trust Attestation in the Policy Type field.

5. In the Access Control Policy section, complete the following:

Field	Description
Name	Enter the name of the rule.
Description	Enter the optional description of the rule.
Platform Fingerprint	Select the platform fingerprint that you want to use. You can select one or more fingerprints. **Note:** Either platform fingerprint or OS fingerprint is required.
OS Fingerprint	Select the OS fingerprint that you want to use. You can select one or more fingerprints. **Note:** Either platform fingerprint or OS fingerprint is required.
Host Unique Fingerprint Check	Check the checkbox if you want CloudControl to use additional measurements besides the fingerprints.
Constraints	
Resource Tag	Enter the additional selection criteria based on tags that are applied to a resource. a. Select the operator for the resource. • If you select Equals, then the rule will be applied only to resources that match the criteria. • If you select Not Equals, resources that match the criteria are excluded. b. Optionally select where the tag originated. If you do not want to specify, you can leave it set to All Tag Origins. c. Select the tag name that is associated with the resource. You can specify a specific tag value, or leave it set to All Tag Values. d. Click **Add**.

6. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.
7. After the trust manifest has been published, in the Assign Resources window click **Assign Resources Now**.

   You can assign the trust manifest to ESXi hosts, DataCenters, or the entire vCenter. This replaces the existing trust manifest.
8. Select the resources that you want to assign and click **Assign**.
9. Click **Close** to close the window.

The trust manifest evaluates all hosts on the resource selected. You can view the results on the vSphere inventory page.

Creating a Trust Attestation Trust Manifest from a YAML File

When you become more familiar with trust manifests, you can create them using a YAML file. We recommend that you start by creating a trust manifest in the GUI by clicking the Details tab. After each save, you can click back and forth between the Details and YAML tabs to see how your changes affect the YAML file.

1. From the **Home** tab, select **Security > Trust Manifests**.
2. On the Manage Trust Manifests page, select **Actions > Create Trust Manifest**.
3. Click the **YAML** tab.
4. Enter a YAML file in the following format:

```
metadata:
  name: Trust Manifest for Trust Attestation policy
  description: ''
policies:
  trustAttestationPolicy:
    trustAttestationRules:
      -
        name: Production and Development Gold Standard Rule
        description: Relevant Platform and OS Fingerprints for Prod and Dev systems
        platformFingerprints:
          - 'Production Gold Standard Platform'
          - 'Development Gold Standard Platform'
        osFingerprints:
          - 'Development Gold Standard OS'
        hostUniqueFingerprintCheck: true
        resourceConstraints:
          tags:
            - operator: Equals
              name: Tenant
              value: Blue
              origin: Appliance Console
              resourceTypes:
                - HostSystem
```

5. Click one of the following:
   - **Validate**—Validate the draft or existing trust manifest.
   - **Save**—Save the trust manifest as a draft.
   - **Save and Publish**—Save the trust manifest and publish it.

   Or click the **Cancel** link to close the trust manifest without saving.

Modifying Trust Manifests

You can modify the rules of a trust manifest, or assign or unassign resources.

Note: Appliance Root must be assigned to a trust manifest. By default, it is assigned to each Global trust manifest. If you assign one of your trust manifests to Appliance Root, you cannot remove that assignment or delete the trust manifest until you assign the Appliance Root to a different trust manifest or back to the Global trust manifest.

Modifying Trust Manifest Rules

1. From the **Home** tab, select **Security > Trust Manifests**.
2. Select the trust manifest that you want to modify and click **Edit**.

Modifying Trust Manifest Resources

1. From the **Home** tab, select **Security > Trust Manifests**.
2. Select the trust manifest that you want to modify.

   To add a new resource:

   a. Select **Actions > Assign Resources**.

   b. Select the resources that you want to add.

   c. Click **Assign**.

   To remove a resource:

   a. Select **Actions > Unassign Resources**.

   b. Select the resources that you want to remove.

   c. Click **Unassign**.
3. Click **Close**.

Assigning a Resource to a Trust Manifest

You can assign a resource to a trust manifest immediately after publishing or from the Manage Trust Manifests page. After you assign the resource, the existing trust manifest that you published is replaced by the updated trust manifest with assigned resources. Only one trust manifest of each type can be assigned to the same resource. For example, if you assign Appliance Root to a trust manifest, the Global trust manifest of the same type loses its association with Appliance Root.

To assign after publishing:

Immediately after a trust manifest is published, you are prompted to assign the trust manifest to a resource.

1. In the Assign Resources window, click **Assign Resources Now**.

   Note: If you are not yet ready to assign resources, click **Not Now**. You can add them later.
2. Select the resource or resources to add to the trust manifest.
3. Click **Assign**.

To assign from the Trust Manifest page:

1. From the **Home** tab, select **Security > Trust Manifests**.
2. Select the trust manifest that you want to modify and select **Actions > Assign Resources**.

3. Select the resource or resources to add to the trust manifest.
4. Click **Assign**.

Chapter 9. Configuration Hardening

About Configuration Hardening

Configuration hardening allows you to improve the security posture of your vSphere, Kubernetes, AWS, or NSX-T Data Center environment by hardening the configuration to meet either your company's specific security policy, industry best practices such as CIS or NIST, or compliance standards such as PCI or HIPAA. By automating the hardening process, you can reduce your operational burden during a compliance audit.

With CloudControl, you can:

- Create and customize templates to use in configuration hardening checks.
- Assess and remediate your environments against the configuration hardening checks defined in the templates.
- Review dashboards, reports and alerts to monitor the results of assessments and remediations.

About Templates

CloudControl uses templates to support all Configuration Hardening activities. CloudControl supports the following types of templates:

- Catalog templates—Read-only collection of hardening operations for each cloud type, for example, vSphere operations catalog or Kubernetes operations catalog.
- System templates—Read-only collection of operations derived from a catalog template for a given compliance standard, for example, the vSphere - HIPAA Security Standards template is derived from the vSphere operations catalog template.

- Custom templates—Templates created by users. In most cases, they are copied or cloned from existing system or catalog templates. Custom templates can be modified and used in configuration hardening policies.

  Note: CloudControl also includes sample custom templates that can immediately be used in a policy. NSX-T does not have a sample custom template.

Templates can contain both assessment and remediation hardening operations. We recommend that you review all operations in the template to ensure that any parameter values are set to those that appropriate for your infrastructure requirements.

About Policies

Configuration Hardening Policies are used to run custom templates. Each policy associates a template with one or more resources or tag-based resource configurations, and can be run manually or as a scheduled activity. Policies can either assess or remediate a resource, but cannot do both.

Kubernetes Configuration Hardening Requirements

You must create a service account before you can run configuration hardening against a Kubernetes resource. The service account is a Linux user with either root or root-equivalent permissions.

- **Root User**—Linux root user can be used as is.
- **Non-Root User**—Linux users without root permissions require the following:
  - The Linux user must have read, write, and execute access to any file on the file system.
  - Edit the `/etc/sudoers` file to add the new Linux user:
    a. Enter the following command to start vi: visudo
    b. Add the following line to the sodoers file:
    ```
    <username> ALL=(ALL) NOPASSWD:ALL
    ```
    c. Save your changes and exit vi.

Viewing Templates and Policies

You can view all of the templates and policies in your system on the Configuration Hardening Management page.

Viewing Templates

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the **Templates** tab.
3. Click the name of the template to view the template dashboard, or click the number in the Operations column to view all of the operations that belong to the template.

   For more information on the template dashboard, see Viewing Template Dashboards on the next page.

Viewing Policies

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the **Policies** tab.

   This page displays the name, description, template, resource type, schedule, last event and status of the policy. From here, you can:

   - Click the name of the policy to view or edit it.
   - Click the template link to view the template dashboard.
   - Click the last event link to view a popup overview of the last run of that policy, and how successful it was. Click inside the overview to view the full details of the assessment. You can view the details in the CloudControl GUI, or download them to read later.

Viewing Template Dashboards

The template dashboard displays all relevant information about the template, and allows you to easily access the operations page for the template.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the **Templates** tab.
3. Click the name of the template that you want to view.

   The template dashboard page displays the following categories of information:

   - Operations Severity Summary—Displays the number of operations in high, medium, and low severity. Click on a severity number to view the Operations page filtered by the selected severity. Click the **x** icon to return to the dashboard.
   - Category Type—A breakdown of the template by category type. Click on a category type in the legend to toggle whether or not it is included in the pie chart.
   - Revisions—A list of change history revisions for the current template.
   - Details—Basic information about the template, including the description, type of template and resource, assigned status, and the created and updated dates.
   - Summary of Operations—Displays the a scrolling list of all operations as well as the number of operations in the following categories:
     - Total operations
     - Configured operations
     - Not configured operations
     - Remediation operations

     Click on an operation type number to view the Mange Operations page filtered by the selected type. Click the **x** icon to return to the dashboard.

Creating a Configuration Hardening Policy

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Policy tab.
3. Click the **Create** button.

   Note: If there are no policies in your system, you can also click the **Add a Configuration Hardening Policy Now** link.
4. In the Create Policy wizard on the Select Type page, select the type of policy that you want to create. This can be one of the following:
   - **Assess Only**—Runs operations on the host to compare the parameter values specified in the template with the actual values on the host.
   - **Remediate Only**—Modifies the parameter values on the host in order to match the values specified in the templates.
5. Click **Continue**.
6. On the Details page, enter the name and optional description of the policy, and specify whether the policy is enabled.
7. Click **Continue**.
8. On the Templates page, select the resource type for the policy. This can be one of the following:
   - **AWS Account**—Runs AWS-related templates against your AWS environment.
   - **ESXi**—Runs vSphere-related templates against your ESXi hosts.
   - **Kubernetes**—Runs Kubernetes-related templates against your Kubernetes environment.

     Important: Configuration hardening is not supported on OpenShift clusters.
   - **NSX-T**—Runs NSX-T-related templates against your NSX-T environment.
9. Select a template to run against your environment.

   The template list displays the name, description and type of operations. You should select a template that contains the type of operations that you selected for the policy.

   Note: You can only select custom templates that have been created in CloudControl. If there are no custom templates for your environment, you must cancel the Create Policy wizard, create the custom templates, then create a new policy. See Creating a Custom Template on page 89.
10. Click **Continue**.

11. On the Assignments page, select one of the following radio buttons and choose what resources to which you want to apply the policy:
    - **Tags**—Select the **Tags** radio button and then choose a tag or tags assigned to the resource. Click the + icon if you want to assign more tags to the resource. If there are no tags assigned, you can click the **Assign Tags Now** link. See Assigning Tags to Resources on page 106.

      Note: You can only assign tags to a resource in the Create Policy wizard. You cannot create new tags. If the tag that you want to use does not exist, you must cancel the Create Policy wizard, create the tags, then create a new policy. See Creating Tags on page 105.

      Important: Kubernetes tags for configuration hardening must specifically be assigned to a cluster master node.

    - **Resources**—Select the **Specific Resources** radio button and then choose one or more resources.

      Note: For vSphere only, you can choose a parent for the resource type. This can be one of the following:
      - vCenter—Allows you to select all ESXi hosts in the selected vCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple vCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
      - Appliance Root—Allows you to select all ESXi hosts under Appliance Root. All onboarded ESXi hosts will be considered for hardening. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
      - DataCenter—Allows you to select all ESXi hosts in the selected DataCenter. All onboarded ESXi hosts in the selected vCenter will be considered for hardening. You can select multiple DataCenters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
      - Cluster—Allows you to select all ESXi hosts in the selected Cluster. All onboarded ESXi hosts in the selected Cluster will be considered for hardening. You can select multiple Clusters. When the Configuration Hardening policy is run, CloudControl retrieves all onboarded ESXi hosts from the vCenter inventory to ensure the list of ESXi hosts is always current.
      - ESXi Host—Allows you to choose which individual ESXi hosts that you want to use as a resource. If additional ESXi hosts are onboarded, they will not be included.

12. Click **Continue**.

13. For vSphere only. On the Resource Constraint page, optionally choose which tag-based resource constraints that you want to use for your ESXi hosts.

    CloudControl tag-based resource constraints can be specified on a ComputeCollection of type VMFolder or directly on a VirtualMachine. This constraint will be used to further filter the VirtualMachines that will be acted upon that are currently running on the ESXi hosts selected in the assignments of this policy.

    a. Click the **Add** button.

    b. In the Add Resource Tag Constraint window, select the operator.

    > **Important:** You can choose Equals or Not Equals, but you cannot use both operators in the same configuration hardening policy. If you add an additional constraint, the value will be automatically set and cannot be updated.

    c. Select where the tag originated. This can be one of the following:

    - All Tag Origins—Applies to all CloudControl and local tags.
    - Appliance Console—Applies to CloudControl tags.
    - Local—Applies to all local tags. The origin name varies depending on your environment.

    d. Select the tag name information and tag value. If you select Equals, then the rule will only be applied to resources with the specified tag name and tag value. If you select Not Equals, then only those resources that match the specified tag name and tag value will be excluded.

    e. Select the resource type. This can be ComputeCollection (VMFolder) or VirtualMachine.

    > **Important:** The resource type must be the same for all constraints. If you add an additional constraint, the value will be automatically set and cannot be updated.

    f. Click **Add**.

14. Click **Continue**.

15. On the Schedule page, select whether or not you want to enable a recurring schedule.

    If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. This can be one of the following:

    - **Daily**—The policy will run every day at the time that you specify.
    - **Hourly**—The policy will run periodically throughout the day, based on the schedule you define.
    - **Weekly**—The policy will run on every day that you select at the time that you specify.

16. Click **Create**.

The newly created policy will be displayed on the Policy tag

Modifying a Configuration Hardening Policy

When you modify a configuration hardening policy, you can make changes to the following:

- name and description
- whether or not the policy or recurring schedule is enabled

- the specific template that you are using for the policy
- the tags or specific resources to which you want to apply to the policy.

Note: You cannot change the Policy type or the Resource type of an existing policy.

Procedure

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, select the policy that you want to modify.
3. Click the **Edit** button.
4. In the Edit Configuration Hardening Policy wizard on the Details page, update the name, description, and the status of the policy.
5. Click the Template tab and select the template that you want to run against your environment.
6. Click **Save** to save your changes but remain in the wizard, **Save and Close** to save your changes and close the wizard, or **Cancel** to close the wizard without saving.
7. Click the Assignments tab and select the tag or specific resource to which you want to apply the policy.

   If you select tags, and there are no tags that are assigned to resources, click the **Assign Tags Now** link and do the following:

   a. On the Apply Tags page, select the tag that you want to apply and click **Continue**.

   b. On the Values page, select the value that you want to use and click **Apply**.

   Important: Kubernetes tags for configuration hardening must specifically be assigned to a cluster master node.
8. Click **Save** to save your changes but remain in the wizard, **Save and Close** to save your changes and close the wizard, or **Cancel** to close the wizard without saving.

9. For vSphere only. On the Resource Constraint page, optionally choose which constraints you want to use for your ESXi hosts.

   CloudControl tag-based resource constraints can only be specified on a ComputeCollection of type VMFolder. This constraint will be used to further filter the VirtualMachines that will be acted upon that are currently running on the ESXi hosts selected in the assignments of this policy.

   a. Click the **Add** button.

   b. In the Add Resource Tag Constraint window, select the operator.

      Important: You can choose Equals or Not Equals, but you cannot use both operators in the same configuration hardening policy. If you add an additional constraint, the value will be automatically set and cannot be updated.

   c. Select where the tag originated. This can be one of the following:

      - All Tag Origins—Applies to all CloudControl and local tags.
      - Appliance Console—Applies to CloudControl tags.
      - Local—Applies to all local tags. The origin name varies depending on your environment.

   d. Select the tag name information and tag value. If you select Equals, then the rule will only be applied to resources with the specified tag name and tag value. If you select Not Equals, then only those resources that match the specified tag name and tag value will be excluded.

   e. Select the resource type. This can be ComputeCollection (VMFolder) or VirtualMachine.

      Important: The resource type must be the same for all constraints. If you add an additional constraint, the value will be automatically set and cannot be updated.

   f. Click **Add**.

10. Click the Schedule tab and select whether or not you want to enable a recurring schedule.

    If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. This can be one of the following:

    - **Daily**—The policy will run every day at the time that you specify.
    - **Hourly**—The policy will run periodically throughout the day, based on the schedule you define.
    - **Weekly**—The policy will run on every day that you select at the time that you specify.

11. Click **Save** to save your changes but remain in the wizard, **Save and Close** to save your changes and close the wizard, or **Cancel** to close the wizard without saving.

Deleting a Policy

When you delete a policy, the template associated with the policy is not deleted.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Policy tab.
3. Select the Policy that you want to delete.
4. Click the **Delete** button.
5. On the confirmation page, click **Delete**.

Creating a Custom Template

When you create a custom template, you can include operations from more than one template.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Template tab.
3. Click the **Create** button.
4. In the Create Template wizard, on the About page, type the name and optional description for the template.
5. Click **Continue**.
6. On the Choose Template page, select the resource type for the custom template. This can be one of the following:
   - **AWS Account**—Runs AWS-related operations.
   - **ESXi**—Runs vSphere-related operations.
   - **Kubernetes**—Runs Kubernetes master node-related operations.
     Important: Configuration hardening is not supported on OpenShift clusters.
   - **NSXDataCenter**—Runs NSX-T-related operations.
7. Select one or more templates to add to your custom template.
8. Click **Continue**.
9. On the Select Operations page, select the operations that you want to include in your custom template.
   By default, all non-duplicate operations are selected. Uncheck the checkbox for each operation that you want to remove.
10. Click **Create**.

Cloning a Configuration Hardening Template

Cloning a template creates an exact copy of the template with the _Copy suffix appended to the name. After cloning, you can rename the template.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Template tab.
3. Select the template that you want to clone and select **Actions > Clone Template**.
4. In the confirmation window, click **Clone**.
5. If you want to rename the template and update the description, select the new template and select **Actions > Edit Template Details**.

Modifying a Custom Template

You can modify the name and description of an existing template or change the operations that belong to the template.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Template tab.
3. Select the custom template that you want to modify and then select one of the following:
   - **Actions > Edit Template Details**
     a. In the Edit Template Details window, update the name and optional description of the template.
     b. Click **Apply**.
   - **Actions > Manage Operations**
     a. On the Manage Operations page, click the **Add** button.
     b. In the Add Operation window, on the Choose Template tab, select the templates whose operations you want to add and click **Continue**.
     c. On the Select Operations tab, select the individual operations that you want to add and click **Add**.
     Use the Filter bar to narrow down your choices.
     d. In the operations list, select any operations that you want to remove and click the **Delete** button.
     e. Click **Delete** in the confirmation box.

Your changes are automatically reflected on the template page.

Importing a Template

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Templates tab.
3. Click the **Import** button.
4. In the Import wizard, click **Browse** and navigate to the template that you want to import.
5. Click **Choose**.
6. Click **Import**.

Exporting a Template

You can only export custom templates. To quickly export a system or catalog template, clone the template and then export the clone.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Templates tab.
3. Select the template that you want to export and click the **Export** button.

The template you selected is automatically exported.

Deleting a Configuration Hardening Template

You can only delete custom or cloned templates that are not associated with a policy.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Template tab.
3. Select the templates that you want to delete. You can select one template or multiple templates.
4. Click the **Delete** button.
5. On the confirmation page, click the **Delete** button.

Running a Configuration Hardening Policy

Note: When you run an remediation policy, the assessment policy will automatically run immediately following its completion. This insures that your compliance score is updated with the new percentage.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Policy tab.
3. Select the Policy that you want to run.
4. Select **Actions > Run Now**.
5. In the confirmation window, click **Run Now**.

You can view the results by clicking on the link in the Last Event column.

Note: If you used resource constraints on your ESXi hosts, you can see which hosts were analyzed and which were skipped.

Terminating a Configuration Hardening Policy

CloudControl administrators can terminate a currently running configuration hardening job.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Policy tab.
3. Select a running configuration hardening policy that you want to terminate.
4. Select **Actions > Terminate**.
5. In the confirmation window, click **Terminate**.

Viewing the Global Compliance Dashboard

The Global Compliance Dashboard allows you to see individual results from running configuration hardening policy for all resources. From any page in CloudControl, click the green Global Compliance Dashboard icon at the top of the page. Alternatively, from the **Home** tab, select **Security > Global Compliance Dashboard**.

Global Compliance Dashboard

The Global Compliance Dashboard page is a visual overview of your current configuration hardening and security postures across all resources. The dashboard displays the following information:

- Current configuration hardening status in a pie chart. Each color on the inner donut represents a different resource. The outer donut displays the count of Compliant, Not Compliant, and Unassessed.
- Recent history of your configuration hardening activities. You can view either assessment or remediation results. Clicking on the different links shows you the following information:
  - Click the date and time link to see the assessment that was completed at that time.
  - Click the template name link to view the details of the particular template.
  - Click the policy name link to view details about the policy.
  - Click the resource name to view details about that particular resource.
- Trending information about your configuration hardening posture.

Click the expander icon in each tile to open the Views page with detailed information. You can also click the options under the **Views** menu. From the Views page, you can click the **x** icon to return to the original location.

Current Configuration Hardening Page

The current configuration hardening page displays the following information:

Field	Description
Resource Name	The name of the resource. Click the name to view the inventory page for that resource.
Resource Type	The type of resource, for example, AWSAccount or ESXi.
Status	The compliance status for that resource.
Templates	The number of templates used by that resource. Click the link to view a list in a pop-up.

You can use the filter bar to narrow down the displayed information.

Configuration Hardening Activity Page

The configuration hardening activity page displays the following information:

Field	Description
Event	The runtime of the particular configuration hardening event. Click the link to view details.
Resource Name	The name of the resource. Click the name to view the inventory page for that resource.
Score	The compliance score for the resource. The score is only displayed for assessment policies. **Note:** The assessment policy is immediately run again following a Remediation policy to ensure that the score is updated.
Policy	The policy that was used for the configuration hardening event. Click the link to view policy details.
Template	The template that was used for the configuration hardening event. Click the link to view template details.
Action Type	Whether the policy was for assessment or remediation.
Elapsed type	The total time to run the policy.

You can use the filter bar to narrow down the displayed information.

Downloading Configuration Hardening Data

After you have run a configuration hardening policy, you can download the details in a CSV file.

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the **Policies** tab.
3. In the Last Event column, click the link for the policy that you want to view.
4. On the Resources Assessed pop-up, click the date and time link to view the results from when the policy was run.

   The Assessed pop-up displays all the information about the job that was run, including the name of the policy and template used, what resource it was run against, how long it took, and the score.
   - Use the Filter to narrow down the results by Name, Time, Category, Severity, and Status.
   - Use the Sort by field to determine the order in which you want to view the results.
   - Click the More details link on any individual operation to view additional details on the operation.
   - Click the Remediation Steps link on any individual operation to view the steps required to remediate that operation if it failed.
5. Click the **Download** button to view the columns that you can select.
6. Select the columns that you want to view, and click **Download**. You can also use the search box to search for particular columns.

Updated Templates, Catalogs, and Operations

When you upgrade CloudControl to a new version, there will often be new or modified catalogs, templates, custom templates, and operations. Many of these changes are new for the specific release, but some may have been added from a configuration hardening template bundle. Those bundles are created in between releases and can be added to your existing release. All interim configuration hardening template bundles will be included in the upgrade.

During the upgrade, all system templates and catalogs will be overwritten with the new version. If you have deleted the CloudControl custom templates, then they will be replaced with a new custom template of the same name. However, if there is an existing CloudControl custom template, the new template will have the same name, but will be appended with a version number in the form _V#, where # is the new version number.

We recommend that you use the most current templates in all of your configuration hardening policies. You can continue to run policies with older versions of templates, however if there are new parameters added to operations and you modify a template containing those operations, you will receive an 'Operation param count mismatch' error.

Uploading Template and Catalog Revisions

HyTrust may periodically release revisions to the existing templates, catalogs, operations, and CloudControl custom templates to correspond with changes to standards. These revisions add new operations or updates to existing operations to ensure that your security posture remains current. With a secure upload, you can safely update your configuration hardening information between CloudControl releases.

Important: All revisions will be provided in the form of a HyTrust signed and certified configuration hardening bundle.

You can only update the bundle one time. All system templates and catalogs will be overwritten with the new version. For more information, see Updated Templates, Catalogs, and Operations above.

Procedure

1. From the Home tab, select **Security > Configuration Hardening**.
2. Click the **Template** tab and then click the **Update** button.
3. In the Update Configuration Hardening Templates window, click the **Browse** button and select the content pack file that you want to upload.
4. Click the **Upload and Validate** button.

   The Content Pack is uploaded, and the Verify Configuration Hardening Update Bundle window displays the pertinent information about the content pack.
5. Review the details and click **Apply Updates**.

   The Configuration Hardening Update Summary window displays the following information:
   - The name and type of any new templates that were added.
   - The name and type of any existing templates that were modified.
   - The name and type of any existing templates that were not affected by the update.
6. Click **OK** to close the window.

You can view the new revision number on the dashboard for each template. See Viewing Template Dashboards on page 83.

Chapter 10. Roles

About Roles

Roles are collections of privileges or permissions that define authorized operations, and usually correspond to an employee's business responsibilities. Roles are assigned using the access control trust manifest. For more information, see About Access Control Policies on page 60.

You can configure roles using basic individual operations, or use Advanced mode to choose vendor-specific parts of that operation.

Note: If you save a role after selecting Advanced mode operations, you will not be able to switch back to Basic mode without removing those operations.

Viewing Roles

1. From the **Home** tab, select **Security > Roles**.

   The system defined roles are displayed. See Default Roles on page 99.

2. From the Roles page, you can do the following:
   - Click the buttons at the top to edit or delete selected roles, or create a new one.
   - Use the **Actions** button to clone or export selected roles, or to import roles.

Creating Roles

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, click the **Create** button.
3. On the Details tab of the Add Role page, enter the name and optional description for the role.
4. Click **Continue**.
5. On the Operations tab of the Add Role page, select the operations that you want the role to perform.

   Use the Filter bar to narrow down your choices.
6. Click **Advanced** for granular selection of the vendor-specific operations. See Advanced Role Operations below.

   Note: If you save a role after selecting Advanced mode operations, you will not be able to switch back to Basic mode without removing those operations.
7. Click **Create**.

Advanced Role Operations

When you create or modify a role, you can now use Basic mode to select individual operations, or use Advanced mode to choose vendor-specific parts of that operation. The Vendor Specific column in the Operations tab displays the number of individual vendor-specific operations. In Basic mode, all vendor-specific operations are selected or deselected by default, so you will see a single digit in this column. When you click a link, you will see the read-only list of vendor-specific operations that are associated with the main operation.

When you select Advanced mode, the Vendor Specific column changes from a single digit to show how many of the vendor-specific operations are selected. For example, if the number was 3, it will change to 3/3, or three of three possible vendor-specific operations selected. If you click the link, the list of vendor-specific operations is now editable. After choosing which operations to keep, click **Apply**. The Vendor Specific column will now list the updated number vendor-specific operations selected. These changes are temporary until you click the **Save** button.

> **Note:** After you save a role after selecting Advanced mode operations, you will not be able to switch back to Basic mode without removing the vendor-specific operations.

Modifying Roles

You can only modify custom roles. If you want to modify a default role, you must clone it first, and then use the cloned role in your access control trust manifest.

> **Important:** Once a role has been assigned to a rule in a trust manifest, you cannot change the name of the role or modify the privileges.

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, select the role that you want to modify and click the **Edit** button.
3. On the Details tab, you can modify the name and optional description for the role.

4. Click the Operations tab, and select the operations that you want the role to perform.

   Use the Filter bar to narrow down your choices.

5. Click **Advanced** for granular selection of the vendor-specific operations. See Advanced Role Operations on the previous page.

   Note: If you save a role after selecting Advanced mode operations, you will not be able to switch back to Basic mode without removing those operations.

6. Click **Save** to save your choices without closing the window, or **Save and Close** to close the window after saving.

Cloning Roles

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, select the role that you want to clone.
3. Select **Actions > Clone**.
4. On the Details tab of the Clone Role page, you can modify the name and optional description that were in the original role. By default, the name is appended with _clone.
5. Click **Continue**.
6. On the Operations tab of the Clone Role page, you can modify the operations that were in the original role.

   Use the Filter bar to narrow down your choices.

7. Click **Clone** to clone the role.

Exporting Roles

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, select the role or roles that you want to export.
3. Select **Actions > Export**.

The roles are saved and downloaded as a .json file.

Importing Roles

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, select **Actions > Import**.
3. On the Import page, browser to the location of the file that you want to import and click **Import**.

Deleting Roles

1. From the **Home** tab, select **Security > Roles**.
2. On the Manage Roles page, select the roles that you want to remove and click the **Delete** button.
   Note: System defined roles cannot be deleted.
3. Click **Delete** in the confirmation window.

Default Roles

The following roles are system roles that are automatically added to CloudControl. These roles are all view-only. If you want to modify a default role, you must clone it first.

Role Name	Role Description
ASC_SuperAdmin	The default super administrator role. Can perform all operations.
ASC_CloudAdmin	The default cloud administrator role. Can perform all operations assigned to the cloud administrator for any of your CloudControl-protected environments.
ASC_CloudControlAuditor	View-only privileges in CloudControl.
ASC_ContainerInfraAdmin	Full access to create/edit/delete/connect operations on pod/deployment/service/namespace/node resources of Kubernetes/OpenShift cluster(s).
ASC_ContainerSecurityAdmin	Full access to all security controls related operations in CloudControl to author and manage the security posture of Kubernetes/OpenShift cluster (s) resources.
ASC_NetworkEngineer	Full access to most networking resources, including logical switches, transport zones, and IP pools. Read-only access to core security-related resources.
ASC_NetworkOperator	Read and write access to most networking resources including logical switches, transport zones, and IP pools. Read-only access to core security-related resources
ASC_LoadBalancerAdmin	Full access to load balancer-related networking resources.
ASC_VPNAdmin	Full access to VPN networking resources.
ASC_SecurityAuditor	Read-only access to security-related resources.
ASC_SecurityOperator	Read-only access to security operations.
ASC_SecurityAdmin	Full access to security-related resources including firewalls, security groups, IP sets, MAC sets, and services.
ASC_StorageAdmin	Full access to all storage operations.

ASC_NetworkAdmin	The default network administrator role. Can manage virtual networks, virtual switches, and VLANS.
ASC_VMPowerUser	Can start, stop, and suspend VMs, view and change most virtual machine configuration settings, and take snapshots.
ASC_DatacenterAdmin	Can perform actions on all resources within datacenters.
ASC_HostAdmin	Can perform ESXi host maintenance, management, and configuration.
ASC_BoundaryControlUser	The Boundary Control role. This role has privileges to authorize keys from KeyControl based on the boundary control trust manifest.

Chapter 11. View Hiding

About View Hiding

CloudControl enables you to restrict users from viewing vSphere resources if they do not have explicit view privileges. Resources can be hidden whether you use the vSphere HTML5 Client or the WCS client.

You can enable view Hiding at the vCenter level. Once enabled, the <resource_type>.View_All_Children operation is used to show if a resource can be viewed. When enabled for a role, you can use that role in an access control trust manifest to restrict what resources can be viewed, or use resource tags to limit what part of the same resource can be viewed.

View hiding is disabled by default as it can take longer for the responses to be filtered.

View Hiding Roles

The view hiding roles can be managed on the Operations tab of a new or existing role. You can navigate to the Roles page, select or create a role, and proceed to the Operations tab. For more information, see Creating Roles on page 97 or Modifying Roles on page 97.

From the Operations tab, you can click View Hiding in the filter bar to view the View_All_Children operations in the following locations:

- Compute
  - Cluster—View Host clusters and all child hosts.
  - Datacenter—View Datacenter and all child folders, hosts, virtual machines, datastores and network resources.
  - HostFolder—View Host folders and all child clusters and hosts.
  - Hostsystem—View Hosts and all child resources.
  - VMFolder—View VM folders and all virtual machines.

- Network
  - Folder—View Network folder and all child distributed virtual switch, networks and portgroups.
  - Port—View DVportgroup.
  - Switch—View DVSwitch and all child portgroups.
- Storage
  - Datastore—View Datastores and all child resources.
  - Folder—View Storage Folder and all child datastore clusters and datastores.

Existing roles may or may not have View_All_Children operations selected. For example, the ASC_NetworkAdmin role by default has the Network folder, port, and switch View_All_Children operations selected. You can either create new roles or modify existing roles as needed for your environment.

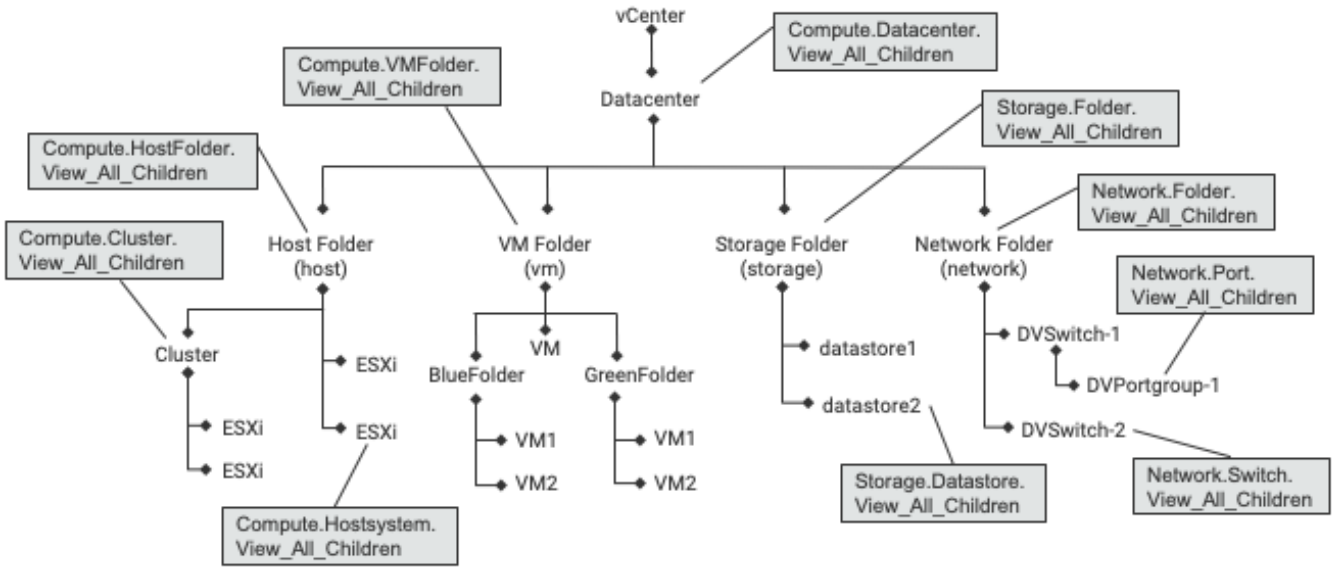
vCenter Resources and View Hiding Operations

Resources are visible when the following criteria are met:

- The user has the View_All_Children privilege on that particular resource.
- The user has the View_All_Children privilege on a child of the resource.
- The user has the View_All_Children privilege on an ancestor of the resource AND the privilege is not overridden by the trust manifest associated with the resource.

For example, using the image below, if the View_All_Children privilege is assigned to the VM folder, then the user can view everything in the VM folder, but nothing in the Host, Storage, or Network folders. If the View_All_Children privilege is assigned to Storage.Datastore, then everything at the datastore level AND the Storage folder can be viewed.

Tags can be assigned to all resources to restrict resource visibility except for individual VMs. VMs are dependent on their parent folder, so in this example, you can use tags on BlueFolder and GreenFolder to affect their respective VMs, but not the any VMs that are under the top-level VM folder.



Enabling or Disabling View Hiding

You can enable or disable view hiding from the vSphere inventory pages.

Enabling View Hiding

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Management** link.
3. On the Management vCenters tab, select the vCenter for which you want to enable view hiding.
4. On the vCenter page, in the Details area, click the **Disabled** link for the View Hiding field.
5. In the View Hiding window, change the Status to enabled and click **Apply**.

Disabling View Hiding

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Management** link.
3. On the Management vCenters tab, select the vCenter for which you want to disable view hiding.
4. On the vCenter page, in the Details area, click the **Enabled** link for the View Hiding field.
5. In the View Hiding window, change the Status to disabled and click **Apply**.

Using Trust Manifests with View Hiding Example

After you have created or modified the role that you want to use, you need to use that role in an access control trust manifest. For this, you will need:

- The role that you want to use.
- The constraints to limit who can view what resources.
- Tags on the resources you want to limit.

For this example, there are individual tenants called Blue and Green. For more information, see the image on vCenter Resources and View Hiding Operations on the previous page. Each tenant has two VMs under the folders BlueFolder or GreenFolder, and you need to ensure that they can only see their own VMs and not any other tenants.

1. Create a role called Tenant_Role that has the Compute.VMFolder.View_All_Children operation.
2. Create an AD user called Blue@tenant.com that you want to grant permissions to view the BlueFolder VMs, and an AD user called Green@tenant.com that you want to grant permissions to view the GreenFolder VMs.
3. Create a new tag called Tenant that has two values: Blue and Green. For more information, see Creating Tags on page 105.
4. Assign the Blue tag to BlueFolder and the Green tag to GreenFolder. For more information, see Assigning Tags to Resources on page 106.

5. Create an access control trust manifest. For more information, see Creating an Access Control Trust Manifest from the CloudControl GUI on page 60.
6. Add a rule to the access control rules that have the following properties:

Field	Expected Value
Name	BlueRule
Role	Tenant_Role
Subjects	Blue@tenant.com
Resource Tag Constraints	Name: Tenant Tag Value: Blue Resource Types: ComputeCollection

7. Repeat the above steps for the Green user and Green tagged resource.
8. Click **Save** and then **Publish**.
9. Assign a resource to your trust manifest. This resource must contain both the BlueFolder and the GreenFolder.
10. Log in to your vCenter as the Blue or Green user to verify that only that resource can be viewed.

Chapter 12. Tagging

About Tags

Tags are a key/value pair that you can use to distinguish and group resources. Each tag can be assigned to multiple resources. CloudControl supports the following types of tags:

- Imported System tags—Any tag or tag assignment imported from a third-party platform, such as Kubernetes. These tags are read-only, but can be used in search and deployment control.
- Customer-defined tags—Any tag created by users. These tags are fully editable, and can be used in search, RBAC, and deployment control. These tags are for use in CloudControl only, and cannot be pushed to Kubernetes.

You can assign any customer-defined tag to a resource, either in the Tag Management page, or when viewing the resource inventory page.

Creating Tags

1. From the **Home** tab, select **Security > Tag Management**.
2. On the Tag Management page, click the **Create** button.
3. In the Create Tag wizard on the Details page, enter the name and select a color to represent the tag.
4. Enter an optional description and click **Continue**.
5. On the Values page, click the **Add** button.
   Note: If there are no values for the tag, you can also click the **Add Values** link.
6. On the Add Tag Value to page, add a tag value and optional description.
7. Click **Add** to add the tag value.
8. Click the **Add** button to add another tag value, or click **Create** to create the tag.

Managing Tags

1. From the **Home** tab, select **Security > Tag Management**.
2. On the Manage Tags page, you can perform the following:
   - View all existing tags.
     You can use the filter to narrow your view.
   - Click the **Create** button to add a new tag.
     See Creating Tags on the previous page.
   - Click on a tag, or select a tag and click the **Edit** button to make changes to an existing custom tag.
     See Modifying Tags below.
     Note: You can only modify custom tags.
   - Select one or more tags and click the **Delete** button to permanently remove tags.
     Note: You can only delete custom tags.
     See Deleting Tags on the next page.

Modifying Tags

1. From the **Home** tab, select **Security > Tag Management**.
2. On the Manage Tags page, click on a tag, or select a tag and click the **Edit** button.
3. In the Tag window, make changes to the Details page, or click **Values** to make changes to the Values page.
4. Click **Save** to save your current changes and make additional changes.
   Note: If you have made changes to either the Details or Values page, you must click Save before you can click the other tab. If you do not, you will be prompted to save or discard your changes before you can continue.
   For more information, see Creating Tags on the previous page.
5. Click **Save and Close** if you have finished making changes.

Assigning Tags to Resources

You can assign tags to any existing resources from the inventory page.

1. From the resource page, select the resource where you want to assign a tag.
2. Select **Actions > Assign Tags**.
3. In the Assign Tags wizard on the Tags page, select the tag that you want to assign.
   You can use the filter to narrow your choices.
4. Click **Continue**.

5. On the Values page , select the tag values that you want to assign to the resource.
6. Click **Assign**.

Batch Assigning Tags to Resources

If you filter on a group of resources, you can batch assign tags to those resources.

1. Navigate to the resource page where you want to assign a tag.
2. Use the filter to narrow down the list of resources.

   For example, for AWS, you could filter on resources to see how many virtual machines are in a particular region. For vSphere, you could filter on host to see how many virtual machines are on that host. For Kubernetes, you could filter on pods to see what containers are on a particular pod.
3. Check the select all checkbox at the top of the list of results. All results are selected, even if they are not displayed.
4. Select **Actions > Assign Tags**.
5. In the Assign Tags wizard on the Tags page, select the tag that you want to assign, or create a new tag.

   You can use the filter to narrow your choices.
6. Click **Continue**.
7. On the Values page, select the tag values that you want to assign to the group of resources.
8. Click **Assign**.

Unassigning Tags from Resources

1. From the resource page, select the resource where you want to unassign a tag.
2. Select **Actions > Unassign Tags**.
3. In the Unassign Tags wizard on the Tags page, select the tag that you want to remove.

   You can use the filter to narrow your choices.
4. Click **Continue**.
5. On the Values page, select the tag values that you want to remove.
6. Click **Unassign**.

Deleting Tags

Note: You can only delete tags that are not assigned to any resources.

1. From the **Home** tab, select **Security > Tag Management**.
2. On the Manage Tags page, select the tag or tags that you want to delete.

3. Click **Delete**.
4. Review your choices, and click **OK** in the confirmation dialog box.

Chapter 13. Log Analysis

About the Log Analysis Page

The Log Analysis page displays all log messages received through CloudControl. Log messages classify and describe all administrative actions and events that have occurred in the virtual infrastructure. By default, CloudControl retains long messages for 180 days.

Log messages are displayed in a table with the following default columns:

- Time
- Priority
- User
- Action
- Resource Name
- Policy Mode
- Status

You can sort each column in ascending or descending order, drag the columns to change the table order, or click the Columns **button** to choose which columns to display.

Note: The Time, Priority, User, Action, and Resource Name columns cannot be hidden.

Viewing Log Messages

1. From the Home tab, select **Security > Log Analysis**.
2. Click a log to view the details of each log message.
3. Click **Close** to close the details window.

Filtering Log Messages

Use the Filter bar to limit the number of log messages displayed.

Click the Filter bar and select **Last Day**, **Last Week**, or **Last Month** to quickly filter by date. If you select a different date range, the filter changes.

To filter by column:

1. Click the Filter bar and:
   - Select the column to use for the filter.
   - Select whether the value will be equal or not equal to the contents of the column.
   - Select the value to filter by. Some values are predefined and can be selected from a list of values, and other values must be manually entered.
2. Click **Add**.

All created filters appear in the Filter bar. You can only have one filter per column type. Click the x for a filter to remove that filter from the list. Click the x for the Filter bar to remove all filters.

Changing the Log Retention

By default, CloudControl retains long messages for 180 days. You

1. From the Home tab, select **Security > Log Analysis** or **System > System Logs**.
2. At the top right corner of the Log Analysis or System Logs page, click the (**change**) link next to the retention time.
3. In the Set Retention Time window, change the number of days that you want to retain logs.
   The retention time should be between 10 and 365 days.
4. Click **Apply**.

Chapter 14. Certificates

Viewing Certificate Details

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. Click the Services or Certificate Authorities tab.
4. Click the link for the service or certificate authority that you want to view.
5. Click **Close**.

Generating a Self-Signed Certificate

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, select a service, and then select **Actions > Generate Self-Signed Certificate**.

4. On the Generate Self-Signed Certificate page Details tab, complete the following information:

Field Name	Description
Common Name	The FQDN used for DNS lookups.
Locality	Optional. The city.
State	Optional. For US and Canadian countries, enter the full state or province name. Do not abbreviate.
Country	The 2-character ISO format country code.
Organization	Optional. The company name.
Organization Unit	Optional. The section name in the company.
Key Size	Select 2048-bit or 4096-bit.

5. Click **Continue**.
6. On the SAN tab, you can add subject alternative hostnames and addresses to the certificate.

   The DNS name and IP address that you used when deploying CloudControl are displayed by default. You can have up to 16 DNS names and 16 IP addresses. To add additional subject alternative names:

   a. Click the **Create** button.

   b. On the Subject Alternative Name window, select either DNS Name or IP Address and add the value in the field.

      For the DNS name, you can also use wildcards before the domain name, for example, *.example.com.

   c. Click **OK**.
7. Click **Continue**.
8. In the confirmation box, click **Continue**.

   After the services are restarted with the new certificate, the browser will automatically be reloaded and you will need to log in to CloudControl again.

Generating a Certificate Signing Request

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, select a service, and then select **Actions > Generate CSR**.

4. On the Generate CSR page Details tab, complete the following information:

Field Name	Description
Common Name	The FQDN used for DNS lookups.
Locality	Optional. The city.
State	Optional. For US and Canadian countries, enter the full state or province name. Do not abbreviate.
Country	The 2-character ISO format country code.
Organization	Optional. The company name.
Organization Unit	Optional. The section name in the company.
Key Size	Select 2048-bit or 4096-bit.

5. Click **Continue**.
6. On the SAN tab, you can add subject alternative host names and addresses to the certificate.

   The DNS name and IP address that you used when deploying CloudControl are displayed by default. You can have up to 16 DNS names and 16 IP addresses. To add additional subject alternative names:

   a. Click the **Create** button.

   b. On the Subject Alternative Name window, select either DNS Name or IP Address and add the value in the field.

      For the DNS name, you can also use wildcards before the domain name, for example, *.example.com.

   c. Click **OK**.
7. Click **Continue**.
8. In the confirmation box, click **Continue**.

   At this point, you can send the CSR to your signing authority to get a signed certificate.

What to Do Next

After you receive the SSL certificate from your signing authority, you will need to install it. See Installing an SSL Certificate on the next page.

Retrieving the Last Certificate Signing Request

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, select a service, and then select **Actions > Retrieve Last CSR**.

   The Last CSR page displays that details for the last CSR that you generated. You can copy the data to send to your certificate authority.
4. Click **Close**.

Installing an SSL Certificate

After you have generated your CSR and sent it to your signing authority, you will receive an SSL certificate. Install this certificate using the same service that you selected when you generated the CSR.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, select a service, and then select **Actions > Install Certificate**.
4. On the Install Certificates page, choose one of the following:
   - Click the **Import** radio button and click the **Browse** button to locate your certificate file.
   - Click the Enter Text radio button and copy and paste the certificate data in the Certificate Data field.

   Important: The certificate must be in Base64-encoded pem format.
5. Click **Continue** to install the certificate.

Installing an Rsyslog Certificate

From the **Home** tab, select **System > System Settings**.

On the System Settings page, select **Settings > Certificates**.

3. On the Services tab, check the **Rsyslog Service** checkbox.

   Important: If you want to use your own certificate for Rsyslog, you will need to generate a certificate signing request, submit it to the signing authority, and then install the SSL first. See Generating a Certificate Signing Request on page 112 and Installing an SSL Certificate above.
4. Select **Actions > Install Certificate**.
5. On the Install Certificates page, choose one of the following:
   - Click the **Import** radio button and click the **Browse** button to locate your certificate file.
   - Click the Enter Text radio button and copy and paste the certificate data in the Certificate Data field.

   Important: The certificate must be in Base64-encoded pem format.
6. Click **Continue** to install the certificate.

Installing a Web Application Certificate

If you plan to use a certificate chain, you must include the following IN THIS ORDER in the Certificate Data text field:

- The signed certificate (SSL) from your generated Certificate Signing Request.
- The Certificate Authority, if necessary.
- The private key (required if the CSR was generated outside of this CloudControl instance).

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, check the Web Application service checkbox.
4. Select **Actions > Install Certificate**.
5. On the Install Certificates page, do one of the following:
   - Click the **Import** radio button and click the **Browse** button to locate your certificate file.
   - Click the Enter Text radio button and copy and paste the certificate data in the Certificate Data field.

   Important: The certificate must be in Base64-encoded pem format.
6. Click **Continue**.
7. Review the certificate details and click **Install**.

   After the services are restarted with the new certificate, the browser will automatically be reloaded and you will need to log in to CloudControl again.

Downloading a Certificate

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. On the Services tab, select a service, and then select **Actions > Dow**

Installing a Certificate Authority

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. Select the Certificate Authorities tab, and click the **Install** button.

   Note: If there are no certificate authorities installed, you can also click the **Install Certificate Authorities Now** link.
4. On the Install Certificates page, do one of the following:
   - Click the **Import** radio button and click the **Browse** button to locate your certificate file.
   - Click the Enter Text radio button and copy and paste the certificate data in the Certificate Data field.

   Important: The certificate must be in Base64-encoded pem format.
5. Click **Continue**.
6. Review the certificate details and click **Install**.

Deleting a Certificate Authority

We recommend that you do not delete a certificate that is used for communication with a resource that has been added to CloudControl. CloudControl will no longer be able to communicate with the resource, and you will no longer be able to view any information on that resource.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Certificates**.
3. Select the Certificate Authorities tab.
4. Select the certificate that you want to delete and click the **Delete** button.
5. Check the confirmation checkbox and click **OK**.

Chapter 15. Boundary Control

About Boundary Control

The Boundary Control feature uses the boundary control trust manifest in HyTrust CloudControl to authenticate and authorize delivery of encryption keys to the data encrypted and managed by HyTrust KeyControl.

When you create a Cloud VM Set in KeyControl, you can link that Cloud VM Set to CloudControl. The link, or applink, is how CloudControl and KeyControl share uplink data.

KeyControl has no reference to boundaries. The boundaries are defined in CloudControl by a trust manifest.

KeyControl requests a key to the encrypted data whenever changes are made to the VM, such as registering a VM, powering on a VM, or moving the VM between hosts in the Cloud VM set. At this point, KeyControl sends an authentication request to CloudControl. CloudControl uses the UUID received from KeyControl to identify the VM, and then authorizes the key delivery only if the VM is located inside the boundary defined by the boundary control trust manifest. If not, then the authorization is denied.

Overview of Boundary Control Steps

To use Boundary Control , you need to perform some tasks in CloudControl and some in KeyControl.

Step	Description	Notes
1	Create a boundary control trust manifest. This is automatically assigned to Appliance Root. Define the conditions when a VM is considered inside the boundary.	See About Boundary Control Policies on page 63.
2	Initiate an app link in CloudControl.	See Initiating an App Link on the next page.
3	Use the CloudControl app link single-use code to register an applink in KeyControl.	See Linking KeyControl with CloudControl in the *HyTrust DataControl Administration Guide*.

Step	Description	Notes
4	Create a Cloud VM Set in KeyControl. In the Select an AppLink to enable Boundary Controls field, select the App Link that you created. **Important:** Both the vCenter and the individual ESXi hosts in the Cloud VM Set must be added to CloudControl in order to use boundary control.	See Creating a Cloud VM Set in the *HyTrust DataControl Administration Guide*.

Initiating an App Link

To connect CloudControl and KeyControl, you will need to initiate an app link and generate the code. The code is a single-use code that is valid for 10 minutes.

KeyControl also requires the CloudControl IP address and certificate. To obtain the CloudControl certificate, see Downloading a Certificate on page 115.

1. From the **Home** tab, select **System > App Links**.
2. Click **Initiate App Link**.
3. In the Initiate App Link window, click **Generate Code**.

   Note: For this release, Boundary Control is the only type of app link supported, and ASC_BoundaryControlUser is the only role.
4. Copy the code to your clipboard. The code and the certificate will be needed by KeyControl when you link KeyControl to CloudControl.
5. Click **Close**.

Manage App Links

The App Links page displays all app links that have been initiated in CloudControl and accepted in KeyControl. Each app link displays the following information:

- Name—The name of the app link when linked to KeyControl.
- App Link ID—The ID for the app link. This is the same for both CloudControl and KeyControl.
- Role—The CloudControl role used by the app link.
- App Link IPs— The CloudControl IP address used for the app link.
- Last Used—The last time the app link was used.
- Created—The time the app link was created.
- Status—The status of the app link. This can be active or deactivated.

You can filter the app links by any of these labels. From this page, you can also initiate new app links or deactivate existing app links.

Deactivating an App Link

If you deactivate an app link, the connection between CloudControl and KeyControl will no longer be valid.

1. From the **Home** tab, select **System > App Links**.
2. Select the app link that you want to remove and click **Deactivate**.
3. In the Deactivate App Link window, check the confirmation checkbox and then click **Deactivate**.

Chapter 16. Trust Attestation

About Trust Attestation

Trust Attestation utilizes Intel® Trusted Execution Technology (Intel® TXT) and ISecL (Intel® Security Libraries) to establish comprehensive hardware-based trust on managed ESXi hosts that use Trusted Platform Modules (TPM) chips. TXT and TPM are used to verify the integrity of the platform.

A fingerprint is a set of host measurements. Fingerprints from a particular host are captured in CloudControl and used to determine the trust status of hosts by adding them to a trust manifest. If the fingerprint of a host matches the fingerprint in an associated trust manifest, then the host is labeled Trusted. Otherwise, the host is labeled Not Trusted. For more information, see About Trust Attestation Policies on page 76.

Trust Attestation is automatically enabled in CloudControl. Trusted hosts can be viewed on the vSphere inventory page. See Viewing Trust Attestation Details and Reports on the next page.

Capturing Trust Attestation Fingerprints

You can capture fingerprints from ESXi hosts managed by CloudControl that use Trusted Platform Modules (TPM) chips.

1. From the **Home** tab, select **Security > Trust Attestation Fingerprints**.
2. On the Trust Attestation Fingerprint Management page, click the **Capture** button.
   Note: If there are no existing trust attestation fingerprints, you can also click the **Capture a Fingerprint now** link.
3. On the Resources tab of the Capture Fingerprints page, select the host where you want to capture the fingerprint.
   CloudControl displays the ESXi hosts with TPM modules.
4. Click **Continue**.

5. On the Fingerprints tab, select the fingerprints that you want to save, and enter the name and optional description for the fingerprints.
   - Platform—Includes the BIOS name and version.
   - OS—Includes the VMware name and version.
6. Click **Create**.

   Tip: You can also capture fingerprints by selecting the host on the vSphere hosts page and then selecting **Actions > Capture Fingerprint**.

Manage Trust Attestation Fingerprints

The Trust Attestation Fingerprint Management page displays all fingerprints that have been captured in CloudControl. Fingerprints with a green checkmark are currently in use by a Trust manifest. Each fingerprint displays the following information:

- Name—The name assigned to the fingerprint.
- Type—The type of fingerprint. This can be platform or OS.
- Description—The optional description given to the fingerprint.
- Details—The details of the fingerprint.
- Captured On—The date the fingerprint was captured by CloudControl.

You can filter the fingerprints by any of these labels. From this page, you can also capture new fingerprints and edit or delete existing fingerprints.

Viewing Trust Attestation Details and Reports

After creating and publishing the trust attestation trust manifest, you can see the results on the inventory pages for the resources assigned to the trust manifest. For each host, you can view the trust attestation status and details, including detailed trust attestation reports.

Note: You can also run a high-level report to see an overview of which hosts are trusted. See Creating a Report on page 138.

1. From the **Home** tab, select **Inventory > vSphere**.
2. On the **vSphere** page, click the **Compute** link, and then click the **Hosts** link.

   You can quickly see which hosts are trusted. CloudControl displays a green check for hosts that are trusted, and a red x for hosts that are not trusted.
3. Click on the host that you want to view.
4. In the Details section, click the Trust Attestation Status link. This can be Trusted, Not Trusted, or Unassessed.

   In the Trust Attestation Report popup, you can quickly see the status of the individual fingerprints. If the measurements were met for both, then both will say Trusted. If not, one or both of the fingerprints will say Not Trusted.

5. Click the expand arrows in the Trust Attestation Report popup for more details.
6. In the Trust Attestation Report page, you can view the full details for which rule and flavor ID does not match the original fingerprint.

   Note: The flavor ID refers to the individual measurement that was not matched.
7. Click the **Download Full Report** button to download the report in PDF format.

Editing Trust Attestation Fingerprints

1. From the **Home** tab, select **Security > Trust Attestation Fingerprints**.
2. On the Trust Attestation Fingerprint Management page, select the fingerprint that you want to modify.
3. Click **Edit**.
4. Modify the name or description of the fingerprint.
5. Click **Apply**.

Deleting a Trust Attestation Fingerprint

1. From the **Home** tab, select **Security > Trust Attestation Fingerprints**.
2. On the Trust Attestation Fingerprint Management page, select the fingerprint that you want to delete.
3. Click **Delete**.

Chapter 17. Multi-Factor Authentication

About Multi-Factor Authentication

CloudControl multi-factor authentication requires users to provide two forms of identification to login. CloudControl supports the following multi-factor authentication types:

- Radius
- Identity Provider

You can also configure a whitelist which allows users to bypass multi-factor authentication and log in directly.

Configuring Multi-Factor Authentication

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Configuration** tab.

3. Select the authentication type that you want to use.
   - If you selected **Radius**, complete the following:

Field	Value
Server IP Address	The RADIUS server IP address.
Port	The port number for the RADIUS server.
Secret Message	The secret message defined for secure communication with the RADIUS server.
Authentication Mode	Select the authentication method you want to use. CloudControl supports: ◦ PAP (Password Authentication Protocol) ◦ CHAP (Challenge Handshake Authentication Protocol)

   - If you selected **Identity Provider**, select the identity provider that you want to use.
     If you do not have an identity provider, see Importing Identity Provider Metadata below.
4. Click **Enable**.

Importing Identity Provider Metadata

To import Identity Provider metadata, you must either have configured multi-factor authentication with the Authentication Type set to Identity Provider, or be in the process or configuring it.

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Configuration** tab.
3. In the Authentication Type field, select Identity Provider.
4. Click **Import**.
   If you do not have an identity provider, you can also click the **Import Identity Provider Metadata Now** link.
5. On the Import Identity Provider Metadata window, select one of the following:
   - Click the **Import File** radio button and click the **Browse** button to locate the metadata that you want to import.
   - Click the **Enter Text** radio button and copy and paste the metadata.
6. Click **Add**.

Configuring the Multi-Factor Authentication Whitelist

Users on the whitelist are exempt from multi-factor authentication and can log in directly.

Adding a user to the whitelist:

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Whitelist** tab.

3. On the Whitelist page, click **Add**.

   Note: If there are no users on the whitelist, you can also click the **Add a User Now** link.

4. On the Add User page, enter the user and an optional description.
5. Click **Add**.

Editing a user on the whitelist:

You can edit the description for users on the whitelist.

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Whitelist** tab.
3. On the Whitelist page, select the user that you want to edit.
4. On the Edit User page, update the description.
5. Click **Apply**.

Removing a user from the whitelist:

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Whitelist** tab.
3. On the Whitelist page, select the user that you want to remove.
4. Click **Delete**.
5. On the confirmation page, click **Delete**.

Disabling Multi-Factor Authentication

1. From the **Home** tab, select **System > Multi-Factor Authentication**.
2. On the Multi-Factor Authentication page, click the **Configuration** tab.
3. Click **Disabled**.

Chapter 18. System Settings

Viewing the System Settings Dashboard

Select **System > System Settings** from the Home tab to view the System Settings dashboard.

The System Settings dashboard displays the following information:

- System Information

  Displays the host name, software version, the management IP address, and whether or not the Vitals Service is enabled.

- Licensing Details

  Displays information about your licenses including the expiration date, status, type of license, and how many days are remaining.

  Click the expander icon to open the Licensing page with detailed information. From the Licensing page, you can click the **x** icon to return to the original location.

- Resources

  Displays information on your certificates, CPU, disk, and memory usage, high availability and networking.

- Recent System Jobs

  Displays links to the recent CloudControl system jobs based upon status. Clicking the number takes you to the System Jobs page filtered by that status.

  Click the expander icon to open the System Jobs page. From the System Jobs page, you can click the **x** icon to return to the original location.

Using the HyTrust Vitals Service

The HyTrust Vitals Service lets you automatically share information about the health of your CloudControl instance with HyTrust Support. When enabled, CloudControl periodically sends an encrypted bundle containing system status and diagnostic information to a secure HyTrust server. HyTrust Support may proactively contact you if the Vitals Service identifies issues with the health of your cluster.

Note: You cannot disable the Vitals Service during the Trial license period.

The following information is always collected, but the Vitals bundles are only sent to HyTrust when the Vitals Service is enabled.

- The Vitals Service checks for potential problems with the CloudControl instance once per day.
- If errors exist, the Vitals Service generates and stores a diagnostic-level Vitals bundle.
- If no error exists, the Vitals Service generates and stores an information-level Vitals bundle every week.

You can generate a Vitals Service request at any time to capture the current state of your system and send the generated Vitals bundle to HyTrust Support for error diagnosis or documentation.

Note: CloudControl sends the encrypted bundle to https://vitals.hytrust.com via port 443.

Enabling the Vitals Service

You have the option of enabling the Vitals Service to transfer Vitals bundles during the CloudControl setup procedure, or you can enable it at any time from the System Settings page.

1. From the **Home** tab, select **System > System Settings**.
2. Select **Actions > Enable Vitals**.
3. Click **OK** in the confirmation window.

   A message appears at the top of the System Settings page to indicate whether or not the Vitals Service was successfully enabled.

Disabling the Vitals Service

1. From the **Home** tab, select **System > System Settings**.
2. Select **Actions > Disable Vitals**.
3. Click **OK** in the confirmation window.

   A message appears at the top of the System Settings page to indicate whether or not the Vitals Service was successfully enabled.

Creating a Vitals bundle

1. From the **Home** tab, select **System > System Settings**.
2. Select **Actions > Create Vitals Bundle**.
3. Click **Yes** in the confirmation window.

   If the Vitals Service is enabled, a bundle will be saved on your system as well as automatically send it to HyTrust.

Downloading a Vitals bundle

1. From the **Home** tab, select **System > System Settings**.
2. Select **Actions > Create Vitals Bundle**.
3. Click **Download** in the confirmation window.
   The Vitals bundle is automatically downloaded.

Viewing the System Jobs Page

The System Jobs displays all system jobs that are schedule to run in CloudControl.

1. Select **Home > System > System Settings**.
2. Click **Views** and then select **System Jobs**.
3. On the System Jobs page, select the **Job Details** tab.
   On the Job Details page, you can view the following:

Column	Description
Job Name	The name of the job. Click the link to view the details. If you want to edit the job, see Editing System Jobs Scheduling below.
Job Description	The description of the job.
Schedule	How often the job is schedule to run.
Next Scheduled Run	The date and time the job will run next.
Last Run	The date and time when the job was last run. Click the link to view the job details.

   You can use the filter to limit the jobs that are displayed.

If you reach this page by clicking on a value in the Recent System Jobs section on the System Settings dashboard, you can click the **x** icon to return to the original location.

Editing System Jobs Scheduling

By default, the system jobs start to run depending on when CloudControl was installed. You can change the scheduling so that they run when you determine is the best time.

Depending on the job, the scheduling can be edited in different ways:

- Some jobs allow you to disable the job.
- Some jobs can only run daily, but you can set the time when they run.
- Some jobs must run daily, but also allow you to run them at hourly periods.
- All jobs allow you to run the job immediately.

You will need to look at the details for each job to see what changes you can make.

Editing the Job Schedule

1. Select **Home > System > System Settings**.
2. Click **Views** and then select **System Jobs**.
3. On the System Jobs page, select the **Job Details** tab.
4. Select the job that you want to edit and click the **Edit** button.
   Alternatively you can simply click the Job Name link.
5. Click the Schedule tab and update the job schedule as necessary.
6. Click **Save**.

Running one or more jobs now

1. From the Job Details tab, select the job or jobs that you want to run immediately.
2. Select **Actions > Run Now**.

Terminating a job

1. From the Job Details tab, select the job or jobs that you want to terminate.
2. Select **Actions > Terminate**.

Viewing the System Jobs Event History

The System Jobs displays the history of all system jobs that have run in CloudControl.

1. Select **Home > System > System Settings**.
2. Click **Views** and then select **System Jobs**.

3. On the System Jobs page, select the **Event History** tab.

   On the Event History page, you can view the following:

Column	Description
Job Name	The name of the job. Click the link to view the details.
Job Description	The description of the job.
Start Time	The date and time when the job was started.
End Time	The date and time when the job ended.
Status	This can be one of the following: • Completed • Failed • Terminated

   You can use the filter to limit the jobs that are displayed.

   The Hide internal jobs checkbox is selected by default. If you want to view internal jobs, uncheck the checkbox.

If you reach this page by clicking on a value in the Recent System Jobs section on the System Settings dashboard, you can click the **x** icon to return to the original location.

Modifying your DNS Settings

Your DNS settings are configured during installation. You can modify them at any time.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > DNS**.
3. On the DNS page, modify the following as necessary:

Field	Description
DNS IP Address	The IP address of the DNS server. You must have at least one DNS server, and up to three DNS server addresses are supported.
Domain Name	The domain name for CloudControl.

4. If you want to verify the connection, click **Test**.
5. Click **Save**.

Modifying your Email Settings

Your SMTP and email information settings are configured during installation. You can modify them at any time.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Email**.
3. On the Email page, select **ON** or **OFF** to enable SMTP.
4. Modify the following as necessary:

Field	Description
SMTP Server Name or IP Address	The name of the SMTP server used by email or its IP address. The name or IP address can be from 2-255 characters and cannot include spaces or the following special characters: `, ~ : ! @ # $ % ^ & ' ( ) [ ] { }`
Port	The TCP Port that the SMTP server uses for communication. The default is port 25.
Sender	The email address from which the system sends email. The email address can be from 1-255 characters, and cannot include spaces.
Security	Select one of the following: None—Use no security for your SMTP server. This is the default. SSL—Use SSL for your SMTP server. TLS—Use TLS for your SMTP server.
User Name	Enter the username for the SMTP server.
Password	Enter the password for the SMTP server.
Re-enter Password	Re-enter the password for the SMTP server.

5. If you want to verify the connection, click **Test**.
6. Click **Save**.

Licensing

CloudControl is a licensed product. You can view an overview about your current license in the Licensing Details section of the System Settings page, and a complete list on the Licensing page.

CloudControl uses https://my.nalpeiron.com on port 443 for the license server.

Viewing Your CloudControl Licenses

1. From the **Home** tab, select **System > System Settings**.

   The Licensing Details section of the System Settings page displays an overview of your current license.

2. Select **Settings > Licensing**.
   - On the Licenses tab, you can view your current licenses, including activation key, entitlements, type, expiration date, and status.
   - On the Entitlements tab, you can view entitlement details, including name, description, and usage of the entitlements.

Adding a License

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Licensing**.
3. Click the **Add** button.
4. In the Add License window, choose one of the following:
   a. Select the **Import License** radio button, then click **Browse** and choose the license file that you want to import.
   b. Select the **Enter License** radio button, then paste the contents of the license file in plain text.
   c. Select the **Activation Key** radio button, then paste the license key.
5. Click **Add**.

Verifying a License

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Licensing**.
3. Select the license that you want to verify and click **Verify**.
4. In the Verify License window, click **Verify**.
   A message appears indicating that the license was verified successfully.

Replacing a License

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Licensing**.
3. Select the license that you want to replace and click **Replace**.
4. In the Replace License window, choose one of the following:
   a. Select the **Import License** radio button, then click **Browse** and choose the license file that you want to import.
   b. Select the **Enter License** radio button, then paste the contents of the license file in plain text.
   c. Select the **Activation Key** radio button, then paste the license key.
5. Click **Replace**.

Removing a License

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Licensing**.
3. Select the license that you want to remove and click the **Delete** button.

Enabling a Proxy Server for the Vitals Service and Licensing Service

You can configure a proxy server to use for both the Vitals Service and licensing.

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Web Proxy**.
3. Enter the IP address for the proxy server and the port number.
4. Enter the username and password for the proxy server.
5. Select Enabled for the services for which you want a proxy.
6. Click **Save**.

Modifying your NTP Settings

NTP servers are configured during installation. You can modify them at any time.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Settings > Date & Time**.
3. On the Date & Time page, select **ON** or **OFF** to enable NTP.
4. Enter one or more NTP servers, or modify the existing NTP servers.
5. If you want to verify the connection, click **Test**.
6. Click **Save**.

Configuring Logging Preferences

You can view or pull CloudControl alert messages in the syslog server. Alerts are generated with the ALERT syslog level classification.

CloudControl stores all of your aggregated log files locally, and you can also use Remote Forwarding to send a copy to your syslog server. You can view the logs in CloudControl on the Security > Log Analysis page. See Viewing Log Messages on page 109.

Configuring Local Logging Preferences

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Logging**.
3. Select the Local tab.
4. Set the logging level. This can be one of the following:
   - FATAL—Exports critical messages only.
   - ERROR—Exports error messages as well as critical messages.
   - WARN—Exports warning messages as well as error and critical messages.
   - INFO—Exports informational messages as well as warning, critical, and error messages.
   - DEBUG—Exports all messages for debugging purposes.
5. Click **Save**.

Configuring Remote Forwarding Preferences

If you plan to use encrypted remote forwarding, you must first generate a self-signed Rsyslog client certificate and a CA certificate and import them into CloudControl. For more information, see Certificates on page 111.

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Logging**.
3. Select the Remote Forwarding tab.
4. Select **Enabled**.
5. Select **Encrypt logs** if you want to encrypt your syslog messages.
6. Set the Log Format. This can be one of the following:
   - Proprietary
   - CEF

   By default, this is set to Proprietary. Click the (**change**) link, select your option, and click **Apply** to change.
7. Click the **Add** button to add a syslog server.

8. On the Add Syslog Server window, complete the following:
   a. Enter the IP address or hostname for the external syslog server.
   b. Enter the port to be used for the syslog server.
   c. Select whether the syslog server should be enabled or disabled.
   d. Set the Log Level for the syslog server. This can be one of the following:
      - FATAL—Exports critical messages only.
      - ERROR—Exports error messages as well as critical messages.
      - WARN—Exports warning messages as well as error and critical messages.
      - INFO—Exports informational messages as well as warning, critical, and error messages.
      - DEBUG—Exports all messages for debugging purposes.
9. Click **Add**.

Viewing System Logs

The System Logs page displays all log messages received through CloudControl. Log messages classify and describe all administrative actions and events that have occurred in the virtual infrastructure. By default, CloudControl retains long messages for 180 days.

To view the system logs page, from the **Home** tab, select **System > System Logs**.

Log messages are displayed in a table with the following default columns:

- Time
- Priority
- User
- Action
- Resource Name
- Policy Mode
- Status

You can sort each column in ascending or descending order, drag the columns to change the table order, or click the Columns **button** to choose which columns to display.

Note: The Time, Priority, User, Action, and Resource Name columns cannot be hidden.

You can also use the filter bar at the top to narrow down which system logs you want to see.

Configuring Alert Monitoring

Before you can configure alerts, you must enable SMTP notifications. For more information, see Modifying your Email Settings on page 130.

Configuring Email Notifications

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Monitoring**.
3. Enable Email Notifications.
4. Enter the sender and the email recipients.
5. Click **Save**.

Configuring SNMP

1. From the **Home** tab, select **System > System Settings**.
2. Select **Settings > Monitoring**.
3. Enable SNMP.
4. Enter the FQDN or IP address of the SNMP server.
5. Enter the community string required to access to the SNMP server.
   Note: SNMP Community strings are used only by devices which support the SNMPv2 protocol.
6. Click **Save**.

You can download the SNMP MIB file in the help box on the screen.

Rebooting the CloudControl GUI

Rebooting CloudControl will trigger a failover and your connection to the CloudControl GUI will be lost. Wait a few minutes for the reboot or failover process to complete before you log back in.

1. From the **Home** tab, select **System > System Settings**.
2. On the System Settings page, select **Actions > Reboot CloudControl**.
3. On the Reboot CloudControl page, click **Reboot**.

Chapter 19. Reporting

Viewing Reports

The Manage Reports page displays all existing reports in your system on the Report Definitions and History tabs. To access this page from the Home tab, select **Security > Reports**.

The reports are a high-level overview suitable for a management summary. You can generate the following types of reports:

- Authentication Authorization Report
- AWS Executive Summary Report
- Configuration Hardening Result Report
- Kubernetes Executive Summary Report
- NSX-T Executive Summary Report
- Trust Attestation Status Report
- vSphere Executive Summary Report

Report Definitions tab

Report Definitions are the templates for all reports that you create, which contain information defining the name and description, who the report is emailed to, and when the report is run. You can create, edit, view, delete, and run them on the Report Definitions tab.

If the report definition was run successfully, you can click the link in the Last Run column to access it. For all but the Configuration Hardening Result Report, you can use the icons to preview the report, download it as a PDF file, or download it as a JPEG graphic file. For the Configuration Hardening Result Report, you can only download .csv or .xls files. You can set the Output Format on the Details tab of the Create/Edit Report Definition window.

Note: The schedule column is not sorted in alphabetical order. It is sorted by Manual or Scheduled.

History tab

The history tab displays all reports that have been run. On this page, you can:

- Use the Filter bar to narrow down your results.
- Click the Report Definition link to view the details of the report.
- Select one or more reports and click the Delete button to remove them from the list.
- Click the icons at the end of each row to preview the report, download it as a PDF file, or download it as a JPEG graphic file.

  For the Configuration Hardening Result Report, you can only download .csv or .xls files. You can set the Output Format on the Details tab of the Create/Edit Report Definition window.

Creating a Report

1. From the **Home** tab, select **Security > Reports**.
2. On the Manage Reports page, click the Report Definitions tab.
3. Click the **Create** button.

   If there are no report definitions in your system, you can also click the **Create Report Definition Now** link.
4. In the Create Report window, enter the following information:

Value	Description
Report Type	The type of report. This can be one of the following: • Authentication Authorization Report • AWS Executive Summary Report • Configuration Hardening Result Report • Kubernetes Executive Summary Report • NSX-T Executive Summary Report • Trust Attestation Status Report • vSphere Executive Summary Report
Name	The name of the report.
Description	The optional description of the report.
Email Report To	The email addresses to which you want to send the report. **Important:** You must have SMTP configured before you can email a report. See Modifying your Email Settings on page 130.

5. On the Details tab, do the following:
   - For all reports except for Configuration Hardening Result Report, select the number of days.
   - For the Configuration Hardening Result Report, complete the following:

Value	Description
Exclude passed operations	If selected, any operations that passed when running the configuration hardening policy will not be included in the report.
Exclude failed operations	If selected, any operations that failed when running the configuration hardening policy will not be included in the report.
Exclude skipped operations	If selected, any operations that were skipped when running the configuration hardening policy will not be included in the report.
Resource Platform	The platform type. This can be AWSAccount, vSphere, or Kubernetes.
Output Format	The output format that you would like to use. You can select xlsx or csv format.
Highlight failed operations	If selected, automatically highlights all failed operations in the xlsx file in red.
Compress CSV output	If selected, automatically compresses the CSV file into a zip file.

6. On the Schedule tab, enable or disable the Recurring Schedule.

   If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. The type can be one of the following:
   - **Daily**—The report will run every day at the time that you specify.
   - **Hourly**—The report will run periodically throughout the day, based on the schedule you define.
   - **Weekly**—The report will run on every day that you select at the time that you specify.
7. Click **Create**.

Editing a Report

1. From the **Home** tab, select **Security > Reports**.
2. On the Manage Reports page, click the Report Definitions tab.
3. Click the name of the report definition that you want to update, or select the report definition and click the **Edit** button.

4. In the About tab of the Edit Report Definition window, update the following information:

Value	Description
Name	The name of the report.
Description	The optional description of the report.
Email Report To	The email addresses to which you want to send the report. **Important:** You must have SMTP configured before you can email a report. See Modifying your Email Settings on page 130.

5. On the Details tab, do the following:
   - For all reports except for Configuration Hardening Result Report, select the number of days.
   - For the Configuration Hardening Result Report, complete the following:

Value	Description
Exclude passed operations	If selected, any operations that passed when running the configuration hardening policy will not be included in the report.
Exclude failed operations	If selected, any operations that failed when running the configuration hardening policy will not be included in the report.
Exclude skipped operations	If selected, any operations that were skipped when running the configuration hardening policy will not be included in the report.
Resource Platform	The platform type. This can be AWSAccount, vSphere, or Kubernetes.
Output Format	The output format that you would like to use. You can select xlsx or csv format.
Highlight failed operations	If selected, automatically highlights all failed operations in the xlsx file in red.
Compress CSV output	If selected, automatically compresses the CSV file into a zip file.

6. On the Schedule tab, enable or disable the Recurring Schedule.

   If enabled, select the type of schedule that you want to use to run the policy, and then specify the start date. The type can be one of the following:
   - **Daily**—The report will run every day at the time that you specify.
   - **Hourly**—The report will run periodically throughout the day, based on the schedule you define.
   - **Weekly**—The report will run on every day that you select at the time that you specify.

7. Click **Apply**.

Deleting Reports and Report Definitions

Deleting a Report Definition

1. From the **Home** tab, select **Security > Reports**.
2. On the Manage Reports page, select the Report Definitions tab.
3. Select the report definition that you want to delete and click **Delete**.
4. In the confirmation window, click **Delete**.

Deleting a Report

1. From the **Home** tab, select **Security > Reports**.
2. On the Manage Reports page, select the History tab.
3. Select the report that you want to delete and click **Delete**.
4. In the confirmation window, click **Delete**.

Appendix A. CloudControl System Console

Accessing the CloudControl System Console

The CloudControl System Console is a TUI (Text-based User Interface), and is accessed by logging in as htadmin. Depending on your appliance type, do one of the following:

Access the CloudControl System Console from a Virtual Appliance for OVA

You can access the CloudControl System Console using one of the following:

- the vCenter Server Console where you installed CloudControl
- an SSH session using the htadmin account

  Note: In CloudControl 6.1 and above, SSH is disabled by default. However, if you are upgrading from 6.0.x, SSH is enabled by default. To modify the settings, see Manage htadmin and SSH Access on page 146.

Access the CloudControl System Console from an AWS Cloud Appliance

To access the CloudControl System Console from an AWS Cloud Appliance, you can use an SSH client in Mac or Linux:

1. Open your command line shell and change the directory to the location of the private key file that you created when you launched the instance.
2. Use the chmod command to make sure your private key file is not publicly viewable. For example, if the name of your private key file is my-key-pair.pem, use the following command:

   ```
   chmod 400 my-key-pair.pem
   ```
3. Use the following SSH command to connect as htadmin to the instance:

   ```
   ssh -i /path/my-key-pair.pem htadmin@public_ip_address
   ```

   Note: The public IP address for the instance is visible on the Amazon EC2 console.

Using the CloudControl System Console

1. Log in to the CloudControl System Console as htadmin.
2. In the CloudControl System Console, enter your selection at the prompt. This can be one of the following:

Option	Prompt	Description
1	Manage Network Settings	Allows you to update your network settings. See Manage your Network Settings below. **Note:** You cannot change networking settings for a cluster member.
2	Manage htadmin and SSH Access	Allows you to modify your htadmin pasword and SSH access. See Manage htadmin and SSH Access on page 146.
3	Manage Support Accounts	Allows you to enable a support user that HyTrust Support can use to reach your system. See Manage Support Accounts on page 147.
4	Reboot or Shut Down CloudControl Node	Allows you to reboot or shut down your CloudControl instance. Choose whether to shut down or reboot CloudControl, and then select Yes.
5	Manage Timeouts and Appearance	Allows you to set your TUI, GUI, and SSH session idle timeouts.
6	Switch to Local Mode Authentication	Allows you to disable your Active Directory settings and return to local authentication mode. See Switch from AD to Local Authentication Mode on page 148.
7	Manage AD Settings	Allows you to view or modify your Active Directory service account name and password. See Viewing or Modifying Active Directory Settings on page 149.
8	Command prompt	Allows you to access the CloudControl CLI. See Using the CLI Command Prompt on page 149.
9	Quit TUI Session	Exits the console. See Exiting the Console on page 150.

Manage your Network Settings

You can modify your network settings for standalone nodes and the primary nodes of a cluster.

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Network Settings`** and press Enter.

3. Select one of the following options:

Option	Prompt	Description
1	Show Current Network Configuration	Select to view the current network configuration on your CloudControl instance.
2	Manage IP Address Settings	Select to change your current management interface. On the Interfaces page, select the network interface to configure and select OK. On the modify IP address settings, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. Click OK to return to the Manage Network Settings page.
3	Disable a Network Interface	Select to disable a network interface.
4	Manage DNS Settings	Select to change your DNS settings. On the Modify DNS settings page, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. You are automatically returned to the Manage Network Settings page.
5	Manage NTP Settings	Select to change your NTP settings. On the Modify NTP network settings page, select Yes, and then update the settings that you want to change. Click OK, then Yes on the confirmation screen. You are automatically returned to the Manage Network Settings page.
6	Manage Static Routes	Select to manage your static routes. See Manage your Static Routes on the next page.
7	Network Diagnostic Tools	Select to test your network connectivity. See Test your Network Connectivity on the next page.

4. When you are finished, select **`Return to Previous Menu`**.

Manage your Static Routes

You can view, add, or delete static routes.

Listing your Current Static Routes

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Network Settings`** and press Enter.
3. On the Manage Network Settings page, select **`Manage Static Routes`** and press Enter.
4. On the Manage Static Routes page, select **`List Current Static Routes`** and select OK.
5. The current static routes are displayed. Select OK to return.

Adding a Static Route

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Network Settings`** and press Enter.
3. On the Manage Network Settings page, select **`Manage Static Routes`** and press Enter.
4. On the Manage Static Routes page, select **`Add Static Route`** and select OK.
5. On the Add a static route page, enter the network address and gateway of the static route to add.
6. Select OK to save and return.

Deleting a Static Route

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Network Settings`** and press Enter.
3. On the Manage Network Settings page, select **`Manage Static Routes`** and press Enter.
4. On the Manage Static Routes page, select **`Delete Static Route`** and select OK.
5. On the Delete a static route page, enter the network address and gateway of the static route to delete.
6. Select OK to save and return.

Test your Network Connectivity

CloudControl attempts to connect to different devices in your network and displays the connection information.

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Network Settings`** and press Enter.
3. On the Manage Network Settings page, select **`Network Diagnostic Tools`** and press Enter.

4. On the Network Diagnostics page, select one of the following and follow the prompts:
   - **Verify DNS Server Response**
   - **Verify NTP Server Response**
   - **Test Remote Server is Reachable**
   - **Test Inbound Ports of Another Server**
5. Select **Return to previous menu** when you are finished.

Manage htadmin and SSH Access

1. Log in to the CloudControl System Console as htadmin.
2. Select **Manage htadmin and SSH Access**.

3. Select one of the following:

Option	Prompt	Description
1	Change htadmin Account Password	Select to change your htadmin password. a. Enter the current password at the prompt. b. Enter your new password. The password must be at least 8 characters long and must include at least one lowercase letter, one uppercase letter, one digit and one of the following special characters: ~, !, @, #, $, %, ^, &, *, (,), -, +. c. Reenter your new password. If the password was changed successfully, the console will display: Password successfully updated. If not, you will receive a message stating why the change was denied.
2	Manage SSH Access to System Menu	Select to allow SSH login access to the htadmin account. You can enable or disable access.
3	Manage SSH Session Idle Timeout	Select to modify the SSH session idle timeout value. The default is 15 minutes. Select 0 to disable timeouts.

4. When you are finished, select `Return to Previous Menu`.

Manage Support Accounts

The htsupport user allows HyTrust support to access your system. You can enable and disable the support user.

Enabling the Support User

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Support Accounts`**.
3. Select **`htsupport (full support access)`**.
4. Select Yes to enable the htsupport account.
5. Enter and confirm a password for the HyTrust support user.

   The password must be at least 8 characters long and must include at least one lowercase letter, one uppercase letter, one digit, and one symbol.

   Note: The password is only valid for 24 hours. The account is automatically disabled after 24 hours, or you can disable it when no longer needed.
6. Exit the console, and then log back in as htsupport with the password that you created. You can also use an ssh client.

HyTrust Support can now assist you further.

Disabling the Support User

The htsupport user password will automatically expire in 24 hours. You can disable the support user at any time before that.

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage Support Accounts`**.
3. Select **`htsupport (full support access)`**.
4. Select Yes to disable the htsupport account.

Switch from AD to Local Authentication Mode

You can run this command if you have enabled Active Directory authentication and need to switch back to the local authentication mode.

Important: If you enable local authentication, you will lose any group mappings that you have set up for AD. If you switch back to AD in the future, you will need to recreate your group mappings.

You might need to switch if there are configuration issues with your AD configuration in the CloudControl GUI. You can switch to local Authentication mode, fix the issues, and then re-enable AD using the GUI.

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Switch to Local Mode Authentication`**.
3. Select Yes if you want to switch to local authentication mode, or No to continue with AD.

4. Log back in to the CloudControl GUI. After switching to local authentication mode, the superadmin account to use should be superadminuser. The password should either be the default password you used when you set up the CloudControl GUI, or the updated password if you changed it. For more information, see Setting Up the CloudControl GUI in the Installation Guide for HyTrust CloudControl.

Viewing or Modifying Active Directory Settings

If your service account password has been changed or locked, you can use this command to change the password or use a different account.

Note: To modify any other AD settings, please use the CloudControl GUI.

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Manage AD Settings`**.
   The current AD settings are displayed.
3. At the Modify AD Service Account prompt, enter Yes to modify your settings or No to return to the main TUI menu.
4. If you selected Yes, then complete the following:
   a. Enter the new service account name or leave it as is and select OK.
   b. Enter the new password for the service account and select OK.

Using the CLI Command Prompt

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Command Prompt`**.
3. At the prompt, enter the CLI command that you want to run.
4. Type **`exit`** to return to the TUI menu.

Editing the SSH Banner File

You can create a custom banner that is displayed at each login before CloudControl prompts you to enter the password. For example:

```
login as: htadmin
Authorized users and uses only.
Activity may be monitored and reported to law enforcement.
htadmin@10.2.2.1's password:
```

After you reboot CloudControl, the updated banner contents remain in the `/etc/ssh_banner` file even after CloudControl is upgraded.

Procedure

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Command Prompt`**.
3. Edit the `/etc/ssh_banner` file using vi or any other editor. For example:
   ```
   vi /etc/ssh_banner
   ```
4. Enter the content of your custom SSH banner. For example:
   ```
   Authorized users and uses only.
   Activity may be monitored and reported to law enforcement.
   [esc]
   ```
5. Save the file. For example:
   ```
   :wq
   ```
6. Type **`exit`** to return to the TUI menu.
7. Select **`Reboot or Shut Down CloudControl Node`**.
8. Select **`Reboot the CloudControl Node`**.
9. At the **`Reboot CloudControl Node now?`** prompt, select Yes.

Exiting the Console

1. Log in to the CloudControl System Console as htadmin.
2. Select **`Quit Console`**.

CloudControl logs out of the console and returns you to the login prompt.

Appendix B. Configuration Assurance

About Configuration Assurance Templates

Beginning with Version 6.0.2, CloudControl has added a Configuration Assurance template. You can use this template to change the settings of certain operational parameters for all protected ESXi hosts. This allows you to configure ESXi hosts so that they conform to site specific requirements.

Important: Do not use the Configuration Assurance template for standard configuration hardening. This template is not appropriate for compliance because the parameter settings can be different than those required by regulatory agencies.

- We highly recommend that you use the Configuration Assurance template during maintenance windows only. Do not use during standard operation.
- You should only use the Configuration Assurance template in a policy where the recurring schedule is Disabled. If the policy is manual only, it will prevent the Configuration Assurance template from running unexpectedly.

Configuration Assurance Parameters

The following parameters can only be edited when using a cloned Configuration Assurance template:

- ASC-vSphere-0012: disable-ssh
  - service-status
  - startup-policy
- ASC-vSphere-0053: config-persistent-logs
  - allow_default_location
  - Syslog.global.logDir
- ASC-vSphere-0083: enable-lockdown-mode
  - enable
  - lockdown-mode

- ASC-vSphere-0094: Disk-Scheduler-With-Reservation
  - Disk.SchedulerWithReservation
- ASC-vSphere-0095: Disk-Use-Device-Reset
  - Disk.UseDeviceReset
- ASC-vSphere-0097: nfs-max-volume
  - NFS.MaxVolumes
- ASC-vSphere-0098: tcp-ip-heap-max-configurator
  - Net.TcpipHeapMax
- ASC-vSphere-0099: suppress-core-dump-warnings
  - UserVars.SuppressCoredumpWarning
- ASC-vSphere-0100: Disk-Use-Lun-Reset
  - Disk.UseLunReset
- ASC-vSphere-0101: tcp-ip-heap-size
  - Net.TcpipHeapSize
- ASC-vSphere-0102: suppress-shell-warnings
  - UserVars.SuppressShellWarning
- ASC-vSphere-0103: vsan-repair-delay
  - VSAN.ClomRepairDelay
- ASC-vSphere-0104: config-firewall-access-sshserver
  - allow_all
  - enable_port
- ASC-vSphere-0105: config-firewall-access-vsphereclient
  - allow_all
  - enable_port
- ASC-vSphere-0106: config-firewall-access-webaccess
  - allow_all
  - enable_port
- ASC-vSphere-0107: config-firewall-access-cim
  - allow_all
  - enable_port
- ASC-vSphere-0108: config-firewall-access-cimsecure
  - allow_all
  - enable_port

- ASC-vSphere-0109: config-firewall-access-cimslp
  - allow_all
  - enable_port
- ASC-vSphere-0110: config-firewall-access-dhcpv6
  - allow_all
  - enable_port
- ASC-vSphere-0111: config-firewall-access-dvssync
  - allow_all
  - enable_port
- ASC-vSphere-0112: config-firewall-access-nfc
  - allow_all
  - enable_port
- ASC-vSphere-0113: config-firewall-access-dhcp
  - allow_all
  - enable_port
- ASC-vSphere-0114: config-firewall-access-dns
  - allow_all
  - enable_port
- ASC-vSphere-0115: config-firewall-access-faulttolerance
  - allow_all
  - enable_port
- ASC-vSphere-0117: config-firewall-access-iofiltervp
  - allow_all
  - enable_port
- ASC-vSphere-0118: config-firewall-access-vmotion
  - allow_all
  - enable_port
- ASC-vSphere-0146: enable-svga-vgaonly
  - svga.vgaonly
- ASC-vSphere-0148: disable-non-essential-3D-features
  - mks.enable3d

- ASC-vSphere-0149: config-firewall-access-snmp
  - allow_all
  - enable_port
- ASC-vSphere-0150: config-firewall-access-syslog
  - allow_all
  - enable_port
- ASC-vSphere-0151: config-firewall-access-vsantransport
  - allow_all
  - enable_port

Configuration Assurance Sample Use Case

The following example shows how to use the Configuration Assurance template to enable SSH on your ESXi hosts.

1. Ensure that you are in a maintenance window, or that you are using a closed system that will not affect your other hosts.
2. Clone the Configuration Assurance template (vSphere - Configuration template).

   See Cloning a Configuration Hardening Template on page 89.
3. Update the operations in the template as necessary. For example, to enable SSH, you would open the disable-ssh operation, change the service-status parameter to true, and then click **Save and Close**.
4. Create a manual assessment policy and add the cloned Configuration Assurance template to that policy. For this example, keep the disable-SSH operation only. For testing purposes, you should only add one ESXi host as a resource.

   Note: If you have not updated the other operations, no changes will be made. However it is easier to keep track if you only include the operations that you plan to change.

   See Creating a Configuration Hardening Policy on page 84.
5. Create a manual remediation policy and add the cloned Configuration Assurance template with the operations that you kept in step 4 to that policy. Use the same ESXi host as a resource.
6. Run the assessment policy and review the results. The assessment should be marked as failed.
7. Run the remediation policy, and review the results. The policy should be marked as compliant, and the selected ESXi host will now have SSH enabled.
8. When you are satisfied with your testing, create a new assessment and remediation policy using the same template and operations, and using all of your ESXi hosts as a resource.
9. Ensure that you are in a maintenance window, and run the assessment and remediation policies.
10. Reset the operations in the template that you changed. In this example, you would open the disable-ssh operation, change the service-status parameter to false, and then click **Save and Close**.

11. Rerun the assessment and remediation policies to disable SSH on all of your ESXi hosts.
12. Exit the maintenance window.

Identifying Configuration Assurance Operations

Because the Configuration Assurance operations share the same name as the standard vSphere configuration hardening operations, they share the same name. If you need to visually identify if a particular operation comes from the Configuration Assurance template or not, do the following:

1. From the Home tab, select **Security > Configuration Hardening**.
2. On the Configuration Hardening Management page, click the Policies tab.
3. Open the policy with the operations that you want to check.

   If the operation is a Configuration Assurance operation, you should see the following:

   - The Version will read HyTrust_1.0
   - The Operation Source will read HyTrust.
   - The Reference link will be missing. Standard vSphere configuration hardening operations have a reference link to the vSphere documentation.

Appendix C. CloudControl Storage Recommendations

In very large vSphere environments, depending on the frequency of assessment and remediation requirements, you may want to adjust your CloudControl storage. Use the following recommendations to increase your storage and improve performance.

Increasing your CloudControl Storage

Depending on your vSphere environment size, we recommend that you use the following storage and memory combinations:

vSphere Environment Size	CloudControl Recommended Storage	CloudControl Recommended Memory
Medium Up to 400 hosts or 4000 VMs	200 GB (default value)	16 GB (default value)
Large Up to 1000 hosts or 10,000 VMs	300 GB	32 GB
Extra Large Up to 2000 hosts or 35,000 VMs	500 GB	32 GB

Note: Of the total allocated storage, 50% is used for CloudControl application storage and 50% is reserved for filesystem snapshots.

Procedure

Note: If you have an HA cluster, you must complete this procedure for both nodes.

1. Ensure that there are no filesystem snapshots in CloudControl. Filesystem snapshots are automatically created during upgrade, and must be deleted before you update your memory or storage.

   Note: Filesystem snapshots were added in CloudControl v 6.3. If you are not on 6.3, skip this step.

Use the following procedure to remove any filesystem snapshots:

a. Log in to the CloudControl System Console as htadmin.

b. Select **`Command Prompt`**.

c. At the prompt, type: **`asc upgrade --delete_snaps`**

d. Type **`exit`** to return to the TUI menu.

2. Power down your CloudControl VM.

   Important: If you have an HA cluster, to avoid failover you must power down the secondary node first, and then power down the primary node.

3. Ensure that you do not have any snapshots on the CloudControl VM. All snapshots must be deleted before you can update your memory or storage.

4. In the vSphere Client or Management vCenter, right-click on your CloudControl VM and select **Edit Settings**.

5. In the Edit Settings window, update the settings in the Memory and Hard Disk 1 rows.

6. Click **OK**.

7. Power on the CloudControl VM.

   Important: If you have an HA cluster, power on the primary node first, and then power on the secondary node.

Manage your Logging Retention Size

By default, CloudControl sets the logging retention to 180 days. If you reduce your logging retention, you can free up extra space in your environment. We recommend the following logging retention periods:

vSphere Environment Size	Retention Period
Medium Up to 400 hosts or 4000 VMs	180 days (default value)
Large Up to 1000 hosts or 10,000 VMs	60 days
Extra Large Up to 2000 hosts or 35,000 VMs	30 days

For more information, see Changing the Log Retention on page 110.

Using CloudControl Purge Jobs

CloudControl has several jobs that are used to manage your configuration hardening data. These jobs run every day and purge some of the configuration hardening data. The high-level information is always retained, as that data is used for the configuration hardening dashboards. Auditors can use the dashboards to ensure their standards are met. However, the data for individual operations and resources can be safely purged.

- PurgeOpResourcesResultsJob—When there are more than 10 million records, all entries over 10 million are purged.
- PurgeHTCCDatabaseJob—Monitors the pgsql partition at /var/lib/pgsql. When this partition reaches 60% utilization, the oldest data will be removed until the disk usage is below 60%.

  Note: 30 days of data is always retained unless you modify ExpiryPurgeValue.

The Config Hardening System-Configuration-Endpoint API can be used to modify the following values:

- ExpiryPurgeValue—The number of days the data is retained. The default is 30 days.
- PgsqlDiskUsageThreshold—The usage percentage for the pgsql partition. The default value is 60% utilization.
- MaxOpResourceResultsRecords—The number of records to be retained. The default is 10 million (10000000) records.

Procedure

1. Locate the System-Configuration-Endpoint API in the Config Hardening section of the online API documentation. (https://<CloudControl_IP>/apidoc)
2. Run the 'Get all System configurations' query and search for ExpiryPurgeValue, PgsqlDiskUsageThreshold, or MaxOpResourceResultsRecords.

   For example:

   ```
   {
   "created": "2020-04-14T15:46:40.142+0000",
   "updated": "2020-04-14T15:46:40.142+0000",
   "name": "ExpiryPurgeValue",
   "uid": "97c14206-0cf4-483e-a68c-883c5eec40b3",
   "value": "30",
   "defaultValue": "30",
   "minValue": "1",
   "maxValue": "90",
   "description": "Threshold days to purge compliance data. Default value is 30 days",
   "categoryType": "Compliant",
   "resourceType": "ASC",
   "updatedBy": "System",
   "enabled": true,
   "internal": true
   },
   ```

3. Use the 'Update a specific system configuration operation' command to update the value in the `"value": "30"` parameter.
4. Repeat for all parameters that you want to update.

For assistance, contact support@hytrust.com.

Appendix D. Using the CloudControl API Documentation

The HyTrust CloudControl API is a RESTful API that provides programmatic access to the various functions of CloudControl. The API documentation is now integrated with the CloudControl GUI. You can access the documentation at: https://<CloudControl_IP>/apidoc.

To view the online API documentation:

1. Select a section from the top pane, for example, System Config.
2. Select the desired category from the left pane, for example, SETTINGS.
3. Review the parameters in the middle pane, and the method, URL, and JSON response in the right pane.

You can use an API client like Insomnia or a development tool like Postman to run your APIs, or write custom Powershell or Python scripts.