Guide to the Secure Configuration of Ubuntu 20.04

> with profile Standard System Security Profile for Ubuntu 20.04
>
> — This profile contains rules to ensure standard security baseline of an Ubuntu 20.04 system. Regardless of your system's workload all of these checks should pass.

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 Ubuntu 20.04. 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	gn-VirtualBox
Benchmark URL	/home/gn/openscap/build/ssg-ubuntu2004-ds.xml
Benchmark ID	xccdf_org.ssgproject.content_benchmark_UBUNTU_20-04
Profile ID	xccdf_org.ssgproject.content_profile_standard
Started at	2025-07-20T11:53:08

Finished at	2025-07-20T11:53:09
Performed by	gn

CPE Platforms

- **cpe:/o:canonical:ubuntu_linux:20.04::~~lts~~~**

Addresses

- **IPv4** 127.0.0.1
- **IPv4** 192.168.1.14
- **IPv6** 0:0:0:0:0:0:0:1
- **IPv6** fd17:625c:f037:a801:1a4d:32d6:d507:5b29
- **IPv6** fd17:625c:f037:a801:d566:bfaa:ac43:2113
- **IPv6** fe80:0:0:0:a655:43b5:2972:e162
- **MAC** 00:00:00:00:00:00
- **MAC** 08:00:27:47:ED:FA

Compliance and Scoring

The target system did not satisfy the conditions of 10 rules! Furthermore, the results of 2 rules were inconclusive. Please review rule results and consider applying remediation.

Rule results

31 passed 10 failed 3 other

Severity of failed rules

1 other 5 low 4 medium

Score

Scoring system	Score	Maximum	Percent
urn:xccdf:scoring:default	37.777775	100.000000	37.78%

Rule Overview

Title	Severity	Result
Guide to the Secure Configuration of Ubuntu 20.04 **10x fail** **2x error** **1x notchecked**		
System Settings **8x fail** **2x error** **1x notchecked**		

Title	Severity	Result
Installing and Maintaining Software **5x fail**		
Disk Partitioning **5x fail**		
Ensure /home Located On Separate Partition	low	**fail**
Ensure /tmp Located On Separate Partition	low	**fail**
Ensure /var Located On Separate Partition	low	**fail**
Ensure /var/log Located On Separate Partition	low	**fail**
Ensure /var/log/audit Located On Separate Partition	low	**fail**
Account and Access Control **1x notchecked**		
Secure Session Configuration Files for Login Accounts **1x notchecked**		
Ensure users own their home directories	medium	**notchecked**
Configure Syslog **1x fail**		
Ensure Proper Configuration of Log Files		
Ensure All Logs are Rotated by logrotate **1x fail**		
Ensure Logrotate Runs Periodically	medium	**fail**
Ensure rsyslog is Installed	medium	**pass**
Enable rsyslog Service	medium	**pass**
File Permissions and Masks **2x fail** **2x error**		
Verify Permissions on Important Files and Directories **2x error**		
Verify Permissions on Files with Local Account Information and Credentials		
Verify Permissions on System.map Files	low	**pass**
Enable Kernel Parameter to Enforce DAC on Hardlinks	medium	**error**
Enable Kernel Parameter to Enforce DAC on Symlinks	medium	**error**
Restrict Programs from Dangerous Execution Patterns **2x fail**		
Disable Core Dumps **1x fail**		
Disable Core Dumps for SUID programs	medium	**fail**

Title	Severity	Result
Enable ExecShield **1x fail**		
Enable Randomized Layout of Virtual Address Space	medium	**fail**
Services **1x fail**		
Apport Service **1x fail**		
Disable Apport Service	unknown	**fail**
Cron and At Daemons		
Deprecated services		
Network Time Protocol		
SSH Server		
System Accounting with auditd **1x fail**		
Ensure the audit Subsystem is Installed	medium	**fail**
Enable auditd Service	medium	**notapplicable**

Generated using OpenSCAP (http://open-scap.org) 1.2.16