Cloud Agent SUDO Commands

May 2018

Overview

The Qualys Cloud Agent offers multiple deployment methods for Linux, Mac, and AIX operating systems to support an organization's security policy for running third-party applications and least privilege configuration.

The Cloud Agent Installation Guides document how the Cloud Agent can be deployed running as root, a sudo user, or privileged user.

This Tech Note describes the current commands executed by the Cloud Agent for deployments that utilize sudo users for configuration of the sudoers file.

Note: Qualys recommends that Cloud Agent is deployed running as root, as required by other security agents, to achieve the highest fidelity assessments with least management overhead.

Use of Commands

The Cloud Agent uses multiple methods to collect metadata to provide asset inventory, vulnerability management, and policy compliance use cases. Some of these methods include running commands to collect list of installed applications and versions, running processes, network interfaces, and so on.

The list of commands is generally static but may change as new vulnerabilities require additional metadata to be collected using other commands. One example is the recent Meltdown/Spectre vulnerabilities that require specific new commands provided by operating system vendors to collect processor and BIOS information.

List of Commands

The following are the commands utilized by the Cloud Agent as of May 2018.

$ORACLE_HOME/bin/lsnrctl	/apps/tomcat/bin/version.sh
/opt/apache-tomcat-7.0.22/bin/version.sh	/opt/asrmanager/bin/asr
/opt/bmc/bladelogic/RSCD/sbin/version	/opt/cdunix/etc/cdver
/opt/cisco/anyconnect/bin/vpn	/opt/cisco/vpn/bin/vpn

© 2018 Qualys, Inc. Under NDA Only. Distribution for Qualys Customers, Prospects, and Partners Only.

/opt/CiscoTrustAgent/sbin/ctastat	/opt/clamav/bin/clamav-config
/opt/glassfishv3/bin/asadmin	/opt/hp/hpsmh/sbin/hpsmhd
/opt/ibm/BPM/v8.0/bin/versionInfo.sh	/opt/ibm/BPM/v8.5/bin/versionInfo.sh
/opt/ibm/BPM/v8.6/bin/versionInfo.sh	/opt/IBM/HTTPServer/bin/apachectl
/opt/IBM/HTTPServer/bin/httpd	/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh
/opt/logstash/bin/logstash	/opt/logstash/bin/logstash-plugin
/opt/mongodb/bin/mongo	/opt/mqipt/bin/mqiptVersion
/opt/mqm/bin/dspmqver	/opt/nwreg2/local/usrbin/nrcmd
/opt/omni/bin/omnicc	/opt/puppet/sbin/puppetd
/opt/qradar/bin/myver	/opt/rsa/am/utils/rsautil
/opt/splunk/bin/splunk	/opt/ssw/oracle/x64/wls_12.2.1.2.0/OPatch/opatch
/opt/sun/webserver/bin/https/bin/webservd	/opt/sun/webserver7/admin-server/bin/startserv
/opt/SUNWappserver/bin/asadmin	/opt/SUNWwbsvr/bin/https/bin/webservd
/opt/SUNWwbsvr/https-admserv/start	/opt/SUNWwbsvr7/admin-server/bin/startserv
/opt/TimesTen/tt70/bin/ttversion	/opt/zimbra/bin/zmcontrol
/shared/weblogic/WLSbin/WLS1213/A_WebLogic/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/B_WebLogic/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/G1_WebLogic/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/G2_WebLogic/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/G3_WebLogic/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/G4_WebLogic/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_AdmConsole/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R1_CCP/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_CCT/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R1_Corp/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_FB1/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R1_FB2/Oracle_Home/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_IVR/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R1_RCS/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_TP/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R1_UMS/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R1_WebLogic/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R2_IVR/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R2_WebLogic/Oracle_Home/OPatch/opatch	/shared/weblogic/WLSbin/WLS1213/R3_WebLogic/Oracle_Home/OPatch/opatch
/shared/weblogic/WLSbin/WLS1213/R4_WebLogic/Oracle_Home/OPatch/opatch	/sun/webserver/bin/https/bin/webservd
/sun/webserver7/admin-server/bin/startserv	/sun/webserver7/bin/wadm
/System/Library/Frameworks/JavaVM.framework/Versions/1.3.1/Commands/java	/System/Library/Frameworks/JavaVM.framework/Versions/1.4.2/Commands/java
/usr/iplanet/servers/https-admserv/start	/usr/local/avamar/bin/mccli
/usr/local/BerkeleyDB.5.1/bin/db_stat	/usr/local/BerkeleyDB.5.2/bin/db_stat
/usr/local/BerkeleyDB.5.3/bin/db_stat	/usr/local/BerkeleyDB.6.0/bin/db_stat
/usr/local/BerkeleyDB/bin/db_stat	/usr/local/bin/db2ls
/usr/local/bin/gpgsm	/usr/local/bin/libmikmod-config
/usr/local/bin/opera	/usr/local/git/bin/git
/usr/local/middleware/domains/AMM/opatch	/usr/local/middleware/domains/CIIM_12300/opatch
/usr/local/middleware/domains/goot6100/opatch	/usr/local/middleware/domains/StoreBudget/opatch
/usr/local/middleware/domains/tpms/opatch	/usr/local/middleware/domains/Tririga10100/opatch

© 2018 Qualys, Inc. Under NDA Only. Distribution for Qualys Customers, Prospects, and Partners Only.

/usr/local/middleware/domains/wfm_online/opatch	/usr/local/middleware/domains/XID/opatch
/usr/local/middleware/user_projects/spo12700/opatch	/usr/local/middleware/wlserver/opatch
/usr/local/nagios/bin/nagios	/usr/local/seamonkey/seamonkey
/usr/local/squid/sbin/squid	/usr/local/subversion/bin/svn
/usr/mqm/bin/dspmqver	/usr/openv/netbackup/bin/bpps
/usr/ucb/ps	acroread
activemq	aex-diagnostics
apk	aria2c
arp	asterisk
avahi-dnsconfd	awk
bogofilter	cabextract
canonical-livepatch	cat
clamav-config	clamscan
cli	convert
cpio	cups-config
curl	cut
cvs	defaults
defaults	df
diskutil	dmidecode
dnsmasq	docker
dovecot	dpkg
dropbear	dropbox
dscl	dspmqcsv;dspmqver
dspmqver	dspmqver
echo	egrep
emgr	env
env	esxupdate
evolution	fetchmail
ffmpeg	find
firefox	firefox
for	free
freebsd-version	freeciv-server
freetype-config	gconftool-2
gem	getdb
ghostscript	gimp
git	gitlab-rake
gnome-panel	gpg
grep	grep
gs	gzip
hadoop	hadoop
HDB	head
httpd	id
ifconfig	ifconfig
imageinfo	ip
ipcs	isainfo
istat	java

© 2018 Qualys, Inc. Under NDA Only. Distribution for Qualys Customers, Prospects, and Partners Only.

jerry	kextstat
kibana	konqueror
ldd	lftp
libpng-config	libreoffice4.3
lighttpd	locate
lookupd	ls
ls	lsattr
lsb_release	lscfg
lslpp	lsmcode
lsmod	lsnrctl
magick	mdls
memcached	mesos-master
mesos-slave	mmm_agentd
modprobe	mount|grep
msfconsole	nagios
named	nano
ndd	netstat
nfsstat	nidump
nmap	node
nodetool	npm
nrpe	ntpd
ntpdc	ntpq
ofxdump	openssl
openvpn	opera
oslevel	ovdeploy
pdns_recursor	perl
pgrep	php
pip	pip3
pkginfo	powershell
ps	psql
psrinfo	puppet
python	r2
radiusd	rails
redis-cli	route
rpcinfo	rpm
rsct/bin/samversion	rssh
rsync	ruby
runuser	rvd
seamonkey	service
sh	sho
show	showmount
showrev	smbclient
smbios	smbstatus
smcwebserver	sneep
snmpget	snort
socat	spamass-milter
spark-shell	spctl
squid	ssh

© 2018 Qualys, Inc. Under NDA Only. Distribution for Qualys Customers, Prospects, and Partners Only.

ssh-server-config-tool	stat
stclient	strings
sudo	supervisord
svcs	svn
svn	sw_vers
sw_vers	sysctl
sysinfo	system_profiler
system_profiler	tar
tcpdump	test
tethereal	tftp
thunderbird	thunderbird
tiffinfo	tmsh
transmission-remote	ttversion
uname	uniq
unzip	uptrack-uname
uustat	vlc
vm_stat	vmstat
vmware	vmware-installer
vmware-toolbox-cmd	vmware-view
weborf	weechat-curses
wget	what
which	wireshark
xcomd	xe
xentop	xl
xmms	ziproxy
zoneadm	

© 2018 Qualys, Inc. Under NDA Only. Distribution for Qualys Customers, Prospects, and Partners Only.