



RED HAT ENTERPRISE LINUX 7 STIG
CHEF DOCUMENTATION

Version 3, Release 1

October 2020

Developed by DISA for the DoD

TABLE OF CONTENTS

Page

1. BACKGROUND 1
2. INSTALLATION 2
2.1 Installing Chef Client 2
2.2 Cookbooks 2
2.2.1 Online Installation 2
2.2.2 Offline Installation 2
3. CONFIGURATION 3
3.1 Simple 3
3.2 Custom 3
4. CONTENT EXTRACTION 4
5. OTHER CONSIDERATIONS 5
5.1 The libvirtd Service 5
5.2 FIPS Mode 5
5.3 Reboot for SELINUX Configuration Changes 5

1. BACKGROUND

Chef is an open source, cross-platform configuration management solution used to define and enforce system and application configurations. This package provides Chef configurations that implement most of the Red Hat Enterprise Linux STIG. While the content has been tested during development, all possible system and environmental factors could not be tested. Before using this content in a production environment, please perform testing with the intended settings in your own test environment. There is no mandate to use this content; it is published as a resource to assist in the application of security guidance to your systems. Use it in the manner and to the extent that it assists with this goal.

2. INSTALLATION

The following instructions are for stand-alone installation using chef-client for testing purposes. A production environment will likely use Chef Server and Chef Clients. See here for details.

2.1 Installing Chef Client

Install the Red Hat Enterprise Linux 7 Chef Client from here. Chef Client version 16 is not supported at this time due to incompatibilities with dependent cookbooks.

2.2 Cookbooks

2.2.1 Online Installation

Unzip **`rhel7STIG-chef.zip`**. Run the **`install.sh`** script. This script downloads from the Internet and copies the required cookbook into the local Chef cookbooks directory via Chef Knife. See here for details.

2.2.2 Offline Installation

Unzip **`rhel7STIG-chef.zip`**. Create an empty text file named **`knife.rb`**. On an Internet-connected PC, download the latest **`puppet_compat`** chef cookbook available here. Transfer the **`puppet_compat`** cookbook to the offline location. Unzip and untar the **`puppet_compat`** cookbook. Move the **`puppet_compat`** cookbook into the cookbook folder.

If the chef-client run is also going to be run offline, ensure that yum is configured with access to appropriate Red Hat repositories. Alternatively, to allow the cookbook to run successfully without access to yum repositories, ensure that the following packages that are managed by this cookbook are preinstalled: aide, screen, openssh-clients, openssh-server, esc, pam_pkcs11, and authconfig-gtk.

3. CONFIGURATION

3.1 Simple

To apply the default STIG Chef configuration to the local machine only, run the **`enforce.sh`** script to enforce the STIG. To tailor the configuration, follow the steps in the next section.

3.2 Custom

To customize, adjust the attributes in the **`cookbooks\rhel7STIG\attributes\default.rb`** file. This file contains configuration data to define which configuration settings to manage and the values for these settings. Edit this configuration file in a text editor to best suit each system's requirements as needed. For example, if you wanted to turn off STIG rule ID 204417, you would set the "Manage" attribute equal to **`false`**. If you wanted to set STIG rule ID 204423's minimum password length to 20, you would set the "**`_etc_security_pwquality_conf_Line`**" attribute to **`'minlen = 20'`**.

```
default['rhel7STIG']['stigrule_204417']['Manage'] = false
default['rhel7STIG']['stigrule_204417']['Setting']['_etc_libuser_conf_Value']
= :install

default['rhel7STIG']['stigrule_204423']['Manage'] = true
default['rhel7STIG']['stigrule_204423']['Setting']['_etc_security_pwquality_c
onf_Line'] = 'minlen = 20'
```

For more information on attributes, see here.

Note: While useful for testing, this approach is not recommended for a production Chef Server environment. Rather than changing the cookbook defaults, which may change in future versions of the cookbook, attributes should be overridden using Chef capabilities such as roles or environments.

4. CONTENT EXTRACTION

This compliance extraction methodology returns results based on a system's compliance with the enforcement content. This may be different from STIG compliance. For example, multiple values may be allowed by the STIG but will be marked as "fail" if the value does not match the single exact value in the enforcement content. Additionally, if a value is customized in such a way to violate a STIG rule it will be marked as "pass" since it matches the enforcement content's expected value.

At the completion of a successful Chef run content extraction of the configuration results into XCCDF results can be performed via a Chef handler. Use of this handler can be controlled via modification of the following variable in the **cookbooks/rhel7STIG/attributes/default.rb** file:

```
default['rhel7STIG']['XCCDF_result']['Manage'] = true
```

Configuration of the handler is controlled via modification of the following variables in the **cookbooks/rhel7STIG/recipes/default.rb** file:

```
chef_handler 'Chef::Handler::StigXml' do
  source "#{Chef::Config[:file_cache_path]}/stig_xml.rb"
  arguments :stigName => 'U_Red_Hat_Enterprise_Linux_7_V2R3_Manual-
xccdf.xml', :path => '/path/where/to/write/results.xml'
```

The above resource controls the arguments to the handler writing the XCCDF results file to the :path using the manual STIG named :stigName. The XCCDF results file is output by default as **/tmp/xccdf-results.xml** if no :path is provided.

Note: the STIG name provided above should match the STIG release and version number that the Chef content is built for.

Chef provides a means of checking compliance without enforcement called **--why-run** mode. To use this mode, run the following:

```
chef-client -z -o rhel7STIG --why-run
```

Note: in order for the content extraction handler to function, a prior run without **--why-run** must have completed successfully.

5. OTHER CONSIDERATIONS

5.1 The libvirtd Service

The libvirtd service modifies some sysctl values upon startup that are relevant to STIG compliance. To prevent this from occurring, disable the libvirtd service if not required by running `systemctl disable libvirtd.service` before rebooting.

5.2 FIPS Mode

This cookbook does not configure the system for FIPS mode. We recommend configuring the system for FIPS mode during initial installation. Additional information for enabling FIPS mode is available here.

5.3 Reboot for SELINUX Configuration Changes

If this cookbook makes changes to SELINUX configuration, it will restart the system to allow the new settings to take effect. If an automatic restart is not desired, disable management of these rules.