Agent 001 configuration

ID	Name	IP address	Version	Manager	Operating system	Registration date	Last keep alive
001	wazuh_agent_ubuntu	172.20.0.8	Wazuh v4.9.0	wazuh-manager-4.9.0-7102	Ubuntu 22.04.3 LTS	May 14, 2024 @ 14:50:11.000	May 15, 2024 @ 16:17:44.000

Group: default

Main configurations

Global configuration

Logging settings that apply to the agent

Write internal logs in plain text	yes
Write internal logs in JSON format	no

Communication

Settings related to the connection with the manager

Configuration profiles	ubuntu, ubuntu22, ubuntu22.04
Time (in seconds) between agent checkings to the manager	10
Time (in seconds) before attempting to reconnect	60
force_reconnect_interval	-
ip_update_interval	-
Auto-restart the agent when receiving valid configuration from manager	yes
Remote configuration is enabled	yes
Method used to encrypt communications	aes

List of managers to connect

Address	Port	Max_retries	Retry_interval	Protocol
wazuh-manager-master	1514	5	10	tcp

enabled	yes
delay_after_enrollment	20
port	1515
ssl_cipher	HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH
auto_method	no

Anti-flooding settings

Copyright © 2023 Wazuh, Inc.

Agent bucket parameters to avoid event flooding

Buffer disabled	no
Queue size	5000
Events per second	500

Agent labels

User-defined information about the agent included in alerts

Auditing and policy monitoring

Policy monitoring

Configuration to ensure compliance with security policies, standards and hardening guides

General

Policy monitoring service disabled	no
Base directory	-
Rootkit files database path	etc/shared/rootkit_files.txt
Rootkit trojans database path	etc/shared/rootkit_trojans.txt
Scan the entire system	no
Skip scan on CIFS/NFS mounts	yes
Frequency (in seconds) to run the scan	43200
Check /dev path	yes
Check files	yes
Check network interfaces	yes
Check processes IDs	yes
Check network ports	yes
Check anomalous system objects	yes
Check trojans	yes
Check UNIX audit	no
ignore	/var/lib/containerd /var/lib/docker/overlay2

Security configuration assessment

Interval	43200
Security configuration assessment enabled	yes
Scan on start	yes
Skip scan on CIFS/NFS mounts	yes
Policies	/var/ossec/ruleset/sca/cis_ubuntu22-04.yml

CIS-CAT

Copyright © 2023 Wazuh, Inc.

Configuration assessment using CIS scanner and SCAP checks

CIS-CAT integration disabled	yes
Scan on start	yes
Interval between scan executions	86400
Path to Java executable directory	wodles/java
Path to CIS-CAT executable directory	wodles/ciscat
ciscat_binary	CIS-CAT.sh
Timeout (in seconds) for scan executions	1800

System threats and incident response

Osquery

Expose an operating system as a high-performance relational database

Osquery integration disabled	yes
Auto-run the Osquery daemon	yes
Use defined labels as decorators	yes
Path to the Osquery results log file	/var/log/osquery/osqueryd.results.log
Path to the Osquery configuration file	/etc/osquery/osquery.conf

Inventory data

Gather relevant information about the operating system, hardware, networking and packages

Syscollector integration disabled	no
Scan on start	yes
Interval between system scans	3600
Scan network interfaces	yes
Scan operating system info	yes
Scan hardware info	yes
Scan installed packages	yes
Scan listening network ports	yes
Scan all network ports	no
Scan current processes	yes
sync_max_eps	10

Active response

Active threat addressing by immediate response

Active response disabled	no

Copyright © 2023 Wazuh, Inc.

Commands

Configuration options of the Command wodle

This module is not configured. Please take a look on how to configure it in commands configuration.

Log data analysis

Log collection

Log analysis from text files, Windows events or syslog outputs

Syslog

File	Logformat	Ignore_binaries	Only-future-events	Target
/var/ossec/logs/active-responses.log	syslog	no	yes	agent
/var/log/dpkg.log	syslog	no	yes	agent

Command

Logformat	Command	Alias	Ignore_binaries	Target	Frequency
command	df -P	df -P	no	agent	360

Full command

Logformat	Command	Alias	Ignore_binaries	Target	Frequency
full_command	netstat -tulpn | sed 's/\([[:alnum:]]\+\)\ \+[[:digit:]]\+\ \+[[:digit:]]\+\ \+ \(.*\):\([[:digit:]]*\)\ \+\([0-9\.\:*]\+\).\+\ \([[:digit:]]*\/[[:alnum:]\-]*\).*/\1 \2 == \3 == \4 \5/' | sort -k 4 -g | sed 's/ == \(.*\) ==/:\1/' | sed 1,2d	netstat listening ports	no	agent	360
full_command	last -n 20	last -n 20	no	agent	360

Integrity monitoring

Identify changes in content, permissions, ownership, and attributes of files

General

Integrity monitoring disabled	no
Interval (in seconds) to run the integrity scan	43200
Skip scan on CIFS/NFS mounts	yes
skip_dev	yes
skip_sys	yes
skip_proc	yes
Scan on start	yes
max_files_per_second	-
No diff directories	/etc/ssl/private.key

Copyright © 2023 Wazuh, Inc.

Ignored files and directories	/etc/mtab /etc/hosts.deny /etc/mail/statistics /etc/random-seed /etc/random.seed /etc/adjtime /etc/httpd/logs /etc/utmpx /etc/wtmpx /etc/cups/certs /etc/dumpdates /etc/svc/volatile
ignore_sregex	.log$\|.swp$
allow_remote_prefilter_cmd	no
max_eps	50
process_priority	10
database	disk

Who data

Restart audit	yes
Startup healthcheck	yes
queue_size	16384

Disk quota

enabled	yes
limit	1048576

File size

enabled	yes
limit	51200

Synchronization

enabled	yes
queue_size	16384
interval	300
max_eps	10
response_timeout	30
max_interval	3600
thread_pool	1

File limit

enabled	yes
entries	100000

Copyright © 2023 Wazuh, Inc.

Monitored directories

RT: Real time | WD: Who-data | Per.: Permission | MT: Modification time | SL: Symbolic link | RL: Recursion level

-	RT	WD	Changes	MD5	SHA1	Per.	Size	Owner	Group	MT	Inode	SHA256	SL	RL
/bin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/boot	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/etc	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/sbin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/usr/bin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256
/usr/sbin	no	no	no	yes	yes	yes	yes	yes	yes	yes	yes	yes	no	256

Copyright © 2023 Wazuh, Inc.