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

Group default configuration

Configurations

name: agent_name

Local files

Location	Log_format
/var/log/my.log	syslog

Osquery

Osquery integration enabled	no
Auto-run the Osquery daemon	yes
bin_path	/usr/bin
Path to the Osquery results log file	/var/log/osquery/osqueryd.results.log
Path to the Osquery configuration file	/etc/osquery/osquery.conf
Use defined labels as decorators	no

Packs

Name	Item
custom_pack	/path/to/custom_pack.conf

Command

Command enabled	no
Command name	test
Command to execute	/bin/bash /root/script.sh
Interval between executions	1d
Ignore command output	no
Run on start	yes
timeout	0
Verify MD5 sum	5aada3704685dad6fd27beb58e6687de
Verify SHA1 sum	da39a3ee5e6b4b0d3255bfef95601890afd80709
Verify SHA256 sum	292a188e498caea5c5fbfb0beca413c980e7a5edf40d47cf70e1dbc33e4f395e

Syscheck

Ignored files and directories	/etc/random-seed /root/dir {"type":"sregex","item":".log$|.tmp"}

OpenSCAP

OpenSCAP integration enabled	no
Timeout (in seconds) for scan executions	1800
Interval between scan executions	1d
Scan on start	yes

Evaluations

Path	Type	Profiles
ssg-centos-7-ds.xml	xccdf	xccdf_org.ssgproject.content_profile_pci-dss xccdf_org.ssgproject.content_profile_common

CIS-CAT

CIS-CAT integration enabled	no
Timeout (in seconds) for scan executions	1800
Interval between scan executions	1d
Scan on start	yes
Path to Java executable directory	/usr/lib/jvm/java-1.8.0-openjdk-amd64/jre/bin
Path to CIS-CAT executable directory	wodles/ciscat

Evaluations

Path	Type	Profile
benchmarks/CIS_Ubuntu_Linux_16.04_LTS_Benchmark_v4.0.0-xccdf.xml	xccdf	xccdf_org.cisecurity.benchmarks_profile_Level_3_-_Server

Syscollector

Syscollector integration enabled	no
Interval between system scans	1h
scan_on_start	yes
Scan hardware info	yes
Scan operating system info	yes
Scan network interfaces	yes
Scan installed packages	yes
Scan current processes	yes

Scan listening netwotk ports

all	no
item	yes

Labels

Value	Key	Hidden
i-052a1838c	aws.instance-id	

Value	Key	Hidden
sg-1103	aws.sec-group	
172.17.0.0	network.ip	
02:42:ac:11:00:02	network.mac	
January 1st, 2017	installation	yes

Rootcheck

Rootkit files database path	/var/ossec/etc/shared/rootkit_files.txt
Rootkit trojans database path	/var/ossec/etc/shared/rootkit_trojans.txt

Security configuration assessment

Security configuration assessment enabled	no
Scan on start	yes
Interval	12h
Skip scan on CIFS/NFS mounts	yes
Policies	system_audit_rcl.yml system_audit_ssh.yml system_audit_pw.yml

profile: jeje

Local files

Location	Log_format
/var/log/linux.log	syslog

profile: database

Local files

Location	Log_format
/var/log/database.log	syslog

Agents in group

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
001	agent	10.0.2.15	Wazuh v3.9.1	master	CentOS Linux 7.5	2019-06-04 08:38:35	2019-06-07 13:00:04
002	agent2	any	-	-	-	2019-06-07 12:57:55	-
003	agent3	any	-	-	-	2019-06-07 12:57:55	-
004	agent4	any	-	-	-	2019-06-07 12:57:55	-
005	agent5	any	-	-	-	2019-06-07 12:57:55	-
006	agent6	any	-	-	-	2019-06-07 12:57:55	-

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
007	agent7	any	-	-	-	2019-06-07 12:57:55	-
008	agent8	any	-	-	-	2019-06-07 12:57:55	-
009	agent9	any	-	-	-	2019-06-07 12:57:55	-
010	agent10	any	-	-	-	2019-06-07 12:57:55	-
011	agent11	any	-	-	-	2019-06-07 12:57:55	-
012	agent12	any	-	-	-	2019-06-07 12:57:55	-
013	agent13	any	-	-	-	2019-06-07 12:57:55	-
014	agent14	any	-	-	-	2019-06-07 12:57:55	-
015	agent15	any	-	-	-	2019-06-07 12:57:55	-
016	agent16	any	-	-	-	2019-06-07 12:57:55	-
017	agent17	any	-	-	-	2019-06-07 12:57:55	-
018	agent18	any	-	-	-	2019-06-07 12:57:55	-
019	agent19	any	-	-	-	2019-06-07 12:57:55	-
020	agent20	any	-	-	-	2019-06-07 12:57:55	-
021	agent21	any	-	-	-	2019-06-07 12:57:55	-
022	agent22	any	-	-	-	2019-06-07 12:57:55	-
023	agent23	any	-	-	-	2019-06-07 12:57:55	-
024	agent24	any	-	-	-	2019-06-07 12:57:55	-
025	agent25	any	-	-	-	2019-06-07 12:57:55	-
026	agent26	any	-	-	-	2019-06-07 12:57:55	-
027	agent27	any	-	-	-	2019-06-07 12:57:55	-
028	agent28	any	-	-	-	2019-06-07 12:57:55	-
029	agent29	any	-	-	-	2019-06-07 12:57:55	-
030	agent30	any	-	-	-	2019-06-07 12:57:55	-
031	agent31	any	-	-	-	2019-06-07 12:57:55	-
032	agent32	any	-	-	-	2019-06-07 12:57:55	-
033	agent33	any	-	-	-	2019-06-07 12:57:55	-
034	agent34	any	-	-	-	2019-06-07 12:57:55	-
035	agent35	any	-	-	-	2019-06-07 12:57:55	-
036	agent36	any	-	-	-	2019-06-07 12:57:55	-
037	agent37	any	-	-	-	2019-06-07 12:57:55	-
038	agent38	any	-	-	-	2019-06-07 12:57:55	-
039	agent39	any	-	-	-	2019-06-07 12:57:55	-
040	agent40	any	-	-	-	2019-06-07 12:57:55	-
041	agent41	any	-	-	-	2019-06-07 12:57:55	-
042	agent42	any	-	-	-	2019-06-07 12:57:55	-
043	agent43	any	-	-	-	2019-06-07 12:57:55	-
044	agent44	any	-	-	-	2019-06-07 12:57:55	-
045	agent45	any	-	-	-	2019-06-07 12:57:55	-
046	agent46	any	-	-	-	2019-06-07 12:57:55	-
047	agent47	any	-	-	-	2019-06-07 12:57:55	-

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
048	agent48	any	-	-	-	2019-06-07 12:57:55	-
049	agent49	any	-	-	-	2019-06-07 12:57:55	-
050	agent50	any	-	-	-	2019-06-07 12:57:55	-
051	agent51	any	-	-	-	2019-06-07 12:57:55	-
052	agent52	any	-	-	-	2019-06-07 12:57:55	-
053	agent53	any	-	-	-	2019-06-07 12:57:55	-
054	agent54	any	-	-	-	2019-06-07 12:57:55	-
055	agent55	any	-	-	-	2019-06-07 12:57:55	-
056	agent56	any	-	-	-	2019-06-07 12:57:55	-
057	agent57	any	-	-	-	2019-06-07 12:57:55	-
058	agent58	any	-	-	-	2019-06-07 12:57:55	-
059	agent59	any	-	-	-	2019-06-07 12:57:55	-
060	agent60	any	-	-	-	2019-06-07 12:57:55	-
061	agent61	any	-	-	-	2019-06-07 12:57:55	-
062	agent62	any	-	-	-	2019-06-07 12:57:55	-
063	agent63	any	-	-	-	2019-06-07 12:57:55	-
064	agent64	any	-	-	-	2019-06-07 12:57:55	-
065	agent65	any	-	-	-	2019-06-07 12:57:55	-
066	agent66	any	-	-	-	2019-06-07 12:57:55	-
067	agent67	any	-	-	-	2019-06-07 12:57:55	-
068	agent68	any	-	-	-	2019-06-07 12:57:55	-
069	agent69	any	-	-	-	2019-06-07 12:57:55	-
070	agent70	any	-	-	-	2019-06-07 12:57:55	-
071	agent71	any	-	-	-	2019-06-07 12:57:55	-
072	agent72	any	-	-	-	2019-06-07 12:57:55	-
073	agent73	any	-	-	-	2019-06-07 12:57:55	-
074	agent74	any	-	-	-	2019-06-07 12:57:55	-
075	agent75	any	-	-	-	2019-06-07 12:57:55	-
076	agent76	any	-	-	-	2019-06-07 12:57:55	-
077	agent77	any	-	-	-	2019-06-07 12:57:55	-
078	agent78	any	-	-	-	2019-06-07 12:57:55	-
079	agent79	any	-	-	-	2019-06-07 12:57:55	-
080	agent80	any	-	-	-	2019-06-07 12:57:55	-
081	agent81	any	-	-	-	2019-06-07 12:57:56	-
082	agent82	any	-	-	-	2019-06-07 12:57:56	-
083	agent83	any	-	-	-	2019-06-07 12:57:56	-
084	agent84	any	-	-	-	2019-06-07 12:57:56	-
085	agent85	any	-	-	-	2019-06-07 12:57:56	-
086	agent86	any	-	-	-	2019-06-07 12:57:56	-
087	agent87	any	-	-	-	2019-06-07 12:57:56	-
088	agent88	any	-	-	-	2019-06-07 12:57:56	-

ID	Name	IP	Version	Manager	OS	Registration date	Last keep alive
089	agent89	any	-	-	-	2019-06-07 12:57:56	-
090	agent90	any	-	-	-	2019-06-07 12:57:56	-
091	agent91	any	-	-	-	2019-06-07 12:57:56	-
092	agent92	any	-	-	-	2019-06-07 12:57:56	-
093	agent93	any	-	-	-	2019-06-07 12:57:56	-
094	agent94	any	-	-	-	2019-06-07 12:57:56	-
095	agent95	any	-	-	-	2019-06-07 12:57:56	-
096	agent96	any	-	-	-	2019-06-07 12:57:56	-
097	agent97	any	-	-	-	2019-06-07 12:57:56	-
098	agent98	any	-	-	-	2019-06-07 12:57:56	-
099	agent99	any	-	-	-	2019-06-07 12:57:56	-
100	agent100	any	-	-	-	2019-06-07 12:57:56	-