Guide to the Secure Configuration of Red Hat Enterprise Linux CoreOS 4

with profile NIST 800-53 Moderate-Impact Baseline for Red Hat Enterprise Linux CoreOS

— This compliance profile reflects the core set of Moderate-Impact Baseline configuration settings for deployment of Red Hat Enterprise Linux CoreOS into U.S. Defense, Intelligence, and Civilian agencies. Development partners and sponsors include the U.S. National Institute of Standards and Technology (NIST), U.S. Department of Defense, the National Security Agency, and Red Hat.

This baseline implements configuration requirements from the following sources:

- NIST 800-53 control selections for Moderate-Impact systems (NIST 800-53)

For any differing configuration requirements, e.g. password lengths, the stricter security setting was chosen. Security Requirement Traceability Guides (RTMs) and sample System Security Configuration Guides are provided via the scap-security-guide-docs package.

This profile reflects U.S. Government consensus content and is developed through the ComplianceAsCode initiative, championed by the National Security Agency. Except for differences in formatting to accommodate publishing processes, this profile mirrors ComplianceAsCode content as minor divergences, such as bugfixes, work through the consensus and release processes.

The SCAP Security Guide Project
https://www.open-scap.org/security-policies/scap-security-guide (https://www.open-scap.org/security-policies/scap-security-guide)

This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux CoreOS 4. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the `scap-security-guide` package which is developed at https://www.open-scap.org/security-policies/scap-security-guide (https://www.open-scap.org/security-policies/scap-security-guide).

Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a *catalog, not a checklist*, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF *Profiles*, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.

> Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.

Evaluation Characteristics

Evaluation target	Unknown
Benchmark URL	/content/ssg-rhcos4-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_RHCOS-4
Profile ID	xccdf_org.ssgproject.content_profile_moderate
Started at	2021-06-22T03:43:52+00:00
Finished at	2021-06-22T03:44:03+00:00
Performed by	unknown user

CPE Platforms

- **cpe:/o:redhat:enterprise_linux_coreos:4**

Addresses

Compliance and Scoring

The target system did not satisfy the conditions of 186 rules! Please review rule results and consider applying remediation.

Rule results

45 passed 186 failed 4

Severity of failed rules

3 9 low 168 medium 6

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	39.341774	100.000000	39.34%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Red Hat Enterprise Linux CoreOS 4 **186x fail** **3x notchecked**		
System Settings **176x fail** **2x notchecked**		
Installing and Maintaining Software **2x fail**		
System and Software Integrity **2x fail**		
Federal Information Processing Standard (FIPS) **1x fail**		
Enable FIPS Mode	high	**fail**
System Cryptographic Policies **1x fail**		
Configure SSH to use System Crypto Policy	medium	**pass**
Configure Kerberos to use System Crypto Policy	medium	**pass**
Configure System Cryptography Policy	high	**fail**
Configure OpenSSL library to use System Crypto Policy	medium	**pass**
Sudo		
Account and Access Control **6x fail**		
Warning Banners for System Accesses **1x fail**		

Title	Severity	Result
Modify the System Login Banner	medium	fail
Protect Physical Console Access 3x fail		
Configure Screen Locking 1x fail		
Configure Console Screen Locking 1x fail		
Prevent user from disabling the screen lock	medium	fail
Disable debug-shell SystemD Service	medium	pass
Disable Ctrl-Alt-Del Burst Action	high	fail
Verify that Interactive Boot is Disabled	medium	pass
Require Authentication for Single User Mode	medium	pass
Disable Ctrl-Alt-Del Reboot Activation	high	fail
Protect Accounts by Restricting Password-Based Login 2x fail		
Restrict Root Logins 1x fail		
Verify Only Root Has UID 0	high	pass
Ensure that System Accounts Do Not Run a Shell Upon Login	medium	pass
Direct root Logins Not Allowed	medium	fail
Verify Proper Storage and Existence of Password Hashes 1x fail		
Verify No netrc Files Exist	medium	pass
Prevent Login to Accounts With Empty Password	high	fail
System Accounting with auditd 120x fail		
Configure auditd Data Retention 5x fail		
Include Local Events in Audit Logs	medium	pass
Configure auditd max_log_file_action Upon Reaching Maximum Log Size	medium	pass
Set hostname as computer node name in audit logs	medium	fail
Configure auditd Disk Error Action on Disk Error	medium	fail
Configure auditd space_left on Low Disk Space	medium	fail
Configure auditd Max Log File Size	medium	pass

Title	Severity	Result
Resolve information before writing to audit logs	medium	pass
Configure auditd flush priority	medium	pass
Configure auditd Disk Full Action when Disk Space Is Full	medium	fail
Configure auditd space_left Action on Low Disk Space	medium	pass
Configure auditd Number of Logs Retained	medium	pass
Set number of records to cause an explicit flush to audit logs	medium	pass
Write Audit Logs to the Disk	medium	pass
Configure auditd admin_space_left Action on Low Disk Space	medium	fail
Configure auditd Rules for Comprehensive Auditing **113x fail**		
Record Attempts to Alter Logon and Logout Events **3x fail**		
Record Attempts to Alter Logon and Logout Events - faillock	medium	fail
Record Attempts to Alter Logon and Logout Events - tallylog	medium	fail
Record Attempts to Alter Logon and Logout Events - lastlog	medium	fail
Record Events that Modify the System's Discretionary Access Controls **13x fail**		
Record Events that Modify the System's Discretionary Access Controls - lremovexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - setxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchmodat	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fsetxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - chown	medium	fail
Record Events that Modify the System's Discretionary Access Controls - lchown	medium	fail

Title	Severity	Result
Record Events that Modify the System's Discretionary Access Controls - fremovexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - lsetxattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - removexattr	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchmod	medium	fail
Record Events that Modify the System's Discretionary Access Controls - chmod	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchown	medium	fail
Record Events that Modify the System's Discretionary Access Controls - fchownat	medium	fail
Record File Deletion Events by User 5x fail		
Ensure auditd Collects File Deletion Events by User - renameat	medium	fail
Ensure auditd Collects File Deletion Events by User - unlinkat	medium	fail
Ensure auditd Collects File Deletion Events by User - rmdir	medium	fail
Ensure auditd Collects File Deletion Events by User - unlink	medium	fail
Ensure auditd Collects File Deletion Events by User - rename	medium	fail
Record Information on Kernel Modules Loading and Unloading 3x fail		
Ensure auditd Collects Information on Kernel Module Loading - init_module	medium	fail
Ensure auditd Collects Information on Kernel Module Loading and Unloading - finit_module	medium	fail
Ensure auditd Collects Information on Kernel Module Unloading - delete_module	medium	fail
Record Information on the Use of Privileged Commands 22x fail		

Title	Severity	Result
Ensure auditd Collects Information on the Use of Privileged Commands - usernetctl	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - newgidmap	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - newuidmap	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - userhelper	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - newgrp	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - mount	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - su	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - umount	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - unix_chkpwd	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - ssh-keysign	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - passwd	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - gpasswd	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - at	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - sudoedit	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - chage	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - postqueue	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - chsh	medium	fail

Title	Severity	Result
Ensure auditd Collects Information on the Use of Privileged Commands - crontab	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - sudo	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - pam_timestamp_check	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - pt_chown	medium	fail
Ensure auditd Collects Information on the Use of Privileged Commands - postdrop	medium	fail
Records Events that Modify Date and Time Information 5x fail		
Record Attempts to Alter Time Through clock_settime	medium	fail
Record Attempts to Alter Time Through stime	medium	fail
Record attempts to alter time through adjtimex	medium	fail
Record attempts to alter time through settimeofday	medium	fail
Record Attempts to Alter the localtime File	medium	fail
Record Execution Attempts to Run SELinux Privileged Commands 6x fail		
Record Any Attempts to Run seunshare	medium	fail
Record Any Attempts to Run restorecon	medium	fail
Record Any Attempts to Run setsebool	medium	fail
Record Any Attempts to Run setfiles	medium	fail
Record Any Attempts to Run semanage	medium	fail
Record Any Attempts to Run chcon	medium	fail
Record Unauthorized Access Attempts Events to Files (unsuccessful) 32x fail		
Record Unsuccessul Delete Attempts to Files - rename	medium	fail
Record Unsuccessul Permission Changes to Files - lremovexattr	medium	fail
Record Unsuccessul Ownership Changes to Files - fchown	medium	fail

Title	Severity	Result
Record Unsuccessful Modification Attempts to Files - open_by_handle_at O_TRUNC_WRITE	medium	fail
Ensure auditd Rules For Unauthorized Attempts To openat Are Ordered Correctly	medium	fail
Record Unsuccessul Ownership Changes to Files - fchownat	medium	fail
Record Unsuccessful Access Attempts to Files - open_by_handle_at	medium	fail
Record Unsuccessful Access Attempts to Files - open	medium	fail
Record Unsuccessful Creation Attempts to Files - open_by_handle_at O_CREAT	medium	fail
Record Unsuccessful Access Attempts to Files - truncate	medium	fail
Record Unsuccessul Delete Attempts to Files - unlinkat	medium	fail
Record Unsuccessul Permission Changes to Files - fsetxattr	medium	fail
Ensure auditd Unauthorized Access Attempts To open_by_handle_at Are Ordered Correctly	medium	fail
Record Unsuccessul Permission Changes to Files - fchmodat	medium	fail
Record Unsuccessul Permission Changes to Files - chmod	medium	fail
Record Unsuccessful Creation Attempts to Files - openat O_CREAT	medium	fail
Record Unsuccessul Delete Attempts to Files - unlink	medium	fail
Record Unsuccessful Access Attempts to Files - openat	medium	fail
Record Unsuccessful Modification Attempts to Files - openat O_TRUNC_WRITE	medium	fail
Record Unsuccessul Permission Changes to Files - removexattr	medium	fail

Title	Severity	Result
Record Unsuccessul Ownership Changes to Files - lchown	medium	**fail**
Record Unsuccessful Access Attempts to Files - creat	medium	**fail**
Record Unsuccessful Modification Attempts to Files - open O_TRUNC_WRITE	medium	**fail**
Record Unsuccessul Permission Changes to Files - setxattr	medium	**fail**
Record Unsuccessul Permission Changes to Files - lsetxattr	medium	**fail**
Record Unsuccessul Ownership Changes to Files - chown	medium	**fail**
Record Unsuccessful Access Attempts to Files - ftruncate	medium	**fail**
Record Unsuccessful Creation Attempts to Files - open O_CREAT	medium	**fail**
Ensure auditd Rules For Unauthorized Attempts To open Are Ordered Correctly	medium	**fail**
Record Unsuccessul Permission Changes to Files - fremovexattr	medium	**fail**
Record Unsuccessul Permission Changes to Files - fchmod	medium	**fail**
Record Unsuccessul Delete Attempts to Files - renameat	medium	**fail**
Record Events that Modify the System's Mandatory Access Controls	medium	**fail**
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/group	medium	**fail**
Record Events that Modify User/Group Information via openat syscall - /etc/passwd	medium	**fail**
System Audit Logs Must Have Mode 0750 or Less Permissive	medium	**pass**
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/gshadow	medium	**fail**

Title	Severity	Result
Record Events that Modify User/Group Information - /etc/gshadow	medium	fail
Record Access Events to Audit Log Directory	medium	fail
Record Attempts to Alter Process and Session Initiation Information	medium	fail
Record Events that Modify User/Group Information - /etc/passwd	medium	fail
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/passwd	medium	fail
Record Events that Modify User/Group Information via open_by_handle_at syscall - /etc/shadow	medium	fail
Record Events that Modify User/Group Information via open syscall - /etc/gshadow	medium	fail
Record Events that Modify User/Group Information via open syscall - /etc/passwd	medium	fail
Record Events that Modify User/Group Information - /etc/group	medium	fail
Record Events that Modify User/Group Information via open syscall - /etc/group	medium	fail
Record Events that Modify User/Group Information - /etc/shadow	medium	fail
Record Events that Modify User/Group Information via open syscall - /etc/shadow	medium	fail
Record Events that Modify the System's Network Environment	medium	fail
Record Events that Modify User/Group Information - /etc/security/opasswd	medium	fail
Ensure auditd Collects System Administrator Actions	medium	fail
System Audit Logs Must Have Mode 0640 or Less Permissive	medium	pass
Record Events that Modify User/Group Information via openat syscall - /etc/shadow	medium	fail
Make the auditd Configuration Immutable	medium	fail

Title	Severity	Result
Record Events that Modify User/Group Information via openat syscall - /etc/gshadow	medium	fail
Ensure auditd Collects Information on Exporting to Media (successful)	medium	fail
Record Events that Modify User/Group Information via openat syscall - /etc/group	medium	fail
System Audit Logs Must Be Owned By Root	medium	pass
Ensure the audit Subsystem is Installed	medium	pass
Enable auditd Service	medium	pass
Extend Audit Backlog Limit for the Audit Daemon	medium	fail
Enable Auditing for Processes Which Start Prior to the Audit Daemon	medium	fail
Network Configuration and Firewalls 25x fail 1x notchecked		
IPv6 6x fail		
Configure IPv6 Settings if Necessary 6x fail		
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv6 Interfaces by Default	medium	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv6 Interfaces	medium	fail
Configure Accepting Router Advertisements on All IPv6 Interfaces	medium	fail
Disable Accepting Router Advertisements on all IPv6 Interfaces by Default	medium	fail
Disable Accepting ICMP Redirects for All IPv6 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv6 Interfaces	medium	fail
iptables and ip6tables		
Uncommon Network Protocols 5x fail		
Disable CAN Support	medium	fail
Disable SCTP Support	medium	fail

Title	Severity	Result
Disable TIPC Support	medium	fail
Disable ATM Support	medium	fail
Disable IEEE 1394 (FireWire) Support	medium	fail
Kernel Parameters Which Affect Networking **13x fail**		
Network Parameters for Hosts Only **2x fail**		
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces by Default	medium	fail
Disable Kernel Parameter for Sending ICMP Redirects on all IPv4 Interfaces	medium	fail
Network Related Kernel Runtime Parameters for Hosts and Routers **11x fail**		
Disable Accepting ICMP Redirects for All IPv4 Interfaces	medium	fail
Enable Kernel Parameter to Log Martian Packets on all IPv4 Interfaces	unknown	fail
Disable Kernel Parameter for Accepting ICMP Redirects by Default on IPv4 Interfaces	medium	fail
Enable Kernel Parameter to Ignore Bogus ICMP Error Responses on IPv4 Interfaces	unknown	fail
Enable Kernel Parameter to Use TCP Syncookies on IPv4 Interfaces	medium	fail
Configure Kernel Parameter for Accepting Secure Redirects By Default	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on IPv4 Interfaces by Default	medium	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces by Default	medium	fail
Enable Kernel Parameter to Ignore ICMP Broadcast Echo Requests on IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Secure ICMP Redirects on all IPv4 Interfaces	medium	fail
Disable Kernel Parameter for Accepting Source-Routed Packets on all IPv4 Interfaces	medium	pass

Title	Severity	Result
Enable Kernel Paremeter to Log Martian Packets on all IPv4 Interfaces by Default	unknown	fail
Enable Kernel Parameter to Use Reverse Path Filtering on all IPv4 Interfaces	medium	pass
Wireless Networking 1x fail 1x notchecked		
Disable Wireless Through Software Configuration 1x fail 1x notchecked		
Disable Bluetooth Service	medium	pass
Disable Bluetooth Kernel Module	medium	fail
Deactivate Wireless Network Interfaces	medium	pass
Disable WiFi or Bluetooth in BIOS	unknown	notchecked
GRUB2 bootloader configuration 1x fail		
Disable vsyscalls	info	informational
Enable Kernel Page-Table Isolation (KPTI)	high	fail
Configure Syslog 1x fail		
Ensure All Logs are Rotated by logrotate 1x fail		
Ensure Logrotate Runs Periodically	medium	fail
SELinux 1x fail		
Configure SELinux Policy	medium	pass
Ensure No Daemons are Unconfined by SELinux	medium	fail
Ensure SELinux Not Disabled in the kernel arguments	medium	pass
Ensure SELinux State is Enforcing	medium	pass
File Permissions and Masks 20x fail 1x notchecked		
Restrict Programs from Dangerous Execution Patterns 11x fail		
Memory Poisoning 1x fail		
Enable page allocator poisoning	medium	fail
Disable Core Dumps 4x fail		
Disable acquiring, saving, and processing core dumps	medium	fail

Title	Severity	Result
Disable storing core dump	medium	fail
Disable core dump backtraces	medium	fail
Disable Core Dumps for All Users	medium	fail
Enable ExecShield		
Restrict Access to Kernel Message Buffer	medium	fail
Harden the operation of the BPF just-in-time compiler	medium	fail
Disable storing core dumps	medium	pass
Restrict usage of ptrace to descendant processes	medium	fail
Disable Kernel Image Loading	medium	fail
Disable Access to Network bpf() Syscall From Unprivileged Processes	medium	fail
Disallow kernel profiling by unprivileged users	medium	fail
Restrict Dynamic Mounting and Unmounting of Filesystems **9x fail** **1x notchecked**		
Disable the Automounter	medium	pass
Disable Booting from USB Devices in Boot Firmware	unknown	notchecked
Disable Mounting of hfs	low	fail
Disable Mounting of squashfs	low	fail
Disable Mounting of cramfs	low	fail
Disable Mounting of freevxfs	low	fail
Disable Kernel Support for USB via Bootloader Configuration	medium	fail
Disable Mounting of jffs2	low	fail
Disable Mounting of hfsplus	low	fail
Disable Modprobe Loading of USB Storage Driver	medium	fail
Disable Mounting of udf	low	fail
Verify Permissions on Important Files and Directories		
Services **10x fail** **1x notchecked**		
SSH Server **2x fail** **1x notchecked**		

Title	Severity	Result
Configure OpenSSH Server if Necessary **2x fail** **1x notchecked**		
Limit Users' SSH Access	unknown	**notchecked**
Set SSH Idle Timeout Interval	medium	**fail**
Disable SSH Support for .rhosts Files	medium	**pass**
Set SSH Client Alive Count Max to zero	medium	**fail**
Verify Group Who Owns SSH Server config file	medium	**pass**
Verify Owner on SSH Server config file	medium	**pass**
Verify Permissions on SSH Server Public *.pub Key Files	medium	**pass**
Verify Permissions on SSH Server Private *_key Key Files	medium	**pass**
Verify Permissions on SSH Server config file	medium	**pass**
USBGuard daemon **4x fail**		
Install usbguard Package	medium	**fail**
Enable the USBGuard Service	medium	**fail**
Log USBGuard daemon audit events using Linux Audit	medium	**fail**
Authorize Human Interface Devices and USB hubs in USBGuard daemon	medium	**fail**
Network Time Protocol **4x fail**		
Enable the NTP Daemon	medium	**pass**
Disable network management of chrony daemon	low	**fail**
Specify Additional Remote NTP Servers	medium	**fail**
Configure Time Service Maxpoll Interval	medium	**fail**
Specify a Remote NTP Server	medium	**pass**
Disable chrony daemon from acting as server	low	**fail**