Welcome to Puppet Comply

Puppet Comply is a tool that assesses the infrastructure you manage with Puppet Enterprise against CIS Benchmarks — the best practices for securely configuring systems from the Center for Internet Security (CIS).

Using Comply, you can:

• Run scans to check the compliance of your infrastructure against CIS Benchmarks on up to 1000 nodes.
• Set your desired compliance — a default benchmark and profile that you want your scans to be measured against.
• Customize profiles to specify which rules you want visible in scan reports.
• Identify the cause and source of compliance failures, and determine what configuration changes must be made to which systems.

Comply uses Puppet Enterprise (PE) to retrieve node and fact information. Once you have installed Comply, you must configure it to integrate with PE.

If this is your first time using Comply, try out our Beginner’s guide to Comply.

<table>
<thead>
<tr>
<th>Puppet Comply docs links</th>
<th>Other useful places</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn the basics:</td>
<td>Comply videos:</td>
</tr>
<tr>
<td>Comply overview</td>
<td>Comply introduction and demo</td>
</tr>
<tr>
<td>Comply terminology</td>
<td>Docs for related Puppet products:</td>
</tr>
<tr>
<td>Beginner’s guide to Comply</td>
<td>Puppet Enterprise</td>
</tr>
<tr>
<td>Release notes</td>
<td>Puppet Forge</td>
</tr>
<tr>
<td>Install and configure Comply:</td>
<td>Get help:</td>
</tr>
<tr>
<td>System requirements</td>
<td>Troubleshooting</td>
</tr>
<tr>
<td>Install Puppet Application Manager</td>
<td>Support portal</td>
</tr>
<tr>
<td>Set up Comply</td>
<td></td>
</tr>
<tr>
<td>Run and manage CIS scans:</td>
<td></td>
</tr>
<tr>
<td>Run a CIS scan</td>
<td></td>
</tr>
<tr>
<td>Set desired compliance</td>
<td></td>
</tr>
<tr>
<td>Create a custom profile</td>
<td></td>
</tr>
<tr>
<td>on page 87</td>
<td></td>
</tr>
<tr>
<td>View scan results</td>
<td></td>
</tr>
</tbody>
</table>

Comply terminology

Key terms to be familiar with when using Puppet Comply.

CIS Benchmarks

Developed by the Center for Internet Security (CIS), CIS Benchmarks are internationally recognized standards and best practices for securely configuring systems. For more information, see CIS Benchmarks.

CIS assessor

Comply integrates with the CIS assessor (CIS-CAT PRO), the scanner tool that assesses CIS benchmarks. As part of the Comply configuration process, Puppet Enterprise (PE) installs the CIS assessor on your target nodes. For more information on the assessor, see CIS-CAT Pro.
Profiles
CIS Benchmarks include different levels of security settings, called profiles. The Level 1 profiles are the base recommendation for every system, and the Level 2 profiles are intended for environments requiring greater security. Comply can scan for either profile.

Rules
Each profile contains multiple rules that define specific elements of system configuration.

Custom profiles
A custom profile is a benchmark profile that you customize to fit your organization's internally defined standards, by specifying which rules you want visible in scan reports. Once you create a custom profile, it appears as an option in Comply when selecting a benchmark and profile.

Desired compliance
Desired compliance is the benchmark and profile that you assign to a node. It becomes the default scan for that node.

For a full list of Puppet terminology, see the Puppet Glossary.

Comply overview
Welcome to the Puppet Comply!
This overview is intended for new users of Comply. We go over what Comply is, how it works, and show a demo of the 1.0.0 release. Before you begin, we recommend familiarizing yourself with our terminology.

What is Comply and how does it work?
Comply is a tool that expands the compliance capabilities of Puppet Enterprise (PE), by integrating with the CIS assessor to scan your infrastructure against the latest CIS Benchmarks. Comply connects to your PE environment and gathers information about your PE managed nodes, including operating system facts and classification node groups. It uses this information to suggest appropriate scans.

You can choose to run ad-hoc scans or desired compliance scans — a default CIS benchmark and profile scan that you assign to a node. Comply can automate desired compliance for you based on the information it gathers about your nodes from PE, or you can manually choose your desired compliance from a list of benchmarks and profiles. You can also create custom profiles to fit internally defined standards, by specifying which rules you want visible in scan reports. Most of the time, you only need to set your desired compliance once.

The scans are run as a task in PE. Scan results populate in the Comply Compliance dashboard, where you can see the number of nodes scanned and their compliance breakdown. In each node listed, there is a further breakdown of rule information which tells you why that rule is important, and steps you can take to fix the rule if it is failing the scans.

To see Comply in action, watch the demo below, or go through the steps yourself in our getting started guide.

For a full list of features, see the release notes.

Comply demo
The following demo walks you through the key features of the Comply 1.0.0 release:

Supported CIS benchmarks
Comply supports the following CIS operating system benchmarks.
## Comply release notes

These are the new features, enhancements, and resolved issues for the Puppet Comply 2.x release series.

### Comply 2.4.0

Released 24 March

New in this release:

- **CIS-CAT Pro Assessor v4.15.0.** Comply 2.4.0 includes the latest version of the CIS-CAT assessor and the following supported associated benchmarks:
  - CentOS Linux 8 (final release)
  - Microsoft Windows 10 v1.12.0.
  - Microsoft Windows Server 2022 v1.0.0
  - Red Hat Enterprise Linux 8 v2.0.0
  - SUSE Linux Enterprise 11 v2.1.1 (final release)

**Note:** The Microsoft Windows 10 benchmark has upgraded from 1.11.0 CIS Microsoft Windows 10 Enterprise Release 21H1 to 1.12.0 CIS Microsoft Windows 10 Enterprise. Comply’s 1.12.0 CIS Microsoft Windows 10 Enterprise benchmark is based on Microsoft Windows 10 Enterprise Release 21H2 and is intended for all versions of the Windows 10 operating system, including older versions. If any of your nodes use custom profiles based on the 1.11.0 CIS Microsoft Windows 10 Enterprise Release 21H1 benchmark, you need to resolve these manually, as they will not automatically update during the upgrade process.

- **Profile and Custom profile.** You can view and sort two new columns on the Inventory page - Profile and Custom profile. The columns allow you to see if a node has a default profile or custom profile assigned to it.
- **Benchmark column.** The Desired compliance column has been renamed to Benchmark.

Resolved in this release:

- **Sync license.** Fixed an issue where a user was logged out of Comply after selecting Sync license on the License page.

---

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
</tr>
<tr>
<td>CentOS</td>
<td>6, 7, 8</td>
</tr>
<tr>
<td>Debian</td>
<td>8, 9, 10</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>6, 7, 8</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>6, 7, 7 STIG, 8</td>
</tr>
<tr>
<td>SUSE Linux Enterprise Server (SLES)</td>
<td>11, 12, 15</td>
</tr>
<tr>
<td>Ubuntu</td>
<td>16.04, 18.04, 20.04, 20.04 STIG</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>10.14, 10.15, 11.0</td>
</tr>
</tbody>
</table>

**Note:** If you use Ubuntu 16.04, you need Curl with mutual TLS support to upgrade and run scans.
Comply 2.3.0
Released 10 February 2022

New in this release:

• **Scheduled scans.** You can now schedule one-off and repeating scans, in addition to running manual ad hoc scans, in Comply.
  
  For more information, see [Scheduled scans](#) on page 89.

• **Environment information.** The Scan list page now shows the scan report environment.

• **CIS-CAT Pro Assessor v4.14.0.** Comply 2.3.0 includes the latest version of the CIS-CAT assessor and the following supported associated benchmarks:
  
  • SUSE Linux Enterprise 12 v3.1.0
  • SUSE Linux Enterprise 15 v1.1.1

This release of the assessor resolves security vulnerability present in embedded, third party dependencies:

• The **OpenDXL Java** Client library, which includes log4j, is now a derivative work of version 0.2.6 which includes log4j 2.17.1.
  
  • The logback-core and logback-classic libraries have been moved to version 1.2.10.

• Comply now supports Kubernetes 1.19 to 1.24. Kubernetes 1.17 and 1.18 are no longer supported.

Resolved in this release:

• **Rule details.** Fixed an bug where the last reported time stamp on the rule detail page did not recognize the user's local timezone.

• **Compliance profiles.** Corrected an issue where the default compliance profile was incorrectly assigned for Windows Server versions.

Comply 2.2.2
Released 20 January 2022

New in this release:

• **Debug mode.** You can now choose to run in debug mode to provide easier access to assessor logs.
  
  For more information, see [Run an ad hoc scan](#) on page 88.

• **CIS-CAT Pro Assessor v4.13.1.** Comply 2.2.2 includes the latest version of the CIS-CAT assessor and the following supported associated benchmarks:
  
  • AlmaLinux OS 8 v1.0.0
  • Amazon Linux 2 STIG v2.0.0
  • Apple macOS 11.0 Big Sur v2.0.0
  • Microsoft Windows Server 2012 (non-R2) v2.3.0
  • RedHat Enterprise Linux 8 STIG v1.0.0

**CIS-CAT Pro Assessor v4.13.1** resolved security vulnerabilities present in the following embedded, third party dependency:

• **log4j-core** - This library was updated to version 2.17.0.

Comply 2.2.1
Released 20 December 2021
New in this release:

**CIS-CAT Pro Assessor v4.13.0.** Comply 2.2.1 includes the latest version of the CIS-CAT assessor and the following supported associated benchmarks:

- Apple macOS 10.15 Catalina v2.0.0
- Red Hat Enterprise Linux 7 STIG v2.0.0

The following benchmark is at end of life (EOL) and is no longer supported:

- Mac OS 10.14

**Security notice:**

- **CIS-CAT Pro Assessor v4.13.0** resolved security vulnerabilities present in the following embedded, third party dependencies:
  - **log4j-core** - This library was updated to version 2.15.0.
  - **bcprov-jdk15on** - This library was updated to version 1.69.
- **Component upgrade to address CVEs.** To address various CVEs, this version includes an upgrade of Kubernetes to 1.19.15.

**Important:** Version 2.15.0 of the log4j-core library addresses the potential escalation of privilege vulnerability. We do not believe Comply is vulnerable to any of the additional risks addressed in the 2.16.0 release, but plan to release an update in the near future which includes version 2.17.0 or later.

**Comply 2.2.0**

Released 18 November 2021.

New in this release:

- **Scan Reports improvements.** Scan reporting functionality is extended to include the ability to access a list of historical scans and view scan details. For more information, see CIS scan report details on page 91.
- **Filtering and sorting.** Filtering and sorting functionality has been implemented on all table columns in the Comply UI.

**Note:** Filter drop-downs display all available options for a given parameter. On pages where multiple filtering options are available, selecting one filter option does not affect the options presented by any other filter drop-down.

- **CIS-CAT Pro Assessor v4.11.0.** Comply 2.2.0 includes the latest version of the CIS-CAT assessor and its associated benchmarks:
  - Microsoft Windows Server 2012 R2 v2.5.0
  - Microsoft Windows Server 2016 STIG v1.1.0
  - SUSE Linux 15 v1.1.0
- **Desired compliance.** The Comply UI has been simplified so that users are no longer required to manually accept the profiles applied by Comply based on fact information from PE.
- **Custom Comply port.** You can now specify a custom Comply port in Puppet Application Manager if you do not want to use the default port (30303). For more information, see System requirements on page 73.
- **Data retention.** The retention period for scan data can now be set on the Puppet Application Manager Config tab. For more information see, Scan results on page 91.

Resolved in this release:

- **Node Deletion.** A fix was added to ensure that nodes deleted in Puppet Enterprise are no longer listed in Comply as available for scanning.
- **License page node count.** Corrected an issue where the number of nodes displayed on the license page was not updated when a node was deleted in Puppet Enterprise.
• **Required installations page.** The required installations page that was part of the assessor install procedure was removed as it was no longer required.

• **Comply-graphql.** Fixed a known issue where the comply-graphql deployment did not become healthy after restoring Comply using Puppet Application Manager.

• **Rule ordering.** Corrected an issue where rules were not always displayed in the correct numerical order.

**Comply 2.1.0**

Released 7 October 2021.

New in this release:

• **Scan Reports.** The Comply UI has a new Scan Reports page that provides a report on rules passed/failed and node compliance from the most recent CIS scan. For more information, see CIS scan report details on page 91.

• **CIS-CAT Pro Assessor v4.9.0.** Comply 2.1.0 includes the latest version of the CIS-CAT assessor and its associated benchmark:
  
  • CentOS Linux 7 v3.1.2

• **Scanner upgrades.** Scanner upgrade in Comply is not forced but optional to allow better management of PE jobs.

| Note: By default in Comply 2.1.0, assessor upgrade does not happen automatically when you upgrade Comply. Assessor upgrade takes place when you instigate a Puppet Enterprise (PE) Puppet run job after Comply is upgraded. For more information, see Upgrade from Comply 2.2.2 to 2.3.0 on page 84 |

Resolved in this release:

• **Desired compliance upgrades.** Fixed an issue where Windows 10 nodes lost their desired compliance after upgrade to Compliance 2.x

• **Upgrade statistics.** Resolved an issue where statistics were overwritten when multiple upgrades take place.

• **Service start up.** Updated Comply so that it now starts when IPv6 is disabled.

• **Preflight failure.** Fixed an issue where preflight checks failed during install when trailing newline returns were present in certificates.

• **Scan wizard.** The Comply scan wizard was updated to correct an issue where the environment name field did not revert to the previous saved value if the scan set up was cancelled.

**Comply 2.0.0**

Released August 2021.

New in this release:
• **CIS-CAT Pro Assessor v4.8.2.** Comply 2.0.0 includes the latest version of the CIS-CAT assessor and its associated benchmarks:
  - Apple macOS 10.14 v1.4.0
  - Apple macOS 10.15 v1.4.0
  - Apple macOS 11.0 v1.2.0
  - CentOS Linux 7 v3.1.1
  - CentOS Linux 8 v1.0.1
  - Debian Linux 8 v2.0.2
  - Microsoft Windows Server 2019 v1.2.1
  - Microsoft Windows Server 2019 STIG v1.0.1
  - Microsoft Windows 10 20H2 v1.10.1
  - Oracle Linux 7 v3.1.1
  - Oracle Linux 8 v1.0.1
  - Red Hat Linux 7 v3.1.1
  - Red Hat Linux 8 v1.0.1
  - Amazon Linux 2 v2.0.0
  - Microsoft Windows 10 21H1 v1.11.0
  - Microsoft Windows Server 2016 v1.3.0
  - Ubuntu Linux 20.04 LTS STIG v1.0.0

• **Automatic upgrades of the CIS-CAT assessor.** Every time you upgrade your Comply application, the assessor automatically upgrades to the latest version. This update also includes the following changes to how you interact with Comply:
  - You can only run a desired compliance scan against nodes with the latest version of the assessor.
  - You can only run a custom scan against benchmarks with the latest version of the assessor.
  - On the node inventory screen, nodes without the latest assessor are highlighted red to indicate that they need upgrading.
  - You can no longer set a desired compliance benchmark against a node that does not have the latest version of the assessor.
  - When the assessor upgrades, custom profiles are automatically updated to use the new benchmarks and profiles, sending you a notification.

• **Assessor upgrades tab.** The Assessor upgrades tab on the Activity feed screen provides a summary of assessor upgrades, including the number of nodes that have passed or failed. Note that this only shows the status of your nodes after the upgrade, and does not update again, even if your nodes change to passing.

• **comply module Secure Sockets Layer (SSL).** This includes changes to how you install and upgrade the Comply module.

Resolved in this release:

• **Comply tries to install 7-zip on Windows.** The comply module no longer installs 7zip on Windows systems.

• **Windows Server Semi Annual Channel (SAC) builds are assigned the wrong CIS profile.** SAC builds are now assigned the correct Windows 2019 profile.

Security notice:

• **Vulnerability in 12.18.3-alpine image.** The release updates the alpine image to 15.13.0.

• **Vulnerability keycloak:15.0.0.** This release updates keycloak to version 15.0.0.

• **Vulnerability in dependencies.** This release upgrades NodeJS to version 14.17.1 and React to version 17.0.2.

For upgrade instructions, see Upgrade from Comply 2.2.2 to 2.3.0 on page 84.

## Comply known issues

These are the known issues for the Puppet Comply 1.x and 2.x releases.
Comply UI pages not loading correctly after an upgrade

If the Comply UI pages are not loading correctly after an upgrade, delete the `comply-graphql` and `comply-scarpy` pods and wait for Comply to automatically restart.

Session timeout in Comply 2.2.0

Comply does not redirect users to the login screen on session timeout and some screens show error messages. Reloading the page in Comply fixes this issue.

Multiple filtering options

On pages where multiple filtering options are available, selecting one filter option does not affect the options presented by any other filter drop-down. This means filter drop-downs display all available options for a given parameter and therefore invalid options may appear for a given filtering scenario.

GraphQL issue after Puppet Application Manager restore in Comply 2.1.0 or earlier

The Comply-GraphQL pod becomes stuck in CrashLoopBackOff after Comply is restored using Puppet Application Manager. This problem is due to an issue with the Hasura database used in Comply 2.1.0 or earlier. Contact Puppet support for help or upgrade to Comply 2.2.0 or later to fix.

Scan report metrics bar node count not matched in Scan Report page Nodes tab table in Comply 2.1.0

If an error occurs after a scan report is sent from PE to Comply (owing, for example, to the Comply module being out-of-date on the node), the number of nodes appearing in the Scan Report page Nodes tab table can differ from the node count that appears in the Scan report metrics bar.

Running scans on CentOS 7 with Comply 1.0.4

The CentOS 7 benchmark in Comply 1.0.4 has been updated to version 3.1.0. If you have already installed Comply and set desired compliance for your CentOS 7 nodes, you need to run the following command on your `comply-scarpy` pod to update the benchmark version from 3.0.0 to 3.1.0:

```bash
kubectl exec --stdin --tty -n <namespace> $(kubectl get pods -n dio-comply | grep comply-scarpy | awk '{print $1}') -- /bin/scarp upgrade-assessor --assessor_version '4.6.0'
```

This ensures Comply uses the latest CISCAT benchmark and profiles.

Running scan tasks in Puppet Enterprise (PE)

Comply uses PE tasks to run compliance scans on nodes. While you can see the scan task in PE, we advise against running them from here as it can have unforeseen effects on both PE and Comply. Instead, run all CIS scans from Comply. You can view the results of the scan in both products.

Beginner’s guide to Comply

Welcome to the Beginner’s guide to Comply! As a new user, you’ll need to perform some initial installation and configuration tasks, and then we’ll show you how to use the core features of Comply.

You’re just a few steps away from enforcing compliant configurations across your infrastructure. Before you begin, we recommend familiarizing yourself with our terminology and Comply overview on page 5.
Step 1: Install and configure Comply

Use the main documentation to install and configure Comply. If you've already completed these steps, proceed to step 2.

- Install Puppet Application Manager (PAM)
- Set up Comply

Related concepts
Install PAM on page 34
You can install Puppet-supported Puppet Application Manager on a single node or in an HA configuration. Both online and offline install packages are available. You can also install it on an existing Kubernetes cluster.

Set up Comply on page 73
To start using Puppet Comply, you must complete the setup process, using both Puppet Application Manager (PAM) and Puppet Enterprise (PE).

Step 2: Set desired compliance

Desired compliance is the benchmark and profile that you to assign to a particular node. It is what is scanned on that node by default. Most of the time, you only need to set this once for your nodes.

Based on fact information from PE, Comply automatically assigns an appropriate benchmark for each operating system, along with a Level 1 profile, to nodes that have not been set. Accepting this option is the quickest way to get up and running with desired compliance.

Alternatively, you can manually choose your own benchmark and profiles. For more information, see Manually set desired compliance.

Step 3: Run a CIS scan

You are now ready to run a scan.

This topic describes how to run an initial ad hoc scan.

1. In Comply, click Scans, and then Run an ad hoc scan.
2. In the Benchmark drop-down, select Desired compliance or a benchmark and profile of your choice.
   If you have not set desired compliance, see Setting desired compliance for instructions.
3. Next, select an option from the Profile drop-down. If you want to use a custom profile for this scan, select the Use an associated custom profile? option and choose the relevant option from the Custom profile drop-down.
   If you have not set desired compliance, see Setting desired compliance for instructions.
4. Click Next to review the PE credentials and environment you want the scan to run on.
5. Click **Next** to see the nodes selected for scanning.

To only scan a subset of nodes, deselect any that you do not want to include.

**Debug mode:** By default, assessor logs are set to WARN level. If you need to troubleshoot an issue you can set the logging level to DEBUG for the scan by clicking **Run in debug mode.** The assessor logs can then be retrieved from the individual node.

On Linux and macOS platforms the assessor log is located at:

```
/opt/puppetlabs/comply/Assessor-CLI/logs/assessor-cli.log
```

On Windows the assessor log is located at:

```
C:/ProgramData/PuppetLabs/comply/Assessor-CLI/logs/assessor-cli.log
```

Note that scanning in debug mode increases the size of the assessor log file significantly.

6. Click **Scan**.

You are taken to the **Activity Feed**, which lists each scan. Scans are run as a task in PE. To see the details of the job, click the job ID to be taken to PE.

**Tip:** You can also run a scan by clicking the **Scan nodes** button at the top right corner on several pages. This option uses the nodes listed on the page you are currently viewing.

7. In Comply, navigate to the **Dashboard** page to see the results of your scan.

See **Viewing scan results** for a description of the scan data.

Congratulations! You've completed the Beginner’s guide to Comply. You're now familiar with the core features and know how to run CIS scans with Comply. To find out how you can enforce and automate CIS benchmarks on your failing nodes, see **Enforce CIS benchmarks** on page 93.

**Related information**

**Enforce CIS benchmarks** on page 93

Puppet Comply provides visibility into your compliance status, but it cannot fix your failing nodes. Instead, you can use Puppet’s Compliance Enforcement Modules (CEM).

**Custom profiles** on page 87

A custom profile is a benchmark profile that you customize to fit your organization's internally defined standards.

**Desired compliance** on page 86

Set your desired compliance. This is the benchmark and profile that you assign to a particular node and which is scanned on that node by default. Generally, you only need to set this once for your nodes.

---

**Puppet Application Manager**

Before you can begin using Puppet Comply, you must install Puppet Application Manager. Puppet Application Manager is an administrative console that provides tools for managing Comply and other Puppet applications.

**Note:** Puppet Application Manager was previously called the platform admin console in the Comply documentation.

**What does Puppet Application Manager do?**

The Puppet Application Manager installation process sets up a managed Kubernetes cluster (or, if you prefer, adds Puppet Application Manager to your existing cluster). Comply runs on this Kubernetes cluster, and Puppet Application Manager manages the cluster for you.

In the Puppet Application Manager UI, you can configure Comply, monitor the cluster’s activity, upgrade to the latest version of the software, and back up your installation.
How do I use Puppet Application Manager to deploy Comply?

Once the cluster is ready, upload your Comply license and provide any needed configuration details about your installation in the Puppet Application Manager UI. You can then deploy the latest version of Comply with one click whenever you're ready.

- Welcome to Puppet Application Manager (PAM) on page 14
  Puppet Application Manager is an administrative console where you can install, access, and manage your Puppet applications. It is also where you can go to access upgrades to new Puppet applications releases.

- PAM UI on page 19
  The Puppet Application Manager (PAM) UI provides administration functionality where you can access and manage your Puppet applications.

- Architecture overview on page 20
  Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

- PAM system requirements on page 23
  You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

- Install PAM on page 34
  You can install Puppet-supported Puppet Application Manager on a single node or in an HA configuration. Both online and offline install packages are available. You can also install it on an existing Kubernetes cluster.

- Working with Puppet applications on page 54
  You can install and upgrade Puppet using the Puppet Application Manager UI.

- Maintenance and tuning on page 57
  Follow these guidelines when you're tuning or performing maintenance on a node running Puppet Application Manager (PAM).

- Upgrading PAM on a Puppet-supported cluster on page 58
  Upgrade Puppet Application Manager (PAM) on a Puppet-supported cluster to take advantage of new features and bug fixes, and to upgrade your cluster to the latest version of Kubernetes when one is available.

- Upgrading PAM on a customer-supported cluster on page 62
  Upgrade Puppet Application Manager (PAM) on your own Kubernetes cluster to take advantage of new features and bug fixes.

- Backing up PAM using snapshots on page 63
  Snapshots are point-in-time backups of your Puppet Application Manager (PAM) deployment, which can be used to roll back to a previous state or restore your installation into a new cluster for disaster recovery.

- Troubleshooting PAM on page 68
  Use this guide to troubleshoot issues with your Puppet Application Manager installation.

Welcome to Puppet Application Manager (PAM)

Puppet Application Manager is an administrative console where you can install, access, and manage your Puppet applications. It is also where you can go to access upgrades to new Puppet applications releases.

Useful links:
Release notes

PAM release notes

These are the new features, enhancements, resolved issues, and deprecations for Puppet Application Manager. Follow the instructions in Upgrading Puppet Application Manager to get the current version.

12 April 2022 (Puppet Application Manager 1.68.0)

New in this release:

- **Install a specific version of an application.** When installing a Puppet application using the automated installation method, you now have the option to specify the application's version by passing the `--app-version-label=<version>` flag to the `kubectl kots install` command. For more information, go to Automate PAM and Puppet application online installations on page 49.
- **Status reporting improvements.** The status reporting tools can now detect when an application is being upgraded.
- **Component upgrades to address CVEs.** To address various CVEs in Envoy, this version includes an upgrade of Project Contour to version 1.20.1.
- **Other component upgrades.** This version includes an upgrade of KOTS to version 1.68.0.

Resolved in this release:

- During image garbage collection, images still in use by the cluster are no longer in danger of being deleted from the private registry in a Kubernetes installer-created cluster.

1 March 2022 (Puppet Application Manager 1.64.0)

Resolved in this release:

- Diffs are now shown correctly in the PAM UI.
- The OpenSSL package is no longer a prerequisite for successful installation on newer Red Hat Enterprise Linux 7 systems.
- You can now successfully install Puppet Application Manager on Red Hat Enterprise Linux 8 systems without the need to force-install the kurl-local audit-libs library.

© 2021 Puppet, Inc.
17 February 2022 (Puppet Application Manager 1.62.0)

**Important:** Version 1.0.2 of the puppetlabs/pam_firewall module is now available. To avoid conflicts, upgrade the module **before** upgrading Puppet Application Manager to version 1.62.0.

New in this release:

- **Kubernetes version upgrade.** For standalone and HA installations, this version includes an upgrade of Kubernetes to version 1.21.8.

  **Important upgrade information:** The upgrade process takes place on all nodes, and first upgrades Kubernetes to version 1.20 before upgrading to version 1.21.8. For a three-node cluster, you can expect the upgrade process to take around an hour. Confirmations are required during the upgrade process.

For legacy installations (installed before May 2021), this version includes an upgrade of Kubernetes to version 1.19.15.

- **Prometheus enabled on standalone architecture.** Beginning with version 1.62.0 Prometheus is enabled by default on all new and existing standalone Puppet Application Manager installations. Prometheus requires an additional 350m CPU and 500MiB of memory, so ensure your system is properly sized before upgrading. Prometheus is an optional component; if you need to disable it to conserve resources, see Optional components on page 71.

- **Automatic certificate rotation.** By default, the self-signed certificates used by Project Contour and Envoy expire after one year. This version includes an update that auto-rotates those certificates before they expire.

- **Component upgrades to address CVEs.** To address various CVEs, this version includes an upgrade of containerd to version 1.4.12.

- **Other component upgrades.** This version includes an upgrade of KOTS to version 1.62.0.

Deprecated in this release:

- **Legacy architecture.** The legacy architecture, which was the version of Puppet Application Manager available for installation prior to May 2021, is now deprecated. (See How to determine your version of Puppet Application Manager if you need to confirm whether you're running the legacy architecture.) The legacy architecture utilizes Rook 1.0, which is incompatible with Kubernetes version 1.20 and newer versions. Kubernetes version 1.19 is no longer receiving security updates. Puppet will continue to update legacy architecture components other than Kubernetes until 30 June 2022. If security advisories against Kubernetes 1.19 arise, the remediation path is to migrate to one of the newer architectures by following the instructions in Disaster recovery or migration using a snapshot on page 66.

  **Important:** Before beginning the migration process from a legacy deployment you must upgrade to PAM version 1.62.0 with the force-reapply-addons flag included in the upgrade command. Find upgrade instructions at PAM legacy upgrades on page 60 and PAM offline legacy upgrades on page 61.

30 November 2021 (Puppet Application Manager 1.56.0)

This release includes an upgrade of KOTS to version 1.56.0, which adds the following improvements:

- **Improved support bundles:** Adds an option to upload a support bundle directly from Puppet Application Manager.

- **Improved troubleshooting:** Adds detailed information on failing pods to the Troubleshoot tab.

6 October 2021 (Puppet Application Manager 1.52.1)

New in this release:

- **Improved statuses.** More granular status levels are now available from the Application tab.
• **Component upgrades to address CVEs.** To address various CVEs, this version includes an upgrade of Kubernetes to 1.19.15.

• **Other component upgrades.** This version includes an upgrade of KOTS to version 1.52.1.

Resolved in this release:

• Generating a support bundle no longer results in unusually high memory use.

• Preflight check logs post to info level for progress messages and to error level for error messages.

**25 August 2021 (Puppet Application Manager 1.49.0)**

New in this release:

• **Component upgrades to address CVEs.** To address various CVEs, this version includes an upgrade of Kubernetes to 1.19.13, an upgrade of Project Contour to 1.18.0, and an upgrade of Velero to 1.6.2.

• **Goldpinger.** High availability architectures now include Goldpinger, which aids the debugging of network issues.

• **containerd upgrade.** This version includes an upgrade of containerd to version 1.4.6, and removes the need to use the `force-reapply-addons` option when upgrading.

• **Other component upgrades.** This version includes an upgrade of KOTS to version 1.49.0, an upgrade of ekco to 0.11.0, an upgrade of Prometheus to 0.49.0, and an upgrade of Rook to 1.5.12.

**30 June 2021 (Puppet Application Manager 1.44.1)**

New in this release:

• **Certificate auto-rotation for standalone architecture.** Certificates are now automatically rotated for the Kubernetes API and Puppet Application Manager UI in the standalone architecture. With this change, certificate auto-rotation is now supported in all Puppet Application Manager architectures.

• **Rook upgrades.** This version includes an upgrade of Rook in the high availability architecture to 1.5.11 and the version of Rook in the legacy architecture to 1.0.4-14.2.21. These upgrades address a vulnerability in Ceph components (CVE-2021-20288).

• **Prometheus upgrade.** This version includes an upgrade of Prometheus in the high availability and legacy architectures to 0.48.1. Additionally, Prometheus disk usage is now limited in order to preserve the storage space required for the usage charts on the Application tab.

• **Other component upgrades.** This version includes an upgrade of KOTS to version 1.44.1, an upgrade of Project Contour to version 1.15.1, and an upgrade of Weave to version 2.8.1.

Resolved in this release:

• Snapshots can now successfully use the Other S3-Compatible Storage option as the storage destination.

To apply this update, add the `force-reapply-addons` option during upgrade. For example:

```
curl <url> | bash -s force-reapply-addons
```

**26 May 2021**

New in this release:

• **runC.** The version of runC has been upgraded to v1.0.0-rc95 to address CVE-2021-30465.

Known issues in this release:

• Running the KOTS installer with the `airgap` and `kurl-registry-ip` flags results in an error.

  As a workaround (if you do not have any applications already installed in the cluster), delete the registry service, recreate the registry service IP and then re-run the installation script with the `kurl-registry-ip` flag.

**10 May 2021 (Puppet Application Manager 1.40.0)**

New in this release:
• Distinct architectures for standalone and high availability deployments of the Puppet Application Manager platform. Standalone supports lower system requirements and resolves inherent flaws in using Ceph on a single node. High availability uses an updated version of Rook for faster, more reliable distributed storage.

| Note: | It is not possible currently to upgrade to these architectures from existing installations. However, migrating applications between them is on the roadmap for a future release. |

• The previous architecture is maintained as the legacy configuration. This version includes an upgrade of Kubernetes to 1.19.10; this upgrade process upgrades through Kubernetes 1.18, and happens on all nodes. It can take ~1 hour to do for a 3-node cluster, and requires confirmations during that period. It also includes an upgrade of Project Contour to version 1.14.1, adds Metrics Server 0.4.1, an upgrade of ekco to 0.10.1, and an upgrade of Prometheus to 2.26.0.

For more information on legacy upgrades, see PAM legacy upgrades on page 60.

15 April 2021 (Puppet Application Manager 1.38.0)

New in this release:

• **Snapshots.** Puppet Application Manager now supports full (instance-level) snapshots, which can be used for application rollbacks and disaster recovery. For more information, see Backing up Puppet Application Manager using snapshots.

• **Component upgrades.** This version includes an upgrade of KOTS to version 1.38.0.

17 February 2021 (Puppet Application Manager 1.29.3)

New in this release:

• **Support for Ubuntu 20.04.** You can now run Puppet Application Manager on Ubuntu 20.04.

• **Component upgrades.** This version includes an upgrade of Prometheus to version 2.22.1 and Prometheus Operator to version 0.44.1, an upgrade of KOTS to version 1.29.3, an upgrade of Project Contour to version 1.12.0, and an upgrade of ekco to version 0.10.0.

3 February 2021 (Puppet Application Manager 1.29.2)

New in this release:

• **Component upgrades.** This version includes an upgrade of KOTS to version 1.29.2, an upgrade of Project Contour to version 1.11.0, and an upgrade of containerd to version 1.4.3.

Resolved in this release:

• During their initial preflight checks, new installations now pull images successfully and no longer report a Failed to pull image error.

7 December 2020

New in this release:

• **Support for Red Hat Enterprise Linux (RHEL) 8 and CentOS 8.** You can now run Puppet Application Manager on RHEL version 8 and CentOS version 8. To support this change, containerd is now used independently of Docker during the installation process.

• **Component upgrades.** This version includes an upgrade of Kubernetes to version 1.17.13.

Related information

Upgrading PAM on a Puppet-supported cluster on page 58

Upgrade Puppet Application Manager (PAM) on a Puppet-supported cluster to take advantage of new features and bug fixes, and to upgrade your cluster to the latest version of Kubernetes when one is available.

Backing up PAM using snapshots on page 63

Snapshots are point-in-time backups of your Puppet Application Manager (PAM) deployment, which can be used to roll back to a previous state or restore your installation into a new cluster for disaster recovery.

© 2021 Puppet, Inc.
Known issues

These are the known issues for Puppet Application Manager (PAM).

**Velero fails if network file system (NFS) snapshot storage is misconfigured**

In Puppet Application Manager version 1.64.0 and newer versions, changes to the configuration of snapshot storage on a network file system (NFS) is appended to Velero containers, rather than replaced. This means that if NFS snapshot storage is misconfigured, attempts to fix the configuration do not correct the problem. This issue manifests as a failure of Velero to start up.

**Installations fail on RHEL 8 systems**

Due to a conflict with the audit-libs library, installations of Puppet Application Manager version 1.62.0 or older fail on Red Hat Enterprise Linux 8 systems. To work around this issue, force installation of the kurl-local audit-libs library version by running `sudo yum install audit-libs-3.0-0.17.20191104git1c2f876.el8.1 --allowerasing`.

**OpenSSL package required for newer RHEL 7 systems**

Attempts to install Puppet Application Manager version 1.62.0 or older on newer Red Hat Enterprise Linux (RHEL) 7 systems fail unless the OpenSSL package is present on the system before installation. To work around this issue, run `yum install openssl` and then re-run the PAM installation script.

**Package updates with yum or DNF fail after upgrading PAM**

If you are unable to run `yum update` or `dnf upgrade` after a PAM upgrade, run one of the following commands to clean up a temporary module added by PAM:

```bash
yum module reset kurl.local
```

or

```bash
dnf module reset kurl.local
```

---

**PAM UI**

The Puppet Application Manager (PAM) UI provides administration functionality where you can access and manage your Puppet applications.

**PAM console menu**

Use the console menu at the top of the Puppet Application Manager UI to manage Puppet Application Manager itself. It has three tabs of interest to us:

- Use the **Dashboard** tab to:
  - Manage your applications
  - See version history
  - Set application configuration settings
  - Access support bundles for troubleshooting
  - Manage licenses
  - View files
  - Configure registry settings
- Use the **Cluster Management** tab to view current information on the nodes in your cluster. You can also use this tab to drain, and add nodes to your cluster.
• Use the Snapshots tab to create point-in-time backups of your deployment, which can be used to roll back to a previous state, or restore your installation into a new cluster for disaster recovery. For more information, see Backing up PAM using snapshots.

You can also use the console menu to Add a new application and to log out of Puppet Application Manager.

Application monitoring graphs

When you have Prometheus installed, the Dashboard tab has an Application sub-tab that provides several simplified graphs for tracking overall health of the system.

• Node CPU Usage (%) shows when hosts are getting overwhelmed (high % usage).
• Node Memory Usage (%) shows when hosts are reaching full memory capacity that may result in processes being killed due to out-of-memory errors.
• Node Available Storage (%) shows when hosts are running out of storage. At 15%, pods may start to be evicted or reads/writes on databases are paused until more storage is made available.
• Volume Available Storage (%) shows when application persistent volumes are getting full (low %) that may lead to problems with a particular application. Note that -

| Note: As of the 30 June 2021 Puppet Application Manager release, the monitoring/Prometheus-Kubernetes pods limit their storage use and are expected to never fall below 10% available storage. |

Puppet Application Manager HA architectures include Prometheus and Grafana. Metrics about how the system is working are sent to Prometheus, and can be displayed with Grafana. Grafana credentials are printed during install, or can be retrieved later with the following command:

```
kubectl -n monitoring get secret grafana-admin -o go-template='{{index .data "admin-user"|base64decode}}:{{index .data "admin-password"|base64decode}}'
```

Related information

Backing up PAM using snapshots on page 63

Snapshots are point-in-time backups of your Puppet Application Manager (PAM) deployment, which can be used to roll back to a previous state or restore your installation into a new cluster for disaster recovery.

Architecture overview

Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

Puppet Application Manager can run on Puppet-supported or customer-supported Kubernetes clusters. For more information on installing on a customer-supported Kubernetes cluster, see Install Puppet applications using Puppet Application Manager and an existing Kubernetes cluster.

| Note: This architecture overview deals with Puppet-supported deployments only. |

Terminology

Throughout this documentation, we use a few terms to describe different roles nodes can take:

• Primary - A primary node runs core Kubernetes components (referred to as the Kubernetes control plane) as well as application workloads. At least three primaries are required to support high availability for Puppet Application Manager. These are also sometimes referred to as masters.
• Secondary - A secondary node runs application workloads. These are also sometimes referred to as workers.

Puppet Application Manager is built on the KOTS (Kubernetes off-the-Shelf) project, and we occasionally use its CLI tools (kubectl, kots) to manage the installation.
Standalone architecture

Standalone is optimized for limited resources, storing data directly on disk. If you need to remove optional components like Prometheus and Grafana to decrease resource utilization, see Optional components on page 71. While additional compute capacity can be added through secondary nodes, this does not provide increased resilience as data is only stored on the node where a component service runs.

For information on migrating data from standalone to HA deployments, see Disaster recovery or migration using a snapshot on page 66.

HA architecture

A high availability (HA) architecture provides high availability for scheduling application services during failure and uses Ceph for distributed storage in case of node failure. Individual applications may still experience some loss of availability (up to 10 minutes) if individual services do not have replicas and need to be rescheduled. For more information, see Reduce recovery time when a node fails. An HA implementation requires a cluster of three primary nodes. Additional compute capacity can be added through secondary nodes.

The HA architecture installs Prometheus and Alertmanager. These are used to provide system monitoring in the Puppet Application Manager UI. Prometheus and Alertmanager are unauthenticated on ports 30900 and 30903, and you are recommended to control access to these ports via firewall rules. For information on how to remove Prometheus and Alertmanager, see Optional components on page 71.

Puppet Application Manager architectures

The following outline some of the core components involved in standalone and HA architectures, and how they communicate.

Note: A complete list of the ports used by Puppet Application Manager is available in the #unique_29/unique_29_Connect_42_pam-port-reqs section of the system requirements documentation.
**Internal ports**

All backplane ports may also be used for inter-process communication within a single host.

The following ports are only used within a single host for inter-process communication:
- TCP 6781, 6782, 6784 (Weave)

---

**Workers**

Secondaries can be added later to add capacity to the cluster.

---

**Control plane**

Three primaries that can also run application workloads.

---

© 2021 Puppet, Inc.
For information on setting up health checks for your load balancer, see Load balancer health checks on page 58

DEPRECATED: Legacy architecture

**Note:** The legacy architecture utilizes Rook 1.0, which is incompatible with Kubernetes version 1.20 and newer versions. Kubernetes version 1.19 is no longer receiving security updates. Puppet will continue to update legacy architecture components other than Kubernetes until **30 June 2022**. If security advisories against Kubernetes 1.19 arise, the remediation path is to migrate to one of the newer architectures by following the instructions in Disaster recovery or migration using a snapshot on page 66.

The Puppet Application Manager legacy architecture reflects an older configuration that used Ceph 1.0 which hosted data directly on the file system. Puppet no longer recommend this for new installs, but maintains it to support existing installs and ensure other components can be kept up-to-date.

The legacy architecture installs Prometheus and Alertmanager. These are used to provide system monitoring in the Puppet Application Manager UI. Prometheus and Alertmanager are unauthenticated on ports 30900 and 30903, and you are recommended to control access to these ports via firewall rules. For information on how to remove Prometheus and Alertmanager, see Optional components on page 71.

For information on upgrading to a newer version of the legacy architecture, see PAM legacy upgrades on page 60 and PAM offline legacy upgrades on page 61.

For information on migrating data from a legacy architecture to a standalone or HA architecture, see Disaster recovery or migration using a snapshot on page 66.

**Related information**

Reduce recovery time when a node fails on page 70
If a node running a non-replicated service like PostgreSQL fails, expect some service downtime.

Install Puppet applications using PAM on a customer-supported Kubernetes cluster on page 35
Use these instructions to install Puppet Application Manager and any Puppet applications on an existing Kubernetes cluster.

PAM legacy upgrades on page 60
Use this method to upgrade Puppet Application Manager (PAM) from a version installed before May 2021.

PAM offline legacy upgrades on page 61
Use this method to upgrade Puppet Application Manager (PAM) on offline nodes from a version installed before April 2021.

Troubleshooting PAM on page 68
Use this guide to troubleshoot issues with your Puppet Application Manager installation.

---

**PAM system requirements**

You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

**Customer-supported cluster hardware requirements**

The following Kubernetes distributions are supported:

- Google Kubernetes Engine
- AWS Elastic Kubernetes Service
- Red Hat OpenShift

If you use a different distribution, contact Puppet Support for more information on compatibility with PAM.

Application requirements:
<table>
<thead>
<tr>
<th>Application</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Ports</th>
<th>Note:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Delivery for Puppet Enterprise (PE)</td>
<td>3 CPU</td>
<td>8 GB</td>
<td>280 GB</td>
<td>Ingress, NodePort 8000</td>
<td>NodePort is configurable</td>
</tr>
<tr>
<td>Puppet Comply</td>
<td>6 CPU</td>
<td>6 GB</td>
<td>35 GB</td>
<td>Ingress, NodePort 30303</td>
<td>NodePort is configurable</td>
</tr>
</tbody>
</table>

Make sure that your Kubernetes cluster meets the minimum requirements:

- Kubernetes version 1.17-1.21.
- A default storage class that can be used for relocatable storage.
- A standard Ingress controller that supports websockets (we have tested with Project Contour and NGINX).
- We currently test and support Google Kubernetes Engine (GKE) clusters.

**Cluster ports**

In addition to the NodePorts used by your Puppet applications, make sure that TCP port 443 is open for your ingress controller.

**Puppet-supported HA cluster hardware requirements**

A high availability (HA) configuration uses multiple servers to provide availability in the event of a server failure. A majority of servers must be available to preserve service availability. Below are suggested configurations for each application.

**Continuous Delivery for Puppet Enterprise (PE)**

Three servers (referred to as primaries during installation) with the following minimum requirements:

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 CPU</td>
<td>10 GB</td>
<td>100 GB on an unformatted storage device</td>
<td>TCP: 80, 443, 2379, 2380, 6443, 6783, 8000, 8800, and 10250</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An additional 100 GB for /var/lib. This is primarily divided among:</td>
<td>UDP: 6783, 6784</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 GB for /var/lib/etcd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10 GB for /var/lib/rook (plus buffer)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 32 GB for /var/lib/kubelet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** The storage backend prefers the file system inhabited by /var/lib/rook to remain below 70% utilization.

SSDs (or similarly low-latency storage) are recommended for /var/lib/etcd and /var/lib/rook.
Puppet Comply

Three servers (referred to as primaries during installation) with the following minimum requirements:

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 CPU</td>
<td>9 GB</td>
<td>100 GB on an unformatted storage device</td>
<td>TCP: 80, 443, 2379, 2380, 6443,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An additional 100 GB for /var/lib. This is primarily divided among:</td>
<td>6783, 8800, 10250, and 30303</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 GB for /var/lib/etcd</td>
<td>UDP: 6783, 6784</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10 GB for /var/lib/rook (plus buffer)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 32 GB for /var/lib/kubelet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The storage backend prefers the file system inhabited by /</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>var/lib/rook to remain below 70% utilization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSDs (or similarly low-latency storage) are recommended for /</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>var/lib/etcd and /var/lib/rook.</td>
<td></td>
</tr>
</tbody>
</table>

Continuous Delivery for Puppet Enterprise (PE) and Puppet Comply

Three servers (referred to as primaries during installation) with the following minimum requirements:

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 CPU</td>
<td>12 GB</td>
<td>150 GB on an unformatted storage device</td>
<td>TCP: 80, 443, 2379, 2380, 6443,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>An additional 100 GB for /var/lib. This is primarily divided among:</td>
<td>6783, 8000, 8800, 10250, and</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 GB for /var/lib/etcd</td>
<td>30303</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10 GB for /var/lib/rook (plus buffer)</td>
<td>UDP: 6783, 6784</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 32 GB for /var/lib/kubelet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The storage backend prefers the file system inhabited by /</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>var/lib/rook to remain below 70% utilization.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SSDs (or similarly low-latency storage) are recommended for /</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>var/lib/etcd and /var/lib/rook.</td>
<td></td>
</tr>
</tbody>
</table>
For a detailed example of an HA configuration running Continuous Delivery for PE and Puppet Comply, see [Example of an HA cluster that supports CDPE and Comply](#).

### Networking requirements

Gigabit Ethernet (1GbE) and a latency of less than 10 milliseconds (ms) between cluster members is sufficient for most deployments. For more information on networking for specific Puppet Application Manager components, see the documentation for Ceph, and etcd.

### Cluster port requirements

Puppet Application Manager (PAM) uses the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Puppet application ports</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Web UI (Relies on Server Name Indication to route requests to the application)</td>
<td>Browser</td>
</tr>
<tr>
<td><strong>Continuous Delivery for Puppet Enterprise (PE)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8000</td>
<td>TCP</td>
<td>Webhook service</td>
<td>Source control</td>
</tr>
<tr>
<td><strong>Puppet Comply</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30303</td>
<td>TCP</td>
<td>Communication with Puppet Enterprise (PE)</td>
<td>PE instance</td>
</tr>
<tr>
<td><strong>Platform ports</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2379</td>
<td>TCP</td>
<td>High availability (HA) communication</td>
<td>etcd on the Kubernetes host</td>
</tr>
<tr>
<td>2380</td>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6443</td>
<td>TCP</td>
<td>Kubernetes API</td>
<td>Admin workstation</td>
</tr>
<tr>
<td>6783</td>
<td>TCP/UDP</td>
<td>Kubernetes networking - Weave</td>
<td>Kubernetes host</td>
</tr>
<tr>
<td>6784</td>
<td>UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8800</td>
<td>TCP</td>
<td>Puppet Application Manager</td>
<td>Admin browser</td>
</tr>
<tr>
<td>10250</td>
<td>TCP</td>
<td>Kubernetes cluster management</td>
<td>Kubernetes host</td>
</tr>
</tbody>
</table>

### IP address range requirements

**Important:** Puppet Application Manager must be installed on nodes with static IP assignments because IP addresses cannot be changed after installation.

Ensure that IP address ranges `10.96.0.0/22` and `10.32.0.0/22` are locally accessible. See [Resolve IP address range conflicts](#) for instructions.

**Note:** The minimum size for CIDR blocks used by PAM are:

- `/23` for pod and service CIDRs
- Default of `/22` is recommended to support future expansion

### Antivirus and antimalware considerations

Antivirus and antimalware software can impact PAM and its applications or prevent them from functioning properly. To avoid issues, exclude the following directories from antivirus and antimalware tools that scan disk write operations:
Firewall modules

If you use the puppetlabs/firewall module to manage your cluster's firewall rules with Puppet, be advised that purging unknown rules from changes breaks Kubernetes communication. To avoid this, apply the puppetlabs/pam_firewall module before installing Puppet Application Manager.

If you've already installed PAM, apply the pam_firewall module and then restart the kube-proxy service to recreate its iptables rules by running the following on a primary:

```
systemctl restart kubelet
kubect1 -n kube-system delete pod -l k8s-app=kube-proxy
kubect1 -n kube-system delete pod -l name=weave-net
```

For more information, see the PAM firewall module.

Supported operating systems

Puppet Application Manager and the applications it supports can be installed on these operating systems:

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Amazon Linux</td>
<td>2</td>
</tr>
<tr>
<td>CentOS</td>
<td>7.4, 7.5, 7.6, 7.7, 7.8, 7.9</td>
</tr>
<tr>
<td></td>
<td>8.1, 8.2, 8.3, 8.4</td>
</tr>
<tr>
<td>Oracle Linux</td>
<td>7.4, 7.5, 7.6, 7.7, 7.8, 7.9</td>
</tr>
<tr>
<td></td>
<td>8.0, 8.1, 8.2, 8.3, 8.4, 8.5</td>
</tr>
<tr>
<td>Red Hat Enterprise Linux (RHEL)</td>
<td>7.4, 7.5, 7.6, 7.7, 7.8, 7.9</td>
</tr>
<tr>
<td></td>
<td>8.1, 8.2, 8.3, 8.4, 8.5</td>
</tr>
<tr>
<td>Ubuntu (General availability kernels)</td>
<td>16.04</td>
</tr>
<tr>
<td></td>
<td>18.04</td>
</tr>
<tr>
<td></td>
<td>20.04</td>
</tr>
</tbody>
</table>

Puppet-supported standalone hardware requirements

Here are the suggested configurations for standalone installations.
### Continuous Delivery for Puppet Enterprise (PE)

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 CPU</td>
<td>8 GB</td>
<td>130 GB for /var/lib and /var/openebsThis is primarily divided among:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 GB for /var/lib/etcd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 32 GB for /var/lib/kubelet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 50 GB for /var/openebs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP: 80, 443, 2379, 2380, 6443, 6783, 8000, 8800, and 10250</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP: 6783, 6784</td>
<td></td>
</tr>
</tbody>
</table>

### Puppet Comply

<table>
<thead>
<tr>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 CPU</td>
<td>6 GB</td>
<td>130 GB for /var/lib and /var/openebsThis is primarily divided among:</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2 GB for /var/lib/etcd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 32 GB for /var/lib/kubelet</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 50 GB for /var/openebs</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TCP: 80, 443, 2379, 2380, 6443, 6783, 8800, 10250, and 30303</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>UDP: 6783, 6784</td>
<td></td>
</tr>
</tbody>
</table>

### Cluster port requirements

Puppet Application Manager uses the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puppet application ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Web UI (Relies on Server Name Indication to route requests to the application)</td>
<td>Browser</td>
</tr>
<tr>
<td>8000</td>
<td>TCP</td>
<td>Webhook service</td>
<td>Source control</td>
</tr>
<tr>
<td>Puppet Comply</td>
<td>TCP</td>
<td>Communication with Puppet Enterprise</td>
<td>PE instance</td>
</tr>
<tr>
<td>30303</td>
<td>TCP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform ports</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6443</td>
<td>TCP</td>
<td>Kubernetes API</td>
<td>Admin workstation</td>
</tr>
<tr>
<td>6783</td>
<td>TCP/ UDP</td>
<td>Kubernetes networking - Weave</td>
<td>Kubernetes host</td>
</tr>
<tr>
<td>6784</td>
<td>UDP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8800</td>
<td>TCP</td>
<td>Puppet Application Manager</td>
<td>Admin browser</td>
</tr>
</tbody>
</table>
IP address range requirements

**Important:** Puppet Application Manager must be installed on nodes with static IP assignments because IP addresses cannot be changed after installation.

Ensure that IP address ranges 10.96.0.0/22 and 10.32.0.0/22 are locally accessible. See Resolve IP address range conflicts for instructions.

**Note:** The minimum size for CIDR blocks used by PAM are:

- /24 for pod and service CIDRs
- Default of /22 is recommended to support future expansion

Antivirus and antimalware considerations

Antivirus and antimalware software can impact PAM and its applications or prevent them from functioning properly. To avoid issues, exclude the following directories from antivirus and antimalware tools that scan disk write operations:

- /var/openebs
- /var/lib/kubelet
- /var/lib/containerd

Firewall modules

If you use the puppetlabs/firewall module to manage your cluster's firewall rules with Puppet, be advised that purging unknown rules from changes breaks Kubernetes communication. To avoid this, apply the puppetlabs/pam_firewall module before installing Puppet Application Manager.

If you've already installed PAM, apply the pam_firewall module and then restart the kube-proxy service to recreate its iptables rules by running the following on a primary:

```
systemctl restart kubelet
kubectl -n kube-system delete pod -l k8s-app=kube-proxy
kubectl -n kube-system delete pod -l name=weave-net
```

For more information, see the PAM firewall module.

Detailed hardware requirements

For additional compute capacity, you can horizontally scale HA and standalone architectures by adding secondary nodes. During installation, only add secondaries after setting up all primaries.

You can add secondaries to HA and standalone architectures; however in standalone architectures, secondaries do not increase availability of the application, and data storage services are pinned to the host they start on and cannot be moved.

Here are the baseline requirements to run cluster services on primaries and secondaries. Any Puppet applications require additional resources on top of these requirements.
### Node type

<table>
<thead>
<tr>
<th>Node type</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Open ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>4 CPU</td>
<td>7 GB</td>
<td>At least 50 GB on an unformatted storage device in addition to application-specific storage (below) for the Ceph storage backend. This can be satisfied by multiple devices if more storage is needed later, but should be balanced across primaries. An additional 100 GB for /var/lib. This is primarily divided among: * 2 GB for /var/lib/etcd * 10 GB for /var/lib/rook (plus buffer) * 32 GB for /var/lib/kubelet * 40 GB for /var/lib/containerd</td>
<td>TCP: 80, 443, 2379, 2380, 6443, 6783, 8800, and 10250 UDP: 6783, 6784</td>
</tr>
<tr>
<td>Secondary</td>
<td>1 CPU</td>
<td>1.5 GB</td>
<td>80 GB for /var/lib. This is primarily divided among: * 32 GB for /var/lib/kubelet * 40 GB for /var/lib/containerd</td>
<td></td>
</tr>
</tbody>
</table>

**Note:** Ceph storage backend prefers the file system inhabited by /var/lib/rook to remain below 70% utilization. SSDs (or similarly low-latency storage) are recommended for /var/lib/etcd and /var/lib/rook.

Applications are composed of multiple smaller services, so you can divide CPU and memory requirements across multiple servers. The listed ports can be accessed from all primaries and secondaries, but only need to be exposed on nodes you include in your load balancer. Apply application-specific storage to all primary nodes.

Application-specific requirements:

<table>
<thead>
<tr>
<th>Application</th>
<th>CPU</th>
<th>Memory</th>
<th>Storage</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Delivery for Puppet Enterprise (PE)</td>
<td>3 CPU</td>
<td>8 GB</td>
<td>50 GB</td>
<td>80, 443, 8000</td>
</tr>
<tr>
<td>Puppet Comply</td>
<td>6 CPU</td>
<td>6 GB</td>
<td>50 GB</td>
<td>80, 443, 30303</td>
</tr>
</tbody>
</table>

The minimum recommended size for a secondary node is 4 CPU and 8 GB of memory to allow some scheduling flexibility for individual services.
Example of an HA cluster capable of running Continuous Delivery for PE and Comply

An HA cluster capable of running both Continuous Delivery for Puppet Enterprise (PE) and Puppet Comply requires 9 CPU and 14 GB of application-specific memory in addition to per-node baselines. You can create a cluster from 4 CPU, 8 GB nodes. Each primary uses all CPU and 7 GB of memory for cluster services, providing 0 CPU and 1 GB of memory for application workloads; each secondary uses 1 CPU and 1.5 GB of memory for cluster services, providing 3 CPU and 6.5 GB of memory for application workloads. Create the cluster as follows:

- Three primaries provide an excess of 3 GB of memory for application workloads. Each primary must have 150 GB of storage in an unformatted, unpartitioned storage device for Ceph and 100 GB of storage for /var/lib.
- Three secondaries provide an excess of 9 CPU and 19.5 GB of memory for application workloads. Each secondary must have 80 GB of storage for /var/lib.
This diagram illustrates the suggested three-node configuration for a cluster capable of running Continuous Delivery for Puppet Enterprise (PE) and Puppet.
Web URL and port requirements for firewalls

Puppet Application Manager interacts with external web URLs for a variety of installation, configuration, upgrade, and deployment tasks. Puppet Application Manager uses the following web URLs for internal and outbound network traffic.

<table>
<thead>
<tr>
<th>Category</th>
<th>URLs</th>
</tr>
</thead>
</table>
| Puppet Application Manager and platform | • get.replicated.com  
|                                  | • registry.replicated.com  
|                                  | • proxy.replicated.com  
|                                  | • api.replicated.com  
|                                  | • k8s.kurl.sh  
|                                  | • kurl-sh.s3.amazonaws.com  
|                                  | • replicated.app  
|                                  | • registry-data.replicated.com                                   |
| Container registries             | • gcr.io  
|                                  | • docker.io  
|                                  | • index.docker.io  
|                                  | • registry-1.docker.io  
|                                  | • auth.docker.io  
|                                  | • production.cloudflare.docker.com  
|                                  | • quay.io                                                      |
| Puppet Enterprise                | • pup.pt  
|                                  | • forgeapi.puppet.com  
|                                  | • pm.puppetlabs.com  
|                                  | • amazonaws.com  
|                                  | • s3.amazonaws.com  
|                                  | • rubygems.org                                                   |

Supported browsers

The following browsers are supported for use with the Puppet Application Manager UI:
<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Current version as of release</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Current version as of release</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Current version as of release</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>Current version as of release</td>
</tr>
</tbody>
</table>

### Install PAM

You can install Puppet-supported Puppet Application Manager on a single node or in an HA configuration. Both online and offline install packages are available. You can also install it on an existing Kubernetes cluster.

Refer to the [Architecture overview](#) for guidance on choosing which Puppet-supported Kubernetes cluster configuration is most appropriate for your needs.

**Important:** The Puppet-supported Puppet Application Manager cluster brings its own container runtime as part of the kURL installation.

- Do not install a container runtime from your operating system (OS) vendor or third-party.
- Do not install PAM on a node that has previously hosted a container runtime from your OS vendor or third-party.

Installing a different container runtime on a node, even if you installed and removed the packages before you installed PAM, causes failures that persist even after you've uninstalled the runtime.

For information on installing Puppet Application Manager on an existing Kubernetes cluster, see [Install Puppet applications using PAM on a customer-supported Kubernetes cluster](#) on page 35.

- [Install Puppet applications using PAM on a customer-supported Kubernetes cluster](#) on page 35

Use these instructions to install Puppet Application Manager and any Puppet applications on an existing Kubernetes cluster.

- [PAM HA online installation](#) on page 37

  The Puppet Application Manager (PAM) installation process creates a Kubernetes cluster for you and walks you through installing your Puppet application on the cluster.

- [PAM HA offline installation](#) on page 41

  Use these instructions to install Puppet Application Manager (PAM) in an air-gapped or offline environment where the Puppet Application Manager host server does not have direct access to the internet.

- [PAM standalone online installation](#) on page 44

  The Puppet Application Manager (PAM) installation process sets up the application manager (with a simple Kubernetes installation for container orchestration) for you and installs the application on the single-node cluster.

- [PAM standalone offline installation](#) on page 47

  Use these instructions to install Puppet Application Manager (PAM) in an offline environment where the Puppet Application Manager host server does not have direct access to the internet.

- [Automate PAM and Puppet application online installations](#) on page 49

  During a fresh online installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

- [Automate PAM and Puppet application offline installations](#) on page 51

  During a fresh offline installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

- [Uninstall PAM](#) on page 53

  Different uninstall procedures are required for Puppet-supported and customer-supported clusters

**Related information**

[Architecture overview](#) on page 20

Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.
Install Puppet applications using PAM on a customer-supported Kubernetes cluster

Use these instructions to install Puppet Application Manager and any Puppet applications on an existing Kubernetes cluster.

**Before you begin**

1. If you haven’t already done so, install kubectl.
2. Puppet Application Manager is expected to work on any certified Kubernetes distribution that meets the following requirements. We validated and support:
   - Google Kubernetes Engine
   - AWS Elastic Kubernetes Service
   - Red Hat OpenShift
   If you use a different distribution, contact Puppet Support for more information on compatibility with PAM.
3. Make sure your Kubernetes cluster meets the minimum requirements:
   - Kubernetes version 1.17-1.21.
   - A default storage class that can be used for relocatable storage.
   - A standard Ingress controller that supports websockets (we have tested with Project Contour and NGINX).
   - We currently test and support Google Kubernetes Engine (GKE) clusters.

   **Note:** If you’re using self-signed certificates on your Ingress controller, you must ensure that your job hardware nodes trust the certificates. Additionally, all nodes that use Continuous Delivery for PE webhooks must trust the certificates, or SSL checking must be disabled on these nodes.

   **Important:** If you are installing Puppet Comply on Puppet Application Manager, the ingress controller must be configured to allow request payloads of up to 32 MB. Ingress controllers used by Amazon EKS commonly default to a 1 MB maximum — this causes all report submissions to fail.

   The ingress must have a generous limit for total connection time. Setting the connection timeout to infinity in conjunction with an idle timeout is recommended.

4. If you are setting up Puppet Application Manager behind a proxy server, the installer supports proxies configured via HTTP_PROXY/HTTPS_PROXY/NO_PROXY environment variables.

   **Restriction:** Using a proxy to connect to external version control systems is currently not supported.

Installation takes several (mostly hands-off) minutes to complete.

1. Install the KOTS (Kubernetes off-the-shelf software) plugin on a workstation that has kubectl access to the cluster. Your kubectl configuration must have sufficient privileges to create cluster-level roles and permissions:

   ```bash
curl https://kots.io/install | bash
   ```
2. If you are performing an offline install, ensure the required images are available in a local registry.
   a) Download the release assets matching the CLI version using the following command:

```
curl -LO https://github.com/replicatedhq/kots/releases/download/v$(kubectl kots version | head -n1 | cut -d' ' -f3)/kotsadm.tar.gz
```

b) Extract the images and push them into a private registry. Registry credentials provided in this step must have push access. These credentials are not stored anywhere or reused later.

```
kubectl kots admin-console push-images ./kotsadm.tar.gz
   --private.registry.host <private.registry.host>/puppet-application-manager
   --registry-username <rw-username>
   --registry-password <rw-password>
```

c) Install Puppet Application Manager using images pushed in the previous step. Registry credentials provided in this step only need to have read access, and they are stored in a Kubernetes secret in the current namespace. These credentials are used to pull the images.

```
kubectl kots install puppet-application-manager
   --kotsadm-namespace puppet-application-manager
   --kotsadm-registry <private.registry.host>
   --registry-username <ro-username>
   --registry-password <ro-password>
```

Note: If you are setting up Puppet Application Manager behind a proxy server, add the `--copy-proxy-env` flag to this command to copy the proxy-related environment values from your environment.

d) You can use similar commands to upload images from the application bundle to your registry to continue to use read-only access when pulling images. Use the same registry namespace (puppet-application-manager) to pull application images.

```
kubectl kots admin-console push-images ./<application-release>.airgap
   --private.registry.host <private.registry.host>/puppet-application-manager
   --registry-username <rw-username>
   --registry-password <rw-password>
```

3. To perform an online install of Puppet Application Manager on your cluster, run the following commands from a workstation that has kubectl access to the cluster.

```
kubectl kots install puppet-application-manager --namespace <target namespace>
```

This installs Puppet Application Manager on the cluster and sets up a port forward on the ClusterIP.

4. Navigate to `http://localhost:8800` and follow the prompts to be guided through the process of uploading a license for the application, configuring a local registry (for offline installs), checking to make sure your infrastructure meets system requirements, and configuring the application.

Note: If you are performing an offline install, download the application bundle and provide it when prompted.

Tip: Clusters like GKE often restrict ports to 30000-32767. The webhook for Continuous Delivery for PE defaults to port 8000. To update this port to something in the allowed range, when configuring the application, use the following steps:

a. On the Puppet Application Manager Dashboard page, under Config > Optional configuration, select View options for using a proxy or external load balancer.

b. Enter a new value for Webhook service port.
5. To configure your installation further, click Config. On this tab, you can configure a public hostname, root user, and other settings. These are written as Kubernetes secrets in the deployment manifests. For information on how to configure your application, see the documentation for that application:
   - Configure Continuous Delivery for PE in an online environment
   - Configure Comply in an online environment

6. To use cert-manager, in the Customize endpoints section, select I have cert manager and in the annotations section, add yours. For example:

   ```
   kubernetes.io/ingress.class: nginx
cert-manager.io/cluster-issuer: letsencrypt-prod
   ```

7. When you are happy with your configuration, click Save config to deploy the application.

   Follow the instructions for configuring and deploying your Puppet applications on Puppet Application Manager. For more information, see Install applications via the PAM UI on page 54.

   For more information on installing Continuous Delivery for PE online, see Install Continuous Delivery for PE.

   For more information on installing Comply online, see Install Comply online.

**Related information**

- Upgrade PAM on a customer-supported online cluster on page 62
- Upgrade PAM on a customer-supported offline cluster on page 63

**PAM HA online installation**

The Puppet Application Manager (PAM) installation process creates a Kubernetes cluster for you and walks you through installing your Puppet application on the cluster.

**Before you begin**

1. Review the Puppet Application Manager system requirements.
2. Note that Swap is not supported for use with this version of Puppet Application Manager (PAM). The installation script attempts to disable Swap if it is enabled.
3. (Optional) If necessary, prepare additional steps related to SELinux and Firewalld:

   The PAM installation script disables SELinux and Firewalld by default. If you want to keep SELinux enabled, append the `--s preserve-selinux-config` switch to the PAM install command. This may require additional configuration to adapt SELinux policy to the installation.

   If you want to keep Firewalld enabled:
   a. Make sure Firewalld is installed on your system.
   b. To prevent the installation from disabling Firewalld, provide a patch file to the PAM install command using `--s installer-spec-file=patch.yaml`, where patch.yaml is the name of your patch file. For reference, here's an example patch file that enables Firewalld during installation, starts the service if it isn't running, and adds rules to open relevant ports:

   ```yaml
   apiVersion: cluster.kurl.sh/v1beta1
   kind: Installer
   metadata:
     name: patch
   spec:
     firewallldConfig:
       firewallld: enabled
       command: ["/bin/bash", ":c"]
   ```

© 2021 Puppet, Inc.
4. Ensure that IP address ranges 10.96.0.0/22 and 10.32.0.0/22 are locally accessible. See Resolve IP address range conflicts for instructions.

**Note:** The minimum size for CIDR blocks used by Puppet Application Manager are:

- **Standalone** -/24 for pod and service CIDRs
- **HA** -/23 for pod and service CIDRs
- Default of /22 is recommended to support future expansion

5. If you are setting up Puppet Application Manager behind a proxy server, the installer supports proxies configured via `HTTP_PROXY`/`HTTPS_PROXY`/`NO_PROXY` environment variables.

**Restriction:** Using a proxy to connect to external version control systems is currently not supported.

6. Set all nodes used in your HA implementation to the UTC timezone.

7. If you use the `puppetlabs/firewall` module to manage your cluster's firewall rules with Puppet, be advised that purging unknown rules from changes breaks Kubernetes communication. To avoid this, apply the `puppetlabs/pam_firewall` module before installing Puppet Application Manager.

This installation process results in a Puppet Application Manager instance that is configured for high availability. Installation takes several (mostly hands-off) minutes to complete.
1. Install and configure a load balancer (or two if you want to segment internal and external traffic - for more information, see Architecture overview). Round-robin load balancing is sufficient. For an HA cluster, the following is required:

- A network (L4, TCP) load balancer for port 6443 across primary nodes. This is required for Kubernetes components to continue operating in the event that a node fails. The port is only accessed by the Kubernetes nodes and any admins using kubectl.
- A network (L4, TCP) or application (L7, HTTP/S) load balancer for ports 80, and 443 across all primaries and secondaries. This maintains access to applications in event of a node failure. Include 8800 if you want external access to the Puppet Application Manager UI.

**Note:** Include port 8000 for webhook callbacks if you are installing Continuous Delivery for PE.
2. From the command line of your first primary node, run the installation script:

```
curl -sSL https://k8s.kurl.sh/puppet-application-manager | sudo bash
```

**Tip:** If you're installing Puppet Application Manager behind a proxy server, using `sudo` might cause the installation to fail. Try running the command as root and replace `sudo bash` with `bash`.

**Note:** An unformatted, unpartitioned storage device is required.

By default this installation automatically uses devices (under `/dev`) matching the pattern `vd[b-z]`. Attach a device to each host. Only devices that match the pattern, and are unformatted, are used.

If necessary, you can override this pattern by providing a patch during installation; append `--installer-spec-file=patch.yaml` to the installation command.

```
apiVersion: cluster.kurl.sh/v1beta1
kind: Installer
metadata:
  name: patch
spec:
  rook:
    blockDeviceFilter: "sd[b-z]"
```

a) When prompted for a load balancer address, enter the address of the DNS entry for your load balancer.

b) The installation script prints the address and password (only shown once, so make careful note of it) for Puppet Application Manager:

```
---
Kotsadm: http://<PUPPET APPLICATION MANAGER ADDRESS>:8800
Login with password (will not be shown again): <PASSWORD>
---
```

**Note:** If you lose this password or wish to change it, see [Reset the Puppet Application Manager password](#) for instructions.

c) When the installation script is complete, run `bash -l` to reload the shell.

**Tip:** If the installation script fails, run the following and upload the results to the Puppet Support team:

```
kubectl support-bundle https://kots.io
```

If you're installing as the root user, run the command directly:

```
/usr/local/bin/kubectl-support_bundle https://kots.io
```

3. Add two additional primary nodes to the installation by following the instructions in the install script:

To add MASTER nodes to this installation, run the following script on your other nodes:

```
curl -sSL https://k8s.kurl.sh/puppet-application-manager-unstable/join.sh | sudo bash -s kubernetes-master-address=...
```

If you want to keep SELinux enabled, append the `--preserve-selinux-config` switch to the install command.

4. Add the two new nodes to your load balancer.
5. Navigate to the Puppet Application Manager UI using the address provided by the installation script (http://<PUPPET APPLICATION MANAGER ADDRESS>:8800) and follow the prompts.

The Puppet Application Manager UI is where you manage Puppet applications. You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets application system requirements.

Follow the instructions for configuring and deploying your Puppet applications on Puppet Application Manager. For more information, see Install applications via the PAM UI on page 54.

For more information on installing Continuous Delivery for PE online, see Install Continuous Delivery for PE.

For more information on installing Comply online, see Install Comply online.

Related information

Reset the PAM password on page 69
As part of the installation process, Puppet Application Manager (PAM) generates a password for you. You can update this password to one of your choosing after installation.

PAM system requirements on page 23
You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

Resolve IP address range conflicts on page 68
When installing Puppet Application Manager, IP address ranges 10.96.0.0/22 and 10.32.0.0/22 must not be used by other nodes on the local network.

Architecture overview on page 20
Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

Using sudo behind a proxy server on page 72
Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you’re running PAM behind a proxy, `sudo` might not work correctly. If you’re having trouble running commands with `sudo`, and you’re behind a proxy, try switching to the root user and running the command without `sudo`.

PAM HA offline installation

Use these instructions to install Puppet Application Manager (PAM) in an air-gapped or offline environment where the Puppet Application Manager host server does not have direct access to the internet.

Before you begin

1. Review the Puppet Application Manager system requirements.
2. Note that Swap is not supported for use with this version of Puppet Application Manager (PAM). The installation script attempts to disable Swap if it is enabled.
3. (Optional) If necessary, prepare additional steps related to SELinux and Firewalld:

   The PAM installation script disables SELinux and Firewalld by default. If you want to keep SELinux enabled, append the `-s preserve-selinux-config` switch to the PAM install command. This may require additional configuration to adapt SELinux policy to the installation.

   If you want to keep Firewalld enabled:
   a. Make sure Firewalld is installed on your system.
   b. To prevent the installation from disabling Firewalld, provide a patch file to the PAM install command using `-s installer-spec-file=patch.yaml`, where `patch.yaml` is the name of your patch file. For reference, here's an example patch file that enables Firewalld during installation, starts the service if it isn't running, and adds rules to open relevant ports:

   ```yaml
   apiVersion: cluster.kurl.sh/v1beta1
   kind: Installer
   ```

© 2021 Puppet, Inc.
metadata:
  name: patch
spec:
  firewalldConfig:
    firewalld: enabled
    command: ["/bin/bash", "-c"]
    args: ["echo 'net.ipv4.ip_forward = 1' | tee -a /etc/sysctl.conf &&
                        sysctl -p"]
  firewalldCmds:
    - ["--permanent", "--zone=trusted", "--add-interface=weave"]
    - ["--zone=external", "--add-masquerade"]
    # SSH port
    - ["--permanent", "--zone=public", "--add-port=22/tcp"]
    # HTTPS port
    - ["--permanent", "--zone=public", "--add-port=443/tcp"]
    # Kubernetes etcd port
    - ["--permanent", "--zone=public", "--add-port=2379-2830/tcp"]
    # Kubernetes API port
    - ["--permanent", "--zone=public", "--add-port=6443/tcp"]
    # Weave Net port
    - ["--permanent", "--zone=public", "--add-port=6783/udp"]
    # Weave Net port
    - ["--permanent", "--zone=public", "--add-port=6783-6874/tcp"]
    # CD4PE Webhook callback port (uncomment line below if needed)
    # - ["--permanent", "--zone=public", "--add-port=8000/tcp"]
    # KOTS UI port
    - ["--permanent", "--zone=public", "--add-port=8800/tcp"]
    # CD4PE Local registry port (offline only, uncomment line below if needed)
    # - ["--permanent", "--zone=public", "--add-port=9001/tcp"]
    # Kubernetes component ports (kubelet, kube-scheduler, kube-controller)
    - ["--permanent", "--zone=public", "--add-port=10250-10252/tcp"]
    # Reload firewall rules
    - ["--reload"]
  bypassFirewalldWarning: true
  disableFirewalld: false
  hardFailOnFirewalld: false
  preserveConfig: false

4. Ensure that IP address ranges 10.96.0.0/22 and 10.32.0.0/22 are locally accessible. See Resolve IP address range conflicts for instructions.

   **Note:** The minimum size for CIDR blocks used by Puppet Application Manager are:
   - **Standalone** -/24 for pod and service CIDRs
   - **HA** -/23 for pod and service CIDRs
   - Default of /22 is recommended to support future expansion

5. Ensure that the nodes can resolve their own hostnames, through either local host mapping or a reachable DNS server.
6. Set all nodes used in your HA implementation to the UTC timezone.
7. If you use the puppetlabs/firewall module to manage your cluster's firewall rules with Puppet, be advised that purging unknown rules from changes breaks Kubernetes communication. To avoid this, apply the puppetlabs/pam_firewall module before installing Puppet Application Manager.
8. If you're restoring a backup from a previous cluster, make sure you include the kurl-registry-ip=<YOUR_IP_ADDRESS> installation option. For more information, see Disaster recovery or migration using a snapshot on page 66.

This installation process results in a basic Puppet Application Manager instance that is configured for optional high availability. Installation takes several (mostly hands-off) minutes to complete.
1. Install and configure a load balancer (or two if you want to segment internal and external traffic - for more information, see Architecture overview). Round-robin load balancing is sufficient. For an HA cluster, the following is required:
   - A network (L4, TCP) load balancer for port 6443 across primary nodes. This is required for Kubernetes components to continue operating in the event that a node fails. The port is only accessed by the Kubernetes nodes and any admins using kubectl.
   - A network (L4, TCP) or application (L7, HTTP/S) load balancer for ports 80, and 443 across all primaries and secondaries. This maintains access to applications in event of a node failure. Include 8800 if you want external access to the Puppet Application Manager UI.

   **Note:** Include port 8000 for webhook callbacks if you are installing Continuous Delivery for PE.

2. From a workstation with internet access, download the cluster installation bundle (note that this bundle is ~4GB):
   
   https://k8s.kurl.sh/bundle/puppet-application-manager.tar.gz

3. Copy the installation bundle to your primary and secondary nodes and unpack it:

   tar xzf puppet-application-manager.tar.gz

4. Run the installation command:

   cat install.sh | sudo bash -s airgap

   **Note:** An unformatted, unpartitioned storage device is required.

   By default this installation automatically uses devices (under /dev) matching the pattern vd[b-z]. Attach a device to each host. Only devices that match the pattern, and are unformatted, are used.

   If necessary, you can override this pattern by providing a patch during installation; append `-s installer-spec-file=patch.yaml` to the installation command.

   ```yaml
   apiVersion: cluster.kurl.sh/v1beta1
   kind: Installer
   metadata:
     name: patch
   spec:
     rook:
       blockDeviceFilter: "sd[b-z]"
   ```

   a) When prompted for a load balancer address, enter the address of the DNS entry for your load balancer.

   b) The installation script prints the address and password (only shown once, so make careful note of it) for Puppet Application Manager:

   ```
   Kotsadm: http://<PUPPET APPLICATION MANAGER ADDRESS>:8800
   Login with password (will not be shown again): <PASSWORD>
   ```

   **Note:** If you lose this password or wish to change it, see Reset the Puppet Application Manager password for instructions.
5. Follow instructions outlined after the following line in the install script:

```bash
cat ./join.sh | sudo bash -s airgap
kubernetes-master-address=...
```

6. Add the two new nodes to your load balancer.

7. Navigate to the Puppet Application Manager UI using the address provided by the installation script (http://<PUPPET APPLICATION MANAGER ADDRESS>:8800) and follow the prompts.

The Puppet Application Manager UI is where you manage Puppet applications. You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets application system requirements.

Follow the instructions for installing your Puppet applications on Puppet Application Manager. For more information, see Install applications via the PAM UI on page 54.

For more information on installing Continuous Delivery for PE offline, see Install Continuous Delivery for PE in an offline environment.

For more information on installing Comply offline, see Install Comply offline.

**Related information**

- Reset the PAM password on page 69
  As part of the installation process, Puppet Application Manager (PAM) generates a password for you. You can update this password to one of your choosing after installation.

- PAM system requirements on page 23
  You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

- Resolve IP address range conflicts on page 68
  When installing Puppet Application Manager, IP address ranges 10.96.0.0/22 and 10.32.0.0/22 must not be used by other nodes on the local network.

- Architecture overview on page 20
  Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

- Using sudo behind a proxy server on page 72
  Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

**PAM standalone online installation**

The Puppet Application Manager (PAM) installation process sets up the application manager (with a simple Kubernetes installation for container orchestration) for you and installs the application on the single-node cluster.

**Before you begin**

1. Review the Puppet Application Manager system requirements.
2. Note that Swap is not supported for use with this version of Puppet Application Manager (PAM). The installation script attempts to disable Swap if it is enabled.
3. (Optional) If necessary, prepare additional steps related to SELinux and Firewalld:

The PAM installation script disables SELinux and Firewalld by default. If you want to keep SELinux enabled, append the `-s preserve-selinux-config` switch to the PAM install command. This may require additional configuration to adapt SELinux policy to the installation.

If you want to keep Firewalld enabled:

a. Make sure Firewalld is installed on your system.

b. To prevent the installation from disabling Firewalld, provide a patch file to the PAM install command using `-s installer-spec-file=patch.yaml`, where `patch.yaml` is the name of your patch file. For reference, here's an example patch file that enables Firewalld during installation, starts the service if it isn't running, and adds rules to open relevant ports:

```yaml
apiVersion: cluster.kurl.sh/v1beta1
code: Installer
metadata:
  name: patch
spec:
  firewalldConfig:
    firewalld: enabled
    command: ["/bin/bash", "-c"]
    args: ["echo 'net.ipv4.ip_forward = 1' | tee -a /etc/sysctl.conf &&
        sysctl -p"]
  firewalldCmds:
    - ["--permanent", "--zone=trusted", "--add-interface=weave"]
    - ["--zone=external", "--add-masquerade"]
    # SSH port
    - ["--permanent", "--zone=public", "--add-port=22/tcp"]
    # HTTPS port
    - ["--permanent", "--zone=public", "--add-port=443/tcp"]
    # Kubernetes etcd port
    - ["--permanent", "--zone=public", "--add-port=2379-2830/tcp"]
    # Kubernetes API port
    - ["--permanent", "--zone=public", "--add-port=6443/tcp"]
    # Weave Net port
    - ["--permanent", "--zone=public", "--add-port=6783/udp"]
    # Weave Net port
    - ["--permanent", "--zone=public", "--add-port=6783-6874/tcp"]
    # CD4PE Webhook callback port (uncomment line below if needed)
    # - ["--permanent", "--zone=public", "--add-port=8000/tcp"]
    # KOTS UI port
    - ["--permanent", "--zone=public", "--add-port=8800/tcp"]
    # CD4PE Local registry port (offline only, uncomment line below if needed)
    # - ["--permanent", "--zone=public", "--add-port=9001/tcp"]
    # Kubernetes component ports (kubelet, kube-scheduler, kube-controller)
    - ["--permanent", "--zone=public", "--add-port=10250-10252/tcp"]
    # Reload firewall rules
    - ["--reload"]
  bypassFirewalldWarning: true
  disableFirewalld: false
  hardFailOnFirewalld: false
  preserveConfig: false
```

4. Ensure that IP address ranges `10.96.0.0/22` and `10.32.0.0/22` are locally accessible. See Resolve IP address range conflicts for instructions.

5. If you use the puppetlabs/firewall module to manage your cluster's firewall rules with Puppet, be advised that purging unknown rules from changes breaks Kubernetes communication. To avoid this, apply the puppetlabs/pam_firewall module before installing Puppet Application Manager.
This installation process results in a basic Puppet Application Manager instance. Installation takes several (mostly hands-off) minutes to complete.

1. From the command line of your node, run the installation script:

   ```bash
curl -sSL https://k8s.kurl.sh/puppet-application-manager-standalone | sudo bash
   ```

   **Tip:** If you're installing Puppet Application Manager behind a proxy server, using `sudo` might cause the installation to fail. Try running the command as root and replace `sudo bash` with `bash`.

   a) When the installation script prints the Puppet Application Manager address and password, make a careful note of these credentials:

   ```
   ---
   Kotsadm: http://<PUPPET APPLICATION MANAGER ADDRESS>:8800
   Login with password (will not be shown again): <PASSWORD>
   ---
   ```

   **Note:** If you lose this password or wish to change it, see [Reset the Puppet Application Manager password](#) for instructions.

   b) When the installation script is complete, run `bash -l` to reload the shell.

   **Tip:** If the installation script fails, run the following and upload the results to the Puppet Support team:

   ```bash
cubectl support-bundle https://kots.io
   ```

   If you're installing as the root user, run the command directly:

   ```bash
/usr/local/bin/kubectl-support_bundle https://kots.io
   ```

2. Navigate to the Puppet Application Manager UI using the address provided by the installation script (`http://<PUPPET APPLICATION MANAGER ADDRESS>:8800`) and follow the prompts.

   The Puppet Application Manager UI is where you manage Puppet applications. You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets application system requirements.

   Follow the instructions for configuring and deploying your Puppet applications on Puppet Application Manager. For more information, see [Install applications via the PAM UI](#) on page 54.

   For more information on installing Continuous Delivery for PE online, see [Install Continuous Delivery for PE](#).

   For more information on installing Comply online, see [Install Comply online](#).

**Related information**

- [Reset the PAM password](#) on page 69
- As part of the installation process, Puppet Application Manager (PAM) generates a password for you. You can update this password to one of your choosing after installation.

- [PAM system requirements](#) on page 23
- You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

- [Resolve IP address range conflicts](#) on page 68
- When installing Puppet Application Manager, IP address ranges `10.96.0.0/22` and `10.32.0.0/22` must not be used by other nodes on the local network.

- [Architecture overview](#) on page 20

© 2021 Puppet, Inc.
Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

**Using sudo behind a proxy server** on page 72

Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

### PAM standalone offline installation

Use these instructions to install Puppet Application Manager (PAM) in an offline environment where the Puppet Application Manager host server does not have direct access to the internet.

#### Before you begin

1. Review the Puppet Application Manager system requirements.
2. Note that Swap is not supported for use with this version of Puppet Application Manager (PAM). The installation script attempts to disable Swap if it is enabled.
3. (Optional) If necessary, prepare additional steps related to SELinux and Firewalld:

   The PAM installation script disables SELinux and Firewalld by default. If you want to keep SELinux enabled, append the `-s preserve-selinux-config` switch to the PAM install command. This may require additional configuration to adapt SELinux policy to the installation.

   If you want to keep Firewalld enabled:
   
   a. Make sure Firewalld is installed on your system.
   
   b. To prevent the installation from disabling Firewalld, provide a patch file to the PAM install command using `--installer-spec-file=patch.yaml`, where `patch.yaml` is the name of your patch file. For reference, here's an example patch file that enables Firewalld during installation, starts the service if it isn't running, and adds rules to open relevant ports:

   ```yaml
   apiVersion: cluster.kurl.sh/v1beta1
   kind: Installer
   metadata:
     name: patch
   spec:
     firewalldConfig:
       firewalld: enabled
       command: ["/bin/bash", "--c"]
       args: ["echo 'net.ipv4.ip_forward = 1' | tee -a /etc/sysctl.conf &&
       sysctl -p"]
     firewalldCmds:
       - ["--permanent", "--zone=trusted", "--add-interface=weave"]
       - ["--zone=external", "--add-masquerade"]
       # SSH port
       - ["--permanent", "--zone=public", "--add-port=22/tcp"]
       # HTTPS port
       - ["--permanent", "--zone=public", "--add-port=443/tcp"]
       # Kubernetes etcd port
       - ["--permanent", "--zone=public", "--add-port=2379-2830/tcp"]
       # Kubernetes API port
       - ["--permanent", "--zone=public", "--add-port=6443/tcp"]
       # Weave Net port
       - ["--permanent", "--zone=public", "--add-port=6783/udp"]
       # Weave Net port
       - ["--permanent", "--zone=public", "--add-port=6783-6874/tcp"]
       # CD4PE Webhook callback port (uncomment line below if needed)
       # - ["--permanent", "--zone=public", "--add-port=8000/tcp"]
       # KOTS UI port
       - ["--permanent", "--zone=public", "--add-port=8800/tcp"]
   ```

© 2021 Puppet, Inc.
This installation process results in a basic Puppet Application Manager instance. Installation takes several (mostly hands-off) minutes to complete.

1. From a workstation with internet access, download the cluster installation bundle (note that this bundle is ~6GB):
   ```bash
   https://k8s.kurl.sh/bundle/puppet-application-manager-standalone.tar.gz
   ```

2. Copy the installation bundle to the host node and unpack it:
   ```bash
tar xzf puppet-application-manager-standalone.tar.gz
   ```

3. Run the installation command:
   ```bash
cat install.sh | sudo bash -s airgap
   ```

   a) The installation script prints the address and password (only shown once, so make careful note of it) for Puppet Application Manager:

   ```bash
   ---
   Kotsadm: http://<PUPPET APPLICATION MANAGER ADDRESS>:8800
   Login with password (will not be shown again): <PASSWORD>
   ---
   ```

   **Note:** If you lose this password or wish to change it, see **Reset the Puppet Application Manager password** for instructions.

4. Navigate to the Puppet Application Manager UI using the address provided by the installation script (http://<PUPPET APPLICATION MANAGER ADDRESS>:8800) and follow the prompts.

   The Puppet Application Manager UI is where you manage Puppet applications. You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets application system requirements.

   Follow the instructions for configuring and deploying your Puppet applications on Puppet Application Manager. For more information, see **Install applications via the PAM UI** on page 54.
For more information on installing Continuous Delivery for PE offline, see Install Continuous Delivery for PE in an offline environment.

For more information on installing Comply offline, see Install Comply offline.

Related information
Reset the PAM password on page 69
As part of the installation process, Puppet Application Manager (PAM) generates a password for you. You can update this password to one of your choosing after installation.

PAM system requirements on page 23
You can install Puppet Application Manager (PAM) on a Puppet-supported cluster or add PAM to a customer-supported cluster. Before installing PAM, ensure that your system meets these requirements.

Resolve IP address range conflicts on page 68
When installing Puppet Application Manager, IP address ranges 10.96.0.0/22 and 10.32.0.0/22 must not be used by other nodes on the local network.

Architecture overview on page 20
Puppet Application Manager runs on Kubernetes. Puppet provides several supported configurations for different use cases.

Using sudo behind a proxy server on page 72
Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use sudo to elevate privileges. If you're running PAM behind a proxy, sudo might not work correctly. If you're having trouble running commands with sudo, and you're behind a proxy, try switching to the root user and running the command without sudo.

Automate PAM and Puppet application online installations
During a fresh online installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

Before you begin
Ensure that your system meets the PAM system requirements on page 23.

1. Install Puppet Application Manager. For detailed instructions, see PAM HA online installation on page 37.
2. Define the configuration values for your Puppet application installation, using Kubernetes YAML format.

```yaml
apiVersion: kots.io/v1beta1
kind: ConfigValues
metadata:
  name: app-config
spec:
  values:
    accept_eula:
      value: has_accepted_eula
    annotations:
      value: "ingress.kubernetes.io/force-ssl-redirect: 'false'"
    hostname:
      value: "<HOSTNAME>"
    root_password:
      value: "<ROOT ACCOUNT PASSWORD>"
```

Tip: View the keyword names for all settings by clicking View files > upstream > config.yaml in Puppet Application Manager.

Replace the values indicated:

- Replace `<HOSTNAME>` with a hostname you want to use to configure an Ingress and to tell job hardware agents and web hooks how to connect to it. You might need to configure your DNS to resolve the hostname to your Kubernetes hosts.
- Replace `<ROOT ACCOUNT PASSWORD>` your chosen password for the application root account. The root account is used to administer your application and has full access to all resources and application-wide settings. This account must NOT be used for testing and deploying control repositories or modules.
- **Optional.** These configuration values disable HTTP-to-HTTPS redirection, so that SSL can be terminated at the load balancer. If you want to run the application over SSL only, change the `force-ssl-redirect` annotation to `true`.
- **Optional.** If your load balancer requires HTTP health checks, you can now enable Ingress settings that do not require Server Name Indication (SNI) for `/status`. To enable this setting, add the following to the config values statement:

```yaml
enable_lb_healthcheck:
  value: "1"
```

Note: The automated installation automatically accepts the Puppet application end user license agreement (EULA). Unless Puppet has otherwise agreed in writing, all software is subject to the terms and conditions of the Puppet Master License Agreement located at https://puppet.com/legal.

3. Write your license file and the configuration values generated in step 1 to the following locations:

- Write your license file to `./replicated_license.yaml`
- Write your configuration values to `./replicated_config.yaml`

4. Add the Puppet application definition to Puppet Application Manager with the license file and configuration values, passing in the Puppet Application Manager password you set in step 4:

```
kubectl kots install <APPLICATION NAME> --namespace default --shared-password <YOUR CHOSEN PASSWORD> --port-forward=false \
  --license-file ./replicated_license.yaml --config-values ./replicated_config.yaml
```

Note: If you want to install a specific version of the application, include the `--app-version-label=<VERSION>` flag in the install command.

5. Wait five minutes to allow the software time to process the change.
   Your configuration values are applied, and if preflight checks have passed, the application is deployed and in the process of starting up.
   The application's status on the Application tab is shown as Missing for several minutes while deployment is underway. To monitor the deployment's progress, run kubectl get pods --watch.
   When the deployment is complete, the application status changes to Ready.

7. Update your DNS or /etc/hosts file to include the hostname you chose during configuration.

8. Installation is now complete! Navigate to https://<HOSTNAME> and sign into Puppet application.

Related information
PAM HA online installation on page 37
The Puppet Application Manager (PAM) installation process creates a Kubernetes cluster for you and walks you through installing your Puppet application on the cluster.

Upgrade an automated online application installation on page 56
If you installed a Puppet application following the automated online installation instructions, run a script to upgrade to the latest version.

Automate PAM and Puppet application offline installations
During a fresh offline installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

Before you begin
Ensure that your system meets the PAM system requirements on page 23.

1. Install Puppet Application Manager. For detailed instructions, see PAM HA offline installation on page 41.
2. Define the configuration values for your Puppet application installation, using Kubernetes YAML format.

```
apiVersion: kots.io/v1beta1
class: ConfigValues
metadata:
  name: app-config
spec:
  values:
    accept_eula:
      value: has_accepted_eula
    annotations:
      value: "ingress.kubernetes.io/force-ssl-redirect: 'false'"
    hostname:
      value: "<HOSTNAME>"
    root_password:
      value: "<ROOT ACCOUNT PASSWORD>"
```

**Tip:** View the keyword names for all settings by clicking **View files > upstream > config.yaml** in Puppet Application Manager.

Replace the values indicated:

- Replace `<HOSTNAME>` with a hostname you want to use to configure an Ingress and to tell job hardware agents and web hooks how to connect to it. You might need to configure your DNS to resolve the hostname to your Kubernetes hosts.
- Replace `<ROOT ACCOUNT PASSWORD>` your chosen password for the application root account. The root account is used to administer your application and has full access to all resources and application-wide settings. This account must NOT be used for testing and deploying control repositories or modules.
- **Optional.** These configuration values disable HTTP-to-HTTPS redirection, so that SSL can be terminated at the load balancer. If you want to run the application over SSL only, change the `force-ssl-redirect` annotation to `true`.
- **Optional.** If your load balancer requires HTTP health checks, you can now enable Ingress settings that do not require Server Name Indication (SNI) for `/status`. To enable this setting, add the following to the config values statement:

```
enable_lb_healthcheck:
  value: "1"
```

**Note:** The automated installation automatically accepts the Puppet application end user license agreement (EULA). Unless Puppet has otherwise agreed in writing, all software is subject to the terms and conditions of the Puppet Master License Agreement located at https://puppet.com/legal.

3. Write your license file and the configuration values generated in step 1 to the following locations:

- Write your license file to `./replicated_license.yaml`
- Write your configuration values to `./replicated_config.yaml`

4. Download the application bundle:

```
curl -L <APPLICATION BUNDLE URL> -o <APPLICATION BUNDLE FILE>
```

5. Copy the application bundle to your primary and secondary nodes and unpack it:

```
tar xzf ./<APPLICATION BUNDLE FILE>
```
6. Run the application install command on your primary node. Replace the `<YOUR CHOSEN PASSWORD>`, `<APPLICATION NAME>`, `<APPLICATION BUNDLE FILE>` values in the example below with your own values:

```
KOTS_PASSWORD=<YOUR CHOSEN PASSWORD>
kubectl kots install <APPLICATION NAME> --namespace default --shared-password $KOTS_PASSWORD --license-file ./license.yaml --config-values ./config.yaml --airgap-bundle ./<APPLICATION BUNDLE FILE> --port-forward=false
# wait several minutes for the application to deploy; if it doesn’t show up, preflights or another error might have occurred
```

**Note:** If you want to install a specific version of the application, include the `--app-version-label=<VERSION>` flag in the install command.

**Related information**

**PAM HA offline installation** on page 41
Use these instructions to install Puppet Application Manager (PAM) in an air-gapped or offline environment where the Puppet Application Manager host server does not have direct access to the internet.

**Upgrade an automated offline application installation** on page 56
If you installed a Puppet application following the automated offline installation instructions, run a script to upgrade to the latest version.

**Uninstall PAM**
Different uninstall procedures are required for Puppet-supported and customer-supported clusters

To uninstall Puppet Application Manager (PAM) from Puppet-supported online clusters, use:

```
curl <installer URL>/tasks.sh | sudo bash -s reset
```

To uninstall Puppet Application Manager from Puppet-supported offline clusters, use:

```
cat tasks.sh | sudo bash -s reset
```

**Important:** You must be aware that the commands above do not completely clean up everything. Specifically, they do not clean up packages and config files, and do not remove the container runtime. They do, however, leave the system in a state that would be safe to restart the installer.

**Uninstall PAM on customer-supported clusters**
To uninstall Puppet Application Manager from customer-supported clusters, use:

```
kubectl delete namespace <pam-namespace>
kubectl delete clusterrolebinding kotsadm-rolebinding
kubectl delete clusterrole kotsadm-role
```

**Related information**

**Using sudo behind a proxy server** on page 72
Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`. 

© 2021 Puppet, Inc.
### Working with Puppet applications

You can install and upgrade Puppet using the Puppet Application Manager UI.

- **Install applications via the PAM UI** on page 54
  The process of adding an application once you've installed Puppet Application Manager is simple.
- **Update a license for online installations** on page 55
  If you have performed online installation of an application, you can use the Puppet Application Manager UI to update your license.
- **Update a license for offline installations** on page 55
  If you have performed offline installation of an application, you can use the Puppet Application Manager UI to update your license.
- **Upgrade an automated online application installation** on page 56
  If you installed a Puppet application following the automated online installation instructions, run a script to upgrade to the latest version.
- **Upgrade an automated offline application installation** on page 56
  If you installed a Puppet application following the automated offline installation instructions, run a script to upgrade to the latest version.

### Install applications via the PAM UI

The process of adding an application once you've installed Puppet Application Manager is simple.

<table>
<thead>
<tr>
<th>Application</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous Delivery for Puppet Enterprise</td>
<td>4.6.0 or later</td>
</tr>
<tr>
<td>Comply</td>
<td>1.0.4 or later</td>
</tr>
</tbody>
</table>

**Important:** Ensure you are using the following Puppet application versions if you want to add more than one Puppet application via the Puppet Application Manager UI:

For information on installing Puppet applications via the command line, see [Automate PAM and Puppet application online installations](#) on page 49 and [Automate PAM and Puppet application offline installations](#) on page 51.

To install a Puppet application using the Puppet Application Manager UI:

1. Log into the Puppet Application Manager UI, and click **Add a new application**.
   - If you have not added a Puppet application before you are prompted to upload a license.
   - If you have already added a Puppet application, click **Add a new application**.
2. Upload your `replicated_license.yaml` file when requested.

**Note:** Once the license file is installed, if offline installations are enabled, you are presented with an option to proceed with an offline setup.

Add the following information to install an offline application:

- **Hostname** - the hostname you want to use to configure an Ingress and to tell job hardware agents and web hooks how to connect to it. You might need to configure your DNS to resolve the hostname to your Kubernetes hosts.

  **Important:** The hostname must be unique for each application you install.

- **Username/Password** - The username and password for the application root account. The root account is used to administer your application and has full access to all resources and application-wide settings. This account must NOT be used for testing and deploying control repositories or modules.

- **Registry namespace** - the registry namespace for the application, e.g. `CD4PE` or `Comply`.

- **Airgap bundle** - upload the relevant application bundle tarball. Click **Continue**.

3. Add any additional required information that is presented on the **Config** page. Configure any other settings on the page relevant to your installation, such as external databases, customized endpoints, a load balancer, or TLS certificates. Click **Save Config** when you are done.

Saving your new configuration settings prompts the creation of a new application version.

4. Click **Go to new version**, which redirects you to the **Version history** tab. The newly created version is shown in the **All versions** section of the page.

5. Monitor the new version’s preflight checks. The **Running Checks** indicator is shown on the screen while your system is checked to make sure your cluster meets minimum system requirements. When the preflight check is complete:

   - If the status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

   **Important:** Do not move on until all preflight checks pass.

   - If the status is **Ready to Deploy**, move on to the next step.

6. Once the version is ready to deploy, click **Deploy**. On the **Application** tab, monitor the application for readiness. The application's status is shown as **Missing** for several minutes while deployment is underway. To monitor the deployment's progress, run `kubectl get pods --watch`.

   When the deployment is complete, the application status changes to **Ready**.

7. Navigate to `https://<HOSTNAME>` (using the hostname you entered on the **Config** screen) and sign into your application.

**Update a license for online installations**

If you have performed online installation of an application, you can use the Puppet Application Manager UI to update your license.

To update the license for an online application:

1. Log in to Puppet Application Manager, click the **License** tab, and then **Sync License**.

2. On the **Version history** tab, click **Deploy**.

   Puppet Application Manager adds “License Change” as the deployment cause on the **Version history** tab.

**Update a license for offline installations**

If you have performed offline installation of an application, you can use the Puppet Application Manager UI to update your license.

To update the license for an offline application:
1. Ask your Puppet sales representative to email you an updated license file.
2. Log in to Puppet Application Manager, click the **License** tab.
3. Drag and drop or upload the updated license file provided by your Puppet sales representative.
4. On the **Version history** tab, click **Deploy**.

   Puppet Application Manager adds “License Change” as the deployment cause on the **Version history** tab.

### Upgrade an automated online application installation

If you installed a Puppet application following the automated online installation instructions, run a script to upgrade to the latest version.

**Important:** Ensure that you are following an approved upgrade path for the application you want to upgrade. For more information, check the relevant application documentation.

1. From the command line of your primary (control plane) node, get the application slug for the application you want to upgrade:

   ```
kubectl kots --namespace <NAMESPACE> get apps
   ```

   Replace `<NAMESPACE>` with the name of the namespace in which you installed PAM (usually `default`).

2. Run the upgrade script:

   ```
kubectl kots upstream upgrade <APPLICATION SLUG> --namespace <NAMESPACE> --deploy
   ```

   Replace `<APPLICATION SLUG>` with the relevant application slug for the application you want to upgrade.

   Replace `<NAMESPACE>` with the name of the namespace in which you installed PAM (usually `default`).

3. Wait five minutes to allow the software time to process the change.


   If preflight checks have passed, the upgraded application is deployed and in the process of starting up. To monitor the deployment's progress, run:

   ```
kubectl get pods --watch
   ```

### Related information

**Automate PAM and Puppet application offline installations** on page 51

During a fresh offline installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

### Upgrade an automated offline application installation

If you installed a Puppet application following the automated offline installation instructions, run a script to upgrade to the latest version.

**Important:** Ensure that you are following an approved upgrade path for the application you want to upgrade. For more information, check the relevant application documentation.

1. Download the application bundle you want to upgrade to. Copy to your primary node.

2. From the command line of your primary (control plane) node, get the application slug for the application you want to upgrade:

   ```
kubectl kots --namespace <NAMESPACE> get apps
   ```

   Replace `<NAMESPACE>` with the name of the namespace in which you installed PAM (usually `default`).
3. Run the upgrade script:

```bash
kubectl kots upstream upgrade <APPLICATION SLUG> --airgap-bundle ./
<APPLICATION BUNDLE FILE> --kotsadm-namespace <REGISTRY NAMESPACE> --
namespace <NAMESPACE> --deploy
```

- Replace `<APPLICATION SLUG>` with the relevant application slug for the application you want to upgrade.
- Replace `<APPLICATION BUNDLE FILE>` with the name of the application bundle file.
- Replace `<REGISTRY NAMESPACE>` with your Registry namespace where images are uploaded.
- Replace `<NAMESPACE>` with the name of the namespace in which you installed PAM (usually default).

4. Wait five minutes to allow the software time to process the change.

5. Navigate to `http://<NODE IP ADDRESS>:8800` and log in with the Puppet Application Manager password.

If preflight checks have passed, the upgraded application is deployed and in the process of starting up. To monitor the deployment's progress, run:

```bash
kubectl get pods --watch
```

**Related information**

**Automate PAM and Puppet application offline installations** on page 51

During a fresh offline installation of Puppet Application Manager (PAM) and a Puppet application, you have the option to configure the software automatically rather than completing the installation script interview.

## Maintenance and tuning

Follow these guidelines when you're tuning or performing maintenance on a node running Puppet Application Manager (PAM).

### How to determine your version of Puppet Application Manager

You can use the following command to determine what version of Puppet Application Manager (PAM) you're using:

```bash
kubectl get installer --sort-by=.metadata.creationTimestamp -o
jsonpath='{{.items[-1:].metadata.name}}' ; echo
```

Depending on which version you've installed, the command returns one of these values:

- **HA architecture**: puppet-application-manager
- **Standalone architecture**: puppet-application-manager-standalone
- **Legacy architecture**: Any other value, for example, puppet-application-manager-legacy, cd4pe, or comply

### Rebooting PAM nodes

Where possible, avoid rebooting or shutting down a PAM node. Shutting down a legacy or HA PAM node incorrectly could result in storage volume corruption and the loss of data.

For tasks such as package updates or security patches, where you must perform a reboot or shut down, follow the procedure below to gracefully shut down the node and ensure that it is drained correctly.

To reboot a node:

1. Shut down services using Ceph-backed storage:

```bash
/opt/ekco/shutdown.sh
```
2. If you're using a high availability (HA) cluster, drain the node:

```
kubectl drain <NODE NAME> --ignore-daemonsets --delete-local-data
```

3. Reboot the node.

**Load balancer health checks**

To set up health checks for the load balancer that your Puppet Application Manager (PAM) applications are running behind, set up rules for these applications and services.

<table>
<thead>
<tr>
<th>Application/service</th>
<th>URL/port</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Puppet application. For example, Continuous Delivery for Puppet Enterprise or Puppet Comply</td>
<td>https://&lt;CDPE HOSTNAME&gt;:443/status</td>
<td>Although Puppet applications might expose other ports (Continuous Delivery for PE exposes ports 443, 80, and 8000), 443 is the HTTPS endpoint, and is the best port to use for health checks.</td>
</tr>
<tr>
<td>Puppet Application Manager (PAM)</td>
<td>https://&lt;KUBERNETES PRIMARY IP&gt;:8800/healthz</td>
<td></td>
</tr>
<tr>
<td>External load balancer endpoint</td>
<td>Port 6443 or https://&lt;KUBERNETES PRIMARY IP&gt;:6443/livez</td>
<td>For information on setting up a TCP probe on an external load balancer endpoint, consult the kURL load balancer documentation.</td>
</tr>
<tr>
<td>Local container registry (for offline installations)</td>
<td>https://&lt;KUBERNETES PRIMARY IP&gt;:9001</td>
<td></td>
</tr>
</tbody>
</table>

**Upgrading PAM on a Puppet-supported cluster**

Upgrade Puppet Application Manager (PAM) on a Puppet-supported cluster to take advantage of new features and bug fixes, and to upgrade your cluster to the latest version of Kubernetes when one is available.

There are four possible upgrade types for Puppet Application Manager installations:

- **Online** - For standalone or HA installations with a connection to the internet.
- **Offline** - For air-gapped standalone or HA installations without a connection to the internet.
- **Online legacy** - For standalone or HA installations created prior to April 2021 with a connection to the internet.
- **Offline legacy** - For air-gapped standalone or HA installations created prior to April 2021 without a connection to the internet.

**Restriction:** You cannot upgrade from a legacy deployment to a non-legacy deployment, or from standalone to HA, or a HA to a standalone deployment.

**How to determine your version of Puppet Application Manager**

You can use the following command to determine what version of Puppet Application Manager (PAM) you're using:

```
kubectl get installer --sort-by=.metadata.creationTimestamp -o jsonpath='{{.items[-1:].metadata.name}'} ; echo
```

Depending on which version you've installed, the command returns one of these values:

- **HA architecture**: puppet-application-manager
- **Standalone architecture**: puppet-application-manager-standalone
• **Legacy architecture**: Any other value, for example, `puppet-application-manager-legacy`, `cd4pe`, or `comply`

## Upgrade PAM online

Upgrade Puppet Application Manager (PAM) to take advantage of new features and bug fixes, and to upgrade your cluster to the latest version of Kubernetes when one is available.

### Before you begin

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at [Backing up PAM using snapshots](#) on page 63.

1. On your first primary node, rerun the installation script, passing in any arguments you included when installing for the first time:

   For standalone deployments, use:
   
   ```bash
   curl -sSL https://k8s.kurl.sh/puppet-application-manager-standalone | sudo bash -s force-reapply-addons
   ```

   For HA deployments, use:
   
   ```bash
   curl -sSL https://k8s.kurl.sh/puppet-application-manager | sudo bash -s force-reapply-addons
   ```

2. If a new version of Kubernetes is available, the installer notes upgrade scripts to run on other nodes in an HA cluster.

   The installer also pauses before draining nodes as part of the Kubernetes upgrade. The node draining process can take several minutes to complete, during which time application workloads are stopped or migrated to other systems. This migration may cause several minutes of downtime while databases are rescheduled.

### Related information

- [Using sudo behind a proxy server](#) on page 72

Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

## Upgrade PAM offline

Users operating in environments without direct access to the internet must use the links below to upgrade to the latest version of Puppet Application Manager (PAM).

### Before you begin

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at [Backing up PAM using snapshots](#) on page 63.

To upgrade Puppet Application Manager:
1. From a workstation with internet access, download the latest version of the installation bundle that is relevant for your installation type:
   For standalone installations, enter the following command (note that this bundle is ~6GB):
   
   ```
   https://k8s.kurl.sh/bundle/puppet-application-manager-standalone.tar.gz
   ```
   
   For HA installations, enter the following command (note that this bundle is ~4GB):
   
   ```
   https://k8s.kurl.sh/bundle/puppet-application-manager.tar.gz
   ```

2. Copy the installation bundle to your primary and secondary nodes and unpack it:
   For standalone installations, use:
   
   ```
   tar xzf puppet-application-manager-standalone.tar.gz
   ```
   
   For HA installations, use:
   
   ```
   tar xzf puppet-application-manager.tar.gz
   ```

3. On your primary node, rerun the installation script, passing in any arguments you included when installing for the first time:

   ```
   cat install.sh | sudo bash -s airgap force-reapply-addons
   ```

   **Note:** This script issues a prompt to run the `task.sh` and `upgrade.sh` scripts on your secondary nodes. Use the versions of these scripts from the downloaded bundle in step 2.

4. If a new version of Kubernetes is available, the installer systems provide upgrade scripts to run on other nodes in an HA cluster. The installer also pauses before draining nodes as part of the Kubernetes upgrade. Node draining is performed as part of a Kubernetes upgrade.

   The node draining process can take several minutes to complete, during which time application workloads are stopped or migrated to other systems. This migration may cause several minutes of downtime while databases are rescheduled.

   When the deployment is complete, sign into Puppet Application Manager - `http://<PUPPET APPLICATION MANAGER ADDRESS>:8800` - and verify that the new version number is displayed in the bottom left corner of the web UI.

### PAM legacy upgrades

Use this method to upgrade Puppet Application Manager (PAM) from a version installed before May 2021.

**Before you begin**

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at [Backing up PAM using snapshots](#) on page 63.

**Restriction:** It is not currently possible to upgrade from an online legacy install to a new offline install configuration. Similarly, upgrades from an offline legacy configuration to a new online install are not currently supported.

The legacy version reflects an older configuration that used Ceph 1.0 which hosted data directly on the file system. Puppet no longer recommend this for new installs, but maintains it to support existing installs and ensure other components can be kept up-to-date.

**Legacy architecture is deprecated:** The legacy architecture utilizes Rook 1.0, which is incompatible with Kubernetes version 1.20 and newer versions. Kubernetes version 1.19 is no longer receiving security updates. Puppet will continue to update legacy architecture components other than Kubernetes until **30 June 2022**. If security
To upgrade a legacy version of Puppet Application Manager on nodes with internet access:

1. On your node (or control plane node if you have a HA deployment), rerun the installation script, passing in any arguments you included when installing for the first time:
   - For standalone installs:
     ```bash
     curl -sSL https://k8s.kurl.sh/puppet-application-manager-legacy | sudo bash -s force-reapply-addons
     ```
   - For HA installs:
     ```bash
     curl -sSL https://k8s.kurl.sh/puppet-application-manager-legacy | sudo bash -s ha force-reapply-addons
     ```

2. If a new version of Kubernetes is available, the systems provide upgrade scripts to run on each node in your cluster.
   Node draining is performed as part of a Kubernetes upgrade. The node draining process can take several minutes to complete.

   **Note:** During the Kubernetes upgrade process, nodes are not able to properly route network connections. If you have a HA deployment, make sure you have load balancers or a multi-node fail-over process in place, or schedule downtime before upgrading.

### PAM offline legacy upgrades

Use this method to upgrade Puppet Application Manager (PAM) on offline nodes from a version installed before April 2021.

#### Before you begin

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at [Backing up PAM using snapshots](#) on page 63.

**Restriction:** It is not currently possible to upgrade from an online legacy install to a new offline install configuration. Similarly, upgrades from an offline legacy configuration to a new online install are not currently supported.

**Legacy architecture is deprecated:** The legacy architecture utilizes Rook 1.0, which is incompatible with Kubernetes version 1.20 and newer versions. Kubernetes version 1.19 is no longer receiving security updates. Puppet will continue to update legacy architecture components other than Kubernetes until **30 June 2022**. If security advisories against Kubernetes 1.19 arise, the remediation path is to migrate to one of the newer architectures by following the instructions in [Disaster recovery or migration using a snapshot](#) on page 66.

To upgrade Puppet Application Manager on nodes without a connection to the internet:

1. From a workstation with internet access, download the latest version of the cluster installation bundle (note that this bundle is ~4GB):
   ```bash
   https://k8s.kurl.sh/bundle/puppet-application-manager-legacy.tar.gz
   ```

2. Copy the installation bundle to your primary and secondary Puppet Application Manager nodes and unpack it:
   ```bash
   tar xzf puppet-application-manager-legacy.tar.gz
   ```
3. Rerun the installation script. Don't forget to pass in any additional arguments you included when installing for the first time you installed the product:

For standalone installs use:

```
cat install.sh | sudo bash -s airgap force-reapply-addons
```

For HA installs use:

```
cat install.sh | sudo bash -s airgap ha force-reapply-addons
```

**Note:** During the upgrade process, follow any prompts to run commands on your other cluster nodes.

When the deployment is complete, sign into Puppet Application Manager and verify that the new version number is displayed in the bottom center of the web UI.

---

**Upgrading PAM on a customer-supported cluster**

Upgrade Puppet Application Manager (PAM) on your own Kubernetes cluster to take advantage of new features and bug fixes.

There are two possible upgrade types for customer-supported Puppet Application Manager deployments:

- **Online** - For standalone or HA installations with a connection to the internet.
- **Offline** - For air-gapped standalone or HA installations without a connection to the internet.

**How to determine your version of Puppet Application Manager**

You can use the following command to determine what version of Puppet Application Manager (PAM) you're using:

```
kubectl get installer --sort-by=.metadata.creationTimestamp -o jsonpath='{.items[-1:].metadata.name}' ; echo
```

Depending on which version you've installed, the command returns one of these values:

- **HA architecture:** puppet-application-manager
- **Standalone architecture:** puppet-application-manager-standalone
- **Legacy architecture:** Any other value, for example, puppet-application-manager-legacy, cd4pe, or comply

**Upgrade PAM on a customer-supported online cluster**

Upgrading Puppet Application Manager (PAM) on a customer-supported online Kubernetes cluster is simple and can be done with a single command.

**Before you begin**

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at Backing up PAM using snapshots on page 63.

To upgrade Puppet Application Manager on a customer-supported online cluster:

1. Upgrade kubectl KOTS:

```
curl https://kots.io/install | bash
```
2. Issue the following KOTS command:

```
kubectl kots admin-console upgrade --namespace <target namespace>
```

**Tip:** Run the `kubectl kots admin-console upgrade -h` command for more usage information.

### Upgrade PAM on a customer-supported offline cluster

Upgrading Puppet Application Manager (PAM) on a customer-supported offline Kubernetes cluster requires a few simple kubectl commands.

#### Before you begin

Make sure you have captured an up-to-date snapshot of your PAM installation, which you can use to fall back the current version if there is an issue with the upgrade process. Learn more about snapshots at Backing up PAM using snapshots on page 63.

To upgrade Puppet Application Manager on a customer-supported offline cluster, perform the following steps from a workstation that has kubectl access to the cluster:

1. Upgrade kubectl KOTS:

   ```
curl https://kots.io/install | bash
   
   ```

2. Ensure the required images are available in your local registry. Download the release assets matching the CLI version using the following command:

   ```
curl -LO https://github.com/replicatedhq/kots/releases/download/v$(kubectl kots version | head -n1 | cut -d' ' -f3)/kotsadm.tar.gz
   
   ```

3. Extract the images and push them to your private registry. Registry credentials provided in this step must have push access. These credentials are not stored anywhere or reused later.

   ```
kubectl kots admin-console push-images ./kotsadm.tar.gz
   --registry-username <rw-username>
   --registry-password <rw-password>
   
   ```

4. After you push the images to your private registry, execute the upgrade command with registry read-only credentials:

   ```
kubectl kots upgrade puppet-application-manager \
--kotsadm-namespace puppet-application-manager \
--kotsadm-registry <private.registry.host> \
--registry-username <ro-username> \
--registry-password <ro-password> \
--namespace <target namespace>
   
   ```

### Backing up PAM using snapshots

Snapshots are point-in-time backups of your Puppet Application Manager (PAM) deployment, which can be used to roll back to a previous state or restore your installation into a new cluster for disaster recovery.

**Related information**

Using sudo behind a proxy server on page 72

Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM
behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

**Full and partial snapshots**

There are two options available when you're creating a snapshot for your Puppet Application Manager (PAM) deployment, full snapshots (also known as instance snapshots) and partial (or application) snapshots. For full disaster recovery, make sure you've configured and scheduled regular full snapshots stored on a remote storage solution such as an S3 bucket or NFS share.

Full snapshots offer a comprehensive backup of your PAM deployment, because they include the core PAM application together with the Puppet applications you've installed in your PAM deployment. You can use a full snapshot to restore your PAM deployment and all of your installed Puppet applications to a previous backup. For example, you could use a full snapshot to revert an undesired configuration change or a failed upgrade, or to migrate your PAM deployment to another Puppet-supported cluster.

Partial snapshots are available from the PAM console, but are limited in their usefulness. To restore from a partial snapshot, you must already have an installed and functioning version of PAM. A functioning PAM installation is needed because the option to restore a partial snapshot can only be accessed from the Snapshots section of the PAM admin console.

Partial snapshots only back up the Puppet application you specified when you configured the snapshot, for example, Continuous Delivery for Puppet Enterprise, or Puppet Comply. They do not back up the underlying PAM deployment. Partial snapshots are sometimes useful if you want to roll back to a previous version of a specific Puppet application that you've installed on your PAM deployment, but are far less versatile than full snapshots. To make sure that you have all disaster recovery options available to you, use a full snapshot wherever possible.

**Configure snapshots**

Before using snapshots, select a storage location, set a snapshot retention period, and indicate whether snapshots are created manually or on a set schedule.

---

**Note:** The snapshots feature was accidentally disabled on some application licenses issued prior to March 2021. If you do not see a Snapshots option in your Puppet Application Manager UI, and you would like to use this feature, please contact our Support team using the Zendesk account provided to you.

A beta version of the snapshots feature, which only supported rollback snapshots, was available prior to the 15 April Puppet Application Manager release. Some features or storage locations mentioned on this page are not available on older versions of Puppet Application Manager.

---

**Important:** Disaster recovery requires that the store backend used for backups is accessible from the new cluster. When setting up snapshots in an offline cluster, make sure to record the registry service IP address with the following command:

```
kubectl -n kurl get svc registry -o jsonpath='{.spec.clusterIP}'
```

be sure to record the value returned by this command as it is required when creating a new cluster to restore to as part of disaster recovery. For more information on restoring from snapshots, see Disaster recovery or migration using a snapshot on page 66.

1. In the upper navigation bar of the Puppet Application Manager UI, click Snapshots > Settings & Schedule.
2. The snapshots feature uses https://velero.io, an open source backup and restore tool. Click Check for Velero to determine whether Velero is present on your cluster, and to install it if needed.

© 2021 Puppet, Inc.
3. Select a destination for your snapshot storage and provide the required configuration information. Supported destinations are listed below. We recommend using an external service or NFS, depending on what is available to you:

- Internal storage (default)
- Amazon S3
- Azure Blob Storage
- Google Cloud Storage
- Other S3-compatible storage
- Network file system (NFS)
- Host path

For **Amazon S3 storage**, provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket</td>
<td>The name of the AWS bucket where snapshots are stored.</td>
</tr>
<tr>
<td>Region</td>
<td>The AWS region the bucket is available in.</td>
</tr>
<tr>
<td>Path</td>
<td>Optional. The path within the bucket where all snapshots are stored.</td>
</tr>
<tr>
<td>Use IAM instance role?</td>
<td>If selected, an IAM instance role is used instead of an access key ID and secret.</td>
</tr>
<tr>
<td>Access key ID</td>
<td>Required only if not using an IAM instance role. The AWS IAM access key ID that can read from and write to the bucket.</td>
</tr>
<tr>
<td>Access key secret</td>
<td>Required only if not using an IAM instance role. The AWS IAM secret access key that is associated with the access key ID.</td>
</tr>
</tbody>
</table>

For **Azure Blob Storage**, provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket</td>
<td>The name of the Azure Blob Storage container where snapshots are stored.</td>
</tr>
<tr>
<td>Path</td>
<td>Optional. The path within the container where all snapshots are stored.</td>
</tr>
<tr>
<td>Subscription ID</td>
<td>Required only for access via service principal or AAD Pod Identity. The subscription ID associated with the target container.</td>
</tr>
<tr>
<td>Tenant ID</td>
<td>Required only for access via service principal. The tenant ID associated with the Azure account of the target container.</td>
</tr>
<tr>
<td>Client ID</td>
<td>Required only for access via service principal. The client ID of a Service Principle with access to the target container.</td>
</tr>
<tr>
<td>Client secret</td>
<td>Required only for access via service principal. The Client Secret of a Service Principle with access to the target container.</td>
</tr>
<tr>
<td>Cloud name</td>
<td>The Azure cloud for the target storage (options: AzurePublicCloud, AzureUSGovernmentCloud, AzureChinaCloud, AzureGermanCloud)</td>
</tr>
<tr>
<td>Resource group</td>
<td>The resource group name of the target container.</td>
</tr>
<tr>
<td>Storage account</td>
<td>The storage account name of the target container.</td>
</tr>
</tbody>
</table>

**Note:** Only connections via service principals are currently supported.

For **Google Cloud Storage**, provide the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bucket</td>
<td>The name of the GCS bucket where snapshots are stored.</td>
</tr>
<tr>
<td>Path</td>
<td>Optional. The path within the bucket where all snapshots are stored.</td>
</tr>
<tr>
<td>Service account</td>
<td>The GCP IAM Service Account JSON file that has permissions to read from and write to the storage location.</td>
</tr>
</tbody>
</table>
4. Click **Update storage settings** to save your storage destination information.
   Depending on your chosen storage provider, saving and configuring your storage provider might take several minutes.

5. Optional: To automatically create new snapshots on a schedule, select **Enable automatic scheduled snapshots** on the **Full snapshots (instance)** tab. (If desired, you can also set up a schedule for capturing partial (application-only) snapshots.)

   You can schedule a new snapshot creation for every hour, day, or week, or you can create a custom schedule by entering a cron expression.

6. Finally, set the retention schedule for your snapshots by selecting the time period after which old snapshots are automatically deleted. The default retention period is one month.

   **Note:** A snapshot's retention period cannot be changed once the snapshot is created. If you update the retention schedule, the new retention period applies only to snapshots created after the update is made.

7. Click **Update schedule** to save your changes.

Snapshots are automatically created according to your specified schedule and saved to the storage location you selected. You can also create an unscheduled snapshot at any time by clicking **Start a snapshot** on the Dashboard or on the Snapshots page.

### Roll back changes using a snapshot

When necessary, you can use a snapshot to roll back to a previous version of your Puppet Application Manager set-up without changing the underlying cluster infrastructure.

To roll back changes:

1. In console menu of the Puppet Application Manager UI, click **Snapshots > Full Snapshots (Instance)**.
2. Select the snapshot you wish to roll back to from the list of available snapshots and click **Restore from this backup**.
3. Follow the instructions to complete either a partial restore or a full restore.

   A full restore is useful if you need to stay on an earlier version of an application and want to disable automatic version updates. Otherwise, a partial restore is the quicker option.

### Disaster recovery or migration using a snapshot

Full disaster recovery is possible using a snapshot. You must create a new cluster to recover to, then follow the process outlined below to recover your instance from a snapshot. You can also use this workflow to migrate data from legacy to standalone deployments, legacy to HA deployments, and between standalone and HA deployments.

#### Before you begin

- On the original system, Puppet Application Manager (PAM) must be configured to support **Full Snapshots (Instance)**.
- Velero must be configured to use an external snapshot destination accessible to both the old and new clusters, such as S3 or NFS.
- Both the old and new clusters must have the same connection status (online/offline). Migrating from offline to online clusters or vice versa is not supported.
- You must use the **30 June 2021** or later release of PAM.
- For offline installs, both the old and new clusters must use the same version of PAM.
- **If you are migrating from a legacy deployment**, before beginning the migration process you must upgrade to PAM version 1.62.0 with the `force-reapply-addons` flag included in the upgrade command.

To perform data migration or disaster recovery:
1. On the original system, find the version of kURL your deployment is using. Save the version information for the next step:

```bash
kubectl get configmap -n kurl kurl-current-config -o jsonpath="{.data.kurl-version}" && echo ""
```

2. Set up a new cluster to house the recovered instance following the system requirements for your applications. **Do not install any Puppet applications after the PAM installation completes. You'll recover your Puppet applications later in the process.**

   - Install PAM using the version of kURL you retrieved earlier:
     - For online installs:
       ```bash
curl -sSL https://k8s.kurl.sh/version/<VERSION STRING>/puppet-application-manager | sudo bash <-s options>
```
     - For offline installs:
       ```bash
curl -O https://k8s.kurl.sh/bundle/version/<VERSION STRING>/puppet-application-manager.tar.gz
```
   - When setting up a new offline cluster as part of disaster recovery, add `kurl-registry-ip=<IP>` to the install options, replacing `<IP>` with the value you recorded when setting up snapshots.

   **Note:** If you do not include the `kurl-registry-ip=<IP>` flag, the registry service will be assigned a new IP address that does not match the IP on the machine where the snapshot was created. You must align the registry service IP address on the new offline cluster to ensure that the restored configuration can pull images from the correct location.

3. To recover using a snapshot saved to a **host path**, ensure user/group 1001 has full access on all nodes by running:

   ```bash
   chown -R 1001:1001 /<PATH/TO/HOSTPATH>
   ```

4. Configure the new cluster to connect to your snapshot storage location. Run the following to see the arguments needed to complete this task:

   ```bash
   kubectl kots -n default velero configure-{hostpath,nfs,aws-s3,other-s3,gcp} --help
   ```

5. Run `kubectl kots get backup` and wait for the list of snapshots to become available. This might take several minutes.

6. Start the restoration process by running `kubectl kots restore --from-backup <BACKUP NAME>`. The restoration process takes several minutes to complete. When the PAM UI is available, use it to monitor the status of the application.

   **Note:** When restoring, wait for all restores to complete before making any changes. The following command waits for pods to finish restoring data from backup. Other pods may not be ready until updated configuration is deployed in the next step:

   ```bash
   kubectl get pod -o json | jq -r '..items[] | select(.metadata.annotations."backup.velero.io/backup-volumes") | .metadata.name' | xargs kubectl wait --for=condition=Ready pod --timeout=20m
   ```

   This command requires the **jq** CLI tool to be installed. It is available in most Linux OS repositories.

© 2021 Puppet, Inc.
7. After the restoration process completes, save your config and deploy:
   a) From the PAM UI, click **Config**.
   b) (Optional) If the new cluster's hostname is different from the old one, update the **Hostname**.
   c) Click **Save Config**.
   d) Deploy the application. You must save your config and deploy even if you haven't made any changes.

   **Note:** If you have installed Continuous Delivery for PE and changed the hostname, you need to update the webhooks that connect Continuous Delivery for PE with your source control provider. For information on how to do this, see Update webhooks.

### Troubleshooting PAM

Use this guide to troubleshoot issues with your Puppet Application Manager installation.

#### How to determine your version of Puppet Application Manager

You can use the following command to determine what version of Puppet Application Manager (PAM) you're using:

```
kubectl get installer --sort-by=.metadata.creationTimestamp -o jsonpath='{{.items[-1].metadata.name}}'; echo
```

Depending on which version you've installed, the command returns one of these values:

- **HA architecture**: `puppet-application-manager`
- **Standalone architecture**: `puppet-application-manager-standalone`
- **Legacy architecture**: Any other value, for example, `puppet-application-manager-legacy`, `cd4pe`, or `comply`

#### Resolve IP address range conflicts

When installing Puppet Application Manager, IP address ranges `10.96.0.0/22` and `10.32.0.0/22` must not be used by other nodes on the local network.

**Note:** The minimum size for CIDR blocks used by Puppet Application Manager are:

- **Standalone** - `/24` for pod and service CIDRs
- **HA** - `/23` for pod and service CIDRs
- Default of `/22` is recommended to support future expansion

To resolve IP address range conflicts, create a `patch.yaml` file and add the `installer-spec-file=patch.yaml` argument when running the installation script (see below):

1. If you use IP addresses internally that overlap `10.32.0.0/22`, add the following to your `patch.yaml` file (`10.40.0.0/23` used here as an example range):

```
apiVersion: cluster.kurl.sh/v1beta1
kind: Installer
metadata:
  name: patch
spec:
  weave:
    podCIDR: 10.40.0.0/23
    podCidrRange: "/23"
```

© 2021 Puppet, Inc.
2. If you use IP addresses internally that overlap 10.96.0.0/22, add the following to your `patch.yaml` file (10.100.0.0/23 used here as an example range):

   ```yaml
   spec:
     ...
     kubernetes:
       serviceCIDR: 10.100.0.0/23
       serviceCidrRange: "/23"
   ```

   **CAUTION:** The `podCIDR` and `serviceCIDR` ranges must not overlap.

3. Once your `patch.yaml` file is set up, add the `installer-spec-file=patch.yaml` argument when you run the installation script:

   ```bash
   cat install.sh | sudo bash -s airgap installer-spec-file=patch.yaml
   ```

   **Remember:** Add the `installer-spec-file=patch.yaml` argument any time you re-run the installation script, such as when reinstalling to upgrade to a new version.

**Related information**

*Using sudo behind a proxy server* on page 72

Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

**Reset the PAM password**

As part of the installation process, Puppet Application Manager (PAM) generates a password for you. You can update this password to one of your choosing after installation.

1. To reset the Puppet Application Manager password, run:

   ```bash
   kubectl -n default kots reset-password
   ```

   The system prompts you to enter a new password of your choosing.

2. If the command fails with an unknown command "kots" for "kubectl" error, it's because `/usr/local/bin` is not in the path. To address this error, either update the path to include `/usr/local/bin`, or run:

   ```bash
   /usr/local/bin/kubectl-kots reset-password default
   ```

**Update the PAM TLS certificate**

A self-signed TLS certificate secures the connection between your browser and Puppet Application Manager (PAM). Once the initial Puppet Application Manager setup process is complete, you can upload new certificates by enabling changes to the installation’s Kubernetes secrets.

Use this process if you chose not to add a TLS certificate when installing Puppet Application Manager, or if you need to update your existing TLS certificate.

1. Enable changes to your installation's `kotsadm-tls` Kubernetes secret by running:

   ```bash
   kubectl -n default annotate secret kotsadm-tls acceptAnonymousUploads=1
   ```

© 2021 Puppet, Inc.
2. Restart the `kurl-proxy` pod to deploy the change by running:

```bash
thebeh correct pods $(kubectl get pods -A | grep kurl-proxy | awk '{print $2}')
```

3. Once the `kurl-proxy` pod restarts and is back up and running, navigate to `https://<HOSTNAME>:8800/tls` and upload your new TLS certificate.

### Reduce recovery time when a node fails

If a node running a non-replicated service like PostgreSQL fails, expect some service downtime.

How much downtime depends on the following factors:

- Timeout for communication between Kubernetes services (at least one minute to mark the node as unreachable).
- Timeout for the ekco service to determine that pods need to be rescheduled. The default is five minutes after node is marked unreachable.
- Time to restart services (at least two minutes, possibly up to five minutes, if there are complex dependencies).

The ekco service can be configured to reschedule pods more quickly by configuring the installation with a `patch.yaml` similar to the following:

```yaml
apiVersion: cluster.kurl.sh/v1beta1
kind: Installer
metadata:
  name: patch
spec:
  ekco:
    nodeUnreachableToleration: 1m
```

Apply the patch during an install or upgrade by including `installer-spec-file=patch.yaml` as an install option.

**Important:** This patch needs to be included during all future upgrades to avoid resetting the option.

### PAM components

Puppet Application Manager (PAM) uses a range of mandatory and optional components.

#### Support services

- Database: PostgreSQL (single instance) - [https://www.postgresql.org/](https://www.postgresql.org/)
- Object storage: previously MinIO - [https://min.io](https://min.io) now Ceph - [https://ceph.io](https://ceph.io)
- `tls`er for basic TLS cert management - [https://github.com/puppetlabs/tls](https://github.com/puppetlabs/tls)
- `kurl_proxy` for HTTPS proxying outside the Ingress (ports besides 80/443): [https://github.com/replicatedhq/kots/tree/v1.36.1/kurl_proxy](https://github.com/replicatedhq/kots/tree/v1.36.1/kurl_proxy)

#### Kubernetes components

- Storage (CSI): Rook - [https://rook.io](https://rook.io), Ceph - [https://ceph.io](https://ceph.io)
- Ingress: Project Contour - [https://projectcontour.io](https://projectcontour.io)
- Kubernetes Cluster: kURL - [https://kurl.sh](https://kurl.sh)
- Embedded kURL Cluster Operator: ekco - [https://github.com/replicatedhq/ekco](https://github.com/replicatedhq/ekco)
- Admin Console: KOTS - [https://kots.io](https://kots.io)
- Snapshots: Velero - [https://velero.io](https://velero.io), Restic - [https://restic.net](https://restic.net)
- Monitoring: Prometheus - [https://prometheus.io](https://prometheus.io)
- Registry: Docker Registry - [https://docs.docker.com/registry/](https://docs.docker.com/registry/)
Optional components

Prometheus (+Grafana) and Velero (+Restic) are optional components:

- Prometheus+Grafana uses 112m/node + 600m CPU, 200MiB/node + 1750MiB RAM
- Velero+Restic uses 500m/node + 500m CPU, 512MiB/node + 128MiB RAM

If you do not need these optional components, they can be omitted from the initial install and further upgrades with a patch similar to the following:

```yaml
apiVersion: cluster.kurl.sh/v1beta1
kind: Installer
metadata:
  name: patch
spec:
  prometheus:
    version: ''
  velero:
    version: ''
```

**Important:** This patch needs to be included during upgrades to avoid adding the components later.

If you want to remove optional components that are already installed, use the following command:

```
kubectl delete ns/monitoring ns/velero
```

Load balancing

The following load balancer requirements are needed for a HA install:

- A network (L4, TCP) load balancer for port 6443 across primary nodes. This is required for Kubernetes components to continue operating in the event that a node fails. The port is only accessed by the Kubernetes nodes and any admins using `kubectl`.
- A network (L4, TCP) or application (L7, HTTP/S) load balancer for ports 80, and 443 across all primaries and secondaries. This maintains access to applications in event of a node failure. Include 8800 if you want external access to the Puppet Application Manager UI.

**Note:** Include port 8000 for webhook callbacks if you are installing Continuous Delivery for PE.

**Important:** If you are using application load balancing, be aware that Ingress items use Server Name Indication (SNI) to route requests, which may require additional configuration with your load balancer. If your load balancer does not support SNI for health checks, enable **Enable load balancer HTTP health check** in the Puppet Application Manager UI **Config** page.

Generate a support bundle

When seeking support, you might be asked to generate and provide a support bundle. This bundle collects a large amount of logs, system information and application diagnostics.

To create a support bundle:

1. In Puppet Application Manager UI, click **Troubleshoot > Generate a support bundle**.
2. Select a method for generating the support bundle:

   - **Generate the bundle automatically.** Click Analyze `<APPLICATION NAME>` (<APPLICATION NAME> is replaced in the UI by the name of the Puppet application you have installed), and Puppet Application Manager generates the bundle for you and uploads it to the **Troubleshoot** page.
   - **Generate the bundle manually.** Click the prompt to generate a custom command for your installation, then run the command on your cluster. Follow the prompts to upload the bundle to Puppet Application Manager.
3. Review the collected data before forwarding it to Puppet, as it may contain sensitive information that you wish to redact.

4. Return to the **Troubleshoot** page, download the newly created support bundle, and send it to your Puppet Support contact.

**Create a support bundle from the command line**

If installation of the Puppet Application Manager, or upload of an app, on an embedded kURL cluster fails, it may not be possible to access the UI to generate a support bundle.

You can generate a support bundle by using the default kots.io spec. To do this, run the following command:

```
kubectl support-bundle https://kots.io
```

On an offline server, you can copy the default kots.io spec by using the following command:

```
curl -o spec.yaml https://kots.io -H 'User-agent:Replicated_Troubleshoot/v1beta1'
```

The spec can then be uploaded to the server. Use the local spec by running:

```
kubectl support-bundle /path/to/spec.yaml
```

If the Puppet Application Manager UI is working and the app is installed, you can use:

```
kubectl support-bundle http://<server-address>:8800/api/v1/troubleshoot/<app-slug>
```

If the app is not installed but the Puppet Application Manager UI is running:

```
kubectl support-bundle http://<server-address>:8800/api/v1/troubleshoot
```

If you do not already have the support-bundle kubectl plugin installed, install it by using the command below:

```
curl https://krew.sh/support-bundle | bash
```

Or by installing krew2 and running:

```
kubectl krew install support-bundle
```

**Using sudo behind a proxy server**

Many of the commands you run to install or configure Puppet Application Manager (PAM) require root access. In the PAM documentation, commands that require root access use `sudo` to elevate privileges. If you're running PAM behind a proxy, `sudo` might not work correctly. If you're having trouble running commands with `sudo`, and you're behind a proxy, try switching to the `root` user and running the command without `sudo`.

**Installing**

To begin using Puppet Comply, you must first complete the initial setup process.

- **System requirements** on page 73

Refer to these system requirements to allow your Puppet Comply application to connect to Puppet Enterprise (PE).

- **Set up Comply** on page 73

To start using Puppet Comply, you must complete the setup process, using both Puppet Application Manager (PAM) and Puppet Enterprise (PE).
• Uninstall Comply on page 83
Uninstall Comply by deleting the Comply application and purging the Kubernetes cluster.

System requirements
Refer to these system requirements to allow your Puppet Comply application to connect to Puppet Enterprise (PE).

Open port requirements
Comply is deployed on a Kubernetes cluster, which requires the following ports:

<table>
<thead>
<tr>
<th>Port</th>
<th>Protocol</th>
<th>Purpose</th>
<th>Source</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>PE ports</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8140</td>
<td>TCP</td>
<td>Preflight checks</td>
<td>Comply</td>
<td>Puppet primary server</td>
</tr>
<tr>
<td>8143</td>
<td>TCP</td>
<td>PE integration</td>
<td>Comply</td>
<td>PE Orchestrator</td>
</tr>
<tr>
<td>8081</td>
<td>TCP</td>
<td>PE integration</td>
<td>Comply</td>
<td>PuppetDB</td>
</tr>
<tr>
<td>4433</td>
<td>TCP</td>
<td>PE integration</td>
<td>Comply</td>
<td>PE RBAC</td>
</tr>
<tr>
<td>Comply ports</td>
<td></td>
<td>Comply access</td>
<td>User browser</td>
<td>Comply UI</td>
</tr>
<tr>
<td>443</td>
<td>TCP</td>
<td>Sending reports</td>
<td>Scan target node</td>
<td>Comply server</td>
</tr>
<tr>
<td>30303</td>
<td>TCP</td>
<td>Assessor downloads and sending reports</td>
<td>Scan target node</td>
<td>Comply</td>
</tr>
</tbody>
</table>

Note: Port 30303 is not needed if you bring your own ingress. You can also set a custom Comply port in the Comply port field on the Config tab in Puppet Application Manager if you do not want to use port 30303.

Supported Puppet Enterprise versions
The following versions of Puppet Enterprise (PE) are supported for use with Comply:

<table>
<thead>
<tr>
<th>PE version</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2019.8.4 and later</td>
<td></td>
</tr>
</tbody>
</table>

For more on PE versions, see Puppet Enterprise support lifecycle.

Set up Comply
To start using Puppet Comply, you must complete the setup process, using both Puppet Application Manager (PAM) and Puppet Enterprise (PE).

Important: Before you set up Comply, make sure you have installed Puppet Application Manager (PAM), Puppet Enterprise (PE) and reviewed the system requirements.

Setting up Comply involves the following steps:

• Configure Comply in Puppet Application Manager (PAM) in an online or offline environment. You can use the default ingress or, if you prefer, a custom NGINX ingress.
• Configure Comply TLS certificates in Puppet Enterprise (PE). You can configure these for the default ingress or, if you prefer, a custom NGINX ingress.
• Install the comply module.
• Classify the nodes you want to scan in PE.
• Deploy Comply.
• Add your PE credentials to Comply.

- Configure Comply in an online environment on page 74
The Comply configuration process creates a Kubernetes cluster and installs the application on that cluster.
- Configure Comply in an offline environment on page 75
Configure Puppet Comply in an air-gapped or offline environment where the Comply host server does not have direct access to the internet.
- Configure Comply for a custom NGINX ingress (online environment) on page 77
The Comply configuration process requires some extra configuration parameters if you use a custom NGINX ingress.
- Configure Comply for a custom NGINX ingress (offline environment) on page 77
Configure Puppet Comply in an air-gapped or offline environment where the Comply host server does not have direct access to the internet.
- Configure Comply TLS certificates for a custom NGINX ingress on page 78
You need to generate certificates for Comply in Puppet Enterprise (PE) to enable automatic upgrades of the CIS-CAT assessor and for tasks to upload reports.
- Configure Comply TLS certificates on page 75
You need to generate certificates for Comply in Puppet Enterprise (PE) to enable automatic upgrades of the CIS-CAT assessor and for tasks to upload reports.
- Install the Comply module on page 80
Install the Comply module from Puppet Forge.
- Classify the nodes you want to scan on page 81
In Puppet Enterprise (PE), classify the nodes you want to scan.
- Deploy Comply on page 82
Now that you have completed the setup process, you can deploy Comply.
- Add your PE credentials to Comply on page 82
To allow Comply to communicate with PE, you must add your PE credentials to Comply.

Configure Comply in an online environment
The Comply configuration process creates a Kubernetes cluster and installs the application on that cluster.

Before you begin
Follow the instructions to install Puppet Application Manager.

1. In Puppet Application Manager, upload your Comply license and follow the prompts.
   You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets Comply system requirements.
   
   Note: The license file is issued by Puppet. If you do not have a license file, contact your Puppet representative. You must also agree to our license agreement. If your licence terms update, for example the expiry date or number of licensed nodes, upload your updated license file to Puppet Application Manager.

2. To configure your installation, click Config.
   a) In the Hostname field, enter the fully qualified domain name (FQDN) that you want to use to access Comply.
      For example, this could be the name of the node you have installed Comply on. If you choose to use an FQDN that is different from the name of this node, you must configure your domain name system (DNS) to resolve the FQDN to the IP address of the Comply node.
   b) Configure any other settings on the page relevant to your installation.
   c) When you have finished making any necessary changes to the configuration, click Continue.
3. Monitor the new version's preflight checks. The **Running Checks** indicator is shown on the screen while your system is checked to make sure your cluster meets minimum system requirements. When the preflight check is complete:

- If the status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

| Important: Do not move on until all preflight checks pass. |

- If the status is **Ready to Deploy**, move on to the next step.

**Generate Comply certificates in PE.**

### Configure Comply in an offline environment

Configure Puppet Comply in an air-gapped or offline environment where the Comply host server does not have direct access to the internet.

#### Before you begin

Follow the instructions to install Puppet Application Manager.

1. In Puppet Application Manager, upload your Comply licence and follow the prompts.

   You'll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets Comply system requirements.

   | Note: The license file is issued by Puppet. If you do not have a license file, contact your Puppet representative. You must also agree to our license agreement. If your licence terms update, for example the expiry date or number of licensed nodes, upload your updated license file to Puppet Application Manager. |

2. When prompted, upload the `.airgap` bundle for the most recent version of Comply.

   | Note: Puppet provides you with a custom URL from which to download the Comply `.airgap` file. Please open a ticket with Puppet Support to receive your custom download URL. |

3. To configure your installation, click **Config**.

   a) In the **Hostname** field, enter the fully qualified domain name (FQDN) that you want to use to access Comply.

      For example, this could be the name of the node you have installed Comply on. If you choose to use an FQDN that is different from the name of this node, you must configure your domain name system (DNS) to resolve the FQDN to the IP address of the Comply node.

   b) Configure any other settings on the page relevant to your installation.

   c) When you have finished making any necessary changes to the configuration, click **Continue**.

4. Monitor the new version's preflight checks. The **Running Checks** indicator is shown on the screen while Comply checks your system to make sure your cluster meets minimum system requirements. When the preflight check is complete:

- If the status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

| Important: Do not move on until all preflight checks pass. |

- If the status is **Ready to Deploy**, move on to the next step.

**Generate Comply certificates in PE.**

### Configure Comply TLS certificates

You need to generate certificates for Comply in Puppet Enterprise (PE) to enable automatic upgrades of the CIS-CAT assessor and for tasks to upload reports.
Before you begin

Make sure you have configured Comply in Puppet Application Manager (PAM).

Certificates are required when setting up Comply for the following interactions:

- **Interactions between Comply and PE.** Interactions between Comply and PE require correct configuration of the CA certificate. Any issues with the CA certificate with regard to communication between Comply and PE result in an error on the Comply UI.
- **Agent runs.** If you have set up the Comply module to download the assessor from the Comply server (as opposed to being hosted locally) then the assessor is downloaded using Mutual Transport Layer Security (MTLS) with the client certificate from the node. The Comply mtls-proxy component requires the configured TLS and CA certificate.
- **Scan task runs.** Running a scan sends reports back into Comply via an HTTP POST. This POST goes through the mtls-proxy and use MTLS with the client certificate from the node.

Configuring Comply TLS certificates involves first generating the certificates in Puppet Enterprise (PE) and then setting up Mutual Transport Layer Security (MTLS) in Puppet Application Manager (PAM). MTLS enables a secure authenticated connection between your nodes and Comply.

For information on troubleshooting problems with certificates, see Troubleshooting TLS issues in Comply on page 95.

1. SSH into your PE primary server and generate the certificates:

```bash
puppetserver ca generate --certname <COMPLY-HOSTNAME>
```

This command does the following:

- Saves the private key to `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem`
- Saves the certificate to `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem`

2. Log in to Puppet Application Manager, click the **Version history** tab, and click **Check for update**.
3. Click the **Config** tab, and scroll down to **Transport layer security (TLS) certificates to interact with PE**.
4. Ensure **Use a NodePort** is selected. If you want to change the Comply port from the default (30303), add the new port number in the **Comply port for PE nodes** field.

   **Note:** To host the assessor on your own supported cluster via NGINX ingress, see Configure Comply for a custom NGINX ingress (online environment) on page 77 and Configure Comply TLS certificates for a custom NGINX ingress on page 78.

5. Enter the hostname of your PE instance in the **PE hostname** field to enable validation of the keys and certificates added in the next step.
6. Upload the signed certificate public key, the private key files, and the CA certificate, with the following locations:

   - Paste the contents of `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem` to the **TLS certificate** field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem` to the **TLS private key** field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/ca/ca_crt.pem` to the **CA certificate** field.

7. Click **Save Config**.
8. Monitor the new version's preflight checks. The **Running Checks** indicator is shown on the screen while your system is checked to make sure your cluster meets minimum system requirements.

   The **Config: Check if we can connect to PE using provided certificates** preflight passes if the certificates are configured correctly.

   • If the preflight checks status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

   **Important:** Do not move on until all preflight checks pass.

   • If the preflight checks status is **Ready to Deploy**, move on to the next step.

9. Click **Deploy**.

   **Install the comply module.**

   **Configure Comply for a custom NGINX ingress (online environment)**

   The Comply configuration process requires some extra configuration parameters if you use a custom NGINX ingress.

   **Before you begin**

   Follow the instructions to **install Puppet Application Manager**.

   1. In Puppet Application Manager, upload your Comply license and follow the prompts.

      You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets Comply system requirements.

      **Note:** The license file is issued by Puppet. If you do not have a license file, contact your Puppet representative. You must also agree to our license agreement. If your licence terms update, for example the expiry date or number of licensed nodes, upload your updated license file to Puppet Application Manager.

   2. To configure your installation, click **Config**.

      a) In the **Hostname** field, enter the fully qualified domain name (FQDN) that you want to use to access Comply.

         For example, this could be the name of the node you have installed Comply on. If you choose to use an FQDN that is different from the name of this node, you must configure your domain name system (DNS) to resolve the FQDN to the IP address of the Comply node.

      b) In the **Configure access** section, add the following annotations to configure the Ingress if you use cert-manager.

         ```
         kubernetes.io/ingress.class: nginx
         cert-manager.io/cluster-issuer: letsencrypt-prod
         ```

      c) Configure any other settings on the page relevant to your installation.

      d) When you have finished, click **Continue**.

   3. Monitor the new version's preflight checks. The **Running Checks** indicator is shown on the screen while your system is checked to make sure your cluster meets minimum system requirements. When the preflight check is complete:

      • If the status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

      **Important:** Do not move on until all preflight checks pass.

      • If the status is **Ready to Deploy**, move on to the next step.

   **Configure Comply TLS certificates for a custom NGINX ingress** on page 78.

   **Configure Comply for a custom NGINX ingress (offline environment)**

   Configure Puppet Comply in an air-gapped or offline environment where the Comply host server does not have direct access to the internet.

© 2021 Puppet, Inc.
Before you begin
Follow the instructions to install Puppet Application Manager.

1. In Puppet Application Manager, upload your Comply licence and follow the prompts.
   You’ll be guided through the process of setting up SSL certificates, uploading a license, and checking to make sure your infrastructure meets Comply system requirements.

   **Note:** The license file is issued by Puppet. If you do not have a license file, contact your Puppet representative. You must also agree to our license agreement. If your licence terms update, for example the expiry date or number of licensed nodes, upload your updated license file to Puppet Application Manager.

2. When prompted, upload the `.airgap` bundle for the most recent version of Comply.

   **Note:** Puppet provides you with a custom URL from which to download the Comply `.airgap` file. Please open a ticket with Puppet Support to receive your custom download URL.

3. To configure your installation, click Config.
   a) In the Hostname field, enter the fully qualified domain name (FQDN) that you want to use to access Comply.
      For example, this could be the name of the node you have installed Comply on. If you choose to use an FQDN that is different from the name of this node, you must configure your domain name system (DNS) to resolve the FQDN to the IP address of the Comply node.
   b) In the Configure access section, add the following annotations to configure the Ingress if you use cert-manager.

      ```
      kubernetes.io/ingress.class: nginx
      cert-manager.io/cluster-issuer: letsencrypt-prod
      ```
   c) Configure any other settings on the page relevant to your installation.
   d) When you have finished making any necessary changes to the configuration, click Continue.

4. Monitor the new version's preflight checks. The Running Checks indicator is shown on the screen while Comply checks your system to make sure your cluster meets minimum system requirements. When the preflight check is complete:
   a) If the status is Checks Failed, click View preflights. Correct the issues and click Re-run. Repeat this step as needed.
   b) If the status is Ready to Deploy, move on to the next step.

   **Important:** Do not move on until all preflight checks pass.

Configure Comply TLS certificates for a custom NGINX ingress

Configure Comply TLS certificates for a custom NGINX ingress

You need to generate certificates for Comply in Puppet Enterprise (PE) to enable automatic upgrades of the CIS-CAT assessor and for tasks to upload reports.

**Before you begin**

Make sure you have configured Comply in Puppet Application Manager (PAM) and you have followed the instructions in Configure Comply for a custom NGINX ingress (online environment) on page 77 or Configure Comply for a custom NGINX ingress (offline environment) on page 77 as appropriate to your implementation.

This process involves generating certificates in Puppet Enterprise (PE) and setting up Mutual Transport Layer Security (MTLS) in Puppet Application Manager (PAM). MTLS enables a secure authenticated connection between your nodes and Comply.

Certificates are required when setting up Comply for the following interactions:
• **Interactions between Comply and PE.** Interactions between Comply and PE require correct configuration of the CA certificate. Any issues with the CA certificate with regard to communication between Comply and PE result in an error on the Comply UI.

• **Agent runs.** If you have set up the Comply module to download the assessor from the Comply server (as opposed to being hosted locally) then the assessor is downloaded using Mutual Transport Layer Security (MTLS) with the client certificate from the node. The Comply mtls-proxy component requires the configured TLS and CA certificate.

• **Scan task runs.** Running a scan sends reports back into Comply via an HTTP POST. This POST goes through the mtls-proxy and use MTLS with the client certificate from the node.

Configuring Comply TLS certificates involves first generating the certificates in Puppet Enterprise (PE) and then setting up Mutual Transport Layer Security (MTLS) in Puppet Application Manager (PAM). MTLS enables a secure authenticated connection between your nodes and Comply.

For information on troubleshooting problems with certificates, see [Troubleshooting TLS issues in Comply](#) on page 95.

1. SSH into your PE primary server and generate the certificates:

   ```bash
puppetserver ca generate --certname <COMPLY-HOSTNAME>
   ```

   This command does the following:

   - Saves the private key to `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem`
   - Saves the certificate to `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem`

2. Log in to Puppet Application Manager, click the [Version history](#) tab, and click [Check for update](#).

3. Click the [Config](#) tab, and scroll down to [Transport layer security (TLS) certificates to interact with PE](#).

4. Select [Use an ingress with a hostname](#).

5. Enter the fully-qualified domain name in the [PE TLS hostname](#) field using the same fully-qualified domain name that you used to generate the TLS certificates.

   **Important:** The fully-qualified domain name in the [PE TLS hostname](#) field MUST be different from that used in the [Hostname](#) field in the Required set-up area.

6. Check that the following annotations are in the [SSL Passthrough Annotation](#) field and add them if not:

   ```
   kubernetes.io/ingress.class: nginx
   nginx.ingress.kubernetes.io/ssl-passthrough: "true"
   ```

   **Note:** If you are not using NGINX, replace these annotations with those specific to your chosen ingress controller. For example, add [OpenShift as an MLTS proxy for PE certificates](#).

7. Enter the hostname of you PE instance in the [PE hostname](#) field to enable validation of the keys and certificates added in the next step.

8. Copy the signed certificate public key, the private key files, and the CA certificate, to the following locations:

   - Paste the contents of `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem` to the [TLS certificate](#) field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem` to the [TLS private key](#) field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/ca/ca_crt.pem` to the [CA certificate](#) field.

9. Click [Save Config](#).
10. Monitor the new version's preflight checks. The **Running Checks** indicator is shown on the screen while Comply checks your system to make sure your cluster meets minimum system requirements. When the preflight check is complete:

- If the status is **Checks Failed**, click **View preflights**. Correct the issues and click **Re-run**. Repeat this step as needed.

**Important:** Do not move on until all preflight checks pass.

If the status is **Ready to Deploy**, move on to the next step.

11. The nginx-ingress controller configuration is configured with the `--enable-ssl-passthrough` setting disabled by default. This feature is required to enable passthrough in Ingress controller, allowing for the connection to be accepted by the application backends.

   a) To edit the configuration inline with the running configuration, execute:

   ```
   kubectl edit deployment -n <namespace> <ingress-controller>
   ```

   b) Find the `spec: configuration` section in the `ingress-nginx-deployment.yaml` and append `--enable-ssl-passthrough` under `containers: -args`. For example:

   ```
   apiVersion: apps/v1
   kind: Deployment
   metadata:
    [...]  
   spec:
    containers:
     - args:
      ...  
     - --enable-ssl-passthrough
   ```

Install the Comply module.

**Install the Comply module**

Install the Comply module from Puppet Forge.

**Before you begin**

Make sure you have generated the Comply certificates in PE.

Modules are self-contained, shareable bundles of code and data. The Comply module contains a Bolt task — the tool that runs the CIS assessor on your nodes.

The Comply module lives on Puppet Forge, a repository of thousands of modules. If you're new to PE and Comply, see Managing environment content with a Puppetfile for more information on the Puppetfile and installing modules.
1. Go to the comply module on the Forge.

Follow the instructions in the r10k or Code Manager drop down to add the module declaration to your Puppetfile. You also need to add its dependencies. For example:

```plaintext
# Puppet comply module
mod 'puppetlabs/comply', '2.4.0'

# dependencies for comply
mod 'puppet/archive', '6.0.2'
mod 'puppetlabs/chocolatey', '6.1.0'
mod 'puppetlabs/inifile', '5.2.0'
mod 'puppetlabs/java', '7.3.0'
mod 'puppetlabs/ruby_task_helper', '0.6.0'
mod 'puppetlabs/stdlib', '8.1.0'
mod 'puppetlabs/powershell', '5.0.0'
mod 'puppetlabs/registry', '4.0.1'
mod 'puppetlabs/pwshlib', '0.10.1'
```

If you don’t specify options, Code Manager installs the latest version and does not update it automatically. To always have the latest version installed, specify `:latest` and it updates automatically when a new version is released. Make sure you are always running the latest version of Comply if you intend to use the `:latest` keyword to update the Comply module. To install a specific version of the module that does not update automatically, specify the version number as a string.

**Important:** If you choose a specific version of the module, it MUST be the same as the Comply version. For example, version 2.3.0 of the module must be installed for Comply 2.3.0.

**Note:** When configuring the Comply module for macOS or CentOS 8, you must set the `manage_java` parameter to `false` as the management of Java is not supported.

2. SSH into your PE primary server and deploy the code:

   ```bash
   puppet-code deploy --all
   ```

Classify the nodes you want to scan in Puppet Enterprise (PE).

**Classify the nodes you want to scan**

In Puppet Enterprise (PE), classify the nodes you want to scan.

**Before you begin**

Make sure you have installed the comply module.

Classification is when you create a node group, add nodes to the group, and assign classes to the group — in this case, the comply class. Classes are the blocks of Puppet code used to configure nodes and assign resources to them. If you are new to Puppet, see Grouping and classifying nodes for more information.

1. In the PE console, click Node groups.
2. Create a new node group or select an existing node group that you want to scan.
3. On the Classes tab — in the Add new class field — select the comply class.
4. Click Add class.
5. In your new comply class, select the scanner_source Parameter.

**Note:** Parameters allow a class to request external data.
6. Change the default parameter **Value** to one of the following assessor distribution files:
   - If using the Puppet supported cluster: https://<COMPLY-HOSTNAME>:30303/assessor
   - If using NGINX Ingress: https://<PE-TLS-FQDN>/assessor

7. Click **Add to node group**, and then commit the changes.

8. Run Puppet **twice**.

   **Deploy Comply.**

**Related information**

- Create a custom profile on page 87
- Create a custom profile based on an existing benchmark.

**Deploy Comply**

Now that you have completed the setup process, you can deploy Comply.

**Before you begin**

Make sure you have classified the nodes you want to scan in Puppet Enterprise (PE).

1. Navigate to Puppet Application Manager. Once the version is ready to deploy, click **Deploy**. On the **Application** tab, monitor the application for readiness.

   The application's status is shown as **Missing** for several minutes while deployment is underway.

   **Tip:** You can monitor the deployment's progress by running `kubectl get pods --watch`.

   When the deployment is complete, the application status changes to **Ready**. Comply is now deployed!

2. Navigate to https://<COMPLY-HOSTNAME> using the name of the Hostname FQDN you created earlier and sign into Comply using the default values:

   - **username:** comply
   - **password:** compliance

   You are then prompted to create a new password.

**Add your PE credentials to Comply.**

To allow Comply to communicate with PE, you must add your PE credentials to Comply.

**Before you begin**

Make sure you have **deployed Comply**.

Adding your PE credentials authenticates Comply with Role Based Access Control (RBAC). Your PE account requires the following permissions:

<table>
<thead>
<tr>
<th>Type</th>
<th>Action</th>
<th>Instance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>View</td>
<td>-</td>
</tr>
<tr>
<td>Job Orchestrator</td>
<td>Start, stop and view jobs</td>
<td>-</td>
</tr>
<tr>
<td>Node Groups</td>
<td>View</td>
<td>All</td>
</tr>
<tr>
<td>Nodes</td>
<td>View node data from PuppetDB</td>
<td>-</td>
</tr>
<tr>
<td>Tasks</td>
<td>Run Tasks</td>
<td>Task: comply::backup_assessor Permitted on: All nodes</td>
</tr>
</tbody>
</table>
### Uninstall Comply

Uninstall Comply by deleting the Comply application and purging the Kubernetes cluster.

1. From the command line of the node where you have Comply installed, run the following command to delete the Comply application:

   ```bash
   # kubectl delete $(kubectl api-resources --verbs=delete -o name | paste -sd "," -) -A -l app.kubernetes.io/part-of=comply
   ```

2. On the same node, run the following command to uninstall the embedded Kubernetes cluster:

   ```bash
   curl https://k8s.kurl.sh/comply/tasks.sh | sudo bash -s reset
   ```

   **Note:** This command resets the Replicated installation with a purge.

3. Reboot your node to clear the `kube-ipvs0` device.

### Upgrading

New versions of Puppet Comply are released regularly. Upgrading to the current version ensures you are always taking advantage of the latest features, fixes, and improvements.

**Important:** The CIS-CAT assessor setup process is embedded in the `comply` module. To ensure you always have the latest version, upgrade the `comply` module before you upgrade the Comply application. Note that you cannot run scans until you complete both of these upgrades.

#### Upgrade from Comply 1.0.4 to 2.4.0

Comply 2.4.0 automatically upgrades the CIS-CAT assessor to the latest version every time you upgrade Comply.

The upgrade process involves generating certificates in Puppet Enterprise (PE) and setting up Mutual Transport Layer Security (MTLS) in Puppet Application Manager (PAM). MTLS enables a secure authenticated connection between your nodes and Comply.
1. SSH into your PE primary server and generate the certificates:

   `puppetserver ca generate --certname <COMPLY-HOSTNAME>`

   This command does the following:
   - Saves the private key to `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem`
   - Saves the certificate to `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem`

2. Log in to Puppet Application Manager, click the Version history tab, and click Check for update.

3. Click the Config tab, and scroll down to Transport layer security (TLS) certificates to interact with PE.

4. Upload the signed certificate public key, the private key files, and the CA certificate, with the following locations:
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/certs/<COMPLY-HOSTNAME>.pem` to the TLS certificate field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/private_keys/<COMPLY-HOSTNAME>.pem` to the TLS private key field.
   - Paste the contents of `/etc/puppetlabs/puppet/ssl/ca/ca_crt.pem` to the CA certificate field.

   **Note:** To host the assessor on your own supported cluster via NGINX ingress, click the Bring your own NGINX ingress check box and enter the FQDN in the PE TLS FQDN field — using the same FQDN that you used to generate the TLS certificates.

5. Click Save Config.

6. Navigate to Puppet Enterprise (PE), and update the default value of the comply class scanner_source parameter to one of the following assessor distribution files:
   - If using the Puppet supported cluster: `https://<COMPLY-HOSTNAME>:30303/assessor`
   - If using NGINX Ingress: `scanner_source` to: `https://<PE-TLS-FQDN>/assessor`

   For more information, see Classify the nodes you want to scan in PE.

7. Click Add to node group, and then commit the changes.

8. Upgrade the comply module.
   a) Update your Puppetfile with the latest version of the comply module and its dependencies.
   b) Deploy code by running the `puppet-code deploy --all` command.

9. Navigate back to Puppet Application Manager. After pre-flight checks have completed successfully, click Go to updated version, and then click Deploy.

   **Note:** If the upgrade of an assessor on a node fails, the node is marked in red on the Inventory page. Failures may be due to network issues. If that is the case, Comply attempts to upgrade the node once connectivity returns. An hourly background task runs to check if nodes have been upgraded or not. If a node does not upgrade and remains red on the Inventory page, run the Puppet agent. If the upgrade continues to fail, see the Puppet agent logs for more information.

---

**Upgrade from Comply 2.2.2 to 2.3.0**

Comply 2.3.0 automatically upgrades the CIS-CAT assessor to the latest version every time you upgrade Comply.

**Before you begin**

Make sure you have generated certificates in Puppet Enterprise (PE) and set up Mutual Transport Layer Security (MTLS) in Puppet Application Manager (PAM). MTLS enables a secure authenticated connection between your nodes and Comply. For more information, see Configure Comply TLS certificates on page 75.
1. If you want Comply to update the CIS-CAT Assessor automatically, select **Automatically kick off PE jobs on assessor upgrade** on the **Config** page in Puppet Application Manager.

   If you select this option, on upgrade Comply kicks off 2 PE agent runs: the first to download the new assessor, and the second update the facts in PE.

   **Tip:** Because this option starts PE jobs automatically on upgrading Comply, systems administrators, especially of larger implementation, may wish to consider leaving this option unchecked. Assessor upgrade then takes place automatically when the next two PE jobs are run.

   Comply requires the latest version of the assessor on the node in order to perform runs. A background task runs to check if nodes have been upgraded every 15 minutes if this option is selected and every hour if it is not selected. If a node does not upgrade and remains red on the **Inventory** page, run the Puppet agent. If the upgrade continues to fail, see the Puppet agent logs for more information.

2. Click **Save Config**.

3. If you have not already configured the **comply** class **scanner_source** parameter, you can do so at this point. Otherwise proceed to the next step. Navigate to Puppet Enterprise (PE), and update the default value of the **comply** class **scanner_source** parameter to one of the following assessor distribution files:

   - If using the Puppet supported cluster: `https://<COMPLY-HOSTNAME>:30303/assessor`
   - If using NGINX Ingress `scanner_source`: `https://<PE-TLS-FQDN>/assessor`

   For more information, see **Classify the nodes you want to scan in PE**.

   Click **Add to node group**, and then commit the changes.

4. Upgrade the **comply** module.

   a) Update your Puppetfile with the latest version of the **comply** module and its dependencies.
   b) Deploy code by running the `puppet-code deploy --all` command.

   **Warning:** When upgrading the **comply** module, running the agent before Comply is updated may cause an error.

5. Navigate back to Puppet Application Manager. After pre-flight checks have completed successfully, click **Go to updated version**, and then click **Deploy**.

   **Note:** If the upgrade of an assessor on a node fails, the node is marked in red on the **Inventory** page. Failures may be due to network issues. If that is the case, Comply attempts to upgrade the node once connectivity returns. An hourly background task runs to check if nodes have been upgraded or not. If a node does not upgrade and remains red on the **Inventory** page, run the Puppet agent. If the upgrade continues to fail, see the Puppet agent logs for more information.

---

**Upgrade Comply in an online environment**

Check for download and deploy updates from the **Version history** tab in the Puppet Application Manager UI.

**Before you begin**

Upgrade the **comply** module.

1. In the Puppet Application Manager UI, click **Version history**.

2. Click **Check for updates**.

   Configure an automatic update check by clicking **Configure automatic updates**. You can check for updates hourly, every four hours, daily, weekly, or at a custom interval.

3. If an update is available, Puppet Application Manager downloads it for you and performs preflight checks on your system to make sure your cluster meets system requirements for the new version. Review the outcome of these checks by clicking **View preflight**.
4. When you're ready to upgrade to the new version of Comply, click Deploy.

**Upgrade Comply in an offline environment**

If your environments do not have direct access to the internet, use the links below to upgrade to the latest version of Comply.

**Before you begin**
Upgrade the comply module.

1. Navigate to the portal provided to you by Puppet in the licence email, for example, https://get.replicated.com/airgap/#/kots/comply/, and login with the password.
2. Select Embedded cluster and download the latest Comply release .airgap file.
4. Select Version history, and upload the new version of the .airgap file that you downloaded in step 2.
5. Click Deploy.

**Desired compliance**

Set your desired compliance. This is the benchmark and profile that you assign to a particular node and which is scanned on that node by default. Generally, you only need to set this once for your nodes.

By default, Comply automatically assigns an appropriate benchmark for each operating system, along with a Level 1 profile, to nodes that have not been set based on fact information from PE. Accepting this option is the quickest way to get up and running with desired compliance.

The ## sign in the Profile assigned column on the Inventory page tells you that the desired compliance is set. You can view the node's information, including its assigned benchmark and profile, by clicking on the row assigned to the node. If you want to change a node's desired compliance, see the instructions for manually setting desired compliance.

Alternatively, if you want to choose a specific benchmark and profile for your nodes, or even a custom profile, option two provides this flexibility.

**Note:** Only one benchmark and profile can be assigned to each node.

**Manually set desired compliance**

If you don't want to use the benchmark and profile the Comply assigns automatically to your node, you can set the benchmark and profile you prefer from the Inventory.

1. In Comply, click the Node column header on the Inventory page.
   Comply lists the nodes that have been classified with the comply class. If you do not see any nodes, ensure you have classified your nodes correctly.
2. Click the node for which you want to specify desired compliance.
   In the window that appears on the right, you can see facts about the node and whether desired compliance has been set.
3. Choose the CIS benchmark and profile that you want to assign to the node.
   The benchmark and profile you set here is the desired compliance option for future scans.
   If you have created a custom profile, you can set it as the desired compliance by clicking **Use an associated custom profile**.
4. Click Update.

The ## sign in the Profile assigned column tells you that the desired compliance is set. You can view the node's information, including its assigned benchmark and profile, by clicking on the node. If you want to change a node's desired compliance, use the drop-down menu and click Update.

Now that you have applied desired compliance, you can use this option to run scans.

Related information
Create a custom profile on page 87
Create a custom profile based on an existing benchmark.

Run an ad hoc scan on page 88
Run your desired compliance scan or an ad hoc scan on your nodes.

Custom profiles

A custom profile is a benchmark profile that you customize to fit your organization's internally defined standards.

You can base a custom profile on an existing benchmark and profile combination, and then specify which rules you want visible in scan reports.

Create a custom profile

Create a custom profile based on an existing benchmark.

1. Navigate to Custom profiles.
2. Click Create custom profile.
3. Select a Benchmark and Profile.
4. Deselect rules in the profile that you do not want to scan, and click Next.
5. Enter the name of the profile and, optionally, a description.
6. Click Save custom profile.

Your custom profile appears as an option when you assign the associated benchmark to a node.

Navigate to Nodes to set your custom profile as the desired compliance for your nodes, or perform an ad hoc scan by selecting your custom profile on the Scans page.

Related information
Manually set desired compliance on page 86
If you don't want to use the benchmark and profile the Comply assigns automatically to your node, you can set the benchmark and profile you prefer from the Inventory.

Run an ad hoc scan on page 88
Run your desired compliance scan or an ad hoc scan on your nodes.

CIS scans

Run your desired compliance scan or an ad hoc scan on your nodes.

Ad hoc, or manual, scans give you the freedom to run a CIS scan on your network straight away. Alternatively, you can schedule scans to run on a regular basis and at times when network traffic is low.

Scan reports provide you with in depth information on not just the timing of scans but the nodes affected and the rules that passed or failed.
Run an ad hoc scan

Run your desired compliance scan or an ad hoc scan on your nodes.

You can run scans on individual nodes by selecting the **Scan node** drop-down on the node's **Node detail** page, and then selecting **desired compliance** or **custom** options if you have those set up. Then follow the scan wizard as outlined in steps 4-7 on this help page.

You can also scan all nodes by selecting the **Scan all nodes** drop-down on the **Dashboard** page, and then selecting **desired compliance** or **custom** options if you have those set up. Then follow the scan wizard as outlined in steps 4-7 on this help page.

1. In Comply, click **Scans**, and then **Run an ad hoc scan**.
2. In the **Benchmark** drop-down, select **Desired compliance** or a benchmark and profile of your choice.
   
   If you have not set desired compliance, see **Setting desired compliance** for instructions.
3. Next, select an option from the **Profile** drop-down. If you want to use a custom profile for this scan, select the **Use an associated custom profile?** option and choose the relevant option from the **Custom profile** drop-down.
   
   If you have not set desired compliance, see **Setting desired compliance** for instructions.
4. Click **Next** to review the PE credentials and environment you want the scan to run on.
5. Click **Next** to see the nodes selected for scanning.
   
   To only scan a subset of nodes, deselect any that you do not want to include.

   **Debug mode:** By default, assessor logs are set to WARN level. If you need to troubleshoot an issue you can set the logging level to DEBUG for the scan by clicking **Run in debug mode**. The assessor logs can then be retrieved from the individual node.

   On Linux and macOS platforms the assessor log is located at:

   `/opt/puppetlabs/comply/Assessor-CLI/logs/assessor-cli.log`

   On Windows the assessor log is located at:

   `C:/ProgramData/PuppetLabs/comply/Assessor-CLI/logs/assessor-cli.log`

   Note that scanning in debug mode increases the size of the assessor log file significantly.

6. Click **Scan**.

   You are taken to the **Activity Feed**, which lists each scan. Scans are run as a task in PE. To see the details of the job, click the job ID to be taken to PE.

   **Tip:** You can also run a scan by clicking the **Scan nodes** button at the top right corner on several pages. This option uses the nodes listed on the page you are currently viewing.

7. In Comply, navigate to the **Dashboard** page to see the results of your scan.

   See **Viewing scan results** for a description of the scan data.

**Related information**

**Enforce CIS benchmarks** on page 93

© 2021 Puppet, Inc.
Puppet Comply provides visibility into your compliance status, but it cannot fix your failing nodes. Instead, you can use Puppet’s Compliance Enforcement Modules (CEM).

**Custom profiles** on page 87
A custom profile is a benchmark profile that you customize to fit your organization's internally defined standards.

**Desired compliance** on page 86
Set your desired compliance. This is the benchmark and profile that you assign to a particular node and which is scanned on that node by default. Generally, you only need to set this once for your nodes.

## Scheduled scans

In addition to manual ad hoc scans, you can also schedule scans.

From the **Scheduled scans** tab on the **Scans** page you can:

- View existing scheduled scans
- Create and edit new scans
- Pause, end or manually start a scheduled scan via the **Actions** drop-down menu.

Comply gives you lots of options with regard to the scheduling of your scans. You can schedule a one-off scan of a scan that repeats periodically:

- You can set scans to happen on individual days of the week, every day, week days only, or weekends only.
- You can set scans to run on any day of the month. Beware though that if you, for example, set a scan to run on Day 31, the scan does not run in months that do not have 31 days.

### Scheduled scans table

The **Scheduled scans table** on the **Scheduled scans** tab provides the following information:

- **Name** - The name assigned to the scan.
- **Nodes** - The number of nodes to be scanned.
- **Start** - The time scheduled for the scan to start according to the selected timezone.
- **End** - The time scheduled for the scan to finish according to the selected timezone.
- **Frequency** - How often the scan is scheduled to run.
- **Last run** - How long ago the last scan of this type started.
- **Status** - Whether the scan is not currently running (**Not started**), has completed (**Ended**), or is currently running (**Active**).

### Create a one-off scheduled scan

Follow a simple workflow to schedule a scan to run once.

To create a one-off scheduled scan:

1. On the **Scans** page, click **Create a scheduled scan**.
2. Select an **Environment**, and click **Next**.
3. Select the nodes you want to scan by clicking the relevant check boxes, and click **Next**.

**Note:** If desired compliance has not been set on any of the nodes you are prompted to select a suggested desired compliance profile from the existing options or exclude those nodes from the scan.

4. Set the schedule:
   a) Select **Once only**.
   b) Add the **Date** you want the scan to run.
   c) Choose a **Time** and indicate your **timezone**.
   d) Click **Next**.

© 2021 Puppet, Inc.
5. Finally, enter the **Scheduled scan name** and an optional **Description**, and click **Save scheduled scan**. The schedule scan information is listed on the **Scheduled scans** tab on the **Scans** page.

### Create a repeating scheduled scan

Follow a simple workflow to schedule a scan to run regularly.

To create a scheduled scan that repeats:

1. On the **Scans** page, click **Create a scheduled scan**.
2. Select an **Environment**, and click **Next**.
3. Select the nodes you want to scan by clicking the relevant check boxes, and click **Next**.

| Note: | If desired compliance has not been set on any of the nodes you are prompted to select a suggested desired compliance profile from the existing options or exclude those nodes from the scan. |

4. Set the schedule:
   a) Select **Repeating**.
   b) Select the desired **Frequency** of the scan:
      - If you choose to run the scan on a **weekly** basis, you have the option to select the day of the week the scan, or you can run it daily, or on weekdays, or weekends only.
      - If you choose to run the scan on a **monthly** basis, select the day of the month you want the scan to run.

| Remember: | Your scan does not run if the month does not include the day you selected. For example, if you choose day 31, your scan cannot run in those months that do not have 31 days. |

c) Choose the **Time** and **Timezone** when you want the scan to run.
d) Optionally, add an **End Date** for the scan schedule.
   If you choose an end date for your scheduled scan, no more scans run on or after that date and no scan reports are produced.
e) Click **Next**.

5. Finally, enter the **Scheduled scan name** and an optional **Description**, and click **Save scheduled scan**. The schedule scan information is listed on the **Scheduled scans** tab on the **Scans** page.

### Update a scheduled scan

Once created, scheduled scan details can be easily edited.

To edit a scheduled scan:

1. on the **Scheduled scans** tab on the **Scans** page, click the row assigned to the scheduled scan you want to change.
2. on the side panel that appears, click **Edit**.
3. The **Review** page that appears allows you to update the **Scheduled scan name** and **Description**. Click **edit/review nodes** to select different nodes to be scanned, and **edit/review schedule** to change the timing of your scheduled scan.
4. Click **Save and exit** when you are done.

### CIS scan reports

The **Scan lists** page displays all scans run within the defined scan data retention period.

The **Scan reports** tab on **Scans** page provides the following information:

- **Name** - the name given to the scan when it was run.
- **Scan type** - currently the only option here is for **ad hoc** scans.
- **Nodes scanned** - the total number of nodes included in the scan.
- **Compliance** - the percentage of nodes that passed compliance in the scan.

© 2021 Puppet, Inc.
• **Time started** - the date and time stamp when the scan was initiated.

Click the row assigned to any scan to go to its **Scan report details** page.

For more information on defining the scan data retention period, see **Scan data retention policy** on page 93.

**Related information**

**CIS scan report details** on page 91

The **Scan report details** page provides info on a selected CIS scan.

**Scan results** on page 91

View the results of your CIS scans and find out whether your nodes are compliant.

**CIS scan report details**

The **Scan report details** page provides info on a selected CIS scan.

The **Scan report metrics bar** at the top of the **Scan Report** page is divided into two sections: **Compliance scan status** and **Puppet Enterprise job status** areas.

The **Compliance scan status** area provides a brief overview of the number of nodes that have passed and failed compliance, as well the error percentage, the rules that couldn't be evaluated across nodes, and the scan initiation date and time.

The **Puppet Enterprise job status** area in the **Scan report metrics bar** shows the number of nodes that ran the CIS scanner job successfully, the number that failed to run the scanner job and the number of nodes that showed an error for the scanner job.

Click **Run an ad hoc scan** to kick off a new scan of your network.

More detailed information on the success and failure of rules is given on the **Nodes** tab. The **Rules** tab provides detail on the performance of individual rules in the scan.

**Rules tab**

The **Rules** table on the **Rules** tab lists all the rules that were assessed as part of the latest scan. The **Rules** table provides information on the rule profile, and the number of nodes on which the rule failed. Click the rule name on any given row to visit the **Rule detail** page for the selected node.

**Nodes tab**

The **Nodes** table on the **Nodes** tab lists all the nodes that were part of the latest scan. The **Nodes** table provides information on the node profile, and the percentage of rules in compliance on each node. Click the node name in any given row to visit the **Node detail** page for the selected node.

**Scan results**

View the results of your CIS scans and find out whether your nodes are compliant.

**Scan report metrics bar**

The **Scan report metrics bar** provides a brief overview of the number of nodes that have passed and failed, as well the error percentage, the rules that couldn't be evaluated across nodes, and the scan initiation date and time.

**Compliance dashboard**

The **Compliance dashboard** provides a breakdown of your latest CIS scan.

It has three components:
• The **Node results** chart shows the percentage of rules that passed and failed across all of your nodes. These percentages are shown with the statuses of **Pass**, **Fail**, **Error**, and **Unknown**.

• The **Desired compliance** chart shows the number of nodes that have desired compliance set. Desired compliance is the default benchmark and profile that you have assigned to that node.

• The **Node results table** lists information about the latest scan for each node.

**Node compliance**

From the **Compliance dashboard**, click a node name to get to the **Node compliance** page, and see the results of the latest scan on that node. The data includes:

• The **Rules checked** chart shows a status breakdown for the latest scan on that node — the rules that passed, failed, had an error, or an unknown status. The percentage displayed in the **Rules checked** pie chart is an aggregate of these four statuses.

Other statuses that are not included in scoring are included in the table below:

<table>
<thead>
<tr>
<th>Value</th>
<th>Included in Scoring?</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>Yes</td>
<td>The target system or component state satisfied all the conditions of the check(s)/rule(s) for the recommendation.</td>
</tr>
<tr>
<td>Fail</td>
<td>Yes</td>
<td>The target system or component state did not satisfy at least one condition of the check(s)/rule(s) for the recommendation.</td>
</tr>
<tr>
<td>Error</td>
<td>Yes</td>
<td>The assessor checking engine encountered a system error and could not complete the test. The status of the target's compliance is not certain.</td>
</tr>
<tr>
<td>Unknown</td>
<td>Yes</td>
<td>Assessor was unable to collect, interpret, or evaluate against the check/rule conditions associated with the recommendation.</td>
</tr>
<tr>
<td>Manual</td>
<td>No</td>
<td>This recommendation cannot be fully automated and requires manual evaluation. On CIS Benchmarks, a recommendation is deemed important during the consensus process but cannot be fully and reliably verified without organizational manual verification. Corresponds to xccdf terminology of &quot;Informational&quot;.</td>
</tr>
<tr>
<td>Not Applicable</td>
<td>No</td>
<td>The rule(s)/check(s) were not applicable to the target. This typically occurs when the wrong benchmark is selected for the platform i.e.: platform mismatch.</td>
</tr>
<tr>
<td>Not Checked</td>
<td>No</td>
<td>The recommendation was not evaluated as there are no rule/check properties.</td>
</tr>
<tr>
<td>Not Selected</td>
<td>No</td>
<td>This recommendation was not part of the profile selected for the configuration assessment.</td>
</tr>
<tr>
<td>Informational</td>
<td>No</td>
<td>This is the same result that is displayed as Manual on the HTML report. The recommendation cannot be fully automated and requires manual evaluation.</td>
</tr>
</tbody>
</table>

• The **Rule scan results** table lists each rule that was checked and the status of that rule from the latest scan.

**Rule results**

From **Node compliance**, click a rule title on the **Rule results** page, and see the details of that rule and the status of the nodes it is checked on. The data includes:
Enforce CIS benchmarks

Puppet Comply provides visibility into your compliance status, but it cannot fix your failing nodes. Instead, you can use Puppet’s Compliance Enforcement Modules (CEM).

Available to premium content subscribers, CEM consists of two modules — cem_linux and cem_windows. These are supported Puppet modules developed specifically to bring your Puppet Enterprise (PE) managed nodes under CIS (Center for Internet Security) compliance.

By default, CEM enforces the latest CIS Level 1 benchmarks on your nodes, automating hundreds of operating system settings — the default profile depends on your operating system. You can also customize these configurations to suit your organization’s policies.

To get started with CEM, you need to add the Forge premium content API key to your primary Puppet server. For instructions, visit cem_linux or cem_windows on Puppet Forge.

Troubleshooting

Use this section to troubleshoot issues with your Puppet Comply installation.

Reset your Comply password

If you forget your password, you can reset it in the user admin console.

1. SSH into your Comply node and run the following commands to retrieve the admin username and password:

   kubectl exec $(kubectl get pod -l app.kubernetes.io/name=comply-auth -o jsonpath="{.items[0].metadata.name}") -- /bin/bash -c 'cat /etc/keycloak/admin-user'

   kubectl exec $(kubectl get pod -l app.kubernetes.io/name=comply-auth -o jsonpath="{.items[0].metadata.name}") -- /bin/bash -c 'cat /etc/keycloak/admin-password'

2. Navigate to https://<COMPLY-HOSTNAME>/auth/admin using the FQDN of your Comply node.
3. Login using the credentials from step 1.
4. Navigate to Users.
5. Click View all users and select the user account you want to update, and click Edit.
6. Select the Credentials tab and the reset password.

## Access logs

If you run into issues with Puppet Comply, you can download the relevant log files. The Comply logs are stored in Puppet Application Manager.

2. Select the Troubleshoot tab, and click Analyse Comply.
3. Download the bundle of log files.

## Resolve Comply domain

If the Puppet Comply gatekeeper is unable to resolve the Comply domain, try the following troubleshooting steps.

When you assign a hostname to Comply, it needs to be resolved by the pods in your Kubernetes cluster. A preflight check verifies the domain you specified in the configuration is resolvable. You must ensure that the nodes can resolve their own hostnames, through either local host mapping or a reachable DNS server.

1. To verify your whether your hostname is resolvable, run the following commands:

   ```bash
   kubectl exec $(kubectl get pod -l app=kotsadm -o jsonpath="{.items[0].metadata.name}") -- /bin/sh -c 'curl --S $<hostname>
   
   If the hostname was resolved, the command returns an exit code 0 with no output.
   If the hostname cannot be resolved, the command returns an exit code 6. Proceed to step 2 to add DNS entries.
   2. To add DNS entries for CoreDNS, run the following command to open the CoreDNS configuration maps:

   ```bash
   kubectl -n kube-system edit configmaps coredns
   
   3. Add a hosts entry below kubernetes. This is where you configure the DNS entry for Comply. For example:

   ```bash
   kubernetes cluster.local in-addr.arpa ip6.arpa {
     pods insecure
     fallthrough in-addr.arpa ip6.arpa
     ttl 30
   }
   hosts {
     10.23.24.25 comply.mycompany.net comply // IP_address canonical_hostname
     [aliases...]
     fallthrough
   }
   prometheus :9153
   
   4. Run the command from step 1 to verify whether the DNS entry was updated:

   ```bash
   kubectl exec $(kubectl get pod -l app=kotsadm -o jsonpath="{.items[0].metadata.name}") -- /bin/sh -c 'curl --S $<hostname>
   
   5. Re-run the preflight checks.
Resolve failed assessor upgrade

If an upgrade of the assessor has failed on one of your nodes, try the following troubleshooting step.

If the upgrade of an assessor on a node fails, the node is marked in red on the Inventory page. Failures may be due to network issues. If that is the case, Comply attempts to upgrade the node once connectivity returns. An hourly background task runs to check if nodes have been upgraded or not. If a node does not upgrade and remains red on the Inventory page, run the Puppet agent. If the upgrade continues to fail, see the Puppet agent logs for more information.

Troubleshooting TLS issues in Comply

Incorrect configuration of TLS certificates when setting up Comply to work with PE can cause agents and/or scan tasks to fail.

There are two main certificate configuration errors that cause problems:

- If the CA certificate configured for Comply in Puppet Application Manager does not match the CA certificate the Puppet Enterprise certificate is signed with, then a trust store issue is returned upon setting up PE or trying to run a scan.
- A hostname issue can arise if a server identity check does not pass. The dnsName in the subjectAltName of the server certificate must match the hostname Comply is communicating with. The hostname configured in the Comply settings page for Puppet Enterprise must match one of the dnsName entries in the PE certificate.

Troubleshooting agent issues

Agents can fail if the certificate is configured incorrectly in two ways:

- The hostname could be the issue - the Comply TLS certificate must have the dnsName which the agent is trying to contact the Comply server with. This is only relevant if you have setup the Comply module to download the assessor from the Comply server. The hostname the Comply server is contacted with is the hostname in the configured scanner_source parameter URL.
- The trust store may also be the problem if the Comply server TLS certificate and the client certificate are not signed by the same CA.

Troubleshooting scan task issues

Scan tasks can also fail if the certificate is configured incorrectly in two ways:

- If the hostname is incorrectly configured - The Comply TLS certificate must have the dnsName which the agent is trying to contact the Comply server with. The hostname used is passed through by the task and can be seen in the PE UI by checking the task parameters. Verify the task parameters to ensure that the hostname is correct.
- If the Comply server TLS certificate and the client certificate are not signed by the same CA a trust store issue occurs and this too can cause the scan task to fail.

Troubleshoot TLS from a node

You can run a simple cURL command to troubleshoot TLS issues from a node.

To troubleshoot TLS from a node:

1. SSH into node and change into SSL subdirectory:

   ```bash
   cd /etc/puppetlabs/puppet/ssl/
   ```
2. Issue the following cURL command replacing values in angle brackets with values relevant to your installation:

```
curl -G --key private_keys/<local host key> --cacert certs/ca.pem --cert ../certs/<local host cert> https://<comply-fqdn>:30303/assessor --output /tmp/assessor.zip
```

**Note:** If you are using your own ingress, issue the following command:

```
curl -G --key private_keys/<local host key> --cacert certs/ca.pem --cert ../certs/<local host cert> https://<PE TLS hostname>/assessor --output /tmp/assessor.zip
```

If this command fails, there is an issue with certificates. The error message can help to identify if there is a CA, client certificate or hostname issue.

- If there is a hostname error, the output resembles the following error message:

```
curl: (60) SSL: no alternative certificate subject name matches target host name '<comply-fqdn>'
```

- If it is a CA issue, the output is likely to be similar to the example below:

```
curl: (60) SSL certificate problem: unable to get local issuer certificate
```

**Important:** This may be because the CA of the https://<comply-fqdn>:30303/assessor (or https://<PE TLS hostname>/assessor) does not match the CA passed to the cURL command or because there is a mismatch with the CA of the client certificate.