Inventory data report

ID	Name	IP	Version	Manager	OS
029	S-DEMO-SIT01	10.101.4.38	Wazuh v3.9.5	S-DEMO-SEC01.example.com	CentOS Linux 7.6

Registration date: 2019-09-11 08:04:04.

Last keep alive: 2019-09-11 10:15:15.

Group: default

Applications, network configuration, open ports and processes running on your monitored systems.

Hardware information

- 4 cores
- Intel(R) Xeon(R) CPU   E5640 @ 2.67GHz
- 7.80GB RAM

OS information

- Linux
- #1 SMP Mon Jul 29 17:46:05 UTC 2019
- x86_64
- 3.10.0-957.27.2.el7.x86_64
- CentOS Linux 7.6

Packages

Name	Architecture	Version	Vendor	Description
mdadm	x86_64	4.1-rc1_2.el7	CentOS	The mdadm program controls Linux md devices (software RAID arrays)
kbd-legacy	noarch	1.15.5-15.el7	CentOS	Legacy data for kbd package
man-pages	noarch	3.53-5.el7	CentOS	Man (manual) pages from the Linux Documentation Project
ncurses-base	noarch	5.9-14.20130511.el7_4	CentOS	Descriptions of common terminals
net-tools	x86_64	2.0-0.24.20131004git.el7	CentOS	Basic networking tools
irqbalance	x86_64	3:1.0.7-11.el7	CentOS	IRQ balancing daemon
rsync	x86_64	3.1.2-6.el7_6.1	CentOS	A program for synchronizing files over a network
biosdevname	x86_64	0.7.3-1.el7	CentOS	Udev helper for naming devices per BIOS names
basesystem	noarch	10.0-7.el7.centos	CentOS	The skeleton package which defines a simple CentOS Linux system
mlocate	x86_64	0.26-8.el7	CentOS	An utility for finding files by name
man-db	x86_64	2.6.3-11.el7	CentOS	Tools for searching and reading man pages
nano	x86_64	2.3.1-10.el7	CentOS	A small text editor
passwd	x86_64	0.79-4.el7	CentOS	An utility for setting or changing passwords using PAM
ncurses-libs	x86_64	5.9-14.20130511.el7_4	CentOS	Ncurses libraries
rng-tools	x86_64	6.3.1-3.el7	CentOS	Random number generator related utilities
libffi	x86_64	3.0.13-18.el7	CentOS	A portable foreign function interface library
rfkill	x86_64	0.4-10.el7	CentOS	A tool for enabling and disabling wireless devices
pcre	x86_64	8.32-17.el7	CentOS	Perl-compatible regular expression library
blktrace	x86_64	1.0.5-8.el7	CentOS	Utilities for performing block layer IO tracing in the linux kernel
p11-kit	x86_64	0.23.5-3.el7	CentOS	Library for loading and sharing PKCS#11 modules
rdate	x86_64	1.4-25.el7	CentOS	Tool for getting the date/time from a remote machine
libtasn1	x86_64	4.10-1.el7	CentOS	The ASN.1 library used in GNUTLS
bpftool	x86_64	3.10.0-957.27.2.el7	CentOS	Inspection and simple manipulation of eBPF programs and maps
coreutils	x86_64	8.22-23.el7	CentOS	A set of basic GNU tools commonly used in shell scripts
libsemanage-python	x86_64	2.5-14.el7	CentOS	semanage python bindings for libsemanage
libgcc	x86_64	4.8.5-36.el7_6.2	CentOS	GCC version 4.8 shared support library
auditbeat	x86_64	7.2.1-1	Elastic	Audit the activities of users and processes on your system.
glibc-common	x86_64	2.17-260.el7_6.6	CentOS	Common binaries and locale data for glibc
readline	x86_64	6.2-10.el7	CentOS	A library for editing typed command lines
fontpackages-filesystem	noarch	1.44-8.el7	CentOS	Directories used by font packages
libuuid	x86_64	2.23.2-59.el7_6.1	CentOS	Universally unique ID library
libcap-ng	x86_64	0.7.5-4.el7	CentOS	An alternate posix capabilities library
dejavu-sans-fonts	noarch	2.33-6.el7	CentOS	Variable-width sans-serif font faces

Name	Architecture	Version	Vendor	Description
libmount	x86_64	2.23.2-59.el7_6.1	CentOS	Device mounting library
cpio	x86_64	2.11-27.el7	CentOS	A GNU archiving program
perl-TimeDate	noarch	1:2.30-2.el7	CentOS	A Perl module for time and date manipulation
python	x86_64	2.7.5-80.el7_6	CentOS	An interpreted, interactive, object-oriented programming language
which	x86_64	2.20-7.el7	CentOS	Displays where a particular program in your path is located
libXext	x86_64	1.3.3-3.el7	CentOS	X.Org X11 libXext runtime library
NetworkManager-libnm	x86_64	1:1.12.0-10.el7_6	CentOS	Libraries for adding NetworkManager support to applications (new API).
sqlite	x86_64	3.7.17-8.el7	CentOS	Library that implements an embeddable SQL database engine
mesa-libGL	x86_64	18.0.5-4.el7_6	CentOS	Mesa libGL runtime libraries and DRI drivers
python-perf	x86_64	3.10.0-957.27.2.el7	CentOS	Python bindings for apps which will manipulate perf events
file-libs	x86_64	5.11-35.el7	CentOS	Libraries for applications using libmagic
perl-IO-Tty	x86_64	1.10-11.el7	CentOS	Perl interface to pseudo tty's
dbus	x86_64	1:1.10.24-13.el7_6	CentOS	D-BUS message bus
libcroco	x86_64	0.6.12-4.el7	CentOS	A CSS2 parsing library
mesa-libEGL	x86_64	18.0.5-4.el7_6	CentOS	Mesa libEGL runtime libraries
cronie	x86_64	1.4.11-20.el7_6	CentOS	Cron daemon for executing programs at set times
tcpflow	x86_64	1.4.5-1.el7	Fedora Project	Network traffic recorder
libsmartcols	x86_64	2.23.2-59.el7_6.1	CentOS	Formatting library for ls-like programs.
libnl3-cli	x86_64	3.2.28-4.el7	CentOS	Command line interface utils for libnl3
aide	x86_64	0.15.1-13.el7	CentOS	Intrusion detection environment
device-mapper	x86_64	7:1.02.149-10.el7_6.8	CentOS	Device mapper utility
groff-base	x86_64	1.22.2-8.el7	CentOS	Parts of the groff formatting system required to display manual pages
deltarpm	x86_64	3.6-3.el7	CentOS	Create deltas between rpms
device-mapper-event	x86_64	7:1.02.149-10.el7_6.8	CentOS	Device-mapper event daemon
e2fsprogs-libs	x86_64	1.42.9-13.el7	CentOS	Ext2/3/4 filesystem-specific shared libraries
tree	x86_64	1.6.0-10.el7	CentOS	File system tree viewer
grub2-tools-extra	x86_64	1:2.02-0.76.el7.centos.1	CentOS	Support tools for GRUB.
slang	x86_64	2.2.4-11.el7	CentOS	The shared library for the S-Lang extension language
iotop	noarch	0.6-4.el7	CentOS	Top like utility for I/O
bind-libs-lite	x86_64	32:9.9.4-74.el7_6.2	CentOS	Libraries for working with the DNS protocol
lzo	x86_64	2.06-8.el7	CentOS	Data compression library with very fast (de)compression
python-backports	x86_64	1.0-8.el7	CentOS	Namespace for backported Python features
lvm2	x86_64	7:2.02.180-10.el7_6.8	CentOS	Userland logical volume management tools
python-decorator	noarch	3.4.0-3.el7	CentOS	Module to simplify usage of decorators
python2-pip	noarch	8.1.2-10.el7	Fedora Project	A tool for installing and managing Python 2 packages
NetworkManager-	x86_64	1:1.12.0-10.el7_6	CentOS	NetworkManager curses-based UI

Name	Architecture	Version	Vendor	Description
tui				
libselinux-python	x86_64	2.5-14.1.el7	CentOS	SELinux python bindings for libselinux
libxslt	x86_64	1.1.28-5.el7	CentOS	Library providing the Gnome XSLT engine
kexec-tools	x86_64	2.0.15-21.el7_6.4	CentOS	The kexec/kdump userspace component.
pyliblzma	x86_64	0.5.3-11.el7	CentOS	Python bindings for lzma
wazuh-agent	x86_64	3.9.5-1	Wazuh, Inc <info@wazuh.com>	Wazuh helps you to gain security visibility into your infrastructure by monitoring hosts at an operating system and application level. It provides the following capabilities: log analysis, file integrity monitoring, intrusions detection and policy and compliance monitoring
iproute	x86_64	4.11.0-14.el7_6.2	CentOS	Advanced IP routing and network device configuration tools
python-websocket-client	noarch	0.56.0-3.git3c25814.el7	CentOS	WebSocket client for python
kernel	x86_64	3.10.0-957.27.2.el7	CentOS	The Linux kernel
iptables	x86_64	1.4.21-28.el7	CentOS	Tools for managing Linux kernel packet filtering capabilities
python-docker-py	noarch	1:1.10.6-9.el7_6	CentOS	An API client for docker written in Python
xmlrpc-c	x86_64	1.32.5-1905.svn2451.el7	CentOS	A lightweight RPC library based on XML and HTTP
less	x86_64	458-9.el7	CentOS	A text file browser similar to more, but better
python2-pyasn1-modules	noarch	0.1.9-7.el7	CentOS	Modules for pyasn1
hunspell	x86_64	1.3.2-15.el7	CentOS	A spell checker and morphological analyzer library
python-babel	noarch	0.9.6-8.el7	CentOS	Library for internationalizing Python applications
mailx	x86_64	12.5-19.el7	CentOS	Enhanced implementation of the mailx command
python-gobject-base	x86_64	3.22.0-1.el7_4.1	CentOS	Python 2 bindings for GObject Introspection base package
python-markupsafe	x86_64	0.11-10.el7	CentOS	Implements a XML/HTML/XHTML Markup safe string for Python
libreport-python	x86_64	2.1.11-42.el7.centos	CentOS	Python bindings for report-libs
fipscheck	x86_64	1.4.1-6.el7	CentOS	A library for integrity verification of FIPS validated modules
python2-ruamel-ordereddict	x86_64	0.4.9-2.el7	Fedora Project	Ordered dictionary with Key Insertion Order
libreport-cli	x86_64	2.1.11-42.el7.centos	CentOS	libreport's command line interface
python2-cryptography	x86_64	1.7.2-2.el7	CentOS	PyCA's cryptography library
hunspell-en-GB	noarch	0.20121024-6.el7	CentOS	UK English hunspell dictionaries
python2-string_utils	noarch	0.6.0-4.el7	Fedora Project	A python module containing utility functions for strings
perl-HTTP-Tiny	noarch	0.033-3.el7	CentOS	Small, simple, correct HTTP/1.1 client
logrotate	x86_64	3.8.6-17.el7	CentOS	Rotates, compresses, removes and mails system log files
python2-openshift	noarch	1:0.8.8-1.el7	Fedora Project	Python client for the OpenShift API
perl-Text-ParseWords	noarch	3.29-4.el7	CentOS	Parse text into an array of tokens or array of arrays

Name	Architecture	Version	Vendor	Description
libselinux-utils	x86_64	2.5-14.1.el7	CentOS	SELinux libselinux utilies

Processes

Name	Effective user	Priority	State
systemd	root	0	Interruptible sleep (waiting for an event to complete)
kthreadd	root	0	Interruptible sleep (waiting for an event to complete)
ksoftirqd/0	root	0	Interruptible sleep (waiting for an event to complete)
kworker/0:0H	root	-20	Interruptible sleep (waiting for an event to complete)
migration/0	root	0	Interruptible sleep (waiting for an event to complete)
rcu_bh	root	0	Interruptible sleep (waiting for an event to complete)
rcu_sched	root	0	Interruptible sleep (waiting for an event to complete)
lru-add-drain	root	-20	Interruptible sleep (waiting for an event to complete)
watchdog/0	root	0	Interruptible sleep (waiting for an event to complete)
watchdog/1	root	0	Interruptible sleep (waiting for an event to complete)
migration/1	root	0	Interruptible sleep (waiting for an event to complete)
ksoftirqd/1	root	0	Interruptible sleep (waiting for an event to complete)
kworker/1:0H	root	-20	Interruptible sleep (waiting for an event to complete)
watchdog/2	root	0	Interruptible sleep (waiting for an event to complete)
migration/2	root	0	Interruptible sleep (waiting for an event to complete)
ksoftirqd/2	root	0	Interruptible sleep (waiting for an event to complete)
kworker/2:0H	root	-20	Interruptible sleep (waiting for an event to complete)
watchdog/3	root	0	Interruptible sleep (waiting for an event to complete)
migration/3	root	0	Interruptible sleep (waiting for an event to complete)
ksoftirqd/3	root	0	Interruptible sleep (waiting for an event to complete)
kworker/3:0H	root	-20	Interruptible sleep (waiting for an event to complete)
kdevtmpfs	root	0	Interruptible sleep (waiting for an event to complete)
netns	root	-20	Interruptible sleep (waiting for an event to complete)
khungtaskd	root	0	Interruptible sleep (waiting for an event to complete)
writeback	root	-20	Interruptible sleep (waiting for an event to complete)
kintegrityd	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
kblockd	root	-20	Interruptible sleep (waiting for an event to complete)
md	root	-20	Interruptible sleep (waiting for an event to complete)
edac-poller	root	-20	Interruptible sleep (waiting for an event to complete)
watchdogd	root	-20	Interruptible sleep (waiting for an event to complete)
kswapd0	root	0	Interruptible sleep (waiting for an event to complete)
ksmd	root	5	Interruptible sleep (waiting for an event to complete)
crypto	root	-20	Interruptible sleep (waiting for an event to complete)
kthrotld	root	-20	Interruptible sleep (waiting for an event to complete)
kmpath_rdacd	root	-20	Interruptible sleep (waiting for an event to complete)
kaluad	root	-20	Interruptible sleep (waiting for an event to complete)

Name	Effective user	Priority	State
kpsmoused	root	-20	Interruptible sleep (waiting for an event to complete)
deferwq	root	-20	Interruptible sleep (waiting for an event to complete)
kworker/2:1	root	0	Interruptible sleep (waiting for an event to complete)
kauditd	root	0	Interruptible sleep (waiting for an event to complete)
mpt_poll_0	root	-20	Interruptible sleep (waiting for an event to complete)
mpt/0	root	-20	Interruptible sleep (waiting for an event to complete)
ata_sff	root	-20	Interruptible sleep (waiting for an event to complete)
scsi_eh_0	root	0	Interruptible sleep (waiting for an event to complete)
scsi_tmf_0	root	-20	Interruptible sleep (waiting for an event to complete)
scsi_eh_1	root	0	Interruptible sleep (waiting for an event to complete)
scsi_tmf_1	root	-20	Interruptible sleep (waiting for an event to complete)
scsi_eh_2	root	0	Interruptible sleep (waiting for an event to complete)
scsi_tmf_2	root	-20	Interruptible sleep (waiting for an event to complete)
ttm_swap	root	-20	Interruptible sleep (waiting for an event to complete)
irq/16-vmwgfx	root	0	Interruptible sleep (waiting for an event to complete)
kworker/1:1H	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
xfsalloc	root	-20	Interruptible sleep (waiting for an event to complete)
xfs_mru_cache	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-buf/dm-0	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-data/dm-0	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-conv/dm-0	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-reclaim/dm-	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-cil/dm-0	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-log/dm-0	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-eofblocks/d	root	-20	Interruptible sleep (waiting for an event to complete)
xfsaild/dm-0	root	0	Interruptible sleep (waiting for an event to complete)
systemd-journal	root	0	Interruptible sleep (waiting for an event to complete)
lvmetad	root	0	Interruptible sleep (waiting for an event to complete)
systemd-udevd	root	0	Interruptible sleep (waiting for an event to complete)
kworker/3:0	root	0	Interruptible sleep (waiting for an event to complete)
xfs-buf/sda1	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-data/sda1	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-conv/sda1	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-cil/sda1	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-reclaim/sda	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-log/sda1	root	-20	Interruptible sleep (waiting for an event to complete)

Name	Effective user	Priority	State
xfs-eofblocks/s	root	-20	Interruptible sleep (waiting for an event to complete)
xfsaild/sda1	root	0	Interruptible sleep (waiting for an event to complete)
kworker/0:1H	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
kdmflush	root	-20	Interruptible sleep (waiting for an event to complete)
bioset	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-buf/dm-5	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-conv/dm-5	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-cil/dm-5	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-data/dm-5	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-log/dm-5	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-reclaim/dm-	root	-20	Interruptible sleep (waiting for an event to complete)
xfs-eofblocks/d	root	-20	Interruptible sleep (waiting for an event to complete)
xfsaild/dm-5	root	0	Interruptible sleep (waiting for an event to complete)

Network ports

Local IP	Local port	Process	State	Protocol
127.0.0.1	40510		listening	tcp
127.0.0.1	33126		listening	tcp
127.0.0.1	10248		listening	tcp
0.0.0.0	9480		listening	tcp
127.0.0.1	10249		listening	tcp
0.0.0.0	10250		listening	tcp
127.0.0.1	9099		listening	tcp
0.0.0.0	10251		listening	tcp
0.0.0.0	6443		listening	tcp
10.101.4.38	2379		listening	tcp
127.0.0.1	2379		listening	tcp
0.0.0.0	9323		listening	tcp
127.0.0.1	5067		listening	tcp
0.0.0.0	10252		listening	tcp
10.101.4.38	2380		listening	tcp
0.0.0.0	9100		listening	tcp
10.101.4.38	8301		listening	tcp
0.0.0.0	10256		listening	tcp
127.0.0.1	10257		listening	tcp
0.0.0.0	179		listening	tcp
127.0.0.1	10259		listening	tcp
0.0.0.0	9107		listening	tcp
0.0.0.0	8500		listening	tcp
0.0.0.0	22		listening	tcp
0.0.0.0	8600		listening	tcp

Network interfaces

Name	Mac	State	MTU	Type
eth0	00:50:56:aa:40:28	up	1500	ethernet
docker0	02:42:a6:e0:7f:50	down	1500	ethernet
calif604128f35f	ee:ee:ee:ee:ee:ee	up	1440	ethernet
tunl0	00:00:00:00	unknown	1440	tunnel
calia6cee398ae0	ee:ee:ee:ee:ee:ee	up	1440	ethernet
caliad561166ebc	ee:ee:ee:ee:ee:ee	up	1440	ethernet
cali59ed96a0a2a	ee:ee:ee:ee:ee:ee	up	1440	ethernet

Network settings

Interface	Address	Netmask	Protocol	Broadcast
	172.17.0.1	255.255.0.0		172.17.255.255
	10.101.4.38	255.255.255.240		10.101.4.47
	10.244.173.192	255.255.255.255		10.244.173.192