

Compliance Scanner for VMware Tanzu v1.0

Compliance Scanner for VMware Tanzu 1.0

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2023 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

Compliance Scanner for PCF	6
Overview	6
Key Features	6
Product Snapshot	7
Ports	7
Limitations	7
Feedback	8
Release Notes for Compliance Scanner for PCF	9
v1.0.0 - General Availability (GA)	9
Features	9
Known Issues	9
v1.0.0-beta.63	10
Features	10
Resolved Issue	10
v1.0.0-beta.25	10
Features	10
Resolved Issues	10
Known Issues	10
v1.0.0-beta.7	11
Features	11
Known Issues	11
Installing and Configuring Compliance Scanner for PCF	12
Prerequisite	12
Install Compliance Scanner	12
Configure Scans	12
Configure Errands	16
Configure Syslog Forwarding	17
Configure Resources	18
Apply Changes from Your Configuration	19
Using Compliance Scanner for PCF	20
Ways to Scan VMs	20
Scan Using the Compliance Scanner Tile	20

Scan the VMs	20
Retrieve Log Files	21
Find Scan Output	22
Scan Using the Command Line	23
Scan and Retrieve Log Files	23
Retrieve Existing Log Files	25
Access Log Files	25
View Tests on VMs	26
 Upgrading Compliance Scanner for PCF	 27
Overview	27
Procedure	27
 Troubleshooting Compliance Scanner for PCF	 28
scan_results Issues	28
scan_results Completed with Error (Exit Code 1)	28
Symptom	28
Explanation	28
Solution	28
scan_results Received Signal Terminated (Exit Code 124)	29
Symptom	29
Explanation	29
Solution	29
scan_results Does Not Include Scans for VMs in the Deployment	29
Symptom	29
Explanation	29
Solution	29
Unable to resolve store domain: no such host	29
Symptom	30
Explanation	30
Solution	30
oscap_store receives ReportFailed (Exit code 1)	30
Symptom	31
Explanation	31
Solution	31
Scan Successful with POST Errors	31
Symptom	31
Explanation	32
Solution	32

Benchmarks for Compliance Scanner for PCF	34
Overview	34
Base Xenial	34
Recommended Security Baseline	34
Strict Security Practices	35
STIG for Ubuntu Xenial	35

Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

Compliance Scanner for PCF provides platform operators and auditors an assessment of each PCF Linux VM running on Xenial stemcells and, if it is compliant, with configuration guidelines.

The following VM types on an Pivotal Operations Manager instance are skipped for scanning and do not have Compliance Scanner deployed on them:

- Linux VMs running on Trusty stemcells
- Non-Linux VMs

Overview

Benchmarks for existing commercial configuration scanners are intended for use against traditional Ubuntu servers. This means that running these benchmark scans against a stemcell results in numerous false positives.

Compliance Scanner addresses this issue by tuning industry-recognized Ubuntu configuration benchmarks for stemcells.

Compliance Scanner packages the following files for deployment on each BOSH-managed Linux VM:

- The OpenSCAP (OSCAP) scanner
- XFiles: A group of YAML files that contains configuration tests written in YAML.
- The XCCDF Generator (XGen): This translates XFiles tests to the SCAP format.

Compliance Scanner is installed through Ops Manager. As part of the installation, it deploys each packaged component to each PCF Linux VM and instantiates a new Linux VM, `oscap_store`, for log retrieval.

Scans are errands that are triggered through Ops Manager. After a successful scan, operators can retrieve reports through the tile. Operators can download these reports to their local machine.

For more information about the tests, test coverage, and test criteria covered by these benchmarks, see the PDF files included on the [Compliance Scanner](#) release page on Pivotal Network.

Key Features

Compliance Scanner includes the following key features:

- Modified version of industry-recognized configuration benchmarks tuned for stemcells
- Bundled tests written in YAML, allowing for easier readability
- Reports of scan results for each Linux VM in the PCF deployment that highlight the compliance posture

Product Snapshot

The following table provides version and version-support information about Compliance Scanner.

Element	Details
Tile version	1.0.0
Release date	July 31, 2019
Software component version	OpenSCAP 1.3.0
Compatible Ops Manager version(s)	2.3, 2.4, 2.5, 2.6, and 2.7
Compatible Pivotal Application Service version(s)	2.3, 2.4, 2.5, 2.6, and 2.7
IaaS support	AWS, Azure, GCP, and vSphere
IPsec support	Yes

Ports

Compliance Scanner uses the following ports:

VM Type	Description	Port
oscap_store	The port used by <code>oscap_store</code> to receive the scan results from VMs with Compliance Scanner. The <code>oscap_store</code> VM initiates scan requests to other VMs and aggregates the results.	28894
VM with Compliance Scanner	The port used by the scanning server running on each of the VMs with Compliance Scanner installed.	28893

Limitations

Compliance Scanner has the following limitations:

- Because of stemcell-related customization, benchmarks are not certified by a governing body.
- Windows VMs are not supported at this time.
- BOSH DNS cannot resolve the `oscap_store` VM URL if there is any capitalization in the network name.



Note: Compliance Scanner can only scan Linux VMs running on Xenial stemcells 97.x and 170.x and later.

Feedback

Please provide any bugs, feature requests, or questions to the [Pivotal Cloud Foundry Feedback list](#).

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Release Notes for Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

These are release notes for Compliance Scanner for PCF.

For product versions and upgrade paths, see [Upgrade Planner](#).

v1.0.0 - General Availability (GA)

Release Date: July 31, 2019

This is the General Availability release of Compliance Scanner.

Features

New features and changes in this release:

- Changes the default port for the `oscap_store` VM to avoid port range collision and installation issues.
- Increases the default value for **Scanner Timeout** to `1200`.
- Changes the default machine type for the `oscap_store` VM to use 2 CPUs and 2 GB of memory.
- Provides additional information in scan results, for an improved experience when using the STIG Viewer tool published by DISA:
 - ✦ Includes the benchmark used in the test results for checklist creation in the viewer.
 - ✦ Adds the severity level field to Xenial benchmark test results.
 - ✦ Adds the group field to test results.
 - ✦ Adds test categories in the `Recommended Security Baseline` and `Strict Security Practices` benchmark test results.

Known Issues

This release has the following known issue:

- BOSH DNS cannot resolve the `oscap_store` VM URL if there is any capitalization in the network name.

v1.0.0-beta.63

Release Date: July 8, 2019

Features

New features and changes in this release:

- Compliance Scanner now uses a client-server architecture for initiating and generating scan results. This new architecture results in the following changes:
 - ✦ Secures the communication between the store VM and all of the scanner VMs through the implementation of mutual TLS (mTLS).
 - ✦ Removes credentials needed to trigger scans from the `oscap_store` VM.
 - ✦ Now uses Ops Manager Root CA certificate to sign the mTLS certificates.
- Adds a configurable **Scanner Timeout** field to limit how long a scan takes. For how to configure this field, see [Configure Scans](#).

Resolved Issue

This release fixes the following issue:

- Compliance Scanner is now compatible with foundations using federated Single Sign-On (SSO) and authorization.

v1.0.0-beta.25

Release Date: April 3, 2019

Features

New features and changes in this release:

- Updates OpenSCAP to v1.3.0.
- Adds `index.html` to provide HTML results.
- Removes dependencies requiring the Pivotal Application Service (PAS) tile. This enables scans on Enterprise Pivotal Container Service (Enterprise PKS)-only environments.

Resolved Issues

This release fixes the following issue:

- Fixes an issue when scanning environments without other tiles.

Known Issues

This release has the following known issue:

- No support for federated SSO and authorization.

v1.0.0-beta.7

Release Date: December 21, 2018

This is the first release of Compliance Scanner.

Features

New features and changes in this release:

- Features the ability to scan all BOSH-managed VMs to verify secure platform configuration
- Contains four bundled benchmarks with tests developed for cloud-native OS stemcells
- Allows high-level scan reports for each VM in LOG, XML, and HTML formats

Known Issues

This release has the following known issues:

- If Compliance Scanner for PCF is scanning a deployment and that deployment is destroyed before the scanning errand is finished, then Apply Changes errors out with the message:
`Cannot iterate over null (null).`
- Some Base Xenial benchmark tests fail. The following table lists the tests that fail and which components they fail on:

Components	ID of Failed Test
<ul style="list-style-type: none">• Diego VM	<ul style="list-style-type: none">• SV-90191r1• SV-90193r3• SV-90235r1• SV-90237r1• SV-90263r2• SV-90277r3• SV-90491r4
<ul style="list-style-type: none">• Clock Global• Cloud Controller• Cloud Controller Worker	<ul style="list-style-type: none">• SV-90191r1• SV-90491r4
<ul style="list-style-type: none">• All components	<ul style="list-style-type: none">• SV-90277r3

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Installing and Configuring Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to install and configure Compliance Scanner for PCF.

Prerequisite

Compliance Scanner runs a scanner daemon on each VM that requires ~100 MB of memory. Before you install Compliance Scanner, you might need to resize your VMs accordingly.

Install Compliance Scanner

To install the Compliance Scanner file on the Pivotal Operations Manager Installation Dashboard:

1. Download the product file from [Pivotal Network](#).
2. Navigate to the Ops Manager Installation Dashboard and click **Import a Product** to upload the product file.
3. Underneath **Import a Product**, click **+** next to the version number of Compliance Scanner. This adds the tile to your staging area.
4. Click the newly added **Compliance Scanner** tile.

Configure Scans

This section is where you configure expected values for tests and select which set of benchmarks to run. To configure your scans:

1. Click **Settings**.

2. Click **Assign AZs and Networks**.
3. Configure the fields as follows:

Field	Description
Place singleton jobs in	Select the AZ that you want the <code>oscap_store</code> VM to run in. The tile runs as a singleton job.
Balance other jobs in	Select the same AZ as above.
Network	Select a subnet for the <code>oscap_store</code> VM. This is typically the same subnet that includes the Pivotal Application Services (PAS) component VMs.

4. Click **Save**.
5. Click **System Variables**.

System Variables

NTP Server IP *

Syslog Host IP *

Syslog Port *

Save

6. Configure the fields in **System Variables** to provide the expected values for the tests:

Field	Description
NTP Server IP	The IP address of your NTP server. You can find this IP address in Bosh Director > Director Config > NTP Server . You can only enter one server IP address. It does not matter which NTP server you enter.
Syslog Host IP	The IP address of your syslog host. You can find this in your PAS tile under Settings > System Logging > Address .
Syslog Port	The port number of the syslog port. You can find this in your PAS tile under Settings > System Logging > Port .

7. Click **Save**.
8. Click **Scan Configuration**.

Scan Configuration

Scan Report Formats *

☒ .log

☒ .xml

☒ .html

Benchmarks *

☒ Base Xenial

☒ Recommended Security Baseline

☒ Strict Security Practices

☒ STIG

Scanner Timeout *

600

Save

9. Enable **Scan Report Formats**. You must select at least one format. The outputs of a scan can be in LOG, XML, and HTML formats.
10. Enable **Benchmarks** for the scanner to run:

Benchmark	Description
Base Xenial	Includes a subset of the amended tests in the STIG benchmark, where failing tests due to architectural differences are removed. This is meant to be used as a measure to see if configurations have been altered.
Recommended Security Baseline	A benchmark with rules that all systems should implement, regardless of user environment or the sensitivity of the app data being processed.
Strict Security Practices	A benchmark with strict rules that are required of systems processing sensitive data or workloads. This is meant to run in addition to the tests in the recommended security baseline benchmark.
STIG for Ubuntu Xenial	Includes all the configuration tests of the published DISA STIG for Ubuntu 16.04, amended with stemcell specific changes. Contains tests that would fail due to architectural differences.

A scan report is generated for each format and benchmark on each Linux VM running on Xenial stemcells. For example, if you select **.xml** and **.log** formats, and **Base Xenial** and **STIG** benchmarks, four log files are created for each VM tested.

For more information about Compliance Scanner benchmarks, see [Benchmarks](#).

11. For **Scanner Timeout**, configure the maximum time in seconds permitted for a scan. The default value is **600**.
12. For **Open File Limit**, configure the maximum number of files that the scanner is permitted to open. If the scanner goes over this limit, the scan fails. The recommended value is at least $1024 + \text{twice the number of VMs}$.
13. Click **Save**.

Configure Errands

Compliance Scanner performs one errand that initiates scanning. This errand is disabled by default. This is so that a scan is not run every time changes are applied.

When this errand is triggered, it initiates the scanning errand on each VM. For more information about initiating the scanning errand, see [Using Compliance Scanner](#).

When configuring the Compliance Scanner tile for the first time, follow these steps:

1. Click **Errands**.

Errands

Errands are scripts that run at designated points during an installation.

Post-Deploy Errands

Run config scans on PAS

Default (Off)

There are no pre-delete errands for this product.

Save

2. Confirm that **Run configured scans** is set to **Default (Off)**.

3. Click **Save**.

Configure Syslog Forwarding

To configure syslog forwarding:

1. Select **Syslog**.

Syslog

Do you want to configure Syslog forwarding?

☐ No, do not forward Syslog

☒ Yes

Address*

Port*

Transport Protocol*

TCP

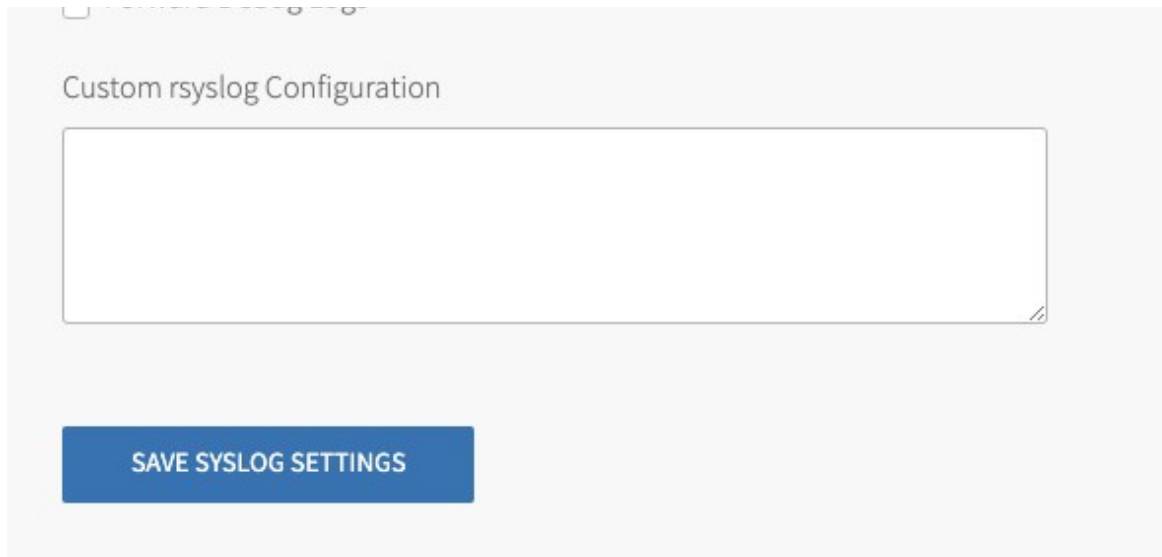
☐ Enable TLS

Permitted Peer*

SSL Certificate*

Queue Size

☐ Forward Debug Logs



Custom rsyslog Configuration

SAVE SYSLOG SETTINGS

2. Select **Yes** for **Do you want to configure Syslog forwarding?**.
3. Configure the fields as follows:

Field	Instructions
Address	Enter the address or host of the syslog server for sending logs, for example, <code>logmanager.example.com</code> .
Port	Enter the port of the syslog server for sending logs, for example, <code>29279</code> .
Transport Protocol	Select the transport protocol used to send system logs to the server. Pivotal recommends TCP.
Enable TLS	If you select TCP, you can also select to send logs encrypted over TLS.
Permitted Peer	Enter either the accepted fingerprint, in SHA1, or the name of the remote peer, for example, <code>*.example.com</code> .
SSL Certificate	Enter the SSL or TLS Certificate(s) for the syslog server. This ensures the logs are transported securely.
Queue Size	Enter an integer. This value specifies the number of log messages held in the buffer. The default value is <code>100000</code> .
Forward Debug Logs	Select this box to forward debug logs to external source. This option is deselected by default. If you select it, you might generate a large amount of log data.
Custom rsyslog Configuration	Enter configuration details for rsyslog. This field requires RainerScript syntax.

4. Click **Save Syslog Settings**.

Configure Resources

The tile creates a new VM called `oscap_store` to store the logs retrieved from all the other VMs that have been scanned.



Note: The `oscap_store` VM does not do anything computationally extensive. Pivotal recommends using the default configurations.

1. Click **Resource Config**.
2. Click **Save**.

Apply Changes from Your Configuration

Your installation is not complete until you apply your configuration changes:

1. Return to the Ops Manager Installation Dashboard.
2. Click **Review Pending Changes**. Verify all products are selected.
3. Click **Apply Changes** to complete the installation of Compliance Scanner.

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Using Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to use Compliance Scanner for PCF.

Compliance Scanner performs one errand that starts scanning. When this errand is triggered, it starts the scanning errand on each VM, including the `oscap_store` VM that the tile creates.

The scanning errand is set to `off` by default. This is because Compliance Scanner only scans tiles that are already present when you deploy it. If you install other tiles during the same time Compliance Scanner is installed, the additional tiles are not scanned.

The scan errand on each VM does generate the Security Content Automation Protocol (SCAP) tests each time by running XGen on XFiles.

Ways to Scan VMs

You can scan VMs using the tile UI or the command line:

- When performing an audit, see [Scan Using the Compliance Scanner Tile](#).
- When setting up automated scans of your VMs, see [Scan Using the Command Line](#).

Scan Using the Compliance Scanner Tile

Scanning VMs involves three procedures:

1. [Scan the VMs](#)
2. [Retrieve Log Files](#)
3. [Find Scan Output](#)

Scan the VMs

To begin scanning, do the following:

1. Confirm that your scan is configured correctly with the benchmarks and log formats you want output.

For more information on configuring your scan, see [Configure Scans](#).

2. Navigate to the Pivotal Operations Manager Installation Dashboard.
3. Click **REVIEW PENDING CHANGES**.
4. Enable the checkboxes for the Compliance Scanner tile and the **Run config scans on PAS** errand.

Review Pending Changes

☐ Select All Products

☒ **Compliance Scanner for PCF**
Version 1.0.0-beta.7

Depends on
Small Footprint PAS (cf) >= 2.3

ERRANDS

Select errands to run during the deploy

☒ Run config scans on PAS

APPLY CHANGES

A scan is triggered at the end.



Note: If there are configuration changes from add-ons or tiles other than Compliance Scanner, leave those products' and errands' checkboxes enabled if you want those changes to be applied. If there are no changes from other sources, only the Compliance Scanner tile needs to have its checkbox enabled.

5. Click **APPLY CHANGES**.

When scanning is finished, a second errand is triggered by the `Run-config-scans-on-PAS` errand to retrieve the logs from each VM. On each VM, there is only one log file per format and one ZIP log file at a time. If you run any subsequent scans these files are overwritten.

Retrieve Log Files

To review the logs for a completed scan using the Compliance Scanner tile, do the following:

1. When the changes have been applied, return to the Installation Dashboard and click the Compliance Scanner tile.

✓ Changes Applied

Your changes were successfully applied.
We recommend that you export a backup of this installation from the actions menu.

CLOSE **RETURN TO DASHBOARD**

2. Click the **Status** tab and download the `oscap_store` log file.

This downloads the log file containing scan results from the `oscap_store` VM to Ops

Manager. If you select the download icon multiple times, a list of ZIP files is created in Ops Manager, each with a different timestamp.

- Click the **Logs** tab and click on the filename of the ZIP log file.


This downloads the scan results from the Ops Manager to your local machine.



The timestamp indicates when the scan was initiated.

- Decompress the downloaded file.

The contents of the downloaded file depend on the formats and benchmarks you selected during configuration. For example, a report in HTML format from the Base Xenial benchmark, might look like this.



Compliance Scanner for PCF Evaluation Report

Guide to the Secure Configuration of Ubuntu stemcell

with profile **base-xenial**

Evaluation Characteristics

Tile version	1.0
Evaluation target	vm-identifier
Benchmark URL	base_xenial.xml
Benchmark ID	xccdf_org.pci.content_benchmark_ubuntu_stemcell
Profile ID	xccdf_org.pci.base-xenial_profile_genx
Started at	2018-12-17T14:47:45
Finished at	2018-12-17T14:48:01
Performed by	Compliance Scanner for PCF

CPE Platforms

- cpe:/o:canonical:ubuntu_linux:0.0

Addresses

- IPV4 127.0.0.1
- IPV4 169.254.0.2
- IPV4 10.0.4.10
- MAC 00:00:00:00:00:00
- MAC 42:01:0A:00:04:0A

[See a larger version of this image.](#)

Find Scan Output

The `oscap_store` ZIP file contains scan results from the `oscap_store` VM. The results of the scan are at the following path:

```
oscap_store/scanner/scan_results/output
```

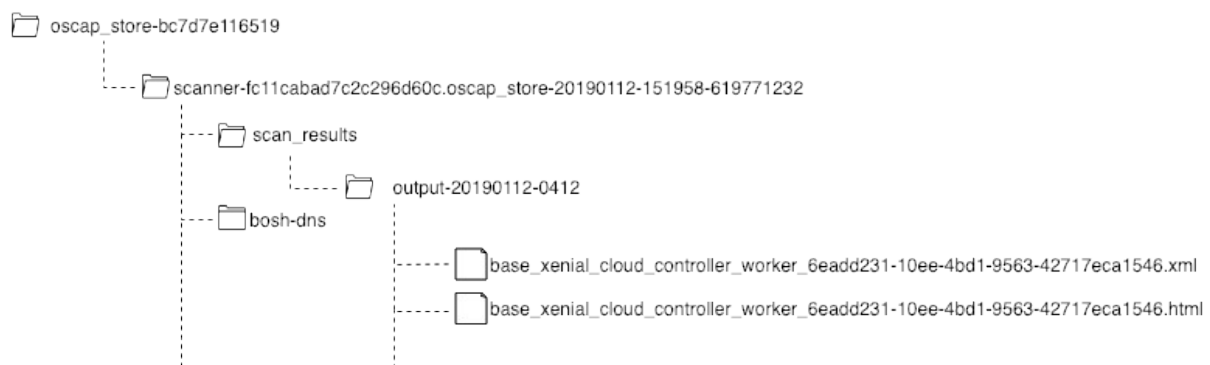
The naming syntax for each log file is the following:

```
BENCHMARK_COMPONENT_UUID.FORMAT
```

Where:

- **BENCHMARK** is the benchmark that was used for the scan.
- **COMPONENT** is the VM that was scanned.
- **UUID** is the UUID for the VM that was scanned.
- **FORMAT** is the format of the file and is one of the formats that you configured in [Configure Scans](#).

For example, the `oscap_store` folder directory looks similar to the following image:



The number of log files in the `output` directory can be calculated as follows:

```
(v + i) * f * b
```

Where:

- **v** is the number of VMs in your PCF deployment.
- **i** is the number of additional instances for any VM in your PCF deployment.
- **f** is the number of formats you configured in [Configure Scans](#).
- **b** is the number of benchmarks you configured in [Configure Scans](#).

Scan Using the Command Line

You also have the option of scanning VMs using the command line. There are two ways to do this:

- [Scan and Retrieve Log Files](#)
- [Retrieve Existing Log Files](#)

Scan and Retrieve Log Files

To start a new scan and retrieve the logs for the completed scan using the command line, do the following:

1. Log in to the BOSH Director.

1. On the Ops Manager VM, create an alias in the BOSH CLI for your BOSH Director IP address. For example:

```
$ bosh alias-env my-env -e 10.0.0.3
```

2. Log in to the BOSH Director, specifying the newly created alias. For example:

```
$ bosh -e my-env log-in
```

2. Run `bosh deployments` to list all the deployment names. For example:

Name	Release(s)	Stemcell(s)
pivotal-container-service	backup-and-restore-sdk/1.8.0	bosh-google-kvm-ubuntu-
xenial-go_agent/97.47	-	
	bosh-dns/1.10.0	
	bosh-dns-aliases/0.0.3	
	bpm/0.6.0	
	cf-mysql/36.14.0	
	docker/32.0.3	
	kubo/0.21.13	
	kubo-service-adapter/1.2.5	
	oscapi/0.1.61	
	pks-telemetry/0.9.4	
scanner-f9822a33c2e0d04cb	bosh-dns/1.10.0	bosh-google-kvm-ubuntu-
xenial-go_agent/170.19	-	
	bosh-dns-aliases/0.0.3	
	clamav/1.4.41	
	ipsec/1.9.14	
	ipsec-verifier/1.9.14	
	oscapi/0.1.61	
service-instance	bosh-dns/1.10.0	bosh-google-kvm-ubuntu-
xenial-go_agent/97.47	-	
	bosh-dns-aliases/0.0.3	pivotal-container-servi
ce	-	
	bpm/0.6.0	
	cfc-etc/1.4.1	
	kubo/0.21.13	

3. Find the `scanner` deployment in the list. It appears as `scanner-DEPLOYMENT-UUID`, where `DEPLOYMENT-UUID` is the UUID of your deployment.
4. Run the following command to start the scan and download the logs:

```
bosh -e my-env -d scanner-DEPLOYMENT-UUID run-errand scan_results --download-logs --logs-dir PATH-TO-SAVE-SCAN-RESULTS
```

Where:

- `scanner-DEPLOYMENT-UUID` is the name of your scanner deployment.
- `PATH-TO-SAVE-SCAN-RESULTS` is the directory in which you would like to save your logs to. You may omit `--logs-dir PATH-TO-SAVE-SCAN-RESULTS` if you want the logs to be saved to your current directory.

For example:

```
bosh -e my-env -d scanner-f9822a33c2e0d04cb run-errand scan_results --download-logs --
```



```
logs-dir scanner/logs/20190131
```



Note: The files generated use the most recent configuration of your tile. To see what the current settings are, see [Configure Scans](#).

Retrieve Existing Log Files

To retrieve existing logs for the most recent completed scan using the command line, use the following command:

```
bosh -e my-env -d scanner-DEPLOYMENT-UUID logs --only=scan_results --dir PATH-TO-SAVE-SCAN-RESULTS
```

Where:

- `scanner-DEPLOYMENT-UUID` is the name of your scanner deployment.
- `PATH-TO-SAVE-SCAN-RESULTS` is the directory in which you would like to save your logs to. You may omit `--dir PATH-TO-SAVE-SCAN-RESULTS` if you want the logs to be saved to your current directory.

For example:

```
bosh -e my-env -d scanner-f9822a33c2e0d04cb logs --only=scan_results --dir scanner/logs/20190131
```

Access Log Files

To access your saved logs, unzip the output ZIP file.

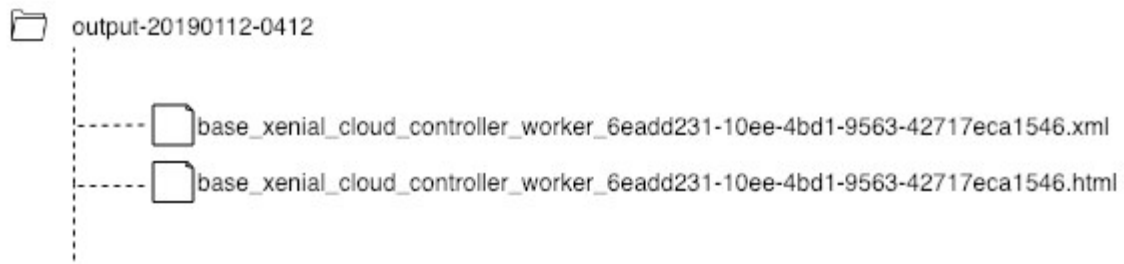
The naming syntax for each log file is the following:

```
BENCHMARK_COMPONENT_UUID.FORMAT
```

Where:

- `BENCHMARK` is the benchmark that was used for the scan.
- `COMPONENT` is the VM that was scanned.
- `UUID` is the UUID for the VM that was scanned.
- `FORMAT` is the format of the file and is one of the formats that you configured in [Configure Scans](#).

For example, the `output` folder directory looks similar to the following image:



View Tests on VMs

For every configuration rule that is checked, there is a corresponding test written in YAML test files residing on each VM. You can use these files as reference for internal test development or to validate that the test matches the description.

To view tests on VMS, do the following:

1. Use the BOSH CLI to SSH into a component VM. For more information, see [BOSH SSH](#).
2. Navigate to the following path:

```
/var/vcap/packages/oscap/xfiles
```

3. Search for the test ID and open the corresponding file.

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Upgrading Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes how to upgrade Compliance Scanner for PCF.

For product versions and upgrade paths, see [Upgrade Planner](#).

Overview

After upgrading Compliance Scanner to a later version, configured properties from your existing tile are brought into the new installation.

Pivotal recommends that you review your **Scan**, **Errand**, and **Resource** settings before applying changes.

Procedure

To upgrade your version of Compliance Scanner to a later version:

1. Download the new version of the product file from Pivotal Network.
2. Follow the procedures found in [Installing and Configuring Compliance Scanner for PCF](#).
3. After applying changes to the Compliance Scanner for PCF tile, **Apply Changes** again for all tiles.
This is so that the version of Compliance Scanner for PCF on the VMs matches the version being used by the scanner.

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Troubleshooting Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic provides instructions for troubleshooting Compliance Scanner for PCF.

scan_results Issues

scan_results Completed with Error (Exit Code 1)

Symptom

Running a scan results in an `exit code 1` error similar to the following:

```
...
Instance    oscap_store/43aba653-4d0a-4cfc-bc72-a136ce33e3e0
Exit Code   1
Stdout      2019/07/05 21:11:04 Starting store on port 28894
            2019/07/05 21:11:05 [10.0.8.6] <nil>

            2019/07/05 21:11:05 Starting scan on 10.0.8.6
            2019/07/05 21:11:05 Get https://10.0.8.6:28893/run: x509: certificate has e
expired or is not yet valid

            Received no scan results

Stderr      -

1 errand(s)
Errand 'scan_results' completed with error (exit code 1)
Exit code 1
```

Explanation

Your certificates have expired.

Solution

Rotate your certificates. For instructions, see [Rotating Certificates](#).

scan_results Received Signal Terminated (Exit Code 124)

Symptom

Running a scan results in an `exit code 124` error similar to the following:

```
...
Instance    oscap_store/43aba653-4d0a-4cfc-bc72-a136ce33e3e0
Exit Code   124
Stdout      2019/06/24 15:43:30 Starting store on port 28894
            2019/06/24 15:43:30 [10.0.8.5] <nil>

            2019/06/24 15:43:30 Starting scan on 10.0.8.5
            2019/06/24 15:43:31 Received signal terminated
            Scanner timed out, did not receive all the scan results in 1200 second(s)
```

Explanation

Your scan has reached the configured timeout period. This may occur if a VM lacks sufficient memory or CPU to finish its scan in time.

Solution

Do one of the following:

- Increase the scan timeout for all VMs. For more information, see **Scanner Timeout** under [Configure Scans](#).
- Increase the memory or CPU resources for any failing scanned VMs.

scan_results Does Not Include Scans for VMs in the Deployment

Symptom

Only scan results for the `oscap_store` VM are being generated. VMs in the deployment are not being scanned.

Explanation

Compliance Scanner is a BOSH add-on, as well as a tile. When a scan is run, the `oscap_store` VM verifies each VM's OSCAP release version. Because of this, the latest OSCAP release must be deployed on all VMs to function properly.

Solution

When installing or upgrading Compliance Scanner, you must **Apply Changes** on PAS (and any other tiles with VMs you want to scan) after applying changes to the Compliance Scanner tile. This is so that the version of Compliance Scanner on the VMs match the version being used by the scanner.

Unable to resolve store domain: no such host

Symptom

Running a scan results in an `exit code 1` error similar to the following:

```
...
Instance    oscap_store/43aba653-4d0a-4cfc-bc72-a136ce33e3e0
Exit Code   1
Stdout      2019/08/05 09:14:01 Starting store on port 28894
            2019/08/05 09:14:01 [172.15.0.3 172.15.0.4 172.15.0.5 172.15.1.5 172.15.1.4]
            <nil>

            2019/08/05 09:14:01 Starting scan on 172.15.0.3
            2019/08/05 09:14:01 Unable to scan 172.15.0.3: 500
            2019/08/05 09:14:01 Starting scan on 172.15.0.4
            2019/08/05 09:14:01 Unable to scan 172.15.0.4: 500
            2019/08/05 09:14:01 Starting scan on 172.15.0.5
            2019/08/05 09:14:01 Unable to scan 172.15.0.5: 500
            2019/08/05 09:14:01 Shutdown
            Received no scan results
```

and produces a `scanner_web_ctl.log` similar to the following:

`/var/vcap/sys/log/config_scanner/scanner_web_ctl.log:`

```
2019/08/05 10:21:34 Lookup store
2019/08/05 10:21:34 Unable to resolve store domain: lookup q-s4.oscap-store.NETWORK-NAME.p-compliance-scanner-5f51f48abb5fbf23b617.bosh on 169.254.0.2:53: no such host
```

Where `NETWORK-NAME` is the name given to the network being used for the Compliance Scanner for PCF tile.

Explanation

BOSH DNS cannot resolve the `oscap_store` VM URL if there is any capitalization in the network's **Name**.

Solution

Verify that the network you selected inside the **Assign AZs and Networks** pane of your Compliance Scanner for PCF tile is not capitalized.

If this is the case, you must edit the name of the network being used to remove the capitalization:

1. On the Pivotal Operations Manager Installation Dashboard, click **BOSH Director**.
2. Click **Create Networks**.
3. Change the network **Name** to a name without capital letters, and click **Save**.
4. Click **Review Pending Changes**, and then **Apply Changes** to all tiles.

This updates the network name property on all VMs.

oscap_store receives ReportFailed (Exit code 1)

Symptom

Running a scan results in an `exit code 1` error similar to the following:

```
...
Instance    oscap_store/43aba653-4d0a-4cfc-bc72-a136ce33e3e0
Exit Code   1
Stdout      2020/03/12 16:51:12 Starting store on port 28894
            2020/03/12 16:51:12 [10.0.0.8 10.0.0.10 10.0.0.9 10.0.0.11]
            2020/03/12 16:51:12 Starting scan on 10.0.0.8
            2020/03/12 16:51:12 Starting scan on 10.0.0.10
            2020/03/12 16:51:12 Starting scan on 10.0.0.9
            2020/03/12 16:51:12 Starting scan on 10.0.0.11
            2020/03/12 16:51:36 ReportFailed
            2020/03/12 16:51:36 Received from 10.0.0.11:59566
            2020/03/12 16:51:36 10.0.0.11:59566 failed: Error from daemon: exit status 1
24 (check the logs at: /var/vcap/sys/log/config_scanner/daemon.log)
            2020/03/12 16:51:36 Attempting to cancel scan on host 10.0.0.9
            2020/03/12 16:51:36 Attempting to cancel scan on host 10.0.0.8
            2020/03/12 16:51:36 Attempting to cancel scan on host 10.0.0.10
            2020/03/12 16:51:36 Failed to cancel scan on host : Get https://10.0.0.10:28
893/cancel: net/http: request canceled while waiting for connection (Client.Timeout exc
ceeded while awaiting headers)
            2020/03/12 16:51:36 Failed to cancel scan on host : Get https://10.0.0.8:288
93/cancel: net/http: request canceled while waiting for connection (Client.Timeout exc
ceeded while awaiting headers)
            2020/03/12 16:51:36 Failed to cancel scan on host : Get https://10.0.0.9:288
93/cancel: net/http: request canceled while waiting for connection (Client.Timeout exc
ceeded while awaiting headers)
            2020/03/12 16:51:36 Shutdown
            Scanner exited with 1 code
```

Explanation

The `oscap_store` receives a `ReportFailed` event from one of the VMs being scanned. The error message `10.0.0.11:59566 failed: Error from daemon: exit status 124` indicates that the scan timed out on that particular VM.

This can happen if a timeout increase was only applied to the `oscap_store` VM.

Solution

Increase the scan timeout for all VMs. For more information, see [Scanner Timeout](#).

Scan Successful with POST Errors

Symptom

Linux VMs without Compliance Scanner installed and all Windows VMs show `POST` errors during a successful scan.

For example:

```
...
```

```

Instance    oscap_store/bcb225db-f29f-4356-9d6a-525cbc99f6e1
Exit Code   0
Stdout      2020-05-13 14:02:42 Starting scan
            2020/05/13 14:02:42 Starting store on port 28894
            2020/05/13 14:02:42 [10.0.4.6 10.0.4.7 10.0.4.5] <nil>
            2020/05/13 14:02:42 Starting scan on 10.0.4.6
            2020/05/13 14:02:42 Starting scan on 10.0.4.7
            2020/05/13 14:02:47 Post https://10.0.4.7:28893/run: net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)
            2020/05/13 14:02:47 Starting scan on 10.0.4.5
            2020/05/13 14:02:47 Post https://10.0.4.5:28893/run: dial tcp 10.0.4.5:28893: connect: connection refused
            2020/05/13 14:03:31 ReportFinished
            2020/05/13 14:03:31 Received oscap_store-bcb225db-f29f-4356-9d6a-525cbc99f6e1.tgz from 10.0.4.6:33670
            2020/05/13 14:03:31 Shutdown
            adding: benchmarks/ (stored 0%)
            adding: benchmarks/CIS-Level-2.xml (deflated 90%)
            adding: benchmarks/Base-Xenial.xml (deflated 93%)
            ...

```

Explanation

Scan results include errors for VMs that Compliance Scanner has skipped:

- **For Windows VMs:**

`net/http: request canceled while waiting for connection (Client.Timeout exceeded while awaiting headers)`

- **For Linux VMs without Compliance Scanner installed and running:**

`dial tcp 10.0.4.5:28893: connect: connection refused`

The above errors do not prevent the remainder of the scans from being completed.

Solution

There are a few situations to consider:

- **If the hosts that provide the errors are Windows VMs:**

This is the expected behavior. Compliance Scanner does not currently support Windows.

- **If the hosts that provide the errors are VMs that you expect to have Compliance Scanner installed and running:**

Perform an “Apply Changes” on the deployment and the Pivotal Compliance Scanner tile to ensure that the VMs have the Compliance Scanner installed and running.

To verify that Compliance Scanner is installed and running, you can run `bosh instances --ps`. Ensure that each VM shows that the `scanner_daemon` and `scanner_web` processes are in a `running` state.

For example:

```
$ bosh instances --ps
```

Instance	Process	Process

State	AZ	IPs	Deployment	
vm/bcb225db-f29f-4356-9d6a-525cbc99f6e1			-	running
	us-east1-b	10.0.4.6	p-compliance-scanner-a7c5cc7f126925f45180	
~			bosh-dns	running
~	-	-	-	
~			bosh-dns-healthcheck	running
~	-	-	-	
~			bosh-dns-resolvconf	running
~	-	-	-	
~			scanner_daemon	running
~	-	-	-	
~			scanner_web	running
~	-	-	-	
~			system-metrics-agent	running
	-	-	-	

[Create a pull request or raise an issue on the source for this page in GitHub](#)

Benchmarks for Compliance Scanner for PCF



Warning: Compliance Scanner for PCF v1.0 is no longer supported because it has reached the End of General Support (EOGS) phase as defined by the [Support Lifecycle Policy](#). To stay up to date with the latest software and security updates, upgrade to a supported version.

Page last updated:

This topic describes the different benchmarks used for scanning in Compliance Scanner for PCF.

Overview

When configuring Compliance Scanner, you choose which benchmarks you want. Benchmarks determine which tests are run by the scanner.

Compliance Scanner offers four scanning benchmarks:

- [Base Xenial](#)
- [Recommended Security Baseline](#)
- [Strict Security Practices](#)
- [STIG for Ubuntu Xenial](#)

Base Xenial

This benchmark is a subset of the full STIG benchmark.

The Base Xenial does not include the STIG tests that fail because of differences between the Xenial stemcells and standard Ubuntu Server image.

Because the removed failed tests do not threaten the security of the system, the remaining tests in the Base Xenial benchmark are a baseline for unaltered stemcells. Use this benchmark to see if the configurations have been further modified.

For information about the STIG benchmark, see [STIG for Ubuntu Xenial](#) below.

Recommended Security Baseline

This benchmark includes tests based on Pivotal's minimum recommended configuration baseline. Your system should implement this benchmark, regardless of the user's deployment or the sensitivity of app data being processed.

Strict Security Practices

Tests covered in this benchmark reflect current best practices. The strict configuration being tested might not be required for low assurance apps. However, the tests become a requirement for systems processing sensitive data and workloads. For example, requiring audit logging takes time and space, but it is required for sensitive tests. This would not be needed when testing a “low assurance” app.

STIG for Ubuntu Xenial

This benchmark contains tests outlined in the Ubuntu 16.04 (Xenial) Security Technical Implementation Guide (STIG) published by the Defense Information Systems Agency (DISA). This benchmark contains the full Ubuntu 16.04 (Xenial) Security Technical Implementation Guide (STIG) set of tests.

This benchmark targets a standard Ubuntu Server. When it is applied to stemcells, certain tests fail for the following reasons:

- The file path specified in the tests is different on the stemcell.
- The failed test is specific to a standard Ubuntu Server image, but is not applicable to a stemcell.
- The failed test adheres to a lower security standard than what Pivotal verifies with the stemcell.

To address failures of the first type, the bundled tests have been updated to reflect the paths used by stemcells. These changes do not compromise the integrity of the tests themselves. The remaining failing tests that highlight stemcell differences can help auditors assess their security posture.

For more information about the Canonical Ubuntu 16.04 LTS STIG guide, use the following link to download a ZIP file of the [Department of Defense's documentation](#).

[Create a pull request or raise an issue on the source for this page in GitHub](#)