## Contents

**Chapter 1. Installation Overview** ................................................................. 5  
  Introduction ........................................................................................................ 5  
  System Requirements .......................................................................................... 6  
  Active Directory Service Account Requirements .............................................. 7  
    Creating the Active Directory Service Account ................................................. 7  
  Supported Browsers ............................................................................................ 7  
  Firewall Requirements ........................................................................................ 8  

**Chapter 2. Installing CloudControl from an OVA** ........................................ 9  
  Overview of the Installation Steps ........................................................................ 9  
  Deploying CloudControl ...................................................................................... 10  
  Power On the Appliance ....................................................................................... 11  
  Configuring the CloudControl Virtual Appliance ............................................... 11  
    Creating a Standalone Node .............................................................................. 11  
    Creating the Primary Node of a Cluster ............................................................ 12  
    Creating a Secondary Node for a Cluster .......................................................... 13  

**Chapter 3. Installing CloudControl from an AMI** ......................................... 15  
  Overview of the Installation Steps ........................................................................ 15  
  AMI Deployment .................................................................................................. 15  
  Creating a Cluster after AMI Deployment ............................................................ 17  

**Chapter 4. Completing the CloudControl Installation Using the GUI** ............ 19  
  Setting Up the CloudControl GUI ...................................................................... 19  
  Configuring Active Directory .............................................................................. 21  

**Chapter 5. Using Clusters in CloudControl** ................................................. 24  
  About CloudControl Clusters ............................................................................ 24  
  Clustering Port Requirements ............................................................................ 24
Chapter 1. Installation Overview

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.
System Requirements

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.

The Installation Guide for HyTrust CloudControl includes information on system requirements and installation instructions for HyTrust CloudControl Version 6.0.2.

You can deploy HyTrust CloudControl as either a Virtual Appliance for OVA, or an AWS Cloud Appliance. Please use the procedures for your specific installation.

Technical Support
For technical support, email support@hytrust.com or visit https://hytrust.com/support.

System Requirements

System Requirements for OVA Deployment
Installing CloudControl as an OVA requires the following per node:
- Enterprise Editions of VMware vSphere, from vSphere 6 update 2 to vSphere 6.7.
- Enough resources to create the CloudControl appliance with:
  - 4 virtual cores (vCPU)
  - 16 GB of memory
  - 90 GB of free datastore space

System Requirements for AMI Deployment
Before installing CloudControl in AWS, please note the following:
- CloudControl uses 16 GB RAM and has 4 CPUs. Please choose an instance type that has the resource capacity for this application.
- The following console accounts use the instance ID of the EC2 instance as the default password:
  - htaadmin
  - htsupport
  - htrescue
  
  **Note:** You will be prompted to change the htaadmin password on first use.
- If you plan to use CloudControl to manage Kubernetes as well as AWS Accounts, you must deploy CloudControl in a VPC that has access to your Kubernetes infrastructure.
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 service account requires the following permissions in AD:

- Domain object: Read memberOf
- User object: attributes memberOf and distinguishedName
- Group object: attributes member, memberOf, and distinguishedName

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.

Supported Browsers

CloudControl requires HTTPS access and has been tested on the following browsers:

- Internet Explorer 11 for Windows 2012 server or greater
- Internet Explorer 11 for Windows 10 or greater
- Firefox 65
- Chrome 71
Firewall Requirements

- HyTrust CloudControl uses Clair, an open source project for the static analysis of vulnerabilities in appc and docker containers. In order for Clair to be able to scan your environment, the following websites must be accessible:
  - Debian: https://security-tracker.debian.org/tracker
  - Ubuntu: https://launchpad.net/ubuntu-cve-tracker
  - Redhat: https://www.redhat.com/security/data/metrics
  - Oracle: https://linux.oracle.com/security/
  - OpenSuse: https://www.suse.com/de-de/support/security/oval/
  - Alpine: http://git.alpinelinux.org/cgit/alpine-secdb/
  - NIST: https://nvd.nist.gov
- For licensing, CloudControl requires that port 443 is open.
# Chapter 2. Installing CloudControl from an OVA

## Overview of the Installation Steps

Installing and configuring CloudControl requires the following tasks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that your environment meets the basic system requirements.</td>
<td>See System Requirements on page 6.</td>
</tr>
<tr>
<td>2</td>
<td>If you plan to use Active Directory, create a service account with the proper permissions.</td>
<td>See Active Directory Service Account Requirements on page 7.</td>
</tr>
<tr>
<td>3</td>
<td>Deploy CloudControl as a VMware vSphere virtual machine, and confirm that the network adapter(s) are properly configured and connected.</td>
<td>See Deploying CloudControl on the next page.</td>
</tr>
<tr>
<td>5</td>
<td>Determine whether you want to use a standalone node or cluster, and then configure the virtual appliance.</td>
<td>See Configuring the CloudControl Virtual Appliance on page 11.</td>
</tr>
<tr>
<td>6</td>
<td>Run the setup wizard in the CloudControl GUI.</td>
<td>See Setting Up the CloudControl GUI on page 19.</td>
</tr>
<tr>
<td>7</td>
<td>If you created a primary node for a one-node cluster, then create a secondary node. For more information, see About CloudControl Clusters on page 24.</td>
<td>See Creating a Secondary Node for a Cluster on page 13.</td>
</tr>
</tbody>
</table>
Deploying CloudControl

The following procedure describes how to deploy the CloudControl virtual appliance to a VMware vSphere cluster.

**Note:** The procedure uses the VMware vSphere client version 6.0.x. If you are using a different version of vSphere, the procedure may be different. If you have any questions, consult your vSphere documentation.

1. Log into the vSphere cluster using the VMware vSphere client or the vSphere Web Client.
2. Navigate to **Inventories > Hosts and Clusters**.
3. In the Navigator Pane, select the resource pool where you plan to deploy CloudControl.
4. Select **File > Deploy OVF Template** from vSphere Client, or **Actions > Deploy OVF Template** from vSphere Web Client.
   **Note:** In this context, OVF and OVA are synonymous.
5. Click **Browse** and select the CloudControl OVA file.
6. On the OVF Template Details wizard page, make sure you have the correct OVA file and click **Next**.
7. On the End User License Agreement page, click **Accept** and then click **Next**.
8. On the Name and Location page, update the name, if necessary, and select the location where you want to deploy CloudControl and click **Next**.
9. On the Storage page, select the destination storage for the virtual machine files, or optionally check the **Disable Storage DRS for this virtual machine** radio button and select a datastore.
10. Click **Next**.
11. On the Disk Format page, choose the format that you want to use, and click **Next**.
12. On the Network Mapping page, choose the networks that you want to use for the NIC, and then click **Next**.
   **Note:** Ensure that the primary NIC is set to the network used to access the CloudControl Management Console.
13. On the Ready to Complete page, review your choices.
14. Click **Finish** to close the installation wizard.
   The vSphere Client starts the deployment process on the vCenter Server resource. You can monitor the progress in the vSphere Client Status panel.
Power On the Appliance

1. Log in to the vSphere Client.
2. Locate the HyTrust CloudControl virtual machine in the inventory.
3. Right-click the CloudControl virtual machine and select Power > Power On.

Configuring the CloudControl Virtual Appliance

The following procedures describe how to configure the CloudControl Virtual Appliance after it has been deployed by vSphere. This requires access to the CloudControl Virtual Appliance Console on the CloudControl VM. After you have finished configuring the virtual appliance, you can use the HyTrust CloudControl graphical user interface (GUI) to complete the configuration process.

Depending on whether you intend to create a standalone node or a cluster, use the appropriate procedure:

- Creating a Standalone Node
- Creating the Primary Node of a Cluster

**Note:** If you create a standalone node, and decide later to create a cluster, you can use the CLI commands to create a cluster. See Using Clusters in CloudControl on page 24.

Creating a Standalone Node

**Important:** If you want to create a cluster, please use the procedure in Creating the Primary Node of a Cluster on the next page.

1. From the vSphere VMware client, right-click the VM on which CloudControl is deployed and select Open Console. Alternatively, select the VM from the list of VMs and click Launch Virtual Machine Console in the vCenter Client toolbar.
2. At the Do you want this node to be part of a HA cluster (Y/n) prompt, type n and press Enter.
3. At the Enter desired Node IP prompt, enter the valid unused IP address that you want to use for the CloudControl IP address and press Enter.
4. At the Enter desired Hostname prompt, enter the hostname to use for CloudControl and press Enter. The hostname can be a maximum of 15 alphanumeric characters and contain one dash [-].
   **Note:** If you register your hostname.domainname in DNS, you can use that fully qualified domain name to access CloudControl in addition to the IP address.
5. At the Enter Netmask prompt, enter the netmask that is appropriate for your subnet and press Enter.
6. At the Enter Default Gateway prompt, enter the IP address of your network gateway server and press Enter.
7. At the Enter DNS Server IP Address prompt, enter the IP address of a DNS server at your site and press Enter.
8. At the Enter DNS Domain name prompt, enter the domain name for the hostname that you entered and press Enter.
9. Review your choices and press Enter to accept the default value of Y, or type n and press Enter to modify your choices.

When the configuration has finished, CloudControl displays a confirmation message stating that the configuration has completed successfully.

**What to Do Next**

The final step of the configuration process is done through the CloudControl GUI. See *Completing the CloudControl Installation Using the GUI* on page 19.

**Creating the Primary Node of a Cluster**

**Important**: If you want to create a standalone node, please use the procedure in *Creating a Standalone Node* on the previous page.

1. From the vSphere VMware client, right-click the VM on which CloudControl is deployed and select Open Console. Alternatively, select the VM from the list of VMs and click Launch Virtual Machine Console in the vCenter Client toolbar.

2. At the Do you want this node to be part of a HA cluster (Y/n) prompt, type Y and press Enter.

3. At the Do you want this node to be the primary node or a secondary (PRI/sec) prompt, type PRI and press Enter.

4. At the Enter desired Virtual Management IP prompt, enter the virtual management IP (VIP) address and press Enter.

   The VIP is an additional IP address that is always associated with the primary node of your cluster. Because it is automatically moved to the active (primary) node, the VIP is the IP address that you should use to access CloudControl. The IP that you specify should be a valid unused IP address in your subnet.

5. At the Enter desired Server Name (name that maps to VIP) prompt, enter the server name to associate with the VIP and press Enter.

   The server name is a virtual name that is mapped to the virtual IP address in the /etc/hosts file. You can use the server name and domain name to access the primary CloudControl in addition to the VIP.

   The hostname can be a maximum of 15 alphanumeric characters and contain one dash [-].

6. At the Enter desired Node IP prompt, enter the valid unused IP address that you want to use for the CloudControl IP address and press Enter. The node IP address remains with the specified node, and is used to communicate with other nodes in the cluster. External requests to the node IP address from a browser will be redirected to the VIP.

7. At the Enter desired Hostname prompt, enter the hostname to use for CloudControl and press Enter.

   The hostname can be a maximum of 15 alphanumeric characters and contain one dash [-].

8. At the Enter Netmask prompt, enter the netmask that is appropriate for your subnet and press Enter.

9. At the Enter Default Gateway prompt, enter the IP address of your network gateway server and press Enter.

10. At the Enter DNS Server IP Address prompt, enter the IP address of a DNS server at your site and press Enter.

11. At the Enter DNS Domain name prompt, enter the domain name for the hostname that you entered and press Enter.
12. Review your choices and press **Enter** to accept the default value of Y, or type **n** and press **Enter** to modify your choices.

When the configuration has finished, CloudControl displays a confirmation message stating that the configuration has completed successfully.

**What to Do Next**

The final step of the configuration process is done through the CloudControl GUI. See *Completing the CloudControl Installation Using the GUI* on page 19.

You can add a secondary node to create your cluster now, or after the configuration is complete.

---

## Creating a Secondary Node for a Cluster

The secondary node should be created on a fresh deployment of CloudControl. Follow the installation steps to deploy the OVA. See *Overview of the Installation Steps* on page 9.

For more information on clustering in CloudControl, see About CloudControl Clusters on page 24.

**Before You Begin**

You must have configured the primary node of your CloudControl cluster. See *Creating the Primary Node of a Cluster* on the previous page.

If you have not yet changed the htadmin password on the primary node, either through the console or through the GUI, you should do so before you set up the secondary node. The secondary node setup prompts for the updated htadmin password.

**Procedure**

1. From the vSphere VMware client, right-click the VM on which CloudControl is deployed and select **Open Console**. Alternatively, select the VM from the list of VMs and click **Launch Virtual Machine Console** in the vCenter Client toolbar.

2. At the Do you want this node to be part of a HA cluster (Y/n) prompt, type **Y** and press **Enter**.

3. At the Do you want this node to be the primary node or a secondary (PRI/sec) prompt, type **sec** and press **Enter**.

4. At the Enter existing Virtual Management IP of the cluster prompt, type the VIP you entered for the primary node and press **Enter**.

5. At the Enter desired Node IP prompt, enter the valid unused IP address that you want to use for the secondary node and press **Enter**.

6. At the Enter Secondary Hostname prompt, enter the hostname to use for the secondary node and press **Enter**.

   The hostname can be a maximum of 15 alphanumeric characters and contain one dash [-].

7. At the Enter primary’s htadmin password prompt, enter the password and press **Enter**.

   CloudControl imports the values from the primary node and displays the settings for netmask, gateway, DNS server IP address, and DNS domain name.
8. At the Do you want to use these settings on secondary (Y/n) prompt, review your choices and press Enter to accept the default value of Y, or type n and press Enter to modify your choices.

When the configuration has finished, CloudControl displays a confirmation message stating that the configuration has completed successfully.

If you have not already configured the CloudControl GUI, see Completing the CloudControl Installation Using the GUI on page 19. The CloudControl GUI only needs to be configured for the primary node.
Chapter 3. Installing CloudControl from an AMI

Overview of the Installation Steps

Installing and configuring CloudControl requires the following tasks:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that your environment meets the basic system requirements.</td>
<td>See System Requirements on page 6.</td>
</tr>
<tr>
<td>2</td>
<td>If you plan to use Active Directory, create a service account with the proper permissions.</td>
<td>See Active Directory Service Account Requirements on page 7.</td>
</tr>
<tr>
<td>3</td>
<td>Deploy CloudControl as an AMI.</td>
<td>See AMI Deployment below.</td>
</tr>
<tr>
<td>4</td>
<td>Run the setup wizard in the CloudControl GUI.</td>
<td>See Setting Up the CloudControl GUI on page 19.</td>
</tr>
<tr>
<td>5</td>
<td>If you created a cluster node, then configure High Availability. For more information, see About CloudControl Clusters on page 24.</td>
<td>See Creating a Cluster after AMI Deployment on page 17.</td>
</tr>
</tbody>
</table>

AMI Deployment

In order to deploy CloudControl on AWS, you need to launch a CloudControl instance on a new or existing VPC.

**Note:** The following procedure is based on the January 2019 AWS Console interface. If your version of the AWS Console is different from what is described below, please see your AWS documentation.

1. Open a web browser and navigate to the Amazon Web Services login page for your company. The default login page is [https://aws.amazon.com/](https://aws.amazon.com/).
2. Log in to the AWS Management Console with your AWS user name and password.
3. In the top menu bar just after your login name, verify that the deployment region is correct. If you need to change it, click the current region and select the new region from the drop-down list.

4. In the top menu bar, select **Services > Compute > EC2**.

5. Click the blue **Launch Instance** button.

6. In the Step 1: Choose an Amazon Machine Image (AMI) page, click **AWS Marketplace** in the left-hand pane.

7. Search the Marketplace for "HyTrust" and select **HyTrust CloudControl for AWS BYOL** (Bring Your Own License). You must obtain a trial license from HyTrust which you will upload when you set up the GUI. See **Setting Up the CloudControl GUI** on page 19.

8. Review the details of the version you selected and click **Continue**.

9. In the Step 2: Choose an Instance Type page, select an instance type. For optimal performance, we recommend that you select a general purpose or compute optimized instance type with SSD Instance storage, such as **t3.xlarge** or **m5.xlarge**. The CloudControl system resource recommendations are 16 GB RAM and 4 CPUs.

10. After you have selected the type, click **Next: Configure Instance Details**.

11. On the Step 3: Configure Instance Details page, set the following options:

   - Number of Instances—Specify the number of instances you want to launch in this field. All instances will run in the same region using the same VPC and instance settings.
     
   - **Tip:** You can use this option to create additional instances to use in a multi-node CloudControl cluster on this VPC without needing to launch additional instances, but you can also add additional CloudControl nodes to the cluster at any time after the initial node has been configured.

   - Network—Select the VPC you want to use for the CloudControl node, or click **Create new VPC** to create a new one.

   - Auto-assign Public IP—Depending on your network architecture, specify how you intend to access the CloudControl GUI. You can either enable public IP or set up a transit VPC between your company’s outgoing gateway and the Amazon VPC.

   - Set all other options on this page according to your corporate standards.

12. When you are done, click **Next: Add Storage**.

13. On the Step 4: Add Storage page, set the following options:

   - Volume Size—Set the size of the disk based on your configuration requirements. The default setting of 70 GB should work for most CloudControl installations.

   - Volume Type—For optimal performance, we recommend setting the volume type to one of the SSD options instead of the default Magnetic volume.

14. When you are done, click **Next: Add Tags**.

15. On the Step 5: Add Tags page, click **Add Tag** and enter a Name tag for the instance:

   - Key—Enter "Name".
   - Value—Enter the name for this CloudControl node.

   Add any other tags as desired.

16. When you are done, click **Next: Configure Security Group**.
17. In the Step 6: Configure Security Group page, do the following:
   a. Ensure that the security group that you pick grants access to the objects managed by CloudControl, including Kubernetes nodes, registries, Active Directory, NTP, DNS, SMTP, and SYSLOG.
   b. Make sure that the **Assign a security group** field is set to **Create a new security group**.
      
      **Note:** You can use an existing security group as long as all of the required ports are open in that security group.
   c. Optionally enter a custom security group name and description in the **Security group name** and **Description** fields.
   d. For each of the required entries in the security group, set the Source IP addresses or security groups that can communicate with CloudControl through the associated ports. We strongly recommend that you do **not** use the default 0.0.0.0/0 notation, which indicates that the ports are open to the world.

CloudControl requires the following ports:
- SSH
- HTTPS

For details about specifying the source IP addresses or security groups, see your AWS documentation.

18. When you are done, click **Review and Launch**.

19. In the Step 7: Review Instance Launch page, verify your selections and click **Launch**.

20. At the prompt, either select an existing key pair or select **Create a new key pair**, specify a key pair name, and download the new private key file for the new key pair.

21. When you are done, click **Launch Instances**. AWS displays a confirmation page stating that your instance is being launched and displays the instance ID.

22. To verify the status of the instance, select **Services > EC2 > Instances** and locate the new instance in the table.

What to Do Next

Wait for 5-10 minutes and then launch https://<CloudControl-IP-Address> in a supported browser to complete the setup process.

The IP address and DNS name can be found on the Description tab for the EC2 instance.

Creating a Cluster after AMI Deployment

When using CloudControl as an AWS Cloud Appliance, you need to create multiple instances during CloudControl AMI deployment and join them together in a cluster. If you plan to allow external access to the cluster, then you can create an AWS Elastic Load Balancer (ELB) to manage it (for more information on ELB, see your AWS documentation). You will need to manually change the VIP to the new primary node after failover.

**Note:** For CloudControl 6.0, you can only create an AWS Cloud Appliance cluster if the nodes are on the same subnet.
1. Deploy two or three CloudControl instances in the same subnet, or availability zone.
   Important: Before you can create a cluster, you must have successfully deployed CloudControl as an AMI and set up the CloudControl GUI on all nodes that will be part of the cluster.

2. Assign a second private IP address to one of the nodes. This will be the VIP.

3. Access the CloudControl TUI from the selected node. See Accessing the TUI on page 34.

4. Log in to CloudControl console as httadmin.


6. Run the following command to create the cluster on the specified node. This node will become the primary.
   ```
   asc ha --form <virtual-IP-address> --virtname <virtual-node-name> --mode primary
   ``
   Where <virtual-IP-address> is the VIP that you assigned above and <virtual-node-name> is the hostname associated with the VIP.

7. On the other nodes that you want to join the cluster, navigate to the CloudControl console and run the following command:
   ```
   asc ha --join <virtual-IP-address> --password <primary-password> --mode secondary
   ``
   Where <virtual-IP-address> is the VIP of the primary node and <primary-password> is the httadmin password for the primary node.

8. If you plan to allow public access, do the following:
   a. Create an Elastic Load Balancer (ELB) and add all node instances as targets. The ELB needs to meet the following criteria:
      - The ELB must be internet-facing.
      - The monitoring group must use HTTPS to port 443 as the health check, and accept 200, 301, and 302 as valid responses.
      - You must have a certificate to use with the ELB public IP address. This can be a new certificate, or you can upload an existing certificate.
   b. Use the DNS name of the ELB to access the cluster from the internet.
      Upon failover, the ELB will automatically redirect traffic to the new primary node.

9. For VIPs, you must manually reassign the VIP to the new primary EC2 instance after failover.
   AWS will not route traffic to the VIP to the new primary node unless you manually associate the VIP to that specific EC2 instance.
Chapter 4. Completing the CloudControl Installation Using the GUI

Setting Up the CloudControl GUI

After deploying CloudControl as either a Virtual Appliance for OVA or a AWS Cloud Appliance, you must run the Setup wizard in the CloudControl GUI.

Note: If you are using a cluster, you only need to set up the CloudControl GUI one time for the primary node.

Before You Begin

See Supported Browsers on page 7 to ensure that you have a supported web browser.

Procedure

1. Open a web browser and navigate to the IP address or hostname that you assigned during the CloudControl Virtual Appliance configuration (for Virtual Appliance for OVA), or that was assigned for you on the Description tab for the EC2 instance (for AWS Cloud Appliance).

   Note: CloudControl uses a self-signed certificate. Depending on your browser, you may receive a message about a problem with the certificate or the connection being untrusted or not private. Simply click past the message.

2. Log into CloudControl using the following credentials:
   - Username: superadminuser
   - Password: Pa$$w0rd123!

   The first time you log into the CloudControl management interface, CloudControl automatically displays a splash screen that lets you start the Setup wizard.

3. In the Welcome to CloudControl splash screen, click Setup Now.


   Note: You must scroll through the EULA before you can accept it.

5. If you have not already changed the CLI console password, you will be prompted to change it now. Enter and confirm the password, and then click Change Now.
6. In the Register page, check the Allow Vitals communication checkbox if you want the Vitals Service to gather information from your system and monitor the health of the system. For more information, see Using the HyTrust Vitals Service in the Administration Guide for HyTrust CloudControl.

7. Under CloudControl Licensing, 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.

   **Note:** You can only add one license during the initial setup. For more information, see Licensing in the Administration Guide for HyTrust CloudControl.

8. Click **Continue**.

9. In the DNS configuration page, specify the following properties:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS IP Address</td>
<td>The IP address of the DNS server. You must have at least one DNS server, and up to three DNS server addresses are supported.</td>
</tr>
<tr>
<td>Domain Name</td>
<td>The domain name for CloudControl.</td>
</tr>
</tbody>
</table>

   **Note:** These field are pre-populated with the values used for the initial setup of the virtual appliance.

10. If you want to verify the connection, click **Test**.

11. Click **Continue**.

12. In the Date & Time configuration window, select **ON** if you want to configure NTP, and enter one or more NTP servers.

13. If you want to verify the connection, click **Test**.

14. Click **Continue**.

15. In the Email configuration page, select **ON** if you want to enable SMTP, and specify the following properties:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP Server Name or IP Address</td>
<td>The name of the SMTP server used by email or its IP address.</td>
</tr>
<tr>
<td></td>
<td>The name or IP address can be from 2-255 characters and cannot include spaces or the following special characters:</td>
</tr>
<tr>
<td></td>
<td>, ~ : ! @ # $ % ^ &amp; ’ ( ) [ ] { }</td>
</tr>
<tr>
<td>Port</td>
<td>The TCP Port that the SMTP server uses for communication. The default is port 25.</td>
</tr>
<tr>
<td>Sender</td>
<td>The email address from which the system sends email.</td>
</tr>
<tr>
<td></td>
<td>The email address can be from 1-255 characters, and cannot include spaces.</td>
</tr>
</tbody>
</table>

16. If you want to verify the connection, click **Test**.

At this point you can either finish the setup and continue with Local Authentication, or configure Active Directory to fully use HyTrust CloudControl.
To continue with Local Authentication:

1. Click **Continue with Local Authentication**.
   
   Local Authentication creates three pre-defined groups and one local user to use CloudControl without AD.

2. To change your password, enter and confirm a new password, and then click **Continue**. Otherwise you can click **Skip** to close the setup confirmation window and start using CloudControl.
   
   **Note**: If you change the password, you will need to log into CloudControl again.

To configure Active Directory:

1. Click **Configure Active Directory Now**.

2. Perform the tasks in **Configuring Active Directory** below.
   
   The setup process automatically finishes when you finish adding Active Directory.

For more information, see Managing Users and Groups in the Administration Guide for HyTrust CloudControl.

---

## Configuring Active Directory

If you choose to configure Active Directory rather than using Local Authentication, you must complete the following:

1. On the Default Domain page of the Configure Active Directory wizard, enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Domain Name</td>
<td>Enter the root domain name to use with Active Directory.</td>
</tr>
<tr>
<td>Account</td>
<td>Enter the name of the service account that you created.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the service account.</td>
</tr>
</tbody>
</table>

2. Click **Continue**.
3. On the Domain Controllers page, 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the domain controller name.</td>
</tr>
<tr>
<td>Security</td>
<td>Select whether you want to use no security or SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for the domain controller or global catalog.</td>
</tr>
<tr>
<td>User Search Context (Base DN)</td>
<td>Enter any additional search methods for users.</td>
</tr>
<tr>
<td>Group Search Context (Base DN)</td>
<td>Enter any additional search methods for groups.</td>
</tr>
</tbody>
</table>

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

4. Click **Add**.

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

6. 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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the global catalog name.</td>
</tr>
<tr>
<td>Security</td>
<td>Select whether you want to use no security or SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the port for the global catalog.</td>
</tr>
<tr>
<td>User Search Context (Base DN)</td>
<td>Enter any additional search methods for users.</td>
</tr>
<tr>
<td>Group Search Context (Base DN)</td>
<td>Enter any additional search methods for groups.</td>
</tr>
</tbody>
</table>

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

7. Click **Add**.

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

9. 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.
     - a. On the Additional Domains page, click **Add a Domain Now** or the **Create** button and enter the domain information.
     - b. Click **Continue**.
   - Click **Skip**.
10. On the Role-Group Mapping page, enter the group name for each role name. The group name is the Active Directory security group name. Enter the AD group name that you want to associate with the default role. The name used in this field must be identical to the group name found in AD.

If you have only one domain, the default domain is listed by default. If you have more than one, select the domain in the drop-down list.

**Important:** You must map at least one Active Directory security group for a successful AD conversion. We recommend mapping SuperAdmin to the ASC_SuperAdmin role.

11. Click **Continue**.

12. On the Summary page, review your changes, then click **Apply**.

13. On the confirmation page click **Apply AD settings and Log Out**.

14. Click **OK** to confirm.

Both the setup process and the Active Directory configuration process completes.

15. After CloudControl restarts, use your AD credentials to log back in.
Chapter 5. Using Clusters in CloudControl

About CloudControl Clusters ................................................................. 24
Clustering Port Requirements ............................................................... 24
Failure Recovery .................................................................................. 25
Creating a Primary Node from a Standalone ........................................... 25
Converting a Standalone to a Secondary Node ....................................... 25
Viewing the Status of a Cluster .............................................................. 26
Initiating a Manual Failover ................................................................... 27
Cluster-related CLI Commands ............................................................... 27

About CloudControl Clusters

Clustering allows you to create a set of CloudControl appliances to run a single instance of the CloudControl. You can use clustering to implement high availability. CloudControl clusters are active/passive. The CloudControl product runs on the primary node, while the other node is a secondary.

The secondary node is kept in sync with the primary node automatically in real time. If the primary node fails, CloudControl automatically switches to run on the secondary node.

- For a Virtual Appliance for OVA, both the primary cluster node and the secondary node are created during OVA deployment. See Creating the Primary Node of a Cluster on page 12 and Creating a Secondary Node for a Cluster on page 13. After CloudControl is installed, you can change the status of the nodes using the CLI.
- For an AWS Cloud Appliance, CloudControl clusters are created after setup using the CLI.

Clustering Port Requirements

The following ports must be open in your firewall (bidirectionally) to enable high availability clustering:

- TCP 2224
- TCP 3121
- TCP 5404
- UDP 5404
- UDP 5405
- TCP 21064
Failure Recovery

If your primary node goes down or otherwise becomes incapable of running CloudControl services, a failover will occur. A secondary node will be promoted to become the new primary. The new primary node will take over the CloudControl virtual IP address and virtual node name, and CloudControl services will be started on the new primary node.

Because the CloudControl database and files are kept in sync, the new primary will have up-to-date CloudControl configuration. You will need to re-login to the CloudControl GUI because the services are running on a new primary, but otherwise you can continue to use CloudControl seamlessly after failover.

Depending on your environment, the state of your cluster after failover will be:

- If the former primary node is still offline, it remains in the cluster as an offline secondary node. If you want to use this node for HA, you must power it on. Once powered on, the former primary node becomes a new secondary node that can be used in case of failover.

- If the former primary is not working and the node remains offline, then you have N-1 online nodes in your cluster. For example, if before the failure you had a 2-node cluster, and the primary failed and is not running, then the new primary is head of a 1-node cluster. If you cannot bring the failed node back online, you may want to add a new secondary to bring the number of nodes back up to 2. To add a new secondary node, see Creating a Secondary Node for a Cluster on page 13 or Converting a Standalone to a Secondary Node below.

Creating a Primary Node from a Standalone

1. Access the CloudControl TUI from your standalone node. See Accessing the TUI on page 34.
2. Log in to CloudControl console as htadmin.
4. Run the following command:

   ```
   asc ha --form <virtual-IP-address> --virtname <virtual-node-name> --mode primary
   ```

   Where <virtual-IP-address> is the virtual management IP that you want to assign to and <virtual-node-name> is the hostname associated with the VIP.

Creating Primary Node Example

```
[nodel:standalone ~]$ asc ha --form 192.0.2.134 --virtname VirtualNode --mode primary
Forming cluster at VIP 192.0.2.134 as primary node...
Stopping services (will be restarted by Pacemaker)...
Form cluster operation succeeded.
[nodel:primary ~]$ 
```

Converting a Standalone to a Secondary Node

If you have an existing CloudControl cluster with a primary node, and you have an existing CloudControl standalone deployment, you can convert the standalone CloudControl to a secondary node in your cluster.
1. Access the CloudControl TUI from the standalone node that will become the secondary node of the cluster. See Accessing the TUI on page 34.

2. Log in to CloudControl console as htdadmin.


4. Run the following command:
   \[ asc ha --join <virtual-IP-address> --password <primary-password> --mode secondary \]
   Where \(<virtual-IP-address>\) is the VIP of the primary node and \(<primary-password>\) is the htdadmin password for the primary node.

Creating Secondary Node Example

\[ [node1:standalone ~]$ asc ha --join 192.0.2.134 --password PrimaryS3crEt! --mode secondary \]
Joining cluster at VIP 192.0.2.134 as secondary node...
Stopping services on this node...
Join cluster operation succeeded.

\[ [node1:secondary ~]$ \]

Viewing the Status of a Cluster

1. On your primary node, log in to CloudControl from the Virtual Machine Console Window or via SSH using your htdadmin credentials.

   \[ \textbf{Note:} \text{The current cluster role is displayed whenever you start the CLI. For example:} \]
   \[ [node1:primary ~]\]

3. Run the following command: \( asc \ ha --status \)

Cluster Status Example:

The following example is a HA cluster with three nodes. The command is run from the primary node, and one of the secondary nodes currently offline.

\[ [node1:primary ~]$ asc ha --status \]
Cluster name: htcc_cluster
Stack: corosync
Current DC: node1 (version 1.1.19-8.el7_6.2-c3c624ea3d) - partition with quorum
Last updated: Thu Jan 24 18:18:53 2019
Last change: Thu Jan 24 18:05:56 2019 by root via cibadmin on node1

3 nodes configured
17 resources configured
Online: [ node1 node2 ]
OFFLINE: [ node3 ]

Full list of resources:
Resource Group: mastergroup
vip (ocf::heartbeat:IPaddr2): Started node1
ht-rsync (systemd:ht-rsync): Started node1
Initiating a Manual Failover

In a test environment, you can induce a failover in an otherwise healthy HA cluster from either the primary or a secondary node.

1. On your primary node, log in to CloudControl from the Virtual Machine Console Window or via SSH using your htadmin credentials.


3. Run the following command: `asc ha --mode secondary`
   The primary becomes a new secondary node, and the secondary node become the new primary.
   
   **Note:** If you have a three-node cluster, the secondary node to be promoted to primary is chosen at random.

4. To revert back to the original primary node, run the following command: `asc ha --mode primary`

Manual Failover Example:

```
[nodel:primary ~]$ asc ha --mode secondary
Making node nodel a secondary (failing over).
Waiting for failover...
Failover successful: New primary is node2.

[nodel:secondary ~]$ asc ha --mode primary
Making node node2 a secondary (failing over).
Waiting for failover...
Failover successful: New primary is nodel.
```

Cluster-related CLI Commands

Use the `asc ha` commands to manage High Availability (HA) on CloudControl.

**Syntax**

```
asc ha [options]
```
### Cluster-related CLI Commands

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>-d or --disband</strong></td>
<td>Disconnect from the HA cluster. This can only be run from a secondary node.</td>
</tr>
<tr>
<td><strong>-h or --help</strong></td>
<td>Displays usage text.</td>
</tr>
<tr>
<td><strong>-i or --interval &lt;minutes&gt;</strong></td>
<td>Sets the file synchronization period between nodes in minutes. Arguments must be in one or more minutes. Use 0 to turn off synchronization. By default, files are synced from the primary to the secondary node(s) every 1 minute.</td>
</tr>
<tr>
<td><strong>--form &lt;virtual-IP-address&gt; --virtname &lt;virtual-node-name&gt; --mode primary</strong></td>
<td>Form a one-node cluster from a node that was previously set up as standalone. This node will become the primary of the new cluster. Requires the virtual IP address and virtual node name for the cluster.</td>
</tr>
<tr>
<td><strong>-j or --join &lt;virtual-IP&gt; --password &lt;password&gt; --mode secondary</strong></td>
<td>Join an existing cluster as a secondary node, with the given virtual IP address and the given htadmin password.</td>
</tr>
<tr>
<td>**-o or --mode {primary</td>
<td>secondary}**</td>
</tr>
<tr>
<td><strong>-remove &lt;nodename&gt;</strong></td>
<td>Remove the specified node from the HA cluster.</td>
</tr>
<tr>
<td><strong>--sshkeyrotate</strong></td>
<td>Rotate the SSH keys used to exchange messages between nodes.</td>
</tr>
<tr>
<td><strong>-t or --status</strong></td>
<td>View the current configuration and operational state of the HA cluster.</td>
</tr>
<tr>
<td><strong>-s or --sync</strong></td>
<td>Forces an immediate synchronization of data between the HA nodes.</td>
</tr>
<tr>
<td>**--virtual-ip {show</td>
<td>&lt;new-virtual-IP&gt;}**</td>
</tr>
<tr>
<td>**--virtname {show</td>
<td>&lt;new-virtual-name&gt;}**</td>
</tr>
</tbody>
</table>

#### Examples

Form a one-node cluster with this node as primary with the given virtual IP address.

```shell
asc ha --form 192.0.2.134 --mode primary
```

Create an HA cluster by adding a secondary CloudControl node with the given IP and the htadmin password:

```shell
asc ha --join 192.0.2.134 --password PrimaryS3crEt! --mode secondary
```

Trigger a failover event from the secondary node:
asc ha --mode primary

Synchronize and then trigger a failover event from the primary node:

asc ha --sync --mode secondary

View the HA configuration and status:

asc ha --status

Remove the current node (where the command is being run) from the HA cluster:

asc ha --disband

Remove node3 from the HA cluster:

asc ha --remove node3
Chapter 6. Upgrading Your CloudControl Software

**Important:** Take a snapshot of the CloudControl appliance before beginning the upgrade process.

When upgrading CloudControl, the procedure for installing the upgrade differs depending on whether the appliance is in standalone mode or is configured as part of a High Availability pair. Please follow the instructions in the correct section for your situation.

**Note:** For version 6.0.2, you can only upgrade from version 6.0.1.

<table>
<thead>
<tr>
<th>Standalone Upgrade Using ISO Upload</th>
<th>30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone Upgrade Using vSphere</td>
<td>31</td>
</tr>
<tr>
<td>HA Pair Upgrade Using ISO Upload</td>
<td>32</td>
</tr>
<tr>
<td>HA Pair Upgrade Using vSphere</td>
<td>32</td>
</tr>
</tbody>
</table>

**Standalone Upgrade Using ISO Upload**

The following procedure shows how to upload the ISO file to the appliance via SFTP.

1. Upload the ISO file to the appliance via SFTP or SCP, using the htdadmin account.
2. Log in to the appliance via SSH using the htdadmin account.
3. At the command shell, enter the following command: 

\$ asc upgrade -i /pathname/filename.iso

where "pathname" and "filename" are the location and file name of the uploaded ISO image.

Example:

\$ asc upgrade -i /home/htadmin/HTCC-6.0.2-602172-upgrade.iso

Extracting Upgrade Package, please wait...

Installing...

--- Validating update
--- Upgrade Initiated
--- Preserve CA certs
--- Stopping services
--- Cleaning old backups
--- Cleaning up packages (pre-install)
--- Upgrading packages
--- Cleaning up packages (post-install)
--- Performing post-install tasks
--- Updating httpd conf
--- Upgrading HTCC DB
--- Upgrading HyTrust DB
--- Restarting services

CloudControl automatically restarts at the end of the upgrade.

4. The ISO image file may now be deleted from the appliance.

**Standalone Upgrade Using vSphere**

The following procedure shows how to mount the ISO image to the appliance using vSphere.

1. Upload the ISO to a datastore using the DataStore Browser.

2. Connect the CD/DVD drive of the appliance to the ISO in the datastore.

3. Log in to the appliance via SSH (or the VM console) using the htadmin account.

4. At the command shell, enter the following command: 

\$ asc upgrade -i

Example:

\$ asc upgrade -i

Extracting Upgrade Package, please wait...

Installing...

--- Validating update
--- Upgrade Initiated
--- Preserve CA certs
--- Stopping services
--- Cleaning old backups
--- Cleaning up packages (pre-install)
--- Upgrading packages
--- Cleaning up packages (post-install)
--- Performing post-install tasks
--- Updating httpd conf
--- Upgrading HTCC DB
--- Upgrading HyTrust DB
--- Restarting services

5. The ISO image may now be disconnected from the appliance and removed from the datastore.

HA Pair Upgrade Using ISO Upload

The following procedure shows how to upload the ISO file to the appliances via SFTP.

1. Upload the ISO file to the appliances via SFTP or SCP, using the htadmin account.

2. Log in to the appliances via SSH using the htadmin account.

3. Remove the secondary node from the cluster by running the following command on the primary:
   
   $ asc ha --remove <secondary_node_name>

4. Apply the upgrade on both the primary and the secondary using the following command:
   
   $ asc upgrade -i /pathname/filename.iso

   where "pathname" and "filename" are the location and file name of the uploaded ISO image.

   Example:
   
   $ asc upgrade -i /home/htadmin/HTCC-6.0.2-602172-upgrade.iso

   Extracting Upgrade Package, please wait...
   Installing...
   --- Validating update
   --- Upgrade Initiated
   --- Preserve CA certs
   --- Stopping services
   --- Cleaning old backups
   --- Cleaning up packages (pre-install)
   --- Upgrading packages
   --- Cleaning up packages (post-install)
   --- Performing post-install tasks
   --- Updating httpd conf
   --- Upgrading HTCC DB
   --- Upgrading HyTrust DB
   --- Restarting services

   CloudControl automatically restarts at the end of the upgrade.

5. To recreate the cluster after upgrading, run the following command on the secondary node:

   $ asc ha --join <vip_of_primary> --password <htadmin_password_on_primary> --mode secondary

6. The ISO image file may now be deleted from the appliance.

HA Pair Upgrade Using vSphere

The following procedure shows how to mount the ISO image to the appliances using vSphere.

1. Upload the ISO to a datastore using the DataStore Browser.

2. Connect the CD/DVD drive of both appliances to the ISO in the datastore.
3. Log in to the appliances via SSH (or the VM console) using the htadmin account.

4. Remove the secondary node from the cluster by running the following command on the primary:
   
   $ asc ha --remove <secondary_node_name>

5. Apply the upgrade on both the primary and the secondary using the following command: $ asc upgrade -i
   
   **Example:**
   
   $ asc upgrade -i
   Extracting Upgrade Package, please wait...
   Installing...
   --- Validating update
   --- Upgrade Initiated
   --- Preserve CA certs
   --- Stopping services
   --- Cleaning old backups
   --- Cleaning up packages (pre-install)
   --- Upgrading packages
   --- Cleaning up packages (post-install)
   --- Performing post-install tasks
   --- Updating httpd conf
   --- Upgrading HTCC DB
   --- Upgrading HyTrust DB
   --- Restarting services

   CloudControl automatically restarts at the end of the upgrade.

6. To recreate the cluster after upgrading, run the following command on the secondary node:
   
   $ asc ha --join <vip_of_primary> --password <htadmin_password_on_primary> --mode secondary

7. The ISO image may now be disconnected from the appliance and removed from the datastore.
Appendix A. Console Text-Based User Interface (TUI)

Accessing the TUI 34
Using the TUI 35
Modify your Network Settings 35
Test your Network Connectivity 36
Changing the htdadmin Password 36
Enable or Disable the Support User 37
Using the CLI Command Prompt 37
Switch from AD to Local Authentication Mode 37
Viewing or Modifying Active Directory Settings 38
Exiting the Console 38

Accessing the TUI

The CloudControl TUI is accessed by logging in as htdadmin. Depending on your appliance type, do one of the following:

Access the TUI from a Virtual Appliance for OVA

You can access the CloudControl TUI using one of the following:

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

Access the TUI from an AWS Cloud Appliance

To access the TUI 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 htdadmin to the instance:

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

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

1. Log in to the CloudControl console as htdadmin.

2. In the CloudControl TUI, enter your selection at the prompt. This can be one of the following:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. View/Modify network settings</td>
<td>Allows you to update the settings you created during CloudControl installation. See Modify your Network Settings below.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You cannot change networking settings for a cluster member.</td>
</tr>
<tr>
<td>2. Test remote server is reachable</td>
<td>Allows you to ping a remote server to ensure that it can be reached. See Test your Network Connectivity on the next page.</td>
</tr>
<tr>
<td>3. Change htdadmin password</td>
<td>Allows you to change your htdadmin password. See Changing the htdadmin Password on the next page.</td>
</tr>
<tr>
<td>4. Enable support user</td>
<td>Allows you to enable a support user that HyTrust Support can use to reach your system. See Enable or Disable the Support User on page 37.</td>
</tr>
<tr>
<td>5. Disable support user</td>
<td>Allows you to disable the support user when it is no longer necessary. See Enable or Disable the Support User on page 37.</td>
</tr>
<tr>
<td>6. Command prompt</td>
<td>Allows you to access the CloudControl CLI. See Using the CLI Command Prompt on page 37.</td>
</tr>
<tr>
<td>7. Switch to Local Mode Authentication</td>
<td>Allows you to disable your Active Directory settings and return to local authentication mode. See Switch from AD to Local Authentication Mode on page 37.</td>
</tr>
<tr>
<td>8. View/Modify AD Settings</td>
<td>Allows you to view or modify your Active Directory service account name and password. See Viewing or Modifying Active Directory Settings on page 38.</td>
</tr>
<tr>
<td>0. Quit console</td>
<td>Exits the console. See Exiting the Console on page 38.</td>
</tr>
</tbody>
</table>

Modify 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 TUI as htdadmin.

2. Select 1. View/Modify network settings and press Enter.
3. The TUI displays the existing settings for your system. For example:

   Please confirm the following settings:
   Cluster role: Standalone
   Virtual Management IP:
   Virtual Hostname:
   Hostname: test
   Node IP: 10.1.1.1
   Netmask: 255.255.255.0
   Gateway: 10.1.1.15
   DNS Server IP: 10.1.1.12
   DNS Domain Name: example.com

4. Type y at the Modify Primary interface network attributes? prompt to edit.

The following settings can be updated:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>Enter the new hostname.</td>
</tr>
<tr>
<td>Node IP</td>
<td>Enter the new node IP.</td>
</tr>
<tr>
<td>Netmask</td>
<td>Enter the new netmask.</td>
</tr>
<tr>
<td>Gateway</td>
<td>Enter the new gateway.</td>
</tr>
<tr>
<td>DNS Server IP</td>
<td>Enter the new DNS server IP.</td>
</tr>
<tr>
<td>DNS Domain Name</td>
<td>Enter the new DNS domain name.</td>
</tr>
</tbody>
</table>

**Test your Network Connectivity**

1. Log in to the CloudControl TUI as htaadmin.
2. Select 2. Test remote server is reachable.
3. Enter the remote service or IP address that you want to test.

CloudControl pings the server and displays the connection information.

**Changing the htaadmin Password**

1. Log in to the CloudControl TUI as htaadmin.
3. Enter the current password at the prompt.
4. 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: ~, !, @, #, $, %, ^, &, *, (, ), -, +.

5. 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.

Enable or Disable the Support User

The htsupport user allows HyTrust support to access your system.

1. Log in to the CloudControl TUI as htdmin.
2. Select 4. Enable support user.
3. Enter and confirm a password for the HyTrust support user. **Note:** The password is only valid for 24 hours.
4. Exit the console, and then log back in as htsupport with the password you created.

HyTrust Support can now assist you further.

**Note:** The htsupport user password will expire in 24 hours, or you can disable the support user at any time by logging in to the CloudControl TUI and selecting 5. Disable support user.

Using the CLI Command Prompt

1. Log in to the CloudControl TUI as htdmin.
3. At the prompt, enter the CLI command that you want to run.
4. Type exit to return to the TUI menu.

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 TUI as htdmin.
2. Select 7. Switch to Local Authentication Mode.
3. At the Are you sure you want to continue? prompt, type y.
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 TUI as htdmin.
2. Select 8. View/Modify AD Settings.
   The current AD settings are displayed.
3. At the Modify AD Service Account prompt, type y to modify your settings or type N to return to the main TUI menu.
4. If you selected y, then complete the following:
   a. At the Enter AD service account prompt, enter the new service account name or hit enter to accept the current value.
   b. At the Enter Password prompt, enter the new password for the service account.

Exiting the Console

1. Log in to the CloudControl TUI as htdmin.
2. Select 0. Quit Console.

CloudControl logs out of the console and returns you to the login prompt.