Pulse One Appliance Getting Started Guide

Supporting Pulse One Appliance 2.0.1903.1

Product Release	**2.0.1903.1**
Published	**11 December 2019**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

https://www.pulsesecure.net

© 2019 Pulse Secure, LLC. All rights reserved.Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States.

All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Pulse One Appliance Getting Started Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Contents

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Preface

Document Conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text Formatting Conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command Syntax Conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

© 2019 Pulse Secure, LLC.

Convention	Description
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION

An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION

A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit **https://support.pulsesecure.net/product-service-policies/**

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: **https://support.pulsesecure.net**
- Search for known bugs: **https://support.pulsesecure.net**
- Find product documentation: **https://www.pulsesecure.net/techpubs**
- Download the latest versions of software and review release notes: **https://support.pulsesecure.net**

© 2019 Pulse Secure, LLC.

- Open a case online in the CSC Case Management tool: **https://support.pulsesecure.net**
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: **https://support.pulsesecure.net**

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: **https://kb.pulsesecure.net**
- Ask questions and find solutions at the Pulse Community online forum: **https://community.pulsesecure.net**

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at **https://support.pulsesecure.net**.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see **https://support.pulsesecure.net/support/support-contacts/**

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Introduction

Pulse One Overview

Pulse One is a management platform that provides unified management and troubleshooting for Pulse Connect Secure (PCS) and Pulse Policy Secure (PPS).

Note: If you want to use Pulse One to configure and use Software Defined Perimeter (SDP), refer to the *Software Defined Perimeter* documentation.

Pulse One provisioning is a two-step process:

1. Bring the appliance online.
2. Upgrade the appliance to a current version.

The following steps outline the installation process:

1. Ensure prerequisites are available, which include:
    - Networking – The appliance needs an external IP address.
    - DNS – DNS is used when creating SSL certificates.
    - SSL certificates – a Certificate Signing Request (CSR) can be created during installation if required.
    - Outbound Ports - Ports must be open to make outbound calls to Apple and Google.
2. Use the CLI interface to configure the network settings.

    Note: This manual describes the use of command line interface (CLI) commands. Where equivalent methods exist to perform tasks in the Pulse One graphical user interface, these are described in the Pulse One Appliance Administration Guide.
3. Activate the device with the provisioning CLI command.
4. Download the most recent version and upgrade.
5. Activate Pulse Workspace using the licensing keys.

© 2019 Pulse Secure, LLC.

Pulse One and Software Defined Perimeter (SDP)

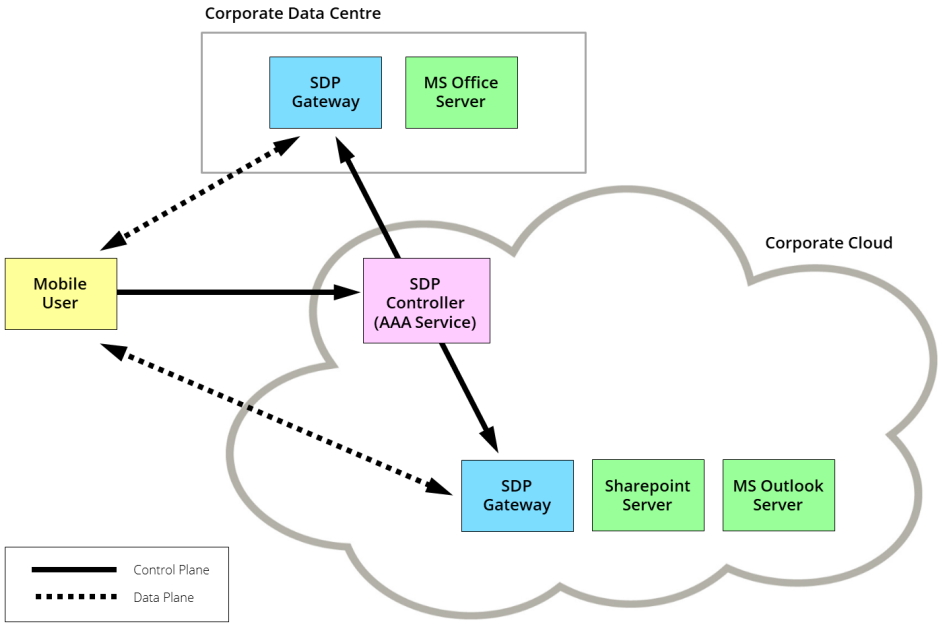
Traditional network-based security (Network Defined Perimeter) architectures use firewalls on the network perimeter to limit access to public IP addresses. This exposes the network to a variety of network-based attacks.

Connectivity in a Software Defined Perimeter (SDP) system is based on a need-to-know model, in which mobile devices are verified and authorized before access to application infrastructure is granted. Application infrastructure cannot be detected remotely, and has no visible DNS information or exposed IP addresses. This protects networked resources from many common network-based attacks.

Pulse Secure SDP uses PCS appliances which individually act as either an SDP controller or an SDP gateway. Mobile users of the Pulse Secure Client perform authentication on an SDP controller which runs an Authentication, Authorization and Accounting (AAA) Service. The SDP controller then enables direct communication between the user and the SDP gateways that protect the user's authorized resources, and enables requested encryption. This does not require the general exposure of public IP addresses. It also separates the control plane and the data plane.

Pulse Secure SDP supports a number of network topologies, and can include both cloud-based and data center-based resources. For example:

FIGURE 1 Software Defined Perimeter Example



Note: For full details of the installation and configuration of SDP, see the *Software Defined Perimeter* documentation.

© 2019 Pulse Secure, LLC.

Pulse One Appliance Architecture

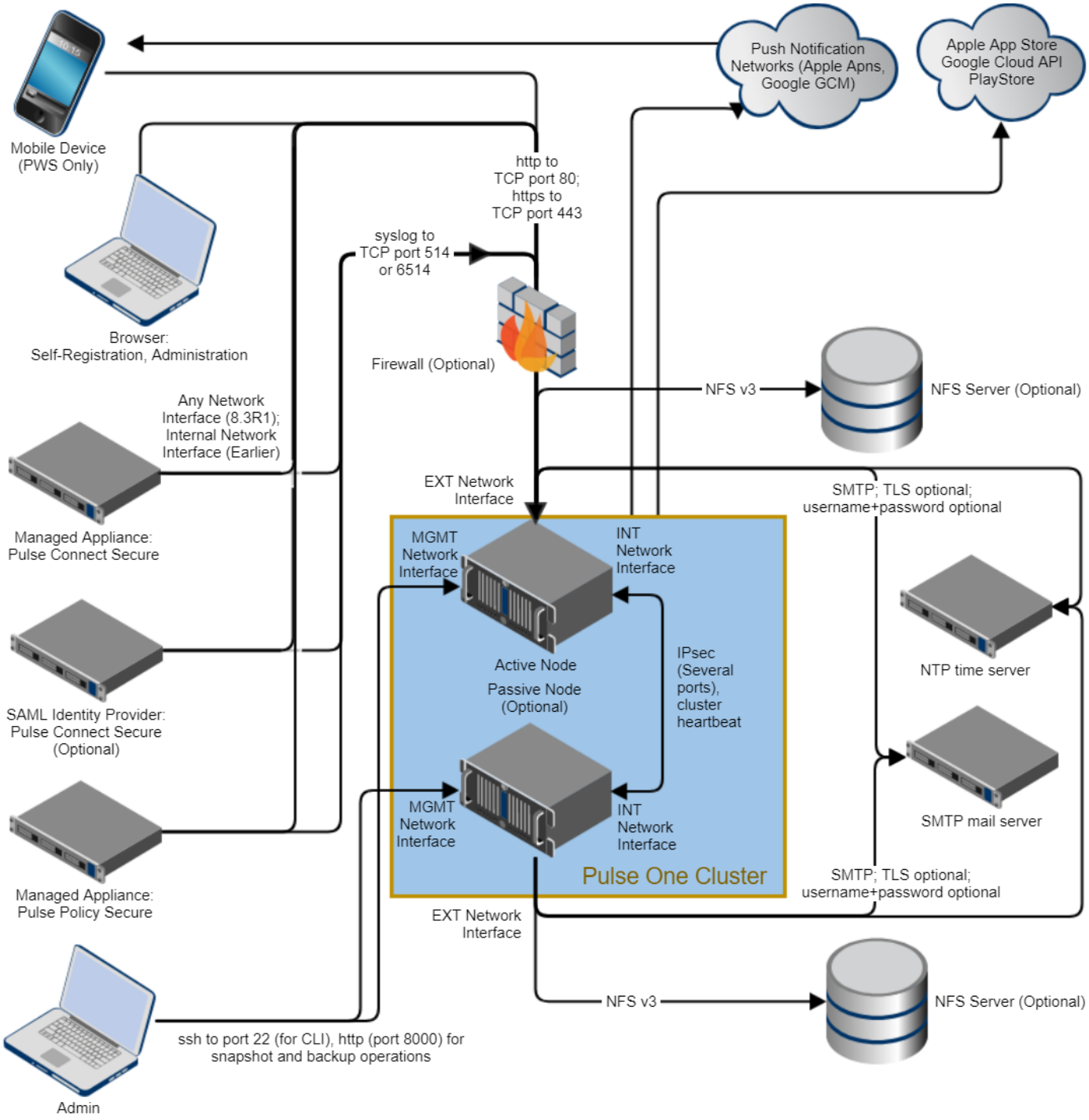
Overview

Pulse Workspace is part of the Pulse One runtime environment, but it has a unique networking and security profile due to its communication with the mobile devices.

The following diagram shows a completely equipped Pulse Secure implementation that includes Pulse One with Workspace (appliance edition). Workspace initiates conversations with mobile devices by sending a "phone home" notification to the devices. Every primary mobile vendor (Apple, Google, Microsoft) has their own proprietary push notification network. The firewall settings must be checked to ensure that the outbound ports and endpoints noted below are not blocked.

© 2019 Pulse Secure, LLC.

FIGURE 2 Pulse One Appliance Architecture



Note: This diagram includes Pulse Workspace operations.

Note: This diagram does not include information for a Software Defined Perimeter implementation. If you want to use Pulse One to configure and use Software Defined Perimeter (SDP), refer to the *Software Defined Perimeter* documentation.

© 2019 Pulse Secure, LLC.

Pulse One/Workspace uses several ports when communicating. Firewalls must be configured to support calls on these ports. In addition to push notifications, Pulse Workspace makes calls to both Apple and Google application stores. These are standard HTTPS web-service calls with no authentication. Pulse Workspace calls these to lookup application searches performed in the Pulse Workspace admin UI. Pulse Workspace also calls the Google EMM Cloud API which requires authenticated access.

Note: To configure a pair of Pulse One appliances to operate as an Active/Passive cluster, refer to **"Configuring an Active/Passive Cluster" on page 45**.

Outbound Ports

Pulse One/Workspace uses the following outbound ports when communicating.

Endpoint	Ports	Authentication	Comments
APNS	2195	Certificate, Token	Port 2195 is used when PWS calls Apple's APNS for sending push notifications to iOS devices. Apple also mentions ports 2196, 5223, and 443: • 2196, which is the Feedback Service, is not used. • 5223 and 443 are ports used by iOS devices when communicating with Apple. Two levels of authentication: • PWS server to APNS cloud uses Pulse push certificate. • Device specific token. See **https://support.apple.com/en-us/HT203609**
GCM	5228 5229 5230	Token	Google mentions 5228 is the primary port while 5229 and 5230 are secondary ports. Pulse Workspace sends notifications to Android devices using GCM notifications.
Apple App Store	443	None	Standard HTTPS call on **https://itunes.apple.com/search** and **https://itunes.apple.com/lookup**. The iTunes API is unauthenticated.
Google Play Store	443	Token	Standard HTTPS call on **https://www.googleapis.com/customsearch/v1**. The Google custom search engine API requires an API key which is not necessarily associated with any particular other credential (ESA/MSA).
Google EMM Cloud API	443	443	Standard HTTPS call on **https://www.googleapis.com/auth/androidenterprise**.

© 2019 Pulse Secure, LLC.

Inbound Ports

Pulse One/Workspace uses the following inbound ports when communicating.

Endpoint	Ports	Authentication	Comments
Browser / Admin UI	443	Password / HAWK	Password is used to initiate a session. The browser client then uses its session to upgrade to HAWK credentials.
PCS/PPS	443	HAWK	
Apple iOS MDM agent	443	Device Cert	Inbound MDM requests are signed with the device certificate, which is verified by the server.
Pulse iOS PWS client	443	OTP/SAML then HAWK	Once the user authenticates with OTP or SAML, the server generates HAWK credentials for the client.
Pulse iOS VPN client			Does not connect to PWS servers. Connects only to VPN servers.
Android Work client			Does not connect to PWS servers. Connects only to Google.
Android Pulse DPC client	443	OTP/SAML then HAWK	Once the user authenticates with OTP or SAML, the server generates HAWK credentials for the client.
	80	n/a	HTTP access. Incoming traffic on this port is automatically redirected to port 443 over HTTPS.
	22	Username / Password	Admin access via SSH to MGMT interface.
	514	No authentication	514 is syslog without authentication/encryption. **Note:** Pulse Secure advises that you always enable TLS (see below) to use port 6514 with authentication and encryption.
	6514	Certificate	6514 is syslog over TLS. **Note:** Pulse Secure advises that you always enable TLS to ensure authentication and encryption.

© 2019 Pulse Secure, LLC.

Installing Pulse One

Introduction

The Pulse One appliance requires its Command Line Interface (CLI) for initial management and configuration.

Note: If you want to install Pulse One as an SDP controller, refer to the *Software Defined Perimeter* documentation.

Note: You must ensure that each of the three Pulse One interfaces (internal, external and management) are set to different subnets.

Note: See the *Pulse One Command Reference Guide* for full details of individual commands.

Installing Pulse One

To install Pulse One, perform the following processes:

Note: If you want to install Pulse One as an SDP controller, refer to the *Software Defined Perimeter* documentation.

Note: You must ensure that each of the three Pulse One interfaces (internal, external and management) are set to different subnets.

1. Reserve an IP address and a fully-qualified domain name (FQDN) for your appliance's external interface.

   For example, *10.64.22.22* and *p1.example.com*.

2. Configure your DNS infrastructure so that the FQDN resolves to the IP address.

3. Choose a Certificate Authority (CA) to create the Pulse One Appliance's certificate.

   Ideally, the CA should be trusted by both browsers and PCS / PPS appliances. To identify the CAs that are trusted by PCS, log into a PCS appliance and navigate to **Configuration > Certificates > Trusted Server CAs**. The same process can be used for PPS.

4. Install an SSH client (if not already present) on your computer:

   - Linux generally includes an SSH client; enter **ssh** at the shell prompt.
   - OSX generally includes an SSH client; start the terminal application and enter **ssh**.
   - Windows 10 generally includes an SSH client; open a command prompt and enter **ssh**.

© 2019 Pulse Secure, LLC.

5. Connect to the appliance's management interface using an SSH client. If SSH is not possible, you can connect to the serial port using Telnet.

   You are prompted for an initial admin username and password.

6. Enter the required information.

   You are logged into the CLI automatically.

7. Create a locksmith user account, in case the initial account's credentials are lost. At the Pulse One prompt:

   ```
   account create locksmith
   ```

   You are prompted for a password for the new user.

   Note: Pulse Secure strongly recommends storing the password securely.

8. Configure the management network interface to use a static IP address rather than DHCP:

   ```
   network interface management --ip <ip_address> --netmask <netmask>
   --gateway <gateway_address>
   ```

9. Configure the external network interface:

   ```
   network interface external --ip <ip_address> --netmask <netmask>
   --gateway <gateway_address>
   ```

   For example:

   ```
   network interface external --ip 10.64.22.22 --netmask 255.255.0.0
   --gateway 10.64.0.1
   ```

   The netmask and gateway must be correct for the subnet.

10. Configure the DNS servers:

    ```
    network dns --primary <ip_address> --secondary <ip_address>
    ```

    The secondary IP address is optional but recommended. For example:

    ```
    network dns --primary 10.64.0.10 --secondary 8.8.8.8
    ```

11. Review your network settings:

    ```
    network show
    ```

    Correct any settings as required.

© 2019 Pulse Secure, LLC.

12. Configure the Simple Mail Transfer Protocol (SMTP) settings. The general syntax is:

```
smtp set --sender <from_email> --server <server_address>
[--port <port_number>] [--username <username> --password] [--tls]
```

Note: Pulse Secure advises that you always enable TLS to ensure the use of authentication and encryption.

- If your SMTP server does not require a username and password, these can be omitted. For example:

```
smtp set --sender p1@example.com --server smtp.example.com
```

- If your SMTP server requires a username and password, include these options on the command line, and enter the password when prompted. For example:

```
smtp set --sender p1@example.com --server smtp.example.com
--username USERNAME --password
```

- If your SMTP server requires encrypted (TLS) connections, also include the *–tls* option:

```
smtp set --sender p1@example.com --server smtp.example.com
--username USERNAME --password –tls
```

Note: For details of the **smtp set** command's other options, refer to the *Pulse One Command Reference*.

13. Configure the Network Time Protocol (NTP) settings:

```
ntp server <ntp server address> --enable
```

For example:

```
ntp server 10.64.72.72 --enable
```

14. Add license keys:

```
licenses add <license key>
```

Note: This step can be done at this time or later.

15. Provision the Pulse One appliance:

```
system provision <pulse_one_FQDN_lower_case> --admin-username <username>
--admin-email <email >
```

The admin username is for logging into the web UI, and can be different from the username for logging into the CLI. For example:

```
system provision p1.example.com --admin-username jsmith
--admin-email jsmith@example.com
```

You are prompted for a password. Pulse Secure recommends a strong password.

© 2019 Pulse Secure, LLC.

Note: This step creates a temporary, self-signed certificate. This allows you to connect to the web UI, though you will receive a certificate warning. If you use a private CA, browsers will also present certificate warnings. Certificate warnings indicate risk, so it is usually better to use a public CA.

16. Generate a Certificate Signing Request (CSR):

    ```
    https csr
    ```

    The CSR is displayed.

17. Select and copy the CSR.
18. In a browser, navigate to your chosen CA, and when prompted for a CSR, paste in the CSR.
19. Obtain from the CA:
    - The root certificate or (if available) the certificate bundle (chain).
    - The certificate issued for your appliance.
20. Enter the root certificate or certificate bundle:

    ```
    https set ca-bundle
    ```

    When prompted, paste in the root certificate or bundle.

21. Enter the certificate issued for your appliance:

    ```
    https set cert
    ```

    When prompted, paste in the certificate issued for your appliance.

22. If you want encryption to be enabled for log collection:

    ```
    log-aggregator settings –tls
    ```

    Note: Pulse Secure advises that you always enable TLS to ensure the use of authentication and encryption.

23. Restart the services to pick up all new settings:

    ```
    services restart
    ```

24. Browse to the /admin path on your appliance's FQDN. For example, browse to

    ```
    https://p1.example.com/admin
    ```

    Your browser should not display a certificate warning.

25. Log into your appliance using your UI username and password.

The Pulse One Appliance is now ready to manage PCS and PPS appliances.

Note: Further steps are required to prepare Pulse One to manage workspaces, or to create a Pulse One cluster.

© 2019 Pulse Secure, LLC.

Configuring Static IP Routes

You can configure static IP routes on Pulse One as required. These enable you to:

- Route traffic to services that Pulse One depends on over a chosen network interface.
- Integrate Pulse One successfully into your network.

If required, you can define one or more static routes for your network using the following CLI commands:

- **network ip route add**. This command adds a static route to the table of static routes.

  The general syntax is:

  ```
  network ip route add <network> via <gateway> dev <interface>
  ```

  Where:

  - <*network*> is the IP address and optional /CIDR formatted netmask.
  - (Optional) <*gateway*> is the IP address of the gateway.
  - <*interface*> is the required Pulse One interface. This can be *internal*, *external* or *management*.

- **network ip route delete**. This command removes a static route from the table of static routes using its <*network*> setting. The general syntax is:

  ```
  network ip route delete <network>
  ```

- **network ip route show**. This command displays the table of static routes, including <network>, <gateway> and <interface> settings. The general format for the table is shown below:

  ```
  routes:
  - gateway: xx.xx.xx.xx
  interface: management
  network: yy.yy.yy.yy/nn
  - gateway: bb.bb.bb.bb
  interface: management
  network: aa.aa.aa.aa/nn
  ```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Configuring Google or Android for Work

Introduction

After the Pulse One Appliance is installed and configured, you can configure Google or Android for Work (AFW) services.

To do this, the domain properties and the Enterprise Service Account (ESA) must be set up. This can be performed:

- Using the Pulse One graphical user interface (see the *Pulse One Appliance Administration Guide* for full details).
- Using CLI Commands, as described in **"Configuring Android For Work Using the CLI" on page 17**.

  Note: See the *Pulse One Command Reference* for full details of individual commands.

Configuring Android For Work Using the CLI

The following commands are used to enter the Google Android identifiers provided with licensing by Pulse Secure.

- To set up AFW enterprise ID, type the following command:

  ```
  p1 domain property set afw_enterprise_id <your_licensed_Google_enterprise_id>
  ```

- To set up AFW domain admin user, type the following command:

  ```
  p1 domain property set afw_domain_admin_user <your_licensed_Google_admin_user>
  ```

- To identify the type of account (either *afw* or *google*), type the following command:

  ```
  p1 domain property set afw_enterprise_type <account_type>
  ```

  Note: Note: Set this to *afw* unless instructed otherwise.

- Check the current value of all domain properties by performing the following command:

  ```
  p1 domain property list
  ```

© 2019 Pulse Secure, LLC.

- To add Google ESA (Enterprise Service Account) credentials provided by Pulse Secure, type the following command:

  ```
  pws config set esa
  ```

  When prompted, copy and paste the ESA credentials.

After these configuration changes, perform a restart to use new settings:

```
services restart
```


© 2019 Pulse Secure, LLC.

Managing Services

Introduction

This chapter describes the service management commands that are supported by the Pulse One CLI.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Viewing Service Status

To view the status of all services, type the following command at the CLI prompt:

```
services status
```

Example output for this command is shown below:

```
   Name       State
------------------
api           Up
backbeat      Up
backend       Up
backend       Up
backend       Up
cache         Up
cellsecrpc    Up
console       Up
data-store    Up
file-store    Up
index         Up
portal        Up
proxy         Up
pws-api       Up
ui-assets     Up
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Starting Services

To start Pulse One services, type the following command at the CLI prompt:

```
services start
```

Example output for this command is shown below:

```
Starting with version "1902"...
Started.
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Viewing Service Logs

To view a list of all service logs, type the following command at the CLI prompt:

```
services logs
```

Example output for this command is shown below:

```
Attaching to api_1, backend_1, backend_2, backend_3, backend_4, backend_5,
   backend_6, backend_7, backend_8, cellsecrpc_1, console_1, file-store_1,
   portal_1, proxy_1, pws-api_1, ui-assets_1
pws-api_1     | spawned uWSGI worker 3 (pid: 16, cores: 1)
pws-api_1     | spawned uWSGI worker 4 (pid: 17, cores: 1)
pws-api_1     | spawned uWSGI worker 5 (pid: 18, cores: 1)
   .
   .(messages)
   .
ui-assets_1   | Starting nginx with CORS origin * (.*)
ui-assets_1   | Starting nginx with CORS origin * (.*)
```

Note: This command supports additional options, see the *Pulse One Command Reference Guide* for full details.

Restarting Services

You can restart one specific service or all services.

To restart all services, type the following command at the CLI prompt:

```
services restart
```

Example output for this command is shown below:

```
Restarting...
Starting with version "1902"...
Started.
Restarted.
```


© 2019 Pulse Secure, LLC.

To restart one or more specific services, type the following command at the CLI prompt:

```
services restart <space-separated list of services>
```

For example, to restart the cache, console and index services:

```
services restart cache console index
Restarting "index, cache, console"...
Restarting uno_console_1 ... done
Restarting uno_cache_1 ... done
Restarting uno_index_1 ... done
Restarted.
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Stopping Services

To stop all services, type the following command at the CLI prompt:

```
services stop
```

Example output for this command is shown below:

```
services stop
Stopping...
Stopping uno_log-collector_1 ... done
Stopping uno_api_1 ... done
Stopping uno_pws-api_1 ... done
Stopping uno_backbeat_1 ... done
Stopping uno_file-api_1 ... done
Stopping uno_cellsecrpc_1 ... done
Stopping uno_portal_1 ... done
Stopping uno_proxy_1 ... done
Stopping uno_log-indexer_1 ... done
Stopping uno_file-store_1 ... done
Stopping uno_backend_3 ... done
Stopping uno_backend_4 ... done
Stopping uno_backend_2 ... done
Stopping uno_backend_1 ... done
Stopping uno_console_1 ... done
Stopping uno_ui-assets_1 ... done
Stopping uno_cache_1 ... done
Stopping uno_index_1 ... done
Stopping uno_data-store_1 ... done
Stopped.
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Working with Backup and Restore

Introduction

The backup feature provides the means to export the following information for backup purposes:

- Pulse One configuration. For example, provisioning configuration values, certs, registered PCS/PPS devices, and so on.
- Pulse One data. For example, search indices, distributed FS data, and so on.

A backup file can be used to restore a configuration to Pulse One.

Please note that:

- It is recommended that you only back up the Active node of a cluster. Backup and restore of a Passive appliance in a cluster is not recommended because the provisioning and associated appliance information cannot be retrieved from a Passive appliance. This is because the cluster needs to be reformed.
- The appliance should be offline before backing up. If the appliance is online, run the services stop command to switch the appliance to offline.
- The backup requires an “external” network interface to be configured.
- The following activities are not supported at this release:
    - Incremental backup.
    - Selective backup.
    - Backup to NFS.
    - Backup encryption.
    - Backup of data stored outside the appliance.
- Importing is limited to the same system version of source and target. For example, a backup archive of v2.0.1901 can only be used to restore to another v2.0.1901 appliance.
- Do not run the system provision command before importing. If the system provision command is run before importing, all Pulse Connect Secure and Pulse Policy Secure appliances may become unregistered.

© 2019 Pulse Secure, LLC.

Creating a Backup File for a Pulse One Configuration

To back up Pulse One config and data files on the appliance:

1. At the CLI command prompt, type the following command:

   ```
   system backup export
   ```

   A message appears:

   ```
   Services will be stopped before initiating backup. Continue? [y/N]:
   ```

2. At the confirmation prompt, type *y* and press *Enter*.

   The following message categories are displayed as the process continues:

   - All services are stopped.
   - The backup starts.
   - The backup files are compiled.

   A following message appears:

   ```
   Download ready at http://xx.xx.xx.xx:8000/backup/download
   MD5: 10e3f47281a8a5c494df8dca7d3c5ddd
   Press Ctrl-C when finished.
   ```

   Note: Do not press *Ctrl-C* at this point.

3. In a browser, access the URL and download the backup file to an accessible location.
4. After the download completes, close the browser.
5. At the CLI command prompt, press *Ctrl-C*.

   The backup process completes. The backup files on the appliance are deleted.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Restoring a Pulse One Configuration from a Backup File

To restore the backup file:

1. At the CLI command prompt, type the following command:

   ```
   system backup import
   ```

   Note: Do not run the system provision command before importing. If this is done, all Pulse Connect Secure and Pulse Policy Secure appliances may become unregistered.

   A message appears:

   ```
   Upload your backup archive here:
   URL: http://xx.xx.xx.xx:8000/backup
   Press Ctrl-C when finished.
   ```

   Note: Do not press *Ctrl-C* at this point.

2. In a browser, access the URL and upload the backup.
3. After the upload completes, close the browser.
4. At the CLI command prompt, press *Ctrl-C*.

   The restore process continues:

   ```
   WARNING: This will replace all Pulse One data and configuration restoring the
   appliance from backup. The data and configuration will not be recoverable.
   Type "DESTROY" to continue:
   ```

5. At the prompt, type *DESTROY*, and press *Enter*.

   The following message categories are displayed as the process continues:

   - All data and configurations are destroyed.
   - All services restart.
   - The backup is restored.
   - The backup file is deleted from the appliance.

   When the import completes, the node is restarted.

   ```
   Restarting system to complete restore.
   You can connect to SSH at xx.xx.xx.xx:22
   Press <ENTER> to log in to Pulse One
   ```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Restoring a Cluster of Pulse One Appliances from a Backup File

To restore the configuration of a two-node Active/Passive cluster:

1. Restore the appliance configuration onto the appliance you want to be Active.
2. Demote the Passive node of the cluster and reboot the appliance.
3. Demote the now-restored Active node of the cluster and reboot the appliance.
4. Ensure the internal interfaces of the clusters are configured correctly.
5. Regenerate the cluster.

© 2019 Pulse Secure, LLC.

Configuring FIPS Mode

Introduction

Federal Information Processing Standard (FIPS) set of standards define security requirements for products that implement cryptographic modules used to secure sensitive but unclassified information.

This chapter describes the FIPS security commands that are supported by the Pulse One CLI.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Viewing FIPS Mode Status

To view the FIPS mode status, type the following command at the CLI prompt:

```
system security show
```

Example output for this command is shown below:

```
FIPS Mode: false
Version: Pulse One version 2.0
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Enabling FIPS Mode

To enable FIPS mode:

1. At the CLI command prompt, type the following command:

   ```
   system security fips --enable
   ```

   The following messages appear:

   ```
   Enabling FIPS mode will stop all services and log you out.
   Continue? [y/N]: y
   ```

2. Confirm by typing *Y* and *Enter* to continue.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Disabling FIPS mode

To disable FIPS mode:

1. At the CLI command prompt, type the following command:

   ```
   system security fips --disable
   ```

   The following messages appear:

   ```
   Enabling FIPS mode will stop all services and log you out.
   Continue? [y/N]: y
   ```

2. Confirm by typing *Y* and *Enter* to continue.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Managing CLI Admin Accounts

Introduction

You can provide additional CLI admin accounts using the Pulse One CLI.

Note: In an Active/Passive cluster of Pulse One nodes, account creation, change, deletion should be done on the Active node. Account changes are replicated automatically to the Passive node.

Listing Admin Accounts

To list all the admin accounts, type the following command at the CLI prompt:

```
account list
```

Example output for this command is shown below:

```
users:
- admin
- jsmith
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Creating an Admin Account

To create a new admin account, type the following command at the CLI prompt:

```
account create <new_account_name>
```

Example output for this command is shown below:

```
account create demo
Password:
Confirm Password:
Created user demo
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Changing an Admin Password

To change the admin password, type the following command at the CLI prompt:

```
account password change
```

Example output for this command is shown below:

```
Current password:
Password:
Confirm Password:
```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Resetting an Admin Password

To reset the admin password:

1. At the CLI command prompt, type the following command:

   ```
   account password reset
   ```

   Example output for this command is shown below:

   ```
   Enter the user whose password needs to be reset: demo
   ```

2. Change or accept the user name, and type RESET to confirm the user name. For example:

   ```
   Enter the user whose password needs to be reset: demo
   Type RESET to confirm: RESET
   Temporary password for user 'demo'
   N3yXa6Jb
   ```

   During your next login, you must change the password.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Deleting an Admin Account

To delete an admin account:

1. At the CLI command prompt, type the following command:

   ```
   account delete <account_name>
   ```

2. Type DELETE to confirm the deletion. For example:

   ```
   account delete demo
   Type DELETE to confirm: DELETE
   User 'demo' deleted.
   ```

See the Pulse One Command Reference Guide for full details of individual commands.

© 2019 Pulse Secure, LLC.

Configuring Pulse One as a Syslog Server

Configuring a Pulse One Appliance as a Syslog Server

To set up Pulse One appliance as a syslog server, perform the following procedure:

1. Log into Pulse One appliance.
2. List all installed licenses to determine if a log aggregator license is present.

   ```
   licenses show
   ```

   The output of this command should contain an entry with a log type of appliances.log_aggregator. For example:

   ```
   - created: '2018-06-21T13:28:5Z7'
     type: unity.appliances.log_aggregator
   ```

3. (Optional) Add a log aggregator license if none is present. Use the following command:

   ```
   license add
   ```

See the *Pulse One Command Reference Guide* for full details of individual commands.

Configuring Individual PCS/PPS Appliances

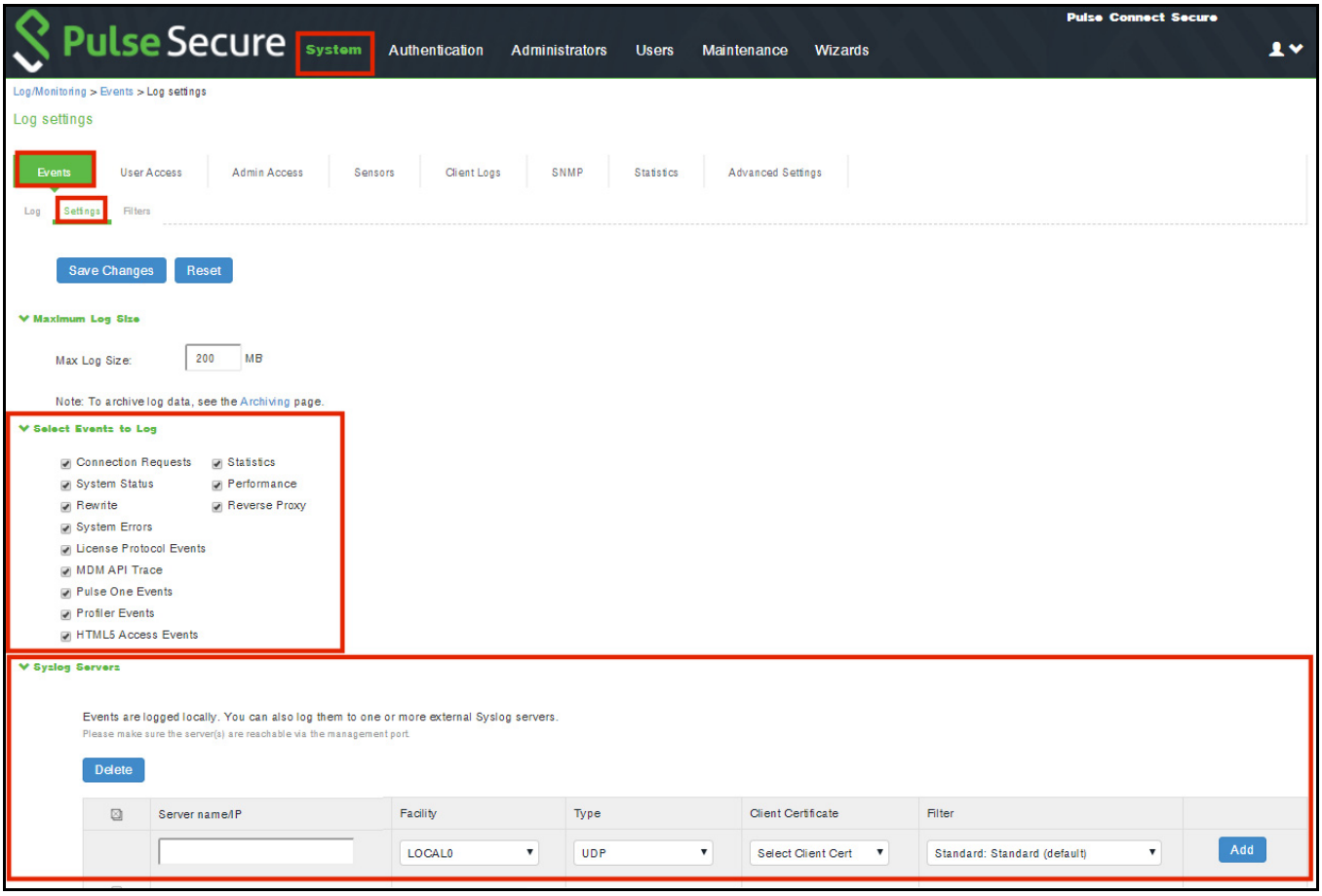
After you have configured Pulse One as a syslog server, you must perform the following steps on each PCS/PPS appliance that will use the syslog server:

1. Log into the PCS/PPS appliance.
2. Navigate to **System > Log/Monitoring > Events > Settings**.

© 2019 Pulse Secure, LLC.

3. Under **Select Events to Log**, select all options that need tracking. For example:

FIGURE 3 Select Events to Log



4. Under **Syslog Servers**:

   - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
   - **Facility**: Select an option from the list. This will identify this log type.

     Note: To distinguish between different log types (*Events*, *User Access*, *Admin Access*), you must select a different **Facility** for each type.

   - **Type**: Select *TCP*.
   - **Client Certificate**: Select *Select Client Cert*.
   - **Filter**: Select *WELF: WELF*

5. Click the **Add** button to add this external syslog server.
6. Click **Save Changes** to save the configuration.
7. Navigate to **System > Log/Monitoring > User Access > Settings**.

© 2019 Pulse Secure, LLC.

8. Under **Syslog Servers**:
    - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
    - **Facility**: Select an option from the list. This will identify this log type.

      Note: To distinguish between different log types (*Events*, *User Access*, *Admin Access*), you must select a different **Facility** for each type.
    - **Type**: Select *TCP*.
    - **Client Certificate**: Select *Select Client Cert*.
    - **Filter**: Select *WELF: WELF*
9. Navigate to **System > Log/Monitoring > Admin Access > Settings**.
10. Under **Syslog Servers**:
    - **Server name/IP**: Enter the FQDN or IP address of the Pulse One appliance.
    - **Facility**: Select an option from the list. This will identify this log type.

      Note: To distinguish between different log types (*Events*, *User Access*, *Admin Access*), you must select a different **Facility** for each type.
    - **Type**: Select *TCP*.
    - **Client Certificate**: Select *Select Client Cert*.
    - **Filter**: Select *WELF: WELF*
11. Select the **Advanced Settings** tab and enable Fault Tolerance for the Pulse One syslog server.

Once you have performed this procedure for each PCS/PPS appliance, the Pulse One syslog server will accumulate logs from all appliances and log types.

Note: If the data partition of the target system is full or reaches the disk-usage threshold, then the forwarded logs will not be stored. Follow the steps in **"Managing System Files and Settings" on page 39** to clear older logs.

© 2019 Pulse Secure, LLC.

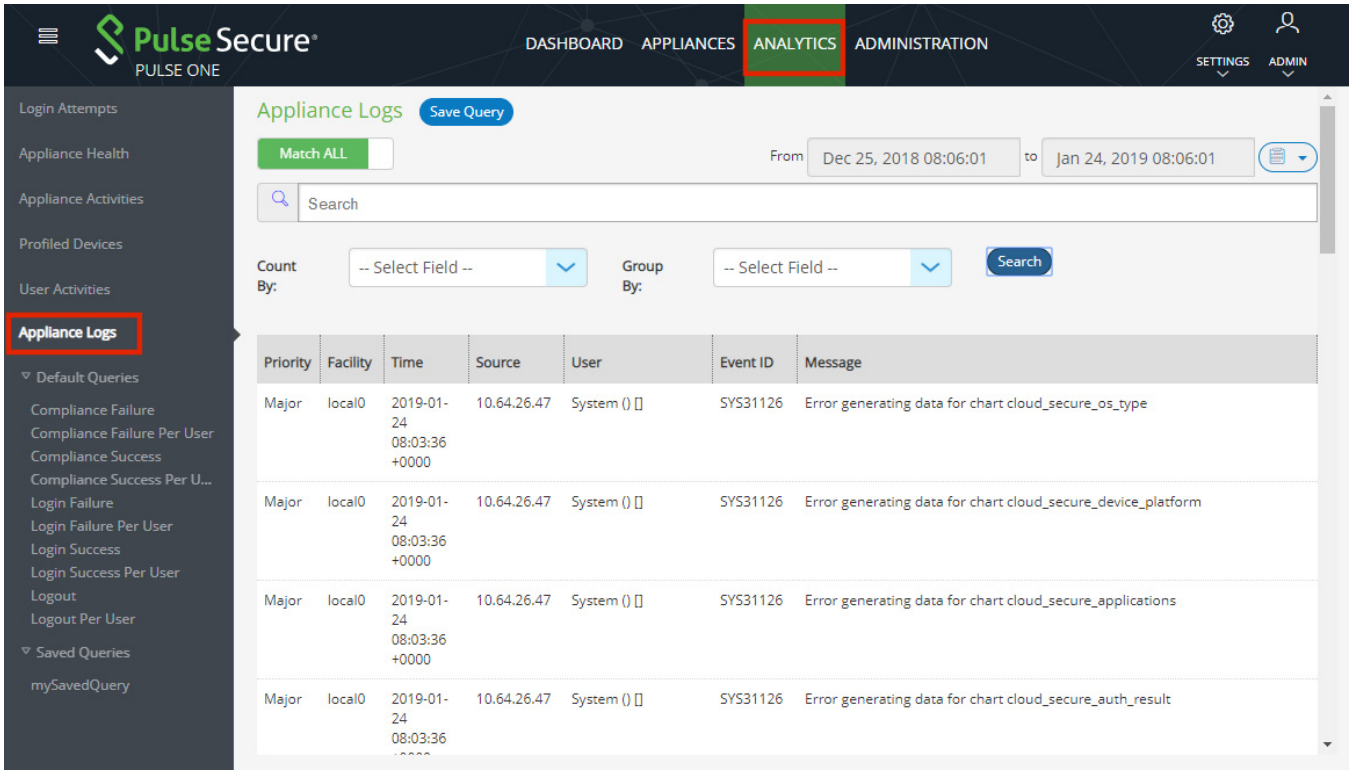
Viewing Accumulated Logs

To view accumulated logs from all log types:

1. Log into Pulse One appliance UI.
2. Navigate to **Administration > Appliance Logs**.

   The **Appliance Logs** page appears. For example:

   FIGURE 4 Pulse One: Appliance Logs



On this page:

- The **Source** column identifies the PCS/PPS appliance that generated the log.
- The **Facility** column identifies the log type, as configured on each PCS/PPS appliance.

© 2019 Pulse Secure, LLC.

Forwarding Appliance Logs to an External Syslog Server

The syslogs from various Pulse Connect Secure and Pulse Policy Secure appliances are forwarded to a Pulse One appliance that is set up as a Syslog server.

Follow the steps to set up another Syslog server as a Syslog target for Pulse One to forward these logs to.

1. Add a syslog target by performing the following command:

   ```
   p1 log-aggregator targets add --port <port> <target server FQDN/IP>
   ```

   For example (with *xx.xx.xx.xx* representing the required IP):

   ```
   p1 log-aggregator targets add --port 333 xx.xx.xx.xx
   xx.xx.xx.xx:333:
     host: xx.xx.xx.xx
     port: 333
     tls: true
   ```

2. Restart the services by performing the following command:

   ```
   services restart
   ```

3. To confirm if the syslog target server is added, type the following command.

   ```
   p1 log-aggregator targets list
   ```

   Example output for this command (with xx.xx.xx.xx representing the required IP) is shown below:

   ```
   xx.xx.xx.xx:333:
     host: xx.xx.xx.xx
     port: 333
     tls: true
   ```

   The syslogs will appear on the Syslog target within a few minutes.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Configuring Pulse One as an NFS Server

Prerequisites

Before proceeding with the setup, ensure that:

- The NFS server is already set up.
- Ensure that either:
    - The PSA-7000 running Pulse One is fully set up and provisioned.
    - The Virtual Machine running Pulse One is fully set up and provisioned.
- If you intend to use the Pulse One appliance in an Active/Passive cluster, mount a separate NFS server for each Pulse One appliance before creating the Active/Passive cluster.
- For the purposes of clustering, to ensure that the NFS servers on either node continue to work as expected, add the IPs of both the internal and external interface to the /etc/exports directory on the NFS server.

Mounting an NFS Server on a Pulse One Appliance

To mount an NFS server on a Pulse One appliance, do the following:

1. Configure and provision the Pulse One appliance.
2. Ensure that the NFS server is configured correctly.
3. Ensure that Pulse One appliance is on a subnet that can reach the NFS server.
4. From the Pulse One CLI, run the following command:

    ```
    p1 log-aggregator show
    ```

    Example output for this command is shown below:

    ```
    keep_days: 30
    type: local
    ```

5. With the above confirmation, mount the NFS server by running the following command:

    ```
    p1 log-aggregator nfs -v <NFS_server_IP or FQDN>:/<path_on_remote_server>
    ```

© 2019 Pulse Secure, LLC.

Note: To use NFS for log storage, both Active and Passive nodes must be configured to use separate NFS mounts.

A message appears:

```
This will delete all existing appliance logs. All services will be stopped if
currently running.
Continue? [y/N]:
```

6. At the confirmation prompt, type *y* and press *Enter*.

   Note: Note: If confirmed, all current logs are lost, so perform this step after the initial set up to avoid loss of needed logs.

7. To check the status of NFS mount, run the following command:

   ```
   p1 log-aggregator show
   ```

   Note: Mounting an NFS server on Pulse One stops all Pulse One services. To continue accessing the Pulse One UI, run the **services start** CLI command.

8. Confirm on the NFS server that Pulse One appliance logs are being synced to it.

   Note: If the data partition of the target system is full or reaches the disk-usage threshold, then the forwarded logs will not be stored. Follow the steps in **"Managing System Files and Settings" on page 39** to clear older logs.

9. Proceed as normal with using Pulse One appliance from the UI.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Unmounting an NFS Server

To unmount NFS server from the Pulse One appliance, do the following:

1. Delete all existing logs:

   ```
   p1 log-aggregator nfs –disable
   ```

   Example output for this command is shown below:

   ```
   This will delete all existing appliance logs. All services will be stopped if
   currently running.
   Continue? [y/N]:
   ```

2. At the confirmation prompt, type *y* and press *Enter*.

   NFS log storage is automatically configured to perform locally.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Managing System Files and Settings

Managing Appliance Logs

In an enterprise that has multiple PCS/PPS appliances forwarding the syslog/NFS appliance logs to a Pulse One server, the assigned data partition will fill up over time. When the partition is full, syslog server will stop receiving logs. See **"Recognizing Low Hard Disk Space" on page 39**.

To prevent a full data partition, you can either:

- Configure the **keep-days** property, see **"Configuring the Log Retention Period" on page 40**.
- Manually delete current syslog files from the CLI, see **"Deleting System Files" on page 40**.

Recognizing Low Hard Disk Space

As your hard disk partition fills up, you may encounter a message similar to the following:

```
------------------------------------------------------------------------
Pulse one is running low on disk space. It is currently 83.000000 full
------------------------------------------------------------------------
```

You can confirm this using the **log-aggregator show** command. Example output is shown below:

```
disk usage: 514.4kb
settings:
   keep_days: 30
   type: local
status: Disabled because disk is 83.0 percent full
```

To prevent this, you can configuring the **keep-days** property to a lower value. This will limit the retention period for logs, and will delete older syslogs indices from the system automatically, see **"Configuring the Log Retention Period" on page 40**.

© 2019 Pulse Secure, LLC.

Configuring the Log Retention Period

To prevent accumulated logs from filling your hard disk partition, you can configure the **keep-days** property to a lower value. This will limit the retention period for logs, and will delete older syslogs indices from the system automatically.

Note: Where you have a larger hard disk partition, you can also increase the retention period to increase the number of retained logs.

Note: Alternatively, you can manually delete your syslogs at any time from the CLI, see **"Deleting System Files" on page 40**.

To configure the **keep-days** property:

1. To change keep_days, type the following command:

   ```
   p1 log-aggregator settings -d <keep_days>
   ```

   A message appears:

   ```
   This might delete some or all of existing appliance logs. All services will be
   stopped if currently running.
   Continue? [y/N]:
   ```

2. At the confirmation prompt, type *y* and press *Enter*.
3. Wait for a few minutes. Based on the **keep_days** value, the older syslog files are removed. The disk will then have free space to receive new syslog data.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Deleting System Files

System file storage will be consumed during the operation of Pulse One.

You can manually clear down system storage using the following CLI commands:

- **system destroy index**. This command deletes all statistics and profiler data.
- **system destroy log-indexer**. This command deletes all received syslog data.

  Note: Alternatively, see **"Configuring the Log Retention Period" on page 40**.
- **system destroy service-logs**. This command deletes all service logs.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Working with System Backups

You can export and import a backup of the system configuration at any time using the following CLI commands:

- **system backup export**. This command exports an archive of system settings as a GZIP TAR (.tgz) file, using a specified interface. See **"Creating a System Backup" on page 41**.
- **system backup import**. This command imports an GZIP TAR (.tgz) file archive and restores the system, using a specified interface. See **"Restoring a System Backup" on page 42**.

You can also use the following CLI command to take a snapshot of your system. Typically, you will do this when it is requested by Pulse Secure Support.

- **system snapshot**. This command takes a snapshot of your complete system configuration and logs. See **"Creating a Pulse One Snapshot" on page 43**.

Note: For appliance backups, see the *Pulse One Administration Guide*.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Creating a System Backup

You can create a backup of your system configuration from the Pulse One command line. This creates a GZIP TAR (.tgz) file from a specified Pulse One interface.

To create a snapshot of Pulse One config and appliance logs:

1. At the CLI command prompt, type the following command:

   ```
   system backup export -i <interface>
   ```

   Where <interface> is set to the required interface, either *external* or *management*.

   Note: Passwords and other secret or private tokens are not captured in the backup.

   Note: If you have Pulse Workspace licensed in your Pulse One, data for this is included in the backup.

   Once the backup file is prepared, a message similar to the following is displayed:

   ```
   Download ready at http://xx.xx.xx.xx:8000/snapshot/download
   MD5: 73c0973a126352559b8be388c8ebc605
   Press Ctrl-C when finished.
   ```

   Note: When this message appears, do not press *CTRL + C*.

2. Start a web browser and access *xx.xx.xx.xx:8000/backup/download.*
3. Save the backup file to an accessible location.

© 2019 Pulse Secure, LLC.

4. Once the download completes, return to the CLI and press *CTRL + C* to complete the backup process.

   Note: If you press CTRL + C before the download completes, the web browser will close, and you will have to start the system snapshot process again.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Restoring a System Backup

You can restore your system configuration from a backup from the Pulse One command line.

To restore your system configuration from a backup file:

1. At the CLI command prompt, type the following command:

   ```
   system backup import -i <interface>
   ```

   Where <interface> is set to the required interface, either *external* or *management*.

   The following message appears:

   ```
   Upload your backup archive here:
   URL: http://xx.xx.xx.xx:8000/backup
   Press Ctrl-C when finished.
   ```

   Note: When this message appears, do not press *CTRL + C*.

2. Start a web browser and access `http://xx.xx.xx.xx:8000/backup`.
3. Using the controls on the web page, upload the backup file you want to restore.
4. Once the backup file upload completes, return to the CLI and press *CTRL + C* to complete the import process.

   Note: If you press *CTRL + C* before the download completes, the web browser will close, and you will have to start the restore process again.

5. After the import process completes, restart all services to put new settings into effect:

   ```
   services restart
   Restarting...
   Starting with version "1902"...
   Started.
   Restarted.
   ```

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

Creating a Pulse One Snapshot

If you need to contact Pulse Support, you may be asked for a snapshot of your Pulse One system. A snapshot will include your Pulse One configuration and logs.

To create a snapshot of Pulse One config and appliance logs:

1. At the CLI command prompt, type the following command:

   ```
   system snapshot
   ```

   Note: Passwords and other secret or private tokens are not captured in the snapshot.

   Note: If you have Pulse Workspace licensed in your Pulse One, data for this is included in the snapshot.

   During the process, a message similar to the following is displayed:

   ```
   Download ready at http://xx.xx.xx.xx:8000/snapshot/download
   MD5: 73c0973a126352559b8be388c8ebc605
   Press Ctrl-C when finished.
   ```

   Note: When this message appears, do not press *CTRL* + *C*.

2. Start a web browser and access *xx.xx.xx.xx:8000/backup/download*.
3. Save the snapshot file to an accessible location.
4. Once the download completes, return to the CLI and press *CTRL* + *C* to complete the snapshot process.

   Note: If you press CTRL + C before the download completes, the web browser will close, and you will have to start the system snapshot process again.

See the *Pulse One Command Reference Guide* for full details of individual commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Configuring an Active/Passive Cluster

Overview

Pulse One appliances support two-node Active/Passive clustering configuration for high availability.

In a two node Active/Passive cluster:

- The *Active* Pulse One node services all requests.
- The *Passive* node is a "hot" standby and maintains a copy of the Active node's data. That is, its appliance configuration, system state, and log messages.
- Active/Passive clustering supports automatic failover in the event of the failure of an Active node. Manual failover is also supported, see **"Failover Scenarios" on page 50**.

All cluster configuration is performed using the Pulse One Command-Line Interface (CLI). The CLI can also be used to monitor the state of the cluster.

Note: The status of the cluster, the status of the current Active node and the automatic failover switch state are always displayed in the Pulse One graphical user interface. Refer to the *Pulse One Appliance Administration Guide*.

Note: The two nodes in the cluster must run the same version of Pulse One.

Note: The cluster does not interact with Pulse Policy Secure Profiler.

© 2019 Pulse Secure, LLC.

Prerequisites

To configure an Active/Passive cluster, the following prerequisites must be fulfilled.

- **Pulse One Appliances** – two Pulse One appliances are required:
  - One will be the Active node and the other will be the Passive node.
  - The Active node must be fully configured.
  - The Passive node must have configured Internal and External network interfaces (see below), but typically has a configured management interface also.
- **SSH access** – to the management interface of the Active and Passive nodes.
- **NFS servers** – configure any required NFS servers before starting to create the cluster, see **"Mounting an NFS Server on a Pulse One Appliance" on page 37**.
- **DNS** – to enable automatic failover of Active to Passive, the hostname of the cluster must resolve to the IP addresses of both the Active node and the Passive node.
- **Managed appliances** – all managed appliances must run version 9.0R2 or above.
- **Network connectivity between the Internal interfaces** – Pulse One state synchronization occurs only via the internal network interface cards (NICs). Please ensure that the internal interface on the Active node can communicate with the Internal interface on the Passive node. See **"Configuring Internal Interfaces" on page 47**.
- **Ports between the Active and Passive nodes** – The following port must be open between the Active and Passive nodes (for when there is a firewall between them):

Protocol	Port	Purpose
TCP/UDP	500	Secure channel service. This is the communication port between the clustered nodes. **Note:** Pulse One recommends that IPv4 Protocol 51 is enabled.

© 2019 Pulse Secure, LLC.

Configuring Internal Interfaces

Pulse One uses the internal interfaces to communicate between the two nodes in an Active/Passive cluster. To enable clustering, each of the two candidate appliances must have its internal interface enabled and have a valid and available IPv4 address assigned to it.

Note: Port 500 is the main communication port for communication between the clustered nodes, see **"Prerequisites" on page 46**. Pulse One recommends that IPv4 Protocol 51 is enabled.

To enable the internal interfaces:

1. Configure the internal Interface of the proposed Active node:

   ```
   network interface internal --ip <IPv4 address> --netmask <subnet mask>
   ```

   For example:

   ```
   network interface internal --ip 10.64.45.172 --netmask 255.255.0.0
   ```

2. Repeat step 1 on the proposed Passive node.

3. Test connectivity between the two appliances:

   ```
   network ping <internal IP address of the counterpart>
   ```

   Note: The IP address used to configure internal or external interface should not be in the range 192.170.0.1 – 192.170.0.254.

See the *Pulse One Command Reference Guide* for full details of individual commands.

Setting Up an Active/Passive Cluster

After meeting all prerequisites, you can set up an Active/Passive cluster.

Perform the following steps:

1. Log into the CLI on the appliance that you want to be the Active node.

2. Set the appliance as the current Active node, type the following command:

   ```
   cluster promote
   ```

© 2019 Pulse Secure, LLC.

Example output for this command is shown below:

```
Promoting node to active cluster node...
Stopping uno_mongo_1 ... done
Removing uno_mongo_1 ... done
Stopping uno_log_collector_1 ... done
Removing uno_log_collector_1 ... done
node:
  id: af714515364b402b84cae007b183dd24
  ip: 192.168.56.101
  mode: active
```

In this example, the node is confirmed as Active.

3. To begin the process of adding a Passive node to form a cluster, run the following command from the Active node:

   ```
   cluster add <Internal IP of intended Passive Node>
   ```

   The output for this command includes a command that you must run on the Passive node. This command includes a cluster join token. For example:

   ```
   To cluster 192.168.56.102 as a Passive Pulse One appliance with an Active
   appliance, you must configure networking on the passive appliance and run the
   following command on it:

   cluster join 192.168.56.101 nv13rvdv
   ```

   In this example, the cluster join token is “nv13rvdv”.

   Note: The cluster join token is valid until the token is regenerated by issuing another cluster add command.

4. Copy the resulting command from the output of the cluster add command.
5. Log into the CLI on the appliance that you want to be the Passive node.
6. Paste the command that was copied in step 4 and press Enter. For example:

   ```
   cluster join 192.168.56.101 nv13rvdv
   ```

   Example output for this command is shown below:

   ```
   WARNING: This will delete all Pulse One data, resetting the appliance to factory
   defaults.
   The data will not be recoverable.
   Type DESTROY to continue:
   ```


© 2019 Pulse Secure, LLC.

7. Type *DESTROY* and press *Enter*. Example output is shown below:

```
Type DESTROY to continue: DESTROY
Resetting data…
Removing directory /data/lost+found
Destroyed.
Joining cluster 192.168.56.101 as a passive node…
```

8. On the Passive node, verify the cluster status of the node:

```
cluster status
```

   Example output for this command is shown below:

```
cluster:
  active_node: 10.64.45.177
  nodes:
    - 10.64.45.177
    - 10.64.45.175
node:
  id: 2dc3c050e9af4b8d85ad32fffc75f2fc
  ip: 10.64.45.175
  mode: passive
```

   Note: For Pulse One appliance in clustered mode, if its peer is not accessible, the **cluster status** command will not return any result.

9. On the Active node, verify the cluster status of the node:

```
cluster status
```

   Example output for this command is shown below:

```
cluster:
  active_node: 10.64.45.177
  nodes:
    - 10.64.45.177
    - 10.64.45.175
node:
  id: af714515364b402b84cae007b183dd24
  ip: 10.64.45.177
  mode: active
```

10. To enable automatic failover, set a failover timeout on the Active node. For example:

```
cluster config -f 2
```

   Example output for this command is shown below:

```
auto_failover: true
auto_failover_timeout: 2 minutes
```

This concludes the setup of the Active/Passive cluster.

© 2019 Pulse Secure, LLC.

Accessing an Active/Passive Cluster

Once your two-node Active/Passive cluster is established, you can access the Active node via a browser.

To do this, you must enter the hostname for the cluster into your browser's address bar and press *Enter*.

Note: After a short time, the graphical user interface for the Active node is displayed. The status of the cluster, the status of the current Active node and the automatic failover switch state are always displayed in the Pulse One GUI. Refer to the *Pulse One Appliance Administration Guide*.

Note: You must have previously configured your DNS to resolve to both IP addresses for the cluster, see **"Prerequisites" on page 46**.

Note: If DNS is not configured to resolve to both IP addresses for the cluster, it is possible to access either node using its IP address. However, this scenario does not support automatic failover. Pulse Secure recommends that you do not access individual clustered nodes using their IP addresses, as this does not support authentication of the server.

Failover Scenarios

When an Active node fails for any reason, the following failover scenarios are supported:

- Automatic failover, see **"Working with Automatic Failover" on page 50**.

  Note: This scenario requires specific configuration, see **"Prerequisites" on page 46** and **"Setting Up an Active/Passive Cluster" on page 47**.

  To recover after an automatic failover, see **"Restoring a Cluster after an Automatic Failover" on page 51**.

- Manual failover using a dual-resolving DNS entry, see **"Performing a Manual Failover with a Dual-Resolving DNS Entry" on page 52**.

- Manual failover using a single DNS entry, see **"Performing a Manual Failover Using a Single DNS Entry" on page 53**.

- Manual failover using an IP address swap, see **"Performing a Manual Failover Using Interface IP Swap" on page 54**.

Working with Automatic Failover

Automatic failover of a two-node Active/Passive cluster is supported by Pulse One appliance.

Note: All PCS/PPS appliances must be at v9.0R2 (or later) to successfully reconnect to Pulse One after automatic failover.

Note: The Active and Passive nodes communicate cluster health using their internal interfaces over port 8001. This port must be open to enable automatic failover, see **"Prerequisites" on page 46**.

© 2019 Pulse Secure, LLC.

When the Active node (A) fails, no user action is required to perform the failover itself:

- In a short time, the Passive node (B) detects the failure.
- The Passive node (B) makes itself a standalone node automatically. This node is effectively a standalone "Active" node which is based on the configuration of the original Active node (A). However, there is no longer an operational cluster.
- All PCS/PPS appliances that are at v9.0R2 (or later) adjust automatically to communicate with the new standalone node (B).
- Pulse One operations continue against the standalone node (B).

Note: When the Passive node in a cluster fails, no action is performed automatically by Pulse One. The Active nodes is unaffected, and the cluster persists when the Passive node returns to service.

To recover the cluster, see **"Restoring a Cluster after an Automatic Failover" on page 51**.

Restoring a Cluster after an Automatic Failover

To restore an Active/Passive cluster after an automatic failover, the administrator must:

1. Bring the failed node (A) back to an operational state.

   At this point, this node (A) may still be configured as an Active node. This is not the required configuration.

   The required configuration is:

   - The recovered node (A) will become the new Passive node.
   - The standalone "Active" node that is servicing requests (B) will become the new Active node.

2. Demote the recovered node (A) to be a standalone node.

   Note: Do not change DNS server prior to performing cluster demote command. Doing so will cause all managed appliances to de-register from Pulse One and they will need to be deleted, added and registered again. Once a Passive node is in a standalone mode, it is safe to configure DNS server to have Pulse One FQDNs resolve to the IP address of the Passive node's external interface.

   Note: After demoting an appliance (Active node or Passive node), reboot the appliance. The Internal port is automatically disabled. If the appliance needs to be clustered again, configure the internal interface prior to executing any clustering commands.

3. Configure the internal interfaces of both nodes, see **"Prerequisites" on page 46**.
4. Promote the standalone "Active" node (B) to be a formal Active node.

© 2019 Pulse Secure, LLC.

5. Join the standalone node (A) as a Passive node to the Active node (B).

   This will reset all data on the Passive node (A).

6. Monitor the synchronization of the nodes using cluster status.

Performing a Manual Failover with a Dual-Resolving DNS Entry

You can configure the DNS entry for the cluster hostname to resolve to the IP addresses of both the Active and Passive nodes. In this scenario, all PCS/PPS appliances can communicate with either functioning node. In the event of a failure, one node is still available, and the appliances will find it automatically.

You may want to perform a manual failover, because either:

- You do not have automatic failover configured, OR
- You have automatic failover configured, but you need to perform scheduled maintenance on the Active node.

To perform a manual failover using a duel-resolving DNS Entry for the cluster hostname:

1. Log into the both the Active and Passive nodes, and ensure that their services are in sync:

   ```
   cluster status
   ```

2. From the CLI of the Passive node, run the following command.

   ```
   cluster demote
   ```

   Note: After demoting an appliance (Active node or Passive node), reboot the appliance. The Internal port is automatically disabled. If the appliance needs to be clustered again, configure the internal interface prior to executing any clustering commands.

3. From the CLI of the Active node, run the following command.

   ```
   cluster demote
   ```

4. Take the Active node out of service:

   ```
   services stop
   ```

   Note: After a short time, the PCS/PPS appliances will automatically communicate with the remaining standalone node, using the dual-resolving DNS.

5. Proceed to log in to the Pulse One admin UI by accessing the cluster hostname.

To revert to using the original node as Active, you must bring the original Active node back into service and perform another manual failover before manually reforming the cluster.

© 2019 Pulse Secure, LLC.

Performing a Manual Failover Using a Single DNS Entry

This procedure may be required if the DNS entry for the cluster hostname resolves to a single IP address. That is, the IP address for the Active node.

Note: Where a dual-resolving DNS entry is used for the cluster hostname, see **"Performing a Manual Failover with a Dual-Resolving DNS Entry" on page 52**.

You may want to perform a manual failover, to either:

- Recover from the failure of an Active node, OR
- Perform scheduled maintenance on the Active node.

To perform a manual failover using a single DNS Entry for the cluster hostname:

1. Log into the both the Active and Passive nodes, and ensure that their services are in sync:

   ```
   cluster status
   ```

2. From the CLI of the Passive node, run the following command.

   ```
   cluster demote
   ```

   Note: Do not change DNS server prior to performing cluster demote command. Doing so will cause all managed appliances to de-register from Pulse One and they will need to be deleted, added and registered again. Once a Passive node is in a standalone mode, it is safe to configure DNS server to have Pulse One FQDNs resolve to the IP address of the Passive node's external interface.

   Note: After demoting an appliance (Active node or Passive node), reboot the appliance. The Internal port is automatically disabled. If the appliance needs to be clustered again, configure the internal interface prior to executing any clustering commands.

3. Navigate to the DNS server. Make the Pulse One FQDN hostname resolve to the IP address of the Passive node EXT Interface. That is, the IP in the DNS entry should now be for the Passive node's EXT interface.
4. Next, set Pulse One DNS record to the IP address (external interface) of the Passive node (which is now demoted to a standalone node).
5. Proceed to log in to the Pulse One admin UI by accessing the Fully Qualified Domain Name on the appliance.

To revert to using the original node as Active, you must repeat this procedure and then manually reform the cluster.

© 2019 Pulse Secure, LLC.

Performing a Manual Failover Using Interface IP Swap

This procedure may be required where your cluster is configured using external interface IP addresses only. That is, there is no DNS entry for the cluster hostname.

You may want to perform a manual failover, to either:

- Recover from the failure of an active node, OR
- Perform scheduled maintenance on the Active node.

To perform a manual failover by manually swapping the external interface IP address for both clustered nodes:

1. Log into the both the Active and Passive nodes, and ensure that their services are in sync:

   ```
   cluster status
   ```

2. From the Passive node, type the following command:

   ```
   cluster demote
   ```

3. Run the following command to change the IP of the Passive node (EXT interface) to the IP of the Active node:

   ```
   network interface external --ip <EXT IP of ACTIVE node>
     --netmask <netmask of ACTIVE node> --gateway <gateway IP address>
   ```

   Note: Do not change the external interface of the Passive node prior to performing cluster demote command. Doing so will cause all managed appliances to de-register from Pulse One and they will need to be deleted, added and registered again. Once the Passive node is in a standalone mode, it is safe to configure its external interface to IP of the Active node.

   Note: After demoting an appliance (Active node or Passive node), reboot the appliance. The Internal port is automatically disabled. If the appliance needs to be clustered again, configure the internal interface prior to executing any clustering commands.

4. Proceed to log in to the Pulse One admin UI by accessing the Fully Qualified Domain Name on the appliance.

   Note: To use NFS for log storage, both Active and Passive nodes must be configured to use separate NFS mounts, see **"Configuring Pulse One as an NFS Server" on page 37**.

To revert to using the original node as Active, you must repeat this procedure and then manually reform the cluster.

© 2019 Pulse Secure, LLC.

Upgrading an Active/Passive Cluster

You can upgrade an operational Active/Passive cluster if required.

The process will depend on whether your cluster is configured to use auto-failover.

If your cluster is configured for auto-failover, the FQDN will resolve to the IP address of the EXT interface on both Active and Passive nodes, see **"Working with Automatic Failover" on page 50**. If this is the case, first perform the following steps:

1. Run the following CLI command on both nodes:

   ```
   cluster status
   ```

2. Ping the FQDN of the cluster to confirm that it resolves to the IP address of the Active node's EXT interface.

Possible outcomes:

- If the Active node is working, remove the Passive node DNS entry that resolves to the cluster FQDN.
- If the Active node is down, and the Passive node has been demoted to standalone and is receiving requests, remove the original Active node DNS entry that resolves to the cluster FQDN. Also, treat the Passive node as Active for the purposes of the upgrade procedure.
- If neither node is working, do not proceed with the upgrade.

Note: It is important to allow time for the DNS entries to reach all managed appliances. The propagation delay depends on your DNS infrastructure. Five minutes is typically sufficient.

Then, to upgrade any cluster, perform the following procedure:

Note: You must ensure that each step is complete before proceeding to the next step.

1. On the Passive node, demote the node to standalone:

   ```
   cluster demote
   ```

2. Stop all services on the Passive node:

   ```
   services stop
   ```

3. On the Active node, demote the node to standalone:

   ```
   cluster demote
   ```

4. Stop all services on the Active node:

   ```
   services stop
   ```

© 2019 Pulse Secure, LLC.

5. (Optional) On the (formerly-Active) standalone node, perform a backup of the node's configuration.

   ```
   system backup export
   ```

   After the appliance backup file is created, download the backup from the displayed URL. This backup can be used to perform a restore if required. See **"Working with Backup and Restore" on page 23** for full details of the backup/restore processes.

   Note: The restore process for a configuration backup must be performed on the same Pulse One software version from which it was backed up. That is, if a backup is created from 1901.1, it should be restored to 1901.1.

6. On the (formerly Active) standalone node, perform a Pulse One upgrade, as described in **"Upgrading the Pulse One Appliance" on page 61**.

7. Start services on the (formerly Active) appliance:

   ```
   services start
   ```

   Note: Wait until all services have started on the Active appliance.

8. On the (formerly Passive) standalone node, perform a Pulse One upgrade, as described in **"Upgrading the Pulse One Appliance" on page 61**.

9. Start services on the (formerly Passive) appliance:

   ```
   services start
   ```

10. After both standalone nodes are upgraded and restarted successfully, re-cluster the nodes. This process is described in **"Setting Up an Active/Passive Cluster" on page 47**.

11. (Optional) If you intend to use auto-failover, add the Passive node entry back into the DNS.

    Note: This addition to the DNS will take some time to propagate to managed appliances. The length of time will depend on your network.

© 2019 Pulse Secure, LLC.

De-clustering the Active/Passive Cluster

To de-cluster the clustered nodes to standalone nodes, do the following:

1. Demote the Passive node first, by running the following command:

   ```
   cluster demote
   ```

2. Confirm that the output of the **cluster demote** command indicates that the node is successfully demoted. For example:

   ```
   node:
     id: <id_string>
     ip: xx.xx.xx.xx
     mode: standalone
   ```

3. Reboot this node.

4. Demote the Active node by running the following command:

   ```
   cluster demote
   ```

5. Confirm that the output of the **cluster demote** command indicates that the node is successfully demoted. For example:

   ```
   node:
     id: <id_string>
     ip: yy.yy.yy.yy
     mode: standalone
   ```

6. Reboot this node.

7. (Optional) If you require the PCS/PPS appliances to continue to communicate with a specific node, either:

   - Update the dual-resolving DNS entry to remove the other node, OR
   - Take the other node out of service. The other node will be used.

Once complete, the de-clustered appliances are running as separate standalone nodes.

Note: Demoting an appliance (either Active node or Passive node) disables its internal interface. If an appliance needs to be clustered again, configure its internal interface before performing the rest of the clustering commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Launching the Management Console

Launching the Pulse One Management Console

To launch the Pulse One management console, go to the address bar in the browser and type the management console address. For example:

```
https://pulseone.example.com
```

Where pulseone.example.com is the FQDN for the Pulse One console.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.

Upgrading the Pulse One Appliance

Prerequisites

Before upgrading the Pulse One appliance:

- You must ensure that the network, gateway, and DNS are configured on the appliance.
- If you are upgrading from Pulse One 2.0 1637, you must ensure that the management port is configured to access the UI.

Note: If the upgrade is from Pulse One 2.0 1649 (or later), the upgrade process preserves all existing data.

Note: If the upgrade is from Pulse One 2.0 1637 (or earlier), the upgrade process does not preserve all existing data.

Note: After an upgrade, the first use of the system storage add CLI command will force the current data storage system to change to an LVM data storage system, and all existing data will be destroyed. To avoid data loss in this case, you must perform a **system backup export** before you use **system storage add**, and then perform a **system backup import** after **system storage add** completes.

Upgrading a Pulse One Appliance

There are three methods of upgrading the Pulse One appliance, depending on your starting software version and preferred method:

- "Upgrading a Pulse One Release (Pre-v2.0.1902)" on page 62.
- "Upgrading Pulse One Release (v2.0.1902 or Later) Using CLI Only" on page 63.
- "Upgrading Pulse One Release (v2.0.1902 or Later) Using Browser/CLI" on page 64.

© 2019 Pulse Secure, LLC.

Upgrading a Pulse One Release (Pre-v2.0.1902)

To upgrade a version of Pulse One appliance that is before version 2.0.1902, do the following:

1. Ensure that there is an accessible external web server running.
2. Log in to the Pulse One appliance and access the CLI.

   Note: The upgrade process reboots the system. Some messages immediately following reboot might be lost if you use SSH to access the CLI, as the SSH session will be disconnected during the reboot and service restarts. Using a serial port CLI session is recommended in such cases.
3. Run the following CLI command:

   ```
   system upgrade <hosted_upgrade_package_URL> <upgrade_package_md5_hash>
   ```

   Note: The MD5 hash is provided by Pulse Secure.

   For example:

   ```
   system upgrade http://example.com/upgrade/pulse-one-2.0.1902.tgz
   1843f9120c564f7684b104adfece11bd
   ```
4. After the upgrade is complete, press *Enter* to reboot the system. Wait for the system to reboot successfully before continuing to the next step.
5. Log back into the system using your preset CLI credentials.
6. Change any of the preset system settings as needed. For all changed settings to take effect, run the following command:

   ```
   services restart
   ```
7. Verify that the upgrade is successful by:
   - Logging into the Pulse One UI.
   - View the **Pulse One Properties**.
   - Confirm that the current running server version is as expected.

See the *Pulse One Command Reference Guide* for full details of individual CLI commands.

© 2019 Pulse Secure, LLC.

Upgrading Pulse One Release (v2.0.1902 or Later) Using CLI Only

You can upgrade a Pulse One appliance using either a CLI-only method or a browser/CLI hybrid method.

This section describes the CLI-only method. For the hybrid method, see **"Upgrading Pulse One Release (v2.0.1902 or Later) Using Browser/CLI" on page 64**.

To upgrade Pulse One appliance v2.0.1902 (or later) using the CLI, do the following:

1. Ensure that there is an accessible external web server running.
2. Log in to the Pulse One appliance and access the CLI.

   Note: The upgrade process reboots the system. Some messages immediately following reboot might be lost if you use SSH to access the CLI, as the SSH session will be disconnected during the reboot and service restarts. Using a serial port CLI session is recommended in such cases.
3. Run the following CLI command:

   ```
   system upgrade cli <hosted_upgrade_package_URL> <upgrade_package_md5_hash>
   ```

   Note: The MD5 hash is provided by Pulse Secure.

   For example:

   ```
   system upgrade cli http://example.com/upgrade/pulse-one-2.0.1902.tgz
   1843f9120c564f7684b104adfece11bd
   ```
4. After the upgrade is complete, press *Enter* to reboot the system. Wait for the system to reboot successfully before continuing to the next step.
5. Log back into the system using your preset CLI credentials.
6. Change any of the preset system settings as needed. For all changed settings to take effect, run the following command:

   ```
   services restart
   ```
7. Verify that the upgrade is successful by:
   - Logging into the Pulse One UI.
   - View the **Pulse One Properties**.
   - Confirm that the current running server version is as expected.

See the *Pulse One Command Reference Guide* for full details of individual CLI commands.

© 2019 Pulse Secure, LLC.

Upgrading Pulse One Release (v2.0.1902 or Later) Using Browser/CLI

You can upgrade a Pulse One appliance using either a CLI-only method or a browser/CLI hybrid method.

This section describes the browser/CLI hybrid method. For the CLI-only method, see **"Upgrading Pulse One Release (v2.0.1902 or Later) Using CLI Only" on page 63**.

Note: You do not need to start an external web server for this method.

To upgrade Pulse One appliance v2.0.1902 (or later) using a combination of CLI and browser, do the following:

1. Download the upgrade package from **https://my.pulsesecure.net**.

   Note: You must locate this package so that it is accessible from your browser.

2. If an MD5 hash of the upgrade package is not provided, create one on the system containing the upgrade package, and record the resulting hash. For example, using the **md5sum** command from the LINUX system prompt, with the upgrade package in the same directory:

   ```
   md5sum pulse-one-2.0.1902.tgz
   1843f9120c564f7684b104adfece11bd pulse-one-2.0.1902.tgz
   ```

   In this example, the generated MD5 checksum for the *pulse-one-2.0.1902.tgz* file is "1843f9120c564f7684b104adfece11bd".

3. Log in to the Pulse One appliance and access the CLI.

   Note: The upgrade process reboots the system. Some messages immediately following reboot might be lost if you use SSH to access the CLI, as the SSH session will be disconnected during the reboot and service restarts. Using a serial port CLI session is recommended in such cases.

4. Run the following CLI command:

   ```
   system upgrade [-i <interface>]
   ```

   Where the optional <*interface*> is *internal*, *external* or *management*.

   The output from this command provides further instructions. For example:

   ```
   Pulse One > system upgrade
   WARNING: Please ensure that backup has been performed (`system backup export`
   command). Data and configuration changes cannot be reverted after upgrade.
   Type "UPGRADE" to continue:
   ```

5. Type *UPGRADE* and press *Return*.

   The output from this command provides further instructions. For example:

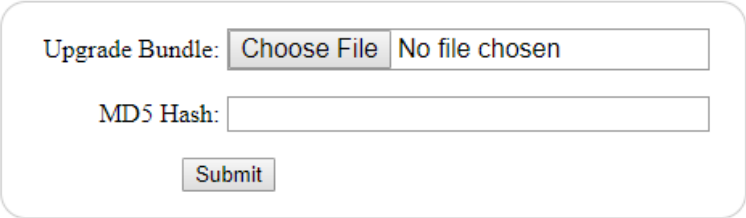
   ```
   Type "UPGRADE" to continue: UPGRADE
   Upload your upgrade bundle here:
   URL: http://10.64.60.14:8000/upgrade
   ```


© 2019 Pulse Secure, LLC.

6. Start a browser, and enter the required URL. In this example, *http://10.64.60.14:8000/upgrade*.

   The following dialog appears in your browser.

   FIGURE 5 Upload an Upgrade Package

7. Click **Choose File** and locate the upgrade package.
8. Enter the **MD5 Hash** for the upgrade package.
9. Click **Submit**.

   The package then uploads via your browser.

   After the upload completes, the Pulse One appliance upgrades and reboots.

10. After the reboot completes, log back into the Pulse One appliance and access the CLI.
11. Change any of the preset system settings as needed. For all changed settings to take effect, run the following command:

    ```
    services restart
    ```

12. Verify that the upgrade is successful by:
    - Logging into the Pulse One UI.
    - View the **Pulse One Properties**.
    - Confirm that the current running server version is as expected.

See the *Pulse One Command Reference Guide* for full details of individual CLI commands.

© 2019 Pulse Secure, LLC.

© 2019 Pulse Secure, LLC.