TECHNICAL DOCUMENTATION

Cloudpath

Cloudpath Enrollment System

Cloudpath Operations Manual

Software Release 5.1

May 2017

Summary: This document describes how to access and manage Cloudpath servers within your network.
Document Type: Reference
Audience: Operations Administrator

Cloudpath

Cloudpath Operations Manual

Software Release 5.1

May 2017

This document contains Ruckus Wireless confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without express written authorization of a Customer Advocacy representative of Ruckus Wireless, Inc. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing, RUCKUS WIRELESS PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Cloudpath Operations Manual

Overview

This document describes how to access and manage the Cloudpath Enrollment System (ES) servers within your network. Basic operations are described in the following sections:

- System Information
- General Maintenance
- Logs
- General System Administration
- Backup and Recovery
- Snapshots
- VM Maintenance
- Upgrades
- Managing Replication
- Reports
- Support
- Command Reference

System Information

This section provides placeholders for referencing the IP addresses and DNS information for each server in the system, as well as login information for each system.

TABLE 1. **System Information**

Name	IP Address	DNS
<ES1>		
<ES2>		
<ES3>		
<ES4>		

Administrative Access

Administrators can manage the system from any Cloudpath server. Web traffic (end-user, API, and OCSP) is distributed across the systems via an external load balancer.

Use the following information to log into the Cloudpath Admin UI or access the system using the console.

TABLE 2. **Admin Access Information**

Interface	Login	Password
Admin UI		
Console/SSH	cpn_service	

Note >>
Use of strong passwords is recommended.

Administrator Roles

Cloudpath supports the following Administrator Roles:

- CA Administrator - Allows full configuration access to the Administrative UI. This administrator role can manage all administrative users.
- Administrator - Allows full configuration access to the Administrative UI, except for Certificate Authorities. This administrator can manage Administrator and Viewer administrative users.
- Viewer - Allows view-only access to Enrollment, User, and Certificate records on the Dashboard, the enrollment Workflow, and the Documentation and Licensing pages. This administrator cannot manage other administrative users.

General Maintenance

SSH

After the initial setup, an administrator can log into the system using SSH on port 8022 and use the command line interface to execute Cloudpath service commands. A service password is required to access the command line interface. See Admin Access Information for details.

The default SSH port number is 8022, but can be changed to port 22 on the Cloudpath *Administration > System > System Services* page.

Command Reference

The Cloudpath command line uses *klish* commands under the *config* menu and common *Cent OS* commands while in the *console* menu (Linux shell).

After a successful login to the service account, the Cloudpath configuration utility (klish) prompt (#) displays. Enter **?** to view the list of available commands.

From the configuration utility, enter the `console` command to access the Linux shell. From the Linux shell, enter the `config` command to access the Cloudpath configuration utility.

Common Commands

When running klish commands on the system, be aware of the difference between similar commands. For example:

- **system** - Reboots the system (virtual machine).
- **system** - Restarts the web server (JBoss).
- **system shutdown** - Shuts down the system. Warning: This requires VM access to boot.

See the full Command Reference at the end of this document for more information.

Testing Network Connectivity

The availability of the system can be monitored at various layers. At the lowest layer, the system responds to ICMP pings.

Positive Testing

The availability and responsiveness of the web server within the system may be monitored using the following URLs:

- https://HOSTNAME/enroll/ping

  This tests the enrollment portal portion of the system, and should return a 200 status.
- http://HOSTNAME/ocsp/ping OR https://HOSTNAME/admin/ocsp/ping

  This tests the admin, API, and OCSP portions of the system and should return a 200 status.

> **Note >>**
> The path is different for HTTPS and HTTP.

Negative Testing

The following URLs may be used for negative testing:

- https://HOSTNAME/ocsp/pingFail

  This should return a 404 error.

Scripts

Use the shell script to install a given application or to perform other tasks from the Linux shell. Scripts can contain commands to be executed sequentially or can use a more complex flow of execution.

Location of script files

You can access Cloudpath scripts from the Linux shell. Scripts are located in the */opt/cloudpath/scripts/* directory.

Cleanup Operations

Data Cleanup

The Cloudpath system is designed to clean up old data and log files. The *Data Cleanup* page (*Administration > Data Cleanup*) provides the ability to schedule automatic cleanup thresholds. In most environments, the default settings for cleanup operations are adequate.

Additionally, you can clean up items using the Cleanup section at the bottom of the associated page. For example, remove authentication server data using the Cleanup section at the bottom of the Modify Authentication Server page, or clean up workflows using the Cleanup section at the bottom of the Configuration > Workflows, Advanced tab.

Welcome Page Todo Items

When you first log into the Cloudpath Admin UI, the Welcome page displays. On this page, a *Todo Items* list may exist. The Todo Items indicates system or configuration issues that should be addressed.

> **Note >>**
> Configuration and Upgrade issues should be addressed by the System Administrator.

If the Todo Item message indicates that the disk partition is almost full, you might consider removing some old wizard versions that are saved.

Remove Old Wizard Versions

A system with multiple updates may contain unused wizard versions. The *Wizard Versions on Disk section* on the *Data Cleanup* page allows you to delete extraneous wizard versions. When you delete a version from the admin UI, it removes both the tar.gz and the extracted wizard files from the */opt/cloudpath/work/admin/versions* directory.

Other Cleanup Operations

The Cloudpath system provides additional cleanup commands, if needed.

For example:

- The **support system clean-disk** command cleans up the JBoss server log.
- The **replication force-cleanup** command forces the removal of the replication setup from the server.

See the full Command Reference at the end of this document for more information.

Firewall Settings

The Cloudpath Admin UI provides a table (*Administration > Firewall Requirements)* that lists the inbound and outbound traffic of your Cloudpath ES. This information is dynamically generated based on the current system configuration and can changes as the system configuration is modified.

Logs

Each system contains rolling logs, which can be reviewed for troubleshooting purposes.

Syslog

The ES web servers are configured to use a syslog as a central repository for VM and other server log messages. To view the syslog configuration, navigate to *Administration > System Services*, and expand the *Logs* service. The Syslog Status displays the syslog configuration information.

Other Logs

View or download additional logs from the *Logs* component. All logs can be run in *Normal* (default) or *Debug* (finer, or verbose) mode.

- **General** - The General log is the JBoss server log file, which are web application log files.
- **SCEP** - Logs related to Simple Certificate Enrollment Protocol (SCEP). The system provides an outward-facing SCEP server interface that allows SCEP clients, such as iOS, to pull certificates via SCEP.
- **OCSP** - Logs related to Online Certificate Status Protocol (OCSP), which is used for obtaining the revocation status of an X.509 digital certificate.
- **Replication** - Logs related to the replication setup and operation. See the Managing Replication section for more information.

Additional logs are located in the */var/log* directory from the Linux shell.

Event Logs

The *Events* log (*Dashboard > Notifications > Events*) displays all system events, such as account logins, enrollments, acceptance of AUPs, registrations, certificate issuance, errors, account updates, and snapshot creation.

Web Server

The Cloudpath web server is an Apache server and provides both and HTTP Access Log and an HTTP Error log. Navigate to *Administration > System Services*, and expand the *Logs* service.

Audit Logs

The system logs all administrative activity initiated from the Admin UI or the console. Audit log files are located in the */var/log/jboss/admin_audit.log* directory from the Linux shell:

Network Diagnostics

The Cloudpath system logs all network activity to and from individual components of the system, including protocols used, whitelists, and packet information. Navigate to *Administration > System Services*, and expand the *Network* service to view or download the *Network Diagnostic* logs.

General System Administration

The ES web server *Administration* tab provides access to system-related operations.

Administrators - During the initial account setup, the Cloudpath ES system sets up an administrator account using the *Company Information* provided during the setup. By default, there is also an *Administrator Group*, which allows administrative access to the Admin UI using credentials from the configured authentication server. This allows users that belong to a specific group to access the system.

Company Information - Used within the URL for enrollments and sponsorships, and included in the onboard CAs.

System Services - Start, stop, and restart servers, view or download log files, manage server certificates, manage SSH, open a support tunnel, and manage SMS and email services.

System Updates - View and manage the Cloudpath build versions.

Replication - Configure two or more servers for replication. Cloudpath supports replication between two servers, for multiple data centers, and redundant servers.

Data Cleanup - Manage database cleanup thresholds for enrollment records, abandoned certificates, vouchers, notifications, manage wizard versions, and other system events.

Firewall Requirements - Displays inbound and outbound traffic from Cloudpath to assist with firewall configuration.

Backup and Recovery

Incremental backups can be performed from the primary server to a mounted CIFS drive using the command line interface from the configuration utility.

- Scheduled backup - Use the **maintenance backup schedule** command to copy the database via SCP or mounted drive.
- Restore backup - Use the **maintenance backup restore** command to copy the backup file and overwrite the existing database.

See the full Command Reference at the end of this document for more information.

How to Export the Database to a File

As a backup, you can export the Cloudpath ES database to a remote server. The export process dumps the Cloudpath ES database to a zipped tar.gz file, with a time-stamp, and transfers it using SCP to a remote server.

To export the database, log into the service account and enter this command from the configuration utility:

```
# maintenance backup create [IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system]
```

For example:

```
# maintenance backup create 172.16.4.20 22 username / home/db/file
```

How to Import the Database From An Existing System

The import database command can be used for recovery or for upgrading the system.

1. On your existing system, shut down the web service for your deployment URL to temporarily discontinue new enrollments. Use this command from the Linux shell:

```
[ServiceAccount@AccountName ~]$ sudo /sbin/service httpd stop
```

2. Log into the system with the new OVA (via SSH or vCenter console) and import the database from the existing system.
3. Use the following command from the new system configuration utility:

```
# maintenance cannibalize [IP address or hostname of existing system]
```

For example:

```
# maintenance cannibalize 172.16.4.20
```

Note >>
The new system must use the same SSH port that is configured in the old system to transfer database files.

You must restart the server after you import the database.

Snapshots

In this guide we refer to snapshots as one version of the different aspects of the system. There are two kinds of snapshots that you need to become familiar with:

- Configuration snapshots, which are snapshots of the Cloudpath workflow configuration.
- VMware snapshots, which preserves the state and data of a virtual machine at a specific point in time.

Configuration Snapshots

A configuration snapshot is a version of a workflow configuration. You can create and maintain multiple versions of each configuration. However, only one snapshot can be active at a time for each deployment location.

Create a configuration snapshot from the Cloudpath Admin UI, *Configuration > Workflow, Snapshots tab* and click the Publish button.

Note >>
Each time the workflow configuration changes, you must create another workflow snapshot.

VM Maintenance

Cloudpath supports both VMware and Hyper-V deployments. See the appropriate section below for tips on VM maintenance.

VMware Maintenance

VMware Snapshots

How to Increase the Virtual Appliance Memory on VMware

How to Expand the MySQL Partition Size

VMware Snapshots

A VMware snapshot is a version of a VM at a specific point in time. As a best practice, we recommend that you take a VM snapshot of your deployment before making any changes to the system.

As a best practice, you should create regular VMware snapshots In clustered environments, create a snapshot of at least one of the servers. We also recommend creating VMware snapshots before making any changes to the system (particularly before and after upgrades).

To create a VMware snapshot:

1. From the virtualization software client (VMware vSphere Client), select your virtual image, right click and select *Snapshot > Take Snapshot*.
2. Enter the *Name* and *Description* of the snapshot. Provide enough details in the *Description* so that other administrators can understand what is in each snapshot.
3. Select *Snapshot machine's virtual memory*.
4. (Optional) If VMware Tools is installed, you can also select *Quiesce guest file system* to pause running processes before you take a snapshot.

How to Increase the Virtual Appliance Memory on VMware

Use these instructions to change the memory configuration of a virtual machine's hardware. The VM must be powered off to edit memory settings.

1. From the vCenter client, power off the virtual appliance.
2. Select the VM, and right-click to *Edit Settings*.
3. With the *Hardware* tab selected, select *Memory*.
4. On the right window pane, increase the *Memory Size*.
5. Click *OK*.
6. Power on and reboot the VM.

How to Expand the MySQL Partition Size

Use these instructions to expand size of the partition used for MySQL database operations.

From the vCenter Client

1. With the VM running, select the VM and right-click to *Edit Settings*.
2. With the *Hardware* tab selected, select *Hard disk 2*.
3. On the right pane, in the *Disk Provisioning* section, increase the *Provisioned Size* to the desired size and click *OK*. If the *Provisioned Size* cannot be selected, try restarting the server using the ***sudo halt*** command.

Hyper-V Maintenance

Hyper-V Checkpoints

How to Increase the VM memory on Hyper-V

Hyper-V Checkpoints

A Hyper-V checkpoint is a version of a VM at a specific point in time. As a best practice, we recommend that you create a VM checkpoint of your deployment before making any changes to the system.

As a best practice, you should create regular checkpoints In clustered environments, create a checkpoint of at least one of the servers. We also recommend creating checkpoints before making any changes to the system (particularly before and after upgrades).

To create a Hyper-V checkpoint:

1. From the Hyper-V Manager, select your virtual machine, right click and select *Checkpoint*.
2. The Hyper-V Manager creates a checkpoint with the current timestamp.
3. Use the bottom right menu to rename, export, or revert checkpoints.

How to Increase the VM memory on Hyper-V

Use these instructions to change the memory configuration of a virtual machine's hardware. The VM must be powered off to edit memory settings.

1. From the Hyper-V Manager, select your virtual machine, right click and select *Settings*.
2. Select *Memory* from the *Hardware* section on the left pane.
3. Increase the RAM, as needed.
4. Click *OK*.
5. Power on and reboot the VM.

Upgrades

Note >>
Under normal conditions, upgrades are not a part of daily operations. Please contact the network administrator or the Cloudpath support team before attempting to upgrade your system.

Upgrade for Local Deployment

Note >>
Certain upgrades, such as those with major operating system changes, require a database import instead of a System Update. Refer to the release notes for your upgrade version for instructions.

There are two methods for upgrading your Cloudpath ES virtual appliance.

1. Update your existing system from the ES Admin UI (*Administration > System Updates).*
2. Set up a virtual appliance using the new OVA and import the database from the existing system. Refer to How to Import the Database From An Existing System.

Managing Replication

Note >>
All operations must be administered from the primary server(s).

Replication States

Use the *Replication Status* page to monitor the health of the servers in the cluster. When configured in a cluster, each server can be in one of several states:

- Not Setup - The ES server has not been configured for replication.
- Running - Replication has been set up and is currently running.
- Stopped - Replication has been configured but the replication service is not running.
- Starting:Synchronizing - The ES server was previously stopped or disabled and is in the process of synchronizing with the master server.
- Offline:Normal - The server is configured for replication, but has been disabled.
- Offline:Error - The server is in an error state and will try to correct the issue. This can take 5 to 10 minutes. If the server is unable to resolve the issue, replication should be disabled for troubleshooting.

Enable or Disable Server

You can enable or disable replication for individual servers or remove the replication configuration completely.

Disabling a Server in the Cluster

If you disable a server in the cluster, this leaves all the replication functionality in place but stops the database updates between the server nodes. When you re-enable, the nodes process the database changes and eventually all servers are back in sync.

Disable is often used for troubleshooting individual server issues, and is required prior to upgrading the system. To enable or disable replication for a server, navigate to *Administration > System > Replication* and toggle the green *Enabled* icon.

The Admin UI displays the replication *Status* as *Stopped* and the *Enabled* icon clear, to indicate that replication has been disabled.

Remove Cluster

To make topology changes, such as adding another server, or replacing an inoperable server in the cluster, you must take down the cluster configuration and rebuild it with the new servers.

How to Remove the Cluster Configuration

When you remove a cluster, Cloudpath deletes all of the replication functionality, but leaves the database in the current state.

Use *Remove Cluster* to add new servers to the cluster. You must remove the cluster from all devices and install replication again on the new servers. To remove a cluster configuration, navigate to *Administration > Replication* and click *Remove Cluster* in the *Maintenance* section.

Upgrading Replicated Systems

You must disable the replication service to upgrade your system. Upgrade each server separately before you re-enable replication for the cluster.

Depending on your network environment and the number of servers in your cluster, this might take some time. The script that updates the database due to an upgrade, and then re-syncs the databases in the cluster, may require more than one pass to complete this process on all servers in the cluster.

Restart RADIUS Server

You might be required to start the onboard RADIUS servers after replication is set up. The onboard RADIUS server on the master server, or hub should remain in a running state, but the server nodes, or slaves, may not start unless restarted from the Admin UI or from a console.

Troubleshooting Replication Issues

This section describes issues to consider when testing or troubleshooting Cloudpath ES servers that have been configured for replication.

Enable/Disable Replication

If replication is configured but does not appear to be working, try disabling and re-enabling individual servers from the *Administration > Replication* page.

DNS

Verify that DNS is properly configured with the FQDN on all hosts.

Hostname

The replication configuration in the Cloudpath ES is set up using the FQDN for each system. If you are running replication, changing the FQDN from the command line interface causes replication to become inoperable.

Check OCSP

Cloudpath provides a check status URL to allow a load balancer to query the status of the OCSP responder. Use the format *http://<Cloudpathhostname>/ocsp/ping*. The return status should be a *Success* message.

For negative testing, use *http://<Cloudpathhostname>/ocsp/pingFail*. The return status is a 404 message.

Web Server Certificates

If you are using a load balancer, the system displays a message when you log in that the URL is a mismatch with the server certificate. You can suppress this message by putting the load balancer URL in *Administrative > Company Info > Vanity URL*.

Firewall Settings

Go to *Administration > Firewall Requirements* to ensure that your firewall ports have been correctly configured for replication.

Replication ports are only provided when replication is configured and running.

Replication Commands

The replication commands are designed for members of the support team to use for troubleshooting. Customers would typically not be required to run these commands unless requested by the support team.

See the full Command Reference at the end of this document for more information about replication commands.

Reports

Records Export

Enrollment and User data can be can be downloaded, as a CSV file or Microsoft Excel spreadsheet.

Use the CSV Export icon or XLS Export icon located at the bottom of any table in the Dashboard.

The Enrollment and User export files are designed to be a quick view of the activity since midnight. To export only certain items in the table, for a specific date and time, or to export items for a longer time period, see Scheduled Reports.

Scheduled Reports

The scheduled report feature allows you to schedule a task to export enrollment record data, by date, or schedule a recurring export. For example, you might schedule an enrollment data report to occur on a weekly, or daily basis. This report can be emailed to one or multiple email addresses.

You can schedule multiple reports. For example, you can create a report that emails an enrollment record report based on enrollments with revoked certificates, and another based on issued certificates.

To schedule a task, go to *Dashboard > Notifications > Scheduled Reports*. The enrollment record data is emailed, as a CSV file, to the specified address, at the scheduled frequency. You can also download an interim report from this page.

Support

Documentation

Refer to the *Support > Documentation* page in the Cloudpath Admin UI for documentation and links that cover all aspects of the system, from setup to configuration and system administration.

Support Tunnel

The Support Tunnel component allows you to open a support tunnel to help you in diagnosing issues with your application or configuration. If requested by a Support Team member, you might be required to enable a support tunnel from the *Administration > System Services > Support Tunnel* page.

Support File

If support has provided a support file, you can upload it from the *Support > Upload Support File* page. This will make changes to the system, so be sure to create a VMware snapshot first.

Password Recovery

If you are locked out of the ES Admin UI, you can log in via SSH and use the **support activate-ui-recovery** command from the service account. This activates a temporary password for a short time period to allow you to log into the ES Admin UI and set up a new Administrator account, or reset a password for an existing account.

If you are locked out of the service account, you can log in via SSH to a *Recovery* account. However, you must contact Cloudpath Networks *Support* to obtain a recovery password.

To receive a recovery password for the service account, you must provide the Cloudpath Support team with the *System Identifier* and current *Version* on your system.

How To Find Your System Identifier

1. Log into the ES Admin UI.
2. Go to *Support > Licensing > Advanced* link in the License Server section.
3. The *System Identifier* is listed on the *Administrative Console Linkage* section.

How To Find Your Current ES Version

1. Go to *Administration* > *System Services* > *Web Server* service.
2. The current build is listed in the *Version* field.

Command Reference

config commands

The **config** commands allow you to change the configuration of the system.

TABLE 3. **config commands**

Command	Description	Parameters and Examples
config	From the Linux shell, this command provides access to the command line configuration utility.	No parameters. `[<serviceacctlogin@<hostname>]$ config`
config admin-access allow-all	Clears restrictions to the administrative functionality so that an administrator can access the Cloudpath Admin UI from any IP address.	No parameters. `config admin-access allow-all`

config admin-access restrict	Restricts which IP addresses have administrative access to the Cloudpath Admin UI.	[Comma separated list of IP addresses/CIDR]
		`config admin-access restrict 172.16.4.20, 172.16.5.18`
		`or`
		`config admin-access restrict 172.16.4.20/24`

config fips-crypto	Enable or disable use of FIPS 140-2 cryptography.	[Enable or Disable] [Requires the service password]
		`# config fips-crypto enable`
		`[sudo] password for cpn_service: enterservicepwd`

config fips-crypto state	Display whether FIPS 140-2 cryptography is enabled.	No parameters. `config fips-crypto state`

TABLE 3. **config commands**

Command	Description	Parameters and Examples
config hostname-restricted restrict	Requests that do not match the hostname are blocked.	No parameters `config hostname-restricted restrict`
config https enable	Sets whether the Apache server should be run as HTTP or HTTPS.	[The HTTPs port to use] `config https enable 55`
config https disable	Sets whether the Apache server should be run as HTTP or HTTPS.	No parameters `config https disable`
config https-servername default	Uses the system's hostname (FQDN).	No parameters `config https-servername default`
config https-servername override	Set the HTTPS server name. This is typically used when operating behind a load balancer.	[This system's network name] `config https-servername test22.company.net`
config network DHCP	Configures whether you want DHCP to assign network IP addresses.	[*true* to use DHCP, *false* to use STATIC IP addresses] `config network DHCP true` This command causes the system to toggle the eth0 and loopback interfaces.
config network restart	Restarts the network after making configuration changes to DHCP settings.	No parameters. `config network restart`
config network STATIC dns	Configures the STATIC IP addresses for the DNS server.	[IP address of the DNS server] `config network STATIC dns 172.16.4.202`
config network STATIC ip	Configures the STATIC IP addresses for the system's eth0 interface, subnet mask, and gateway.	[IP address, subnet mask, and gateway for the eth0 interface] `config network STATIC ip 172.16.6.35 255.255.252.0 172.16.4.1`
config ntp	Sets the NTP server	[IP address of the NTP server] `config ntp 172.16.2.106`

TABLE 3. **config commands**

Command	Description	Parameters and Examples
config ntp sync-now	Forces an ntpdate to the configured NTP server.	[hostname for shared db] `config ntp sync-now`
config proxy set	Sets the HTTP proxy. Requires a reboot. The HTTP port and HTTPS port must be the same. This is the port number for the HTTP proxy tunnel. The [proxy-bypass-hosts] parameter (optional) is a comma-separated list of hosts that should bypass the proxy. Use *config clear-proxy* to remove the configuration.	[HTTP hostname] [HTTP port] [HTTPS hostname] [HTTPS port] [proxy-bypass-hosts] `config proxy hostA 80 hostB 80 hostC,hostD`
config proxy remove	Removes the HTTP proxy	No parameters `config proxy remove`

config ssh enable	Enables SSH access. The default port is 8022, or you can select port 22.	[SSH port]
		`config ssh enable`
		`or`
		`config ssh enable 22`

config ssh disable	Disables SSH access.	[SSH port] `config ssh disable`
config sslv3 allow	Permits SSLv3 protocol on HTTPS connections.	No parmaters `config sslv3 allow`

TABLE 3. **config commands**

Command	Description	Parameters and Examples
config sslv3 block	Prevents SSLv3 protocol on HTTPS connections.	No parameters `config sslv3 block`

config timezone	Sets the timezone to be used.	[Zone name]
		`config timezone`
		This command displays a list of acceptable timezones.
		When prompted, enter the desired timezone as shown.
		`America/Denver`
		Alternately, you can enter the correct timezone as part of the command.
		`config timezone America/Denver`

console command

TABLE 4. **console command**

Command	Description
console	Provides access to the Linux shell (command line).

diag commands

The **diag** commands provide diagnostic tests for network connectivity.

TABLE 5. **diag commands**

Command	Description	Parameters and Examples
diag arp-table	Displays arp table.	No parameters. `diag arp-table`
diag dns-lookup	Performs a DNS lookup.	[IP address of the host to resolve] `diag dns-lookup 172.16.4.64`
diag interfaces	Displays network interfaces.	No parameters. `diag interfaces`
diag ping	Sends ICMP IPv4 messages to network hosts.	[IP address of the host] `diag ping 172.16.2.1`

TABLE 5. **diag commands**

Command	Description	Parameters and Examples
diag routing-table	Displays routing table.	No parameters. `diag routing-table`
diag rpm-version	Displays the current version for the rpms.	No parameters. `diag rpm-version`
diag schema-version	Displays the status of database updates	No parameters. `diag schema-version`

maintenance commands

The **maintenance** commands import or export the Cloudpath database.

TABLE 6. **maintenance commands**

Command	Description	Parameters and Examples
maintenance backup create	Create a backup file (zipped tar.gz) of the Cloudpath database and SCP it to a remote server.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] `maintenance backup create 172.16.4.20 22 username /home/db/file`
maintenance backup restore mount	Restore a backup from a locally mounted drive	No parameters. `maintenance backup restore mount`
maintenance backup restore scp	Restore a backup file from a remote server via SCP.	[IP address or hostname of the remote server] [Port number] [Remote username] [Path to file location on the remote system] `maintenance backup restore scp 172.16.4.20 22 username /home/db/file`

TABLE 6. **maintenance commands**

Command	Description	Parameters and Examples

maintenance backup schedule mount	Creates a recurring backup via a locally mounted drive.
	Note the different syntax examples for cifs and nfs drive types.
		[Username for remote drive] [Path to mount] [Path within mount to backup directory] [Type of drive (cifs or nfs)] [true to merge changes into full backup, false to not merge]
		`Syntax for cifs:`
		`# maintenance backup schedule mount admin \\\\\\172.128.4.20\\backup\\test servername-cifs cifs true`
		`Syntax for nfs:`
		`# maintenance backup schedule mount '' 172.128.4.20:/backup/ servername-nfs nfs true`

maintenance backup schedule scp	Creates a recurring backup via SCP to a remote server	[IP address or hostname of the remote server] [Remote port number] [Remote username] [Path to the remote system to place the backup file] [Pattern for the cron schedule] `maintenance backup schedule scp 172.16.4.20 22 username /path/to /file 0 0 * * 3` (Note the space between minute, hour, day, month schedule parameters.) For more information about cron schedule parameters, refer to Linux documentation.
maintenance backup unschedule mount	Removes the previously set up cron job for copying the system database to a remote server via mounted (CIFS) drive.	No parameters. `maintenance backup unschedule mount`

TABLE 6. **maintenance commands**

Command	Description	Parameters and Examples
maintenance backup unschedule scp	Removes the previously set up cron job for copying the system database to a remote server via SCP.	No parameters. `maintenance backup unscheduled scp`
maintenance cannibalize	Extract the configuration from a remote system and overwrite this system. The new system must have the same network settings as the old system, from which the database was exported. The Cloudpath uses the SSH port configured in the new system to transfer the database files.	[IP address or hostname of the remote server] `maintenance cannibalize 172.16.4.20`

replication commands

The replication commands are designed for members of the support team to use for troubleshooting. Customers would typically not be required to run these commands unless requested by the support team.

> **Note >>**
> In most cases, gathering log data through the Cloudpath Admin UI, *Collect Replication Logs* button, is sufficient for troubleshooting purposes.

TABLE 7. **replication commands**

Command	Description	Parameters and Examples
replication force-cleanup	Forces the removal of the replication setup.	No parameters. `replication force-cleanup`

replication replicator	Perform an operation on the replication server.	[start][stop][restart][status][offline][online]
		`replication replicator restart`
		`or`
		`replication replicator status`

replication show-cluster	Displays the state of the cluster.	No parameters. `replication show-cluster`

TABLE 7. **replication commands**

Command	Description	Parameters and Examples
replication show-log	Show log.	No parameters. `replication show-log`

replication trepctl	Performs an operation on a service (ex. alpha, bravo, charlie).	[FQDN of the server node][service name][status/online/offline]
		`replication trepctl test23.company.net alpha status`
		`or`
		`replication trepctl test23.company.net bravo offline`

replication validate-cluster	Displays whether replication can be set up on this server. **Note:** This command should only be used before replication is set up.	No parameters. `replication validate-cluster`

show commands

The **show** commands display the current configuration.

TABLE 8. **show commands**

Command	Description
show config	Shows currently operating configuration.
show date	Shows current date.
show logs	Shows application and server logs.
show logs apache-access	Shows contents of Apache server access logs.
show logs apache-error	Shows contents of Apache server error logs.
show logs application	Shows contents of JBoss logs.
show logs config	Shows contents of config log.
show proxy	Shows HTTP proxy information.
show timezone	Shows currently configured timezone.

support commands

The **support** commands enable or disable the support tunnel.

TABLE 9. **support commands**

Command	Description
support activate-ui-recovery	Activates a temporary password, which allows you to log into the Cloudpath Admin UI with the *recovery* username. This command requires the *service* password. The recovery user credentials are only valid for 5 minutes.
support database login	Allows you to log into the database. The password for this command is only available to support staff.
support database reset-schema	Resets the status of the last database schema version.
support database schema-version	Lists the database schema version.
support database shrink	Depending on the size of the database, this operation may take some time to complete.
support database view-size	Displays the amount of data n the database.
support https restore certificate	Resets HTTPS to self-signed certificate.
support https restore ciphers-and-protocols	Resets https to default SSL ciphers and protocol.
support support-tunnel enable	Start support tunnel on port 8022.
support support-tunnel disable	Stop support tunnel.
support system apply-patches	Applies patches for the current version. The system will reboot.
support system benchmark	Perform CPU and disk IO tests.
support system clean-disk	The Cloudpath runs a clean-disk script on a schedule. This command allows an administrator to clean up the jboss.log manually.

system commands

The **system** commands control system operations

Note >>
If the boot password requirement has been set, you must enter a password to complete these commands.

TABLE 10. **system commands**

Command	Description
system reboot	Reboots system.
system restart	Restarts the JBoss and Apache servers.
system shutdown	Shuts down the system. This command requires VMware access to boot the system.
system status	Lists the status of key services (web server, firewall, NTP, RADIUS, etc.)