Copyright and Legal Notice

HyTrust CloudControl® v 5.6

Copyright © 2019 HyTrust, Inc. All Rights Reserved.

HyTrust, HyTrust, Inc., Virtualization Under Control, HyTrust CloudAdvisor, HyTrust CloudControl, HyTrust DataControl, HyTrust KeyControl and other HyTrust product names are trademarks of HyTrust, Inc. Other trademarks are recognized as belonging to their respective owners. The content of this guide is furnished for informational use only and is subject to change without notice. HyTrust assumes no responsibility or liability for any errors or inaccuracies that may appear in the content contained in this guide. Except as allowed by license, no part of this material may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without the written permission of the copyright owner, except where permitted by law.

# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>What's New</td>
<td>14</td>
</tr>
<tr>
<td><strong>Chapter 1. Using the CloudControl Management Console</strong></td>
<td>17</td>
</tr>
<tr>
<td>Management Console Overview</td>
<td>17</td>
</tr>
<tr>
<td>Starting the CloudControl Management Console</td>
<td>17</td>
</tr>
<tr>
<td><strong>Chapter 2. Authentication</strong></td>
<td>18</td>
</tr>
<tr>
<td>Authentication and Authorization Overview</td>
<td>18</td>
</tr>
<tr>
<td>Configuring Active Directory</td>
<td>19</td>
</tr>
<tr>
<td>Creating a New Service Account in Active Directory</td>
<td>19</td>
</tr>
<tr>
<td>Service Account Privileges</td>
<td>20</td>
</tr>
<tr>
<td>Creating Security Groups in Active Directory</td>
<td>20</td>
</tr>
<tr>
<td>Unified Authentication</td>
<td>20</td>
</tr>
<tr>
<td>Integrating CloudControl with Active Directory</td>
<td>21</td>
</tr>
<tr>
<td>Updating the AD Service Account or Role-Group Mapping</td>
<td>24</td>
</tr>
<tr>
<td>Using the Authentication Configuration Page</td>
<td>25</td>
</tr>
<tr>
<td>Root Domain Tab</td>
<td>25</td>
</tr>
<tr>
<td>Configuration Types Tab</td>
<td>25</td>
</tr>
<tr>
<td>Global Catalogs Tab</td>
<td>26</td>
</tr>
<tr>
<td>Domains Tab</td>
<td>26</td>
</tr>
<tr>
<td>Service Account Tab</td>
<td>27</td>
</tr>
<tr>
<td>Advanced Tab</td>
<td>27</td>
</tr>
<tr>
<td>Authentication Modes</td>
<td>28</td>
</tr>
<tr>
<td>Smart Card Authentication</td>
<td>28</td>
</tr>
<tr>
<td>Two-Factor Authentication</td>
<td>29</td>
</tr>
<tr>
<td><strong>Chapter 3. Managing Hosts</strong></td>
<td>35</td>
</tr>
<tr>
<td>Adding Hosts to CloudControl</td>
<td>35</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Modifying Managed Hosts</td>
<td>37</td>
</tr>
<tr>
<td>Removing Managed Hosts</td>
<td>37</td>
</tr>
<tr>
<td>Global Published IP Address</td>
<td>37</td>
</tr>
<tr>
<td>Enabling or Disabling Global PIP</td>
<td>38</td>
</tr>
<tr>
<td>Adding a Global PIP to a Single Host</td>
<td>38</td>
</tr>
<tr>
<td>Adding a Global PIP to Multiple Hosts</td>
<td>39</td>
</tr>
<tr>
<td>Viewing ESXi Host Connectivity Information when using Global PIP</td>
<td>39</td>
</tr>
<tr>
<td>Connecting to an Individual Host Through Global PIP</td>
<td>39</td>
</tr>
<tr>
<td>Global PIP API</td>
<td>41</td>
</tr>
<tr>
<td>Configuring Web Client Server Operations</td>
<td>42</td>
</tr>
<tr>
<td>Trust Attestation Service Configuration</td>
<td>42</td>
</tr>
<tr>
<td>Configuring TAS</td>
<td>43</td>
</tr>
<tr>
<td>Enabling a Good Known Host</td>
<td>43</td>
</tr>
<tr>
<td>Disabling a Good Known Host</td>
<td>44</td>
</tr>
<tr>
<td>Verify and Update Host Trust</td>
<td>44</td>
</tr>
<tr>
<td>Host Icons used in CloudControl</td>
<td>45</td>
</tr>
<tr>
<td>Approved Hosts</td>
<td>45</td>
</tr>
<tr>
<td>Adding Approved Hosts</td>
<td>46</td>
</tr>
<tr>
<td>Removing Approved Hosts</td>
<td>46</td>
</tr>
<tr>
<td>Using Filters to View Managed Hosts</td>
<td>46</td>
</tr>
<tr>
<td><strong>Chapter 4. Configuring Security Options</strong></td>
<td>47</td>
</tr>
<tr>
<td>Static Routes</td>
<td>47</td>
</tr>
<tr>
<td>Root Password Vaulting</td>
<td>48</td>
</tr>
<tr>
<td>Set Recovery Passcode</td>
<td>48</td>
</tr>
<tr>
<td>Enable Root Password Vaulting</td>
<td>49</td>
</tr>
<tr>
<td>Request a Temporary Root Password</td>
<td>49</td>
</tr>
<tr>
<td>Cancel a Temporary Root Password</td>
<td>50</td>
</tr>
<tr>
<td>Configuring Monitor Mode</td>
<td>50</td>
</tr>
<tr>
<td>Enabling Monitor Mode</td>
<td>51</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Disabling Monitor Mode</td>
<td>51</td>
</tr>
<tr>
<td>Scheduled Events</td>
<td>51</td>
</tr>
<tr>
<td>Adding a Scheduled Event</td>
<td>52</td>
</tr>
<tr>
<td>Editing a Scheduled Event</td>
<td>53</td>
</tr>
<tr>
<td>Deleting a Scheduled Event</td>
<td>54</td>
</tr>
<tr>
<td>Monitoring with SMTP and SNMP in CloudControl</td>
<td>54</td>
</tr>
<tr>
<td>Configuring Monitoring and Notifications</td>
<td>55</td>
</tr>
<tr>
<td>Managing Certificates</td>
<td>55</td>
</tr>
<tr>
<td>About Certificates</td>
<td>55</td>
</tr>
<tr>
<td>Generating a Certificate Signing Request</td>
<td>56</td>
</tr>
<tr>
<td>Generating a Self-Signed Certificate</td>
<td>58</td>
</tr>
<tr>
<td>Installing a Signed Certificate</td>
<td>59</td>
</tr>
<tr>
<td>Installing a Third-Party Root Certificate</td>
<td>60</td>
</tr>
<tr>
<td>Installing Autoimport Certificates</td>
<td>60</td>
</tr>
<tr>
<td>Changing Password Requirements for ascadminuser</td>
<td>61</td>
</tr>
<tr>
<td>Changing the ascadminuser Password</td>
<td>62</td>
</tr>
<tr>
<td>Session Timeouts</td>
<td>62</td>
</tr>
<tr>
<td>Command Line Prompts</td>
<td>62</td>
</tr>
<tr>
<td>SSH Banners</td>
<td>64</td>
</tr>
<tr>
<td>Editing the SSH Banner File</td>
<td>64</td>
</tr>
<tr>
<td>Chapter 5. Compliance</td>
<td>65</td>
</tr>
<tr>
<td>Compliance Overview</td>
<td>65</td>
</tr>
<tr>
<td>Assessment</td>
<td>65</td>
</tr>
<tr>
<td>Remediation</td>
<td>66</td>
</tr>
<tr>
<td>Rollback to Previous</td>
<td>66</td>
</tr>
<tr>
<td>Revert to Initial</td>
<td>66</td>
</tr>
<tr>
<td>Host Compliance</td>
<td>67</td>
</tr>
<tr>
<td>Assessing Hosts</td>
<td>68</td>
</tr>
<tr>
<td>Remediating Hosts</td>
<td>69</td>
</tr>
</tbody>
</table>
Revert to Initial State ........................................................................................................70
Rollback to Previous State ...............................................................................................70
Compliance History ...........................................................................................................70
Host Configuration Templates .........................................................................................70
  System Templates ...........................................................................................................71
  Custom Templates .........................................................................................................71
  Copying a Template .......................................................................................................73
vSphere Catalogs ...............................................................................................................73
NSX Catalogs ....................................................................................................................74

Chapter 6. Access Policies .................................................................................................75
  Access Policies Overview ...............................................................................................75
  Viewing the Current Policy .........................................................................................75
  Changing the Current Policy .........................................................................................75
  Policy Definitions and Behavior ...................................................................................76
  Policy Resource .............................................................................................................76
  Roles ...............................................................................................................................76
  Domain User Group ......................................................................................................77
  Rules ...............................................................................................................................77
  Constraints ....................................................................................................................78
  RuleSets .........................................................................................................................80
  Labels .............................................................................................................................81
  User Attributes .............................................................................................................83
  PolicyTags .....................................................................................................................85
  PolicyTags Provisioning .................................................................................................87
  Separation of Duties ......................................................................................................89
  Policy Interaction ..........................................................................................................89
  Restricting Visibility ......................................................................................................93
  Visibility Privileges for NSX and vSphere Objects .......................................................94
  Using Constraints with Visibility Privileges ...............................................................95
Chapter 7. Alerts

Alerts Overview .................................................. 97
Configuring Alerts .................................................. 97
Alert Definitions .................................................... 98
ASC Alert Definitions .............................................. 98
Resource Alert Definitions ...................................... 98
Configuring ASC Alert Definitions ............................. 99
Adding Resource Alert Definitions .............................. 101
Editing Resource Alert Definitions .............................. 102
Viewing Alert Definition Details ............................... 103
Deleting Alert Definitions ........................................ 103
Enabling or Disabling Alert Definitions ........................ 103
vSphere Operations for Resources ............................. 103
Alert Viewing ....................................................... 104
Viewing Alert Messages in CloudControl .................... 105
Email Notifications ................................................ 105
Viewing Alerts in the Syslog Server ........................... 105
Using Alerts Examples ............................................ 106

Chapter 8. Secondary Approval .................................. 109
Secondary Approval Overview .................................. 109
Secondary Approval Requirements ............................ 110
Best Practices for Secondary Approval ....................... 110
Configuring Secondary Approval .............................. 110
Creating a Secondary Approval Control ...................... 111
Viewing Secondary Approval Controls ....................... 112
List of Secondary Approval Operations ....................... 112
Pending Secondary Approval Requests ....................... 114
| Approving a Pending Request | 114 |
| Denying a Pending Request | 115 |
| Viewing Request History | 115 |

**Chapter 9. Dashboard Management**

Using the CloudControl Appliance Dashboard | 116
Admin Access Dashboard | 116
Compliance Dashboard | 117
Protection Dashboard | 120
Recent Activity Dashboard | 123
Appliance Health | 126

**Chapter 10. Log Viewer**

Log Viewer Overview | 130
Filters | 130
Heatmap | 131
Leaderboard | 132
Log Messages | 133
Saving Filters | 135
Exporting Log Files to CSV | 136
Logging Overview | 136
Appliance and Host Logging | 137
Syslog in CloudControl | 137
Encrypting Syslog | 137
Configuring CloudControl Logging | 138
Host Default Logging Configuration | 139
Managing Logging Retention Configuration | 139
Appliance Health and Logging Service Alerts | 140
Viewing Log Messages from the CLI | 141
Obtaining the Troubleshooting Bundle | 141
Obtaining System Logs | 141
### Chapter 11. Monitoring Hosts and Networks ................................................................. 143
- Enabling Monitoring ......................................................................................... 143
- Network Resource Monitoring ..................................................................... 143
- Protected Host Monitoring ........................................................................... 144
- Viewing NRM and PHM Status ...................................................................... 144

### Chapter 12. Maintaining the Appliance ................................................................. 145
- Licenses ........................................................................................................... 145
- CloudControl Services .................................................................................. 146
- Using the HyTrust Vitals Service .................................................................. 147
- Enabling Proxy Server for the Vitals Service and Licensing Service .......... 147
- Backing Up the CloudControl Appliance ...................................................... 148
- Rebooting CloudControl ............................................................................... 148
- Viewing Jobs .................................................................................................. 149
- Searches ......................................................................................................... 149

### Chapter 13. Reports .............................................................................................. 152
- Reports Overview .......................................................................................... 152
- Configuring Reports ....................................................................................... 152
- Report Definitions ......................................................................................... 152
  - Adding Report Definitions ............................................................................ 153
  - Editing Report Definitions ........................................................................... 154
  - Deleting Report Definitions ........................................................................ 154
- Report Types .................................................................................................. 154
  - Authentication Login Report ....................................................................... 154
  - Authentication Operation Report ................................................................. 155
  - Continuous Monitoring Assessment Report .............................................. 156
  - Root of Trust - Attempted Changes Denied Report .................................. 156
  - Root of Trust - Good Known Host (GKH) Report ...................................... 157
  - Root of Trust - Current Hosts and Trust Status Report ......................... 157
- Exporting Reports ............................................................................................ 158
<table>
<thead>
<tr>
<th>Chapter 14. VMware NSX in CloudControl</th>
<th>161</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using VMware NSX in CloudControl Overview</td>
<td>161</td>
</tr>
<tr>
<td>NSX Host Management</td>
<td>163</td>
</tr>
<tr>
<td>Adding VMware NSX with vCenter</td>
<td>163</td>
</tr>
<tr>
<td>Adding VMware NSX as a Host</td>
<td>165</td>
</tr>
<tr>
<td>Restarting the CloudControl Application Server</td>
<td>165</td>
</tr>
<tr>
<td>NSX Compatibility</td>
<td>166</td>
</tr>
<tr>
<td>Testing NSX Compatibility</td>
<td>166</td>
</tr>
<tr>
<td>Manually Testing NSX Compatibility</td>
<td>167</td>
</tr>
<tr>
<td>Automatically Testing NSX Compatibility</td>
<td>167</td>
</tr>
<tr>
<td>Policy</td>
<td>167</td>
</tr>
<tr>
<td>Refreshing Policy Resources</td>
<td>168</td>
</tr>
<tr>
<td>NSX Cross vCenter Support</td>
<td>168</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 15. Boundary Control</th>
<th>169</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boundary Control Overview</td>
<td>169</td>
</tr>
<tr>
<td>Boundary Control Use Cases</td>
<td>169</td>
</tr>
<tr>
<td>CloudControl Updates for Boundary Control</td>
<td>170</td>
</tr>
<tr>
<td>Boundary Control System Requirements</td>
<td>170</td>
</tr>
<tr>
<td>CloudControl Requirements for Boundary Control</td>
<td>170</td>
</tr>
<tr>
<td>HyTrust KeyControl Requirements</td>
<td>171</td>
</tr>
<tr>
<td>Creating the Default Boundary Control Rule</td>
<td>171</td>
</tr>
<tr>
<td>Enabling Boundary Control</td>
<td>171</td>
</tr>
<tr>
<td>Registering KeyControl with CloudControl</td>
<td>172</td>
</tr>
<tr>
<td>Creating a VM Set with Boundary Control Enabled</td>
<td>172</td>
</tr>
</tbody>
</table>
Authenticating a VM for Key Delivery ................................................................. 175
App Links in CloudControl and DataControl ...................................................... 177
Creating an App Link One Time Code ................................................................. 177

Chapter 16. CloudControl with Auto Deployed ESXi Hosts .................................... 179
Auto Deploy Overview ......................................................................................... 179
Auto Deploy Alerts .............................................................................................. 179
Auto Deploy Scheduled Events ........................................................................... 180
Upgrade CloudControl with Auto Deploy-enabled vCenter Servers ......................... 180

Chapter 17. Using the vSphere HTML5 Client ......................................................... 181
Download and Import the vSphere Client Metadata .............................................. 181
Running the vSphere Client using the PIP ............................................................ 181

Appendix A. Default Roles and Permissions ......................................................... 182
NSX Roles ............................................................................................................. 183
vSphere 6.x Roles ................................................................................................. 184
CloudControl Appliance Management ................................................................. 186
Other Roles ........................................................................................................... 187

Appendix B. Root Password Recovery .................................................................. 188

Appendix C. Search Filters ................................................................................... 190

Appendix D. CloudControl Command Line Interface (CLI) ................................... 192
Using the CloudControl CLI .............................................................................. 192
asc auth ............................................................................................................... 192
asc backup ......................................................................................................... 193
asc certs ............................................................................................................. 196
asc firewall ....................................................................................................... 199
asc ha .................................................................................................................... 200
asc log ............................................................................................................... 204
asc monitor ....................................................................................................... 206
asc network ....................................................................................................... 208
asc policy ......................................................................................................... 210
Appendix E. Supported Authentication Modes .............................................. 220
  CloudControl Service Account .......................................................... 220
  IWA Support .................................................................................... 220
  Smart Card Support ........................................................................... 221

Authentication Modes ............................................................................. 221
  Use CloudControl Service Account (default) ...................................... 221
  Smart Card Authentication .................................................................. 221
  Use pass through without CloudControl Service Account ................. 222
  Smart Card Authentication .................................................................. 222
  Use pass through with CloudControl Service Account .................... 222
  Smart Card Authentication .................................................................. 223

Appendix F. REST API Guide ................................................................... 224

REST API Overview .................................................................................. 224
Accessing APIs ....................................................................................... 224
Authentication ......................................................................................... 224
  Authentication Token ......................................................................... 224
  Logout ............................................................................................... 226
Resource/Host Management ................................................................... 227
  Resource .......................................................................................... 227
  Host Systems .................................................................................. 235
  Virtual Machines ............................................................................. 256
  Management Systems ..................................................................... 265
  Label Management .......................................................................... 281
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 5.6

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary Approval</td>
<td>Added a Permitted Operation Count to limit the number of times an operations is permitted during the given duration.</td>
<td>Approving a Pending Request on page 114</td>
</tr>
<tr>
<td>Proxy Server Support</td>
<td>Allows you to use a proxy server to communicate with the Vitals Service and Licensing server.</td>
<td>In the Configuring the Management Interface or Configuring the Management Console sections in the Installation Guide for HyTrust CloudControl. Enabling Proxy Server for the Vitals Service and Licensing Service on page 147</td>
</tr>
<tr>
<td>NSX Security Tags</td>
<td>The NSX security tag(s) constraint can be used to achieve logical segmentation on NSX security tags. When used in a rule, it limits the ability of NSX users to perform NSX security tag operations, such as editing, deleting, or assigning or unassigning tags, on the specified tag.</td>
<td>Constraints on page 78</td>
</tr>
<tr>
<td>Compliance Templates Enhancements</td>
<td>Added new compliance operations for vSphere 6.0, 6.5 and 6.7.</td>
<td>See the CloudControl Compliance Operations Guide.</td>
</tr>
</tbody>
</table>
## What's New in CloudControl, Version 5.5

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Published IP (Global PIP)</td>
<td>You can now use a Global published IP address (Global PIP) instead of dedicated published IP addresses (PIP) for your protected ESXi hosts.</td>
<td>Global Published IP Address on page 37</td>
</tr>
<tr>
<td>Firewall improvements</td>
<td>You can now remove the SSH RSA key fingerprints for all protected ESXi hosts in CloudControl.</td>
<td>asc firewall on page 199</td>
</tr>
<tr>
<td>Restricting View Privileges</td>
<td>Added support for the vSphere HTML5 client.</td>
<td>Restricting Visibility on page 93</td>
</tr>
<tr>
<td>Compliance Templates Enhancements</td>
<td>Added the VMware 6.7 ESXi template, and new compliance operations for vSphere 6.0, 6.5 and 6.7.</td>
<td>See the CloudControl Compliance Operations Guide.</td>
</tr>
<tr>
<td>Vitals Service</td>
<td>Automatic Vitals Reporting lets you automatically share information about the health of your CloudControl cluster with HyTrust Support.</td>
<td>Using the HyTrust Vitals Service on page 147</td>
</tr>
<tr>
<td>vRealize Orchestrator</td>
<td>Added support for vRealize Orchestrator (vRO).</td>
<td>Using vRealize Orchestrator with CloudControl on page 303</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>Added new SNMP Traps.</td>
<td>SNMP Traps on page 306</td>
</tr>
<tr>
<td>Encrypted Syslog</td>
<td>Added updates to encrypted syslog.</td>
<td>Encrypting Syslog on page 137</td>
</tr>
</tbody>
</table>

## What's New in CloudControl, Version 5.4.2

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
</table>
| Advanced Intrusion Detection Environment (AIDE) Enhancements | You can now:  
- View the `asc monitor --fileaudit` command output in syslog as well as the console.  
- Run the `asc monitor --fileprofile` command to reinitialize the AIDE database.  
- Run the `asc monitor --filemon` command to enable a cron job. | asc monitor on page 206 |
<p>| Two-Factor Authentication Whitelist | Allows you to create a whitelist for two-factor authentication so that your tools can connect to vCenter through CloudControl without being prompted for two-factor authentication. | Two-Factor Authentication Whitelist on page 33 |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dual Site HA Configuration</td>
<td>Allows you to configure HA on two different subnets.</td>
<td>GUI: See the Configuring High Availability chapter in the Installation Guide for HyTrust CloudControl CLI: asc ha on page 200</td>
</tr>
</tbody>
</table>

**What's New in CloudControl, Version 5.4**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
<th>Where Documented</th>
</tr>
</thead>
<tbody>
<tr>
<td>ascrescue account</td>
<td>Allows you to add an additional layer of security between you and CloudControl support.</td>
<td>asc service on page 215</td>
</tr>
<tr>
<td>Remote backups</td>
<td>Allows you to schedule and create remote backups.</td>
<td>asc backup on page 193</td>
</tr>
</tbody>
</table>
| Active Directory Enhancements | • Added manual refresh of the User-to-Group map cache.  
  • Added domain controller status refresh.  
  • Allows you to set primary and secondary global catalogs and domain controllers. | Authentication on page 18                                                        |
| vSphere Client Enhancements   | Added support for vSphere 6.5 U2, including Content Library operations. | Using the vSphere HTML5 Client on page 181                                         |
| New Compliance Templates      | Added new compliance operations and the following compliance templates:  
  • GDPR HTCC ESXi  
  • NERC CIP 5.0 ESXi  
  • NIST 800-171 ESXi | See the CloudControl Compliance Operations Guide.                                  |
| Certificate Enhancements      | CloudControl now automatically downloads vCenter and PSC certificates so you can easily install them. | Installing Autoimport Certificates on page 60                                     |
| Viewing Hosts Enhancements    | Added RPV Enabled and RPV Disabled to the list of filters on the Hosts page. | Using Filters to View Managed Hosts on page 46                                     |
| Rules Enhancements            | You can now import and export rules.             | Importing Rules on page 78 and Exporting Rules on page 77                        |

HyTrust CloudControl v 5.6  Administration Guide 16
Chapter 1. Using the CloudControl Management Console

Management Console Overview

Use the web-based CloudControl Management Console to customize CloudControl configuration settings and set up policies for safeguarding your managed virtual infrastructure environment. The management console provides menus to set authentication options for users, add vCenter servers and hosts to the protected infrastructure, define templates and policy checks to enforce security of protected virtual infrastructure, and view and configure logs.

Starting the CloudControl Management Console

After you complete the initial configuration, as discussed in the HyTrust CloudControl Installation Guide, authorized users can now access the web-based CloudControl Management Console to set up CloudControl to safeguard your managed virtual infrastructure environment.

To start the CloudControl Management Console:

1. Open a web browser and enter the URL location of the CloudControl virtual machine (as shown in the vSphere Client console after powering up the CloudControl virtual machine). For example:
   
   https://htcc.example.com/asc

   **Note:** Only secure HTTPS sessions are supported. All HTTP connections are redirected to HTTPS.

2. On the login screen, enter your CloudControl username and password and click **Login**.

   **Note:** If you are using Active Directory (AD) authentication and roles, you can log in using a CloudControl user who is a member of the group with the ASC_SuperAdmin role. For a list of available CloudControl roles and the corresponding permissions granted to group members on login, see Default Roles and Permissions on page 182.
Chapter 2. Authentication

Authentication and Authorization Overview ................................................................. 18
Configuring Active Directory ....................................................................................... 19
Unified Authentication ................................................................................................. 20
Integrating CloudControl with Active Directory ......................................................... 21
Updating the AD Service Account or Role-Group Mapping ......................................... 24
Using the Authentication Configuration Page ............................................................ 25
Authentication Modes .................................................................................................. 28

Authentication and Authorization Overview

CloudControl uses the following types of user authentication:

- **Demo mode**—supports default, built-in users only. CloudControl operates in Demo mode after installation. Demo mode is only intended for product evaluation and testing. When you install CloudControl in a production environment, you should immediately convert CloudControl to use Directory Service mode.

- **Directory Service mode**—uses Microsoft® Active Directory (AD) for authentication.
  
  For additional security, you can add two-factor authentication with RADIUS Server, TACACS+, or RSA SecurID. For more information, see Two-Factor Authentication on page 29.

While in Demo mode, CloudControl contains a number of uniquely-defined roles. There are several special demo users (stored locally) who are assigned specific roles to access and perform operations on the virtual infrastructure. Demo users cannot be modified and you cannot change their passwords. The default password for all Demo users is Pa$$w0rd123!. The roles available in Demo mode are listed in Default Roles and Permissions on page 182.

  **Note:** Once CloudControl is configured for Directory Service mode authentication and authorization, Demo mode cannot be re-enabled.

While converting CloudControl to Directory Service mode, default rules are created that map existing user groups in the directory service to the default CloudControl roles. This allows administrators to enable role-based access to the virtual infrastructure simply by adding the user identities to these directory groups, based on their individual responsibilities. CloudControl provides three types of authentication using the Service Account. These authentication modes can be used for Integrated Windows Authentication as well as Smart Card Authentication. See Supported Authentication Modes on page 220.

Instead of using the existing directory service security groups, you may find it helpful to manually create specific groups in your directory service for each CloudControl group prior to converting CloudControl to Directory Service mode. This would allow for a 1:1 mapping between directory group names and CloudControl roles. At a minimum, one directory security group (e.g., SuperAdmin) must be mapped to the ASC_SuperAdmin role in CloudControl.
You can define custom rules that restrict entitlement based on the specific virtual infrastructure objects that users need to access and manage. These rules can be based on the pre-defined roles or you can use custom user-defined roles. Rules create a relationship between a group, one or more objects, and one CloudControl role. The directory group has a defined entitlement based on a rule. The entitlement specifies operations that users in the group may perform on the objects.

For example, the ASC_NetworkAdmin role specifies privileges to perform AddPortGroup and RemoveVirtualSwitch operations. Therefore, all members of the HT_NetworkAdmin directory security group are allowed to perform these operations on a policy resource, such as a CloudControl managed vCenter Server, and all objects, including the networking subsystem, in that vCenter Server.

A collection of rules currently enforced by CloudControl constitutes a deployed or active policy. Policy, rules, and role definitions can be defined using the CloudControl Management Console. Further details regarding policy, rules, and roles can be found in Access Policies on page 75.

### Configuring Active Directory

Directory Service mode allows you to use Active Directory (AD) for authenticating virtual infrastructure users as well as CloudControl Management Console users, and requires that you create an CloudControl service account in your AD server.

Before creating the CloudControl service account, ensure you have a good understanding of where the service accounts, groups, and users are currently stored in AD. The CloudControl supports the ability to have the service account in one container (CN) or organizational unit (OU) while the CloudControl groups reside in a different CN or OU. Support for multiple domains within a single AD forest is also available by using the advanced settings within the AD conversion wizard. For more information, see Integrating CloudControl with Active Directory on page 21.

CloudControl integrates directly with AD via LDAP protocols using the CloudControl service account credentials. CloudControl uses the service account to query AD and ascertain the appropriate group membership for the users. This interaction occurs each time a user attempts to access the virtual infrastructure.

**Note:** Before you configure Active Directory, ensure that your network configuration settings have been applied. For more information, see the Installation Guide for HyTrust CloudControl.

### Creating a New Service Account in Active Directory

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.

When you are asked to assign the password to the new service account:
4. Enter the password in the **Password** and **Confirm password** fields.
5. Deselect the **User must change password at next logon** checkbox.
6. Select the **Password never expires** checkbox.
7. Click **Next**.

**Service Account Privileges**

The new CloudControl service account is created with only query privileges on the CloudControl server AD forest. In some environments, the AD administrator may have modified the default account privileges.

The CloudControl 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, on the Object tab in the CloudControl service account properties.

**Creating Security Groups in Active Directory**

Default CloudControl rules are created by mapping existing user groups in AD to default roles in CloudControl when CloudControl is converted to Directory Service mode. In a complex environment with a large number of administrators, it is common to create unique AD group names that correspond to each of the CloudControl default roles. At a minimum, one AD security group must be mapped for the AD conversion to be successful. For example, you could map SuperAdmin to the ASC_SuperAdmin role. AD group names do not need to follow the CloudControl naming convention.

You can retrieve the necessary Active Directory users and group information with ReadOnly privileges.

Perform the following to create the CloudControl security groups in AD:

1. Create a security group for each CloudControl role described in Default Roles and Permissions on page 182.
2. For each group, assign the Group scope to Global and the Group type to Security.
   CloudControl supports security groups with domain local, domain global, and/universal scope. Check with your AD administrator to confirm the proper setting for your environment.

**Unified Authentication**

CloudControl intercepts all requests destined for CloudControl-protected hosts, such as ESXi and vCenter Server, and authenticates the user against the Directory Service. Authentication of the user, including session ID, lasts for the full session. Once a session is established, authorization to perform a particular operation, including directory group membership, can occur on multiple occasions per session.
After CloudControl authenticates the user, it performs an authorization check for each request based on the local policy data. If authorized, CloudControl forwards the request to the target server using a special service account.

**Note:** CloudControl has the ability to follow the domain controller and global catalog referrals in a single Active Directory forest. If your Active Directory environment is set up to follow referrals, please contact HyTrust Support to help you enable this feature in CloudControl.

The following example shows the authentication and authorization process:

1. CloudControl obtains the user's identity when the user attempts to log in.
2. CloudControl queries the Directory Service to authenticate the user and validate the user's password. CloudControl also obtains information about the user's group membership to authorize every operation the user attempts to perform, for example:
   a. Identify the requested operation (i.e., start a virtual machine or change the iSCSI configuration on the server).
   b. Identify the object a user is targeting for an operation (i.e., VM 'mref 449' or esx54.example.com).
   c. Query the CloudControl policy database to identify the list of user groups authorized to perform the requested operation on the specified object and determine if the current user is a member of an authorized user group.
   d. CloudControl logs information about the operation, the user, and the object involved.

If the user is authorized, CloudControl reissues the operation request and sends it to the CloudControl protected host, such as vCenter Server or ESXi, to which the original login request was routed. Otherwise, CloudControl returns an error message to the user.

## Integrating CloudControl with Active Directory

**Important:** Once you convert CloudControl to Directory Service mode for authentication and authorization, you cannot revert to Demo mode.

### Before You Begin

We recommend that you manually create CloudControl-specific security groups in AD before the conversion. For more information, see [Creating Security Groups in Active Directory](#) on the previous page.

### Procedure

1. Select **Configuration > Authentication**.
2. On the Authentication Configuration page, select the **Directory Service** radio button and click **Apply**.
3. In the Active Directory Conversion Wizard, on the Configure Service Account page, enter the Domain Name where your AD is located using the following format:
   
   `corp.example.com`

   CloudControl supports either a single or multiple domain forest. If your AD forest includes only a single domain, the forest root domain will include all your users, groups, and resources.
4. Enter the AD CloudControl service account information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Enabled</td>
<td>Check the <strong>SSL Enabled</strong> checkbox if your AD uses SSL. If you need to configure your AD using SSL, the AD SSL certificate should be imported before AD configuration. SSL is disabled by default.</td>
</tr>
<tr>
<td>Service Account Name</td>
<td>The CloudControl service account user name in AD, for example ascserviceaccount. If the service account is located in a different domain, enter the full path, for example <a href="mailto:ascserviceaccount@subdomain.corp.example.com">ascserviceaccount@subdomain.corp.example.com</a>.</td>
</tr>
<tr>
<td>Service Account Password</td>
<td>The AD password for your service account.</td>
</tr>
<tr>
<td>Confirm Service Account Password</td>
<td>Reenter the AD password for your service account.</td>
</tr>
</tbody>
</table>

**Important:** The CloudControl service account must exist in AD before you convert CloudControl to Directory Service mode.

5. In the **Configuration Methods** area, specify either automated discovery or manual configuration.

**Important:** Automated discovery is often sufficient to complete the conversion. CloudControl uses the service account credentials to automatically discover the list of forest global catalogs and domain controllers to use when authenticating users. However, if you want to set priorities for your domain controllers and global catalogs, you must use manual configuration.

If you selected **Automated Discovery**, do the following:

a. On the Configure Service Account page, click **Next**.

b. On the Active Directory Discovered Domains page, ensure that all the available domains are selected.

c. To change the default configuration for the Automated Discovery method, check the **View Active Directory Advanced Settings** checkbox and click **Next**.

d. On the Active Directory Advanced Settings page, you can update the SSL settings, custom ports, search contexts.

e. Click **Next**.

**Note:** If automated discovery fails, return to the Configure Service Account page and select the **Manual Configuration** radio button.
If you selected **Manual Configuration**, do the following:

a. On the Configure Service Account page, click **Next**.

b. On the Active Directory Advanced Settings page, enter the root domain and the default domain for your AD.

   specify the root domain, preferred global catalog, domain names, and custom ports.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controllers</td>
<td></td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Check the checkbox if your domain controller uses SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the domain controller port.</td>
</tr>
</tbody>
</table>

**Note:** The Add and Delete buttons in the Domain Controllers panel are active only when the Configuration Type is set to Manual Configuration. For automated discovery these values are populated automatically.

c. In the Global Catalogs area, click **Enable SSL** if your global catalog uses SSL, and enter the global catalog port number.

d. Click the **Add** button, and then enter the global catalog name and the priority.

   **Note:** The priority can be either primary or secondary. CloudControl will always attempt to use the primary first, then failover to secondary if the first cannot be reached. The secondary global catalog will not be promoted to primary, and is only used until the global catalog marked as primary is available.

e. In the Domain Controllers area, click **Enable SSL** if your domain controller uses SSL, and enter the domain controller port number.

f. Click the **Add** button and enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>The AD default domain name.</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>The AD default domain controller.</td>
</tr>
<tr>
<td>User Search Context (Base DN)</td>
<td>Enter the base distinguished name where to start searching for users.</td>
</tr>
<tr>
<td>Group Search Context (Base DN)</td>
<td>Enter the base distinguished name where to start searching for groups.</td>
</tr>
<tr>
<td>Priority</td>
<td>Select Primary or Secondary to set the priority.</td>
</tr>
</tbody>
</table>

   **Note:** CloudControl will always attempt to use the primary first, then failover to secondary if the first cannot be reached. The secondary domain controller will not be promoted to primary, and is only used until the domain controller marked as primary is available.

g. Click **Next**.
6. On the Rule Conversion page, map your CloudControl roles to AD groups.
   In CloudControl, rules are defined by their domain user group and assigned role. Any rules that are specifically mapped will have associated AD groups. All other CloudControl rules are created without specified values, which can be defined at a later date.
   - **Role**—The CloudControl role name.
   - **Domain Name**—The AD domain name. Select the desired domain from the drop-down list.
   - **Group Name**—The AD security group name. Enter the AD group name you wish to associate with the default role. This field uses auto-fill to complete the field entry. The name used in this field must be identical to the name found in AD.
     
     **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.

7. Click **Next**.

8. On the summary page, confirm the AD settings. Review the information to make sure the Domain Controllers, Rule Conversion, and Service Account settings are accurate.

9. Click **Finish** to convert CloudControl to Directory Service mode.

Once the conversion process is complete, you need to use your AD credentials to login to the CloudControl Management Console.

**Note:** Before you login to CloudControl with your AD credentials, confirm that you have manually added users to the proper CloudControl security groups in AD. See Default Roles and Permissions on page 182 for a list of available CloudControl roles, groups, and the corresponding permissions granted to group members when they log in.

---

# Updating the AD Service Account or Role-Group Mapping

1. Select **Configuration > Authentication**.

2. On the Root Domain tab on the Authentication Configuration page, click **Update**.

3. On the Configure Service Account page, update the domain name or service account information as necessary.

4. Click **Next**.

5. On the Active Directory Advanced Settings page, update the your global catalog or domain controllers as necessary.
   
   **Note:** If you selected Automated Discovery you cannot add a priority to the global catalog or domain controllers.

6. Click **Next**.

7. On the Role-Group Mapping page, update the group names as necessary.

8. Click **Finish** to close the Active Directory Conversion Wizard.
Using the Authentication Configuration Page

From the Authentication Configuration page you can view or update the Active Directory settings in CloudControl. It contains the following sections:

- Root Domain Tab below
- Configuration Types Tab below
- Global Catalogs Tab on the next page
- Domains Tab on the next page
- Service Account Tab on page 27
- Advanced Tab on page 27

Root Domain Tab

The Root Domain tab on the Authentication Configuration page displays the root domain for your Active Directory. To change the root domain, see Updating the AD Service Account or Role-Group Mapping on the previous page.

Configuration Types Tab

The Configuration Types tab contains the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Type</td>
<td>Select the <strong>Automated Discovery</strong> radio button and click <strong>Apply</strong> to change to automated discovery. CloudControl automatically reconfigures Active Directory settings. Select the <strong>Manual Configuration</strong> radio button and click <strong>Apply</strong> to change to manual configuration and manually enter the Active Directory settings information.</td>
</tr>
<tr>
<td>Directory Service Refresh</td>
<td>For Automated Discovery only, specify the time interval in minutes at which Active Directory settings will be re-discovered.</td>
</tr>
<tr>
<td>Refresh</td>
<td>For Automated Discovery only, click the <strong>Refresh</strong> button to manually refresh the Active Directory settings immediately.</td>
</tr>
</tbody>
</table>
Global Catalogs Tab

The Global Catalogs tab contains the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Catalogs</td>
<td>For Automated Discovery, you can only view the global catalogs. For Manual Configuration, you can update the global catalogs and change the priority.</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Check the SSL Enabled checkbox if your domain controller uses SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter or update the domain controller port.</td>
</tr>
</tbody>
</table>

To add a new global catalog in manual configuration:

1. Click Add in the Domain Controllers section.
2. In the Authentication Configuration dialog box, enter the global catalog.
3. Select the priority.
4. Click OK to close the dialog box.
5. Click Apply to save the changes.

Domains Tab

The Domains tab displays the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Domain</td>
<td>Displays the default domain name. For Automated Discovery, you can change the default domain using the drop-down menu. For manual configuration, you can change the default domain by typing in the Default Domain field.</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>Displays the domain controllers. This is read-only.</td>
</tr>
<tr>
<td>SSL Enabled</td>
<td>Check the SSL Enabled checkbox if your default domain uses SSL.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter or update the default domain port.</td>
</tr>
</tbody>
</table>

To add a new domain controller in manual configuration:

1. Click Add in the Domain Controllers section.
2. In the Authentication Configuration dialog box, enter the default domain name and domain controller.
3. Enter search values for the User Search Context (Base DN) and Group Search Context (Base DN). CloudControl uses the values provided in the search context fields as starting points to locate users and their groups in Active Directory. Once it locates the users and their group information, CloudControl builds the User-to-Group Map Cache and the Nested Group Map Cache.

You can specify search contexts such as DC (Domain Component), OU (Organizational Unit), and CN (Common Name), and their values.

For Automated Discovery, the search context fields are populated automatically using the Root Domain context as the default.

4. Select the priority.

5. Click OK to close the dialog box.

6. Click Apply to save the changes.

### Service Account Tab

On the Service Account tab, you can update the service account name and password.

We recommend that you do not modify the settings.

### Advanced Tab

The Advanced tab contains the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-to-Group Map Cache Timeout (minutes)</td>
<td>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.</td>
</tr>
<tr>
<td>Enable Nested Group Search</td>
<td>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.</td>
</tr>
<tr>
<td>Nested Group Map Cache Timeout (minutes)</td>
<td>If Enable Nested Group Search is enabled, this configures how long CloudControl will cache recursive group memberships, or 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. We recommend that you use the default value of 60 minutes.</td>
</tr>
</tbody>
</table>
### Authentication Modes

CloudControl uses Service Account to authenticate users against Active Directory. The authentication modes use different combinations of user credentials and provide different views of objects on the vCenter Server. For more information, see [Supported Authentication Modes](#) on page 220.

### Smart Card Authentication

To use smart card authentication, you must have the following:

- CloudControl must be in Directory Service mode.
- VMware SSO services must be installed and configured to run using an AD domain account, with the appropriate AD domain(s) as identity sources.
- VMware vCenter Server services must be installed and configured to run using an AD domain account instead of a local computer account.
- Configure the vCenter Server host to Use Pass through with HTCC Service Account authentication mode—see [Supported Authentication Modes](#) on page 220.

For details on VMware requirements, refer to the appropriate VMware vSphere documentation.

### Configuring the vCenter Server for Smart Card Mode in CloudControl

1. Open the Compliance > Hosts page.
2. Click the name of the vCenter Server host you want to configure for Smart Card authentication.
3. Open the Advanced tab.
4. Select the Use Pass through with CloudControl Service Account authentication mode.
Two-Factor Authentication

CloudControl two-factor authentication requires users to provide two forms of identification (a password/PIN and a token) to login. CloudControl supports the following two-factor authentication types:

- RSA SecurID
- RADIUS Server Authentication
- TACACS+ Authentication

(Note: OTP is not supported with TACACS+.)

Two-Factor Prerequisites

- Two-factor authentication requires CloudControl to be in Directory Service mode.
- The RSA SecurID, TACACS+, and RADIUS servers must be accessible to CloudControl.
  (Note: Provide CloudControl Node (eth0) IP as trusted sources in two-factor servers.)
- Standalone CloudControl—When CloudControl is configured in VIP, also add VIP as a trusted source and agent. When CloudControl is configured in VIP, the node IP is used as the Client IP in RSA. Add RSA_AGENT_HOST=<FQDN of NodeIP> to rsa-api.properties to ensure a successful authentication.
- HA Pair—When CloudControl is configured in HA mode with VIP, also add both Node (eth0) IPs and VIP as trusted sources.
- For RADIUS support, an Active Identity Server must be configured and accessible to CloudControl.

RSA SecurID

Configuring CloudControl to use RSA SecurID authentication requires the following:

- Agent Host Configuration below
- Generating an RSA Configuration File on the next page
- Configuring the Appliance for RSA SecurID on the next page
- Creating a New Pin on the next page

Agent Host Configuration

To facilitate communication between CloudControl and the RSA Authentication Manager or RSA SecurID Appliance, an Authentication Agent record must be added to the RSA Authentication Manager local database. The Authentication Agent record identifies CloudControl within its database and contains information about communication and encryption.
The following information is needed to create the Authentication Agent record:

- The CloudControl hostname
- The CloudControl management IP address

To create an Authentication Agent record:

1. In the RSA Security Console menu, select **Access > Authentication Agents > Add New**.
2. Enter the IP address of CloudControl.
3. Click the **Resolve Hostname** button to auto-generate the hostname.
4. Click the **Save** button to create your new Authentication Agent record.

### Generating an RSA Configuration File

Perform the following to generate the `sdconf.rec` file from the RSA Authentication Manager:

1. In the RSA Security Console select **Access > Authentication Agents > Generate Configuration File**.
2. Configure or confirm the **Agent Timeout** and **Retries** settings.
3. Click the **Generate Config File** button.
4. Download and extract the `sdconf.rec` file from the zip file.

### Configuring the Appliance for RSA SecurID

1. In the CloudControl Management Console, select **Configuration > Two-Factor**.
2. On the Two-Factor Configuration page, click the **RSA SecurID** tab.
   
   **Note:** The Enable SecurID checkbox is grayed out if the `sdconf.rec` file has never been added to CloudControl.
3. Click **Browse** and navigate to the `sdconf.rec` file that you generated from your RSA Authentication Manager.
4. Click **Apply** to upload the configuration file.
   
   A confirmation message appears if the configuration file successfully uploads.
5. Reload the page.
6. Check the **Enable SecurID** checkbox.
7. Click **Apply** to enable RSA SecurID.

### Creating a New Pin

Set up a new pin to use when you log into a CloudControl instance that uses RSA SecurID.
1. Start the CloudControl Management Console.

2. On the RSA SecurID login page, enter the following information and click Login:
   - **Username**—Enter your AD account username.
   - **RSA Passcode**—Enter the RSA SecurID token that was auto-generated from your RSA SecurID device.

3. Click Login.

4. On the RSA SecurID page, enter a new pin number and reenter it to confirm. You will use the new pin number when you log into CloudControl in the future.

5. Click OK.
   - A message displays indicating that the pin has been updated.

6. After the token code has changed, log in using your AD account username and your new RSA passcode.
   - **Note:** The RSA passcode is a concatenation of your new pin and a newly-generated RSA SecurID token. For example, if your pin is 1234, and your token is 56789, you would enter 123456789 for the RSA Passcode. The token you used when creating your pin is no longer valid.

Access to CloudControl via the vSphere Client, Web Client Server, SSH, or HTTP is supported using your RSA SecurID credentials.

Contact your RSA administrator if you need to change your RSA SecurID pin.

**RADIUS Authentication**

This authentication type supports any RADIUS server. A RADIUS server must be set up and be accessible to CloudControl before you can use this type of authentication.

**Configuring CloudControl for RADIUS Authentication**

1. Select **Configuration > Two-Factor**.

2. On the Two-Factor Configuration page, click the **RADIUS Server** tab.

3. Check the **Enable RADIUS Server Authentication** checkbox.
4. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RADIUS Authentication Server IP Address</td>
<td>Enter the IP address for the RADIUS authentication server.</td>
</tr>
<tr>
<td>RADIUS Authentication Server Port Number</td>
<td>Enter the port number for RADIUS authentication server messages.</td>
</tr>
<tr>
<td>RADIUS Accounting Port Number</td>
<td>Enter the port number for RADIUS accounting messages.</td>
</tr>
<tr>
<td>RADIUS Server Secret Message</td>
<td>Enter the secret message for the RADIUS server.</td>
</tr>
</tbody>
</table>

5. Select the **Authentication Mode**. This can be one of the following:
   - **PAP**—Password Authentication Protocol.
   - **CHAP**—Challenge-Handshake Authentication Protocol.

6. Click **Apply**.

7. Log out of CloudControl.

### Generating a one-time password

The following procedure describes how to generate a one-time password using the ActivIdentity Soft Token client. If you are not using the ActivIdentity client, refer to your RADIUS product documentation for information about generating a one-time password.

1. Open the ActivIdentity Soft Token client.
2. Enter your pin.
3. Click **OK**.
   - The Soft Token client generates a one time password.
4. Copy the password to the clipboard.
   - This one-time password is used as the password when you log in to CloudControl.

### Logging in to CloudControl with RADIUS Authentication

1. Start the CloudControl Management console.
2. On the CloudControl login page, enter your username.
3. Generate the ActivIdentity one-time password, and paste it in the Password field.
   - For more information, see Generating a one-time password above.
4. Click **Login**.
CloudControl authenticates the user against the RADIUS server.

**TACACS+ Authentication**

CloudControl supports TACACS+ authentication, which is an Authentication, Authorization and Accounting (AAA) protocol.

_Note: OTP is not supported with TACACS+._

1. Select **Configuration > Two-Factor**.
2. On the Two-Factor Configuration page, click the **TACACS+ Server** tab.
3. Check the **Enable TACACS+ Authentication Server** checkbox.
4. Enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TACACS+ Authentication Server IP Address</td>
<td>Enter the IP address for the RADIUS authentication server.</td>
</tr>
<tr>
<td>TACACS+ Authentication Server Port Number</td>
<td>Enter the port number for RADIUS authentication server messages.</td>
</tr>
<tr>
<td>TACACS+ Authentication Server Secret Message</td>
<td>Enter the secret message for the RADIUS server.</td>
</tr>
<tr>
<td>Test Account Username</td>
<td>Enter the username of the test account to be used to authenticate the TACACS+ server.</td>
</tr>
<tr>
<td>Test Account Password</td>
<td>Enter the password of the test account to be used to authenticate the TACACS+ server.</td>
</tr>
</tbody>
</table>

5. Select the **Authentication Mode**. This can be one of the following:
   - **CHAP**—Challenge-Handshake Authentication Protocol.
   - **PAP**—Password Authentication Protocol.
   - **ASCII**—Transmits the username and password in clear, unencrypted text.
6. Click **Apply**.

**Two-Factor Authentication Whitelist**

Beginning with HyTrust CloudControl version 5.4.2, you can create a whitelist for tools to be exempted from two-factor authentication. When added to a whitelist, your tools can connect to vCenter through CloudControl without being prompted for two-factor authentication.
Adding Users to a Two-Factor Authentication Whitelist

1. In the CloudControl Management Console, select Configuration > Two-Factor.
2. On the Two-Factor Configuration page, click the Whitelist tab.
3. Click the Add button.
4. Enter the username that you want to add in \textit{username@domain} format.
5. Click OK.

Removing Users from a Two-Factor Authentication Whitelist

1. In the CloudControl Management Console, select Configuration > Two-Factor.
2. On the Two-Factor Configuration page, click the Whitelist tab.
3. Check the checkbox for the username that you want to remove.
4. Click OK.
5. Click OK in the confirmation box.
Chapter 3. Managing Hosts

Managing hosts with CloudControl allows you to enforce access policies, configure and run compliance templates, and monitor general security posture of a virtual infrastructure.

Adding Hosts to CloudControl

To add a new host:

1. Select Compliance > Hosts.
2. On the Hosts page, click Add.
3. In the Add Host Wizard dialog box, select the type of host that you want to add and click Next.
   - **vCenter, vSphere Web Client Server, and VMware NSX**—Adds a vCenter Server host, a vSphere Web Client Server host, and NSX Manager.
   - **vSphere Web Client Server Only**—Adds only a Web Client Server host.
     *Note:* For vSphere 6.0 and above, you cannot add only a Web Client Server (WCS) host. You can either add WCS with a vCenter host, or select Other Hosts. CloudControl automatically protects WCS for each vCenter added.
   - **Other Hosts**—Select this to add a host of any other type, such as unmanaged ESXi, or an ESXi host newly added to a protected vCenter.
4. On the Host Login page, enter the following information:
   - The fully qualified hostname or IP address of the host.
   - The administrator User ID and Password for the host.
     *Note:* Passwords for hosts can contain either the left angle bracket (<) or the right angle bracket (>) characters, but not both.
5. Optionally, expand the Advanced Properties section to view the VI SDK, HTTP, and HTTPS port settings. We recommend that you maintain the default settings.

   Note: Ports to communicate with vSphere 6.0 components through the firewall are:
   - CloudControl <-> WCS - 443 instead of 9443.
   - 443 is the preferred port though 9443 continues to be valid.
   - CloudControl <-> PSC - 444.

6. Click Next.

   CloudControl attempts to automatically detect the host type. Supported host types are vCenter Server, ESXi, NSX and WCS.

7. On the Host Details page, enter the following and click Next.

   - Friendly Name—A unique name to identify the vCenter Server, or the specified ESXi host, in the list of CloudControl hosts.
     This does not have to be the same name as used in DNS. Spaces and special characters are allowed, but the name should not exceed 64 characters.
   - Description—A description for the host.
   - Protected—Select this checkbox to have CloudControl protect both the vCenter Server, and the ESXi hosts it manages. This choice is selected by default.

8. Click Next.

9. On the Published IP (PIP) page, enter the following and click Next.

   - Published Hostname/IP—The hostname/IP address to use to route all traffic to this host.
   - Published IP Mask—The subnet mask to use to route all traffic to this host.

10. If applicable, on the vSphere Web Client Server Configuration page enter the following and click Next.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The service account to be used for CloudControl. The same account must be used across all vCenter Servers connected to the Web Client Server. Important: If you plan to use the NSX proxy in CloudControl, this account must be the same as the Service Account used to map NSX with vCenter at the infrastructure level.</td>
</tr>
<tr>
<td>Password</td>
<td>The CloudControl Service Account password.</td>
</tr>
<tr>
<td>Https Service Port</td>
<td>The Web Client Server HTTPS port number.</td>
</tr>
<tr>
<td>Published vSphere Web Client Server Hostname/IP</td>
<td>The published hostname/IP address for the Web Client Server.</td>
</tr>
<tr>
<td>Published Netmask</td>
<td>The published subnet mask for the Web Client Server.</td>
</tr>
</tbody>
</table>
11. On the Authentication Mode Configuration page, enter the following and click **Next**.
   - **Use CloudControl Service Account (default)**—Select this to use the CloudControl Service Account for authentication when establishing sessions from CloudControl to vCenter Server. This is the default mode, and only one administrative account is required on vCenter Server.
   - **Use Pass through without CloudControl Service Account**—Select this to use the user’s account for authentication when establishing sessions from CloudControl to vCenter Server. In this mode, a vCenter Server account must be configured for each user.
   - **Use Pass through with CloudControl Service Account**—Select this to use the user’s account for initial authentication but use the CloudControl Service Account for all other operations. Select this mode if using Smart Card for authentication. Refer to the Smart Card Authentication section in the Administration Guide for HyTrust CloudControl for more information on Smart Card support.

12. On the Complete Host Add page, click **Finish**.

### Modifying Managed Hosts

To modify an CloudControl protected host:

1. Select **Compliance > Hosts**.
2. On the Hosts page, click on the host in the Hosts column that you want to modify.
3. On the Edit Host page make any changes, for example, adding Labels, enabling Root Password Vaulting, or adding the PIP.
4. Click **OK** to save the changes.

### Removing Managed Hosts

**Important:** If the host that is being removed manages other hosts, for example, vSphere Client, then all associated hosts will also be removed.

1. From the CloudControl Management Console, select **Compliance > Hosts**.
2. On the Hosts page, select the checkbox next to the host(s) that you want to remove.
3. Click **Remove**.

### Global Published IP Address

Beginning with HyTrust CloudControl release 5.5, you can now use a Global published IP (Global PIP) instead of assigning a dedicated published IP (PIP) to each of your ESXi hosts protected by CloudControl. With Global PIP, instead of individual IP addresses, one IP address is created for all of your ESXi hosts. Once added to CloudControl, the hosts are automatically assigned four ports to distinguish them from other hosts. The ports assigned are used for the following:

- HTTP traffic
- HTTPS traffic
Enabling or Disabling Global PIP

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 at any time. Once Global PIP is enabled you must manually choose to select Global PIP for each ESXi host. You can update one or more hosts at the same time. However, you cannot disable Global PIP if any hosts are using the Global PIP. All hosts protected with Global PIP should either be removed, or edited to use either a dedicated PIP or no PIP. Hosts will remain protected, whether or not they have a dedicated PIP.

**Important:** You cannot use the VMware Remote Console (VMRC) to launch ESXi hosts with a Global PIP. Use the web browser instead.

### Enabling or Disabling Global PIP

#### Enable Global PIP

You can enable Global PIP during installation, when you add an ESXi host, or at any time on the Network Configuration page.

1. Select **Configuration > Network Configuration**.
2. On the Network Configuration page, in the ESXi Global Published IP section, check the **Enable ESXi Global PIP** checkbox.
3. Enter the IP address that you want to use for the Global PIP.
4. Click **Apply**.

#### Disable Global PIP

1. Select **Configuration > Network Configuration**.
2. On the Network Configuration page, in the ESXi Global Published IP section, uncheck the **Enable ESXi Global PIP** checkbox.
3. Click **Apply**.

### Adding a Global PIP to a Single Host

1. Select **Compliance > Hosts**.
2. On the Hosts page, select the ESXi host that you want to configure.
3. On the Edit Host page, click the Published IP tab.
4. Check the **Use ESXi Global Published IP** checkbox.
5. Click **OK**.
Adding a Global PIP to Multiple Hosts

1. Select Compliance > Hosts.
2. On the Hosts page, check the checkbox for each ESXi host that you want to configure.
3. On the Edit Host (Multiple Hosts) page, click the Published IP tab.
4. Check the Use ESXi Global Published IP checkbox.
5. Click OK in the confirmation box.
6. Click OK.

All selected hosts are now using a Global PIP.

Viewing ESXi Host Connectivity Information when using Global PIP

1. Open a web browser and enter the following URL: https://<Global-PIP>/
   Where <Global-PIP> is the IP address that you entered for your ESXi Global PIP.
   Note: Only secure HTTPS sessions are supported. All HTTP connections are redirected to HTTPS.
2. On the login screen, enter your CloudControl username and password and click Login.
3. On the ESXi Host Connectivity Information page, click the Expand All icon to expand the list.
4. Select the ESXi host that you want to view. The page displays the following:
   - Host Name—The name of the ESXi host that you selected.
   - URL—The link to log in to the ESXi host. The URL uses the following format: https://<Global-PIP>:<HTTPS-port>.
   - IP—The Global PIP.
   - HTTPS port—The HTTPS port used to log in to the ESXi host.
   - HTTP port—The HTTP port used to log in to the ESXi host.
   - SSH port—The SSH port used to log in to the ESXi host.

Connecting to an Individual Host Through Global PIP

CloudControl provides the following ways of connecting to one of your individual protected hosts through Global PIP:

- Accessing the Host using the Web Browser on the next page
- Accessing the Host Directly using SSH on the next page
- Accessing the Host using the CLI Host Menu on the next page
Connecting to an Individual Host Through Global PIP

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.

1. Retrieve the Global PIP and the HTTPS port for the ESXi host to which you want to connect. See Viewing ESXi Host Connectivity Information when using 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 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 ESXi Host Connectivity Information when using 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 number, you can establish an SSH connection and then use the command line menu to navigate to the desired host. You must have the system.anonymous 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.
Global PIP API

Retrieves all Global PIP connectivity information in a JSON object.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostmenu

Request Method

GET

Request Header

Auth-Token

2D9F8F8F32BB860B3BE74FF0CE36AE88

Accept

application/json

cURL Example


Success Response

Response Header

Date: Tue, 11 Jun 2019 08:28:50 GMT
Server: Apache-Coyote/1.1
X-FRAME-OPTIONS: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
Content-Type: application/json
Set-Cookie: JSESSIONID=9F7B8497EB60BEA5F118EFD368642422; Path=/asc/; Secure;HttpOnly
Transfer-Encoding: chunked

Response Body

{"status":true,"data": [{"id": "com.hytrust.root", "type": "Appliance Root", "children": []}, {"id": "2ddaf157-02c7-49d1-9500-549c01b7c1", "text": "vcsa-14.test.hytrust.com", "type": "VirtualCenter", "children": [{"id": "24b5c614-21f8-4792-83db-62a59507f264", "text": "DC-2", "children": [{"id": "56db8776-a0b0-4c19-8bca-eb4e1630fa", "text": "esxi-17.test.hytrust.com", "type": "HostSystem", "publishedIp": "10.222.73.77", "httpPort": 80, "httpsPort": 443, "sshPort": 2218}]
}]}]}
Configuring Web Client Server Operations

By default, unknown Web Client Server (WCS) operations are denied as they are not recognized by CloudControl. If you want to allow unknown WCS operations, they are permitted for all users on that particular WCS. Otherwise unknown operations on that WCS are permitted only for users with the Asc.UnknownOp privilege.

To permit unknown WCS operations:

1. Select Compliance > Hosts.
2. Select the WCS host where you want to allow unknown WCS operations.
3. On the Edit Host page, click the Advanced tab.
4. Check the Permit Unknown WCS Operations checkbox.
5. Click OK.

Trust Attestation Service Configuration

Trust Attestation Service (TAS) utilizes Intel® Trusted Execution Technology (Intel® TXT) to establish comprehensive hardware based trust on managed ESXi hosts.

A feature of the Intel® Xeon® processor, Intel TXT establishes a root of trust through measurements when the hardware and pre-launch software components are in a known good state. Administrators can use the result to set policies for sensitive data and workload placement onto groups of servers known as trusted compute pools.

Note: TAS requirements are listed in the System Requirements section in the Installation Guide for HyTrust CloudControl.
Configuring TAS

Before You Begin

Ensure that all of the TAS system requirements have been met. See the System Requirements section in the Installation Guide for HyTrust CloudControl.

Procedure

1. Log in to CloudControl via SSH.
2. Enter the following command to run the TAS setup:
   ```bash
   asc tas -s
   ```
   - Use FQDNs when adding hosts to CloudControl, if the hosts were added to vCenter Server using FQDNs.
   - Use IP Addresses when adding hosts to CloudControl, if the hosts were added to vCenter Server using IP Addresses.
   - Configure and enable an NTP Server for CloudControl.
     Note: We recommend using the same NTP server for CloudControl, vCenter, and all hosts in the system. If your NTP server is not set up, minimize the time difference between these systems to less than 5 minutes.

CloudControl can establish platform trust by requesting the TAS server to verify the correct bootable image of hypervisor with the help of Intel TXT on the host platform. Platform trust can also be re-verified at any time and the policies enforced by CloudControl can automatically adjust based on the individual trust status of each host.

For a full list of `asc tas` commands and their functions, see CloudControl Command Line Interface (CLI) on page 192.

Enabling a Good Known Host

Enabling a Good Known Host indicates that you know and trust the host, and allows CloudControl to use this host when allocating and testing other hosts with the same BIOS and hypervisor versions for trust.

Before You Begin

Ensure that TAS has been configured. See Configuring TAS above.

Procedure

1. Select Compliance > Hosts.
2. On the Hosts page, select the host that you want to modify and click Edit.
3. On the Edit Host page, click the Trust Attestation tab.
   Note: The Trust Attestation tab appears only after the TAS server has been setup and configured.
4. Check the Good Known Host (BIOS and VMM) checkbox.
   Important: Do not enable more than one Good Known Host with the same BIOS and hypervisor versions.
Disabling a Good Known Host

1. Select Compliance > Host.
2. On the Hosts page, select the host that you want to modify and click Edit.
3. On the Edit Host page, click the Trust Attestation tab.
4. Clear the Good Known Host (BIOS and VMM) checkbox.
   This revokes the TAS status for all hosts with the same BIOS and hypervisor versions.
5. Click OK in the pop-up window to confirm.
6. Click OK.

Verify and Update Host Trust

CloudControl enables you to verify and update the host trust by performing a complete attestation cycle, consisting of registering, creating whitelists, and updating Trust status. You can use one of the following methods.

- Manually select the hosts and click the Update Trust button.
- Enable the Refresh Trust Status scheduled event. For more information, see Scheduled Events on page 51.

   **Important:** Because CloudControl v 5.6 requires all Good Known Hosts to be verified by both BIOS and VMM, you must run the Refresh Trust Status scheduled event when upgrading to ensure that all qualifications are met.

   Good Known Hosts from previous versions will not display the Good Known Host icon until verified.

CloudControl automatically detects and updates the Trust Status of all TPM-enabled Intel TXT ESXi hosts on boot.

**Important:** Do not check the Automatically Update Good Known Values (BIOS and VMM upgrades) checkbox. This is only to be used during upgrades to import new values from the upgraded host. This is insecure, and we recommend that you leave it disabled unless it is being used for an upgrade. Contact support@hytrust.com for more information.

5. Optionally click the Trusted button for the View Host Trust Attestation Report.

   A dump file of the Trust report opens in a separate page. The file displays both a short report and the event logs.

6. Click OK to confirm your selection.

7. Click OK.

   The Good Known Host icon (('/') displays next to the host name. You can mouse-over the icon to see the host BIOS and hypervisor versions.

Once a Good Known Host is enabled, all other hosts under the same vCenter with the same BIOS and hypervisor versions are automatically marked as trusted. A Good Known Host must be enabled for each different BIOS and hypervisor version of your hosts.

**Important:** If you apply ESXi patches, or otherwise change the signature of the Good Known Host, you may have to reboot the host two or more times before all changes to the OS are finalized. In this situation, the trust values need to be taken and trust reestablished after all reboots have finished. For more information, please contact support@hytrust.com.
To manually verify and update host trust:

1. Select Compliance > Hosts.
2. On the Hosts page, select the Intel TXT ESXi host(s) that you want to validate and click Update Trust.

   Trusted hosts display the Trusted Host icon, and the TRUSTED policy label appears in the resource tree for the host.

   If a host is not trusted, the Untrusted Host icon is displayed.

**Host Icons used in CloudControl**

The following icons are used to describe hosts in CloudControl:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Blocked icon" /></td>
<td>Blocked icon. Additional configuration is required before CloudControl can assess or protect these hosts.</td>
</tr>
<tr>
<td><img src="image" alt="Gold shield" /></td>
<td>Gold shield. The host is fully protected by CloudControl.</td>
</tr>
<tr>
<td><img src="image" alt="Silver shield" /></td>
<td>Silver shield. ESXi hosts that do not have a PIP assigned. CloudControl controls all future management communications based on the configured access and segmentation policies.</td>
</tr>
<tr>
<td><img src="image" alt="Non-approved host with PIP" /></td>
<td>Non-approved host with PIP. The host is not on the approved host list set by your administrators.</td>
</tr>
<tr>
<td><img src="image" alt="Non-approved host without PIP" /></td>
<td>Non-approved host without a PIP. The host is not on the approved host list set by your administrators.</td>
</tr>
<tr>
<td><img src="image" alt="Trusted Host" /></td>
<td>Trusted Host.</td>
</tr>
<tr>
<td><img src="image" alt="Good Known Host" /></td>
<td>Good Known Host.</td>
</tr>
<tr>
<td><img src="image" alt="Untrusted Host" /></td>
<td>Untrusted Host.</td>
</tr>
</tbody>
</table>

**Approved Hosts**

CloudControl allows administrators to manage the Approved Host list. If an unapproved host is selected CloudControl delivers a warning that the host is unapproved.

Select Configuration > Approved Hosts to see the current list of approved hosts.

The Approved Hosts page displays the following:
• **Host Version**—The host version.

• **Patch Level**—The approved host patch level.

• **Host Type**—The host type.

CloudControl-protected approved hosts are indicated with 🌟 on the Compliance > Hosts and Policy > Resources pages, while non-approved hosts are indicated with ⚒.

### Adding Approved Hosts

1. Select Configuration > Approved Hosts.
2. On the Approved Hosts page, click Add.
3. Specify the new approved host type, host version, and patch level.
   
   **Important:** The patch level must match exactly what appears in the list of hosts. You may want to copy and paste the patch level from the Compliance > Hosts page to ensure that it is entered correctly.
4. Click OK.

### Removing Approved Hosts

1. Select Configuration > Approved Hosts.
2. On the Approved Hosts page, select the host or hosts that you want to remove, and click Remove.
3. Click OK to verify.

### Using Filters to View Managed Hosts

You can search through your protected hosts by using the filters on the Hosts page.

1. Select Compliance > Hosts.
2. On the Hosts page, use the Type drop-down to filter what you want to view.
Chapter 4. Configuring Security Options

Static Routes .................................................................................................................................................. 47
Root Password Vaulting ................................................................................................................................. 48
Configuring Monitor Mode ............................................................................................................................ 50
Scheduled Events ........................................................................................................................................ 51
Monitoring with SMTP and SNMP in CloudControl ...................................................................................... 54
Managing Certificates ................................................................................................................................ 55
Changing Password Requirements for ascadminuser .................................................................................... 61
Session Timeouts ......................................................................................................................................... 62
Command Line Prompts ............................................................................................................................... 62
SSH Banners ............................................................................................................................................... 64

Static Routes

You may need to set a static route to CloudControl if you are trying to access the CloudControl Management Console from a client that is not on the same subnet as CloudControl.

1. Select Configuration > Static Routes.
   The Static Routes page allows you to view any existing static routes and add new static routes.

2. Click Add.

3. On the Add Static Route page, enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Address</td>
<td>The IP address of the client.</td>
</tr>
<tr>
<td>Mask</td>
<td>The subnet mask of the client.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The gateway IP address where the client is located.</td>
</tr>
<tr>
<td>Device</td>
<td>The interface to route the traffic through. Enter 1 to route traffic through the Eth0 interface.</td>
</tr>
</tbody>
</table>

4. Click OK.
Root Password Vaulting

Root Password Vaulting is a feature that allows CloudControl to manage the root password of individual hosts. For each host, the user can select the 'Root Password Vaulting' checkbox on the General tab when adding or editing hosts—see Modifying Managed Hosts on page 37. CloudControl will create a new secure root password on the selected host and store it in a password ‘vault’. CloudControl automatically rotates or updates the root password on the host on a regular basis (as specified by the Host Password Update scheduled event—see Scheduled Events on page 51).

An Enterprise or appropriate evaluation license is required to implement this feature.

CloudControl only supports Root Password Vaulting for ESXi 4.1 update 1 or later hosts. For unsupported ESXi hosts, if the host becomes inaccessible (as determined by assessment or some other host operation that repeatedly caused a connection or credential error), the recommended user action is to remove the host and add it back to CloudControl.

**Important:** We recommend that you export all log files to a SIEM or syslog tool to insure the RPV logs and hashes are exported and not stored in CloudControl.

If CloudControl becomes unavailable contact HyTrust Support.

Privileges

The following privileges are associated with Root Password Vaulting:

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asc.RootPasswordVaulting.Administration</td>
<td>Allocated to the ASC_ESXMAadmin and ASC_SuperAdmin Roles. Those Roles can configure Recovery Password and enable or disable RPV.</td>
</tr>
<tr>
<td>Asc.RootPasswordVaulting.PasswordRequest</td>
<td>Allocated to the ASC_VIAdmin, ASC_ESXMAadmin and ASC_SuperAdmin Roles. These Roles can issue passwords or cancel passwords for RPV enabled ESXi hosts.</td>
</tr>
</tbody>
</table>

Prerequisites

Perform the following before enabling Root Password Vaulting:

- Set the CloudControl Recovery Passcode. The recovery passcode is used to provide an emergency mechanism to recover root passwords if CloudControl is not available.

- We highly recommend that you configure an external syslog server. In the unlikely event that CloudControl becomes unavailable, accessing the CloudControl log file from the external syslog server is the only mechanism for recovering a root password.

Set Recovery Passcode

When the passcode is changed, the new passcode immediately overrides the current passcode and the root account credentials in the log file are re-encrypted. The root password is rotated on hosts with Root Password Vaulting enabled.

1. Select **Configuration > Root Password Vaulting**.
2. On the Set the Recovery Passcode page, enter a Recovery Passcode, and retype to confirm.

3. Click **Apply**.

The recovery passcode is now set and you can enable Root Password Vaulting on your CloudControl managed hosts.

### Enable Root Password Vaulting

*Note:* Root Password Vaulting can only be enabled for a host after it has been added and configured.

To enable root password vaulting:

1. Select **Compliance > Hosts** in the CloudControl Management Console.

2. Click on a host in the list.

3. Select the **Root Password Vaulting** checkbox on the **General** tab.
   
   *Note:* The **Root Password Vaulting** checkbox is visible only to the users who have the **Asc.RootPasswordVaulting.Administration** privilege.

4. Enter the root credentials of the selected host when prompted.

5. Click **OK** to save your settings.

Once you've enabled root password vaulting, a key icon (🔒) is displayed next to the hostname on the Hosts summary page.

### Request a Temporary Root Password

Once Root Password Vaulting is enabled for the host, an authorized user can request a temporary root password to access the host.

1. Select **Compliance > Hosts**.

2. On the Hosts page, select the checkbox next to the host for which you want to request a temporary root password.

3. Click **Issue Password**.

4. On the Issue a temporary password page, complete the following information:
   
   - **Reason**—The reason for the request, for example, enter the change management ticket, or other tracking information.
     
   - **Expiration**—The amount of time (in hours) before the temporary root password expires. The minimum expiration period is one hour and the maximum is 24 hours.

5. Click **Issue Password**.

   A User ID and Temporary Password appear on the screen and will also be added to the log.
   
   *Note:* You have two minutes to accept the temporary root password for the designated host.

6. Click **OK** to activate the temporary password.

7. At the prompt, enter the credentials you use to log into CloudControl and click **OK**.
The Hosts summary page appears if the password is issued successfully. Otherwise, the Issue Temporary Password page appears where you can request the password again after 2 minutes.

Once your host has a temporary root password it can be accessed out-of-band of CloudControl until the password expires. To test this, connect to the Service Console via IPKVM, IPMI, etc., and confirm that the temporary root credentials are valid. Also, if you have an additional IP address assigned to your host that CloudControl is not managing you can access your host from this second IP address.

When a temporary root password expires, CloudControl automatically replaces the temporary password with a new random secure password.

When Root Password Vaulting is enabled, CloudControl does not support SSH login using root credentials to a protected host using PIP. AD users can still login with an SSH session to the protected host through CloudControl.

**Cancel a Temporary Root Password**

To cancel a temporary root password:

1. Select Compliance > Hosts.
2. On the Hosts page, select the checkbox next to the desired host for which you want to cancel a temporary password.
3. Click Cancel Password.

When a cancel password request is made, CloudControl replaces the temporary password with a new random secure password.

In the unlikely event CloudControl becomes unavailable, contact HyTrust Support.

**Configuring Monitor Mode**

Monitor Mode is a special mode in which CloudControl grants permission for all vSphere Client operations, regardless of the deployed access policy. While in Monitor Mode, CloudControl still evaluates the deployed access policy and logs the event; however, the access policy is not enforced and the operation is permitted—see Log Viewer on page 130.

Monitor Mode is useful for observing usage patterns in the logs without having to modify the current vCenter Server deployments in a way that is noticeable to end-users.

When Monitor Mode is enabled, Secondary Approval is automatically disabled (if enabled).

By default, only users in the following roles can enable/disable Monitor Mode:

- ASC_SuperAdmin
- ASC_DCAdmin
- ASC_PolicyAdmin

The Asc.MonitorMode privilege allows a CloudControl user to enable or disable Monitor Mode.
Enabling Monitor Mode

Secondary Approval is disabled when enabling Monitor Mode.

2. On the Rules page, check the Monitor Only checkbox.
   A message appears indicating rules/policy will no longer be enforced and Secondary Approval will be disabled
3. Click OK.

Monitor Mode is now enabled, Secondary Approval is disabled, and the deployed access policy is no longer enforced.

When CloudControl is in Monitor Mode, the text Monitor Mode appears at the top of each page in the CloudControl Management Console.

Disabling Monitor Mode

To disable Monitor Mode:

2. On the Rules page, deselect the Monitor Only checkbox.
   A message appears indicating rules will now be enforced.
3. Click OK.

Monitor Mode is now disabled and the deployed access policy is now being enforced.

You can now re-enable Secondary Approval if desired. For more information, see Secondary Approval on page 109.

Scheduled Events

Scheduled events allow you to run a defined compliance security template on one or more hosts at a specific time or at a specific interval. When CloudControl executes a scheduled event with a security template, the security template with all of its individual sub-tests and operations will run on each assigned host.

Note: Scheduled Events are restricted by host type. If you assign an ESXi template to a scheduled event only ESXi hosts can be added to that event. For an auto deploy vCenter Server host, run a Scheduled Event using the last known template associated with the host to refresh and deploy the vCenter Server in CloudControl.

Select Compliance > Scheduled Events to view all CloudControl scheduled events.

By default, the following scheduled events are enabled:

- Directory Service Sync—Syncs CloudControl with the current Directory Service setup, and maps each user to their corresponding admin categories. This is used for the Admin Access Dashboard.
- Get Host IP address changes—Updates host IP address changes to all other protected hosts.
• **License Monitor SNMP Trap**—Allows the SNMP Traps for licensing to be run.

• **Purge Database**—Purges old data from the database. If the database disk space utilization exceeds the amount set in the Threshold for Full Vacuum (%) field on the Services page, it also runs a full vacuum to reclaim space. For more information, see *CloudControl Services* on page 146.

• **Refresh Auto Deploy Status**—Checks all protected vCenters to detect if they have enabled Auto Deploy, and if Auto Deploy service is running.

• **Refresh ELM Setup**—Discovers any newly added vCenters in ELM setup.

• **Refresh Patch Levels**—Updates the patch level for all hosts.

• **Trending Compliance**—Aggregates the number of compliant hosts for the Compliance Dashboard.

• **Trending RBAC Protection**—Handles trending the RBAC protection status for all known resources within CloudControl. This is used for the Protection Dashboard.

• **Update Hosts Passwords**—Updates the managed passwords for protected hosts.

By default, the following scheduled events are disabled:

• **Export assessment data**—Exports the assessment data to the *Assessments.csv* file.

• **Export asset data**—Exports the host and virtual machine data to the *Assets.csv* file.

• **Get vCenter events**—Updates the log with events from all protected vCenter Servers.

• **Inventory Refresh**—Updates the host policy to include resource changes resulting from a Distributed Resource Scheduler (DRS) activity.

• **Refresh Trust Status**—Updates the trust status for all hosts.

• **Refresh Host Socket Count**—Updates the socket count for all hosts.

• **Update Esxi Resource MOR**—Updates the ESXi-specific managed object reference for your vSphere resources in the CloudControl database.

**Adding a Scheduled Event**

1. Select **Compliance > Scheduled Events**.

2. On the Scheduled Events page, click **Add**.
3. On the Add Scheduled Event page, complete the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Enter the name of the scheduled event.</td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>Enter an optional description of the scheduled event.</td>
</tr>
<tr>
<td><strong>Start</strong></td>
<td>Enter the date and time to start the scheduled event. The default is the current date and time in CloudControl.</td>
</tr>
<tr>
<td><strong>Interval (Minutes)</strong></td>
<td>The amount of time in minutes between each run of this scheduled event. The valid range of values is 1–525600 (1 year).</td>
</tr>
<tr>
<td><strong>Compliance Type</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Assess—Determines if the values match the template or label.</td>
</tr>
<tr>
<td></td>
<td>• Remediate—Assesses and modifies values that do not match the template or label.</td>
</tr>
<tr>
<td><strong>Compliance Mode</strong></td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Label</td>
</tr>
<tr>
<td></td>
<td>• Template</td>
</tr>
<tr>
<td><strong>Label</strong></td>
<td>If you selected Label, choose the label that you want to use for the scheduled event.</td>
</tr>
<tr>
<td><strong>Template</strong></td>
<td>If you selected Template, choose the template that you want to use for the scheduled event. Note: If you select Template, you can also select specific hosts on which to run the scheduled event. 1. Click Add in the Hosts section. 2. On the Add Host to Scheduled Event past, select the hosts on which you want to run the scheduled event. Note: Only hosts that match the selected template type will be displayed. 3. Select the hosts to run this scheduled event on. (Only hosts matching the selected template type appear in the list.) 4. Click OK.</td>
</tr>
<tr>
<td><strong>Enabled</strong></td>
<td>Check the Enabled checkbox if you want the scheduled event to run. If the checkbox is not selected, the scheduled event will remain in your list of scheduled events, but will not run.</td>
</tr>
</tbody>
</table>

4. Click OK to save the scheduled event.

**Editing a Scheduled Event**

You can enable or disable a scheduled event as well as change its start time and interval.
Deleting a Scheduled Event

Deleting a scheduled event permanently removes it. If you think you might use the event at a later time, you should disable it instead.

1. Select **Compliance > Scheduled Events**.
2. Check the checkbox next to the scheduled event or events that you want to delete.
3. Click **Delete**.
4. Click **OK** in the confirmation box.

Monitoring with SMTP and SNMP in CloudControl

You can configure CloudControl to notify an administrator if a service or resource becomes unavailable. We recommend that you configure monitoring services, especially when using High Availability (HA).

**Note:** SMTP notifications and SNMP monitoring operate the same as on Linux-based systems.

You may receive the following notifications:

<table>
<thead>
<tr>
<th>Message</th>
<th>ID</th>
<th>SNMP OID</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor Transition to Disabled</td>
<td>MON0000</td>
<td>1.3.6.1.4.1.33095.0.1100</td>
<td>The appliance indicates that a monitored service is now disabled.</td>
</tr>
<tr>
<td>Monitor Transition to Healthy</td>
<td>MON0001</td>
<td>1.3.6.1.4.1.33095.0.1101</td>
<td>The appliance indicates a service or resource has returned to normal operation.</td>
</tr>
<tr>
<td>Monitor Transition to Warning</td>
<td>MON0002</td>
<td>1.3.6.1.4.1.33095.0.1102</td>
<td>The appliance indicates a service or resource is in a warning state.</td>
</tr>
<tr>
<td>Monitor Transition to Failure</td>
<td>MON0003</td>
<td>1.3.6.1.4.1.33095.0.1103</td>
<td>The appliance indicates a service or resource issue is causing service interruption.</td>
</tr>
</tbody>
</table>
Configuring Monitoring and Notifications

To enable and configure SMTP notifications and SNMP monitoring:

1. Select Configuration > Monitoring.

2. On the Monitoring page, in the SMTP Notifications area, complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SMTP</td>
<td>Check the checkbox to enable SMTP notifications in CloudControl.</td>
</tr>
<tr>
<td>SMTP Host</td>
<td>Enter the SMTP hostname.</td>
</tr>
<tr>
<td>Enable Monitoring</td>
<td>Check the checkbox to enable SNMP monitoring in CloudControl.</td>
</tr>
<tr>
<td>Email Address (FROM)</td>
<td>Enter the email address that you want to appear in the From field when you receive notifications.</td>
</tr>
<tr>
<td>Email Address (TO)</td>
<td>Enter the email address where you want to send notifications.</td>
</tr>
</tbody>
</table>

3. In the SNMP Service area, complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SNMP</td>
<td>Check the checkbox to enable SNMP monitoring in CloudControl.</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>Enter the FQDN or IP address of the SNMP server.</td>
</tr>
<tr>
<td>SNMP Community String</td>
<td>Enter the community string required to access to the SNMP server. The default string is 'public'. Note: SNMP Community strings are used only by devices which support the SNMPv1 and SNMPv2c protocol.</td>
</tr>
</tbody>
</table>

Important: Please use the Node IP address on the management network interface for SNMP (see Configuring the Management Interface in the Installation Guide for HyTrust CloudControl). Do not use the virtual management IP address (VIP). We recommend that you allocate port 161 for SNMP GET and port 162 for SNMP SEND.

See SNMP Trap Alerts on page 305 to view the CloudControl traps.

4. Click Apply.

Managing Certificates

Note: For the CLI commands on managing certificates, see asc certs on page 196.

About Certificates

CloudControl supports the following types of certificates:

Note: All certificates must be in PEM (Base 64) format.
• **Services**
  - Rsyslog—Used only for encrypted syslog.
  - Single Sign On (Encryption)—Used to encrypt messages between CloudControl and the PSC. This is reserved for future use as currently vSphere does not require encrypted messages.
  - Single Sign On (Signing)—Used to sign the SAML requests which CloudControl sends to the PSC. The PSC then uses that certificate to verify that requests are from CloudControl. The SSO certificates are included in the metadata that we export to vSphere.
  - Web Application—Used to communicate with the CloudControl GUI and as a SOAP/PIP proxy.

For each service, you can generate a self-signed certificate, generate a certificate signing request (CSR), and install a signed certificate.

• **Certificate Authorities**—Stores digital certificates verified by a CA and certificates of trusted CAs.
  
  **Note:** When protecting NSX Manager, certificates for all NSX Manager appliances must be imported as certificate authorities into CloudControl.

• **Autoimport Certificates**—Displays a list of the CloudControl-protected vCenter and PSC certificates.

You must restart CloudControl before any new certificates are used. For more information, see Rebooting CloudControl on page 148.

You can see the status of your certificates on the Appliance Health page. If your certificates have expired, you need to replace them.

### Generating a Certificate Signing Request

To generate a Certificate Signing Request (CSR):

1. Select **Configuration > Certificates**.

2. Click the Services tab, and click the service that you want to use:
   - Single Sign On (Encryption)
   - Single Sign On (Signing)
   - Web Application
   - Rsyslog (used for syslog encryption only)

3. On the Certificate Details page for your selection, click **Generate CSR**.
4. Update the following properties in the Certificate Subject Field Configuration section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Displays the service that you selected.</td>
</tr>
<tr>
<td>Common Name</td>
<td>The FQDN used for DNS lookups.</td>
</tr>
<tr>
<td>Locality</td>
<td>Optional. The city.</td>
</tr>
<tr>
<td>State</td>
<td>Optional. For US and Canadian countries, enter the full state or province name. Do not abbreviate.</td>
</tr>
<tr>
<td>Country</td>
<td>The 2-character ISO format country code.</td>
</tr>
<tr>
<td>Organization</td>
<td>Optional. The company name.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Optional. The section name in the company.</td>
</tr>
</tbody>
</table>

5. If you selected Web Application, you can also update the Subject Alternative Name Configuration section:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Automatically Detected DNS Names</td>
<td>If the checkbox is checked, the list of detected names is displayed underneath. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
<tr>
<td>Include Automatically Detected IP Addresses</td>
<td>If the checkbox is checked, the list of detected IP addresses is displayed underneath. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
<tr>
<td>Include Additional DNS Names and IP Addresses</td>
<td>If the checkbox is checked, you can enter your own values in the Additional Names and IP Addresses field. The limit is 16 comma-separated DNS names or IP addresses. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
</tbody>
</table>

For example:

![Subject Alternative Name Configuration](image)

6. Click **OK**.

Once the CSR is generated, you can copy it into an email and submit it to a Certificate Authority (CA) to have it issue a certificate. You can install the signed certificate after you receive it from your CA.
Generating a Self-Signed Certificate

Because the Web Application certificate is required to communicate with the CloudControl GUI, CloudControl immediately restarts when you generate a Web Application certificate.

For Single Sign On, generating the certificate loads the certificate and restarts the certificate service, but does not restart CloudControl. You must manually restart CloudControl to use the certificate.

1. Select **Configuration > Certificates**.

2. Click the **Services** tab, and click the service that you want to use:
   - Single Sign On (Encryption)
   - Single Sign On (Signing)
   - Web Application

3. On the Certificate Details page for your selection, click **Generate Self-Signed**.

4. Update the following properties in the Certificate Subject Field Configuration section:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Displays the service that you selected.</td>
</tr>
<tr>
<td>Common Name</td>
<td>The FQDN used for DNS lookups.</td>
</tr>
<tr>
<td>Locality</td>
<td>Optional. The city</td>
</tr>
<tr>
<td>State</td>
<td>Optional. For US and Canadian countries, enter the full state or province name. Do not abbreviate.</td>
</tr>
<tr>
<td>Country</td>
<td>The 2-character ISO format country code.</td>
</tr>
<tr>
<td>Organization</td>
<td>Optional. The company name.</td>
</tr>
<tr>
<td>Organization Unit</td>
<td>Optional. The section name in the company.</td>
</tr>
</tbody>
</table>
5. If you selected Web Application, you can also update the Subject Alternative Name Configuration section:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include Automatically Detected DNS Names</td>
<td>If the checkbox is checked, the list of detected names is displayed underneath. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
<tr>
<td>Include Automatically Detected IP Addresses</td>
<td>If the checkbox is checked, the list of detected IP addresses is displayed underneath. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
<tr>
<td>Include Additional DNS Names and IP Addresses</td>
<td>If the checkbox is checked, you can enter your own values in the Additional Names and IP Addresses field. The limit is 16 comma-separated DNS names or IP addresses. Clear the checkbox if you do not want those values included in the certificate.</td>
</tr>
</tbody>
</table>

For example:

```
  Subject Alternative Name Configuration
  Include Automatically Detected DNS Names
    Automatically Detected DNS Names: test1.example.com
  Include Automatically Detected IP Addresses
    Automatically Detected IP Addresses: 10.222.1.110
  Include Additional DNS Names and IP Addresses
    Additional DNS Names and IP Addresses: test2.example.com, 10.222.1.111, 10.222.1.112
```

6. Click OK.

**Installing a Signed Certificate**

To install a signed certificate you will need the certificate, the CA for that certificate, and an RSA private key.

- For CSRs generated within CloudControl, the CloudControl private key is automatically used.
- For external certificates, you will need to supply the private key for that certificate.

**Note:** CloudControl immediately restarts when you install a Web Application certificate. You may need to refresh your browser.
1. Select **Configuration > Certificates**.
2. Click the **Services** tab, and click the service that you want to use:
   - Single Sign On (Encryption)
   - Single Sign On (Signing)
   - Web Application
   - Rsyslog
3. Click **Install**.
4. On the Install Certificate page for the service that you selected, choose one of the following:
   a. Click the **Enter Text** tab.
   b. Paste the contents of your certificate, the CA for that certificate (and, if applicable, the intermediate CA), and its RSA private key into the window.
   c. Click **OK**.

   OR

   a. Click the **Import** tab.
   b. Upload a single file that contains the certificate, the CA for that certificate (and, if applicable, the intermediate CA), and its RSA private key.
   c. Click **OK**.

---

**Installing a Third-Party Root Certificate**

You can install a root certificate from any third-party Certificate Authority (public or private) not already pre-installed in CloudControl.

1. Select **Configuration > Certificates**.
2. Click the **Certificate Authorities** tab.
3. Click the **Install** button.
4. Click **Browse** to select a CA certificate file in PEM format to upload.
5. Click **OK**.

---

**Installing Autoimport Certificates**

The Autoimport Certificates tab displays all certificates associated with the vCenter or PSC of your protected hosts that have not been installed. After you install, the certificates are displayed on the Certificate Authority page.

**Note:** You can only install vCenter or PSC certificates from the Autoimport Certificates tab, not ESXi host certificates. To install ESXi host certificates use the **asc certs** command. For more information, see **asc certs** on page 196.
1. Select **Configuration > Certificates**.
2. Click the **Autoimport Certificates** tab.
3. Select the certificate or certificates that you want to install.
4. Click the **Install** button.

## Changing Password Requirements for ascadminuser

The local CloudControl administrator account (ascadminuser) password complexity is based on the default settings built into the CloudControl operating system (CentOS). You can enhance these default settings if your environment requires additional password complexity.

1. Log in to the CloudControl Management Console as the ascadminuser.
2. Select **Configuration > Password Requirements**.
3. On the Password Requirements page, update the following fields as necessary:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Length</td>
<td>Set the minimum password length. The default is 8 characters.</td>
</tr>
<tr>
<td>Minimum Uppercase</td>
<td>Set the minimum number of required uppercase characters.</td>
</tr>
<tr>
<td>Minimum Lowercase</td>
<td>Set the minimum number of required lowercase characters.</td>
</tr>
<tr>
<td>Minimum Digits</td>
<td>Set the minimum number of required numeric digits (0-9).</td>
</tr>
<tr>
<td>Minimum Non-Alphanumeric</td>
<td>Set the minimum number of required special characters. You cannot use spaces.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of passwords before reuse</td>
<td>Set the number of passwords stored before a user can use the same password again.</td>
</tr>
<tr>
<td>Maximum number of login attempts per connection</td>
<td>Set the maximum number of failed login attempts before the account is locked.</td>
</tr>
<tr>
<td>Maximum number of password change attempts</td>
<td>Set the number of times a user can attempt to change a password without meeting the password requirements before the account is locked.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.

**Important:** After changing password requirements, you must change your ascadminuser password to meet the new requirements.
Changing the ascadminuser Password

To change the ascadminuser password:

1. Login to CloudControl from the Virtual Machine Console Window within vCenter Server or via SSH using your ascadminuser credentials.
2. From the command prompt, type: `passwd` to change your password.
3. Enter your new ascadminuser password. The new password must conform to the newly defined password requirements.

Session Timeouts

CloudControl allows you to enforce session timeouts for both CloudControl GUI and SSH sessions. It is a compliance requirement to initiate an information system timeout after 15 minutes of no activity. However, you can configure the CloudControl Web and SSH session timeouts per your requirements.

1. Select Configure > Session Timeout Interval.
2. Enter the values for CloudControl Admin Web Session Timeout and SSH Session Timeout in minutes.
3. Click Apply.

Command Line Prompts

The CloudControl command line shows the configuration state of hosts as the command prompt.

The table below lists the CloudControl command prompts that are displayed at various host configuration states:

<table>
<thead>
<tr>
<th>CloudControl Command Prompts for Host Configuration States</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td></td>
</tr>
<tr>
<td>Unconfigured</td>
<td>A newly deployed unconfigured CloudControl instance.</td>
</tr>
<tr>
<td>Standalone</td>
<td>A CloudControl instance running as a single node.</td>
</tr>
<tr>
<td>Primary</td>
<td>The primary CloudControl instance in an HA pair</td>
</tr>
<tr>
<td>Secondary</td>
<td>The secondary CloudControl instance in an HA pair</td>
</tr>
<tr>
<td>Disbanded</td>
<td>The secondary system in a HA pair, which is currently disband</td>
</tr>
<tr>
<td>Failed</td>
<td>A failed primary</td>
</tr>
<tr>
<td>Unknown</td>
<td>Unidentified configuration state</td>
</tr>
</tbody>
</table>

After HyTrust CloudControl is deployed, when you login to the CloudControl console using ascadminuser credentials, the command line shows as localhost: unconfigured.
After CloudControl is configured through GUI, you will see the command prompt displayed as standalone.

When High Availability is configured, the Primary and Secondary nodes show their HA states as the command prompt. When an HA pair is disbanded, the CloudControl nodes show standalone as the command prompt.
SSH Banners

A custom SSH banner in CloudControl warns users who are trying to access CloudControl or its protected resources via SSH against unauthorized use. The banner is displayed after a user enters the login details and before they are prompted to enter the password. You can add your own banner content by editing the /etc/ssh_banner file. The /etc/ssh_banner file is empty by default. You can edit it to add your own banner content.

Editing the SSH Banner File

1. Login to CloudControl via SSH using the ascadminuser credentials.
2. Edit the /etc/ssh_banner file using vi or any other editor. For example:
   ```
   vi /etc/ssh_banner
   ```
3. Enter the content of your custom SSH banner. For example:
   ```
   a Authorized users and uses only.
   Activity may be monitored and reported to law enforcement.
   [esc]
   ```
4. Save the file. For example:
   ```
   :wq
   ```
5. Reboot CloudControl.

You will see your custom banner displayed at each login before CloudControl prompts you to enter the password. For example:

```
login as: superadminuser
Authorized users and uses only.
Activity may be monitored and reported to law enforcement.
superadminuser@10.2.2.1's password:
```

The updated banner contents remain in the /etc/ssh_banner file even after CloudControl is upgraded.
Chapter 5. Compliance

Compliance Overview .......................................................... 65
Host Compliance .................................................................... 67
Compliance History ............................................................... 70
Host Configuration Templates ............................................... 70
vSphere Catalogs ................................................................. 73
NSX Catalogs ....................................................................... 74

Compliance Overview

To maintain host configurations in accordance with VMware Hardening Guides and compliance guidelines provided by various regulatory authorities, CloudControl offers four compliance processes:

- Assessment
- Remediation
- Rollback to Previous
- Revert to Initial

These compliance processes check, adjust or reset configuration values on hosts. These processes may be executed on a regular basis using scheduled events—see Scheduled Events on page 51.

Assessment

CloudControl facilitates compliance with various security guidelines by allowing the comparison of configuration values on a host against a template, which is a collection of host configuration parameters and their defined correct values.

Assessment is the process of running operations, or tests, on the host to compare the parameter value specified in the template with the actual value configured on the host. For any given operation, if the configured value is different from the value specified in the template, the assessment operation fails.

CloudControl presents assessment results in the form of a compliance percentage. The compliance percentage of an assessment is calculated by dividing the number of successful operations (i.e., the configured value matched the desired value in the template) by the total number of operations run against the host.
Remediation

Remediation modifies parameter values on the hosts based on the desired values defined in templates (in contrast to assessment, which evaluates but does not change values). A Remediation action will first run the assessment operation against the target host. If the assessment operation fails, CloudControl will modify the host parameter value(s) to match the value(s) defined in the template.

The remediation process tries to fix the parameters that are non-compliant based on the operations defined for the template. If the remediation results in full compliance, the compliance percentage is set to 100%. If not, the percentage is calculated based on the number of compliance operations that passed for the selected template.

Rollback to Previous

CloudControl maintains a record of the parameter values for hosts prior to the last remediation. The rollback feature allows the users to reset the host configuration values to the state prior to the last remediation.

Revert to Initial

CloudControl maintains baseline values for every parameter remediated on a host by recording the value before the first remediation occurs. The revert operation resets the value for every remediated parameter to its baseline value.

For example, if a host was first remediated for operation x1 during Remediation1, for operation x2 during Remediation2, and for operation y1 during Remediation3, then the value at the state before each remediation took place will be as follows:
The value at the state before Remediation1 was performed is a baseline value for Operation x1.
The value at the state before Remediation2 was performed is a baseline value for Operation x2.
The value at the state before Remediation3 was performed is a baseline value for Operation y1.

A revert operation on this host will reset the values of x1, x2, and y1 to the state before each parameter (operation value) was first remediated.

Host Compliance

You can view the list of CloudControl-protected hosts on the Compliance > Hosts page in the CloudControl Management Console, along with corresponding compliance scores based on the security compliance template that was last run against a host.

Note: Host compliance is displayed based on the DNS name of the host (IP address or FQDN), not the friendly name.

On the Hosts page, you can:

- View details of specific host configuration, assess or remediate hosts based on a template.
- Issue or cancel temporary host password. For more information, see Root Password Vaulting on page 48.
- Update trust on an Intel TXT enabled ESXi host. For more information, see Trust Attestation Service Configuration on page 42.
- Add or remove hosts from CloudControl protection. For more information, see Host Configuration Templates on page 70.

The following information is provided in the columns on the Hosts page:

- **Hosts:** The name of the host. Click a host to view/edit its settings.
- **Host Type:** The host type (ESXi Host, vCenter Server, etc.).
- **Patch Level:** The host version.
- **Last Run Template:** Displays the last security compliance template that was assessed on the host.

- **Last Run:** Displays the date and time when the last assessment ran (or Never if an assessment has not yet run). Click the date and time link to access the latest test results performed on the selected host. For more information, see Assessing Hosts below.

  A value of N/A indicates assessments are not supported on the host.

- **Compliance:** Shows the host compliance percentage if a host was assessed. This refers to the percentage of operations or operations that passed assessment. Click the percentage link to access the latest test results performed on the selected host. For more information, see Assessing Hosts below.

  The calculation is based on the last run template on the host and the latest test results for the host. For example, in a given template, if 10 operations ran and 8 passed, the ‘Compliance’ shows 80%.

The following buttons are available on the Hosts page:

- **Add**—Opens the Add Host Wizard, which you can use to add a new host to CloudControl. For more information, see Adding Hosts to CloudControl on page 35.

- **Edit**—Opens the Edit Host page, where you can change the configuration settings for the selected hosts. You can also click on the name of the host in the Hosts column to change the configuration settings for that specific host. For more information, see Modifying Managed Hosts on page 37.

- **Remove**—Removes the selected host(s) or vCenter Server(s) from CloudControl protection. For more information, see Removing Managed Hosts on page 37.

- **Compliance**—Opens the **Compliance Action** page, where you can select the **Compliance Type** to run on the selected host(s). The **Compliance Type** drop-down provides four options: Assess, RemEDIATE, Rollback to Previous and Revert to Initial.

- **Update Firewall**—Refreshes the firewall rules on CloudControl for each of the selected hosts.

- **Export as CSV**—Exports the test results for the selected host(s) to a Comma-Separated-Value (CSV) file. You can also specify a time frame to export the historical Assess RemEDIATE Compliance (ARC) test results performed for each selected host.

- **Issue Password**—Issues a temporary one-time root password after the Root Password Vaulting feature is enabled. For more information, see Request a Temporary Root Password on page 49.

- **Cancel Password**—Cancels an issued temporary one-time root password. CloudControl will automatically replace the temporary root password with a new random secure password and store the new password. For more information, see Cancel a Temporary Root Password on page 50.

- **Update Trust:** Updates Intel TXT host’s trust with the TAS server. If a host is trusted, then CloudControl assigns a **Trusted Host** ( ) icon to the host. If not, an **Untrusted Host** ( ) icon is assigned. For more information, see Verify and Update Host Trust on page 44.

---

### Assessing Hosts

Compliance template operations on protected hosts can occur as scheduled events or ad hoc. Ad hoc operations are performed immediately, whereas scheduled operations are performed at a specified date and time in the future. See Scheduled Events on page 51 for information on scheduling template events.

To perform an ad hoc assessment:
1. Select **Compliance > Hosts**.

2. Select one or more hosts and click the **Compliance** button.

3. On the Compliance Action page, leave the **Compliance Type** field set to the default value **Assess**.

4. In the **Template** drop-down, select the template to be used in the assessment and click **OK**.
   All the operations contained in the compliance template will run for the selected host(s). After the assessment is complete, CloudControl updates the information in the Last Run and Compliance columns for the selected host(s).

5. Click the date and time link in the **Last Run** column to display the assessment results for a specific host.
   - CloudControl displays the most recent Pass/Fail results for all the operations in the template that was last run against the host.
   - The Date/Time column displays the date and time of the last test-run.

   **Note:** Dates and times displayed on the Test Results page are shown in the local date and time set on the client computer, for example, the local machine where the browser window is running the CloudControl Management Console.

6. Optionally click the **Export as CSV** button to output the test results to a Comma-Separated-Value (CSV) file. You can do this either on the Test Results or the Hosts page.

### Remediating Hosts

Remediation performs the same operations as assessment, but also attempts to address any deviations from the compliance template encountered when the operations are run. While assessment can use both system and custom templates, remediation requires custom templates. Only custom templates can be toggled between remediation and assessment.

For more information on creating custom templates, see [Cloning a System Template](#) on page 71. When cloned, custom templates become available in the Template drop down when Remediation is selected in the Compliance Action section of the Compliance > Hosts page.

1. Select Compliance > Hosts.

2. On the Hosts page, select one or more hosts of similar type and click the **Compliance** button.

3. On the Compliance Action page, select **Remediate** from the Compliance Type drop-down list.

4. Select the compliance template that you want to use.

5. Click **OK**.
   All the operations in the compliance template will run for the selected host(s). After the remediation is complete, the CloudControl updates the information in the Last Run and Compliance columns for the selected host(s).

6. Click the date and time link in the Last Run column to display the test results for a specific host.
   CloudControl displays the most recent Pass/Fail test results for all the operations in the current template assigned to the host.
   The Date/Time column displays the date and time of the last test-run.

   **Note:** Dates and times displayed on the Test Results page are shown in the local date and time set on the client computer (i.e., the local machine where the browser window is running the CloudControl Management Console).
7. If desired, click the Export as CSV button to output the test results to a comma-separated-value (CSV) file. You can do this either on the Test Results page or the Hosts page.

**Revert to Initial State**

1. Select Compliance > Hosts.
2. On the Hosts page, select one or more hosts to revert and click the Compliance button.
3. On the Compliance Action page, select Revert to Initial from the Compliance Type drop-down list.
4. Click OK to start the revert process.
5. Click OK to confirm.

After the revert operation is complete, the operation appears under the Last Run Template list on the Hosts page.

**Rollback to Previous State**

To rollback to the state prior to the last remediation, go to the Compliance > Hosts page, select the host(s) you would like to rollback, and click the Compliance button.

1. Select Compliance > Hosts.
2. On the Hosts page, select the hosts that you want to rollback and click Compliance.
3. On the Compliance page, from the Compliance Type drop-down, select Rollback to Previous.
4. Click OK to start the rollback process.
5. Click OK to confirm.

After Rollback to Previous operation is complete, it appears under the Last Run Template list on the Hosts page.

**Compliance History**

The Compliance History page is accessible from the Appliance Dashboard, and allows you to view or audit historical CloudControl compliance testing information.

From the Compliance Dashboard Details panel, click the History icon to view.

The Compliance History page displays a graph showing the historical overall compliance percentage of the selected host.

- Mouse-over an individual graph point to view a quick summary of the compliance testing.
- Click on an individual graph point to view the full details.

**Host Configuration Templates**

CloudControl supports the following host configuration template types:
You can assign a specific security compliance template to each host from the Add/Edit Host page. For more information, see Managing Hosts on page 35.

**Note:** Ensure that you review all operations that require parameters before assessing or remediating a host. Parameters can only be assigned in custom templates.

### System Templates

System Templates are pre-packaged templates installed automatically with the appliance. CloudControl provides these templates as a starting point to help meet your compliance requirements. Copy these templates to configure the allowed operations based on your compliance requirements.

You can view the currently available templates on the Compliance > Templates page. From the Templates page you can:

- Click on a specific template name to display the Edit Template page, where you can view all the individual operations included in that template.
- Click **Copy** to create a new custom template based on the selected system template. You can also add operations to this template and customize it for your compliance needs. CloudControl also gives an option to select and copy individual operations listed on this page.

For more information, refer to the websites of the standard-setting organizations:

- **CIS:** [http://www.cisecurity.org/](http://www.cisecurity.org/)
- **PCI DSS:** [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/)

### Cloning a System Template

CloudControl users cannot modify the default System templates, but can clone the templates. Cloning makes a copy of the system template, which can then be modified. Cloned templates provide the flexibility to add, delete or copy the operations, assign them a risk score, and add a custom description. Users can also set custom parameters and determine the assignment (assess or remediate) for each operation. Some operations that are part of the original read-only templates may only be configured for assessment, while others may be configured to remediate the host.

1. Select **Compliance > Templates**.
2. On the Templates page, select the System template(s) that you want to clone and click **Clone**. Cloned templates are visible on the Custom tab, with _copy appended to the original template name.

### Custom Templates

You can add, delete, clone, export, and import custom templates.
Adding a Custom Template

To add a Custom template:

1. Select Compliance > Templates.
2. On the Templates page, click the Custom tab and click Add.
3. On the Add Template page, enter the template name and optional description.
4. Click OK.
5. If applicable, specify the Host Type.
6. Add the individual operations (checks and operations) to the template.
7. Click Add.
8. Select the operations to add.
9. Click OK.
10. Verify the operations are correct and click OK.

Deleting a Custom Template

1. Select Compliance > Templates.
2. On the Templates page, click the Custom tab.
3. Select the Custom template(s) that you want to delete and click Delete.

Cloning a Custom Template

To clone a Custom template:

1. Select Compliance > Templates.
2. On the Templates page, click the Custom tab.
3. Select the Custom template(s) that you want to clone and click the Clone button.
   The cloned template(s) will appear in the list with _copy appended to their name.

Importing a Custom Template

1. Select Compliance > Templates.
2. On the Templates page, click the Custom tab.
3. Click the Import button.
4. On the Import Templates page, click Browse and select the template file you want to import as a new template.
5. Click Import.
Copying a Template

1. Select **Compliance > Templates**.
2. On the Templates page, click the **Custom** tab.
3. Select the template that you want to export and click **Export**.

Exporting a Custom Template

1. Select **Compliance > Templates**.
2. On the Templates page, click the **Custom** tab.
3. Select the template that you want to export and click **Export**.

Copying a Template

To copy a template:

1. Open the Compliance > Templates page.
2. Click the name of the System template you want to copy or open the Custom tab and click the name of the Custom template you want to copy.
3. Click the **Copy** button.
4. Change the name and description, if desired.
5. Click **OK**.
6. Specify the operations to perform and click **OK**.

The **Custom** template tab opens and the new template appears in the list.

vSphere Catalogs

Two vSphere operations catalogs are available by default in CloudControl: the **VMware Operations Catalog ESXi** and the **VMware Operations Catalog Matrix ESXi**. The **VMware Operations Catalog ESXi** lists the vSphere Hardening Guide operations.

The **VMware Operations Catalog Matrix ESXi** lists the vSphere Hardening Guide (VHG) operations (ESXi, VM) and the description of compliance guides that recommend those operations. The catalogs include all the vSphere operations that are supported by CloudControl.

Supported operations are listed on the **Compliance > Templates > Edit Template VMware Operations Catalog ESXi** page. The columns include the information such as name of the operation, description, and the associated risk score.
NSX Catalogs

CloudControl supports operations that are grouped together in the NSX Operations Catalog Matrix. The matrix is located at **Compliance > Templates > Edit Template NSX Operations Catalog Matrix**.

Supported operations include:

- Verify that NTP is authorized.
- Enable remote syslog to configure remote logging for NSX Manager.
- Ensure that the NSX Manager certificate is valid.
- Enable in-protocol MDS authentication for OSPF and password for BGP.
- Ensure IPv6 is disabled and not configured if it is not in use.
- Disable SSH unless it is needed for diagnostics or troubleshooting.
- Follow VMware Security Advisories and apply patches.
- Secure the Controller network.
- Prevents excluding audit logs and system events from backup.
- Secure the backup directory.
- Ensure that IPv4 DNS is authorized and secure the DNS server.
- Ensure that the SFTP server on which backup is done is hardened.
- Ensure that the syslog server is authorized and the configuration is appropriate.
- Use SFTP for backup and restoration.
- Use Load Balance - SRCID for the VXLAN vmknic teaming policy.
Chapter 6. Access Policies

Access Policies Overview

Before creating and deploying access policies on a virtual infrastructure, confirm that CloudControl is protecting the vCenter Server and all the imported hosts. For more information on importing a vCenter Server, adding a host, or protecting these resources, see the Installation Guide for HyTrust CloudControl.

After importing a vCenter Server, CloudControl adds the vCenter Server object structure to a new draft policy and deploys it automatically.

Any time a new virtual machine, host, switch or port group is created, or added, the new object is automatically added to the CloudControl policy and the deployed policy is enforced on the new object. This is referred to as a Structure Changing Operation (SCO). A multi-user locking mechanism safeguards against conflicts in policy changes.

We recommend that you schedule manual policy changes, such as creating new rules, for times when change control on the virtual infrastructure is enforced and no new virtualized objects are being created.

Viewing the Current Policy

An CloudControl Policy is a combination of all rules defined in the system. The Deployed policy is the policy in effect.

Select Policy > Resources to view the current deployed policy.

Changing the Current Policy

Most pages under the Policy menu include both Create Draft and Deploy buttons. If a particular button on any of the Policy sub menu pages is disabled, such as, the Add, Delete, or Discard Changes button, be sure to click the Create Draft button first.

If changes were made within your virtual infrastructure where a user needed access and went around the CloudControl, you must manually refresh the policy resource tree by clicking the Refresh button before creating a new policy definition—in Draft mode the Refresh button is disabled.

To make a change in the deployed policy, such as adding a new rule to the vCenter Server:
1. Open any Policy page.
2. Click the Create Draft button. This copies the Deployed policy to a Draft policy.
3. Make your desired changes to the Draft policy using the various policy pages.
   **Note:** Ensure Draft is selected in the Type or Policy drop-down list on the policy pages when making your changes.
4. Click the Deploy button to replace the current Deployed policy with the Draft policy.
   **Note:** An archived policy is created from the previous Deployed policy. Archived policies exist as an audit trail only. There is no mechanism to roll back to an archived policy.

### Policy Definitions and Behavior

This section provides details on the policy definitions within CloudControl.

#### Policy Resource

A policy resource is any object that is part of the Policy Resource tree. Select Policy > Resources to view the objects that make up the Policy Resource tree.

![Policy Resources for Policy "Deployed"](image)

**Note:** Draft Rules, RuleSets, and Labels are visible in the Policy Resource tree, but do not take effect until the draft policy is deployed.

### Roles

Roles are collections of privileges or permissions that define authorized operations, usually defined along the same lines as roles or duties that users perform within an organization. A Role may also become an attribute of a Rule.

Roles may be modified, added, and deleted from the Policy > Roles page.
Domain User Group

After converting to Directory Service mode, CloudControl uses its service account to query group membership in the Active Directory (AD). When creating a rule, an existing domain user group can be mapped to a CloudControl role. Within AD, members of the domain user group must be manually assigned before the rule can be used.

Rules

Rules are relationships between AD domain user groups, objects, and entitled operations for a specific role. Rules may be added, deleted, assigned to single or multiple resources, or assigned to RuleSets. You can also import or export the existing rules.

Default rules are always assigned to the root of the resource tree and affect all child objects in the tree.

You use the Policy > Rules page to perform single or multiple Rule assignment to Resources or RuleSets.

**Note:** You can also propagate rules down the entire policy resource tree.

Rules are always defined by their domain user group and assigned role. A rule may exist without a defined constraint.

Rules apply to the object to which they are assigned, for example, the VMs folder. If the Propagate option is selected, and no RuleSets are assigned locally, they also apply to all the child objects of the folder.

Exporting Rules

You can only export rules assigned to Appliance Root. Rules assigned to resource assignments other than Appliance Root, ruleset assignments, and user and host attribute constraints will not be exported.
1. Select **Policy > Rules**.
2. Select the rule or rules that you want to export.
3. Click the **Export** button.

**Importing Rules**

*Note:* You can only import rules when a policy draft is created.

1. Select **Policy > Rules**.
2. On the Rules page, click **Create Draft**.
3. Click the **Import** button.
4. On the Rules Import page, click **Choose File** and navigate to the location of the file that you want to import.
5. Click **Open** to select the file and click **Next**.
6. Review the rules that will not be imported and click **Next**.
7. Click **Finish** to import the rules.
8. Click **Deploy**.

**Constraints**

Constraints are assigned to Rules, and allow you to restrict access to a resource.

1. Select **Policy > Rules**.
2. On the Rules page, click **Create Draft**.
3. Click the rule that you want to modify.
4. In the Constraints section, click the **Add** button to create a constraint.
5. On the Rule Constraints page, select the Constraint Type from the drop-down list. This can be one of the following:

<table>
<thead>
<tr>
<th>Constraint Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Protocol</td>
<td>Restricts access by the client protocol, for example, SSH, Browser (HTTPS), vSphere Windows or Web client, or REST API.</td>
</tr>
<tr>
<td>Client IP Range</td>
<td>Restricts access by the IP address range. Enter the start and end IP address of the range.</td>
</tr>
<tr>
<td>Client IP Match</td>
<td>Restricts access by the exact IP address entered.</td>
</tr>
<tr>
<td>Match VM Label(s)</td>
<td>Restricts access by the virtual machine label assigned to a resource. If the virtual machine label does not match, any operations are denied. Click Exclude VM Label to deny all access to the selected label.</td>
</tr>
<tr>
<td>Match Host Label(s)</td>
<td>Restricts access by the host label assigned to a resource. If the host label does not match, any operations are denied. Click Exclude Host Label to deny all access to the selected label.</td>
</tr>
<tr>
<td>Match Label(s) by Name</td>
<td>Restricts access by the name label assigned to a resource. If the name label does not match, any operations are denied. Click Exclude Label by Name to deny all access to the selected label.</td>
</tr>
<tr>
<td>Match Network Label(s)</td>
<td>Restricts access by the network label assigned to a resource. If the network label does not match, any operations are denied. Click Exclude Network Label to deny all access to the selected label.</td>
</tr>
<tr>
<td>Match Host Attribute(s)</td>
<td>Restricts access by the host attributes assigned to a resource. If one or more of the attributes does not match, any operations are denied. Click Exclude Host Attribute(s) to deny all access to the selected attributes.</td>
</tr>
<tr>
<td>NSX Security Tag(s)</td>
<td>Restricts access to the specified NSX security tag. When used in a rule, it limits the ability of NSX users to perform NSX security tag operations, such as editing, deleting, or assigning or unassigning tags, on the specified tag.</td>
</tr>
<tr>
<td>User Attribute(s)</td>
<td>Restricts access by the user attributes assigned to a resource. If one or more of the user attributes do not match, any operations are denied. Click Exclude User Attribute(s) to deny all access to the selected attributes.</td>
</tr>
</tbody>
</table>

**Note**: Labels must be created and assigned to a policy resource before they can be used as part of a rule constraint.

6. Click OK to add the constraint.

**Note**: If more than one constraint exists in a given rule, then all constraints must be satisfied before the operation can proceed. However, if you have more than one label in a single constraint, than the operation can proceed if any of the labels is satisfied.

7. Click OK to close the Edit Rule page.

8. Click Deploy to save the changes.
RuleSets

RuleSets are a collection of rules, that, when present disable direct rules assigned to an object. Each RuleSet contains a rule or set of rules, each with its own domain user group, role, and constraint. Each RuleSet can also be assigned to one or more policy resources.

If a policy resource includes more than one RuleSet, each RuleSet is evaluated independently—the conditions of only one must be met for the operation to proceed.

By default, RuleSets always propagate down the policy resource tree.

Note: If a policy resource is associated with a RuleSet without a rule, then all access to that policy resource is denied. Because a deployed RuleSet creates a new policy resource domain for a given object, we recommend that you also include a rule within each RuleSet that contains the SuperAdmin domain user group and the ASC_SuperAdmin role.

By default, the CoreAppliance RuleSet does not include superadmin privileges. If superadmin needs access to the policy objects containing the CoreAppliance RuleSet, add a rule within the RuleSet that contains the SuperAdmin domain user group and the ASC_SuperAdmin role.

Adding a RuleSet

2. On the RuleSets page, click Create Draft, and then click Add.
3. On the Add RuleSet page, enter the name and optional description for the RuleSet.
4. Click OK.
5. On the Edit RuleSet page, you can assign Resources and Rules. For more information, see Assigning Resources to RuleSets below or Assigning Rules to RuleSets on the next page.
6. Click OK.

Assigning Resources to RuleSets

You can assign one or more resources to an existing RuleSet.

2. On the RuleSets page, click the Create Draft button.
3. Click the RuleSet that you want to modify.
4. On the Edit RuleSet page, in the Assigned Resources section, click Assign.
5. On the Assign RuleSets to Policy Resources page, select the resource or resources that you want to add. You can use the Search field or the resource checkboxes to narrow your search.
6. Click OK to add the selected resources.
7. Click OK to close the Edit RuleSet page.
## Assigning Rules to RuleSets

1. Select **Policy > RuleSets**.
2. On the RuleSets page, click the **Create Draft** button.
3. Click the RuleSet that you want to modify.
4. On the Edit RuleSet page, in the Assigned Rules section, click **Assign**.
5. On the Assign Rules to RuleSets page, select the rule or rules that you want to add.
   - You can use the Search field to narrow your search.
6. Click **OK** to add the selected rules.
7. Click **OK** to close the Edit RuleSet page.

## Labels

Labels are used to classify or categorize policy resources. Labels are useful when defining rule constraints. For example, virtual machines can be constrained to start only on the hosts with a specific label (e.g., *production*).

Labels can both be associated with a template and assigned to hosts. The association of labels with templates and hosts gives users an ability to create scheduled events based on labels. Every time a scheduled event based on a particular label is run, the hosts associated with that label are assessed or remediated against the template associated with that label.

A single template may be associated with multiple labels. However, any given label may only be associated with one template. This avoids a template conflict, a situation where two templates with the same operations but different parameter values may be assessed or remediated against a host.

CloudControl includes the following built-in labels:

- DEV
- FirewallVM
- HIPAA
- INFRASTRUCTURE
- MONITORING
- PCI
- PROD
- PROD-HA
- QA
- SAL1
- SAL2
- SAL3
- SAL4
- SECURITY
- SENSITIVE
- STAGING
- TRUSTED
- UNTRUSTED

Although not a requirement, the recommended usage for the TRUSTED and UNTRUSTED labels is in environments utilizing the Intel TXT platform.

Note: Labels with the following constraint types should only be assigned to hosts or port groups: Network Label Match and Host Label Match. Labels associated with the Label Match by Name constraint can be assigned to any object in the policy resource tree. These constraints only take effect after the corresponding Labels are assigned to the proper policy resource(s).

Adding a Label

To add a new label to the labels list:

2. On the Policy Labels page, click Create Draft.
   CloudControl displays a message: The draft policy is now ready for editing.
   The Type drop-down displays Draft. The Add, Delete and Assign buttons are enabled.
3. Click on the Add button.
4. On the Add Label page, enter the name in the Name field, and select a custom template from the Associated Template drop-down.
   The newly created label will be associated with the custom template selected here.
   CloudControl displays the message: The label was successfully added. You can now associate it with a policy resource.
   The Assign button is enabled.
5. Click on the Assign button.
6. On the Assign Policy Labels to Policy Resources page, select the appropriate resource type.
   For example, when you check the Host checkbox, CloudControl displays all available hosts under the Search Results column.
7. Click on the checkbox next to a resource you want to associate with the new label.
8. Click OK.
   The selected resource appears under the list of the resources that are associated with the new label.
9. Click OK to return to the Policy Labels page.
   The new label appears under the list of labels.
10. Click on the **Deploy** button.
    You will see the message: *Policy was successfully deployed.*

### Deleting a Label

Users can only delete labels that are not associated with any resource.

To delete a label:

1. Go to the **Policy > Policy Labels** page.
2. Make sure the **Type** is **Draft**. If not, click on the **Create Draft** button.
3. Select the label(s) you want to delete by clicking the checkbox(es) next to the label name(s).
4. Click the **Delete** button.

If the label is associated with any hosts, CloudControl displays an error message.

If the selected label is not associated with any resource, then it is deleted.

5. Click the **Deploy** button to save the changes.

### User Attributes

User attributes allow you to add additional authorization control to your operations. User attributes are defined in CloudControl and are based on Directory Service attributes or attributes in an X.509 certificate.

- **Attribute Name**—The attribute name from the Directory Service or X.509 certificate. The name and location depends upon your provider type. For example, for Active Directory, the attribute name is found on the **Attribute Editor** tab in the Properties dialog box.
- **Attribute Provider**—The provider where the attribute name is found. This is either Directory Service or X.509 certificate.

- **User Attribute Type**—Whether the attribute value is a string or Boolean.

After you create the user attribute, you can add it as a constraint, and then add that constraint to a Rule.

**Adding a User Attribute**

1. Select **Policy > User Attributes**.
2. On the User Attributes page, click **Add**.
3. On the Add User Attribute, complete the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute Name</td>
<td>Enter the name for the user attribute.</td>
</tr>
<tr>
<td>Attribute Provider</td>
<td>Select DIRECTORY_SERVICE or X509_Certificate.</td>
</tr>
<tr>
<td>User Attribute Type</td>
<td>Select STRING or BOOLEAN.</td>
</tr>
</tbody>
</table>

4. Click **OK**.  
The new User Attribute is added to the User Attributes page.

**Uploading a User Attributes File**

You can upload an XML file containing a list of user attributes definitions in the following format:

```xml
<?xml version="1.0"?>
<user-attributes>
  <user-attribute>
    <name>Attribute-1</name>
    <attribute-provider>DIRECTORY_SERVICE</attribute-provider>
    <type>STRING</type>
  </user-attribute>
</user-attributes>
```

1. Select **Policy > User Attributes**.
2. On the User Attributes page, click **Upload**.
3. On the Upload User Attributes page, click **Browse**.
4. Select the XML file that you want to upload and click **Open**.
5. Click **OK** to upload the file.

**Adding a User Attribute Constraint Type**

1. Select **Policy > Rules**.
2. On the Rules page, click **Create Draft**.
3. Click the rule that you want to modify.
4. In the Constraints section, click the Add button to create a constraint.
5. On the Rule Constraints page, select **User Attribute(s)** from the Constraint Type drop-down list.
6. Enter values for the user attributes.
7. Check the **Exclude Attribute** checkbox if you want to exclude the attributes.
8. Click **OK**.

**PolicyTags**

PolicyTags provide boundary control capabilities based on Intel’s Trusted Execution Technology (Intel TXT). CloudControl leverages Intel TXT-enabled processors to securely write administrator-defined descriptors to the hardware. Using this capability, CloudControl users can define boundary policies for virtualized applications. Once boundary policies are defined, they can be applied to any TPM (Trusted Platform Module) enabled hosts. To enforce those policies, add them to Rules as a Host Attribute constraint type. Using the Exclude Host Attributes directive allows users to exclude the hosts with matching PolicyTags values from the Rule.

For more information, see **Rules** on page 77.

**Defining PolicyTags in CloudControl**

1. Select Policy > **PolicyTags**.
2. On the PolicyTags page, click **Add**.
3. On the Add PolicyTag page, choose the PolicyTag Type and enter the appropriate value.
   - State/Province—Assign State/Province.
   - Physical Data Center (PDC)—Assign Physical Data Center name or region.
   - Region (Logical)—Assign a geographical region.
   - Classification—Assign custom PolicyTags value.
4. Click **OK**.

The PolicyTags page displays the PolicyTag that you added. Click **Add** to add another PolicyTag.

**Assigning PolicyTags to Hosts**

**Before You Begin**

PolicyTags can only be applied to TPM-enabled hosts. Before applying PolicyTags, ensure that TPM is supported on the host and enabled in the BIOS.

To verify that an ESXi host is TPM-enabled, perform one of the following:
• Log into the vCenter Managed Object Browser, scroll to ‘host’, select the host, select ‘capability’, and scroll to ‘tpmSupported’. The value should be ‘true’.

For more information, after selecting the hosts, scroll to the bottom and select ‘QueryTPMAttestationReport’. Select ‘Invoke Method’ and a comprehensive report of the hosts TPM information will be displayed. If the host is not TPM-enabled, this selection will return ‘false’.

• From an SSH session or from PowerCLI, run the esxcli hardware trustedboot get command.

When run from a TPM-enabled host, you should see the following output:

```
Drtm Enabled: true
Tpm Present: true
```

### Procedure

1. Select **Compliance > Hosts**.
2. On the Hosts page, check the checkbox for the TPM-enabled host and click **Edit**.
3. On the Edit Hosts page, select the **PolicyTag** tab.
4. Select the appropriate PolicyTag value for each of the following fields:
   - Country
   - State/Province
   - Region (Logical)
   - Physical Data Center (PDC)
   - Classification
5. Click **OK**.

CloudControl displays a JGrowl error message that prompts users to PXE boot the host(s) to activate the PolicyTag assignment.

### Enforcing PolicyTags

The values defined for each of the PolicyTags types are available on the Rule Constraints page under the **Match Host Attribute(s)** constraint type. PolicyTags are added to Rules as constraints. A Rule is assigned to hosts, and is applied only to the hosts with the matching PolicyTag values. If a Rule assigned to hosts has constraints with the **Exclude Host Attributes** directive, the hosts with the matching PolicyTag values are ignored or excluded from the Rule.

1. Select **Policy > Rules**.
2. On the Policy Rules page, click the **Create Draft** button
3. Click on the Rule to which you want to assign PolicyTags constraints.
4. Click the **Add** button under the **Constraints** panel.
5. On the Rule Constraints page, select **Match Host Attribute(s)** from the **Constraint Type** drop-down.

CloudControl displays all PolicyTags with defined values.

6. Select appropriate values for the PolicyTags.
7. If you want the rule to exclude the hosts with PolicyTag values that match the selected PolicyTag values, click the **Exclude Host Attributes** checkbox.

8. Click **OK**.
   The selected PolicyTags with values are assigned to that rule.

9. Click **OK**.

10. Click **Deploy**.

   Once PolicyTags are assigned, they are enforced immediately. After assignment, if the PolicyTags are not provisioned, operations governed by the particular rules are denied until the PolicyTags are provisioned.

**PolicyTags Provisioning**

When PolicyTags are assigned to a host, the PolicyTag Service creates a certificate on the Trust Attestation Server (TAS) with the host’s UUID and the tags assigned to that host. The process of PolicyTags Provisioning involves pulling or applying the certificate to the physical host. This process is initiated by PXE booting the host.

**PolicyTags Evaluation**

For every Rule in the policy that has PolicyTags constraints and is assigned to a host, the following logic is executed each time the Rule is evaluated.

1. CloudControl checks the configured PolicyTags values and the provisioned PolicyTags values on the host.

2. If the configured PolicyTags values match the provisioned PolicyTags values, then it proceeds to check the Rule’s constraint values.

3. If the Rule’s PolicyTags constraint values match the provisioned PolicyTags values on the host, then CloudControl enforces the rule on that host.

   Depending on the Rule, operations on that host are allowed or denied.
   - If the host’s PolicyTag values do not match the Rule’s PolicyTag constraint value, then the action defined in the Rule is not applied to those hosts.
   - If the Exclude Constraints directive is used for the Rule, the action defined in the Rule is applied only to the hosts whose PolicyTags values do not match the Rule’s PolicyTag constraint values.

**PXE Server Configuration**

**Prerequisites:**

- A working PXE server configured with supporting technologies (DHCP, TFTP, and NFS share).
- The Asset Tag provisioning image (assettag.iso).
- The TPM for any hosts to be provisioned must be in the clear state with Intel TXT activated.
Configuration:

1. Extract the contents of assettag.iso and copy the casper folder to the NFS share directory on the PXE server.

2. Copy the SSL certificate located at: /etc/intel/cloudsecurity/ssl.crt.pem from your Asset Tag Management server to the PXE server, and place it in the NFS share directory of the PXE server.

3. On the PXE server, edit the /tftpboot/pxe/bootloader.cfg file and add the following arguments:
   - atag_cert='http://<PXE IP Address>/<nfsshare>/ssl.crt.pem'
   - atag_username='admin'
   - atag_password='password'
   - atag_server='http://<IP Address>:<Port>/mtwilson/v2'

   **Note:** Make the following changes to the file before saving:
   - Replace <PXE IP Address> with the IP address or hostname of the PXE server.
   - Replace <nfsshare> with the path to the NFS share.
   - Replace <IP Address> and <Port> with the IP address or hostname and port of the Asset Tag Management server on the PXE network.

Provisioning Hosts

1. Reboot the host.

2. Clear TPM in BIOS.

3. Reboot the host and enable TPM in BIOS.

4. PXE boot the host.

   The system will boot and the Asset Tag Provisioning Agent script will run when the Asset Tag Provisioning Image (ISO) loads. The script will contact the Trust Attestation Server and retrieve the latest valid certificate for the host’s hardware UUID.

5. Reboot the host once again and enable TPM in the BIOS.

6. Reboot the host to its normal operating system.

   The host’s TPM state will be: Enabled + Activated + Owned.

   Each POST takes about 3 to 5 minutes.

7. Open the web browser running CloudControl and select **Policy > Resources**.

8. Verify that the PolicyTags have been provisioned.

   - If the tag icon next to the host being provisioned is blue, then the PolicyTags assigned to the host are provisioned.

   - If the tag icon is yellow, that means the PolicyTags assigned to the host are not provisioned.

   - If the provisioning process was not successful, you may have to clear the TPM once again and repeat the process.
Typical TPM states

- Disabled
- Enabled
- Enabled + Activated
- Enabled + Activated + Owned

Separation of Duties

CloudControl provides the capability to define roles as a collection of privileges on a per-role basis, allowing system administrators to control which CloudControl roles can perform what operations within the virtual infrastructure. This is called separation of duties.

2. On the Roles page, click on the name of the role for which you want to manage.
3. On the Edit Role page, check the checkbox next to a privilege to allow or deny the operation on the specified vCenter managed object type for this role. If the checkbox is partially checked, then some operations at a lower level are allowed.
4. Click OK to save the changes.

Default Roles Explained

CloudControl ships with a number of roles to help configure granular role-based access controls (RBAC) in a virtual environment. A role is a collection of access privileges that is mapped to a specific operation.

Privileges belong to specific roles. For example, power on the VM operation is mapped to the VirtualMachine.Interact.PowerOn privilege, and this privilege belongs to a few roles such as ASC_VMPowerUser and ASC_SuperAdmin. For more information, see Default Roles and Permissions on page 182.

Policy Interaction

The CloudControl Policy Engine carries out the following work flow when a user performs an operation on a given policy resource:

1. If a RuleSet is found during the process of walking up the resource tree, the local rule or rules that are shared on the same node as the RuleSet are ignored. The policy engine then evaluates the RuleSet.
   - If a true statement is found, the requested operation is allowed.
   - If a false statement is found, the policy engine terminates the user request and the operation is not allowed.
2. If there are no RuleSets, then the CloudControl Policy Engine looks at the local rule or rules assigned to the resource object.
   - If a true statement is found from the local rule or rules, the requested operation is allowed.
   - If a false statement is found from the local rule or rules, the policy engine walks up the policy tree to the next node and applies the same line of reasoning.

Example Policies

It is recommended that a user with sufficient credentials (i.e., ASC_SuperAdmin role) login to the CloudControl Management Console to create the policies and perform the tasks described in this section.

Note: The examples in this section are only meant to provide insight into typical CloudControl policy scenarios and may not match your exact requirements and environment.

You should be familiar with how to create rules and assign CloudControl rules and constraints as described previously.

Example 1—Allow Two Different Administrator Groups to Use Separate Host Clusters and Inventory Folders

This example shows how to set up an CloudControl policy that allows two different administrator groups to use separate host clusters and inventory folders.

- AdminGroupA:
  - Create VMs in FolderA (inventory folder)
  - Create hosts in ClusterA
- AdminGroupB:
  - Create VMs in FolderB (inventory folder)
  - Create hosts in ClusterB

Policy Setup

1. Assume the user has Login privilege for the vCenter.
2. Assume the following objects are created in the vCenter.
   - Inventory folders: FolderA, FolderB
   - Host clusters: ClusterA, ClusterB
3. Create the necessary rules.
   - RuleA (AdminGroupA, AllPriv-Role)
   - RuleB (AdminGroupB, AllPriv-Role)
4. Assign the rules.
   - RuleA to resources ClusterA, FolderA, Network folder, and Datastore folder
   - RuleB to resources ClusterB, FolderB, Network folder, and Datastore folder
In this setup, an AdminGroupA user can create a VM in ClusterA and FolderA, but cannot move that VM to FolderB or any host in ClusterB.

**Example 2—Allow Two Different Administrator Groups to Manage Separate Virtual Machines Using OS Label**

This example shows how to set up an CloudControl policy that allows two different administrator groups to manage separate virtual machines.

- **WinAdmin**—Manage all VMs with a WinVM label.
- **UnixAdmin**—Manage all VMs with a UnixVM label.

**Policy Setup**

1. Assume the user has Login privilege for the vCenter.
2. Assign labels based on operating system type.
   - **WinVM**—Assign to all VMs with Windows OS.
   - **UnixVM**—Assign to all VMs with Unix OS.
3. Create the necessary rules.
   - WinRule (WinAdmin, AllPriv-Role)
4. Add the WinVM label to the following constraints:
   - Match VM Label
   - UnixRule (UnixAdmin, AllPriv-Role)
5. Add the UnixVM label to the following constraints:
   - Match VM Label
6. Assign the rules.
   - WinRule to the CloudControl.
   - UnixRule to the CloudControl.

In this setup, a WinAdmin user can only manage VMs with a WinVM label, and a UnixAdmin user can only manage VMs with a UnixVM label.

**Example 3—Segmenting Out Part of the Virtual Machine Infrastructure**

This example shows how to set up an CloudControl policy that allows two different administrator groups to manage separate virtual machines.

- **PciAdmin:**
  Manage VMs with a PCI label on hosts and networks with a PCI label.
- **SysAdmin:**
  Manage VMs without a PCI label on hosts and network without a PCI label.
Policy Setup

1. Assume the user has Login privilege for the vCenter.

2. Assign the PCI label to all VMs, hosts, and port groups to be managed by the PciAdmin group.

3. Create the necessary rules.
   PciRule (PciAdmin, AllPriv-Role)

4. Add the PCI label to the following constraints:
   - Match VM Label
   - Host Label Match
   - Network Label Match
   - SysRule (SysAdmin, AllPriv-Role)

5. Add the PCI label and select the Exclude... checkbox to the following constraints:
   - Match VM Label
   - Host Label Match
   - Network Label Match

6. Assign the rules.
   - SysRule to CloudControl.
   - PciRule to CloudControl.

In this setup, a PciAdmin user can only manage VMs with a PCI label and a SysAdmin user can only manage VMs without a PCI label.

Example 4—Allow SysAdmin Group to Manage All Objects, But Cannot Move Virtual Machines with PCI Label

This is a special case example that shows how to set up an CloudControl policy that allows the SysAdmin group to manage all objects, but cannot move VMs with a PCI label to hosts and networks without a PCI label.

Policy Setup

1. Assume the user has Login privilege for the vCenter.

2. Assign the PCI label to all VMs, hosts, and port groups as appropriate.

3. Create the necessary rules.
   PciRule (SysAdmin, AllPriv-Role)
4. Add the PCI label to the following constraints:
   - Match VM Label
   - Host Label Match
   - Network Label Match
   - SysRule (SysAdmin, AllPriv-Role)

5. Add the PCI label and select the Exclude... checkbox to the following constraints:
   - Match VM Label
   - Host Label Match
   - Network Label Match

6. Assign the rules.
   - SysRule to the vCenter/CloudControl.
   - PciRule to the vCenter/CloudControl.

In this setup, a SysAdmin user can manage all VMs, but cannot move VMs with a PCI label to a host or network without a PCI label.

### Restricting Visibility

CloudControl enables you to restrict users from viewing objects if they do not have explicit view privileges. Restricting visibility privileges is supported only on the following:

- vSphere WCS versions 6.0, 6.5 and 6.7
- vSphere HTML5 Client versions 6.5 and 6.7

By default, NSX and vSphere users can only view the following:

- NSX users can only view networking and security objects related to NSX. In the following figure, the items marked NSX View are visible to NSX users. The top-level vSphere objects marked vSphere View are visible, but all items under those objects will be hidden.

- vSphere users can only view vSphere objects. In the following figure, the items marked vSphere View are visible to vSphere users. The items marked NSX View will be hidden. You can also restrict vSphere users so that they can only view particular vSphere objects. For more information, see Visibility Privileges for NSX and vSphere Objects on the next page.
Visibility Privileges for NSX and vSphere Objects

CloudControl uses the following privileges to grant views to NSX and vSphere objects:

<table>
<thead>
<tr>
<th>Privilege Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSXPlugin.View_All</td>
<td>Allows users to view all NSX objects.</td>
</tr>
<tr>
<td>DataCenter.View_All</td>
<td>Allows users to view all vSphere objects.</td>
</tr>
</tbody>
</table>

**Note:**

- If a user needs to view both NSX and vSphere objects, you can assign the view_all privilege directly to that user. For example, if you grant the NSXPlugin.View_All privilege to a particular vSphere user, that user will be able to view all NSX objects.
- If an NSX user does not have the NSXPlugin.View_All privilege and attempts to access NSX operations that are restricted, they will see the following message: No NSX Managers available. Verify current user has role assigned on NSX manager.

For vSphere, you can also grant or restrict access to vSphere managed inventory objects. Views for vSphere are restricted on a hierarchical basis. For example, if you grant the datacenter view, then the user can view everything in that datacenter. If you restrict the datacenter view, then the datacenter and all of its contents are hidden.

**Note:** If the vCenter environment is in linked mode, users have the same level of visibility privileges in all vCenters registered to the Platform Services Controller.
Using Constraints with Visibility Privileges

You can use the **Match Label(s) by Name** constraint to further restrict vSphere views.

For example, in an environment with two data centers, you can create a name label of DataCenter1 and DataCenter2, and assign one name label to each data center. If you create a rule with the DataCenter1 **Match Label(s) by Name** constraint, then only users that have that rule assigned to the role can view DataCenter1.

If you check the **Exclude Label by Name** checkbox, then users with that rule assigned can only view DataCenter2.

**Note:** Only the **Match Label(s) by Name** constraint is supported with restricted visibility privileges.

Granting Visibility to NSX Objects

Grant NSX view privileges to users with permission to view NSX objects.

1. Log in to the CloudControl Management Console as an admin user with the permissions to modify roles and privileges.
2. Select **Policy > Roles**.
3. On the **Policy > Roles** page, click **Create Draft**.
4. Click the role that you want to modify.
5. On the **Policy > Roles > Edit Role <role_name>** page, check the NSXPlugin checkbox to grant the View_All privilege.

<table>
<thead>
<tr>
<th>vSphere Managed Inventory Object</th>
<th>Privilege Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Datacenter</td>
<td>Datacenter.View_All</td>
<td>Allows vSphere users to view the datacenter and all child resources.</td>
</tr>
<tr>
<td>Folder</td>
<td>Folder.View_All</td>
<td>Allows vSphere users to view a folder and all child resources. <strong>Note:</strong> Because all resources have default folders, any user with the Folder.View_All privilege can view all resources.</td>
</tr>
<tr>
<td>Datastore</td>
<td>Datastore.View_All</td>
<td>Allows vSphere users to view a datastore and all files included.</td>
</tr>
<tr>
<td>Cluster</td>
<td>Host.Inventory.Cluster.View_All</td>
<td>Allows vSphere users to view a cluster and all child resources.</td>
</tr>
<tr>
<td>Host</td>
<td>Host.Inventory.View_All</td>
<td>Allows vSphere users to view a host and its child resources.</td>
</tr>
<tr>
<td>DVSwitch</td>
<td>DVSwitch.View_All</td>
<td>Allows vSphere users to view a distributed virtual switch and its child resources.</td>
</tr>
</tbody>
</table>
6. Click OK to return to the Policy > Roles page.
7. Click Deploy to save the changes.

Granting Visibility to vSphere Objects

Grant vSphere view privileges to users with permission to view vSphere objects.

1. Log in to the CloudControl Management Console as an admin user with the permissions to modify roles and privileges.
4. Click the role that you want to modify.
5. On the Policy > Roles > Edit Role <role_name> page, modify the appropriate vSphere privileges:
   1. Expand the resource that you want to modify. This can be one of the following:
      - Datacenter
      - Folder
      - Datastore
      - Host > Inventory > Cluster
      - Host > Inventory
      - DVSwitch
   2. Check the View_All privilege for each resource that you want to grant, and clear the View_All privilege for each resource that you want to restrict.
6. Click OK to return to the Policy > Roles page.
7. Click Deploy to save the changes.
Chapter 7. Alerts

Alerts Overview

Alerts provide a method to receive immediate notifications based on the operations performed by users or by CloudControl itself. When CloudControl or a user performs an operation matching an alert, the appliance generates that particular alert. If configured, an email with the activity details is sent to the user. This email contains a link to open the Alert Viewer in CloudControl which provides additional details.

The following are the CloudControl privileges that users must have in order to receive alerts.

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asc.Alerts.Configure</td>
<td>Allows a CloudControl user to configure and view Alerts.</td>
</tr>
<tr>
<td>Asc.Alerts.View</td>
<td>Allows a CloudControl user to view Alerts.</td>
</tr>
</tbody>
</table>

Configuring Alerts

Note: Before you can configure alerts, you must enable SMTP notifications. For more information, see Configuring Monitoring and Notifications on page 55.

1. In the CloudControl Management Console, select Configuration > Alerts.

2. On the Alerts Configuration page, configure the following settings:
   - Enable—Enables (selected) or disables (deselected) the CloudControl Alerts.
     Note: If the Enable check box is not visible, a message appears indicating that SMTP needs to be configured.
   - Enable email notifications—Enables or disables sending an email notification when an alert is generated.
   - Email Address (FROM)—The email address that displays in the From field when an alert email notification is sent.

3. Click Apply.

The ASC Alert Definitions and Resource Alert Definitions tabs appear. Click the appropriate tab to manage your alert definitions.
Alert Definitions

Two types of Alert Definitions are available on the Alerts Configuration page: ASC Alert Definitions and Resource Alert Definitions. The ASC Alert Definitions provide alert definitions for CloudControl operations. The Resource Alert Definitions currently provide alert definitions for vSphere operations.

ASC Alert Definitions

The following ASC alert definitions are available in CloudControl:

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance Drift Alert</td>
<td>The Compliance Drift alert is generated when the number of failed operations during an assessment is greater than or equal to the specified threshold. Users can specify any hosts and a template that will be run against them. Alternatively, users can select hosts with a specific label. When hosts with a specific label are selected, an alert is generated based on results of manual assessments or assessments run as scheduled events, on all hosts associated with that particular label.</td>
</tr>
<tr>
<td>Template Conflict Alert</td>
<td>When a host is remediated against multiple label-based templates with the same operations but different parameter values, the Template Conflict Alert is triggered. As soon as the first conflicting operation is found, the Template Conflict Alert is triggered and other conflicting operations are not reported. Users can enable or disable, but cannot delete this alert.</td>
</tr>
</tbody>
</table>
| Trust Status Change Alert     | When the trust status of any protected host changes, the Trust Status Change alert is triggered. The trust status of protected hosts may change as a result of actions such as:  
  - Manually updating the trust using the **Update Trust** button on the **Compliance > Hosts** page.  
  - Making a host a **Good Known Host**.  
  - Editing a host. |
| vSphere 6 ELM Setup Change Alert | When CloudControl detects that a vCenter Server Enhanced Linked Mode set up is modified, the vSphere ELM Setup Change Alert is triggered. Users can enable or disable, but cannot delete this alert. |
| vSphere Auto Deploy ESXi Config Alert | If CloudControl detects any change while re-protecting an ESXi host, it will generate an alert based on that change. |

Resource Alert Definitions

CloudControl includes the following built-in Resource Alert definitions:
- **Critical PCI Assets Deleted**: VM, network, or a host with label PCI, SAL1, or SENSITIVE is deleted.
- **Critical PCI Assets Powered Off**: VM or a host with PCI label is powered off.
- **Critical PCI Workloads Deletion Denied**: A request to delete VM with PCI, SAL1, or SENSITIVE label is denied.
- **Denial of Service Attack**: Denial of login. The alert gets triggered if there are 10 login attempts per minute on any protected host.
- **Sensitive Workloads Moved**: 2 VMs with SENSITIVE label migrate or are attempted to move within 5 minutes.
- **VM / Workload Sprawl**: 2 VMs created or added within 5 minutes.

Apart from the built-in alerts, users can also customize and add alerts for Roles, Labels, Resource Types and/or Operations.

For the list of built-in labels, see [Labels](#) on page 81.

To view the [Resource Alert Definitions](#), click on the Resource Alert Definitions tab on the Configuration > Alerts page.

---

**Configuring ASC Alert Definitions**

CloudControl has the following ASC Alert Definitions that are enabled by default:

- Compliance Drift Operation
- Template Conflict Operation
- Trust Status Change Operation
- vSphere Auto Deploy ESXi Config Operation
- vSphere6 ELM Setup Change

You can edit these alerts, or create a new alert for Compliance Drift or Trust Status Change.

**Adding Compliance Drift ASC Alert Definitions**

1. Select **Configuration > Alerts**.
2. On the Alerts Configuration page, click the **ASC Alert Definitions** tab and click **Add**.
3. Enter the name for the ASC Alert Definition.
4. Choose **Compliance Drift** to issue an alert whenever the compliance of a host drops below the threshold that you set.
5. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any Host</strong>— Sends an alert when the compliance of the selected host type drops below the threshold.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosts with Label(s)</strong>— Sends an alert when the compliance of a host with the specified label drops below the threshold.</td>
</tr>
<tr>
<td>Host Type</td>
<td>If you selected Any Host, select one of the following to limit your selection:</td>
</tr>
<tr>
<td></td>
<td>• Any—All hosts.</td>
</tr>
<tr>
<td></td>
<td>• ESXi—ESXi hosts only.</td>
</tr>
<tr>
<td></td>
<td>• NSX—NSX hosts only.</td>
</tr>
<tr>
<td>Labels</td>
<td>If you selected Host with Label(s), select one or more labels.</td>
</tr>
<tr>
<td>Template</td>
<td>Select the template for which compliance is assessed, or select <strong>Any</strong> to use all templates.</td>
</tr>
<tr>
<td>Minimum Failed Compliance Operations</td>
<td>Select the minimum number of failed operations required to trigger the alert.</td>
</tr>
<tr>
<td>Alert Risk Score</td>
<td>Select the risk value of the alert. CloudControl uses this value to prioritize the processing of alert definitions. The lower the risk score value, the higher the priority.</td>
</tr>
</tbody>
</table>

6. To enable email for this alert, check the **Enable Email** checkbox and enter an email address.

7. Click **Test Email** to send a sample email to the address you entered.

8. Click **OK**.

**Adding Trust Status Change ASC Alert Definitions**

1. Select **Configuration > Alerts**.

2. On the Alerts Configuration page, click the **ASC Alert Definitions** tab and click **Add**.

3. Enter the name for the ASC Alert Definition.

4. Choose **Trust Status Change** to issue an alert when the trust status of a protected host changes.
5. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hosts</td>
<td>Select one of the following:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Any Host</strong>—Sends an alert when the trust status changes for any protected host of the selected host type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hosts with Label(s)</strong>—Sends an alert when the trust status changes for hosts with the selected label.</td>
</tr>
<tr>
<td>Host Type</td>
<td>If you selected Any Host, select one of the following to limit the hosts:</td>
</tr>
<tr>
<td></td>
<td>• Any—All hosts.</td>
</tr>
<tr>
<td></td>
<td>• ESXi—ESXi hosts only.</td>
</tr>
<tr>
<td></td>
<td>• NSX—NSX hosts only.</td>
</tr>
<tr>
<td>Labels</td>
<td>If you selected Host with Label(s), select one or more labels.</td>
</tr>
<tr>
<td>Alert Risk Score</td>
<td>Select the risk value of the alert. CloudControl uses this value to prioritize the processing of alert definitions. The lower the risk score value, the higher the priority.</td>
</tr>
</tbody>
</table>

6. To enable email for this alert, check the **Enable Email** checkbox and enter an email address.

7. Click **Test Email** to send a sample email to the address you entered.

8. Click **OK**.

### Editing ASC Alert Definitions

1. Select **Configuration > Alerts**.
2. On the Alerts Configuration page, click the **ASC Alert Definitions** tab.
3. Select the ASC Alert Definition that you want to edit and click **Edit**.
4. Update the information as necessary. For more information on the fields, see Adding Compliance Drift ASC Alert Definitions on page 99.
5. Click **OK**.

### Adding Resource Alert Definitions

**Important:** Adding a new alert definition causes all existing alert definition threshold counters to reset.

1. Select **Configuration > Alerts**.
2. On the Alerts Configuration page, click the **Resource Alert Definitions** tab and click **Add**.
3. Click **Add**.
4. Enter the following information to specify the alert definition criteria:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter the name of the alert.</td>
</tr>
<tr>
<td>Role</td>
<td>Select the role for which the alert definition applies.</td>
</tr>
<tr>
<td>Labels</td>
<td>Select the resource label(s) for which the alert definition applies.</td>
</tr>
<tr>
<td>Resource Types</td>
<td>Select the resource type(s) for which the alert definition applies.</td>
</tr>
<tr>
<td>Resource Name</td>
<td>Select the resource name for which the alert definition applies. Only resources that match the selected labels and/or resource types are displayed.</td>
</tr>
<tr>
<td>Operations</td>
<td>Select the operation that will trigger the alert. Only operations that match the selected resource types are displayed.</td>
</tr>
<tr>
<td>Status</td>
<td>The authorization status for which the alert definition applies.</td>
</tr>
<tr>
<td>Alert Risk Score</td>
<td>Select the risk value of the alert. CloudControl uses this value to prioritize the processing of alert definitions. The lower the risk score value, the higher the priority.</td>
</tr>
<tr>
<td>Threshold Count</td>
<td>Select the number of events that must occur within the Threshold Duration before an alert is generated. The maximum is 1000. To disable, use 0 for both the Threshold Count and Threshold Duration.</td>
</tr>
<tr>
<td>Threshold Duration</td>
<td>The amount of time, in minutes, to wait for the number of events set with the Threshold Count to occur before an alert is generated. The maximum is 1000. To disable, use 0 for both the Threshold Count and Threshold Duration.</td>
</tr>
</tbody>
</table>

*Note:* You must specify values for at least one of the following fields: Roles, Labels, Resource Types, Resource Name, or Status.

5. To enable email for this alert, check the Enable Email checkbox and enter an email address.

6. Click Test Email to send a sample email to the address you entered.

7. Click OK.

**Editing Resource Alert Definitions**

1. Open the Configuration > Alerts page.

2. Click the Resource Alert Definitions tab.

3. Select the alert definition to modify and click Edit.

4. Update the information as necessary. For more information on the fields, see Adding Resource Alert Definitions on the previous page.

5. Click OK.
Viewing Alert Definition Details

There are two ways to view alert definition details:

- Using the Alert Viewer
- Using the Alert Edit page (requires alert configure privilege)

Deleting Alert Definitions

1. Select Configuration > Alerts.
2. Click the ASC Alert Definitions or Resource Alert Definitions tab.
3. Select the alert definition(s) that you want to delete and click Delete.
4. In the Alerts Configuration dialog box, click OK.

Enabling or Disabling Alert Definitions

1. Select Configuration > Alerts.
2. Click the ASC Alert Definitions or Resource Alert Definitions tab.
3. Select the alert definition(s) that you want to enable and click Enable.
4. Select the alert definition(s) that you want to disable and click Disable.

The Enabled column on the Alert Definitions page displays the following information for each alert:

- true—The alert is enabled.
- false—The alert is disabled.

vSphere Operations for Resources

CloudControl offers built-in operations for each of the resource types in vSphere.

<table>
<thead>
<tr>
<th>Operation Resource</th>
<th>Creat</th>
<th>Update</th>
<th>Delete</th>
<th>Copy/Clone</th>
<th>Move/Migrate</th>
<th>Power-on</th>
<th>Power-off</th>
<th>Suspend</th>
<th>Restart</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter</td>
<td>YES</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>YES</td>
</tr>
<tr>
<td>Hosts</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Virtual Machine</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Clusters</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Alert Viewing

You can view the CloudControl alert messages using one of the following:

- the CloudControl Alert Viewer
- email alert notifications
- syslog server

<table>
<thead>
<tr>
<th>Operation Resource</th>
<th>Create</th>
<th>Update</th>
<th>Delete</th>
<th>Copy/Clone</th>
<th>Move/Migrate</th>
<th>Power-on</th>
<th>Power-off</th>
<th>Suspend</th>
<th>Restart</th>
<th>Login</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Centers</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Stores</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Networks</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtual Switches</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Groups</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Virtual Switches</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Distributed Port Groups</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Datacenter Clusters</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Host Storage System Folder</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vApp</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Resource Pool</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Snapshot</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Viewing Alert Messages in CloudControl

The Alert Viewer page displays the CloudControl alert messages in the CloudControl Management Console.

1. Select General > Alert Viewer.
   The top section of the Alert Viewer summarizes the alerts which have been generated. From here, you can use the search field to locate a particular alert, or filter by log priority or risk score.

2. Click on an alert entry in the Date column to populate the Alert Details section on the bottom of the page.

3. Click the Definition tab to view detailed information on the specified alert.

4. Click the Related Alerts tab to view events related to the alert. For example, if you are viewing a Compliance Drift alert, you would see a list of assessment results that caused the alert.

5. Click on an entry in the Date column to view the full assessment information.

Email Notifications

If email notifications are configured and enabled, you can receive alert notifications in email. Each email contains a direct link to the alert in the CloudControl Alert Viewer.

For more information on setting up email alert notifications, see Configuring ASC Alert Definitions on page 99 or Adding Resource Alert Definitions on page 101.

Adding Resource Alert Definitions on page 101Viewing Alert Messages in CloudControl above

Viewing Alerts in the Syslog Server

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

To view alert messages in syslog:

1. SSH into CloudControl as the ascadminuser.

2. Type the following command: view asc.log

3. Type /ALERT to locate the alert messages in the log.

Example:

Mar 26 21:58:49 vc.test.hytrust.com local5:ALERT msgid=ALT0005 app=HTTPS dst=10.222.73.130 src=10.222.73.130 suser=superadmin msg=Generated alert requestedstate= (
"alertType":"ASC","name":"Compliance Drift for HTCC","riskScore":1,"email":"abc@abc.com","operations":"JobRunner","template":"any","ascAlertType" 
:"COMPLIANCE","minFailedOps":1,"actualFailedOps":9)
Using Alerts Examples

CloudControl includes a number of built-in alert definitions for both CloudControl and Resource operations as a starting point for creating custom definitions. This section walks through the process of using the built-in alert definitions as well as creating custom alert definitions.

The examples in this section provide insight into common alert scenarios and may not match your exact requirements and environment.

Example 1—Asset with the PCI or SENSITIVE Label is Deleted

This example shows how to generate an alert whenever an asset (VM, Host, or Network) resource with the PCI or SENSITIVE label is deleted.

1. Enable Alerts—see Configuring Alerts on page 97.
2. Ensure the Critical PCI Assets Deleted built-in alert is enabled—see Enabling or Disabling Alert Definitions on page 103.
3. Assign the PCI or SENSITIVE label to the network, host, or virtual machine asset(s) for which CloudControl will generate an alert if it is deleted.

Make sure to add the labels to the parent network resource for each vSwitch for which you want to generate this alert.

Example 2—Generate an Email Alert Notification when a Login Attempt is Denied

This example shows how to generate an email alert notification whenever a login attempt is denied.

1. Enable Alerts and email notifications—see Configuring Alerts on page 97.
2. Ensure the Denial of Service Attack built-in alert is enabled—see Enabling or Disabling Alert Definitions on page 103.

This built-in alert definition generates an alert, when 10 login attempts—successful or not, occur in the span of a minute on a CloudControl-protected host and sends an email notification of the alert.

Example 3—Asset with the PCI Label is Powered Off

This example shows how to generate an alert whenever an asset (VM, Host, or Network) resource with the 'PCI' label is powered off, shutdown, or stopped.

1. Enable Alerts—see Configuring Alerts.
2. Ensure the Critical PCI Assets Powered Off built-in alert is enabled—see Enabling or Disabling Alert Definitions on page 103.
3. Assign the PCI label to the network, host, or virtual machine asset(s) for which CloudControl will generate an alert when it is powered off.

Example 4—Production Distributed vSwitch Deleted

This example shows how to create a custom alert definition to generate an alert when a distributed vSwitch with the label Production is deleted.
1. Enable Alerts and email notifications—see Configuring Alerts.


3. Configure the following settings:
   - **Name**: Specify a descriptive name (e.g., Production vSwitch deleted).
   - **Labels**: Select the PROD label.
   - **Resource Types**: Select vSwitch.
   - **Operations**: Select Delete.
   - **Status**: Select Permit (alternatively, select Any to be alerted when an attempt to delete a vSwitch occurs).
   - Select the Enable Email checkbox.
   - **Email**: Enter the email address of your network administrator to send the email notification.

3. Assign the PROD label to each production vSwitch for which CloudControl will generate an alert when it is deleted.

Using this custom alert definition causes an alert to be generated and an email notification is sent to the network administrator when a CloudControl-protected production vSwitch is deleted.

**Example 5—Snapshot Overuse**

1. Enable Alerts and email notifications—see Configuring Alerts.


3. Configure the following settings:
   - **Name**: Specify a descriptive name (e.g., Test/Development VM Snapshot abuse).
   - **Labels**: Select the DEV and QA labels.
   - **Resource Types**: Select Snapshot.
   - **Operations**: Select Create/Add.
   - **Status**: Select Permit.
   - **Threshold Count**: Set to 5.
   - **Threshold Duration**: Set to 720.
   - Select the Enable Email check box.
   - **Email**: Enter the email address of your storage administrator to send the email notification.

3. Assign the DEV or QA label to each test or development virtual machine for which CloudControl will generate an alert when it has accumulated 5 snapshots within a 12 hour period.

This custom alert definition causes CloudControl to generate an alert and send an email notification to the storage administrator when a CloudControl-protected test or development virtual machine has accumulated 5 snapshots within a 12 hour period.
Example 6—Compliance Drift

This example shows how to generate an alert whenever the compliance of a host drops below the user-defined threshold.

The built-in Compliance Drift alert definition causes CloudControl to generate an alert whenever compliance assessment fails on any host. This can be customized/made more selective by selecting Hosts with labels, Templates, Minimum Failed Compliance Operations, Alert Risk Score etc.

1. Add a vCenter to CloudControl—see Adding vCenter Server Managed Hosts in the Installation Guide for HyTrust CloudControl.

2. Configure one or more managed hosts see— Configuring Managed Hosts section in the Installation Guide.

3. On the Compliance > Hosts page, select one of the managed hosts and click the Compliance button.

4. On the next page, select Assess as a Compliance Type.

5. Select a template to assess the host against, and click OK. CloudControl runs the selected template on the selected host and lists that template under the Last Run Template column.

Go to the General> Log Viewer page to verify details of the compliance operation.

To see the generated alert, go to the General > Alert Viewer page.
Chapter 8. Secondary Approval

Secondary Approval Overview

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. You must have an Enterprise or appropriate evaluation license to use Secondary Approval.

When a user attempts to perform a vSphere operation that requires secondary approval, CloudControl does the following:

- notifies the requester that approval is needed
- sends an email notification to the approval group that can authorize the request
- adds the request to the pending list
- waits for an authorized user to approve or deny the request

Once a request is approved or denied, CloudControl sends an email notification to the requester and the approver. If you select CC Approvers when configuring Secondary Approval, all members of the approver group will also receive an email notification.

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

By default, only users in the ASC_SuperAdmin role are assigned privileges to configure Secondary Approval and approve Secondary Approval requests. CloudControl uses the following privileges to specify control of Secondary Approval operations:

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asc.SecondaryApproval.Approver</td>
<td>Allows a CloudControl user to approve or deny Secondary Approval requests.</td>
</tr>
<tr>
<td>Asc.SecondaryApproval.Configurer</td>
<td>Allows a CloudControl user to configure Secondary Approval settings and create Secondary Approval controls</td>
</tr>
</tbody>
</table>
Secondary Approval Requirements

Before configuring Secondary Approval, the following are required:

- SMTP notifications must be enabled. For more information, see Configuring Monitoring and Notifications on page 55.
- CloudControl must be in Directory Service mode. For more information, see Authentication on page 18.
- CloudControl must not be in Monitor Mode. For more information, see Disabling Monitor Mode on page 51.
- At least one VM must exist in inventory in addition to vCenters and hosts.
- One or more hosts must be configured in CloudControl before Secondary Approval can be defined.

**Important:** New edge firewall privileges were added for HyTrust CloudControl version 5.2. If you had configured secondary approval for edge firewall operations on previous versions of CloudControl, you must reconfigure secondary approval.

Best Practices for Secondary Approval

To best protect your resources, use the following guidelines when setting up secondary approval controls:

- If you want to require secondary approval on the Delete VM command for a set of VM resources, you should also place secondary approval controls on the following commands:
  - the Delete Folder command for any folder to which the VM belongs
  - the Delete vApp command for any vApp to which the VM belongs

  This ensures that the VMs are not accidentally deleted if any of the parent Folders or vApps are deleted.

- If you want to require secondary approval on the Power Off VM command, you should also place secondary approval controls on the Power Off vApp command for any related vApps.

Configuring Secondary Approval

1. In the CloudControl Management Console, select **Configuration > Secondary Approval**.
   
   **Note:** Before enabling Secondary Approval, only the Configuration tab is visible. After Secondary Approval is enabled, the Secondary Approval Controls tab is visible.

2. Click the **Enable** checkbox to enable Secondary Approval.
   
   **Note:** If the checkbox is not visible, you will see an error message prompting you to configure AD or SMTP.
3. Complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC Approvers</td>
<td>Check the checkbox to send an email notification to all users in the approval group when someone in the group approves or denies a request.</td>
</tr>
<tr>
<td>Default Duration</td>
<td>Enter the default amount of time, in hours, that the user can perform the requested operation. For example, if you set this to 2 hours, and a user requests to migrate a VM, if the request is approved, the user has 2 hours to migrate the VM before their permission is revoked. <strong>Note:</strong> This value can be overridden when an individual request is approved.</td>
</tr>
<tr>
<td>Email Address (FROM)</td>
<td>Enter the email address that you want to be displayed in the From field when a Secondary Approval email is sent.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.

**Creating a Secondary Approval Control**

The secondary approval control allows you to determine what groups and what operations require secondary approval.

1. Select **Configuration > Secondary Approval**.
2. On the Secondary Approval Configuration page, click the **Secondary Approval Controls** tab.
3. Click **Add** to open the Secondary Approval Wizard.
4. On the Select Requestor Groups page, select the group(s) for which this Secondary Approval control applies. Users in the selected groups will require secondary approval to perform certain operations.
   
   Only AD groups which are mapped to a CloudControl role are displayed.
5. Click **Next**.
6. On the Select Operations page, select the compute or network operation(s) to which this Secondary Approval control applies.
7. Click **Next**.
8. On the Select Resources page, select the resources to which this Secondary Approval rule applies and click **Next**.
9. On the Select Approver Groups, select the checkbox next to the AD groups whose users can approve the operations in this rule.
   
   Only AD groups associated with CloudControl roles that have the Secondary Approval/Approver privilege appear.
10. Enter the email address or email list where CloudControl sends approval requests.
11. Click **Next**.
12. On the Secondary Approval Control Summary page, verify the Secondary Approval control selections and click **Finish**.
**Viewing Secondary Approval Controls**

All existing secondary approval controls are displayed on the Secondary Approval Controls tab on the Secondary Approval Configuration page. From here, you can:

- Click the Requestors link to view the full details of the secondary approval control.
- Check the checkbox for a secondary approval control and click **Edit** to update the settings.
- Check the checkbox for a secondary approval control and click **Delete** to delete the secondary approval control.
- Check the checkbox for a secondary approval control and click **Enable** to enable the secondary approval control. **Note**: When first created, secondary approval controls are enabled by default.
- Check the checkbox for a secondary approval control and click **Disable** to disable the secondary approval control without deleting it.

**List of Secondary Approval Operations**

CloudControl allows you to place secondary approval controls on the following operations:

**Compute Operations (Operations on VMs, vApps, Folders)**

- **Clone VM**—Clone a Virtual Machine.
- **Create VM**—Create a Virtual Machine.
- **Delete All VM Snapshots**—Delete all the snapshots associated with a virtual machine.
- **Delete Folder**—Delete a folder.
- **Delete VM from Disk**—Delete a virtual machine and removes all its related files from disk.
- **Delete VM from Inventory**—Unregister a virtual machine from the vCenter inventory, leaving all its files on disk.
- **Delete a VM Snapshot**—Delete a single virtual machine snapshot.
- **Delete vApp from Disk**—Delete a vApp and removes all relates files from disk.
- **Delete vApp from Inventory**—Unregister a vApp from the vCenter inventory, leaving all its related files on disk.
- **Edit VM Settings**—Edit virtual machine settings such as memory, CPU, and NICs etc.
- **Migrate VM**—Migrate a virtual machine to a different host.
- **Move Cluster**—Move a cluster to a different location.
- **Move Folder**—Move a folder to a different folder.
- **Move VM from a Folder**—Move a virtual machine from its current folder to another folder.
- **Move vApp**—Move a vApp to another folder.
List of Secondary Approval Operations

- **Open VM Console**—Opens a web console.
  
  *Note:* VMRC is not supported by secondary approval.

- **Power Off VM**—Power off a virtual machine.

- **Power Off vApp**—Power off all the virtual machines associated with a vApp.

- **Power On VM**—Power on a virtual machine.

- **Restart VM Guest**—Restart a virtual machine guest OS.

- **Revert VM to Snapshot**—Revert a virtual machine to any of its existing snapshots.

- **Shutdown VM Guest**—Shutdown a virtual machine guest OS.

- **Shutdown vApp**—Shut down the OS of all virtual machines associated with a vApp.

- **Suspend VM**—Suspend a virtual machine from running.

- **Suspend vApp**—Suspend all the virtual machines in the vApp from running.

**Network (NSX) Operations**

*Note:* Network operations are only visible if NSX is installed.

- **Assign Security Policy**—Assign a security policy.

- **Create DHCP**—Enable a DHCP server on an edge services gateway.

- **Create Edge Firewall**—Create an edge firewall.

- **Create Edge Firewall Rule**—Create an edge firewall rule.

- **Create Edge Service Gateway**—Create an edge services gateway.

- **Create Firewall**—Create a distributed firewall.

- **Create IPsec**—Create an IPsec on an edge services gateway.

- **Create Load Balancer**—Enable a load balancer on an edge services gateway.

- **Create Object Group**—Enable an Object Group.

- **Create Security Policy**—Enable a Security Policy.

- **Create VPN**—Create a VPN on an edge services gateway.

- **Delete DHCP**—Disable a DHCP server on an edge services gateway.

- **Delete Edge Firewall**—Delete an edge firewall.

- **Delete Edge Firewall Rule**—Delete an edge firewall rule.

- **Delete Edge Services Gateway**—Delete an edge services gateway.

- **Delete Firewall**—Delete a distributed firewall.

- **Delete IPsec**—Delete an IPsec on an edge services gateway.
• Delete Object Group—Delete an Object Group.
• Delete Security Policy—Delete a Security Policy.
• Delete Load Balancer—Disable a load balancer on an edge services gateway.
• Delete VPN—Delete a VPN on an edge services gateway.
• Edit DHCP—Edit properties of a DHCP server on an edge services gateway.
• Edit Edge Firewall—Edit properties of an edge firewall.
• Edit Edge Firewall Rule—Edit an edge firewall rule.
• Edit Edge Services Gateway—Edit general properties of an edge services gateway.
• Edit Firewall—Edit a distributed firewall.
• Edit IPsec—Edit an IPsec on an edge services gateway.
• Edit Load Balancer—Edit a load balancer properties on an edge services gateway.
• Edit Object Group—Edit an Object Group.
• Edit Security Policy—Edit a Security Policy.
• Edit VPN—Edit a VPN on an edge services gateway.

Pending Secondary Approval Requests

All secondary approval requests are displayed on the Policy > Secondary Approval Requests page. Users with the appropriate permissions can deny or approve these requests. Each request displays the following information:

• Requestor—The user who initiated the request. Click on a Requestor to display the approve or deny request page.
• Resource—The resource the user was attempting to use.
• Operation—The operation the user was attempting to perform.
• Approver Groups—The user group whose members can approve or deny the request.
• Request Time—The date and time the request was initiated.
• Status—Shows the request is pending approval.

Note: Only users in the authorized approver group for the request which triggered the control can see a request.

Approving a Pending Request

2. On the Secondary Approval Requests page, click the Pending Requests tab.
3. Check the checkbox for the request that you want to approve and click Approve.
4. On the Secondary Approval Requests page, click the Approve radio button.
5. Enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start</td>
<td>Enter the date and time when the approval window will start.</td>
</tr>
<tr>
<td>Duration (Hours)</td>
<td>Enter the number of hours that the approval window will last. The default value is the duration that you entered when you configured Secondary Approval.</td>
</tr>
<tr>
<td>Permitted Operation Count</td>
<td>The number of times this operation is permitted within the given duration. The valid range is 0-100, with 0 being unlimited.</td>
</tr>
<tr>
<td>Email</td>
<td>The email field is pre-populated with the requestor’s email address. If necessary, enter a different or additional email addresses.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter any optional comments regarding this request.</td>
</tr>
</tbody>
</table>

Note: If you received a Request for Secondary Approval email notification, clicking the link will take you directly to this page.

6. Click Apply.

An email is sent to the requestor and the approver that indicates that the request was approved. If you selected CC Approvers when you configured Secondary Approval, all members of the approver group will also receive an email.

Denying a Pending Request

2. On the Secondary Approval Requests page, click the Pending Requests tab.
3. Check the checkbox for the request that you want to deny and click Deny.
4. On the Secondary Approval Requests page, click the Deny radio button.
5. If necessary, update the Email field. This field is pre-populated with the requestor’s email address.
6. Enter any optional comments regarding this request.
7. Click Apply.

An email is sent to the requestor and the approver that indicates that the request was denied. If you selected CC Approvers when you configured Secondary Approval, all members of the approver group will also receive an email.

Viewing Request History

2. On the Secondary Approval Requests page, click the History tab.
3. Click the link for the request that you want to view.
   The Secondary Approval Details page displays the full request details, including the requestor, requested operation, approver, and whether the request was approved or denied.
Chapter 9. Dashboard Management

Using the CloudControl Appliance Dashboard ................................................................. 116
Admin Access Dashboard .................................................................................................... 117
Compliance Dashboard ....................................................................................................... 120
Protection Dashboard .......................................................................................................... 123
Recent Activity Dashboard ................................................................................................. 126
Appliance Health ................................................................................................................. 128

Using the CloudControl Appliance Dashboard

The appliance dashboard displays the following security widgets:

- Compliance—Displays host compliance to currently enforced templates.
- Admin Access—Displays the number of administrators per category
- Protection—Displays resources and whether they are protected by RBAC policies.

Click the close button to remove widgets from the main display area. When closed, the widgets are represented by icons on the sidebar. Click the sidebar icon to return the widget to the main display area.

When displayed, each widget has the four following buttons in its title bar:

- Show Summary—Displays a visual graphic of current state and trending chart over time. This is the default display for each widget.
- Show Details—Displays information to drill down further for more information regarding the particular security posture metric.
- Help—Displays popup with description of the security metric represented by the widget.
- Close—Returns the widget to the selection bar.

The Admin Access dashboard and Compliance dashboard widgets also have enhanced configuration controls. You can configure a minimum and maximum range to control what their desired state is supposed to be in order to see how this changes over time in the trending charts.

You can export the graphical summaries on all open widgets to PDF. Close a widget if you do not want to include it in the PDF.

From the Details views, you can export all visible columns to a CSV file.

Note: Viewing the dashboard requires the Management.Dashboard.View privilege. Additionally, the Asc.ArcView privilege is required to view the compliance drill-down information for the Compliance widget.
Admin Access Dashboard

Use the Admin Access Dashboard to view the number of administrators per category in order to understand the distribution of access in the virtual environment applicable to the resources managed by CloudControl.

- In most cases, the admin category is assigned based on which category the user has the highest percentage of privileges. For example, if a user has 30% of the management operations available, but only one or two available in other categories, the user will be assigned as a Management Admin.
- Super Admin is assigned when a user has privileges for over 75% of the total number of operations in all categories.
- Power Admin is assigned when a user has privileges for over 25% of the total number of operations in at least two categories.

The donut chart represents all users with the privilege to perform admin operations in the current state, divided into six possible sectors. Admin operations involve managing the separation of duties by creating, updating, or deleting resources. Read operations are not considered when categorizing users. For more information, see Separation of Duties on page 89.

Four of the sectors are composed of users that primarily have privilege to perform admin operations involving one of the following resource categories:

- Network resources
- Management system resources
- Compute resources
- Storage resources

The two additional sectors involve multiple resource categories:

- **PowerAdmins**: Administrators that primarily have privileges to perform admin operations involving resources in more than one resource category.
- **SuperAdmins**: Administrators mapped to a role that contains a full set of privileges (super-set) as defined by the vendor (VMware).
The administrator groups are calculated based on synching with the current Directory Service setup and the policy mapping enforced in CloudControl such as group-to-role mappings and rules created.

Sector size is defined by the percent of administrators that have been categorized to a particular administrator category. Labels on the sectors specify the number of administrators in that group.

The legend displays the color and group name for each type of administrator. Clicking on a sector will direct the user to the details panel that displays the list of administrators filtered by that sector’s resource group. For example, clicking the PowerAdmin sector of the donut chart shows the details about all the users in the PowerAdmin category.

The configuration control for Admin Access Dashboard is the Acceptable Range Configuration. This allows the user to set the acceptable number of PowerAdmins and SuperAdmins. If the number of PowerAdmins or SuperAdmins is out of the specified range, the donut chart will have a (f) icon in its center — hovering over the icon displays the Out of range message.
The donut chart displays the results from the most current Directory Service synchronization. In order to refresh this information, the user must trigger the synchronization by clicking the **Start Directory Service Sync now** refresh button. CloudControl prevents the synchronization event from running more often than 15 minutes in order to prevent the domain controller in Active Directory from being overwhelmed with queries from CloudControl.

Similar to scheduled compliance events, the Directory Service synchronization is a configurable scheduled event that can run with a frequency between every 15 minutes to once daily. However, if the CloudControl console is restarted or shut off, the **Admin Access Directory Service** is synced as soon as CloudControl is powered on again.

### Trending

The trending graph shows the admin counts per category over time, where each line represents change in the number of admins in a particular category. The data begins from the time CloudControl was deployed or upgraded to 5.0.

The horizontal axis is date and the vertical axis is the count of admins per category. The legend in the center of the widget corresponds to the categories in both the current state (donut chart) and trending graph.

![Admin distribution over time](image)

**Admin Categories**
- PowerAdmin
- Compute
- Storage
- Network
- Management
- SuperAdmin

Trending Chart with Admin Count Out of Range

The Acceptable Range Configuration control allows the user to set a minimum and maximum number of PowerAdmin and SuperAdmin users. If, at a given unit of time, there are too few or too many PowerAdmin or SuperAdmin users, the navigator chart will be yellow. When the number of these users is within the specified range, the navigator chart will be green.

### Details

The details panel shows each user, which groups the user belongs to, the roles assigned to the user, the admin's category, and the user's number of operations per admin category. The Privileged operations per category for each user are the unique operations per category. If a user is mapped to two roles, a particular operation is counted only once even if both roles have that operation.
Admin Access - Classification of Admins based on their access privileges

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
<th>Role</th>
<th>Privilege.</th>
<th>Operation Category</th>
<th>Applicable Resource Type</th>
<th>Privileged operations per category</th>
</tr>
</thead>
<tbody>
<tr>
<td>appadmin</td>
<td>testH_T_AppAdmin</td>
<td>ASC_AppAdmin</td>
<td>Management Admin</td>
<td>0</td>
<td>37</td>
<td>0 0</td>
</tr>
<tr>
<td>arcadmin</td>
<td>testH_T_ARCAadmin</td>
<td>ASC_ARCAadmin</td>
<td>Management Admin</td>
<td>0</td>
<td>27</td>
<td>0 0</td>
</tr>
<tr>
<td>accesasstor</td>
<td>testH_T_ARCAsstor</td>
<td>ASC_ARCAsstor</td>
<td>Management Admin</td>
<td>0</td>
<td>2</td>
<td>0 0</td>
</tr>
<tr>
<td>backupadmin</td>
<td>testH_T_BackupAdmin</td>
<td>ASC_BackupAdmin</td>
<td>Power Admin</td>
<td>57</td>
<td>28</td>
<td>24 2</td>
</tr>
<tr>
<td>coreappadmin</td>
<td>testH_T_CoreAppAdmin</td>
<td>ASC_CoreAppAdmin</td>
<td>Storage Admin</td>
<td>41</td>
<td>26</td>
<td>12 2</td>
</tr>
<tr>
<td>coreadmin</td>
<td>testH_T_DCAdmin</td>
<td>ASC_DCAdmin</td>
<td>Power Admin</td>
<td>286</td>
<td>112</td>
<td>47 63</td>
</tr>
<tr>
<td>esxadmin</td>
<td>testH_T_ESXAdmin</td>
<td>ASC_ESXAdmin</td>
<td>Power Admin</td>
<td>154</td>
<td>53</td>
<td>31 28</td>
</tr>
<tr>
<td>esxadmin</td>
<td>testH_T_ESXAdmin</td>
<td>ASC_ESXAdmin</td>
<td>Power Admin</td>
<td>114</td>
<td>103</td>
<td>88 15</td>
</tr>
</tbody>
</table>

Admin Access Dashboard Details Panel

Clicking on a cell in the Role column will open up a new tab to the right of the Users tab, titled the name of the role. This tab displays the operations that are contributing to that user’s currently mapped admin category. Multiple Role panels can be added to the Admin Access Dashboard Details Panel at once, and can be exited by clicking the (x) on the tab.

The columns in each Role panel are:
- Operation.
- Vendor Name.
- Privilege.
- Operation Category.
- Applicable Resource Type.

All columns can be reordered and sorted for easier data manipulation.

See Access Policies on page 75 for more information on how users are mapped to groups in the directory service, and how policies are created on these groups.

Compliance Dashboard

Users can view the current and trending state of their virtual infrastructure’s hosts compliance in regards to their currently enforced templates. A template is enforced if it is associated with a host’s last compliance event (either assessment or remediation). For more information on the compliance of hosts and administrator use cases, see Compliance on page 65.

Current State

The current state of compliance is represented by the number of hosts that are in compliance with an enforced template, noncompliant with an enforced template, or haven’t had any form of compliance assessment yet. You can also filter by Host Type or Label to further limit what hosts are displayed.
Compliance Dashboard

The summary display shows a donut chart that represents all the hosts divided into 3 possible sectors.

- **Compliant**: hosts that are 100% compliant with the template enforced
- **Noncompliant**: hosts that are less than 100% compliant with the template enforced
- **Unassessed**: hosts that have had no form of assessment or remediation performed on them

Each sector size is defined by the percent of hosts that are Compliant, Noncompliant or Unassessed out of the total number of hosts.

Clicking on a sector will open the details panel that displays the hosts that contributed to the selected sector.

For example, clicking on the **Compliant** sector displays compliant hosts information in the Details panel as shown below.

Similar to the Admin Access donut chart, a warning sign can appear on the Compliance donut chart, when the overall hosts compliance is below the configured compliance goal.

**Details**

The Compliance > Details panel displays data about the current state of all the hosts, depending on the last template run on each.
Compliance Dashboard

- Hostname
- Host Type
- Version
- Label
- Last Run Template
- Last Run (as a timestamp)
- Compliance (as a percentage — %)
- Status

Data can be filtered by the above fields, excluding Last Run and Compliance Percentage. Also, data can be sorted by Hostname, Host Type, and Version.

Click the Last Run link to view a list of all operations and their result. Click the icon in the History column to view the Compliance History page. For more information, see Compliance History on page 70.

Trending

The representation for the compliance over time displays the percentage of compliance for all applicable hosts since CloudControl was freshly installed or upgraded.

This component is a stacked area graph where the y-axis is a percentage (0-100) and the x-axis is time. The line represents the change in percentage of compliant, noncompliant, and unassessed hosts out of the total number of hosts from the time CloudControl was deployed. The user can define the scheduled event frequency, which ranges from every 15 minutes to once a day, using the Compliance > Scheduled Events tab. The event is titled “Trending Compliance.”
As reflected in the Compliance Dashboard figure above, the donut represents the current compliance state of hosts, where current is time-relevant because the data for the chart is pulled from the last scheduled compliance event.

If an assessed host becomes unreachable or is made unprotected through the CloudControl console, its compliance state displays the results from the last compliance event run, which could be assessment or remediation.

In the Compliance title bar, the Compliance Goal Configuration control allows the user to determine their desired compliance goal. If, at a given unit of time, the overall hosts compliance is below the compliance goal, the navigator color will be yellow; otherwise it will be green.

Protection Dashboard

This dashboard specifies Role Based Access Control. If a resource is shown as protected in this dashboard, it means that the resource has access control enforced, based on the CloudControl policy’s user-role configuration. Users can view the percentage of protected and unprotected resources, where the green section of each bar represents the percentage of protected resources in that category and the red section of each bar represents the percentage of unprotected resources. The number in the center of each colored section displays the number of hosts in that section.

For example, in the figure Protection Dashboard below, the far left bar, 18 is the number of protected resources in the Compute category. These groups match the four resource groups that administrators have access to, as visible in the Admin Access Dashboard. See also, Compute, Management, Network, and Storage.
Protection Dashboard

The data collection for this dashboard is also a scheduled event titled Trending RBAC Protection, like Directory Service Sync (for the Admin Access Dashboard) and Trending Compliance.

This scheduled event can be configured in Compliance > Scheduled Events. Trending RBAC Protection can also run at intervals from every 15 minutes to once a day.

Clicking on a section of the bar graph will redirect to the Details panel, showing data filtered on the specific resource group (represented in the bar graph), and will list resources protected under all applicable CloudControl Controls or unprotected under at least one CloudControl Control. For example, clicking on the Protected section of the Network bar will display.

![Protection - Classification of resources based on whether they are protected with RBAC policy](image)

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network</td>
<td>PortCollection</td>
<td>true</td>
</tr>
<tr>
<td>Management Network</td>
<td>PortCollection</td>
<td>true</td>
</tr>
<tr>
<td>VM Network</td>
<td>PortCollection</td>
<td>true</td>
</tr>
<tr>
<td>VM Network</td>
<td>PortCollection</td>
<td>true</td>
</tr>
<tr>
<td>uLAN 2694-DPortGroup</td>
<td>PortCollection</td>
<td>true</td>
</tr>
<tr>
<td>uLAN 2694-DPortGroup</td>
<td>PortCollection</td>
<td>true</td>
</tr>
</tbody>
</table>

Click Resources on Bar Graph for Details

**Trending**

The representation for Protection over time displays the change in percentage of protected resources for each group for all applicable hosts since CloudControl was freshly installed or upgraded. Each colored line represents a separate group, according to the legend.
**Protection Dashboard**

**Trending Number of Protected Resources by Category**

Each time the **Trending RBAC Protection** scheduled event runs, the counts for the resource categories will be plotted on the trending chart.

**Details**

This table lists out resources from one of the four resource groups, and their protection status under each applicable CloudControl Control. Each of the resource groups has a selection of different subgroups to classify the resources, as listed below:

- **Compute**: VirtualMachine, HostSystem, ResourcePool, HostSystemCollection
- **Management**: ManagementSystem
- **Network**: SDNController, NetworkServiceContainer, Firewall, IPSec, Switch, VPNServer, LoadBalancer, DHCPServer, Router, NetworkSystemCollection
- **Storage**: DataStore, StorageSystemCollection
Recent Activity Dashboard

Navigate to this dashboard by selecting **Recent > Activity** to the left of the Overview tab on the General Dashboard. This tab displays up to four recent activity widgets. Each widget displays a heatmap for filtered log messages. The default widgets are:

- **Users**: filtered by most active user in the environment.
- **Actions**: filtered by most performed action.
- **Resources**: filtered by most accessed resource.

You can modify the default widgets by adding filters as necessary and by revising the name.
Recent Activity Dashboard

Customized widgets can be added by clicking the (+) symbol on the empty widget, which is located at the bottom of the Recent Activity tab.

Clicking on the (+) sign will open a customizable widget, where the user must enter a unique title and can add filters. When filters are not applied, the new widget shows a heatmap for all log messages. When a filter is applied the widget will show a heatmap for the log messages defined by the filter.

In all widgets, hovering over a square in the heatmap (where each square represents a day) will display the date and number of log messages recorded on that day. Hovering over a day on which no log messages were recorded only displays the date. Click on a colored square (indicating activity) to redirect to the Log Viewer, with the same filters applied and the date/time range according to the selected date: from the start to the end of the day selected in the Recent Activity widget.
Appliance Health

Custom Recent Activity Widget + Hover to See Number of Daily Logs

All widgets can be closed (removed from the display) by clicking the (x) in the title bar. This will save the filter and return the widget to the collapsible selection bar on the right. Dragging closed widgets from the selection bar to the display will open them. Although only four widgets can be displayed at a time, users can have more than four widget icons in the selection bar. If you mouse-over the widgets in the selection bar, you can see what filters are being used.

**Note:** Click the Trash icon in the title bar to delete the widget without saving its configuration.

**Appliance Health**

Open the **General > Health** page to view a summary about the environment and state of CloudControl. The **Appliance Health** page consists of the following sections:

- **General**—Displays general information, including the hostname, installed software version, the management IP address, policy enforcement status, and whether or not the Vitals Service is enabled.
  
  The Policy field displays Enforced if you are running CloudControl normally, and Monitor if you are running in Monitor Mode. For more information, see **Configuring Monitor Mode** on page 50.
  
  For more information on the Vitals Service see **Using the HyTrust Vitals Service** on page 147.

- **License Information**—Displays license information, including the customer name, entitlement number, status, type, the number of protected and licensed hosts and sockets allowed, and maintenance and support expiration dates. For more information see **Licenses** on page 145.

- **Services**—Displays the status of all CloudControl related services, including **Appliance Health and Logging Service Alerts** on page 140.
Appliance Health

- **Resources**—Displays the state and usage of resources in CloudControl, including CPU, disk and memory usage, certificates, and network status. CloudControl administrators can monitor system usage and take appropriate actions as needed.

  The Backup and Restore field displays the following:
  - Disabled—Indicates that a backup has never been run. Once you create a backup, this will change to Healthy.
  - Healthy—A backup has been successfully made, and if you are using RPV, the backup is more recent than the last RPV rotation.
  - Warning—The backup is older than the last RPV rotation. Create a new backup to return to Healthy state.

  The CPU Usage, Disk Usage, and Memory Usage fields display a green bar with the percentage used. Click the green bars to view detailed graphs that display usage by day, week, month and year.
Log Viewer Overview

The **General > Log Viewer** dashboard displays CloudControl log messages from the CloudControl Management Console. Log messages classify and describe all administrative actions and events that have taken place in the virtual infrastructure.

There are four parts to the Log Viewer:

- Filters
- Heatmap
- Leaderboard
- Log Messages
Filters

Log messages can be filtered by any of the Column fields, which are listed in the drop down menu when clicking on the Column search bar. These fields match the options for columns on the Log Messages grid.

- Clicking on the Value search bar will display a list of any defined or suggested values for the selected column field; this list is updated as the user types.
- Clicking on the (=) will toggle between equals and does not equal. Adding a filter will alter all the other features on the Log Viewer: the heatmap, leaderboard and message table are all affected by the conditions specified in the filter(s).

Filter by Column field

By default, the system filters are applied, but filters can be toggled by clicking the Filter out system messages button (see the top-center button in the Filter by Column field figure shown below). Multiple filters can be applied, including multiple from the same Column field. Filters can be deleted by clicking the (x) next to the column field or the value, if it exists.
Heatmap

The heatmap shows daily activity by representing the number of logs on a particular day with a colored square corresponding to high or low activity. Squares representing days are grey when there is no activity, and lie on a color gradient from green to red if there is any activity.

Heatmap View Mode

Click one of the following to change how you view the heatmap:

- 6 months—Displays six months at a time. Each cell is equivalent to one day, and the current day is outlined in red.
  
  Hovering over a square in the heatmap will display the day of the week, date, and number of log messages recorded on that day, if any (as defined by the filters applied). Clicking on a square will update the leaderboard and log messages to display only the details for that specific day.

- 7 days—Displays seven days at a time. Each cell is equivalent to one hour, and the current hour (in 24-hour notation) is outlined in red.
  
  Hovering over a square in the heatmap will display the hour, date, and number of log messages recorded in that hour, if any (as defined by the filters applied). Clicking on a square will update the leaderboard and log messages to display only the details for that specific hour.

Heatmap Legend:

The heatmap legend is available only when the view mode is set to 6 months. By default, the color gradient is spread out to represent a number of ranges:

- Less than 20 log messages
- Between 20 to 40 log messages
- 40 to 80
- 80 to 120
- 120 to 200
- More than 200 messages

To configure the heatmap legend:
1. Click the **Settings** icon and choose one of the following:
   - Use default legend - the provided out of box ranges will be used;
   - Use previous week - this option is available after CloudControl has been deployed for at least 7 days. If the user decides that previous week log counts are normal, he/she can choose this option and as a result new ranges will be generated for the legend.
   - Select "normal" range - the user can select any other date range that is at least 7 days long.

2. Click **OK**.
   The heatmap colors change according to your selection.

---

**Leaderboard**

The leaderboard displays the top 5 most active users, top 5 most frequently done actions and top 5 most accessed resources based on the content of the log (with applied filters).

<table>
<thead>
<tr>
<th>Top Users</th>
<th>superadminuser</th>
<th>superadmin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top Actions</td>
<td>ScheduledEvent</td>
<td>Ho... Ge...</td>
</tr>
<tr>
<td>Top Resources</td>
<td>HyTrust CloudControl Dashboard Service</td>
<td>Appliance A... 1...</td>
</tr>
</tbody>
</table>

Leaderboard + Hover for Number of Messages

Hovering over a user, action, or resource in the leaderboard will display the number of filtered log messages associated with it. Clicking on a user, action, or resource will add it as a filter. For example, clicking on superadminuser in the leaderboard will add a filter for **User = superadminuser** to the previously applied filters.

---

**Log Messages**

The Log Message table displays all messages (as restricted by filters) with the following default fields:

- Date
- Priority
- User
- Action
- Resource Name
- Status
Users can select which fields they would like as columns. All column options are displayed in the Table Options menu, on the top right corner of the grid. These fields match the **Column Field** options when creating filters.

Users can sort the table alphabetically in ascending or descending order, by clicking on any column header. Hovering over the date and time pickers above the table will display an option to show all messages or filter to the last hour, day or week. If a square on the heatmap has been clicked, the Log Message table will be filtered to that day.

Log Messages filtered to 08/20/2016 + Filter by date options

Each log message is condensed into the grid, but can be clicked on to expand. The detailed view shows all of the information for a log message, including the ones not visible in the table. To navigate away from the detailed log message, clicking the circular grey **Scroll to Top** widget brings the display back to the top of the **Log Viewer** page.

Clicking on a log message in the table will automatically scroll down the page to the Details area. To disable the auto-scroll, go to the table menu and deselect the "Auto-scroll to details" option.

A user can click on the log message tabs for more detailed information on Prior/Requested Delta, Prior/Requested State, and Payload data.
Saving Filters

You can save filters that you create in the log viewer.

1. Select **General > Log Viewer**.
2. On the Log Viewer page, set up the filter that you want to save.
3. Click **Save filters** to add the filter to the Saved Filters list.
4. Click **Saved Filters** and select a filter that you saved to verify.
5. To remove saved filters from the list, click **Saved Filters** and click the x next to the filter.
6. Click **Clear filters** to clear the current filter from the buffer.
Exporting Log Files to CSV

You can export up to 1000 records at a time. If you have more than 1000 log files, use the filters and date range to reduce the number of records.

1. Select General > Log Viewer.
2. On the Log Viewer page, set up filters or use saved filters to limit the data that you want to export.
3. Click the Table Options icon and select Export to CSV.
   If you have too many log files, you will be prompted to reduce the number of records.

Logging Overview

Logs provide a record of the events occurring within the virtual infrastructure. The CloudControl logs are useful for performing auditing, forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends. Plus a user can assess long-term problems pertaining to the virtual infrastructure security, compliance monitoring, and enforcement.

Individual log entries contain information related to a specific event that has occurred within a system or network. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems.

Log messages generally contain a date and time stamp, hostname, priority, a message ID, and additional information describing who performed (or tried to perform) an action, from what location, to what target object.

CloudControl log messages have the following format:
Date: Host: Priority: Message ID: Message

Logs retrieved from a vCenter Server have the following format:
Date(posted): Date(event) VC: Host: Message (as logged by vCenter)

   Note: By default, vCenter Server events are not sent to CloudControl. You can enable the Get vCenter events scheduled event from the Compliance > Scheduled Events page to update the CloudControl log with events from all protected vCenter Servers. While CloudControl has a comprehensive view of all user initiated vSphere operations in the virtual infrastructure, importing vCenter Server events may be useful for completeness and to include automated events such as DRS.

For information on the log level classifications, see Syslog Severity Level Classifications on page 160.

All local log files generated on the CloudControl host are stored in the /var/log/asc directory, even if CloudControl is configured to export logs to an external syslog server.

Log Retention Timeframes and Log Rotation

The minimum log retention value is 7 and the default is set to the maximum, which is 180 days.

Log files are rotated when they reach their maximum allotted size.
Appliance and Host Logging

By default, CloudControl stores aggregated syslog files locally. However, you can configure CloudControl to send its logs to an external syslog server, which you can specify by IP address. All local CloudControl log files are stored in the /var/log/asc directory. The /var/log directory is configured as a separate virtual disk per CIS benchmark recommendations for ESXi hosts.

Log files are rotated when they reach their maximum allotted size. If you set the log level to include debug messages, the logs and log rate increases significantly. The CloudControl-specific logs may be downloaded or purged. For CloudControl-protected ESXi hosts, you can specify options to store logs on the host (local), or you can choose to send the logs to an explicit syslog server. The default is to log messages in a file stored locally on each host.

You may explicitly set up individual host logging locations and set individual host logging options when you initially add a host to be protected by CloudControl (use the Advanced tab on the Add Host page). You can also go back later to select a host from the Edit Host page (Compliance > Hosts) and modify its current logging location.

Note: The Syslog Server setting on the Advanced tab of the Add/Edit Host page will override the Syslog Server setting under the Host Default Logging Configuration section on the Configuration > Logging page.

You can use the ASC-vsphere-0007 operation in a template (Compliance > Templates) to set up logging to a remote logging server. To learn more about deploying security templates, see Host Configuration Templates on page 70.

For details on the Logging Configuration page settings see Configuring CloudControl Logging on the next page, Host Default Logging Configuration on page 139 and Managing Logging Retention Configuration on page 139.

For details on the states associated with Logging, see Appliance Health and Logging Service Alerts on page 140.

Syslog in CloudControl

CloudControl uses syslog for logging. You can configuring individual syslog servers on the Logging page.

Note: If you want to configure multiple syslog servers, you must use the CLI. For more information, see asc log on page 204.

Syslog traffic will be outbound from the management IP address of the primary or standalone node. However, if the VIP is configured, then the syslog traffic will use the VIP instead.

For non-encrypted syslog, the port number is 514/UDP. If you use encrypted syslog, the default port number is 6514/TCP.

Note: You cannot modify any port numbers in the CloudControl GUI. You can change the port number for TCP (for encrypted syslog only) using the asc log --targetPort <port_number> command in the CLI.

Encrypting Syslog

Encrypting syslog requires a Rsyslog certificate, a certificate authority, and an RSA private key.
1. Generate a CSR for the Rsyslog certificate:
   a. Select **Configuration > Certificates**.
   b. Click the Services tab, and click the Rsyslog service.
   c. On the Certificate Details page, click **Generate CSR**.
   d. Update the properties in the Certificate Subject Field Configuration section, and click **OK**.
      **Note:** When you generate a CSR, the CloudControl private key is automatically used.

2. Submit the CSR to a Certificate Authority (CA) to have it issue a certificate. The certificate authority should be the same as the one you are using for CloudControl.

3. Import the new certificate:
   a. Select **Configuration > Certificates**.
   b. Click the Services tab, and click the Rsyslog service.
   c. On the Certificate Details page, click **Install**.
   d. Import the certificate file or paste the certificate data into the field.
   e. Click **OK**.

   Alternatively, you can do one of the following:
   - On the Certificate Details page for Rsyslog, click **Install**. Paste the contents of your Rsyslog certificate, the CA for that certificate (and, if applicable, the intermediate CA), and its RSA private key into the window and click **OK**.
   - On the Certificate Details page for Rsyslog, click **Import**. Upload a single file that contains the certificate, the CA for that certificate (and, if applicable, the intermediate CA), and its RSA private key and click **OK**.

**What to Do Next**
Configure your encrypted syslog server. See **Configuring CloudControl Logging** below.

**Configuring CloudControl Logging**

To specify the CloudControl and ESXi Host default logging configurations:

1. Select **Configuration > Logging**.
2. On the Logging Configuration page, configure the logging levels in the HTCC Logging Configuration area:
   - **Logging Level**—Set the level of logging to capture. Levels are FATAL, ERROR, WARN, INFO, and DEBUG. For more information, see Syslog Severity Level Classifications on page 160.
   - **CloudControl Logging Aggregation**—Specify whether the CloudControl aggregated syslog files are stored locally (the default) or sent to an external syslog server.
     If you selected External, select or enter values for the following fields:
     - **CloudControl Logging Aggregation Template Type**—Choose the logging format type, HyTrust Proprietary or Common Event Format (CEF).
     - **CloudControl Syslog Servers**—Enter a comma-separated list of external syslog server IP addresses.
     - **Encrypt Syslog**—Enable (selected) or disable (deselected) TLS authentication encryption for messages sent to the external syslog server.
   - **Manage Logs**—Click the Download button to download the CloudControl log files.

3. In the Default Logging Aggregation area, choose your Default Logging Aggregation:
   - **Local**—Log files for CloudControl-protected hosts are stored locally.
   - **Explicit Syslog Server**—Log files are sent to an external syslog server.

4. If you selected Explicit Syslog Server, enter the IP address or hostname for the external syslog server.
   **Important:** Do not enter a port number. CloudControl uses 6514/TCP by default for encrypted syslog. You can change the port number using the CLI. See asc log on page 204.

5. Configure the default logging aggregation locations. For more information, see Managing Logging Retention Configuration below.

6. Click **Apply**.

---

**Host Default Logging Configuration**

The following fields are available in the Host Default Logging Configuration section on the Configuration > Logging page:

- **Default Logging Aggregation**—Specify whether CloudControl-protected hosts store log files locally (the default) or send them to an external syslog server.

The following field is available for external syslog servers:

- **Default Syslog Server**—The IP address of the external syslog server. This field is only available if hosts send log files to an external syslog server.

---

**Managing Logging Retention Configuration**

You can configure how long-long logs are retained by setting the minimum number of days to maintain logs. The default minimum is 7 days and the maximum is 180 days.

CloudControl automatically purges logs every day according to the number of days you set. However, you can run the purge job at any time.
Changing the Log Retention

1. Select **Configuration > Logging**.
2. In the Log message retention period (Days) field, set the number of days that you want to purge every day.
3. Click **Apply**.
   The number of days will be purged the next time the daily scheduled event runs.

Purging Logs Immediately

1. Select **Configuration > Logging**.
2. In the Log message retention period (Days) field, set the number of days that you want to purge.
3. Click **Purge Logs**.
   The number of days that you set will be purged immediately. However, the value will not be saved and used for the daily scheduled event unless you click the **Apply** button.

Appliance Health and Logging Service Alerts

Open the **General > Health** page to view a summary about the environment and state of CloudControl. For more information, see **Appliance Health** on page 128.

The Logging Service is located in the Service section of the Appliance Health page. If there are no alerts, the Logging Service displays **OK**. If a storage impact occurs during logging, the Logging Service displays an alert message.

The following example shows an alert for a storage impact that occurred during logging.

<table>
<thead>
<tr>
<th>Services</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database</td>
<td>OK</td>
</tr>
<tr>
<td>HTTP/SOAP Proxy</td>
<td>OK</td>
</tr>
<tr>
<td>Internal Services (xinetd)</td>
<td>OK</td>
</tr>
<tr>
<td>Logging Service</td>
<td>Log messages are consuming 1146976 kB of storage, alert threshold is 1024 MB.</td>
</tr>
<tr>
<td>Name Resolution (DNS)</td>
<td>OK</td>
</tr>
<tr>
<td>Network Time (NTP)</td>
<td>Disabled</td>
</tr>
<tr>
<td>Remote Access (SSH)</td>
<td>OK</td>
</tr>
<tr>
<td>Route Discovery (RIP)</td>
<td>Disabled</td>
</tr>
<tr>
<td>SNMP Service</td>
<td>Disabled</td>
</tr>
<tr>
<td>SSH Proxy</td>
<td>No Configured Hosts</td>
</tr>
<tr>
<td>Scheduler</td>
<td>OK</td>
</tr>
<tr>
<td>System Logging</td>
<td>OK</td>
</tr>
<tr>
<td>VMware Tools</td>
<td>OK</td>
</tr>
</tbody>
</table>
Viewing Log Messages from the CLI

You can view CloudControl log messages in their entirety from the command line interface (CLI) using the `asc log` command in CloudControl. For more information, see CloudControl Command Line Interface (CLI) on page 192.

An example log message from the `proxy-ssh.log` file looks as follows:

```
Mar 16 16:35:38 localhost proxy-ssh [7066]: [root@172.16.1.200] - [172.16.1.22] Authenticating user
```

The `proxy-ssh.log` shows all SSH connection messages. Each message includes details about who tried to do what from where.

Obtaining the Troubleshooting Bundle

You can use the CLI or the GUI to obtain the CloudControl troubleshooting bundle to send it to HyTrust Support.

Using the CLI

1. Login via SSH to CloudControl using the ascadminuser credentials.
2. Enter the following command:
   ```
   asc log --accept -t
   ```
   **Note:** The `--accept` argument in the `asc log -t` command is to indicate that you have read and accepted the privacy warning displayed on the screen after you enter the command. Data from the virtual appliance is collected and stored in a zip file when executing the commands: `asc log -t` or `asc log -t -f`. It includes database entries, log activity, IP addresses, host names, usage patterns, time stamps, and other environmental information. We do not disclose the information collected to the third parties. All information collected is solely used to aid in the running, debugging, and/or optimizing a service and/or enhancing customer relationships.
   The `asc log -t` command generates a troubleshooting archive zip file (`asc-state.zip`) and saves it in the `/var/log/asc` directory. For more information, see CloudControl Command Line Interface (CLI) on page 192.
3. Once the zip file has been created, use secure copy (SCP) to move the file to a local client machine and then contact HyTrust Support for further assistance.

Using the GUI

1. Select **Maintenance > Troubleshooting**.
2. On the Troubleshooting page, select the type of support log bundle that you want to download. This can be Full or Partial.
3. Click **Download**.

Obtaining System Logs

This section describes how to obtain the CloudControl system log file(s).

To obtain the CloudControl system logs:

1. Open the **Configuration > Logging page**.
2. Click the **Download** button and save the archive (**asc.log.zip**).
Chapter 11. Monitoring Hosts and Networks

Enabling Monitoring

CloudControl can perform ICMP ping tests and port scanning for its dependent network infrastructure and protected resources, as well as send notifications using the `asc monitor` CLI command. For more information, see `asc monitor` on page 206.

SNMP alerts are generated when a service or resource transitions between OK, Warning, and Failed and are distributed via SNMP, SMTP, or syslog. A PHM connectivity issue to a vCenter Server is a Failed state, and a connectivity issue to an ESXi is a Warning state.

You can enable SNMP monitoring using the CLI or from the Monitoring page in the CloudControl Management Console. For more information, see Configuring Monitoring and Notifications on page 55.

Monitoring is enabled by default if the vCenter Server and any corresponding hosts are protected by CloudControl.

Network Resource Monitoring

CloudControl scans all routers, time servers, name servers, log servers, SNMP trap receivers, SMTP servers, and Active Directory/LDAP service ports during its health monitoring routine, which runs at 2 minute intervals (via a cron job). This is called network resource monitoring (NRM). The results are shown in the Services section on Appliance Health dashboard. For more information, see Appliance Health on page 128.

For example, if a DNS server is offline, the Name Resolution (DNS) service in the Appliance Dashboard will show offline. In the CloudControl CLI, the service will show Warning.

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NTP</td>
<td>123/udp</td>
<td>Test connectivity to the Network Time Server</td>
</tr>
<tr>
<td>SNMP Manager</td>
<td>161/udp</td>
<td>Test connectivity to the SNMP Server</td>
</tr>
<tr>
<td>SNMP Trap</td>
<td>162/udp</td>
<td>Not monitored, but used to generate SNMP messages</td>
</tr>
<tr>
<td>SMTP</td>
<td>25/tcp</td>
<td>Test connectivity to the Mail server</td>
</tr>
<tr>
<td>SYSLOG</td>
<td>514/udp</td>
<td>514 is the default port, but you can specify any other port</td>
</tr>
<tr>
<td>DNS</td>
<td>53/udp or 53/tcp</td>
<td>Test connectivity to the DNS servers (Normally udp)</td>
</tr>
</tbody>
</table>
Protected Host Monitoring

CloudControl uses the monit service to perform ICMP ping tests to all protected vCenter Servers and ESXi hosts. This is called Protected Host Monitoring (PHM). All failures are listed under the Resources section in the Appliance Health dashboard. For more information, see Appliance Health on page 128.

In the CloudControl CLI, an offline ESXi host state will show Warning, and an offline protected vCenter Server will show Failed.

<table>
<thead>
<tr>
<th>Service</th>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>TCP/443</td>
<td>Port 443 is the default port</td>
</tr>
<tr>
<td>HTTP</td>
<td>TCP/80</td>
<td>Port 80 is the default port</td>
</tr>
</tbody>
</table>

Viewing NRM and PHM Status

You can view NRM and PHM status on the appliance dashboard or via the CLI. The Appliance Dashboard shows both NRM and PHM warnings and errors.

You can also use the `asc monitor` command in the CLI to view NRM and PHM errors and warnings.

For more information on how to use NRM and PHM, see `asc monitor` on page 206.
Chapter 12. Maintaining the Appliance

Licenses

Select Maintenance > License to view details about your current license and update to a different license.

Information tab

The Information tab on the License page displays the following:

- Customer Name
- Customer Number
- Entitlement Number
- Status
- Number of Protected Hosts
- Number of Licensed Host CPU Sockets
- Number of Protected Host CPU Sockets
- Number of Licensed NSX CPU Sockets
- Number of Protected NSX CPU Sockets
- License Type
- Maintenance Expiration Date
- Support Expiration Date

The license information is also available on the CloudControl dashboard. For additional information, see Admin Access Dashboard on page 117, Protection Dashboard on page 123, or Scheduled Events on page 51.
A default scheduled event **Refresh Host Socket Count** monitors the host socket count and refreshes it at the interval of 10080 minutes, or one week. This scheduled event is disabled by default. It can be modified for the time interval parameter, but cannot be deleted.

Additional licenses, including maintenance and support renewals, may be obtained by contacting sales@hytrust.com.

**Update Tab**

To update your license do the following:

1. From the Update tab on the Licensing page, click **Choose File**.
2. Navigate to the location of the file that you want to import and click **Open**.
   - **Note**: The license file must be in .XML format.
3. Click **Apply**.

**CloudControl Services**

Use the Maintenance > Services page to manage services running on CloudControl. The following services are available:

- **CloudControl Application Server (Proxies, Admin GUI, REST APIs)**—Click **Restart** to restart the CloudControl HTTP/SOAP proxy.
  - **Note**: Restarting requires that you log back in to the CloudControl Management Console.

- **SSH Proxy Status**—Displays the current status of the SSH proxy.

- **Start/Stop SSH Proxy**—Click **Stop** or **Start** to change the status of the SSH proxy.

- **Proxy Denial Message**—This message is presented to any user that attempts to perform an operation that goes beyond their privilege level in both SSH and the vSphere Client. By default, the message is: Permission denied due to security policy, but you can customize the denial message.

- **Reindex Policy Items**—Click the **ReIndex** button if you are having trouble searching for rules or resources that should be present or if you are seeing unexpected duplicates.

- **Job and Policy History Retention (days)**—Sets the number of days to keep data before purging. All job history and policy history data older than the days set will be purged. The default value is 90 days.

- **Threshold for Full Vacuum(%)**—Sets the minimum threshold to trigger a garbage collection process on the database. When database disk space utilization exceeds this threshold, a full vacuum will be performed when the Purge Database scheduled event is run. Valid values are between 50% and 75%.
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.

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 must enable the Vitals Service to transfer Vitals bundles HyTrust Support.

1. Select **Maintenance > Services**.
2. Check the **Enable Vitals Transfer** checkbox.
3. Click **Apply**.

Creating and Sending a New Vitals Bundle

To immediately create and send a Vitals bundle to HyTrust Support:

1. Select **Maintenance > Services**.
2. In the Create a new Vitals support bundle field, click **Create**.

**Note:** The Vitals Service must be enabled before you can send the new Vitals bundle to HyTrust Support.

Disabling the Vitals Service

1. Select **Maintenance > Services**.
2. Uncheck the **Enable Vitals Transfer** checkbox.
3. Click **Apply**.

Enabling Proxy Server for the Vitals Service and Licensing Service

The Network Configuration page allows you to enable the proxy server or view your settings.
1. Select **Configuration > Network**.

2. On the Network Configuration page, navigate to the Proxy Server section.

3. View or modify the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server IP</td>
<td>The IP address of the proxy server to use with the Vitals Service and Licensing service.</td>
</tr>
<tr>
<td>Proxy Server Port</td>
<td>The port for the proxy server.</td>
</tr>
<tr>
<td>Proxy User Name</td>
<td>The username for the proxy server.</td>
</tr>
<tr>
<td>Proxy User Password</td>
<td>The password for the proxy server.</td>
</tr>
<tr>
<td>Enable License Proxy</td>
<td>Check the checkbox to use the proxy server to contact the Licensing service.</td>
</tr>
<tr>
<td>Enable Vitals Proxy</td>
<td>Check the checkbox to use the proxy server to contact the Vitals Service.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.

### Backing Up the CloudControl Appliance

CloudControl supports the following types of backup:

- Appliance configuration backups using the `asc backup` CLI command. For more information, see `asc backup` on page 193.

- Full snapshot-based backups or clones using VMware or third-party tools.

  **Important:** If HyTrust CloudControl is restored from a backup or clone, the infrastructure, for example, vCenter, may assign a new MAC address to its network adapter. This can happen even if the original CloudControl instance is powered off or even removed from the environment. Before powering on a CloudControl appliance in this situation, please change the MAC address back to the original value from when the backup was taken.

### Rebooting CloudControl

1. Select **Maintenance > Troubleshooting**.

2. On the Troubleshooting page, click **Reboot**.
Viewing Jobs

Select **Maintenance > Jobs** to see the Jobs page. On the Jobs page, you can view the following information for both running and completed jobs:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kill</td>
<td>Displays N/A if no action can be taken. If a job is in the Running state, you can click the Kill Service (redeem) icon to manually kill the job.</td>
</tr>
<tr>
<td>Service</td>
<td>The type of service.</td>
</tr>
<tr>
<td>Started</td>
<td>The date and time when the job was started.</td>
</tr>
<tr>
<td>Ended</td>
<td>The date and time when the job ended.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user account that initiated the job.</td>
</tr>
<tr>
<td>Host</td>
<td>The host which initiated the job.</td>
</tr>
<tr>
<td>Template</td>
<td>The template or operation used for the job.</td>
</tr>
<tr>
<td>Status</td>
<td>The status of the job.</td>
</tr>
</tbody>
</table>

Searches

CloudControl supports searching vCenter Server resources from the General > Search page when assigning Rules, RuleSets, or Labels to policy resources and when assigning rules to RuleSets. You can also narrow your searches using filters to locate a particular object such as a Host, Virtual Machine, or vSwitch.
If a resource is selected, more details about the resource are shown on the right pane. You can also hover the mouse cursor over an item in the search results to view its resource tree path (and other details such as the virtual center and data center).
For details about the fields within CloudControl that are indexed, or to see some sample queries using the search field, click on the help (_tooltip) icon or refer to Search Filters on page 190.

Searching is also supported in the Log Viewer—see Log Viewer on page 130.
Chapter 13. Reports

Reports Overview

CloudControl allows users to view historical information about the protected virtual infrastructure using reports. Reports may be viewed in real-time or defined as a scheduled event that generates and emails a report at a specific time-interval in CSV or PDF format.

To start generating reports, configure reports in CloudControl and then add Report Definitions.

Configuring Reports

1. Select General > Reports.
2. On the Configuration tab, check the Enable checkbox to enable report generation.
3. To receive reports in email, check the Enable email notifications checkbox and enter the email address in the Email Address (FROM) field.
   
   Note: SMTP must be enabled to enable notifications.

   After reports are enabled, the Reports Definitions tab displays.
   
   You can only generate one report at a time.

Report Definitions

CloudControl allows you to customize reports by specifying options such as report parameters, viewing options, and date ranges.

These options are listed on the General > Reports > Add Report Definition and General > Reports > Edit Report Definition pages.
Report Panel

The Report Type drop-down on the Report panel lists the available report types. Enter the name of the report in the Name field. This name is used as an identifier to differentiate the report definitions of the same report type. It is also used to name the scheduled event that may be created while adding a report definition.

Parameters Panel

The Parameters panel lists options for the Host Selection. The list of parameters available for customizing reports varies by report type.

Scheduled Events Panel

The Scheduled Events panel shows the viewing options for reports.

- Select View to generate and view the report in real-time.
- Select Create Scheduled Event to display the field options to create a scheduled event for that report. Enter the following information to create a scheduled event:
  - Name: Name of the scheduled event.
  - Description: Description of the scheduled event.
  - Start: Start date and time of the scheduled event.
  - Interval Type: Specify the interval at which to generate the report.
  - Report Format Type: Specify the format of the report output, CSV or PDF.
  - To and From email addresses: Enter the appropriate email addresses.

Checking the Enabled checkbox enables the scheduled event directly from the General > Report > Add ReportDefinition page or the General > Report > Edit Report Definition page.

CloudControl generates the report at a user-specified date and time based on the report definition. The generated report is in either CSV or PDF format and is emailed to a user-specified email address.

Date Range Panel

The Date Range panel provides options to generate reports at a specific time-interval. This time-period can be for the last N days in the range of 1-90 days or a date-range on the calendar. The generated report is for a user-specified number of days in the past, including the day the report is generated. The generated report is for the time-period between the Start Date and the End Date.

Adding Report Definitions

1. Select General > Reports.
3. On the Add Definitions page, complete the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report</td>
<td>Select the Report Type and enter the name for the report.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Fill in the appropriate parameters. The parameters vary depending on the report type selected.</td>
</tr>
<tr>
<td>Action</td>
<td>Select View to see the report immediately, or Create Scheduled Event to have the report generated periodically at a specific date and time.</td>
</tr>
<tr>
<td>Date Range</td>
<td>Select the date range to be included in the report.</td>
</tr>
</tbody>
</table>

4. Click **Apply**.

**Editing Report Definitions**

1. Select **General > Reports**.
2. On the Report Definitions tab, select the report definition that you want to modify and click **Edit**.
3. Update the report details as necessary.
4. Click **Apply** to save the changes.

**Deleting Report Definitions**

1. Select **General > Reports**.
2. On the Report Definitions tab, select the report definitions that you want to delete and click **Delete**.
3. Click **OK** on the confirmation dialog box.

**Report Types**

You can generate several types of reports using CloudControl.

**Authentication Login Report**

**Overview**

The Authentication Login Report provides information about attempted logins that failed and/or were allowed. The CloudControl users may have attempted to login using any authentication method via services like AD or RSA.

**Parameters**

Parameters for the Authentication Login Report are:

- Authentication Type: Authentication Login Report can be customized for different authentication types. Those are:
- All for all login types
- AD for Active Directory logins
- RSA for RSA user-logins
- SmartCard for authentication using smart-card credentials
- Demo for authentication using CloudControl demo mode
- RADIUS for RADIUS server authentication
- Status: Select Allowed checkbox for users who were allowed to login and Denied checkbox for users who were denied the access.

Select both check boxes to generate the report for both passed (Allowed) and failed (Denied) login attempts.

**Report Format**

Format of the generated *Authentication Login Report* is as shown below.

Report details of a login attempt includes Admin Name, Role, Source IP, Destination IP, Resource Name, Resource Type, Protocol, whether the login was Allowed/ Denied, and Date/Time of the login attempt. The report also includes Authentication Access Status in the form of a pie chart, which shows total number of login attempts that were allowed or denied.

**Authentication Operation Report**

**Overview**

The *Authorization Operation Report* lists all the users who attempted to perform an operation and if they were allowed or denied.

**Parameters**

The following parameters are available to customize this report:

**Status**: Select *Allowed* checkbox for users who were allowed to perform operations or *Denied* checkbox to list the users who were denied the permission to perform operations.

**Report Format**

The Authorization Operation Report lists information such as Admin Name, Group, Source IP, Operation they tried to perform, whether the attempted operation was allowed or denied, Resource name, Resource Type, Protocol, and Date and Time of the attempted operation. Clicking on the date link opens the *Log Viewer*, which shows the log information about that particular operation attempt.

The report also displays the total number of admins that were allowed or denied the permission to perform the operation in the form of a pie chart.
Continuous Monitoring Assessment Report

Overview

The Continuous Monitoring Assessment Report (CMAR) gives a summary of the assessments performed and failed during a specific time period. The report is customizable by specifying a time and a date range. CloudControl gives an option to generate and view the report in real-time or to create a scheduled event to generate the report at a specific time.

The report gives high-level information of assessment failure results for all hosts in the given time-period. It is linked to other reports that drill down to the specific assessment results for every listed host.

Parameters

- **Any**: Selecting the Any option generates a report for all hosts or for a specific label or template.
- **By Label**: Selecting the By Label option generates the report for all the hosts associated with that particular label. Click on the By Label radio button. It will enable the Labels combo-box with list of labels.
- **Labels**: Select a label from the list.
- **By Template**: Selecting the By Template option enables the Template drop-down that lists all the available templates.
- **By Hostname/IP**: Selecting the By Hostname/IP enables the Selected Host field that lists the available hosts.

Selecting **By Template** enables the **Template** drop-down.

Selecting **By Hostname/IP** template enables the **Selected Host** field. Start typing in the field and the list of available hosts will appear.

Report Format

The Continuous Monitoring Assessment Report gives high-level information about assessment failure results for hosts. It lists user-specified criteria and a summary of assessment results. The report shows details such as percentage failed, number of assessments failed, the template and labels of all the hosts assessed in the specified time-period. The report also gives pass/failed assessment status for hosts in the form of a pie chart. This report links to the host-specific reports for each of the hosts assessed in the given time-period.

Drill-down reports provide the details of assessment failure results for every host that was assessed in a user-specified time period. These reports summarize information in terms of the date a host was assessed, action performed (e.g., Assess), number of failed operations out of total operations performed, and the template against which it was assessed. Like the high-level report, it shows the fail/pass status for total number of operations in the form of a pie chart.

The Date column in the drill-down report lists the date and time stamps as a hyperlink for each of the assessments. Click on this link to see the complete details about failed operations for any particular assessment.

Root of Trust - Attempted Changes Denied Report

Overview

The Root of Trust: Attempted changes that were denied because of compute pool policy Report lists all the attempted operations on VMs that were denied because those VMs were not in the Trusted Compute Pool. In other words, this report lists attempted operations on VMs that were denied because the target host was Untrusted.
Parameters

Host Selection:

- **Any**—Generate the report for any ESXi hosts with any label.
- **By Host type**—Generate the report for ESXi hosts.
- **By Label/PolicyTag**—Generate the report for hosts with a specific Label or PolicyTag.

Report Format

The generated report lists the parameters used and provides details such as Host IP, Host Type, Attempted Operation on that host, Labels/PolicyTags, Name of the admin who attempted that operation, role of the admin, and Date and Time when the operation was attempted.

Root of Trust - Good Known Host (GKH) Report

Overview

The Root of Trust- Good Known Host Report lists all Good Known Hosts present in CloudControl at the time the report was generated.

Parameters

There are no parameters required for this report.

Report Format

The Root of Trust-GKH Report provides details such as Host IP, Labels/Policy Tags, Host Type, BIOS Patch Level, VMM Patch Level, Date/Time the host was assigned a Good Known Host status. Clicking on the date link opens the Log Viewer which shows the log information about has information about this host becoming a Good Known Host.

Root of Trust - Current Hosts and Trust Status Report

Overview

The *Root of Trust - Current Hosts and Trust Status Report* lists all hosts and their trust status at the time the report was generated.

Parameters

**Trust Status:** Specify Trust Status as a listing criteria for this report. To customize the report output based on the trust status of hosts, select:

- **All** for all hosts,
- **Trusted** for trusted hosts,
- **Untrusted** for the hosts whose status has been changed from trusted to untrusted, and
- **Unknown** for the hosts whose trust status is not known.
Report Format

The report gives details such as host name, Label/Policy Tag on the host, host IP, host type, Trust Status, BIOS Patch Level, VMM Patch Level, GKH relationship. The report shows total number of hosts that are TRUSTED, UNTRUSTED or UNKNOWN in the form of a pie chart.

Exporting Reports

Generated reports can be exported to the CSV or the PDF format.

To export the report, click on the PDF or CSV button on the top left corner of the generated report.

![Report](image)

Using Scheduled Events to Generate Reports

CloudControl offers the functionality to generate reports as a scheduled event. This allows the users to view or email the report at specific time-intervals. The date range for Scheduled Events is last N days. The Specify Range option is not available for the reports generated as Scheduled Events.

You can create a Scheduled Event for a report at the time of adding a report definition, or you can edit an existing report and create a Scheduled Event.

Editing Reports to Include Scheduled Events

To edit an existing report go to General > Reports and click on the Edit button.
1. Go to the **Scheduled Events** panel.
2. Select the **Create Scheduled Event** radio button.

The **Scheduled Events** panel displays the options to create a scheduled event for the report.

3. Enter **Name**, **Description**, **Start** date and time, and **Interval Type** in minutes, hours or days.
4. Select the **Report Format Type**: PDF or CSV
5. Enter From and To email addresses.
6. Click on the **Enabled** checkbox to enable receiving the report by email.
7. Click **Apply**.

The report is generated in a user-selected format and is emailed on a user-specified date at a user-specified time.

### Editing Scheduled Events for Reports

To edit the scheduled event for a report, go to either **Compliance > Scheduled Events** or **General > Reports**.

1. Select the report you want to edit and click on it.
   - The **Edit Report Definition** screen appears.
   - The **Scheduled Events** panel displays the options.
2. Edit the details and click **Apply**.

### Configuring Syslog Settings

CloudControl logs all operations initiated on protected vCenter Server or ESXi hosts, for all methods of access, and stores the corresponding log entries in a central location.

**Note:** Optionally, you can have CloudControl automatically retrieve the vCenter Server events and have them included in the CloudControl log files. (Enable the predefined Get vCenter events scheduled event to activate vCenter Server event retrieval—see **Configuring Security Options** on page 47.)
Log entries are human readable and include information on the user initiating the operation, user group affiliation, origin (method of access and source), object being manipulated, the operation itself, and whether the operation was authorized. CloudControl provides detailed logs to support easy audit and compliance reporting, and log file export.

**Syslog Severity Level Classifications**

Individual log entries are classified by importance. For example, all successful operations are classified as INFO level log entries. Events that have security implications such as failed authorization, are logged with WARN level.

There are five log level classifications:

- **FATAL**—Severe errors, usually involving a crash.
- **ERROR**—Runtime errors, intermittent network issues, recoverable errors such as dropping network packets, etc.
- **WARN**—Non-fatal, unexpected behavior, and proactive monitoring notifications. Security events, such as failed authorizations, are also logged at this level.
- **INFO**—Generally interesting events, such as virtual machine moves and configuration changes. Also includes all virtual infrastructure events, including successful and failed authentications, authorizations, and changes to virtual infrastructure configurations that were locked down by CloudControl.
- **DEBUG**—Support messages about the internal operations of CloudControl that are intended for use by HyTrust Support.

You can view syslog events using the built-in log viewer (*General > Log Viewer*).
Chapter 14. VMware NSX in CloudControl

Using VMware NSX in CloudControl Overview .......................................................... 161
NSX Host Management .............................................................................................. 163
NSX Compatibility ...................................................................................................... 166
Testing NSX Compatibility ........................................................................................ 166
Policy .......................................................................................................................... 167
Refreshing Policy Resources ...................................................................................... 168
NSX Cross vCenter Support ...................................................................................... 168

Using VMware NSX in CloudControl Overview

CloudControl supports the following VMware NSX versions for vSphere 6.x:

- 6.2.7
- 6.2.8
- 6.3.2
- 6.3.3

CloudControl authorizes CUD (Create, Update, Delete) operations on key NSX resources such as Logical Switches, Edges, Routers, Firewalls, Security Groups, and Security Policies. This allows you to use role-based access control to inspect NSX admin operations and apply CloudControl policies to NSX resources. To protect and proxy NSX resources in CloudControl, you need a valid CloudControl license that includes NSX support.

**Note:** Read or view operations are not authorized or logged.
NSX resources are imported into CloudControl as follows:

<table>
<thead>
<tr>
<th>NSX Resource Type</th>
<th>CloudControl Resource Type</th>
<th>Operations Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Logical Router</td>
<td>Router</td>
<td>Supports CUD operations on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Router Service</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td>Edge Gateway Services</td>
<td>Network Service Containers</td>
<td>Supports CUD operations on:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Gateway Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• DHCP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Load Balancer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP Sec VPN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• VPN(L2/SSL)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Firewall</td>
</tr>
<tr>
<td>Security Group</td>
<td>ObjectGroup</td>
<td>CUD operations</td>
</tr>
<tr>
<td>Security Policy</td>
<td>SecurityPolicy</td>
<td>CUD operations</td>
</tr>
<tr>
<td>Distributed Firewall</td>
<td>Firewall</td>
<td>CUD operations</td>
</tr>
<tr>
<td>Logical Switch</td>
<td>Switch</td>
<td>CUD operations</td>
</tr>
<tr>
<td>Controller</td>
<td>Controller</td>
<td>CUD operations</td>
</tr>
<tr>
<td>IP Set</td>
<td>IPAddressGroup</td>
<td>CUD operations</td>
</tr>
<tr>
<td>MAC Set</td>
<td>MacAddressGroup</td>
<td>CUD operations</td>
</tr>
<tr>
<td>Distributed Firewall Section</td>
<td>Firewall Section</td>
<td>CUD operations</td>
</tr>
</tbody>
</table>

**Important:**

- Before CloudControl version 5.2, the same firewall privileges were used for distributed firewall, edge firewall, and router firewall. Beginning with version 5.2, new firewall privileges have been added for edge firewall and router firewall. The new privileges have been added to the SuperAdmin, SecurityAdmin, and NetworkEngineer roles. You will need to manually assign the privileges to any custom roles used for edge or router firewall.

- Beginning with CloudControl version 5.3, we now support multi-tenant Distributed Firewall configuration through WCS and REST API. For REST API, the following privileges have been updated:

<table>
<thead>
<tr>
<th>Previous Privilege Name</th>
<th>Updated Privilege Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network.Firewall_Rule*</td>
<td>Network.FirewallRule*</td>
</tr>
<tr>
<td>Network.Firewall_Policy*</td>
<td>Network.FirewallPolicy*</td>
</tr>
</tbody>
</table>
Beginning with CloudControl version 5.3, new privileges have been added for IP Set, MAC Set, and Distributed Firewall Section to the SuperAdmin, SecurityAdmin, and NetworkEngineer roles. You will need to manually assign the privileges to any custom roles using the previous privileges.

The following NSX resource types are updated:

<table>
<thead>
<tr>
<th>NSX Resource Type</th>
<th>CloudControl Previous Resource Type</th>
<th>CloudControl Current Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Set</td>
<td>IPCollection</td>
<td>IPAddressGroup</td>
</tr>
<tr>
<td>Mac Set</td>
<td>MacCollection</td>
<td>MacAddressGroup</td>
</tr>
<tr>
<td>Service Group</td>
<td>ServiceCollection</td>
<td>ServiceGroup</td>
</tr>
<tr>
<td>Security Group</td>
<td>ObjectCollection</td>
<td>ObjectGroup</td>
</tr>
</tbody>
</table>

NSX Host Management

You can add NSX resources in CloudControl using one of the following methods:

- Adding VMware NSX with vCenter
- Adding VMware NSX as a host

**Note:** NSX can also be configured with vCenter using the CloudControl Add Host wizard as part of the ELM configuration.

Adding VMware NSX with vCenter

Before You Begin

Ensure that NSX is configured for use in vCenter. You can then use the Add Host Wizard to add a vCenter server with VMware NSX.

Procedure

1. Select **Compliance > Hosts**.
2. On the Hosts page, click **Add**.
3. In the Add Host wizard, on the Host Type page, select the **vCenter, vSphere Web Client Server and VMware NSX** radio button and click **Next**.
4. On the Host Login page, enter the Hostname/IP and log in credentials for the vCenter and click **Next**.
5. On the Host Details page, enter the Friendly Name, check the **Protected** checkbox and click **Next**.
6. On the Published IP page, enter the Published Hostname/IP and Published IP Mask, and click **Next**.
7. On the vSphere Web Client Server Configuration page, enter the following information and click **Next**:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The service account to be used for CloudControl. The same account must be used across all vCenter Servers connected to the Web Client Server. <strong>Important</strong>: If you plan to use the NSX proxy in CloudControl, this account must have the Enterprise Administrator role in NSX.</td>
</tr>
<tr>
<td>Password</td>
<td>The CloudControl Service Account password.</td>
</tr>
<tr>
<td>Https Service Port</td>
<td>The Web Client Server HTTPS port number.</td>
</tr>
<tr>
<td>Published vSphere Web Client Server Hostname/IP</td>
<td>The published hostname/IP address for the Web Client Server.</td>
</tr>
<tr>
<td>Published Netmask</td>
<td>The published subnet mask for the Web Client Server.</td>
</tr>
</tbody>
</table>

CloudControl verifies that there is an NSX plugin associated with the vCenter before continuing.

8. On the VMware NSX Configuration page, enter the following information and then click **Next**.
   - VMware NSX Hostname/IP
   - Service Account
   - Service Account Password
   - HTTPS Port
   - Friendly Name (Optional)
   - Description (Optional)
   - Protected
     - The Protected checkbox is disabled until CloudControl can verify the compatibility, and enabled after the detected version of VMware NSX is determined to be supported.
   - Published VMware NSX Hostname/IP (Optional)
   - Published Netmask (Optional)

   **Note**: If you do not have the NSX configuration information, you can skip this step and add the information later. See Adding VMware NSX as a Host on the next page.

9. Click **Finish**.

If the patch level of VMware NSX is not supported, CloudControl downloads the appropriate VMware NSX files. Restart the CloudControl application server to enable full VMware NSX support. See Restarting the CloudControl Application Server on the next page.

If an error occurs while upgrading the VMware NSX files, see the corresponding log message. If CloudControl already supports NSX, no message is displayed.
Adding VMware NSX as a Host

If your vCenter is already configured and protected by CloudControl, you can add VMware NSX as a separate host.

1. Select Compliance > Hosts and click Add on the Hosts page.
2. On the Host Type page, select VMware NSX and click Next.
3. On the VMware NSX Configuration page, enter the following information and click Next.
   - VMware NSX Hostname/IP
   - Service Account
   - Service Account Password
   - HTTPS Port
   - Friendly Name (Optional)
   - Description (Optional)
   - Protected
     The Protected checkbox is enabled if the detected patch level of VMware NSX that is being added is supported, and is disabled if CloudControl is currently not maintaining any supporting files for VMware NSX.
   - Published VMware NSX Hostname/IP (Optional)
   - Published Netmask (Optional)
     CloudControl looks for the vCenter associated with the NSX Host and displays the details on the VMware NSX and vCenter Mapping page. If CloudControl was not maintaining any supporting files for VMware NSX, it downloads them at this point and displays the following message:
     The required VMware NSX files have been downloaded. To enable full NSX support, please restart the CloudControl Application Server (requires admin privileges)
4. Click Next.
5. Click Finish to complete the configuration.
   CloudControl downloads version-specific VMware NSX files as needed. Restart the CloudControl application server to enable full VMware NSX support. See Restarting the CloudControl Application Server below.
6. On the Compliance > Hosts page, select the NSX host that you just added.
7. Check the Protected checkbox on the General tab on the Edit Host page and click OK.

After the Add Host process is complete and VMware NSX is protected, you will have to manually refresh the CloudControl resources. See Refreshing Policy Resources on page 168.

Restarting the CloudControl Application Server

To enable full VMware NSX support, restart the CloudControl Application Server. You must have the Asc.Administration privilege to perform this action.
1. Select **Maintenance > Servers**.

2. On the Services page, locate the CloudControl Application Server and click the **Restart** button.

3. Click **OK** to acknowledge the warning message.

4. After the CloudControl application server finishes restarting, log in to CloudControl.

5. Select **Compliance > Hosts**, and locate the VMware NSX host that you added.

6. If the VMware NSX host is not protected, select the NSX host.

7. On the **Edit Host** page, click the **General** tab and check the **Protected** checkbox.
   
   **Note:** In the Edit NSX Host > Advanced tab, the **Permit unknown NSX operations** checkbox applies only for NSX Rest Proxy APIs.

8. Click **OK**.

After the Add Host process is complete and VMware NSX is protected, you need to manually refresh the CloudControl resources. For more information, see **Refreshing Policy Resources** on page 168.

**NSX Compatibility**

Currently CloudControl supports several versions of VMware NSX. These versions have been tested in the HyTrust environment and are compatible with the latest CloudControl release. Users may also be able to import and protect newer VMware NSX releases with minor changes, even though they are not tested by HyTrust. Any major VMware NSX releases that are not explicitly supported by HyTrust are incompatible with CloudControl. As a general guideline, VMware NSX compatibility with CloudControl falls into the following categories:

- **Tested and compatible with CloudControl**
  
  Several major VMware NSX versions are tested in the HyTrust environment. These versions are fully compatible with CloudControl.

- **Not tested but may be compatible with CloudControl**
  
  Some minor versions of VMware NSX that were not tested in the HyTrust environment may also be compatible with CloudControl.

- **Incompatible**
  
  Any major VMware NSX releases that are not tested and explicitly supported by CloudControl are incompatible with CloudControl.

**Testing NSX Compatibility**

CloudControl maintains the latest version of supporting files for VMware NSX. When a VMware NSX host is imported during the Add Host process, CloudControl checks its compatibility. If CloudControl detects a newer compatible version of VMware NSX, it downloads the newer version of supporting files.

If an admin upgrades a VMware NSX host in the vCenter, you can test its compatibility with CloudControl using one of the following methods:
The page includes instructions on testing NSX compatibility in CloudControl. It outlines two methods: manual and automatic.

**Manually Testing NSX Compatibility**

CloudControl allows you to manually test the compatibility of protected NSX hosts.

1. Select **Compliance > Hosts**.
2. On the Hosts page, select a VMware NSX host that needs to be tested for its compatibility with CloudControl.
3. Click the **Test NSX Compatibility** button.
   - If the selected VMware NSX host is compatible with CloudControl it displays a message stating that there is no change in the patch level.
   - If the upgraded version is not already supported, CloudControl downloads the necessary files. To enable full CloudControl support for the VMware NSX, restart the CloudControl Application Server. For more information, see the [Restarting the CloudControl Application Server](#) on page 165.
   - If the detected version of selected VMware NSX is not supported or if an error occurs when downloading the necessary VMware NSX files, CloudControl displays an error message. The error will also be listed in the log messages.

**Automatically Testing NSX Compatibility**

Use the **Inventory Refresh** scheduled event to periodically check for any changes in protected CloudControl resources, including resource version changes. When the Inventory Refresh scheduled event runs at its scheduled time, CloudControl detects the version changes in protected VMware NSX hosts and downloads the necessary files if the new version is not already supported.

For more information, see [Scheduled Events](#) on page 51.

**Policy**

Role-based access control is the only Policy feature available for NSX resources in CloudControl. The predefined NSX roles in CloudControl allow users to achieve granular control over operations performed on NSX resources. The following NSX roles are available in CloudControl by default:

- ASC_SecurityAdmin
- ASC_SecurityOperator
- ASC_SecurityAuditor
- ASC_NetworkEngineer
- ASC_NetworkOperator
- ASC_LoadBalancerAdmin
These roles have different sets of privileges assigned to them. For more information, see Default Roles and Permissions on page 182.

Refreshing Policy Resources

After the Add Host process is complete and VMware NSX is protected, you will have to manually refresh the CloudControl resources.

1. Select Policy > Resources.
2. Click the Refresh button.

NSX resources are listed under the resource tree on the Policy > Resources page.

NSX Cross vCenter Support

NSX Manager is the centralized network management component of NSX. It provides an aggregated system view. Every vCenter has its own NSX Manager. In CloudControl, for every imported vCenter, an associated NSX Manager is shown along with its associated resources.

To add and protect an NSX Manager in CloudControl, you must first add the vCenter it manages. For vCenters that are already configured and protected in CloudControl, there is an option to add NSX Manager and associated resources. In order to support all features of Cross vCenter NSX in CloudControl, all NSX Managers should be protected along with ELM environment.
Chapter 15. Boundary Control

Boundary Control Overview
The Boundary Control feature uses Policy Rules and Constraints in HyTrust CloudControl to authenticate and authorize delivery of encryption keys to the data encrypted and managed by HyTrust KeyControl.

A Boundary is a logical territory defined by PolicyTags or Label Constraints in Policy Rules. Rules define privileges for user groups to perform operations on resources. Constraints limit the scope of a Rule. PolicyTags constraints set geographical boundaries on resources. Constraints can also be labels that put resources in certain categories. Every time a user attempts to operate on a resource, the operation is permitted or denied based on the Rules and Constraints assigned to that resource.

When KeyControl requests a key to the encrypted data, it sends an authentication request to HyTrust CloudControl. Based on the information received from the KeyControl Server, CloudControl identifies the VM, and authorizes the key delivery only if the VM is located within the defined Boundary.

**Important:** When you set up Boundary Control and define your boundary, please be aware of the potentially disruptive effects if a VM migrates outside the boundary. For example, if you enable boundary control for hosts in a VMWare DRS cluster, all hosts in the DRS cluster must be within the defined boundary. If you miss a host, you might see a situation where vCenter moves a VM to a node in the DRS cluster that is outside the boundary. If that happens, the VM will be shut down by HyTrust Boundary Control.

Boundary Control Use Cases

**Data Sovereignty**

Data privacy laws (especially in the Euro zone) stipulate that data captured in a given country must remain housed exclusively on servers in that country. There are restrictions on how and under what circumstances that data may be transmitted beyond the borders of that country. In virtualized environments, this presents numerous challenges because users can access data from anywhere in the world. Anyone can copy entire virtual machines and move the data outside the areas of physical data centers. The Boundary Control feature extends the data encryption capabilities of HyTrust DataControl by integrating Policy-based access control in HyTrust CloudControl. By placing geographical and/or label-based Policy Constraints, the encryption keys can be delivered only to the VM that resides in the specified Boundary.
Organizational Boundaries

Boundary Control can provide access control across departments in a large company that has big data centers and data is shared by different departments. In such companies, organizational boundaries provide data security and privacy across departments through Policy-based access control.

Regulatory Compliance

Many companies are subject to regulations such as the Payment Card Industry (PCI), Sarbanes-Oxley Act (SOX), Health Insurance Portability (HIPAA), and others. For many of these regulations, host systems for workloads subject to laws, rules, and regulations require that special configurations and controls must be in place so that all hosts in the infrastructure are compliant. A major portion of these compliance regulations requires that the information gathered must remain absolutely private.

These customers need an auditable and enforceable way to ensure that information subject to the regulation is only hosted, run, and decrypted on hosts properly configured and approved for compliance, and only retrieved by appropriately authorized end users.

CloudControl Updates for Boundary Control

The Boundary Control feature allows HyTrust KeyControl to perform authentication and authorization operations by accessing CloudControl APIs. In order to use Boundary Control, users must have certain privileges. The following new CloudControl privileges are available for this purpose:

- Asc.KeyDelivery: Authorizes the delivery of encryption keys.
- Asc.Register: Authorizes the KeyControl to register VMs with CloudControl.

A new default role called ASC_BCAdmin in CloudControl has both of these privileges. The ASC_BCAdmin credentials are used as a service account in HyTrust DataControl.

Boundary Control System Requirements

CloudControl Requirements for Boundary Control

The following are the system requirements for the Boundary Control feature:

- An appropriate license including activation of Boundary Control.
- Assign ASC_BCAdmin privileges to the service account that will be used by KeyControl to authorize against CloudControl.
- Create a new user group called HT_BCAdmin in Active Directory.
HyTrust KeyControl Requirements

- When converting CloudControl to Directory Service mode, map the ASC_BCAdmin role to HT_BCAdmin user group. For more information on Active Directory settings, see Integrating CloudControl with Active Directory on page 21.
- Create Labels and apply them to the appropriate resources. For more information, see Labels on page 81.
- If you are using ESXi hosts with Intel TXT to establish hardware-based trust, you need to create, assign, and provision PolicyTags. For more information, see PolicyTags on page 85.
- Create a default Boundary Control Rule. See Creating the Default Boundary Control Rule below.

Creating the Default Boundary Control Rule

3. Click OK.
4. On the Edit Rule page, check the Propagate checkbox to ensure that the rule propagates to all resources under the Appliance Root.
5. Under Constraints, click Add and add the Constraint Type Match VM Label(s) or Match Host Attribute(s) that you want to use. You can use either constraint type or both together.  
   Note: Before you can use the Match Host Attribute(s) constraint, you must create PolicyTags. For more information, see PolicyTags on page 85.
6. Click OK.
7. On the Policy > Rules page, click Assign to assign the new Boundary Control Rule to the HyTrust CloudControl Appliance Root as well as the registered VMs.
8. Click OK.
9. Deploy the policy.

Enabling Boundary Control

Perform the tasks in this section to enable Boundary Control.
Registering KeyControl with CloudControl

To establish access controls you must first register KeyControl with HyTrust CloudControl:

1. Login to HyTrust KeyControl.
2. Select Settings > Default Settings.
3. Click the Boundary Control tab and enter the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server</td>
<td>Enter the CloudControl IP address.</td>
</tr>
<tr>
<td>Login</td>
<td>Enter the login for the ASC_BCAdmin user group service account.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the password for the ASC_BCAdmin user group service account.</td>
</tr>
</tbody>
</table>

4. Click Register.

After Boundary Control is enabled in KeyControl, you can create Cloud VM Sets with Boundary Control enabled. You can apply Boundary Control rules to the VMs registered under these VM Sets.

HyTrust KeyControl communicates with CloudControl. CloudControl checks if it meets licensing requirements and establishes connection with KeyControl.

Creating a VM Set with Boundary Control Enabled

**Note:** You can enable the Boundary Control feature only when creating a new VM Set. You cannot disable the Boundary Control feature on a VM Set once it is created.

For more information on KeyControl, see the HyTrust DataControl Administration Guide.

1. Create a VM Set with Boundary Control enabled in HyTrust KeyControl using the following information:
   1. Enter the name of the VM set.
   2. Select Cloud Admin or KeyControl Admin.
   3. Enter an optional description.
   4. Check the Enable Boundary Control checkbox.
2. Register the VMs with KeyControl using the `hcl register` command in Linux or the Windows CLI.

```
[root@centos-bc1 ~]# hcl register -a -h centos-bc1 -d Testing 10.230.44.15
Please provide the KeyControl login details
username: secroot
password:

Available Cloud VM Sets
---------------------------------------------------------------
Boundary Control
No Boundary Control
DemoVmSet
---------------------------------------------------------------

Please specify Cloud VM Set to which this VM should be added: Boundary Control

Certificate passphrase might be required
Certificate successfully unpacked
Registered as centos-bc1 with KeyControl node(s) 10.230.44.15
Completing authentication for centos-bc1 on KeyControl node(s) 10.230.44.15
Authentication complete, machine ready to use
Getting KeyControl Mapping information

This VM can be added to one of the following KeyControl Mappings
1 : Boundary Control HTKC Mapping

Please select KeyControl Mapping (0 to skip): 1
KeyControl Mapping
server description kc1, ip 10.230.44.15, port 443
Updated KeyControl list with KeyControl nodes 10.230.44.15:443
[root@centos-bc1 ~]#
```

To register using the GUI, perform the following:
1. Login to the Windows VM.
2. Go to the Start menu and click on **HyTrust GUI** from the **HyTrust** menu.
3. In the DataControl Policy Agent window, click **Register** and enter the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KeyControl Name/IP</td>
<td>Enter the name or IP address of the KeyControl Server.</td>
</tr>
<tr>
<td>KeyControl Port</td>
<td>Enter the port number of the KeyControl server.</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the Cloud Administration username.</td>
</tr>
<tr>
<td>Password</td>
<td>Enter the Cloud Administration password.</td>
</tr>
<tr>
<td>Cloud VM Set</td>
<td>Enter the Boundary Control-enabled VM Set in which this VM will reside.</td>
</tr>
<tr>
<td>Sec KeyControl Name</td>
<td>Enter the second node in the KeyControl cluster.</td>
</tr>
<tr>
<td>Sec KeyControl Port</td>
<td>Enter the port for the second node in the KeyControl cluster.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Enter the name of the VM.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter an optional description of the VM registration.</td>
</tr>
</tbody>
</table>

4. Click **Register**.
   After a VM is authorized, you can view the authorization details in the CloudControl Log Viewer.
Authenticating a VM for Key Delivery

When a user requests access to an encryption key, the DataControl Policy Agent sends the VM information to the KeyControl Server. A sequence of events follows:

1. The KeyControl Server passes the VM information to CloudControl.
2. CloudControl checks the Rules and Constraints assigned to that VM.
3. CloudControl grants the access to the encryption keys only if the Constraint values on the VM match the constraint values in the Rule.

If CloudControl cannot authenticate VMs for key delivery, the data on the VMs that were authenticated by CloudControl during that interval is accessible until the current authentication interval expires. This can happen in the following scenarios:

- If password for BCAdmin is changed between the heartbeat/re-authentication intervals.

OR

- If CloudControl loses the connection with KeyControl.
The following figure shows the output of the hcl status command for the VM that was moved outside the Boundary.
App Links in CloudControl and DataControl

**Important:** App Links are supported for HyTrust DataControl 4.0 and greater releases.

App Links allow CloudControl to establish a secure HMAC encrypted channel between another trusted application. CloudControl creates a single use code that is valid for 10 minutes. During that interval, the code is shared with DataControl 4.0.

When configured, DataControl can securely communicate with CloudControl and DataControl user privileges can be restricted by role. You can use either default roles or custom roles to limit DataControl user privileges.

CloudControl administrators require the Management.AppLink.Create privilege to be able to create a single use code. By default, this privilege is restricted to the superadmin user group.

You can view active App Links on the App Links tab on the App Link page.

Creating an App Link One Time Code

The One Time Code is single use, and is valid for only 10 minutes.

**Important:** App Links are supported for DataControl 4.0 and greater releases.
1. Select **Configuration > App Links**.
2. On the App Links page, click the **One Time Code** tab.
3. Select the Role where you want to apply the App Link, for example, ASC_AppLinkAdmin.
4. Click **Submit**.

Use this One Time Code in the HyTrust KeyControl GUI to create the App Link.
Chapter 16. CloudControl with Auto Deployed ESXi Hosts

Auto Deploy Overview

You can use CloudControl to protect the ESXi hosts which are provisioned through Auto Deploy for vSphere versions 6.0 and 6.5. CloudControl does the following:

- Identifies the vCenter Servers that have Auto Deploy Service enabled.
- Monitors ESXi hosts that are provisioned through Auto Deploy for reboot. When the ESXi host is powered on, CloudControl reconfigures the ESXi host and recreates the service account provided the following conditions are met:
  - The root credentials of the ESXi host are not changed in the host profile that is attached to the ESXi host. Use the same credentials to add the ESXi host in CloudControl.
  - Both the FQDN and the IP address of the ESXi host should remain unchanged.

CloudControl supports Auto Deploy on stateless, stateless caching, and stateful ESXi hosts.

For more information, see Installing ESXi Using vSphere Auto Deploy in the ESXi and vSphere Server 6.0 documentation.

Auto Deploy Alerts

CloudControl generates Auto Deploy alerts using the vSphere Auto Deploy ESXi Config Alert. When enabled, these alerts are sent when:

- CloudControl fails to configure a protected auto deployed ESXi host upon reboot.
- If RPV is enabled for an auto deployed ESXi Host in pre-5.1 CloudControl, and CloudControl is upgraded to 5.1 or later, and the host is rebooted before you reenable RPV and run the Auto Deploy Status Refresh scheduled event.

For more information, see Upgrade CloudControl with Auto Deploy-enabled vCenter Servers on the next page.
Auto Deploy Scheduled Events

CloudControl uses the Refresh Auto Deploy Status scheduled event to ensure that the ESXi hosts under the Auto Deploy-enabled vCenter remain protected. You can enable the Refresh Auto Deploy Status on the Compliance > Scheduled Events page.

When the Refresh Auto Deploy Status scheduled event runs, it checks all protected vCenters to detect if they have enabled Auto Deploy, and if Auto Deploy service is running. If Auto Deploy is disabled, then CloudControl does not monitor reboot detection for the ESXi hosts for that vCenter Server. If Auto Deploy is enabled, then CloudControl starts tracking the ESXi hosts under the vCenter Server for reboot detection.

For more information, see Scheduled Events on page 51.

Upgrade CloudControl with Auto Deploy-enabled vCenter Servers

When you upgrade CloudControl, you should manually run the Refresh Auto Deploy Status scheduled event to locate any protected vCenter Servers with the Auto Deploy Service enabled.

If alerts are not enabled, the error message is logged and displays in the Log Viewer. For more information, see Log Viewer on page 130

**Important:** The IP address and the root password should not be changed for the CloudControl protected auto-deployed hosts.

RPV Considerations

If any protected ESXi host is RPV enabled, perform the following tasks before rebooting the host:

1. Disable RPV.
2. Provide the root credentials that are specified in the Host profile.
3. Enable RPV.
4. Run the Refresh Auto Deploy Status scheduled event.

Check Compliance Drift

After the host state changes to Power on, CloudControl assesses the host using the last known template, if any. Use the dashboard to check for possible Compliance Drift. If Compliance Drift occurs, we recommend that you use the Remediate action.
Chapter 17. Using the vSphere HTML5 Client

You can access the vSphere Client through CloudControl. The vSphere Client is supported for vSphere versions 6.5 through 6.7.

**Important:** CloudControl does not support the embedded Platform Services Controller (PSC) in the vSphere Client. Users who log into the vSphere Client using the CloudControl proxy cannot access the PSC UI without specific VMware privileges, and any PSC UI operations are not authorized or logged by CloudControl.

**Note:** If a vSphere Client user attempts to perform operations that are not allowed, a warning icon is displayed at the bottom-right of the screen instead of a browser pop-up window.

**Download and Import the vSphere Client Metadata**

You must import the HTML5 client metadata for each host that you want to use to access the vSphere Client.

1. Select **Compliance > Hosts**.
2. Select a vCenter Web Client Server from your list of hosts.
3. Click **Download HTML5 Client Metadata** to download the metadata file.
   **Note:** If the metadata buttons are not visible, you may be missing the Asc.SAMLConfig privilege. Contact your CloudControl administrator to have the Asc.SAMLConfig privilege added.
4. Log directly into WCS as administrator. Do not use the PIP.
5. From the **Home** icon, select **Administration > Single Sign-on > Configuration**.
6. On the Configuration page, click **SAML Service Providers**, then click **Import** to import the metadata file that you downloaded.
   **Note:** You may need to install a certificate if you have not previously configured the web client. For more information, see **Managing Certificates** on page 55.

**Running the vSphere Client using the PIP**

1. Open a browser and log in to the vSphere Client.
   The vSphere Client is located at the following address: https://<pip-address>/ui.
2. Verify that you can view the host where you imported the HTML5 client metadata.
Appendix A. Default Roles and Permissions

CloudControl ships with a number of preconfigured roles to help administrators configure granular role-based access controls (RBAC) in the virtual environment. A role is a collection of access privileges. Each access privilege is mapped to a specific operation. For example, power on VM operation is mapped to the VirtualMachine.Interact.PowerOn privilege, and this privilege belongs to a few roles such as ASC_VMPowerUser and ASC_SuperAdmin.

The ASC_SuperAdmin role is the super-set of all access privileges available in CloudControl. A user mapped to this role is capable of performing any operation in the virtual/cloud environment as well as configuring the CloudControl appliance itself.

The CloudControl preconfigured roles are grouped into the following categories:

- **NSX Roles** on the next page
- **vSphere 6.x Roles** on page 184
- **CloudControl Appliance Management** on page 186
- **Other Roles** on page 187
NSX Roles

NSX roles define what access users can have to the NSX resource. The following preconfigured NSX roles are shipped with CloudControl:

- ASC_SecurityAuditor
- ASC_SecurityOperator
- ASC_SecurityAdministrator
- ASC_LoadBalanceAdmin
- ASC_NetworkOperator
- ASC_NetworkEngineer

**Note:** No NSX roles have privileges to operate within the virtual infrastructure.

<table>
<thead>
<tr>
<th>CloudControl Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASC_SecurityAdmin</td>
<td>Users with the ASC_SecurityAdmin role have access to CloudControl and NSX resources. They can define policies in CloudControl, apply Firewall policies, and have CUD privileges on Security Groups, Security Policies, Firewalls, Firewall Rules, ACLs, and Security Profiles.</td>
</tr>
<tr>
<td>ASC_SecurityOperator</td>
<td>Users with the ASC_SecurityOperator role have read-only access to core security-related resources, including Firewalls, Security Groups, Security Policies, Security Tags, IP Sets, MAC Sets, Services, Service Groups, and Flow-Monitored objects. They can access the CloudControl dashboard and view configured policies and violation reports.</td>
</tr>
<tr>
<td>ASC_SecurityAuditor</td>
<td>Users with the ASC_SecurityAuditor role have read-only access to security-related resources, including Security Groups, Security Policies, Firewalls, Firewall Rules, ACLs, and Security Profiles. These users have no access to the CloudControl dashboard.</td>
</tr>
</tbody>
</table>
### vSphere 6.x Roles

The vSphere role category contains the following roles:

- ASC_BasicLogin
- ASC_BackupAdmin
- ASC_VMUser
- ASC_VMPowerUser
- ASC_VIAdminUser
- ASC_StorageAdmin
- ASC_ESXAdmin
- ASC_ESXAdmin
- ASC_DCAdmin
- ASC_NetworkAdmin

<table>
<thead>
<tr>
<th>CloudControl Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASC_NetworkEngineer</td>
<td>Users with the ASC_NetworkEngineer role have full access to most networking resources, including Logical Switches, Routers, Firewall, Network Service Containers and Services, Transport Zones, and IP Pools. They have read-only access to core security-related resources such as Security Groups, Security Policies, ACLs, and Security Profiles, and have no access to the CloudControl dashboard.</td>
</tr>
<tr>
<td>ASC_LoadBalancerAdmin</td>
<td>Users with the ASC_LoadBalancerAdmin role have full access to Load Balancer-related resources, including Load Balancers, VIPs, Pools, and Pool members. They have read-only access to other networking resources and have no access to the CloudControl dashboard.</td>
</tr>
<tr>
<td>ASC_NetworkOperator</td>
<td>Users with the ASC_NetworkOperator role have read-only access to most networking resources, including Logical Switches, Routers, Network Service Containers and Services, Transport Zones, and IP Pools. They have no access to security-related resources, and have no access to the CloudControl dashboard.</td>
</tr>
<tr>
<td>CloudControl Role</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Backup Administrator (ASC_BackupAdmin)</td>
<td>Users with the ASC_BackupAdmin role can back up and restore virtual machines (guests).</td>
</tr>
<tr>
<td>Basic Login (ASC_BasicLogin)</td>
<td>Users with the ASC_BasicLogin role can perform some basic operations, such as login.</td>
</tr>
<tr>
<td>Datacenter Administrator (ASC_DCAdmin)</td>
<td>Users with the ASC_DCAdmin role can set up VMware vCenter Server data centers and perform actions on all resources within virtual datacenters.</td>
</tr>
<tr>
<td>ESXi Maintenance Administrator</td>
<td>Users with the ASC_ESXMAdmin role can install patches, change ESXi host configurations, and reboot ESXi hosts. They can also perform ESXi host maintenance (use SSH, change configuration, reboot, configure SSL, Virtual Resource Pools management) and CloudControl configuration, assessment, and remediation (ARC). These users have no virtual machine privileges.</td>
</tr>
<tr>
<td>Network Administrator (ASC_NetworkAdmin)</td>
<td>Users with the ASC_NetworkAdmin role can manage virtual switches, network resource pools, VLANs, and other network configuration settings.</td>
</tr>
<tr>
<td>Storage Administrator (ASC_StorageAdmin)</td>
<td>Users with the ASC_StorageAdmin role can define VMFS volumes and mapping to LUNs including masking and zoning. They can define iSCSI access paths, manage NFS volumes, manage HSM and data retention, administer storage and disk replacement, manage backups, manage datastores and datastore clusters, and perform datastore copy, move, rename, upload and download operations in datastore files.</td>
</tr>
<tr>
<td>Virtual Infrastructure Administrator (ASC_VIAdmin)</td>
<td>Users with the ASC_VIAdmin role can perform virtual infrastructure operations including configuring DRS and VMware HA, initiate VMotion, assign hosts to resource pools, and Virtual Resource Pools and guest aliases management. They have limited privileges on ESXi hosts.</td>
</tr>
<tr>
<td>Virtual Machine Power User (ASC_VMPowerUser)</td>
<td>Users with the ASC_VMPowerUser role can perform actions on virtual machines and resource objects, including view and change most virtual machine configuration settings, guest alias management, take snapshots, and schedule tasks. These users have all privileges for scheduled task privileges group, and selected privileges for global items, datastore, and virtual machine privileges groups. However, they do not have privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups.</td>
</tr>
<tr>
<td>Virtual Machine User (ASC_VMUser)</td>
<td>Users with the ASC_VMUser role can interact with virtual machines, but not change the virtual machine configuration. They have full privileges for the scheduled task privileges group and selected privileges for the global items and virtual machine privileges groups. However, they do not have privileges for folder, datacenter, datastore, network, host, resource, alarms, sessions, performance, and permissions privileges groups.</td>
</tr>
</tbody>
</table>
CloudControl Appliance Management

CloudControl appliance management roles define what access users have to the CloudControl appliance itself. It contains the following roles:

- ASC_ARCAssessor
- ASC_ApplAdmin
- ASC_ARCArCAdmin
- ASC_RoleAdmin
- ASC_PolicyAdmin
- ASC_CoreApplAdmin
- ASC_VMPowerUser

### CloudControl Appliance Management Roles

<table>
<thead>
<tr>
<th>CloudControl Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudControl Administrator (ASC_ApplAdmin)</td>
<td>Users with the ASC_ApplAdmin role can install CloudControl and configuration networking, HA, and logging. They have no privileges to manipulate the virtual infrastructure.</td>
</tr>
<tr>
<td>ARC Administrator (ASC_ARCArCAdmin)</td>
<td>Users with the ASC_ARCArCAdmin role can create and modify ARC templates, add ARC targets, assess ARC, and remediate ARC.</td>
</tr>
<tr>
<td>ARC Assessor (ASC_ARCAssessor)</td>
<td>Users with the ASC_ARCAssessor role can perform ARC assessments and view ARC results.</td>
</tr>
</tbody>
</table>
### CloudControl Role

<table>
<thead>
<tr>
<th>CloudControl Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Appliance Administrator (ASC_CoreApplAdmin)</td>
<td>Users with the ASC_CoreApplAdmin role can install and configure core appliance virtual machines.</td>
</tr>
<tr>
<td>Policy Administrator (ASC_PolicyAdmin)</td>
<td>Users with the ASC_PolicyAdmin role can create and modify policies, labels, and constraints.</td>
</tr>
<tr>
<td>Role Administrator (ASC_RoleAdmin)</td>
<td>Users with the ASC_RoleAdmin role can create and modify roles and privileges.</td>
</tr>
<tr>
<td>Virtual Machine Power User (ASC_VMPowerUser)</td>
<td>Users with the ASC_VMPowerUser role can perform actions on virtual machines and resource objects, including view and change most virtual machine configuration settings, guest alias management, take snapshots, and schedule tasks. These users have all privileges for scheduled task privileges group, and selected privileges for global items, datastore, and virtual machine privileges groups. However, they do not have privileges for folder, datacenter, network, host, resource, alarms, sessions, performance, and permissions privileges groups.</td>
</tr>
</tbody>
</table>

### Other Roles

CloudControl also ships with the following predefined roles:

<table>
<thead>
<tr>
<th>CloudControl Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASC_ThirdParty</td>
<td>Users with the ASC_ThirdParty role can execute REST calls from ThirdParty applications.</td>
</tr>
<tr>
<td>ASC_BCAAdmin</td>
<td>Users with the ASC_BCAAdmin role can perform key delivery and registration operations for the Boundary Control feature.</td>
</tr>
<tr>
<td>ASC_AppLinkAdmin</td>
<td>Users with the ASC_AppLinkAdmin role can perform key delivery and registration operations for the Boundary Control feature, as well as applink and label operations. They have read, view, create and update privileges as well as API access.</td>
</tr>
</tbody>
</table>
Appendix B. Root Password Recovery

For the purpose of emergency recovery, ESXi host root passwords are encrypted with a strong key derived from the user provided passcode and forwarded to the syslog server for inclusion in the asc.log file.

**Important:** We recommend that you export all log files to a SIEM or syslog tool to insure the RPV logs and hashes are exported and not stored in CloudControl.

1. Deploy a new CloudControl using the OVA file. The new CloudControl must be the same version and build number as the CloudControl that failed.

2. Power on the new CloudControl and log in as ascadminuser with the password `Pa$w0rd123!`.

3. Assign new credentials to the local CloudControl administrator account (ascadminuser). For more information, see Changing the ascadminuser Password on page 62.

4. Obtain the passcode that was assigned when Root Password Vaulting was initially configured in CloudControl:
   a. Obtain a copy of the CloudControl logs with the last 15 days of events if the RPV settings are set to the default of 5 days (3 cycles).
      **Note:** If the RPV settings are set to 30 days, we recommend obtaining 3 log cycles (3 x 30 = 90 days of RPV hashes).
   b. Locate the HEX strings of the encrypted username and password in the logs for each host where the password needs to be recovered (addresses and hashes will vary between hosts).

   Filter syslog:
   - Category (actionCategory): ARC
   - MSG ID (msgId) = ARC0032
   - Description: Update root account
5. Retrieve the root account password using the following command:

```
host <IP address> to <username_hash> - <password_hash>
```

The syslog output will be in the following format (per host):

```
Update root account: host <IP address> to <username_hash> - <password_hash>
```

<table>
<thead>
<tr>
<th>Description</th>
<th>Resource Name</th>
<th>Resource Type</th>
<th>Destination</th>
<th>Policy</th>
<th>Category</th>
<th>Msg ID</th>
</tr>
</thead>
</table>

6. In the CloudControl console instance that you opened in Step 2, enter the following command to recover the root password:

```
recoverpassword -k '<original-RPV-password>' -u <username_hash> -p <password_hash>
```

If there have been RPV algorithm changes, you can also add the -a <algorithmValue> variable.

Example: `recoverpassword -k 'Test@1234' -u 84373E37A739F3B807D50AB1CE003D -p B315DF3AB5730F2276E00DF529A19454F3BDCF89346E1E6BA8EFE87827D44B -a 3`

**Note:** To avoid Unix shell misinterpreting or ignoring special characters, enclose the password in single quotes at the command line.
Appendix C. Search Filters

CloudControl allows you to search for the following policy resource attributes:

- Description
- FQDN
- Friendly Name
- IP Address
- Label
- Patch Level
- Published IP Address
- Resource Type
- RuleSet
- Template Type
- Trust Status

You can refine your searches using the following wild-card characters:

Search Wildcard Characters

<table>
<thead>
<tr>
<th>Character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>?</td>
<td>Replace a single character.</td>
</tr>
<tr>
<td>*</td>
<td>Replace one or more characters.</td>
</tr>
</tbody>
</table>

**Note:** By default, the search returns results matching any of the specified terms (an OR operation). Enclose the words with quotation marks to return results that match the exact string (an AND operation).

The CloudControl Management Console Search page (General > Search) contains filters, in the form of check-boxes, to help you narrow down the search results to certain resource types in a typical network.

Below is the list of available filters.

- Cluster
- DataCenter
- Datastore
- Folder
- Host
- Network
- Portgroup
- Resource Pool
- Show Archived Versions
- Virtual Application
- Virtual Center
- Virtual Machine

**Note:** The **Show Archived Versions** filter extends the search to older policies that have been archived. These policies are hidden from normal search results.
Using the CloudControl CLI

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

- the vSphere Client Console tab
- the vCenter Server Console
- an SSH session using the ascadminuser account.

Type `asc` in the CLI to view the available CloudControl CLI commands. To learn more about each command, type the full name, for example `asc backup`. You can also include the `-h` or `--help` option for detailed syntax usage.

**Note:** For all values that contain spaces, you should surround them by a single quote. For example: `asc monitor -m 'This is a test.'`

**asc auth**

Use this command to run user authentication and authorization tests.
Syntax

asc auth [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --iterations &lt;count&gt;</td>
<td>The number of times in integers to repeat the authentication or authorization test. If the count is not specified, the default value is 1.</td>
</tr>
<tr>
<td>-l, --listoperations</td>
<td>List all authorization test operations.</td>
</tr>
<tr>
<td>-o, --operation &lt;op&gt;</td>
<td>The operation to use for the authorization test.</td>
</tr>
<tr>
<td></td>
<td>Note: The --operation option requires the --target option.</td>
</tr>
<tr>
<td>-p, --password &lt;password&gt;</td>
<td>The Active Directory user password.</td>
</tr>
<tr>
<td></td>
<td>Note: The password can also be specified using the HTPW environment variable.</td>
</tr>
<tr>
<td>-t, --target &lt;IP_address&gt;</td>
<td>The IP address of the protected host to use for policy and rules evaluation.</td>
</tr>
<tr>
<td>-u, --username &lt;username&gt;</td>
<td>The Active Directory username to test.</td>
</tr>
</tbody>
</table>

Examples

Authenticate the user joe:

HTCC$ asc auth -u joe -p joespass

List all authentication and authorization test operations:

HTCC$ asc auth -l

Authorize the AddHost operation for the user abc on the host 10.1.10.105:

HTCC$ asc auth -u abc -o AddHost -t 10.1.10.105

asc backup

Use this command to backup and restore the CloudControl configuration. You can use the backup files for disaster recovery and configuration migration.

Syntax

asc backup [options]
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>-b, --backup [file]</code></td>
<td>Create a configuration backup archive. Specifying the archive file name is optional.</td>
</tr>
<tr>
<td><code>-h, --help</code></td>
<td>Display usage text.</td>
</tr>
<tr>
<td><code>-n, --nocrypt</code></td>
<td>Create an unencrypted backup image. Unencrypted backup data must be stored and transported securely. Must be used with the <code>asc backup</code> command. Once you use the <code>--password</code> option, you can no longer use the <code>--nocrypt</code> option on the same backup file.</td>
</tr>
<tr>
<td><code>-p, --password &lt;password&gt;</code></td>
<td>Set or verify the configuration backup archive password. The configuration backup archive password can also be specified using the <code>PASSWORD</code> environment variable. For example, <code>export PASSWORD='secret123!'</code>. If a password was specified when you created the archive, you must use the <code>--password</code> option to restore the archive. <strong>Important:</strong> Once you use the <code>--password</code> option, you can no longer use the <code>--nocrypt</code> option on the same backup file.</td>
</tr>
<tr>
<td><code>-r, --restore [file]</code></td>
<td>Restore a configuration backup archive. This option uses the CD-ROM by default or takes an optional backup ISO filename. The <code>--password</code> argument or environment variable is required if the archive is encrypted.</td>
</tr>
<tr>
<td><code>-t, --test</code></td>
<td>Validate the command line arguments without performing any actions.</td>
</tr>
<tr>
<td><code>-v, --verify [file]</code></td>
<td>Validate the configuration backup archive file. This option uses the CD-ROM by default or takes an optional backup ISO filename. The <code>--password</code> argument or environment variable is required if the archive is encrypted.</td>
</tr>
<tr>
<td><code>--setpassword</code></td>
<td>Sets the default password used to encrypt the backup archive.</td>
</tr>
</tbody>
</table>
| `--setlocation` | Sets the default location used to archive the backup ISO. Use one of the following parameters:  
  - `scp://<user>:<password>@<host>/<destination_directory>`  
  - `nfs://<host>/<destination_directory>`  
  - `local`  
  **Note:** All parameters are validated, and passwords are not logged. |
| `--getlocation` | Retrieves the location used to store the backup images using `--setlocation`. If the location includes a password, it will be obfuscated.                                                                 |
| `--schedule` | Set the schedule for the backup job. Requires the `--interval` parameter.                                                                                                                                 |
Option | Description
--- | ---
--interval | The frequency to perform the backup used with the schedule command. This can be one of the following:
- d—days
- h—hours
- m—minutes
Setting the schedule overwrites any existing schedule. Schedules can be manually modified with 'crontab -e'.
--setcopies | Sets the number of backup images to keep. Set to '0' to retain all copies.
--getcopies | Retrieves the number of backup images that you set.
--unschedule | Deletes the schedule. This can also be achieved with 'crontab -r'.
--start <time> | Specifies when the backup will be run. Requires the time in hh:mm format.

Examples

Create an encrypted backup with a specified filename:
```
asc backup --backup /tmp/20120515_backup.iso --password 'secret123!'  
```
Create an encrypted backup with the default filename:
```
export PASSWORD='secret123!'  
asc backup --backup
```
Create an unencrypted backup with the default filename:
```
asc backup --backup --nocrypt
```
Validate a backup file:
```
asc backup --verify /tmp/20120515_backup.iso --password 'secret123!'  
```
Validate a backup on the CD-ROM:
```
asc backup --verify --password 'secret123!'  
```
Restore an encrypted backup file:
```
asc backup --restore /tmp/20120515_backup.iso --password 'secret123!'  
```
Restore an encrypted backup from the CD-ROM:
```
asc backup --restore --password 'secret123!'  
```
```
or
export PASSWORD='secret123!'  
asc backup --restore
```
Create an ongoing remote backup at the specified location.
asc backup --setlocation scp://admin:password123@10.1.1.1/root/backups --setcopies 5 --schedule --start 03:45 --interval 24h

Retrieve the remote location information:
asc backup --getlocation

asc certs

Use this command to manage x509 and CA certificates.

Syntax

asc certs [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --authority</td>
<td>Use this option when performing operations on a certificate authority (CA) certificate set.</td>
</tr>
</tbody>
</table>
| -b or --bulkimport | Perform bulk import of certificates from hosts into the database. The following options are available for this command:  
  -f or --bulkfile—Specifies the bulk input file for '--bulkimport' option.  
  --bulkchain—Walk the certificate chain when using '--bulkimport'.  
  -y or --yes—Do not prompt for response. Currently used when performing '--bulkimport'.  
  **Note:** This command imports vCenter and ESXi host certificates, not PCS certificates. |
| -c, --cert [file] | The fully qualified certificate target file path. The contents of this file are overwritten. This option defines the certificate file location automatically. |
| --cabundle      | By default, CloudControl contains a bundle of certificates, but they are not imported. Use this command if you want to import the certificate bundle. The following options are available for this command:  
  enable—Imports the certificate bundle into your installation.  
  refresh—Refreshes the existing certificate bundle.  
  disable—Removes the certificate bundle from your installation. |
| -d, --delete <service> | Delete the specified CA certificate by service name.  
  **Implies:** --authority. |
| --fipsmodeon     | Enables FIPSMode |
| --fipsmodeoff    | Disables FIPSMode |
| -g, --genselfsigned [file] | Generate a self-signed certificate using a local key.  
  This option accepts a temporary fully qualified filename as an argument with certificate data as contents. See --c or --csr help text for file content syntax. |
<p>| -h, --help       | Display usage text. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-i, --import &lt;file&gt;</td>
<td>Validate and install a certificate issued by a CA. Requires a temporary qualified filename as an argument. The temporary file contains the certificate as issued by the certificate authority. The -s option is also required.</td>
</tr>
<tr>
<td>-k, --key [file]</td>
<td>The fully qualified key target file path. The contents of this file are overwritten. Specifying the -s option defines the key file location automatically.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Lists the certificates installed locally and descriptions of each. List output is one certificate per line with each value separated by a double length underscore (__) . The format is as follows:</td>
</tr>
<tr>
<td></td>
<td>svc_t__cn_o_l_st_c__ou__exp_isd_s__</td>
</tr>
<tr>
<td></td>
<td>icn_io_iou_v</td>
</tr>
<tr>
<td></td>
<td>Where:</td>
</tr>
<tr>
<td></td>
<td>- svc—Service name. Valid values are gui, sso_signing, or sso_encryption.</td>
</tr>
<tr>
<td></td>
<td>- t—Type. Valid values are ss (self-signed) or ext (external).</td>
</tr>
<tr>
<td></td>
<td>- cn—Common name</td>
</tr>
<tr>
<td></td>
<td>- c—Organization</td>
</tr>
<tr>
<td></td>
<td>- l—Locality</td>
</tr>
<tr>
<td></td>
<td>- st—State/region</td>
</tr>
<tr>
<td></td>
<td>- c—Country code</td>
</tr>
<tr>
<td></td>
<td>- ou—Organizational unit</td>
</tr>
<tr>
<td></td>
<td>- exp—Expiration date stamp or the duration in days for CSR/self-signed generation</td>
</tr>
<tr>
<td></td>
<td>- isd—Issued date stamp</td>
</tr>
<tr>
<td></td>
<td>- s—Serial number (real certs only)</td>
</tr>
<tr>
<td></td>
<td>- v—TLS version</td>
</tr>
<tr>
<td></td>
<td>- icn—Issuers common name</td>
</tr>
<tr>
<td></td>
<td>- io—Issuers organization</td>
</tr>
<tr>
<td></td>
<td>- iou—Issuers organizational unit</td>
</tr>
<tr>
<td></td>
<td>- key—Key length in bits</td>
</tr>
<tr>
<td></td>
<td>- dns—DNS Subject Alternative Name fields (comma separated)</td>
</tr>
<tr>
<td></td>
<td>- ips—IP Subject Alternative Name fields (comma separated)</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| -q, --csr | Generate a certificate request using a local key. This option accepts a temporary qualified filename as an argument with certificate data as contents. One entry per line prefixed by a two character certificate datatype identifier. Sample temporary file contents (field separator is ' _'): svc_t_cn_o_l_st_c_ou_exp_isd_s_v_icn_io_iou_key_dns_ips Where:  
  - svn—Service name. Valid values are: gui—CloudControl Management Console ssoSigning—CloudControl  
  - cn—Common name  
  - o—Organization  
  - l—Locality  
  - st—State/region  
  - c—Country code  
  - ou—Organizational unit  
  - exp—Expiration date stamp or the duration in days for CSR/self-signed generation  
  - dns—DNS Subject Alternative Name fields (comma separated)  
  - ips—IP Subject Alternative Name fields (comma separated) |
| -r, --random <length> | Generate a random string of the specified length. |
| --rotate | Perform password rotation for the secure keystore Note: This will restart CloudControl. |
| --sandns | Returns a list of DNS entries of the CloudControl appliance and protected resources to be added as SAN entries to certificates and certificate requests. |
| --sanips | Returns a list of IP addresses of the CloudControl appliance and protected resources to be added as SAN entries to certificates and certificate requests. |
| -s, --service | The service to apply the certificate to. Valid values are: gui—CloudControl Management Console log—CloudControl Logging Service |
| -t, --csrtool | Runs the CSR tool which allows user to generate a CSR with SAN. |
| -v, --verbose | Enable verbose output. |
| -vv | Enable debug output. |

**Examples**

Import all certificates from CloudControl-protected hosts:

`asc certs -b -y`

List all certificates installed:

`asc certs -l`
List all certificate authority (CA) certificates:

`asc certs -l -a`

Validate and install a certificate for the CloudControl Management Console service:

`asc certs -s gui --import /tmp/newCert.pem`

Export the current key and certificate to files:

`asc certs -k /foo/mykey.pem -c /foo/ssCert.pem`

Delete the ca0025 service certificate authority certificate:

`asc certs -a -d ca0025`

Generate a 32 character random string:

`asc certs -r 32`

Imports the bundle of certificates:

`asc certs -cabundle enable`

Import the SSO signing keys:

`asc certs -i /usr/local/asc/etc/ssosigncert.pem -s sso_signing`

Enable FIPS mode:

`asc certs --fipsmodeon`

Discover the DNS entries that can be added as SAN entries:

`asc certs --sandns`

Discover the IP addresses that can be added as SAN entries:

`asc certs --sanips`

**asc firewall**

Use this command to manage firewall services.

### Syntax

```
asc firewall [options]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add &lt;IP_address&gt;</td>
<td>Add the specified protected host to the firewall.</td>
</tr>
<tr>
<td>-c, --class [x]</td>
<td>The type of host to be protected. This option defines the default proxy and forward settings for the specified class type. The x option implies a source rule exception.</td>
</tr>
<tr>
<td>--cleanRSAkeys true</td>
<td>Removes the SSH RSA key fingerprints from /root/.ssh/known_hosts and /home/ascadminuser/.ssh/knownhosts for all protected ESXi hosts in CloudControl.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-cp, --closeport</td>
<td>Block access to the specified local TCP and UDP ports on the appliance.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td></td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Lists all protected hosts, proxy redirects, and port forwards. This can be</td>
</tr>
<tr>
<td></td>
<td>combined with the -class option to filter results.</td>
</tr>
<tr>
<td>-m, --message</td>
<td>Specify the message to use in log files and configuration file change</td>
</tr>
<tr>
<td>&lt;message&gt;</td>
<td>journals for firewall related activities.</td>
</tr>
<tr>
<td>-op, --openport</td>
<td>Open access to the specified local TCP and UDP ports on the appliance.</td>
</tr>
<tr>
<td>&lt;port&gt;</td>
<td></td>
</tr>
<tr>
<td>-r, --remove</td>
<td>Remove the specified protected host from the firewall.</td>
</tr>
<tr>
<td>&lt;IP_address&gt;</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

Add an IP address proxy exception. The IP address will not be proxied.

```bash
asc firewall -a 1.2.3.4 -c x
```

List all firewall exception IP addresses:

```bash
asc firewall -l -c x
```

Remove a firewall exception by IP address:

```bash
asc firewall -r 1.2.3.4
```

Disable access to port 8091:

```bash
asc firewall -cp 8091
```

Enable access to port 8091:

```bash
asc firewall -op 8091
```

Remove the SSH RSA key fingerprints for all protected ESXi hosts.

```bash
asc firewall --cleanRSAkeys true
```

**asc ha**

Use this command to manage OS and application-level High Availability (HA) on CloudControl.

**Syntax**

```bash
asc ha [options]
```
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --disband</td>
<td>Disconnect the CloudControl from the HA cluster. This can be run from the primary or secondary CloudControl nodes.</td>
</tr>
<tr>
<td>--disable-password-sync</td>
<td>Enables the synchronization of the 'ascadminuser' password.</td>
</tr>
<tr>
<td>--dualSiteHaConf</td>
<td>Used to add and modify VIP and PIP configuration for the secondary host to allow your primary and secondary PIP to be located in separate subnets. See the Configuring High Availability chapter in the Installation Guide for HyTrust CloudControl for full usage instructions.</td>
</tr>
<tr>
<td>--dualSiteHaConf --list</td>
<td>Lists the contents of the VIP and PIP configuration file for the dual site HA configuration.</td>
</tr>
<tr>
<td>--dualSiteHaConf --delete</td>
<td>Deletes the existing VIP and PIP configuration file for the dual site HA configuration.</td>
</tr>
<tr>
<td>-e, --peertest</td>
<td>Test the health of the remote system and automatically failover if needed.</td>
</tr>
<tr>
<td>--enable-password-sync</td>
<td>Enables the synchronization of the 'ascadminuser' password.</td>
</tr>
<tr>
<td>-f, --failover {auto</td>
<td>manual}</td>
</tr>
<tr>
<td></td>
<td>• auto—Enable automatic failover. The secondary CloudControl can assume primary functions if the primary CloudControl has been offline for the timeout interval.</td>
</tr>
<tr>
<td></td>
<td>• manual—Disable automatic failover.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>--haclean</td>
<td>Clean old HA sync data keeping only the three most recent data sets. Use --haclean --all to clear all HA sync data sets.</td>
</tr>
<tr>
<td>--interval &lt;minutes&gt;</td>
<td>Sets the data synchronization period, in minutes, between CloudControl nodes. The default is 10 minutes, and the valid range is 2-1440 minutes.</td>
</tr>
<tr>
<td>-j, --join</td>
<td>Join two CloudControl nodes to create an HA cluster. This can be run from either the primary or secondary node. This requires the IP address and password for the node that you want to join, and the status (mode) of the node you are joining from.</td>
</tr>
<tr>
<td>-o, --mode {primary</td>
<td>secondary}</td>
</tr>
<tr>
<td></td>
<td>• primary—The main CloudControl node where all traffic is routed.</td>
</tr>
<tr>
<td></td>
<td>• secondary—The backup or standby CloudControl node.</td>
</tr>
<tr>
<td></td>
<td>Changing the HA mode triggers a failover event.</td>
</tr>
<tr>
<td>-n, --nosync</td>
<td>Do not perform an initial synchronization of data between HA nodes during a join, or prior to initiating a failover.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-p, --password &lt;password&gt;</td>
<td>The password of the remote CloudControl. Required when joining an HA cluster. Optionally, the password can be supplied via the HTHAPW environment variable.</td>
</tr>
<tr>
<td>-s, --sync</td>
<td>Forces an immediate synchronization of data between HA CloudControl nodes.</td>
</tr>
<tr>
<td>--sshkeyrotate</td>
<td>Rotates the SSH keys on the primary and secondary nodes of an existing cluster. After rotating, use the asc ha --status command to verify. Note: If there is a failure during key rotation, disband the cluster on both nodes and reform using the asc ha --setup command.</td>
</tr>
<tr>
<td>--sshkeytest</td>
<td>Tests the network connection between the two HA CloudControl nodes and verifies the SSH keys.</td>
</tr>
<tr>
<td>-t, --status</td>
<td>View the current configuration and operational state of the HA cluster.</td>
</tr>
<tr>
<td>-u, --timeout &lt;minutes&gt;</td>
<td>Sets the primary CloudControl monitoring minimum time threshold, in minutes, before an automatic failover event occurs. The minimum value is 10.</td>
</tr>
<tr>
<td>-v, --pollinterval &lt;minutes&gt;</td>
<td>Sets the health monitoring period, in minutes, before automatic failover mode is enabled.</td>
</tr>
<tr>
<td>--virtual-ip</td>
<td>Set the CloudControl Service IP address.</td>
</tr>
</tbody>
</table>

**Examples**

Trigger a failover event from the secondary node:

```
asc ha --mode primary
```

Synchronize and trigger a failover event from the primary node:

```
asc ha --sync --mode secondary
```

View the HA configuration and status:

```
asc ha --status
```

Create an HA cluster from the primary CloudControl node:

```
asc ha --join <secondary-IP-address> --password SecondaryS3crEt --mode primary
```

Create an HA cluster from the secondary CloudControl node:

```
asc ha --join <primary-IP-address> --password PrimaryS3crEt --mode secondary
```

Leave the HA cluster from either the primary or secondary node:

```
asc ha --disband
```

Enable automatic failover:

```
asc ha --failover auto
```

Disable automatic failover:
asc ha --failover manual

**Perform an automatic failover immediately:**

asc ha --failover now

**Set up HA with a remote secondary node and one PIP:**

asc ha --dualSiteHaConf

Do you want configure VIP for secondary?(yes/no) yes

Configuring : VIP

Primary FQDN [test.hytrust.com]:
Primary VIP [10.222.73.214]:
Primary Netmask [255.255.0.0]:
Secondary FQDN [test.hytrust.com]:
Secondary VIP [10.222.73.215]:
Secondary Netmask [255.255.255.0]:

Configuring : PIP

vCenter Published DNS on Primary [vcsa31-pip.test.hytrust.com]:
vCenter PIP on Primary [10.222.73.219]:
Primary Netmask [255.255.0.0]:
vCenter Published DNS on Secondary [vcsa31-pip.test.hytrust.com]:
vCenter PIP on Secondary [10.222.73.220]:
Secondary Netmask [255.255.255.0]:

Do you want to configure PIP for secondary node?(yes/no) no

Success: The High Availability system has been updated

**Listing the dual HA setup configuration:**

asc ha --dualSiteHaConf --list

Type : VIP
Primary FQDN : test.hytrust.com
Primary IP : 10.222.73.213
Primary Netmask : 255.255.0.0
Secondary FQDN : test.hytrust.com
Secondary IP : 10.222.73.212
Secondary Netmask : 255.255.255.0

Type : PIP
Primary FQDN : vcsa31-pip.test.hytrust.com
Primary IP : 10.222.73.219
Primary Netmask : 255.255.0.0
Secondary FQDN : vcsa31-pip.test.hytrust.com
Secondary IP : 10.222.73.218
Secondary Netmask : 255.255.255.0
Success: The High Availability system has been updated

Deleting a dual HA setup configuration:
asc ha --dualSiteHaConf --delete
Do you want to delete VIP configuration for test.hytrust.com - 10.222.73.214? (yes/no) no
Do you want to delete PIP configuration for vcsa31-pip.test.hytrust.com - 10.222.73.219? (yes/no) no
Do you want to delete PIP configuration for vc2.test.hytrust.com - 10.222.73.222? (yes/no) yes
Success: The High Availability system has been updated

asc log

Use this command to manage system logging.

Syntax

asc log [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --accept</td>
<td>A required argument for --troubleshoot to acknowledge data sensitivity concerns.</td>
</tr>
<tr>
<td>-f, --full</td>
<td>An optional argument to include all log data, not just recent log data. Only works with --troubleshoot.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l, --level &lt;level&gt;</td>
<td>Specifies which messages to export to the remote logging servers. Valid values are:</td>
</tr>
<tr>
<td></td>
<td>• 0 or emerg</td>
</tr>
<tr>
<td></td>
<td>• 1 or alert</td>
</tr>
<tr>
<td></td>
<td>• 2 or crit</td>
</tr>
<tr>
<td></td>
<td>• 3 or err</td>
</tr>
<tr>
<td></td>
<td>• 4 or warning</td>
</tr>
<tr>
<td></td>
<td>• 5 or notice</td>
</tr>
<tr>
<td></td>
<td>• 6 or info</td>
</tr>
<tr>
<td></td>
<td>• 7 or debug</td>
</tr>
<tr>
<td></td>
<td>Either the number or the text can be used.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for logging related activities.</td>
</tr>
<tr>
<td>-p, --purge</td>
<td>Delete all system and audit logs. This action cannot be undone.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-r, --reset</td>
<td>Stop remote logging and return to local logging.</td>
</tr>
<tr>
<td>-s, --syslog &lt;target&gt;</td>
<td>Set the remote syslog logging server(s). Either hostname or IP address can be specified. You can configure multiple syslog servers at the same time.</td>
</tr>
<tr>
<td>--targetPort &lt;port_number&gt;</td>
<td>Specify a target port for TCP-TLS transport. By default, encrypted syslog uses port 6514. Note: You can only specify one port number even if you set multiple encrypted syslog servers.</td>
</tr>
<tr>
<td>-t, --troubleshoot</td>
<td>Generates a troubleshooting archive of recent log data for diagnostic purposes. Requires the --accept option to acknowledge data sensitivity concerns. Include the --full option to include all log data, not just recent log data.</td>
</tr>
<tr>
<td>-x, --crypto</td>
<td>Use TLS encryption for outbound logging connections. The remote syslog server(s) must support TLS. TLS certificates for this service are managed using the htCerts.pl utility.</td>
</tr>
</tbody>
</table>

**Examples**

Permanently delete all system and audit logs:

```
asc log -p
```

Set a remote syslog server and use TLS encryption:

```
asc log -s logger.company.com -x
```

Set two remote syslog servers, the log level, and no encryption:

```
asc log -s log1.company.com -s log2.company.com -l warning
```

Stop remote logging:

```
asc log -r
```

Set the logging level to notice:

```
asc log -l 5
```

or

```
asc log -l notice
```

Create a troubleshooting file for HyTrust Support diagnostics and include all log data:

```
asc log -t -f --accept
```

Create a small troubleshooting file with recent log data only:

```
asc log -t --accept
```

Create an encrypted syslog with a specific TCP port number:

```
asc log -s syslog.company.com --targetport 10514 -x
```
asc monitor

Perform CloudControl monitoring management.

Syntax

asc monitor [options]

Options for asc monitor command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| -a, --fileaudit [--config] [--system] [--verbose] | Audits the local filesystem to identify possible intrusions. This option invokes the Advanced Intrusion Detection Environment (AIDE) using CloudControl validated reference data. CloudControl maintains two different AIDE databases for file system integrity:  
  - config—includes files that change as part of normal system functionality, for example, when you enable or disable a feature.  
  - system—includes all other files in the system.  
By default, this command runs against both databases. If you specify one, the command only runs against the specified database. The output is sent to syslog as well as to the console. |
| -P, --fileprofile [--config] [--system] | Recreates the reference database used by AIDE based on the current contents of the file system. You can specify the config or system database, or recreate both.  
**Note:** To prevent unauthorized editing of the database, after you run the --fileprofile command, you will receive a "archive file is corrupt" warning the next time you run the --fileaudit command. Contact support@hytrust.com to remove this warning. |
| --filemon (on|off) [--filemoninterval <minutes>] | Enables automatic monitoring of file integrity using AIDE. This option enables or disables a cron job that runs the asc monitor --fileaudit command, and is disabled by default. When you enable the job, it will run every 24 hours using your cron schedule. You can change the frequency by entering the number of minutes using the optional --filemoninterval option.  
**Note:** You cannot specify the config or system databases in a cron job. |
<p>| -c, --community &lt;string&gt; | Specify the SNMP community string. |
| -e, --email &lt;email_address&gt; | Set an email address where system notifications will be sent. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-f, --force</td>
<td>Ignore failed connection attempts to mail servers and SNMP trap recipient hosts.</td>
</tr>
<tr>
<td>-H, --health</td>
<td>Perform a health check on the CloudControl.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-k, --network {on</td>
<td>off}</td>
</tr>
<tr>
<td>-l, --trial</td>
<td>Send an SNMP, SMTP, and syslog test alert notice. Include the --message option to send a specific message.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for monitoring related activities. If the message contains spaces, you must surround it by single or double quotation marks.</td>
</tr>
<tr>
<td>-n, --snmp {on</td>
<td>off}</td>
</tr>
<tr>
<td>-p, --protected {on</td>
<td>off}</td>
</tr>
<tr>
<td>-s, --server &lt;smtp_server&gt;</td>
<td>Set the SMTP server to use for sending email notifications.</td>
</tr>
<tr>
<td>-t, --trap &lt;trap_host&gt;</td>
<td>Set an SNMP Trap recipient host.</td>
</tr>
<tr>
<td>-u, --status</td>
<td>Display a report showing service, resource state, and monitoring configuration.</td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>Enable verbose output.</td>
</tr>
</tbody>
</table>

### Examples

Perform an audit of the local CloudControl filesystem:

```
asc monitor --fileaudit
```

Perform an audit of the config database in the local CloudControl filesystem:

```
asc monitor --fileaudit --config
```

Recreate the AIDE reference database:

```
asc monitor --fileprofile
```

Set the `asc monitor --fileprofile` job to run every 120 minutes.

```
asc monitor --filemon on --filemoninterval 120
```
Set the SMTP notification server and target address:
asc monitor -s mail.foo.com -e user@foo.com

Enable the SNMP server and set its community and trap recipient host:
asc monitor -n on -c public -t 1.2.3.4

Send an SMTP and SNMP test with a message:
asc monitor -l -m 'Hello monitoring systems'

View a system status report:
asc monitor --status

Set an SMTP server:
asc monitor -s smtp.foo.com

Set a single SNMP Trap recipient host:
asc monitor -t trapd.foo.com

Set two SNMP Trap recipient hosts:
asc monitor -t trapd.foo.com -t trapd2.foo.com

Enable the SNMP server:
asc monitor -n on

Disable the SNMP server:
asc monitor -n off

Set the SNMP community string:
asc monitor -c public

or
asc monitor -c othercommunity

Specify a single email address where notifications will be sent:
asc monitor -e admin@foo.com

Specify three email addresses where notification will be sent:
asc monitor -e admin@foo.com -e other@foo.com -e third@elsewhere.org

Disable network resource monitoring (NRM):
asc monitor --network off

Enable protected host monitoring (PHM):
asc monitor --protected on

asc network

Perform CloudControl network resource management.
Syntax

asc network [options]

Options for asc network command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --disable</td>
<td>Disable a network device. The --interface option is required.</td>
</tr>
<tr>
<td>-dn, --domainname &lt;domain&gt;</td>
<td>Set the domain name. Multiple domain names can be specified to define the host lookup domain search suffixes.</td>
</tr>
<tr>
<td>-e, --enable</td>
<td>Enable a network device. The --interface option is required.</td>
</tr>
<tr>
<td>-gw, --gateway &lt;gateway&gt;</td>
<td>Define the default gateway for a network device. The --interface option is required.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-hn, --hostname &lt;name&gt;</td>
<td>Set the unqualified hostname of the appliance.</td>
</tr>
<tr>
<td>-i, --interface &lt;device&gt;</td>
<td>The name of the network device to configure. The interface name prod can be used to imply eth0.</td>
</tr>
<tr>
<td>-ip, --ipaddress</td>
<td>Specify the IPv4 address or the text dhcp as an argument. The --interface option is required.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for network related activities.</td>
</tr>
<tr>
<td>-nm, --netmask &lt;mask&gt;</td>
<td>Set the subnet mask. The --interface option is required.</td>
</tr>
<tr>
<td>-ns, --nameserver &lt;nameserver&gt;</td>
<td>Set the name servers. Up to three name servers are supported.</td>
</tr>
<tr>
<td>-s, --status</td>
<td>Display network device status. Use the --interface option to only show status for a specific device.</td>
</tr>
<tr>
<td>-t, --topology &lt;mode&gt;</td>
<td>Set the appliance mode of operation to proxy. In proxy mode eth0 is used for primary traffic and eth2 is optionally used for High Availability.</td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>Enable verbose output.</td>
</tr>
</tbody>
</table>

Examples

Set the IP address, subnet mask and gateway for the eth0 network device:

asc network -i eth0 -ip 1.2.3.4 -nm 255.255.255.0 -gw 1.2.3.254
Set the hostname, domain name, and two name servers for the CloudControl:
asc network -hn asc01 -dn example.com -ns 1.1.1.1 -ns 1.2.3.4

Retrieve the status of all networking devices:
asc network --status

Disable the eth0 network device:
asc network --i eth0 --disable

Set the network topology to proxy (Mapped) mode:
asc network -t proxy

Set three domain names for the CloudControl
asc network -dn example.com -dn dept.example.com -dn search.org

Set the hostname for the CloudControl:
asc network -hn asc01

asc policy

Use this command to manage CloudControl policies.

Syntax
asc policy [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-C, --copies</td>
<td>Set the number of copies to keep for the specified log. Requires --log.</td>
</tr>
<tr>
<td>-g, --getcipher</td>
<td>Get the current SSL Cipher and SSL Protocol string.</td>
</tr>
<tr>
<td>--getpurge</td>
<td>Displays the current number of days to keep history and policy history data before purging.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-j, --job &lt;days&gt;</td>
<td>Delete job history data older than the specified number of days. The value for &lt;days&gt; must be an integer greater than 7.</td>
</tr>
<tr>
<td>-l, --log</td>
<td>Change the log rotation policy for the specified log. Requires the log name and the number of copies as an argument.</td>
</tr>
<tr>
<td>-o, --object-hiding {true</td>
<td>false}</td>
</tr>
<tr>
<td>-p, --purge &lt;days&gt;</td>
<td>Delete policy data older than the specified number of days. The value for &lt;days&gt; must be an integer greater than 7.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-r, --refreshsco {true</td>
<td>false}</td>
</tr>
<tr>
<td>--setpurge &lt;days&gt;</td>
<td>Sets the number of days to keep data before purging. All job history and policy history data older than the days set will be purged. The default value is 90 days.</td>
</tr>
<tr>
<td>-s, --status</td>
<td>Display whether Structure Changing Operations (SCO) are authorized.</td>
</tr>
<tr>
<td>-t, --setprotocol</td>
<td>Set the SSL Protocol string. Use + to include and - to remove protocols. This can be one of the following: SSLv2, SSLv3, TLSv1, TLSv1.1, TLSv1.2, or all. Your settings will persist during a reboot of CloudControl, but not during a failover event. In an HA environment, you must run this command against both the primary and the secondary nodes for the settings to persist across nodes.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: Running this command requires CloudControl to restart.</td>
</tr>
<tr>
<td>-w, --setcipher</td>
<td>Set the SSL cipher string. Use colons to separate the cipher strings. Use + to move ciphers to the end of the list, - to delete ciphers from the list, and ! to permanently delete the ciphers. Your settings will persist during a reboot of CloudControl, but not during a failover event. In an HA environment, you must run this command against both the primary and the secondary nodes for the settings to persist.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The cipher must be an existing openssl cipher.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong>: Running this command requires CloudControl to restart.</td>
</tr>
</tbody>
</table>

### Examples

List the current SCO policy settings:

```bash
asc policy -s
```

Disable Structure Changing Operation (SCO) automatic refresh:

```bash
asc policy -r false
```

Enable Structure Changing Operation (SCO) automatic refresh:

```bash
asc policy -r true
```

Set the purge interval to delete all data more than 10 days old:

```bash
asc policy --setpurge 10
```

Disable the restricting visibility feature:

```bash
asc policy --object-hiding false
```

Change the log rotation policy to 20 copies and save to the ASC log file:

```bash
asc policy --log asc --copies 20
```

View your existing ciphers and protocols:
asc policy --getcipher

Set the OpenSSL cipher string for TLS to comply with FIPS restrictions:

asc policy --setcipher 'TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL'

The following ciphers will be allowed:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA384
- DHE-DSS-AES256-GCM-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-DSS-AES256-SHA256
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDH-ECDSA-AES256-SHA384
- AES256-GCM-SHA384
- AES256-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA256
- DHE-DSS-AES128-GCM-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-DSS-AES128-SHA256
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-ECDSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-SHA256
- AES256-SHA
- AES128-SHA
- DES-CBC3-SHA

Setting the SSL cipher suite string will interrupt production services.
Set SSL Cipher Suite? yes
Production services restarted. Please Wait.
Success: Policy management completed

Set the SSL Protocol string to allow disable all TLS modes except for TLS 1.2:

**Note:** You should run this with the `asc policy --setcipher 'TLSv1.2+FIPS:kRSA+FIPS:!eNULL:!aNULL'` command.

```
asc policy -t '-TLSv1 -TLSv1.1 +TLSv1.2'
```

Setting the SSL Protocol String will interrupt production services.
Do you want to set the SSL Protocol String? yes
Production services restarted. Please Wait.
Success: Policy management completed

### asc restore

Use this command to restore CloudControl to a clean, uninitialized state.

**Syntax**

```
asc restore [options]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>--system-restore</td>
<td>Perform a system restore operation.</td>
</tr>
<tr>
<td>--keep-net</td>
<td>Preserve the network configuration when performing a restore.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> The <code>--keep-net</code> option should only be used if the node will be reused as a secondary. Do not use this option for a node that will be reused as a primary node.</td>
</tr>
</tbody>
</table>

**Examples**

Perform a full system restore, resetting the network configuration:
```
asc restore --systemrestore
```

Perform a system restore, preserving the existing network configuration for a secondary node:
```
asc restore --systemrestore --keep-net
```

### asc route

Perform CloudControl static route management.
Syntax

asc route [options]

Options for asc route command

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Add a static route. The --interface option is required.</td>
</tr>
<tr>
<td>-e, --edit &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Modify an existing static route. The --interface option is required.</td>
</tr>
<tr>
<td>-f, --ospf {on</td>
<td>off}</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --interface &lt;device&gt;</td>
<td>The name of the network device to configure.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Display the current static route configuration. Use the --interface option to only show static routes for a specific device.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for static route related activities.</td>
</tr>
<tr>
<td>-o, --old &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>The original route to be replaced by an edited route. The --interface option is required.</td>
</tr>
<tr>
<td>-r, --del &lt;IP address&gt;/&lt;mask&gt;:&lt;gateway&gt;</td>
<td>Delete a static route.</td>
</tr>
</tbody>
</table>

Examples

Add a static route to network 1.2.3.0/255.255.255.0 via eth0, with gateway 10.20.30.1:
asc route -a 1.2.3.0/255.255.255.0:10.20.30.1 -i eth0
or
asc route -a 1.2.3.4/24:10.20.30.1:eth0

Remove a static route to network 1.2.3.0/255.255.255.0:
asc route -r 1.2.3.0/255.255.255.0
or
asc route -r 1.2.3.0/24

List all static routes:
asc route -l

List static routes for the interface eth0:
asc route -l -i eth0
Edit an existing static route:

```
asc route -e 1.2.3.0/255.255.255.0:10.20.30.1 -i eth0
```

or

```
asc route -e 1.2.3.4/24:10.20.30.1:eth0
```

**asc service**

Use this command to perform generic CloudControl service management and simple configuration file changes.

**Syntax**

```
asc service [options]
```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c, --cleantmp</td>
<td>Cleans the /tmp file system.</td>
</tr>
<tr>
<td>-f, --configfile &lt;file&gt;</td>
<td>Specify the configuration file(s) to read or modify. Multiple files can be specified. Searches and changes are processed to each file in the order specified.</td>
</tr>
<tr>
<td>-C or --create-rescue</td>
<td>Creates the ascrescue account to add an additional layer of security. The ascsupport account, used by HyTrust Support, can not be logged into until you log in to the ascrescue account and hand over the session. <strong>Note:</strong> At first login, the password to the ascrescue account is 'hytrust'. You must change the password before you can use it.</td>
</tr>
<tr>
<td>-d, --disable</td>
<td>Disable a service. The <strong>--servicename</strong> option is required.</td>
</tr>
<tr>
<td>-e, --enable</td>
<td>Enable a service. The <strong>--servicename</strong> option is required.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l or --lockdown</td>
<td>Locks down user accounts to prevent unauthorized users from logging in with a &quot;su &lt;user&gt;&quot; command. Use this command after creating the ascrescue account.</td>
</tr>
<tr>
<td>-m, --message &lt;message&gt;</td>
<td>Specify the message to use in log files and configuration file change journals for service related activities.</td>
</tr>
<tr>
<td>-n, --servicename &lt;service&gt;</td>
<td>The name of the service to manage. The name must match the name of the service init script in the directory /etc/init.d/. Multiple service names can be specified and are managed in the order specified.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>--proxy [vital,license] [true</td>
<td>false] --proxyserver &lt;IP_Address:Port&gt; --proxyuser &lt;user-name&gt; --proxypassword &lt;proxy-user-password&gt;</td>
</tr>
<tr>
<td>-R, --reboot</td>
<td>Reboot the CloudControl appliance.</td>
</tr>
<tr>
<td>-r, --revert</td>
<td>Revert the specified configuration file parameters to their previous value.</td>
</tr>
<tr>
<td>-s, --status</td>
<td>Checks to see if a specified service is running.</td>
</tr>
<tr>
<td>-v, --verbose</td>
<td>Enable verbose output.</td>
</tr>
<tr>
<td>-vv</td>
<td>Enable debug output.</td>
</tr>
</tbody>
</table>

Examples

Disable the NTP, Tomcat, and PostgresSQL services:

```
asc service -d -n ntpd -n postgresql -n tomcat7
```

Specify multiple services to manage:

```
asc service -n ntpd -n httpd -n monit
```

Enable a proxy server.

```
asc service --proxy vital,license:true --proxyserver 1.1.1.1:1234 --proxyuser MyUserName --proxypassword MyPassword.
```

Check if the Tomcat service is running:

```
asc service -n tomcat7 -s
```

- If up, you will see the following:
  - Service rsyslog is up
  - Success: Service settings updated

- If down, you will see the following:
  - Service tomcat7 is down
  - Success: Service settings updated

Create the ascrescue account to prevent support from logging into your system without a handoff:

```
[htcc:standalone ~]$ asc service --create-rescue
```

Created the 'ascrescue' account. Please log in using the default password 'hytrust' and change the password. The 'ascadnmnuser' password can be updated from the 'ascrescue' account by executing 'sudo passwd ascadminuser'.

Success: Account settings updated

```
[htcc:standalone ~]$ ssh ascrescue@<host.example.com>
```
The authenticity of host '<host.example.com>' (<host.example.com>)' can't be established.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '<host.example.com>' (RSA) to the list of known hosts.
ascrescue@<host.example.com>'s password:
You are required to change your password immediately (root enforced)
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user ascrescue.
Changing password for ascrescue.
(current) UNIX password:
New password:
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Connection to <host.example.com> closed.
[htcc:standalone ~]$ asc service --lockdown ascadminuser
Preventing 'ascadminuser' from elevating account to 'ascsupport'.
Success: Account settings updated
[htcc:standalone ~]$ asc service --lockdown ascrescue
Preventing 'ascrescue' from changing the 'ascadminuser' password.
Success: Account settings updated

asc ssh

Use this command to perform CloudControl SSH Proxy service management.

Syntax

gss ssh [options]

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-a, --add &lt;command&gt;</td>
<td>Add a custom command and its associated operation. The --operation option is required.</td>
</tr>
<tr>
<td>-d, --disable</td>
<td>Disable the SSH Proxy.</td>
</tr>
<tr>
<td>-e, --enable</td>
<td>Enable the SSH Proxy or reload its configuration if it is already running.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-l, --list</td>
<td>Display all custom commands and their associated operations. Use with the --operation option to list all known operations.</td>
</tr>
<tr>
<td>-o, --operation [&lt;op&gt;]</td>
<td>List, add, or remove custom SSH command operations. Used with the --list, --add, or --remove options.</td>
</tr>
<tr>
<td>-r, --remove &lt;command&gt;</td>
<td>Remove a custom command.</td>
</tr>
<tr>
<td>-s, --stream {on</td>
<td>off}</td>
</tr>
</tbody>
</table>

**Examples**

List all custom user commands and their associated operations:

```bash
asc ssh -l
```

Lists all known operations:

```bash
asc ssh -l -o
```

Search for unknown commands in the SSH Proxy log:

```bash
asc ssh -f
```

Add a custom command associated with the whitelist operation:

```bash
asc ssh -a '/bin/date' -o 'whitelist'
```

Remove the custom command '/bin/date':

```bash
asc ssh -r '/bin/date'
```

Disable the stream log:

```bash
asc ssh -s off
```

Disable the SSH Proxy service:

```bash
asc ssh -d
```

**asc TAS-Intel**

Use this command to manage the Intel Trust Attestation Services.

**Syntax**

```bash
asc TAS-Intel [options]
```

or

```bash
asc tas [options]
```
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h or --help</td>
<td>Displays usage text.</td>
</tr>
<tr>
<td>-s or --setup</td>
<td>Sets up Intel TAS environment on CloudControl.</td>
</tr>
<tr>
<td>-u or --unsetup</td>
<td>Deinitialize the Intel TAS environment on the CloudControl.</td>
</tr>
<tr>
<td>-V or --version</td>
<td>Displays the version of utilities and underlying library.</td>
</tr>
<tr>
<td>-e or --export-certs</td>
<td>Exports the Hardware Policy Tag certificates from the Host Verification service.</td>
</tr>
</tbody>
</table>

**asc upgrade**

Use this command to perform software updates and license key management.

**Syntax**

```asc upgrade [options]```

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d, --db</td>
<td>Update version data in the local database for GUI reference. The <code>--iso</code> option is implied.</td>
</tr>
<tr>
<td>-h, --help</td>
<td>Display usage text.</td>
</tr>
<tr>
<td>-i, --iso [&lt;iso_file&gt;]</td>
<td>Use a virtual DVD-ROM device or local ISO image file. The <code>--db</code> option is implied.</td>
</tr>
</tbody>
</table>

After performing the upgrade, it is required to reboot the CloudControl instance.

**Examples**

Upgrade using an attached ISO image:
```asc upgrade -i```

Upgrade using a local ISO image file:
```asc upgrade -i /tmp/UpgradeFile.iso```

Synchronize the local database version data with the installed version:
```asc upgrade -d```
Appendix E. Supported Authentication Modes

HyTrust CloudControl (CloudControl) authenticates users for every attempted login and/or operation on vCenter Server. It provides three authentication modes, in which it employs different authentication methods in combination with different vCenter settings. Those authentication modes are:

- CloudControl Service Account (default) and best practice
- Pass through without CloudControl Service Account
- Pass through with CloudControl Service Account

The following table provides detailed information about required user account configurations on vCenter Server, credentials used for vCenter operations, restrictions on object views, and recommended use for each of the modes.

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Required Account Settings</th>
<th>Credentials used for vCenter Operations</th>
<th>Restrictions on Object Views</th>
<th>Recommended Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use CloudControl Service Account</td>
<td>Only the Service Account must be provisioned on vCenter Server for CloudControl purposes.</td>
<td>Service Account</td>
<td>No restrictions on object views</td>
<td>Recommended, default setting</td>
</tr>
<tr>
<td>Use pass through without CloudControl Service Account</td>
<td>Every user must be configured and provisioned with appropriate privileges on vCenter Server.</td>
<td>Active Directory Credentials of the authenticated user</td>
<td>Object views restricted based on user privileges on vCenter Server</td>
<td>For restricted object views</td>
</tr>
<tr>
<td>Use pass through with CloudControl Service Account</td>
<td>Provision individual users with login privileges only on vCenter Server. Provision Service Account normally.</td>
<td>Service Account</td>
<td>No restrictions on object views</td>
<td>Smart Card authentication</td>
</tr>
</tbody>
</table>

CloudControl Service Account

CloudControl uses Service Account credentials to integrate directly with Active Directory (AD) via LDAP protocols. It also uses the Service Account to query Active Directory and confirm the appropriate group membership for the users. For more information on how to configure the Service Account in Active Directory, see Service Account Privileges on page 20.

IWA Support

Integrated Windows Authentication (IWA) is commonly used in the context of alternative credential options such as Smart Card and PIV-II card authentication. Unlike basic authentication, IWA does not prompt for a user name and password. Instead, it uses the current Windows login information on the client to authenticate users.
Smart Card Support

For Smart Card users, a Windows session is initiated using their Smart Card credentials. Smart Card users log in to the vSphere client with the **Use Windows session credentials** option selected. IWA passes the same Smart Card credentials that were used to initiate the Windows session, to the vSphere client. The vSphere client passes the authentication token sent by IWA to CloudControl, which then passes it to vCenter Server.

Authentication Modes

**Use CloudControl Service Account (default)**

The following figure describes the authentication process using CloudControl Service Account.

In this authentication mode, users login to the vSphere client using their Active Directory credentials. CloudControl authenticates users’ AD credentials and logs in to vCenter Server using the Service Account credentials provided in the CloudControl configuration. The Service Account must be configured on vCenter Server and CloudControl performs all operations using the Service Account credentials.

Users are not required to exist or be configured on vCenter Server. The user’s view of objects is not restricted.

Smart Card Authentication

Smart Card users login to the vSphere client with the IWA option enabled. This causes the vSphere client and CloudControl to pass their Windows session authentication token directly to vCenter Server. vCenter Server authenticates the user against Active Directory. After authentication, all operations on the vCenter Server are authorized based on the CloudControl policy and CloudControl performs them using the Service Account credentials.
Use pass through without CloudControl Service Account

The following figure describes pass through without using CloudControl Service Account.

Use pass through without CloudControl Service Account

In this authentication mode, users login to the vSphere client using their AD credentials. CloudControl authenticates them against Active Directory, and logs in to vCenter Server using their AD credentials. CloudControl performs operations on vCenter Server with the users' AD credentials.

In this authentication mode, every user must exist and be configured with appropriate permissions on vCenter Server. The user's view of objects is determined by their role defined on vCenter Server.

Smart Card Authentication

Smart Card users login to the vSphere client with the IWA option enabled. This causes the vSphere client and CloudControl to pass their Windows session authentication token directly to vCenter Server. vCenter Server authenticates the user against Active Directory. After authentication, all operations on vCenter Server are authorized based on the CloudControl policy and CloudControl performs them with the user's Active Directory credentials.

Use pass through with CloudControl Service Account

The following figure describes pass through using CloudControl Service Account.
In this authentication mode, users login to the vSphere client using their Active Directory credentials. CloudControl authenticates them against Active Directory and also passes the credentials to vCenter Server for authentication. Once authenticated, CloudControl performs operations using the Service Account credentials.

In this mode, every user must exist and be configured with login permissions on vCenter Server. The user’s view of objects is not restricted.

**Smart Card Authentication**

Smart Card users login to the vSphere client with the IWA option enabled. This causes the vSphere client and CloudControl to pass their Windows session authentication token directly to vCenter Server, which authenticates the user against Active Directory. After authentication, all operations on vCenter Server are authorized according to the CloudControl policy and CloudControl performs them using the Service Account credentials.
Appendix F. REST API Guide

REST API Overview

You can access objects in CloudControl through a set of REST APIs.

Note: If a VIP is configured, then all API calls must be made using the VIP as the <hostname>.

Accessing APIs

CloudControl REST APIs can be accessed by using different methods:

- **cURL**: cURL is a command line tool that interacts with REST APIs.
- **REST Client**: REST clients let users create and test custom HTTP requests. These are available as browser plug-ins.
- **Programmatic access**: REST APIs can be accessed using any programming language.

CloudControl REST APIs use JSON for both request and response bodies.

Note: Only authenticated users with an authorized CloudControl account can access the CloudControl REST APIs.

Authentication

To authenticate a user, the username and password are specified in the header field of the request.

Authentication Token

A successful API login response includes an authentication token. The token expires if a session is inactive for more than one hour. Every API call must include the authentication token received at the time of login. The generated cookie should be used in every subsequent request.
Login

Authenticates the CloudControl user via username and password credentials supplied in the request header.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/login

Request Method

POST

Request Header

Authorization

Basic <base64 encoded username:password>

Accept

application/json

Content-Type

application/json

cURL Example

```
```

Success Response

Response Header

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=C1407A67958F59A0CDE9221C8161B5F7; Path=/asc/; Secure; HttpOnly
Auth-Token: C1407A67958F59A0CDE9221C8161B5F7
Date: Mon, 15 Sep 2014 23:23:09 GMT
Content-Type: application/json
Transfer-Encoding: chunked
Response Body

{"status":true}

Failure Response

Response Body

{"status":false,"error":{"code":"AUN0004","message":"Source: RAPI The authentication for superadmin is declined via Active Directory."}}

Response Body Fields/Objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>error</td>
<td>Error object</td>
<td>error code and message</td>
</tr>
</tbody>
</table>

Error object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>boolean</td>
<td>error code</td>
</tr>
<tr>
<td>message</td>
<td>String</td>
<td>error message</td>
</tr>
</tbody>
</table>

Logout

Logs out users from CloudControl. Use this upon completion of any API session.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/logout

Request Method

POST

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88
Accept
application/json

Content-Type
application/json

cURL Example

```
```

Success Response

Response Body

```json
{"status":true}
```

Failure Response

Response Body

```json
{"status":false,"error":{"code":"AUN0204","message":"Invalid session."}}
```

Resource/Host Management

The Resource/Host Management APIs allow operations on resources such as hosts, virtual machines, and vCenter.

Resource

Resource APIs retrieve information for generic resources.

Get All Resources

Gets all resources available in CloudControl.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources
Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example


Get resources sorted by a property

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources?sortby={sortby}

Valid parameters for sorting are: uid, name, description. Current version of APIs only support single sorting. By default sorting results are in ascending order.

Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json
Content-Type
application/json

cURL Example

Get resources by pagination

Request URI
https://<CloudControl_hostname>/asc/api/rest/v1/resources?page={page}&pagesize={pagesize}
https://<CloudControl_hostname>/asc/api/rest/v1/resources?page={page}
Default value for pagesize is 100
Default value for page is 1
If no page or pagesize is provided on the RAPI url, the first page with pagesize 100 records will be returned.

Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example
Get resources by uid

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources?uid={uid}

Default value for pagesize is 100

Default value for page is 1

If no page or pagesize is provided on the RAPI url, the first page with pagesize 100 records will be returned.

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Get resources by name

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources?name={name}

Valid "name" parameter includes:

Full or partial resource name
Resource

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example

$curl -b cookies -i -k https://<CloudControl_hostname>/asc/api/rest/v1/resources?name=esxi-17.test

Get resources by type

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources?type={type}

Valid "type" parameters are: ManagementSystem, HostSystem, VirtualMachine

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json
Content-Type
application/json

cURL Example

```bash
```

Success Response

Response Body

```json
{
    "status": true,
    "resource": [
        {
            "name": "Appliance Root",
            "uid": "com.hytrust.root",
            "resourceType": "Root",
            "trustStatus": "Unknown",
            "label": [
                {
                    "name": "DEV",
                    "uid": "DEV"
                }
            ],
            "description": "Web Client Server",
            "resourceType": "ManagementSystem",
            "trustStatus": "Unknown"
        },
        {
            "name": "10.222.73.140",
            "uid": "4038ef9d-4164-4520-8a3f-93158aa26c76",
            "description": "Web Client Server",
            "resourceType": "ManagementSystem",
            "trustStatus": "Unknown"
        },
        {
            "name": "vm2",
            "uid": "ef1e690a-b724-4b9b-916b-25bd45df7e19",
            "description": "@esxi-17.test.hytrust.com",
            "resourceType": "VirtualMachine",
            "resourceUuid": "564dd518-c90f-fbd8-2556-e0419eb6f632",
            "macAddress": "00:50:56:ad:55:68",
            "trustStatus": "Unknown"
        },
        {
            "name": "esxi-17.test.hytrust.com",
            "uid": "256211e2-339d-4d33-b0bb-b9497e34fed8",
            "description": "HostSystem:host-43@https://10.222.73.140:443/sdk",
            "resourceType": "HostSystem",
            "resourceUuid": "42118cae-14a6-60fa-8e2f-e3786ebb089",
            "trustStatus": "Unknown"
        }
    ]
}
```

Failure Response

Response Body

```json
{
    "status": false,
    "error": {
        "code": "AUN0204",
        "message": "Invalid session."
    }
}
```
## Response Body Fields/Objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>resource</td>
<td>Collection of Resource objects</td>
<td>all the resources</td>
</tr>
</tbody>
</table>

## Resource object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the object</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>resourceUuid</td>
<td>string</td>
<td>the hardware/BIOS uuid of the host or vm</td>
</tr>
<tr>
<td>description</td>
<td>string[255]</td>
<td>description of the object</td>
</tr>
<tr>
<td>resourceType</td>
<td>enum</td>
<td>type of resource [VM,Host,MgmtSystem …]</td>
</tr>
<tr>
<td>dnsName</td>
<td>string</td>
<td>primary DNS Name</td>
</tr>
<tr>
<td>ipAddress</td>
<td>string</td>
<td>primary IP address</td>
</tr>
<tr>
<td>macAddress</td>
<td>string</td>
<td>primary MAC address</td>
</tr>
<tr>
<td>trustStatus</td>
<td>enum</td>
<td>Trust Status of the resource. Initially applies to physical hosts. In the future, this concept will be extended to other resources</td>
</tr>
<tr>
<td>networkName</td>
<td>string</td>
<td>The network to which the resource belongs.</td>
</tr>
<tr>
<td>networkId</td>
<td>string[255]</td>
<td>uid of the network</td>
</tr>
<tr>
<td>label</td>
<td>Collection of Label objects</td>
<td>All the labels assigned to the resource</td>
</tr>
</tbody>
</table>

## Label object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the label</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>complianceTemplate</td>
<td>complianceTemplate object</td>
<td>The compliance template associated to the label</td>
</tr>
</tbody>
</table>
ComplianceTemplate object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the compliance template</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
</tbody>
</table>

Get Resources Associated to a Label

Gets all the resources with the labeluid provided in the request header.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources?labeluid={labeluid}
https://<CloudControl_hostname>/asc/api/rest/v1/resources/hosts?labeluid={labeluid}
https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?labeluid={labeluid}
https://<CloudControl_hostname>/asc/api/rest/v1/resources/managedsystems?labeluid={labeluid}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example

Success Response

Response Body

{"status":true,
 "resource":[
 {"name":"Appliance Root",
 "uid":"com.hytrust.root",
 "resourceType":"Root",
 "trustStatus":"Unknown",
 "label": [
 {"name":"DEV",
 "uid":"DEV"}
 ],
 {"name":"VM1",
 "uid":"02fd66db-d8e4-4d2e-aec6-31ac3efa0427",
 "description": "@tpmtest-hp01.eng.hytrust.com",
 "resourceType": "VirtualMachine",
 "resourceUuid": "420e1b82-3fd6-e5f1-c6e9-12ace50e24bd",
 "trustStatus": "Unknown",
 "label": [
 {"name": "DEV",
 "uid": "DEV"}
 ]
 ]
 }

Failure Response

Response Body

{"status":false,"error":{"code":"AUN0204","message":"Invalid session."}}

Host Systems

Gets all the hosts available in CloudControl.

Get All Host Systems

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems

Request Method

GET
Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Get all hostsystems sorted by a property

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?sortby={sortby}

Valid "sortby" parameters are: "uid", "name", "biosVersion", "vmmVersion", "hostVendor", "mleName"

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json
**cURL Example**

```
```

**Get HostSystems by pagination**

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?page={page}&pagesize={pagesize}

Default value for pagesize is 100.

Default value for page is 1.

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json

**cURL Example**

```
```

```
```

**Success Response**

**Response Body**

```json
{"status":true,
```
"hostSystem": [
  {
    "name": "esxi-17.test.hytrust.com",
    "uid": "256211e2-339d-4d33-b0bb-b9497e34fed8",
    "resourceType": "HostSystem",
    "resourceUuid": "42118cae-14a6-60fa-8e2f-e3786eeb5089",
    "dnsName": "esxi-17.test.hytrust.com",
    "ipAddress": "10.222.73.217",
    "trustStatus": "Unknown",
    "hostType": "vSphereESXi",
    "isBios": true,
    "isVmm": true,
    "hostVersion": "VMware ESXi 5.1.0 build-799733",
    "isGoodKnownHost": false,
    "isRegisteredWithTas": false,
    "isTpmEnabled": false,
    "isPolicyTagActivated": false,
    "isManaged": true,
    "mgmtSystemId": "d762c68e-8e78-418c-9704-1b9add49d176",
    "protectedResourceDetails": {
      "portHttp": 80,
      "portHttps": 443,
      "portSdk": 80,
      "portSdks": 443,
      "portSsh": 22,
      "publishedDnsName": "10.222.73.237",
      "publishedNetMask": "255.255.255.0",
      "isACL": false,
      "isPassThru": false,
      "isPassThruServiceAccount": false,
      "isProxyEnabled": false,
      "isProxyDHCPEnabled": false,
      "isRootPasswordEnabled": false,
    }
  }
]
"isSshEnabled":false,
"isUsingHttps":true,
"isUsingSdks":true,
"isProtected":false,
"isSupported":true}

}

} }

Failure Response

Response Body

{"status":false,"error":
{""code":"AUN0204","message":"Invalid session."} }

Response Body Fields/Objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>hostSystem</td>
<td>collection of HostSystem objects</td>
<td>all the host systems</td>
</tr>
</tbody>
</table>

HostSystem Object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the object</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>resourceUuid</td>
<td>string</td>
<td>the hardware/BIOS uuid of the host or vm</td>
</tr>
<tr>
<td>description</td>
<td>string[255]</td>
<td>description of object</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>resourceType</td>
<td>enum</td>
<td>type of resource [VM, Host, MgmtSystem …]</td>
</tr>
<tr>
<td>dnsName</td>
<td>string</td>
<td>primary DNS Name</td>
</tr>
<tr>
<td>ipAddress</td>
<td>string</td>
<td>primary IP address</td>
</tr>
<tr>
<td>macAddress</td>
<td>string</td>
<td>primary MAC address</td>
</tr>
<tr>
<td>trustStatus</td>
<td>enum</td>
<td>Trust Status of the resource. Initially applies to physical hosts. In the future, this concept will be extended to other resources</td>
</tr>
<tr>
<td>networkName</td>
<td>string</td>
<td>The network to which the resource belongs</td>
</tr>
<tr>
<td>networkId</td>
<td>string[255]</td>
<td>uid of network</td>
</tr>
<tr>
<td>label</td>
<td>collection of Label objects</td>
<td>All the labels assigned to the resource</td>
</tr>
<tr>
<td>hostType</td>
<td>enum</td>
<td>type of host [vSphere ESXi…]</td>
</tr>
<tr>
<td>isBios</td>
<td>boolean</td>
<td>is BIOS enabled on this host</td>
</tr>
<tr>
<td>isVmm</td>
<td>boolean</td>
<td>is VMM enabled on this host</td>
</tr>
<tr>
<td>biosVersion</td>
<td>string</td>
<td>BIOS version</td>
</tr>
<tr>
<td>vmmVersion</td>
<td>string</td>
<td>VMM version</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>hostVendor</td>
<td>string</td>
<td>name of the hardware vendor</td>
</tr>
<tr>
<td>hostVersion</td>
<td>string</td>
<td>version of the host system</td>
</tr>
<tr>
<td>mleName</td>
<td>string</td>
<td>MLE name for TAS</td>
</tr>
<tr>
<td>isGoodKnownHost</td>
<td>boolean</td>
<td>This flag is set to true if the host is a Good Known Host</td>
</tr>
<tr>
<td>isRegisteredWithTas</td>
<td>boolean</td>
<td>is this system registered with TAS</td>
</tr>
<tr>
<td>isManaged</td>
<td>boolean</td>
<td>is host managed by a management system</td>
</tr>
<tr>
<td>mgmtSystemId</td>
<td>string[255]</td>
<td>uid of the management system managing this host</td>
</tr>
<tr>
<td>protectedResourceData</td>
<td>ProtectedResourceData</td>
<td>details on the protected resource</td>
</tr>
<tr>
<td>isTpmEnabled</td>
<td>boolean</td>
<td>This flag is set to true if TPM is enabled on a given host</td>
</tr>
<tr>
<td>isPolicyTagActivated</td>
<td>boolean</td>
<td>This flag is set to true if the PolicyTags associated with the Host has been provisioned onto the Host system</td>
</tr>
<tr>
<td>policyTag</td>
<td>Collection of PolicyTag Objects</td>
<td>All the PolicyTags assigned to the HostSystem</td>
</tr>
</tbody>
</table>
## Label object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>name of the label</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>complianceTemplate</td>
<td>ComplianceTemplate object</td>
<td>The compliance template associated to the label</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>syslogDnsName</td>
<td>string</td>
<td>DNS name of the syslog server</td>
</tr>
<tr>
<td>syslogIpAddress</td>
<td>string</td>
<td>IP address of the syslog server</td>
</tr>
<tr>
<td>isAcl</td>
<td>boolean</td>
<td>is ACL enabled on system</td>
</tr>
<tr>
<td>isPassThru</td>
<td>boolean</td>
<td>is proxy configured for pass through</td>
</tr>
<tr>
<td>isPassThruServiceAccount</td>
<td>boolean</td>
<td>is proxy configured for pass through Service Account?</td>
</tr>
<tr>
<td>isProxyEnabled</td>
<td>boolean</td>
<td>is proxy enabled for this resource</td>
</tr>
<tr>
<td>isProxyDhcpEnabled</td>
<td>boolean</td>
<td>is DHCP enabled for proxy?</td>
</tr>
<tr>
<td>isRootPasswordEnabled</td>
<td>boolean</td>
<td>is root password enabled</td>
</tr>
<tr>
<td>isSshEnabled</td>
<td>boolean</td>
<td>is SSH enabled</td>
</tr>
<tr>
<td>isUsingHttps</td>
<td>boolean</td>
<td>is resource accessed using HTTPS</td>
</tr>
<tr>
<td>isUsingSdks</td>
<td>boolean</td>
<td>is resource SDK accessed using HTTPS</td>
</tr>
<tr>
<td>isProtected</td>
<td>boolean</td>
<td>is resource protected</td>
</tr>
<tr>
<td>isSupported</td>
<td>boolean</td>
<td>is resource type/version supported</td>
</tr>
</tbody>
</table>
**PolicyTag Object**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the PolicyTag (COUNTRY, STATE, REGION, PDC, CLASSIFICATION)</td>
</tr>
<tr>
<td>value</td>
<td>string</td>
<td>value of the PolicyTag for a specific name</td>
</tr>
</tbody>
</table>

**Get hostsystems by uid**

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?uid={uid}

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json

**cURL Example**

```
```
Get Host Systems by Host Type

Gets hosts based on the 'host type' provided in the request query parameter.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?hostType={hostsystemtype}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example

```bash
```

Hostsystem-type can be: vSphereESXi.

Success Response

Response Body

Same as Get Host Systems by Host Type

Get Host Systems by Name

Gets hosts based on the host name provided in the request query parameter.
Host Systems

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?name={hostsystemname}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example

```
$curl -b cookies -i -k https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?name=esxi-17.test.hytrust.com
```

Success Response

Response Body

Same as Get Host Systems by Type

Get Host Systems by IP

Gets hosts based on the IP address provided in the request header.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?ipaddress={ipaddress}
Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example


Success Response

Response Body
Same as Get Host Systems by Type

Get Host Systems by Protected Info

Gets hosts based on the protected/unprotected criteria provided in the request query parameter.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?isprotected={isprotectedboolean}

Request Method
GET
Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Success Response

Response Body

Same as Get Host Systems by Host Type.

Get Host Systems Associated to a Label

Gets hosts based on the label provided in the request query parameter.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems?labeluid={labeluid}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88
Accept

application/json

Content-Type

application/json

cURL Example

```
```

Success Response

Response Body

Same as Get Host Systems by Host Type.

Add a Host System

Adds a host to CloudControl based on the information provided in the request body.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems

Request Method

POST

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json
Request Body

{ "accountInfo":
  { "user": "root",
    "password": "<password>",
    "hostSystem":
      { "name": "esxi-17.test.hytrust.com",
        "dnsName": "esxi-17.test.hytrust.com",
        "ipAddress": "10.222.73.217",
        "hostType": "vSphereESXi",
        "mgmtSystemId": "d762c68e-8e78-418c-9704-1b9add49d176",
        "isManaged": "true",
        "protectedResourceDetails":
          { "publishedDnsName": "10.222.73.237",
            "publishedNetMask": "255.255.255.0",
            "isACL": false,
            "isPassThru": false,
            "isPassThruServiceAccount": false,
            "isProxyEnabled": false,
            "isProxyDHCPEnabled": false,
            "isRootPasswordEnabled": false,
            "isSshEnabled": false
          }
      }
  }
}

cURL Example


Success Response

Response Body

{ "status": true,
"hostSystem":[
{
"name":"esxi-17.test.hytrust.com",
"uid":"eed3953c-9af6-4084-b843-966601b290f7",
"resourceType":"HostSystem",
"dnsName":"esxi-17.test.hytrust.com",
"ipAddress":"10.222.73.217",
"trustStatus":"Unknown",
"hostType":"vSphereESXi",
"isBios":true,
"isVmm":true,
"hostVersion":"VMware ESXi 5.1.0 build-799733",
"isGoodKnownHost":false,
"isRegisteredWithTas":false,
"isTpmEnabled":false,
"isPolicyTagActivated":false,
"isManaged":true,
"protectedResourceDetails":{
"portHttp":80,
"portHttps":443,
"portSdk":80,
"portSdks":443,
"portSsh":22,
"publishedIpAddress":"10.222.73.237",
"publishedDnsName":"10.222.73.237",
"publishedNetMask":"255.255.255.0",
"isACL":false,
"isPassThru":false,
"isPassThruServiceAccount":false,
"isProxyEnabled":true,
"isProxyDHCPEnabled":false,
"isRootPasswordEnabled":false,
"isSshEnabled":false,
}]}
"isUsingHttps":true,
"isUsingSdks":true,
"isProtected":false,
"isSupported":true
}
}

Delete a Host System

Deletes the host specified in the request.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems/{dnsname/ipaddress}

Request Method

DELETE

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Success Response

Response Body

{"status":true}
Failure Response

Response Body

{"status":false,
"error":
{"code":"ARC0123",
"message":"Hostsystem not found for 10.222.73.217"}
}

Update a Host System

Updates the host based on the provided information.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostsystems/{dnsname/ipaddress}

Request Method

PUT

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

Request Body

{"accountInfo" :
{"user" : "root",
"password" : "<password>"},
"hostSystem" :
{"name": "esxi-17.test.hytrust.newname.com",
"dnsName": "esxi-17.test.hytrust.com",
"ipAddress": "10.222.73.217",
"hostType": "vSphereESXi",
"isManaged": "true",
"mgmtSystemId": "d762c68e-8e78-418c-9704-1b9add49d176",
"protectedResourceDetails": {
"publishedDnsName": "10.222.73.237",
"publishedNetMask": "255.255.255.0",
"isACL": false,
"isPassThru": false,
"isPassThruServiceAccount": false,
"isProxyEnabled": false,
"isProxyDHCPEnabled": false,
"isRootPasswordEnabled": false,
"isSshEnabled": false
}
}

cURL Example


Success Response

Response Body

{"status":true,
"hostSystem": [
"name": "esxi-17.test.hytrust.com.newName",
"uid": "eed3953c-9af6-484b-b843-966801c290f7",
"resourceType": "HostSystem",
"dnsName": "esxi-17.test.hytrust.com",
]"}
"ipAddress":"10.222.73.217",
"trustStatus":"Unknown",
"hostType":"vSphereESXi",
"isBios":true,
"isVmm":true,
"hostVersion":"VMware ESXi 5.1.0 build-799733",
"isGoodKnownHost":false,
"isRegisteredWithTas":false,
"isTpmEnabled":false,
"isPolicyTagActivated":false,
"isManaged":true,
"protectedResourceDetails":
{
"portHttp":80,
"portHttps":443,
"portSdk":80,
"portSdks":443,
"portSsh":22,
"publishedIpAddress":"10.222.73.237",
"publishedDnsName":"10.222.73.237",
"publishedNetMask":"255.255.255.0",
"isACL":false,
"isPassThru":false,
"isPassThruServiceAccount":false,
"isProxyEnabled":true,
"isProxyDHCPEnabled":false,
"isRootPasswordEnabled":false,
"isSshEnabled":false,
"isUsingHttps":true,
"isUsingSdks":true,
"isProtected":false,
"isSupported":true
}
Virtual Machines

Gets all the available virtual machines.

Get All Virtual Machines

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Get all virtual machines sorted by a property

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?sortby={sortby}

Valid "sortby" parameters include: "uid", "name", "parentname".
Request Method
GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Get virtual machines by pagination

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?page={page}&pagesize={pagesize}
https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?page={page}

Default value for pagesize is 100.
Default value for page is 1.

Request Method
GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88
Virtual Machines

Accept
application/json

Content-Type
application/json

cURL Example


Success Response

Response Body

```json
{"status":true,
 "virtualMachine":[
  {
   "name":"vm1",
   "uid":"723fb59d-62a7-4744-b383-4e2b58bd1e0",
   "description":"@esxi-17.test.hytrust.com",
   "resourceType":"VirtualMachine",
   "resourceUuid":"564dff6a-4fba-2c2b-a4fc-78948b184b3e",
   "macAddress":"00:50:56:ad:55:5f",
   "trustStatus":"Unknown",
   "parentName":"esxi-17.test.hytrust.com",
   "parentId":"1ed69511-a580-432f-ac89-441dbfb50af8",
   "guestOS":"Ubuntu Linux (64-bit)"
  }
 ]
}
```

Response Body Fields/Objects
### Virtual Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>virtualMachine</td>
<td>Collection of VirtualMachine objects</td>
<td>all the virtual machines</td>
</tr>
</tbody>
</table>

### VirtualSystem Object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the object</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>resourceUuid</td>
<td>string</td>
<td>the hardware/BIOS uuid of the host or vm</td>
</tr>
<tr>
<td>description</td>
<td>string[255]</td>
<td>description of object</td>
</tr>
<tr>
<td>resourceType</td>
<td>enum</td>
<td>type of resource [VM,Host,MgmtSystem]</td>
</tr>
<tr>
<td>dnsName</td>
<td>string</td>
<td>primary DNS Name</td>
</tr>
<tr>
<td>ipAddress</td>
<td>string</td>
<td>primary IP address</td>
</tr>
<tr>
<td>macAddress</td>
<td>string</td>
<td>primary MAC address</td>
</tr>
<tr>
<td>trustStatus</td>
<td>enum</td>
<td>Trust Status of the resource. Initially applies to physical hosts. In the future, this concept will be extended to other resources</td>
</tr>
<tr>
<td>networkName</td>
<td>string</td>
<td>The network, the resource belongs to.</td>
</tr>
<tr>
<td>networkId</td>
<td>string[255]</td>
<td>uid of network</td>
</tr>
<tr>
<td>label</td>
<td>Collection of Label objects</td>
<td>All the labels assigned to the resource</td>
</tr>
</tbody>
</table>
### Virtual Machines

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmType</td>
<td>enum</td>
<td>type of Virtual Machine</td>
</tr>
<tr>
<td>parentName</td>
<td>string[255]</td>
<td>name by which the parent Host System can be looked up using RAPI</td>
</tr>
<tr>
<td>parentId</td>
<td>string[255]</td>
<td>globally unique id that identifies the Host System</td>
</tr>
<tr>
<td>guestOs</td>
<td>string</td>
<td>name of guest operating system</td>
</tr>
<tr>
<td>mgmtSystemId</td>
<td>string[255]</td>
<td>uid of the management system</td>
</tr>
</tbody>
</table>

### Label object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>name of the label</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>complianceTemplate</td>
<td>ComplianceTemplate object</td>
<td>The compliance template associated with the label</td>
</tr>
</tbody>
</table>

### ComplianceTemplate object

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>name of the compliance template</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
</tbody>
</table>

### Get Virtual Machines by uid

Gets virtual machine based on the specified name.
Virtual Machines

Request URI
https://<CloudControl.hostname>/asc/api/rest/v1/resources/virtualmachines?uid={uid}

Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example


Get Virtual Machines by Name

Gets virtual machine based on the specified name.

Request URI
https://<CloudControl.hostname>/asc/api/rest/v1/resources/virtualmachines?name={vmname}

Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88
**Accept**

application/json

**Content-Type**

application/json

**cURL Example**

```
```

**Success Response**

**Response Body**

Same as ‘Get All Virtual Machines’

**Get Virtual Machines by Host Name**

Gets virtual machines on a particular host based on provided host name.

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?hostsystemname={hostsystemname}

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json
cURL Example


Success Response

Response Body

Same as Get All Virtual Machines

Get Virtual Machines by Type

Gets virtual machines based on the specified type.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?vmtype={vmtype}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example

Success Response

Response Body
Same as Get All Virtual Machines.

Get Virtual Machines with a given Label

Gets virtual machines based on a specified labeluid.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/virtualmachines?labeluid={labeluid}

Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example


Success Response

Response Body
Same as Get All Virtual Machines.
Management Systems

Provides information specific to management systems, such as vCenter.

Get All Management Systems

Gets all the available management systems.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementSystems

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Get all management systems sorted by a property

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementSystems?sortby={sortby}

Valid "sortby" parameters are: "uid", "name", "portHttp", "portHttps"
Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Success Response

Response Body

{"status":true,
 "managementSystem": [
{"name":"10.222.73.140",
 "uid":"7e68a936-7ee1-4845-aab7-623829db4abd",
 "resourceType":"ManagementSystem",
 "resourceUuid":"6C48D81E-95B5-4AC9-AAA4-336D6CC299C2",
 "dnsName":"10.222.73.140",
 "ipAddress":"10.222.73.140",
 "trustStatus":"Unknown",
 "mgmtSystemType":"VirtualCenter",
 "protectedResourceDetails":
}
Response Body Fields/Objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>managementsystem</td>
<td>Collection of ManagementSystem objects</td>
<td>all the management systems</td>
</tr>
</tbody>
</table>

Managementsystem Object
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>name of the object</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>resourceUuid</td>
<td>string</td>
<td>the hardware/BIOS uuid of the host or vm</td>
</tr>
<tr>
<td>description</td>
<td>string[255]</td>
<td>description of object</td>
</tr>
<tr>
<td>resourceType</td>
<td>enum</td>
<td>type of resource [VM,Host,MgmtSystem]</td>
</tr>
<tr>
<td>dnsName</td>
<td>string</td>
<td>primary DNS Name</td>
</tr>
<tr>
<td>ipAddress</td>
<td>string</td>
<td>primary IP address</td>
</tr>
<tr>
<td>macAddress</td>
<td>string</td>
<td>primary MAC address</td>
</tr>
<tr>
<td>trustStatus</td>
<td>enum</td>
<td>Trust Status of the resource. Initially applies to Physical hosts. Overtime this concept would be extended to other resources</td>
</tr>
<tr>
<td>networkName</td>
<td>string</td>
<td>The network, the resource belongs to.</td>
</tr>
<tr>
<td>networkId</td>
<td>string[255]</td>
<td>uid of network</td>
</tr>
<tr>
<td>label</td>
<td>Collection of Label objects</td>
<td>All the labels assigned to the resource</td>
</tr>
<tr>
<td>mgmtSystemType</td>
<td>enum</td>
<td>type of management system [VirtualCenter, HTCC, HTKC, OpenStack]</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>protectedResourceDetails</td>
<td>Object</td>
<td>details on the protected resource.</td>
</tr>
<tr>
<td>Label object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>name of the label</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>complianceTemplate</td>
<td>ComplianceTemplate</td>
<td>The compliance template associated to the label</td>
</tr>
<tr>
<td>ComplianceTemplate object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>name of the compliance template</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>ProtectedResourceDetails Object</td>
<td></td>
<td></td>
</tr>
<tr>
<td>portHttp</td>
<td>integer</td>
<td>HTTP port</td>
</tr>
<tr>
<td>portHttps</td>
<td>integer</td>
<td>HTTPS port</td>
</tr>
<tr>
<td>portSdk</td>
<td>integer</td>
<td>SDK port</td>
</tr>
<tr>
<td>portSdks</td>
<td>integer</td>
<td>secured SDK port</td>
</tr>
<tr>
<td>portSsh</td>
<td>integer</td>
<td>SSH port</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>publishedDnsName</td>
<td>string</td>
<td>DNS name of the published IP address</td>
</tr>
<tr>
<td>publishedIpAddress</td>
<td>string</td>
<td>published IP address</td>
</tr>
<tr>
<td>publishedNetMask</td>
<td>string</td>
<td>NetMask of the Published interface</td>
</tr>
<tr>
<td>syslogDnsName</td>
<td>string</td>
<td>DNS name of the syslog server</td>
</tr>
<tr>
<td>syslogIpAddress</td>
<td>string</td>
<td>IP address of the syslog server</td>
</tr>
<tr>
<td>isAcl</td>
<td>boolean</td>
<td>is ACL enabled on system</td>
</tr>
<tr>
<td>isPassThru</td>
<td>boolean</td>
<td>is proxy configured for pass thru</td>
</tr>
<tr>
<td>isPassThruServiceAccount</td>
<td>boolean</td>
<td>is proxy configured for pass thru?</td>
</tr>
<tr>
<td>isProxyEnabled</td>
<td>boolean</td>
<td>is proxy enabled for this resource</td>
</tr>
<tr>
<td>isProxyDhcpEnabled</td>
<td>boolean</td>
<td>is DHCP enabled for proxy</td>
</tr>
<tr>
<td>isRootPasswordEnabled</td>
<td>boolean</td>
<td>is root password enabled</td>
</tr>
<tr>
<td>isSshEnabled</td>
<td>boolean</td>
<td>is SSH enabled</td>
</tr>
<tr>
<td>isUsingHttps</td>
<td>boolean</td>
<td>is resource accessed using HTTPS</td>
</tr>
<tr>
<td>isUsingSdks</td>
<td>boolean</td>
<td>is resource SDK accessed using HTTPS</td>
</tr>
<tr>
<td>isProtected</td>
<td>boolean</td>
<td>is resource protected</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>isSupported</td>
<td>boolean</td>
<td>is resource type/version supported</td>
</tr>
</tbody>
</table>

**Get managementsystems by uid**

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?mgmtsystemtype={mgmtsystemtype}

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json

**cURL Example**

```
```

**Get Management Systems by Type**

Gets management systems based on the specified type.
Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?mgmtsystemtype={mgmtsystemtype}

Managementsystem-type can be VirtualCenter, HTCC, HTKC, OpenStack, WebClientServer.

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Success Response

Response Body

Same as Get All Management Systems

Get Management Systems by Name

Gets management systems based on the specified name.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?name={mgmtsystemname}
Request Method
GET

Request Header

Auth-Token
9427E55E019E4DD6C30011B9B5E7AA88

Accept
application/json

Content-Type
application/json

cURL Example

Success Response

Response Body
Same as Get All Management Systems.

Get Management Systems by IP

Gets management system based on the specified IP.

Request URI
https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?ipaddress={ipaddress}

Request Method
GET
Request Header

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json

**cURL Example**

```bash
```

**Success Response**

**Response Body**

Same as Get All Management Systems

**Get Management Systems Associated to a Label**

Gets management systems based on the specified label.

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?labeluid={labeluid}

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88
Accept

application/json

Content-Type

application/json

cURL Example

$curl -b cookies -i -k https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems?labeluid=DEV

Success Response

Response Body

Same as Get All Management Systems.

Add a Management System

Adds a management system based on the provided information.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems

Request Method

POST

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json
Request Body

```json
{ "accountInfo":
{ "user": "administrator",
"password": "<password>",
"managementSystem":{
"name": "10.222.73.140VC",
"dnsName": "10.222.73.140",
"ipAddress": "10.222.73.140",
"mgmtSystemType": "VirtualCenter",
"protectedResourceDetails":
{ "publishedIpAddress": "10.222.73.160",
"publishedDnsName": "10.222.73.160",
"publishedNetMask": "255.255.255.0",
"isACL": false,
"isPassThru": false,
"isPassThruServiceAccount": false,
"isProxyEnabled": false,
"isProxyDHCPEnabled": false,
"isRootPasswordEnabled": false,
"isSshEnabled": false
}
}
}
```

cURL Example

```
```

Success Response

Response Body

```json
{ "status": true,
"managementSystem": [ ]
}
Delete a Management System

Deletes a management system.
Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems/{dnsname/ipaddress}

Request Method

DELETE

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

cURL Example


Success Response

Response Body

{"status":true}

Update a Management System

Updates a management system based on the provided information.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/resources/managementsystems/{dnsname/ipaddress}

Request Method

PUT
Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json

Request Body

{"accountInfo":
    {
        "user": "administrator",
        "password": "<password>"},
    "managementSystem":{
        "name":"10.222.73.140VCNewName",
        "dnsName":"10.222.73.140",
        "ipAddress":"10.222.73.140",
        "mgmtSystemType":"VirtualCenter",
        "protectedResourceDetails":{
            "publishedIpAddress":"10.222.73.160",
            "publishedDnsName":"10.222.73.160",
            "publishedNetMask":"255.255.255.0",
            "isACL":false,
            "isPassThru":false,
            "isPassThruServiceAccount":false,
            "isProxyEnabled":false,
            "isProxyDHCPEnabled":false,
            "isRootPasswordEnabled":false,
            "isSshEnabled":false
        }
    }
}
cURL Example

```
```

Success Response

Response Body

```json
{"status":true,
 "managementSystem": [
  {"name":"10.222.73.140VCNewName",
   "uid":"7e68a936-7ee1-4845-aab7-623829db4abd",
   "resourceType":"ManagementSystem",
   "resourceUuid":"6C48D81E-95B5-4AC9-AAA4-336D6CC299C2",
   "dnsName":"10.222.73.140",
   "ipAddress":"10.222.73.140",
   "trustStatus":"Unknown",
   "mgmtSystemType":"VirtualCenter",
   "protectedResourceDetails":
    {"portHttp":80,
     "portHttps":443,
     "portSdk":80,
     "portSdks":443,
     "portSsh":22,
     "publishedIpAddress":"10.222.73.160",
     "publishedDnsName":"10.222.73.160",
     "publishedNetMask":"255.255.255.0",
     "isACL":false,
     "isPassThru":false,
     "isPassThruServiceAccount":false,
     "isProxyEnabled":false,
```
"isProxyDHCPEnabled":false,
"isRootPasswordEnabled":false,
"isSshEnabled":false,
"isUsingHttps":true,
"isUsingSdks":true,
"isProtected":false,
"isSupported":true}

}}

Label Management

The Label APIs allows CRUD operations on labels. These APIs also allow other label-based operations such as assigning labels to resources and getting templates associated with specific labels.

Get All Labels

Gets all the labels in CloudControl.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/labels

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json
cURL Example

```bash
```

Success Response

Response Body

```json
{"status":true,
 "label": [
  {"name":"CoreAppliance",
   "uid":"29c079d0-015d-4896-b99b-dbfdd5b33e68"},
  {"name":"DEV",
   "uid":"DEV"},
  {"name":"yuan label 1",
   "uid":"fd4504f9-a4e4-4007-98e4-110ae10d0a77",
   "complianceTemplate":
    {"name":"SOX ESXi_yuan_copy",
     "uid":"c430ebbd-ff70-401a-9fd1-597c17fae35c"}
  }
 ]
}
```

Response Body Fields/Objects

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Boolean</td>
<td>true/false</td>
</tr>
<tr>
<td>label</td>
<td>Collection of Label Objects</td>
<td>all the labels</td>
</tr>
</tbody>
</table>

Label object
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>name of the label</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
<tr>
<td>complianceTemplate</td>
<td>ComplianceTemplate object</td>
<td>The compliance template associated to the label</td>
</tr>
</tbody>
</table>

**ComplianceTemplate object**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>name of the compliance template</td>
</tr>
<tr>
<td>uid</td>
<td>string[255]</td>
<td>globally unique id</td>
</tr>
</tbody>
</table>

**Get Label by uid**

Gets labels based on the specified uid.

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/labels/{uid}

**Request Method**

GET

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json
Content-Type

application/json

cURL Example

```
$curl -b cookies -i -k https://<CloudControl_hostname>/asc/api/rest/v1/labels/fd4504f9-a4e4-4007-98e4-110ae10d0a77 -H "Accept: application/json" -H "Auth-Token: 9427E55E019E4DD6C30011B9B5E7AA88"
```

Success Response

Response Body

```
{"status":true,
 "label":[
 {"name":"yuan label 1",
  "uid":"fd4504f9-a4e4-4007-98e4-110ae10d0a77",
  "complianceTemplate":
   {"name":"SOX ESXi_yuan_copy",
    "uid":"c430ebbd-ff70-401a-9fd1-597c17fae35c"}
 }]
}
```

Get Compliance Template Associated to Label

Gets a compliance template associated with the specified label.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/compliancetemplates?labeluid={labeluid}

Request Method

GET

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json
Content-Type

application/json

cURL Example

$curl -b cookies -i -k https://<CloudControl_hostname>/asc/api/rest/v1/compliancetemplates?labeluid=fd4504f9-a4e4-4007-98e4-110ae10d0a77 -H "Accept: application/json" -H "Auth-Token: 9427E55E019E4DD6C30011B9B5E7AA88"

Success Response

Response Body

{"status":true,  "complianceTemplate": [  {"name":"SOX ESXi_yuan_copy",  "uid":"c430ebbd-ff70-401a-9fd1-597c17fae35c"} ]}

Failure Response:

Response Body

{"status":false,  "error":{"code":"500","message":"ARC0160"}}

Add Labels

Creates a new label.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/labels

Request Method

POST

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88
Accept

application/json

Content-Type

application/json

Request Body

{
"label": [
  {
    "name": "custLabelA",
  },
  {
    "name": "custLabelB"
  }
]
}
or
{
  "label": [
    {
      "name": "custLabelA",
      "complianceTemplate":
      {
        "name": "PCI DSS 3.0 ESXi"
      },
    },
    {
      "name": "custLabelB"
    }
  ]
}

cURL Example


Success Response

Response Body

{
  "status": true,
  "label": [
    {
      "name": "custLabelA",
      "uid": "8fffc521-003d-43e8-ad02-5d5c4ffe0b07",
      "complianceTemplate":
      {
        "name": "PCI DSS 3.0 ESXi"
      }
    }
  ]
}
"uid": "11d00120-7570-4a99-a18d-b617b102a095"},
{"name": "custLabelB",
"uid": "c942ca48-dc38-44a5-a5ba-7fe735c73e66"}
]
}

**Update Labels**

Updates labels based on specified information.

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/labels

**Request Method**

PUT

**Request Header**

**Auth-Token**

9427E55E019E4DD6C30011B9B5E7AA88

**Accept**

application/json

**Content-Type**

application/json

**Request Body**

{"label": [
{"name": "custLabelA1",
"uid": "8fffc521-003d-43e8-ad02-5d5c4ffe0b07"},
{"name": "custLabelB2",
"uid": "c942ca48-dc38-44a5-a5ba-7fe735c73e66",
"complianceTemplate": {"name": "CIS ESXi"}]
]
cURL Example

```
```

Success Response

Response Body

```
{"status":true,
 "label":[
   {
    "name":"custLabelA1",
    "uid":"8fffc521-003d-43e8-ad02-5d5c4ffe0b07"},
   {
    "name":"custLabelA2",
    "uid":"c942ca48-dc38-44a5-a5ba-7fe735c73e66",
    "complianceTemplate":
    {
     "name":"CIS ESXi",
     "uid":"acd5ba72-a822-4cda-a636-013f3985aad7"}
   }
 ]
}
```

Delete Labels

Deletes labels.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/labels

Request Method

DELETE

Request Header

```
Authorization
9427E55E019E4DD6C30011B9B5E7AA88
Accept
application/json
```
Content-Type

application/json

Request Body

{"label": [
  {"uid": "8fffc521-003d-43e8-ad02-5d5c4ffe0b07"},
  {"uid": "c942ca48-dc38-44a5-a5ba-7fe735c73e66"}
]}

cURL Example


Success Response

Response Body

{"status":true}

Assign a Label to Resources

Assigns the specified label to resources.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/labels/{labeluid}/resources

Request Method

PUT

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json
Content-Type

application/json

Request Body

{ "resource": [
  { "uid": "256211e2-339d-4d33-b0bb-b9497e34fed8" },
  { "uid": "ef1e690a-b724-4b9b-916b-25bd45df7e19" }
]

\cURL Example


Un-assign a Label from Resources

Removes a label assigned to resources.

Request URI

https://<CloudControl_hostname>/asc/api/rest/v1/labels/\{labeluid\}/resources

Request Method

DELETE

Request Header

Auth-Token

9427E55E019E4DD6C30011B9B5E7AA88

Accept

application/json

Content-Type

application/json
Request Body

```json
{  "resource": [    {"uid":"256211e2-339d-4d33-b0bb-b9497e34fed8"},    {"uid":"ef1e690a-b724-4b9b-916b-25bd45df7e19"}
  ]}
```

cURL Example

```
```

**Global PIP**

Retrieves all Global PIP connectivity information in a JSON object.

**Request URI**

https://<CloudControl_hostname>/asc/api/rest/v1/resources/hostmenu

**Request Method**

GET

**Request Header**

Auth-Token
2D9F8F8F32BB860B3BE74FF0CE36AE88

Accept
application/json

**cURL Example**

```
```
Success Response

Response Header

Date: Tue, 11 Jun 2019 08:28:50 GMT
Server: Apache-Coyote/1.1
X-FRAME-OPTIONS: SAMEORIGIN
X-Content-Type-Options: nosniff
X-XSS-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000
Content-Type: application/json
Set-Cookie: JSESSIONID=9F7B8497EB60BEA5F118EFD368642422; Path=/asc/; Secure;HttpOnly
Transfer-Encoding: chunked

Response Body


Failure Response

Response Body

{"status":false,"error":{"code":"API0076","message":"No hosts to be returned"}}
Appendix G. CloudControl REST Proxy

Rest Proxy Overview

CloudControl offers a REST Proxy framework that provides authentication and authorization of REST-based services that support information management platforms such as VMware NSX. The CloudControl REST Proxy parses the REST API payload and authenticates and authorizes the request based on access control set up using CloudControl. For the CloudControl REST Proxy to protect a REST API on a host it must be an CloudControl Protected Host that:

- Provides the Published IP (PIP) for Proxy.
- Imports the Host’s Certificate, if needed.

CloudControl REST Proxy currently supports the VMware NSX environment. Contact HyTrust Customer Support for the most current list of supported platforms.

Disabling Unknown NSX Manager Operations

By default, unknown NSX operations over Rest APIs are permitted. However, unknown NSX Rest APIs are not currently recognized by CloudControl. You can configure CloudControl to disable unknown NSX Rest operations per NSX.

1. Select Compliance > Host.
2. On the Hosts page, click the VMware NSX host that you want to modify.
3. On the Edit Host page, click the Advanced tab, and then clear the Permit unknown NSX operations checkbox.
4. Click OK.

Log Content

The following API information is available in the CloudControl REST Proxy logs:

- Action
Supported APIs

The following table lists the available CloudControl REST Proxy logs.

<table>
<thead>
<tr>
<th>Log</th>
<th>Action</th>
<th>Response Returned</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogViewer</td>
<td>Authentication</td>
<td>Success/Failure</td>
</tr>
<tr>
<td></td>
<td>Authorization</td>
<td>Permit/Deny</td>
</tr>
<tr>
<td>CloudControl Internal Logs</td>
<td></td>
<td>Success/Failure</td>
</tr>
<tr>
<td>Debug</td>
<td>Logs in a separate file</td>
<td>/var/log/asc/htcc-services-rest-proxy.debug</td>
</tr>
</tbody>
</table>

**Supported APIs**

The CloudControl REST Proxy currently supports all NSX Distributed and Edge Firewall, Object Group, Security Policy, Security Tag, IP Set, MAC Set, Distributed Firewall Section, and DFW in Cross vCenter APIs.

**Note:** CloudControl supports granular level authorization for NSX REST APIs with enhanced privilege mapping for operations.

Contact HyTrust Customer Support for the most current list of supported NSX APIs.

**REST Proxy API Error Responses**

The following table displays typical error messages CloudControl sends to the REST Proxy API client.

<table>
<thead>
<tr>
<th>REST Proxy API Action</th>
<th>Response Type</th>
<th>Sample Return Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>AUN0004</td>
<td>&lt;?xml version=&quot;1.0&quot; encoding=&quot;UTF-8&quot;?&gt;&lt;error&gt;&lt;details&gt;The authentication for dadminuser is declined&lt;/details&gt;&lt;errorCode&gt;AUN0004&lt;/errorCode&gt;&lt;/error&gt;</td>
</tr>
<tr>
<td>Authorization</td>
<td>AUN0135</td>
<td>&lt;?xml version=&quot;1.0&quot; encoding=&quot;UTF-8&quot;?&gt;&lt;error&gt;&lt;details&gt;Permission denied due to security policy&lt;/details&gt;&lt;errorCode&gt;AUN0135&lt;/errorCode&gt;&lt;/error&gt;</td>
</tr>
</tbody>
</table>
### Error Response Status Codes

Users may have to revise their scripts to incorporate the CloudControl REST Proxy Status Codes displayed in the following table:

<table>
<thead>
<tr>
<th>Scenario</th>
<th>NSX Status Code on Direct IP</th>
<th>REST Proxy Status Code on Published IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Invalid Credentials</td>
<td>403 Forbidden</td>
<td>403</td>
</tr>
<tr>
<td>Invalid URL</td>
<td>404 Not Found</td>
<td>404</td>
</tr>
<tr>
<td>Without authorization header</td>
<td>403 Forbidden</td>
<td>403</td>
</tr>
<tr>
<td>Invalid input data</td>
<td>400 Bad Request</td>
<td>400</td>
</tr>
<tr>
<td>Invalid ETag</td>
<td>412 Precondition Failed</td>
<td>412</td>
</tr>
<tr>
<td>Without mentioning method type</td>
<td>501 Not Implemented</td>
<td>501</td>
</tr>
<tr>
<td>Without If-Match Header</td>
<td>500 Internal Server Error</td>
<td>500</td>
</tr>
<tr>
<td>Wrong payload</td>
<td>400 Bad Request</td>
<td>400</td>
</tr>
</tbody>
</table>

```xml
<?xml version="1.0" encoding="UTF-8"?><error><details>Unexpected error with the server</details><errorCode>RSP04500</errorCode></error>
```
Appendix H. vSphere 6.x Support in CloudControl

CloudControl vSphere 6.x Support Overview ......................................................... 296
Enhanced Link Mode (ELM) ..................................................................................... 296
ELM Support in CloudControl ............................................................................... 297
vSphere 6x Deployment Topologies ...................................................................... 297
Single Sign-On in vSphere 6.x .............................................................................. 298
Login and Authentication in CloudControl ......................................................... 298
Configuring ELM ................................................................................................. 299
vSphere 6.x Enhanced Linked Mode (ELM) Set Up .............................................. 299
Configuring the vSphere 6x Web Client Server in CloudControl ..................... 301
vSphere 6.x Upgrade or Migration Notes ............................................................. 302
vCenter High Availability (VCHA) Support ......................................................... 302

CloudControl vSphere 6.x Support Overview

CloudControl supports the following new features introduced in vSphere 6.x: Single Sign-On authentication, Enhanced Linked Mode (ELM), and new deployment topologies that are implemented using Platform Services Controller.

CloudControl supports cross vCenter vMotion and all existing operations on vCenters except for Long Distance vMotion.

Note: TLS 1.0 is not supported with vSphere 6.5.

Enhanced Link Mode (ELM)

vCenter Linked Mode provides the following capabilities for managing various vCenter instances:

- Offers a single management overview of multiple vCenter instances
- Provides a single login for multiple vCenter Server
- Shows a common inventory view and allows for searching of objects across vCenters.
- Replicates licenses, roles and permissions between vCenter instances.

There are two basic architectures for deploying vSphere 6.x:
- vCenter Server with an embedded Platform Services Controller (PSC).
- vCenter Server with External Platform Services Controller.

As a result of these architectures, Platform Services Controllers can be linked together. This enables an aggregate view of any vCenter Server that is configured to use the SSO domain. This feature is called Enhanced Linked Mode (ELM). Once you provide the connection details and SSO credentials for one of the ELM VCs, CloudControl will auto-discover all the VCs/PSCs.

vCenter Server with an Embedded Platform Services Controller is ideal for small environments.

**ELM Support in CloudControl**

CloudControl provides the following new features and functionalities for ELM support:
- Auto discovery of ELM setup.
- Auto discovery of NSX in ELM.
- Ability to specify range of PIPs for ELM setup.
- Ability to discover and auto protect VCs if ELM setup is expanded.
- Ability to discover and auto remove VCs if ELM setup is scaled down.
- Alerts sent/raised in cases where CloudControl is not able to auto-protect VCs of an expanded ELM set up.
- Modernized resource tree representation of ELM topology.
- Enforces CloudControl policy at PSC/SSO Domain level which propagates down to entities below them.
- Improved Add Host flow UI.

**vSphere 6x Deployment Topologies**

The following ELM topologies are supported by CloudControl:

**Recommended 1 (R1)**

- 1 Single Sign-On domain
- 1 Single Sign-On site
- 1 vCenter Server with embedded Platform Services Controller
Recommended 2 (R2)

- 1 Single Sign-On domain
- 1 Single Sign-On site
- 1 external Platform Services Controllers
- 1 or more vCenter Server with external Platform Services Controllers

Recommended 3 (R3)

- 1 Single Sign-On domain
- 2 or more Single Sign-On sites
- 2 or more external Platform Services Controllers
- 2 or more vCenter Server with external Platform Services Controller

Recommended 4 (R4)

- 1 Single Sign-On domain
- 1 Single Sign-On site
- 2 or more external Platform Services Controllers
- 1 or more vCenter Server with external Platform Services Controllers
- 1 third-party load balancer

Single Sign-On in vSphere 6.x

The Single Sign-On (SSO) authentication method in vSphere 6.x provides a secure way to login to the vSphere resources. It eliminates the need to authenticate a user by each of the vSphere components separately. Users login to the vSphere Web Client using their vSphere credentials and get authenticated through the configured SSO server. For any subsequent logins, vSphere does not ask the user for credentials.

Login and Authentication in CloudControl

CloudControl supports authentication through Active Directory. To support SSO authentication, the Published IP (PIP) of the protected Web Client Server must be registered with the SSO server. For more information, see Configuring the vSphere 6x Web Client Server in CloudControl on page 301.

There are three authentication modes available in CloudControl when authenticating a user against Active Directory:
- Use CloudControl Service Account (default)
- Use Pass Through without CloudControl Service Account
- Use Pass Through with CloudControl Service Account

The Single Sign-On over PIP will work for vCenters belonging to or sharing a common Platform Services Controller. However, for vCenters belonging to different Platform Services Controllers, credentials will have to be provided again.

The SSO authentication occurs as described in the following steps:

1. User opens the Web Client using PIP. The Web Client Server creates a SAML metadata request which is sent to the SSO server through the browser.
   - The SSO server looks for a browser cookie CastleSessionNNNNNNNN, where NNNNNNNN is the name of the SSO domain. If the cookie exists and is valid, then the user has already been authenticated.
   - The SSO server presents the login form to the user, if the cookie does not exist.

2. User enters the login credentials.
   - The SSO server authenticates the user if the credentials are valid.
   - The SSO server creates an authentication cookie and sends it to the browser.
   - The browser saves the newly created cookie which is used to authenticate the user at the future logins.

3. When PIP of the Web Client Server changes, you must re-import the SAML metadata in order to access the new PIP. For more information, see Configuring the vSphere 6x Web Client Server in CloudControl on page 301.

---

**Configuring ELM**

For vSphere 6.x you cannot add only WCS. For protecting vSphere 6.x, the valid options are:

- vCenter, vSphere Web Client Server and VMware NSX.
- Other Hosts.

When you select either of these two options, CloudControl will automatically protect WCS for each VC.

You must provide connection details and SSO credentials for one of the VCs of the ELM. All others will be auto-discovered and populated on the UI.

For more information on ELM, see VMWare Enhanced Link Mode documentation.

---

**vSphere 6.x Enhanced Linked Mode (ELM) Set Up**

1. Select **Compliance > Hosts**.
2. On the Hosts page, click **Add**.
3. On the Add Host Wizard, select the type of host you are adding, and click **Next**.
4. On the Host Login page, enter the following:
   - The fully qualified hostname or IP address of vCenter Server (or Host).
   - The administrator User ID and Password for vCenter Server (or root credentials for a host).
     **Note:** You will not be able to add a host with a password that contains both, the left angle bracket (‘<’) and the right angle bracket (’>’) characters. However, passwords with either character are supported.

     Optionally, you can modify the values in the Advanced Properties section which define the ports on which CloudControl communicates with the vCenter. In most cases, the default values can be used.
     **Note:** The advanced properties apply to all vCenters in the ELM setup.

5. Click **Next**.

The ELM SetUp Details page appears.

When vCenter version 6.x is detected, CloudControl performs auto discovery and discovers all vCenters, PSC and WCS in the ELM setup and displays them in the ELM Setup Detail page.

The initial display shows:
   - Consolidated VC/WCS details.
   - PSC details.
   - PIP and Netmask values.
     When a specific PIP is assigned to a host CloudControl looks up the hostname and, if found, assigns it to target.
   - WCS list with HTTPS Port value. For vSphere 6.x the default is 443.

6. Optionally, you can:
   1. Define a Friendly Name and Description for each vCenter.
   2. Establish a PIP range in the Published IP Range pane that CloudControl will assign to vCenters in the ELM setup.
      A PIP range can be defined in addition to existing published IP and Netmask values displayed in the VC/WCS Details pane. A combination of both the PIP range and the existing published IPs is allowed.
      When you define a IP range it must not be less than the number of vCenters in the ELM setup.
   3. Name extra IP that can be used later to auto-protect discovered vCenters in the ELM setup.
   4. Configure a port number to be used for each WCS. For vSphere 6.x, the default port number is 443.

CloudControl protects all vCenters that are discovered in the ELM setup.

7. Click **Next**.
Configuring the vSphere 6x Web Client Server in CloudControl

The NSX Details page displays the:
- NSX endpoints with PIP and Netmask columns.
- Protected checkbox for all the NSX managers.
  
  **Note:** The resource tree for NSX Manager is shown under PSC as a peer of the vCenter.

8. On the NSX Details page, click **Next**.

9. On the Complete Host Add page, click **Finish**.

If there is a separate NSX account, the same values can be configured as a Service Account on this page.

### Configuring the vSphere 6x Web Client Server in CloudControl

SSO authentication occurs through SAML requests and responses between CloudControl, the browser, the Web Client Server, and the SSO server. The Web Client Server and the SSO server exchange SAML metadata to establish a session. SAML-enabled services query SAML metadata information frequently during the authentication process.

The PIP of every Web Client protected by CloudControl must be registered with the SSO server. You must download the metadata file in CloudControl and then upload it to the Web Client.

1. Login to the CloudControl Management Console as administrator.

2. Ensure that the WCS and PCS Certificates are installed.
   
   If the Platform Services Controller (PSC) is not embedded with vCenter, the PSC certificate needs to be imported separately into CloudControl. If PSC is embedded with vCenter, importing the vCenter certificate is sufficient. For more information see **Managing Certificates** on page 55.
   
   **Note:** To obtain the certificate for an external PSC, you need to connect to the PSC using your browser and download the certificate. The procedure may differ depending on the browser and version that you are using. Alternatively, you can contact your vSphere administrator to obtain the certificate.

3. Select **Compliance > Hosts** and select the Web Client Server from the list of protected resources.

4. Click **Download Web Client Metadata** to download the metadata for the Web Client.
   
   **Note:** You can also click **Download HTML 5 Client Metadata** to download the metadata for the vSphere Client.

5. Log directly into WCS as administrator. Do not use the PIP.
6. From the Home icon, select Administration > Single Sign-on > Configuration.

7. On the Configuration page, click SAML Service Providers, then click Import to import the metadata file that you downloaded. If you downloaded more than one file, upload them one at a time.

   **Note:** If the metadata buttons are not visible, you may be missing the Asc.SAMLConfig privilege. Contact your CloudControl administrator to have the Asc.SAMLConfig privilege added.

---

**vSphere 6.x Upgrade or Migration Notes**

When you upgrade or migrate a vCenter Server with an embedded or external Platform Services Controller (PSC), be aware of the following:

- With an embedded PSC, the vCenter Server, the vCenter Server components, and the services included in the Platform Services Controller are deployed on the same system.
- With an external PSC, you need to manually reimport the PSC certificates to CloudControl.

**Important:** After you upgrade or migrate, you should run the following scheduled events:

1. Refresh Patch Levels—Updates the patch level for all hosts.
2. Refresh ELM Setup—Updates the resource tree for the upgraded VC, and discovers and protects any VCs which are part of the same VC.

---

**vCenter High Availability (VCHA) Support**

Beginning with CloudControl Version 5.6, we now offer support for the vSphere 6.5 vCenter High Availability. The following VCHA operations are supported:

- Deploying VCHA using either the Basic or Advanced option. The passive and witness virtual machines will be visible in the CloudControl resource tree.
  - Basic—CloudControl authorizes the VCHA setup, which adds the two new virtual machines automatically.
  - Advanced—CloudControl users must manually clone the two virtual machines, and then configure VCHA.

   **Note:** If the passive and witness virtual machines are not visible in the CloudControl resource tree, perform a manual policy refresh.

- Initiating failover tasks
- Editing VCHA
- Removing VCHA.
Appendix I. Using vRealize Orchestrator with CloudControl

Beginning with HyTrust CloudControl version 5.5, you can use vRealize Orchestrator (vRO) to manage vCenters that are protected by CloudControl. vRO is a general purpose IT automation product that allows you to automate various operations in a VMware vSphere data center.

CloudControl supports the following VMware vCenter Server versions with vRO version 7.2.0 and 7.3.0:

- 6.5 U1
- 6.5.0
- 6.0 U3
- 6.0 U2
- 6.0 U1
- 6.0.0

vRO Access

To access your CloudControl protected vCenters, supply the CloudControl PIP, username, and password in the 'Create vCenter instance' workflow in the vRealize Orchestrator Client. You must also configure vRO to use vSphere Authentication with the Platform Service Controller instance that contains the vCenter.

For protected vCenters accessed via vRO, CloudControl manages the following:

- All vCenter policy definitions.
- All audit logs for administration actions.
- RBAC Authorization.

For example, if you start a workflow to create a VM with vRO, CloudControl authorizes and logs the action.

vRO Connection Methods

By default, vRO allows you to choose which connection method you’d like to use to connect to the vCenter instances.

<table>
<thead>
<tr>
<th>Connection Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Share a unique session</td>
<td>Creates only one connection to vCenter using the user credentials used to add vCenter in vRO. All operations performed on this vCenter will use same connection no matter what user is logged in to the vRO client. We recommend that you do not use this method. CloudControl will receive, authorize, and log all of the actions as if they are from the same user, which provides no RBAC benefits.</td>
</tr>
<tr>
<td>Session per user</td>
<td>Creates a new connection to vCenter server for each individual user. We recommend that you use this method.</td>
</tr>
</tbody>
</table>
Limitations

- CloudControl only supports the vRO client, not the vRO WCS plugin.

- If you are in CloudControl Demo mode, the 'session per user' method does not function correctly. Because there is no authentication enabled, you will receive multiple log messages from CloudControl stating that authorization has failed.

- All users that log in to vRO must have the System.Anonymous and System.Read privileges. Without these privileges, vRO will show the vCenter as unusable, and you will receive multiple DENY messages from CloudControl.
Appendix J. SNMP Trap Alerts

About SNMP Trap Alerts

CloudControl provides a variety of alerts that can be trapped by SNMP collectors. It can take up to 15 minutes for a specific trap to be generated.

SNMP Trap Details

Beginning in HyTrust CloudControl version 5.4, we are augmenting each SNMP Trap message with a set of Key=Value pair string objects to provide details regarding what caused the trap to be sent. The MIB/OID strings are located in /usr/share/snmp/mibs/ASC-MIB.txt. Load the HyTrust MIB into your analysis tool to parse the messages.

Refer to your analysis tool documentation for how to import or load MIBs.

<table>
<thead>
<tr>
<th>OID Identifier</th>
<th>Value</th>
<th>MIB Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv2-SMI::enterprises.33095.0.1001.1</td>
<td>STRING: &lt;service_name&gt;</td>
<td>faultedService</td>
</tr>
<tr>
<td>SNMPv2-SMI::enterprises.33095.0.1001.2</td>
<td>STRING: &lt;host_FQDN&gt;</td>
<td>faultedFQDN</td>
</tr>
<tr>
<td>SNMPv2-SMI::enterprises.33095.0.1001.3</td>
<td>STRING: &lt;host_IP&gt;</td>
<td>faultedIP</td>
</tr>
<tr>
<td>SNMPv2-SMI::enterprises.33095.0.1001.4</td>
<td>INTEGER: &lt;statusCode&gt;</td>
<td>statusCode</td>
</tr>
<tr>
<td>SNMPv2-SMI::enterprises.33095.0.1001.5</td>
<td>STRING: &lt;serviceType&gt;</td>
<td>faultedServiceType</td>
</tr>
</tbody>
</table>

Each fault will generate a single SNMP Trap message.

SNMP Service Status

The following statuses are assigned to any service on CloudControl:

<table>
<thead>
<tr>
<th>Status Number</th>
<th>Status Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Healthy—The service is healthy and running fine.</td>
</tr>
<tr>
<td>2</td>
<td>Warning—The service is having issues and approaching failure.</td>
</tr>
</tbody>
</table>
### SNMP Traps

CloudControl uses the following SNMP traps:

#### Protected Host

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
</table>
| Protected Host Monitoring   | Warning when the host is unreachable, Healthy when CloudControl can communicate with the host again.  
**Note:** This trap requires that protected host monitoring is enabled using the CLI command `asc monitor --protected on`. | Healthy | 1           |
|                             |                                                                            | Warning| 2           |

#### Networking

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router Monitoring</td>
<td>Warning when the router is unreachable, Healthy when CloudControl can communicate with the router again.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td>SMTP Server Monitoring</td>
<td>Warning when the email server is unreachable, Healthy when CloudControl can communicate with the email server again.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td>NTP Monitoring</td>
<td>Warning when the NTP server is unreachable, Healthy when CloudControl can communicate with the NTP server again.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
</tbody>
</table>

#### High Availability (HA)

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CloudControl HA Host</td>
<td>Critical when secondary HA node is offline, Healthy when the node is back online and successfully synced.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
</tbody>
</table>
## Authentication

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA Server Connection Monitoring</td>
<td>Warning when the RSA server is unreachable, Healthy when CloudControl can communicate with the RSA server again.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
</tbody>
</table>

## Appliance Health

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Monitoring</td>
<td>Trigger points are based on the 15-minute running load-average divided by the number of the vCPUs in the appliance. Warning threshold is reached at a 1.0 to 1 ratio, Critical is reached at a 5.0 to 1 ratio, Healthy when the CPU utilization returns to a lower ratio.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
<tr>
<td>Memory Monitoring</td>
<td>Trigger points are based on the swap usage and RAM usage. For swap, Warning threshold is reached when 20% of swap space is used, Critical when 70% swap space is used, Healthy when swap has returned to less than 20%. For RAM, Warning threshold is reached when 95% of all RAM is used, Healthy when memory use has returned to less than 95%. If RAM is at the Warning threshold, and swap is at Critical, you will receive a Critical message for both RAM and swap.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
<tr>
<td>Disk Monitoring</td>
<td>Warning at 85% disk usage, Critical at 95%, Healthy when database disk usage has returned to less than 85%.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
<tr>
<td>Scheduled Jobs Monitoring</td>
<td>Warning when a scheduled job has failed, Healthy when the job has recovered.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td>Backup and Restore Monitoring</td>
<td>Warning when the backup is outdated and was created after the last RPV event, Healthy when the backup is now up to date.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td>License (Support and Maintenance Expiry) Monitoring</td>
<td>Warning at 10 days before the license expires, Critical at 3 days before, Healthy when the license is updated. <strong>Note:</strong> This trap requires that the License Monitor SNMP Trap scheduled event is enabled.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
</tbody>
</table>
SNMP Trap Examples

HyTrust High Availability

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Status</th>
<th>Status Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>License (CPU and Host Capacity) Monitoring</td>
<td>Warning when 75% of the licensed sockets are in use, Critical when 90% are in use, Healthy when the license is updated.</td>
<td>Healthy</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td>Note: This trap requires that the License Monitor SNMP Trap scheduled event is enabled.</td>
<td>Warning</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical</td>
<td>3</td>
</tr>
</tbody>
</table>

SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.33095.0.1101
SNMPv2-SMI::enterprises.33095.0.1101 = STRING: "HyTrust High Availability (HA) changed status to healthy (OK) from warning (Warning: Secondary Database Disk Usage: 93%"
SNMPv2-SMI::enterprises.33095.0.1001.1 = STRING: "High Availability (HA)"
SNMPv2-SMI::enterprises.33095.0.1001.2 = STRING: "UNKNOWN"
SNMPv2-SMI::enterprises.33095.0.1001.3 = STRING: "10.222.73.133"
SNMPv2-SMI::enterprises.33095.0.1001.4 = INTEGER: 1

SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.33095.0.1102
SNMPv2-SMI::enterprises.33095.0.1102 = STRING: "HyTrust High Availability (HA) changed status to warning (Warning: Secondary Networking: Router 10.222.73.1 is offline) from failed (Failed: The secondary node HA interface is offline)"
SNMPv2-SMI::enterprises.33095.0.1001.1 = STRING: "High Availability (HA)"
SNMPv2-SMI::enterprises.33095.0.1001.2 = STRING: "UNKNOWN"
SNMPv2-SMI::enterprises.33095.0.1001.3 = STRING: "10.222.73.133"
SNMPv2-SMI::enterprises.33095.0.1001.4 = INTEGER: 2

SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.33095.0.1103
SNMPv2-SMI::enterprises.33095.0.1103 = STRING: "HyTrust High Availability (HA) changed status to failed (Failed: The secondary node HA interface is offline) from warning (Warning: Secondary Networking: Router 10.222.73.1 is offline)"
SNMPv2-SMI::enterprises.33095.0.1001.1 = STRING: "High Availability (HA)"
SNMPv2-SMI::enterprises.33095.0.1001.2 = STRING: "UNKNOWN"
SNMPv2-SMI::enterprises.33095.0.1001.3 = STRING: "10.222.73.133"
SNMPv2-SMI::enterprises.33095.0.1001.4 = INTEGER: 3
Protected Host Monitoring:

[UDP: [10.230.34.139]:55646->[10.222.82.60]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10758564) 1 day, 5:53:05.64
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.33095.0.1101
SNMPv2-SMI::enterprises.33095.0.1101 = STRING: "HyTrust Protected Host Monitoring changed status to healthy (OK) from warning (Offline: 10.230.34.36)"
SNMPv2-SMI::enterprises.33095.0.1001.1 = STRING: "Protected Host Monitoring"
SNMPv2-SMI::enterprises.33095.0.1001.2 = STRING: "green-esxi2.htcc.com"
SNMPv2-SMI::enterprises.33095.0.1001.3 = STRING: "10.230.34.36"
SNMPv2-SMI::enterprises.33095.0.1001.4 = INTEGER: 1

[UDP: [10.230.34.139]:34171->[10.222.82.60]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (10747824) 1 day, 5:51:18.24
SNMPv2-MIB::snmpTrapOID.0 = OID: SNMPv2-SMI::enterprises.33095.0.1102
SNMPv2-SMI::enterprises.33095.0.1102 = STRING: "HyTrust Protected Host Monitoring changed status to warning (Offline: 10.230.34.36) from healthy (OK)"
SNMPv2-SMI::enterprises.33095.0.1001.1 = STRING: "Protected Host Monitoring"
SNMPv2-SMI::enterprises.33095.0.1001.2 = STRING: "green-esxi2.htcc.com"
SNMPv2-SMI::enterprises.33095.0.1001.3 = STRING: "10.230.34.36"
SNMPv2-SMI::enterprises.33095.0.1001.4 = INTEGER: 2