Cloudpath

XpressConnect Enrollment System

How to Set Up Clustering With Enrollment System Servers

Software Release 4.2

December 2015

Summary: This document describes the different topologies supported when clustering Enrollment System servers, how to prepare your system, how to configure clustering using the ES Admin UI, and how to monitor the status of the replication.
Document Type: Configuration
Audience: Network Administrator

How to Set Up Clustering With XpressConnect Enrollment System Servers

Software Release 4.2

December 2015

How to Set Up Clustering With Enrollment System Servers

In addition to VMware-based high availability, the Enrollment System supports replication (native clustering) capabilities. Clustering provides high-availability and high-scalability using two or more servers with all servers being available for active use.

Replication Topologies

The ES supports replication between two servers, or between servers in a star pattern. Replication between two servers allows two master servers to replicate with both servers being available for active use. Replication in a star pattern allows 3 or more servers to replicate, with all servers being available for active use.

When using replication in ES, the data is pushed from one server to the other server(s).

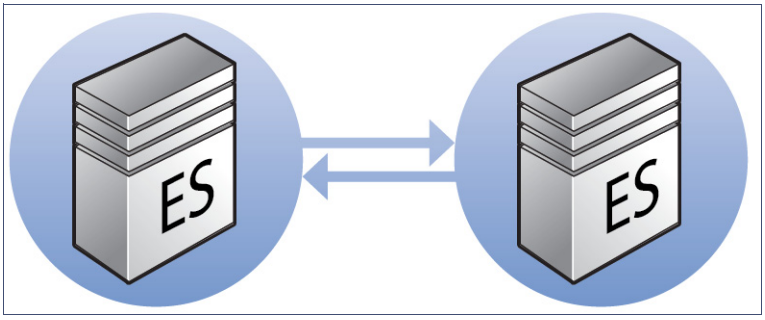
- With the two-server configuration, the data is pushed from the server from which replication is configured to the second server.
- With the star-pattern configuration, the data is pushed from the hub server (the server from which replication is configured) to the other server nodes.

In both configurations, all nodes are active and the database is synchronized to all nodes. The ES does not support an active-passive configuration.

Two-Server Topology

The two-server configuration is a master-master configuration, where the servers continuously replicate and both servers are available for active use, such as a live backup. A two-server configuration is useful when you have two sites and have active enrollments running on both sites simultaneously.

FIGURE 1. Master-Master Configuration

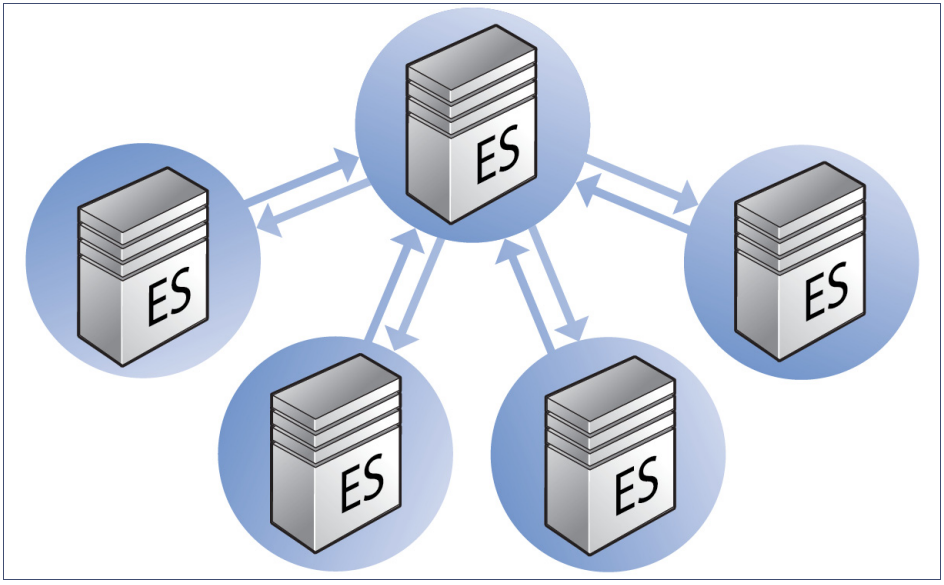


Star Topology

A star pattern is useful when you want information shared between multiple data servers through a central hub. This allows information to be replicated to a central host and then replicated back out to the other server nodes. In a multi-site configuration the star pattern can be used to concentrate information at head office, while allowing the different locations and sites to also have a copy of all the data.

The star pattern is suitable for environments with a higher load, or where you need redundancy. We recommend using 3 servers, with two set up for load balancing and the third as the hub. Although the hub server can be used for enrollments, we suggest using it primarily for backup. With the star topology, the hub is the master server, and the database is copied from the master to the other server nodes (slaves).

FIGURE 2. Star Pattern Configuration



If the hub server becomes inoperable, replication stops, but the server nodes continue to onboard users. If a slave becomes inoperable, the hub and remaining servers continue to function normally.

Prerequisites

To configure replication, set up 2 or more ES virtual appliances with the same OVA. When configuring these virtual appliances, all application and network properties must be the same for all servers in the cluster.

Note >>
For replication setup, all hosts must be able to communicate with all other nodes. However, after replication setup is complete, you can restrict communications, if needed. For replicated servers to continually sync, the hub must be able to access each server node, but each server node needs access only to the hub.

Each server must have a unique *FQDN Hostname* and network *IP address.* The DNS servers and gateway need not be the same as long as there is network connectivity between the servers. However, all server nodes must use the same SSH port as the hub.

Note >>
When using replication, the *FQDN Hostname* of your system cannot change.

Firewall Requirements

The ES Admin UI provides a table that lists the inbound and outbound traffic of your Enrollment System. This information is dynamically generated based on the current system configuration and can changes as the system configuration is modified.

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

Test Connectivity

Be configuring replication, be sure that each system can resolve DNS and that each virtual appliance can communicate with the other server nodes to be replicated.

Check OCSP

The ES provides a check status URL to allow a load balancer to query the status of the OCSP responder.

Note >>
This check is supported using **HTTP** only.

Use the format *http://<ES hostname>/ocsp/ping*. For example, enter *http://test22.company.com/ocsp/ping*. The return status should be a *Success* message.

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

Configuring Replication

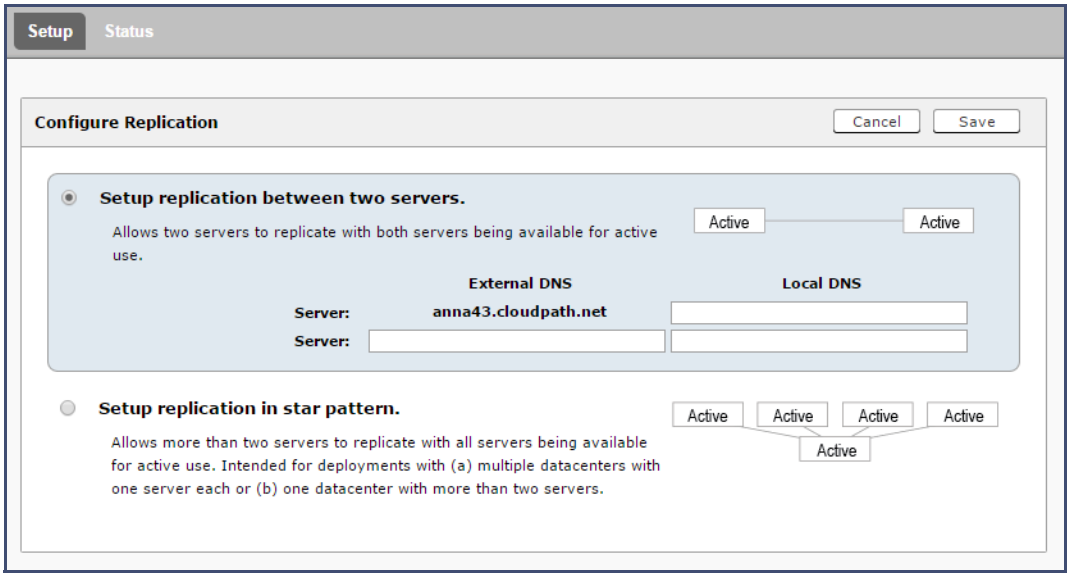
This section describes how to configure replication using the ES Admin UI.

Replication Setup

Choose one VMware server as the Master node. This is the server from which you set up replication in the ES Admin UI.

1. Go to *Administration* > *System* > *Replication*.
2. Click the *Edit* icon.
3. Select the replication pattern. See Replication Topologies for information about which topology to choose.

FIGURE 3. Configure Replication



4. Enter the *External Server DNS* for the nodes. This is the *FQDN Hostname* of the ES server configured in the initial system setup.

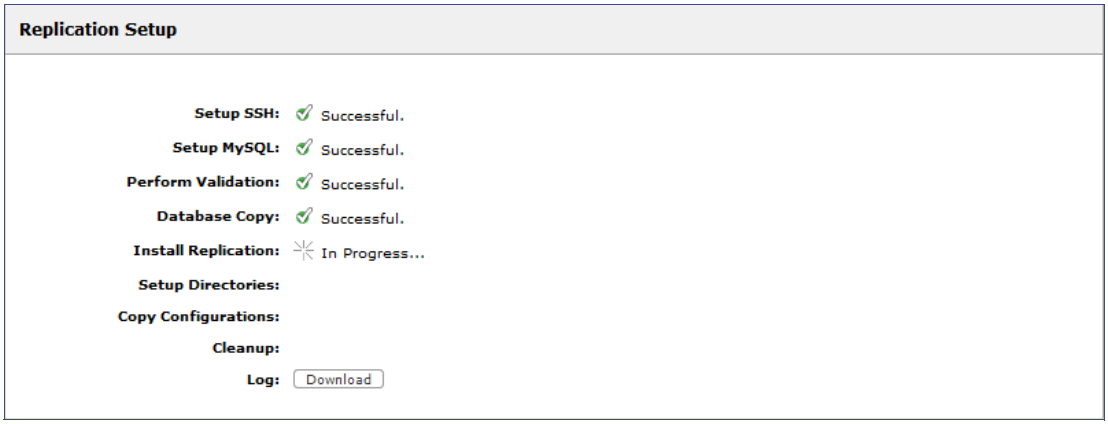
> **Note >>**
> If your environment is set up for Network Address Translation (NAT) behind a firewall, enter both the *External* and *Internal DNS* hostnames for the ES servers in the cluster.

5. Click *Save*.

The Enrollment System saves the data from the server node from which replication was configured, then copies the database to the other server nodes. This can take a while, depending on the number of server nodes and the size of the database.

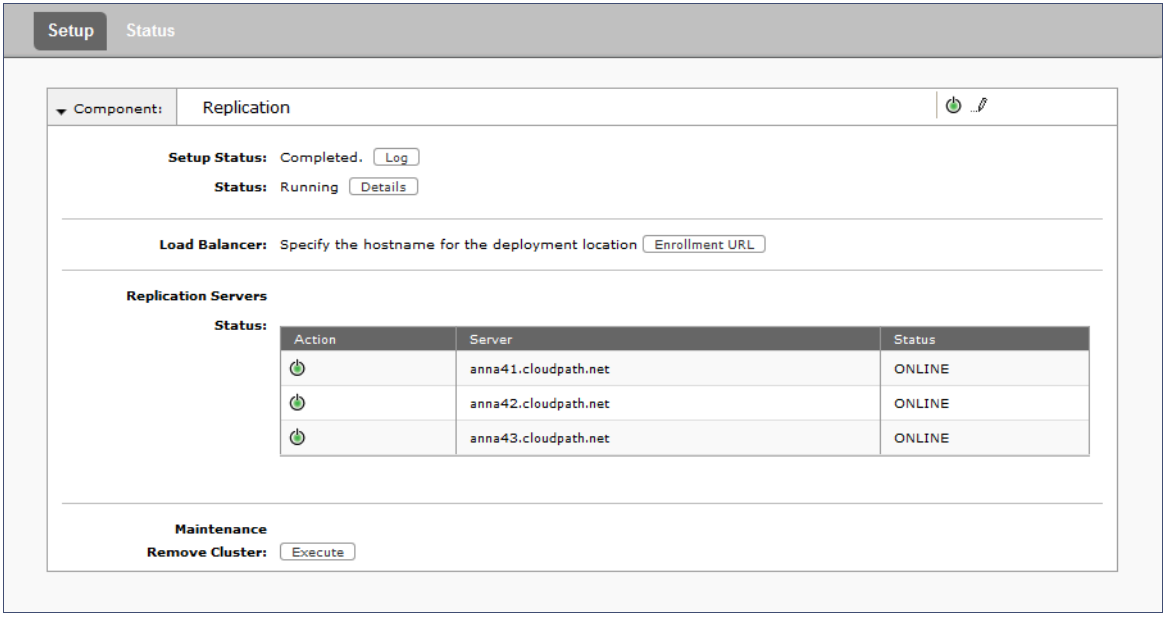
The *Replication Setup* page displays the progress of the operation.

FIGURE 4. Replication In-Progress



When all processes are complete and display a *Success* status, click *Next* to return to the replication *Setup* page. The *Setup Status* should be in the *Completed* state and the *Status* in the *Running* state. The ES provides a log file for the replication setup process.

FIGURE 5. Replication Enabled and Running



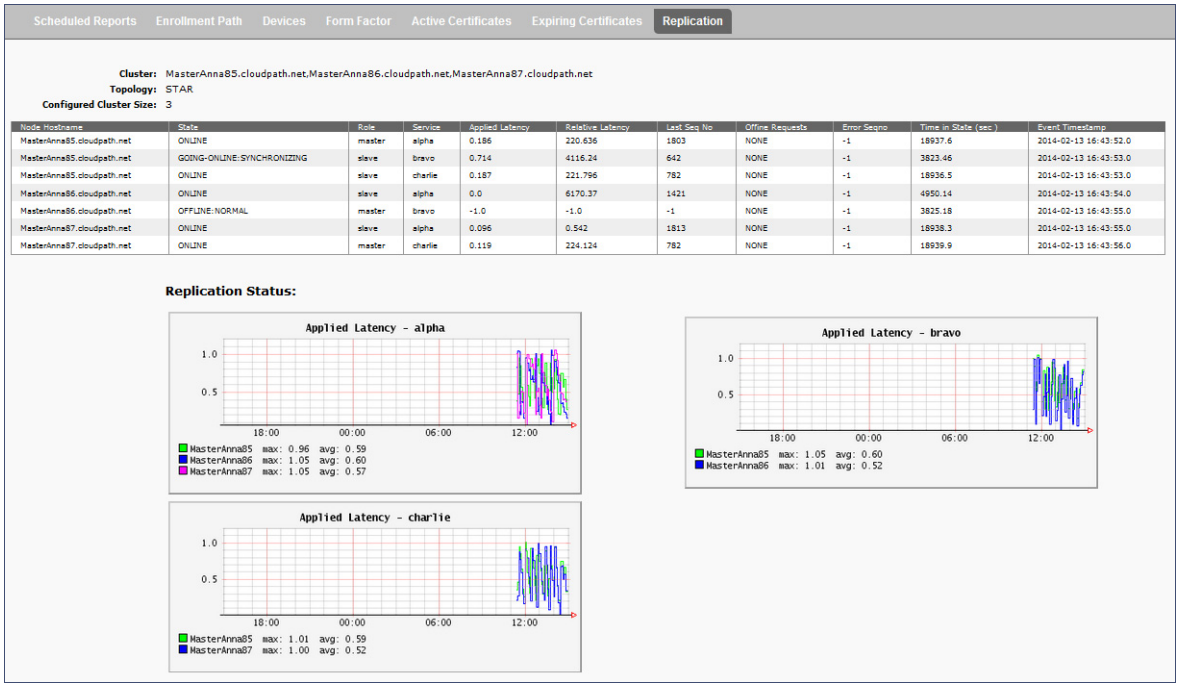
The *Replication Servers* table lists all servers in the cluster. After setup, all servers should be *Enabled* (green icon) and *ONLINE*. Click the *Details* button to view the replication *Status* page.

The *Collect Replication Logs* button is typically used for troubleshooting. This gathers the necessary log information and saves it to a tar.gz file. This file can be sent to the support team upon request.

Replication Status

The *Replication Status* page (*Administration* > *System* > *Replication* > *Status*) displays the state of each server in the cluster and the applied latency.

FIGURE 6. Replication Status



When replication is running, you can make configuration changes on the ES Admin UI and the other nodes stay in sync with one another. Enrollments can be managed by any server in the cluster and all servers in the cluster maintain the enrollment records for all servers in the cluster.

Managing the Cluster

Use the Replication Status to monitor the health of the ES servers in the cluster.

Replication States

With replication, an Enrollment System 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 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 disable replication for a server:

1. Go to *Administration* > *System* > *Replication* and toggle the green *Enabled* icon.
2. Confirm that you want to disable replication.

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

> **Note >>**
> After re-enabling replication, it takes a few minutes for the *Replication Status* page to show that all servers are back *Online*.

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, the ES 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:

1. Go to *Administration* > *System* > *Replication* and click *Remove Cluster* in the *Maintenance* section.

2. Confirm that you want to uninstall replication.

FIGURE 7. Remove Cluster Confirmation

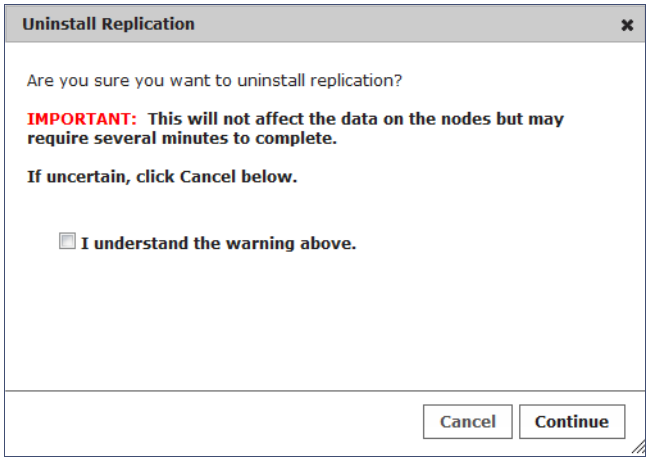


FIGURE 8. You are returned to the *Replication Setup* page.

Upgrading Replicated Systems

Upgrades

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.

> **Note >>**
> Refer to the release notes or upgrade instructions for details about upgrading to a specific version.

Troubleshooting Replication

This section describes issues to consider when testing or troubleshooting Enrollment System 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* > *System* > *Replication* page.

DNS

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

Hostname

The replication configuration in the Enrollment System 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.

Load Balancer Enrollment URL

If you are using a load balancer with your replication setup, the *Deployment Location Enrollment URL* must contain the hostname of the load balancer, and not the Enrollment System virtual appliance.

1. On the *Replication Setup* page, in the *Load Balancer* section, click *Enrollment URL*.
2. On *Deployment Locations* page, expand the *Deployment Location*, and click *Change*.
3. On the *Modify Enrollment URL* page, enter the hostname of the load balancer in the first (hostname) field.

> **Note >>**
> If you are not using a load balancer, the deployment URL for the master server becomes the deployment URL for all servers in the cluster.

Check OCSP

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

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

Web Server Certificates

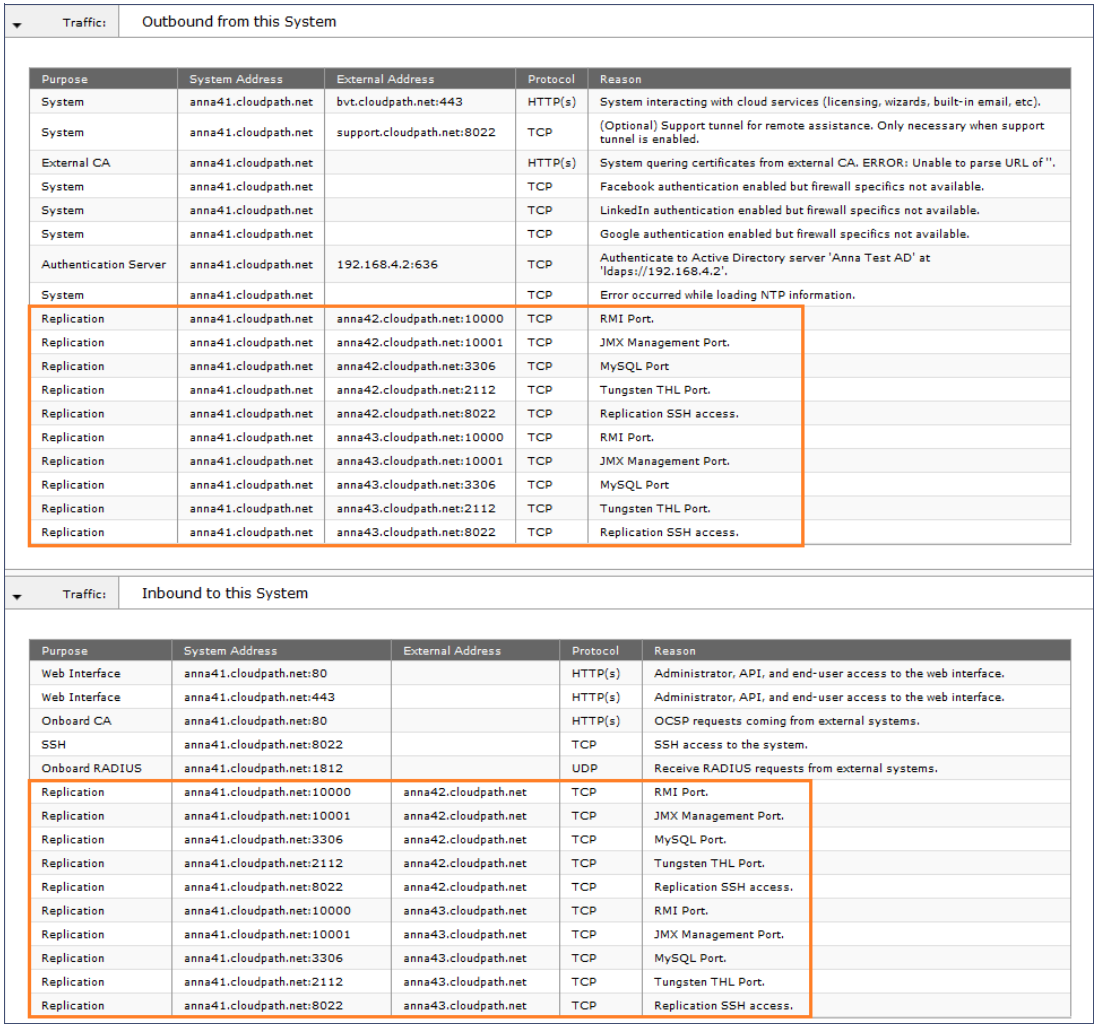
If you are using a load balancer, the system displays a message when you log in that the URL is a mismatch with the server certificate. You can suppress this message by putting the load balancer URL in *Administrative-* > *Company Info* > *Vanity URL*.

Firewall Settings

The ES Admin UI provides a table that lists the inbound and outbound traffic of your Enrollment System. This information is dynamically generated based on the current system configuration and can changes as the system configuration is modified.

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

FIGURE 9. Firewall Requirements



Traffic: Outbound from this System

Purpose	System Address	External Address	Protocol	Reason
System	anna41.cloudpath.net	bvt.cloudpath.net:443	HTTP(s)	System interacting with cloud services (licensing, wizards, built-in email, etc).
System	anna41.cloudpath.net	support.cloudpath.net:8022	TCP	(Optional) Support tunnel for remote assistance. Only necessary when support tunnel is enabled.
External CA	anna41.cloudpath.net		HTTP(s)	System quering certificates from external CA. ERROR: Unable to parse URL of ''.
System	anna41.cloudpath.net		TCP	Facebook authentication enabled but firewall specifics not available.
System	anna41.cloudpath.net		TCP	LinkedIn authentication enabled but firewall specifics not available.
System	anna41.cloudpath.net		TCP	Google authentication enabled but firewall specifics not available.
Authentication Server	anna41.cloudpath.net	192.168.4.2:636	TCP	Authenticate to Active Directory server 'Anna Test AD' at 'ldaps://192.168.4.2'.
System	anna41.cloudpath.net		TCP	Error occurred while loading NTP information.
Replication	anna41.cloudpath.net	anna42.cloudpath.net:10000	TCP	RMI Port.
Replication	anna41.cloudpath.net	anna42.cloudpath.net:10001	TCP	JMX Management Port.
Replication	anna41.cloudpath.net	anna42.cloudpath.net:3306	TCP	MySQL Port
Replication	anna41.cloudpath.net	anna42.cloudpath.net:2112	TCP	Tungsten THL Port.
Replication	anna41.cloudpath.net	anna42.cloudpath.net:8022	TCP	Replication SSH access.
Replication	anna41.cloudpath.net	anna43.cloudpath.net:10000	TCP	RMI Port.
Replication	anna41.cloudpath.net	anna43.cloudpath.net:10001	TCP	JMX Management Port.
Replication	anna41.cloudpath.net	anna43.cloudpath.net:3306	TCP	MySQL Port
Replication	anna41.cloudpath.net	anna43.cloudpath.net:2112	TCP	Tungsten THL Port.
Replication	anna41.cloudpath.net	anna43.cloudpath.net:8022	TCP	Replication SSH access.

Traffic: Inbound to this System

Purpose	System Address	External Address	Protocol	Reason
Web Interface	anna41.cloudpath.net:80		HTTP(s)	Administrator, API, and end-user access to the web interface.
Web Interface	anna41.cloudpath.net:443		HTTP(s)	Administrator, API, and end-user access to the web interface.
Onboard CA	anna41.cloudpath.net:80		HTTP(s)	OCSP requests coming from external systems.
SSH	anna41.cloudpath.net:8022		TCP	SSH access to the system.
Onboard RADIUS	anna41.cloudpath.net:1812		UDP	Receive RADIUS requests from external systems.
Replication	anna41.cloudpath.net:10000	anna42.cloudpath.net	TCP	RMI Port.
Replication	anna41.cloudpath.net:10001	anna42.cloudpath.net	TCP	JMX Management Port.
Replication	anna41.cloudpath.net:3306	anna42.cloudpath.net	TCP	MySQL Port.
Replication	anna41.cloudpath.net:2112	anna42.cloudpath.net	TCP	Tungsten THL Port.
Replication	anna41.cloudpath.net:8022	anna42.cloudpath.net	TCP	Replication SSH access.
Replication	anna41.cloudpath.net:10000	anna43.cloudpath.net	TCP	RMI Port.
Replication	anna41.cloudpath.net:10001	anna43.cloudpath.net	TCP	JMX Management Port.
Replication	anna41.cloudpath.net:3306	anna43.cloudpath.net	TCP	MySQL Port.
Replication	anna41.cloudpath.net:2112	anna43.cloudpath.net	TCP	Tungsten THL Port.
Replication	anna41.cloudpath.net:8022	anna43.cloudpath.net	TCP	Replication SSH access.

Replication ports are 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.

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

Replication commands are run from the command-line configuration utility prompt (**#**).

> **Tip >>**
> From the command-line configuration utility, enter the `console` command to access the Linux shell. From the Linux shell, enter the `config` command to access the command-line configuration utility.

TABLE 1. 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`
replication show-log	Show log.	No parameters. `#replication show-log`

TABLE 1. **replication commands**

Command	Description	Parameters and Examples

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`

Additional Documentation

You can find detailed information in the Enrollment System configuration guides, located on the left-menu *Support* tab of the ES Admin UI.

About Cloudpath

Cloudpath Networks, Inc. provides software solutions and services that simplify the adoption of standards-based security, including WPA2-Enterprise and 802.1X, in diverse BYOD environments. Our goal is to make secure as simple as insecure; simple for network administrators to deploy and simple for users to access.

To learn more about the XpressConnect Enrollment System and how it can simplify your wireless environment, visit www.cloudpath.net or contact a Cloudpath representative.

If you need technical assistance, discover a bug, or have other technical questions, email support at support@cloudpath.net.

Contact Information

General Inquiries:info@cloudpath.net

Support:support@cloudpath.net

Sales:sales@cloudpath.net

Media:media@cloudpath.net

Marketing:marketing@cloudpath.net

Phone:+1 303.647.1495 (US)

+1 866.472.6053 (US)
+44 (01) 161.261.1400 (UK)
Fax:+1 760.462.4569
Address:1120 W 122nd Ave, Suite 302
Westminster, CO 80234 USA