info@wazuh.com
https://wazuh.com

NIST 800-53 report

Warning. Agent is disconnected

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
002	ubuntu-devangs	192.168.1.51	Wazuh v4.14.1	wazuh-server	Ubuntu 20.04.6 LTS	Jan 8, 2026 @ 01:14:39.000	Jan 8, 2026 @ 11:45:15.000

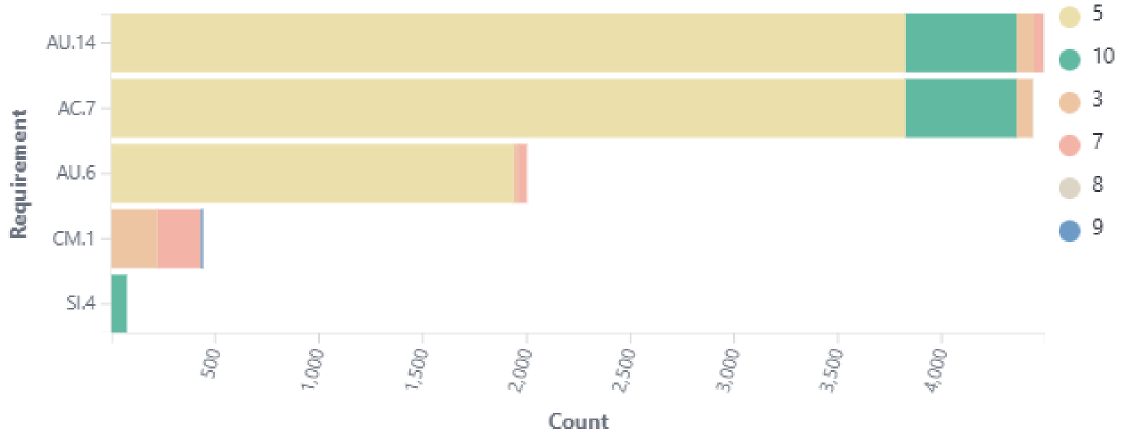
Group: default

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

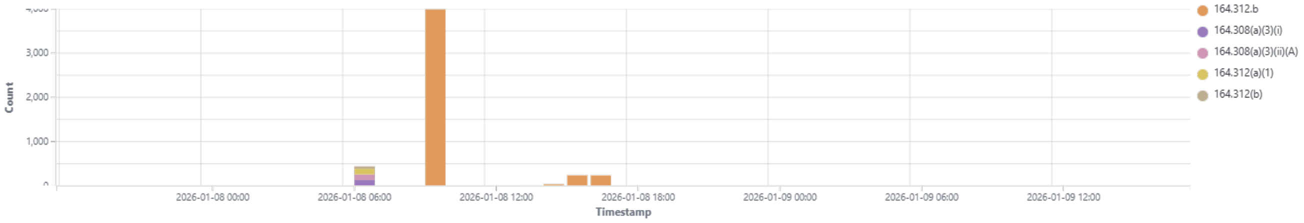
2026-01-07T17:22:49 to 2026-01-09T17:22:49

manager.name: wazuh-server AND rule.nist_800_53: * AND agent.id: 002

Requirements distributed by level



Requirements over time

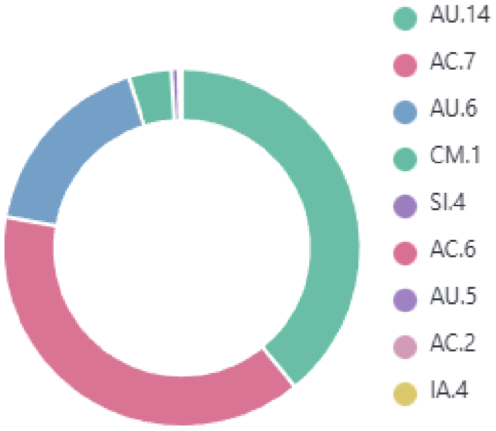


Stats

4,949
Total alerts

10
Max rule level

Top 10 requirements



Alerts summary

Requirement	Level	Description	Count
AU.14	5	sshd: Attempt to login using a non-existent user	1936
AC.7	5	sshd: Attempt to login using a non-existent user	1936
AU.6	5	sshd: Attempt to login using a non-existent user	1936
AU.14	5	sshd: authentication failed.	1224
AC.7	5	sshd: authentication failed.	1224
AU.14	5	PAM: User login failed.	475
AC.7	5	PAM: User login failed.	475
AU.14	10	syslog: User missed the password more than one time	410
AC.7	10	syslog: User missed the password more than one time	410
AU.14	5	syslog: User authentication failure.	191
AC.7	5	syslog: User authentication failure.	191
AU.14	10	PAM: Multiple failed logins in a small period of time.	64
AC.7	10	PAM: Multiple failed logins in a small period of time.	64
SI.4	10	PAM: Multiple failed logins in a small period of time.	64
AU.14	10	Multiple authentication failures.	48
AC.7	10	Multiple authentication failures.	48
AU.14	3	PAM: Login session opened.	30
AC.7	3	PAM: Login session opened.	30
AU.14	3	PAM: Login session closed.	28
AC.7	3	PAM: Login session closed.	28
AU.14	7	Dpkg (Debian Package) half configured.	19
AU.14	7	New dpkg (Debian Package) installed.	19
AU.6	7	Dpkg (Debian Package) half configured.	19
AU.6	7	New dpkg (Debian Package) installed.	19
AU.14	3	Successful sudo to ROOT executed.	18
AC.7	3	Successful sudo to ROOT executed.	18
AU.6	3	New dpkg (Debian Package) requested to install.	12
AU.14	10	sshd: brute force trying to get access to the system. Authentication failed.	9
AC.7	10	sshd: brute force trying to get access to the system. Authentication failed.	9
SI.4	10	sshd: brute force trying to get access to the system. Authentication failed.	9
AU.14	7	Listened ports status (netstat) changed (new port opened or closed).	6
AU.6	7	Listened ports status (netstat) changed (new port opened or closed).	6
AU.14	3	Wazuh agent disconnected.	4
AU.14	3	Wazuh agent started.	4
AU.6	3	Wazuh agent disconnected.	4
AU.6	3	Wazuh agent started.	4

Requirement	Level	Description	Count
AU.14	8	New user added to the system.	3
AC.7	8	New user added to the system.	3
AU.14	10	Three failed attempts to run sudo	2
AC.7	10	Three failed attempts to run sudo	2
AU.6	3	New wazuh agent connected.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Disable Automounting.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure /etc/shadow password fields are not empty.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AppArmor is installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure Automatic Error Reporting is not enabled.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure DHCP Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure DNS Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure FTP Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure HTTP Proxy Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure HTTP server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure IMAP and POP3 server are not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure IPv6 status is identified.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure LDAP client is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure LDAP server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NFS is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NIS Client is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure NIS Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure RPC is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SNMP Server is not installed.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled.	2
CM.1	3	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH HostbasedAuthentication is disabled.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure /tmp is a separate partition.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AIDE is	2

Requirement	Level	Description	Count
		installed.	
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure AppArmor is enabled in the bootloader configuration.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure Avahi Server is not installed.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure CUPS is not installed.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure GNOME Display Manager is removed.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure X Window System is not installed.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure access to the su command is restricted.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure actions as another user are always logged.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure all AppArmor Profiles are enforcing.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure at is restricted to authorized users.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit log storage size is configured.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit logs are not automatically deleted.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure audit_backlog_limit is sufficient.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditd is installed.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditd service is enabled and active.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure auditing for processes that start prior to auditd is enabled.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure bluetooth is disabled.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure bootloader password is set.	2
CM.1	7	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure changes to system administration scope (sudoers) is collected.	2
AU.14	10	sshd: brute force trying to get access to the system. Non existent user.	1
AU.14	3	sshd: authentication success.	1
AU.14	8	New group added to the system.	1
AC.7	10	sshd: brute force trying to get access to the system. Non existent user.	1
AC.7	3	sshd: authentication success.	1
AC.7	8	New group added to the system.	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH AllowTcpForwarding is disabled.: Status changed from 'not applicable' to failed	1

Requirement	Level	Description	Count
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH Idle Timeout Interval is configured.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH LogLevel is appropriate.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH LoginGraceTime is set to one minute or less.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH MaxAuthTries is set to 4 or less.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH MaxStartups is configured.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH X11 forwarding is disabled.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH access is limited.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH root login is disabled.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure SSH warning banner is configured.: Status changed from 'not applicable' to failed	1
CM.1	9	CIS Ubuntu Linux 20.04 LTS Benchmark v2.0.0: Ensure only strong MAC algorithms are used.: Status changed from 'not applicable' to failed	1
SI.4	10	sshd: brute force trying to get access to the system. Non existent user.	1