TP ICAP

Qualys Cloud Agent

Linux Server Deployment Guide

Version 0.5  
TP ICAP Classification: Internal

Document History

|  |  |  |
| --- | --- | --- |
| Version | Description | Author |
| 0.1 | Qualys Cloud Agent Linux Server Deployment Guide | Christopher Atienza |
| 0.2 | Qualys Cloud Agent Linux Server Deployment Guide Satellite Ansible Role | Christopher Atienza |
| 0.3 | Manual Installation and customized created scripts | Christopher Atienza |
| 0.4 | Modified based on 2.6 Qualys Cloud Agent Deployment | Christopher Atienza |
| 0.5 |  |  |

Document Review

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Name | Job title | Date reviewed |
| 0.1 |  |  |  |
| 0.2 |  |  |  |
| 0.3 |  |  |  |
| 0.4 |  |  |  |
| 0.5 |  |  |  |

Document Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Name | Job title | Date approved |
|  |  |  |  |

Related Documents

|  |  |
| --- | --- |
| Name | Location |
| Qualys Cloud Agent Linux Server Deployment Guide | Stored on Teams |

Location:

Content

[Document Authorization 4](#_Toc43409567)

[About This Document 4](#_Toc43409568)

[Before You Begin 4](#_Toc43409569)

[1. Introduction 5](#_Toc43409570)

[2. RPM Package Content 5](#_Toc43409571)

[3. Privileges and access 8](#_Toc43409572)

[4. Qualys Cloud Gateways 8](#_Toc43409573)

[4.1 List of Qualys Cloud Gateways 8](#_Toc43409574)

[4.2 Proxy configuration 9](#_Toc43409575)

[4.3 Qualys Gateway load distribution 9](#_Toc43409576)

[4.4 Sample Distribution of Qualys gateways per Subnet. 10](#_Toc43409577)

[4.5 Qualys Cloud Agent Certificate Configuration 10](#_Toc43409578)

[5. Qualys Cloud Agent ActivationID and CustomerID 12](#_Toc43409579)

[6. Method 1: Linux Qualys Cloud Agent deployment - Manual 12](#_Toc43409580)

[6.1 Running the **agentinstall.sh** script 14](#_Toc43409581)

[7. Method 2: Linux Qualys Cloud Agent deployment –Automation (Ansible) 15](#_Toc43409582)

[7.1 How does it work and what does the Ansible Role do in Qualys Agent Deployment? 17](#_Toc43409583)

[8. Qualys Cloud Agent Logs 19](#_Toc43409584)

[8.1 /etc/qualys/cloud-agent/qagent-log.conf file content 19](#_Toc43409585)

[9. Qualys Cloud Agent Main Configuration file 20](#_Toc43409586)

[9.1 APAC: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content 20](#_Toc43409587)

[9.2 AMER: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content 20](#_Toc43409588)

[9.3 EMEA: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content 21](#_Toc43409589)

[10. Qualys Cloud Agent connectivity verification 22](#_Toc43409590)

[11. Start and Stopping the Qualys Cloud Agent services, 22](#_Toc43409591)

[11.1 To stop the Qualys Cloud Agent Service 22](#_Toc43409592)

[11.2 To start the Qualys Cloud Agent Service 23](#_Toc43409593)

## Document Authorization

This document is developed with the proprietary information of TP ICAP and owned by TP ICAP. No part of this document may be reproduced, stored, copied, or transmitted in any form or by means of electronic, mechanical, photocopying or otherwise, without the express consent of TP ICAP or TP ICAP. This document is intended for internal use within TP ICAP only and not meant for external distribution. This document is confidential and intended for the following target audience which includes, but not limited to: TP ICAP Cyber Security team, Linux Platform team assigned to execute Qualys cloud agents installation and configuration.

## About This Document

This document intended for Linux/Unix Admin who manage TPICA Linux/Unix server environment deploying Qualys Cloud Agent.

## Before You Begin

It is important to understand the **Qualys Cloud agent** which is a lightweight scanner that enables 2-second global visibility. Cloud Agents collect data from across your entire infrastructure, and consolidate it in the Qualys Cloud Platform for you to view. The Cloud Agent can be installed on any host, such as a laptop, desktop, server, or virtual machine—on premises, mobile, or in the cloud. It can be easily deployed via a compact, silent, lightweight installer; via common software management automation; or via the command line. As system changes occur, Cloud Agents push updates to the central Cloud Platform, rather than the central system polling agents for updates.

The agent is designed to have minimal impact on the system and the network. It normally consumes <1% of CPU resources, peaking at 5% during normal operation. It’s self-updating and self-healing, keeping itself up to date with no need to reboot.

Qualys Cloud Agents bring additional, continuous monitoring capabilities to our Vulnerability Management tools. This eliminates the need for establishing scanning windows or integrations with credential vaults for systems, as well as the need to actually know where a particular asset resides

**Qualys Cloud Agent Gateway (CAG**) Service is a cluster of virtual appliances managed from the Qualys Cloud Platform to securely connect agents deployed anywhere. The objective is to securely send Cloud Agent traffic to a CAG virtual appliance located within restricted or sensitive on-premises networks, which can further send the vulnerability, host data to the Qualys cloud portal. The CAG enables to:

* Secure connectivity of Cloud Agents on assets to the Qualys Cloud Platform without need to open access for each asset to the platform.
* Optimize the bandwidth utilized by large Cloud Agent deployments.

The CAG needs to be configured as a proxy in every agent being deployed based on the region of the asset on which the agent is getting deployed.

## Introduction

The Cloud Agent provides a continuous view of assets for vulnerability management, policy compliance, and asset inventory without the need for credential management, scan windows, and firewall changes required by network scanner deployments. The Cloud Agent delivers visibility and security solutions for assets that are not able or not easily scanned from the network including remote/roaming users, distributed offices, and cloud server instances.

This document contains the test cases executed for Linux Qualys Cloud agent on three non-production servers selected on sample basis. Detailed logs and snapshots have been captured on real-time basis for the duration of the test window.

The Cloud Agent Platform is designed for the agent and platform to work in concert to provide a high level of accuracy and fidelity, low end-to-end processing times, and minimal resource impact on the asset.

The agent is designed to capture the metadata of the operating system, installed applications, and system configurations as needed by the different activated service modules, and upload the metadata to the platform for analysis, correlation, reporting, and alerting. The agent does not perform local processing or analysis; it only performs metadata collection which keeps resource usage extremely low with 5 MB RAM, 0.01% CPU at idle, and peak usage and network bandwidth tuneable using comprehensive configuration performance parameters. The overall range of performance parameters captured during testing was 0.0% - 0.3% CPU and memory was 0.1% to 8% (*This 8% was exceptional case and the reason for it has been explained in the Conclusion*). Normal load on memory was varying from 0.1% to 0.3%.

The Cloud Agent supports Vulnerability Management QIDs and Policy Compliance CIDs similar to the authenticated local checks performed by the network scanner, with some current limitations. The Cloud Agent is the preferred method for assets like dynamic IP client machines, remote/roaming users, static and ephemeral cloud instances, and systems sensitive to external scanning where it’s not possible or practical to do network scanning. All communications are initiated by the agent outbound from the agent to the platform through Qualys Gateways configured in each region.

## RPM Package Content

Qualys Cloud Agent package can be download at TPICAP central file repository.

Package installer URL:   
 <http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/qualys-cloud-agent.x86_64.rpm>

The package version were qualys-cloud-agent-2.6.0-88 with multi proxy support.

**File/Directory Content:** qualys-cloud-agent.x86\_64.rpm

/etc/init.d/qualys-cloud-agent

/etc/qualys/cloud-agent

/etc/qualys/cloud-agent/.centos/etc/qualys/cloud-agent/.centos/qualys-cloud-agent

/etc/qualys/cloud-agent/.centos/qualys-cloud-agent-restart

/etc/qualys/cloud-agent/.suse

/etc/qualys/cloud-agent/.suse/qualys-cloud-agent

/etc/qualys/cloud-agent/.systemd

/etc/qualys/cloud-agent/.systemd/deb

/etc/qualys/cloud-agent/.systemd/qualys-cloud-agent-uninstall.service

/etc/qualys/cloud-agent/.systemd/qualys-cloud-agent.service

/etc/qualys/cloud-agent/cert

/etc/qualys/cloud-agent/cloud-agent\_pub.cert

/etc/qualys/cloud-agent/fim-plugin-supportedtypes\_list.cfg

/etc/qualys/cloud-agent/fim-plugin.cfg

/etc/qualys/cloud-agent/fim-plugin.conf

/etc/qualys/cloud-agent/qagent-fim-log.conf

/etc/qualys/cloud-agent/qagent-log.conf

/etc/qualys/cloud-agent/qagent-udc-log.conf

/etc/qualys/cloud-agent/qagent.config

/etc/qualys/cloud-agent/qualys-cloud-agent.conf

/usr/local/qualys/cloud-agent

/usr/local/qualys/cloud-agent/Config.db

/usr/local/qualys/cloud-agent/Default\_Config.db

/usr/local/qualys/cloud-agent/bin

/usr/local/qualys/cloud-agent/bin/check\_fimc\_in\_auditd.sh

/usr/local/qualys/cloud-agent/bin/cloudagentctl.sh

/usr/local/qualys/cloud-agent/bin/fim-audisp-policy.te

/usr/local/qualys/cloud-agent/bin/fim-auditd-policy.te

/usr/local/qualys/cloud-agent/bin/fim-plugin

/usr/local/qualys/cloud-agent/bin/fim-plugin-install.sh

/usr/local/qualys/cloud-agent/bin/fim-plugin-uninstall.sh

/usr/local/qualys/cloud-agent/bin/fimc

/usr/local/qualys/cloud-agent/bin/qagent\_hostid.sh

/usr/local/qualys/cloud-agent/bin/qagent\_restart.sh

/usr/local/qualys/cloud-agent/bin/qagent\_uninstall.sh

/usr/local/qualys/cloud-agent/bin/qualys-cloud-agent

/usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh

/usr/local/qualys/cloud-agent/bin/qualys-udc-scan

/usr/local/qualys/cloud-agent/bin/string-util

/usr/local/qualys/cloud-agent/lib

/usr/local/qualys/cloud-agent/lib/libPocoCrypto.so

/usr/local/qualys/cloud-agent/lib/libPocoCrypto.so.64

/usr/local/qualys/cloud-agent/lib/libPocoFoundation.so

/usr/local/qualys/cloud-agent/lib/libPocoFoundation.so.64

/usr/local/qualys/cloud-agent/lib/libPocoJSON.so

/usr/local/qualys/cloud-agent/lib/libPocoJSON.so.64

/usr/local/qualys/cloud-agent/lib/libPocoUtil.so

/usr/local/qualys/cloud-agent/lib/libPocoUtil.so.64

/usr/local/qualys/cloud-agent/lib/libPocoXML.so

/usr/local/qualys/cloud-agent/lib/libPocoXML.so.64

/usr/local/qualys/cloud-agent/lib/libaudit.so

/usr/local/qualys/cloud-agent/lib/libaudit.so.0

/usr/local/qualys/cloud-agent/lib/libaudit.so.1

/usr/local/qualys/cloud-agent/lib/libaudit.so.1.0.0

/usr/local/qualys/cloud-agent/lib/libcrypto.so

/usr/local/qualys/cloud-agent/lib/libcrypto.so.1.1

/usr/local/qualys/cloud-agent/lib/libcurl.so

/usr/local/qualys/cloud-agent/lib/libcurl.so.4

/usr/local/qualys/cloud-agent/lib/libcurl.so.4.6.0

/usr/local/qualys/cloud-agent/lib/libev.so

/usr/local/qualys/cloud-agent/lib/libev.so.4

/usr/local/qualys/cloud-agent/lib/libev.so.4.0.0

/usr/local/qualys/cloud-agent/lib/libfim.so

/usr/local/qualys/cloud-agent/lib/libfimctl.so

/usr/local/qualys/cloud-agent/lib/libgcc\_s.so.1

/usr/local/qualys/cloud-agent/lib/liblzma.so

/usr/local/qualys/cloud-agent/lib/liblzma.so.5

/usr/local/qualys/cloud-agent/lib/liblzma.so.5.2.2

/usr/local/qualys/cloud-agent/lib/libpcre2-16.so.0

/usr/local/qualys/cloud-agent/lib/libpcre2-16.so.0.1.0

/usr/local/qualys/cloud-agent/lib/libpcre2-32.so.0

/usr/local/qualys/cloud-agent/lib/libpcre2-32.so.0.1.0

/usr/local/qualys/cloud-agent/lib/libpcre2-8.so.0

/usr/local/qualys/cloud-agent/lib/libpcre2-8.so.0.1.0

/usr/local/qualys/cloud-agent/lib/libpcre2-posix.so.0

/usr/local/qualys/cloud-agent/lib/libpcre2-posix.so.0.0.0

/usr/local/qualys/cloud-agent/lib/libqualys-cloud-agent.so

/usr/local/qualys/cloud-agent/lib/libsqlite3.so

/usr/local/qualys/cloud-agent/lib/libsqlite3.so.0

/usr/local/qualys/cloud-agent/lib/libsqlite3.so.0.8.6

/usr/local/qualys/cloud-agent/lib/libssl.so

/usr/local/qualys/cloud-agent/lib/libssl.so.1.1

/usr/local/qualys/cloud-agent/lib/libstdc++.so.6

/usr/local/qualys/cloud-agent/lib/libstdc++.so.6.0.19

/usr/share/doc/qualys-cloud-agent-2.6.0-88

/usr/share/doc/qualys-cloud-agent-2.6.0-88/COPYING.curl

/usr/share/doc/qualys-cloud-agent-2.6.0-88/COPYING.libproxy

/usr/share/doc/qualys-cloud-agent-2.6.0-88/COPYING.pcre2

/usr/share/doc/qualys-cloud-agent-2.6.0-88/COPYING.xz

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENCE.pcre2

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.jansson

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.libaudit

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.libev

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.lua.html

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.openssl

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.poco

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.rapidjson

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.sqlite

/usr/share/doc/qualys-cloud-agent-2.6.0-88/LICENSE.tinyxml

/usr/share/doc/qualys-cloud-agent-2.6.0-88/README

/var/spool/qualys

## Privileges and access

In TPICAP Qualys cloud agent deployment, as required by the Security team the qualys cloud agent service will be running as non-root account with Sudo root delegation.

In this case the following service account were created and used as default user account.

Service account details:

Username: svcqca UID: 2708

Groupname: svcqca GID: 2708

Sudoers entries:

The following entries must be added in order to run as non-root service account

For RHEL 7.3 and below, under /etc/sudoers

For 7.4 and above, under /etc/sudoers/sudoers\_qualys

Entries required:

%svcqca ALL=(ALL) NOPASSWD: ALL

Sudoer test verification:   
 As svcqca login, run “sudo -l”, output must be similar below.

User svcqca may run the following commands on this host:

**(ALL) NOPASSWD: ALL**

## Qualys Cloud Gateways

### List of Qualys Cloud Gateways

|  |  |  |  |
| --- | --- | --- | --- |
| **EMEA** | **FQDN** | **IP Address** | **Region** |
| ldn1lx0132 | ldn1lx0132.corp.ad.tullib.com | 10.90.73.22 | EMEA |
| ldn1lx0130 | ldn1lx0130.corp.ad.tullib.com | 10.90.144.14 | EMEA |
| ldn1lx0129 | ldn1lx0129.corp.ad.tullib.com | 10.90.144.13 | EMEA |
| ldn1lx0128 | ldn1lx0128.corp.ad.tullib.com | 10.90.168.9 | EMEA |
| ldn1lx0127 | ldn1lx0127.corp.ad.tullib.com | 10.90.168.8 | EMEA |
| ldn1lx0126 | ldn1lx0126.corp.ad.tullib.com | 10.90.72.60 | EMEA |
| ldn2lx0125 | ldn2lx0125.corp.ad.tullib.com | 10.91.72.53 | EMEA |
| ldn2lx0126 | ldn2lx0126.corp.ad.tullib.com | 10.91.72.60 | EMEA |
| ldn2lx0127 | ldn2lx0127.corp.ad.tullib.com | 10.91.168.8 | EMEA |
| ldn2lx0128 | ldn2lx0128.corp.ad.tullib.com | 10.91.168.9 | EMEA |
| ldn2lx0129 | ldn2lx0129.corp.ad.tullib.com | 10.91.144.23 | EMEA |
| ldn2lx0130 | ldn2lx0130.corp.ad.tullib.com | 10.91.144.14 | EMEA |
| njc1lx0001 | njc1lx0001.corp.ad.tullib.com | 10.144.32.102 | AMER |
| njc2lx0002 | njc2lx0002.corp.ad.tullib.com | 10.1.237.59 | AMER |
| sng1lx0012 | sng1lx0012.corp.ad.tullib.com | 10.203.32.159 | APAC |
| sng2lx0012 | sng2lx0012.corp.ad.tullib.com | 10.200.48.56 | APAC |

### Proxy configuration

In Qualys Cloud deployment in Linux/Windows or Desktop environments, the maximum gateways can be configured will be up to five per agent, refer to Section 4.1 for List of allowed Qualys gateways.

The Cloud Agent will use the first proxy server in the list for its connection, if it fails to connect, the agent will use the next configured proxy server in the list until all proxy servers are attempted.

Each time the Cloud Agent connects to the Qualys Platform, it always uses the first proxy server in the ordered list.

. Here are the steps to enable the Linux agent to use a proxy for communication with our cloud platform:   
1) if /etc/sysconfig/**qualys-cloud-agent** file doesn't exist create it should be owned by: **svcqca:svcqca**  
2) add 1 of the following lines to the file (**1 line only**):   
  
The following example shows how to set multiple proxies:

https\_proxy=”https://**<FQDN1>**:8080;https://**<FQDN2>**:8080”

APAC

https\_proxy=”https://sng1lx0012.corp.ad.tullib.com:8080**;**https://sng2lx0012.corp.ad.tullib.com:8080”

AMER

https\_proxy=”https://njc1lx0001.corp.ad.tullib.com:8080**;**https://njc2lx0002.corp.ad.tullib.com:8080”

EMEA

https\_proxy=”https://ldn1lx0126.corp.ad.tullib.com:8080**;**https://ldn1lx0127.corp.ad.tullib.com:8080**;**https://ldn1lx0128.corp.ad.tullib.com:8080**;**https://ldn1lx0129.corp.ad.tullib.com:8080**;**https://ldn1lx0130.corp.ad.tullib.com:8080”

### Qualys Gateway load distribution

To distribute the load of each Qualys gateways per region, we set the primary gateway randomized and put it into master list file containing all the TPICAP subnets and its Qualys Gateways allocation. Due to long list of the file, we just provided a sample proxy settings allocated in a subnet. **Refer to Section 4.4**.

File location:

Automation Build Management Server: For new build server

ldnpinfuxm03:/etc/ansible/roles/common-tools-realm/files/**subnetgwdist**

File format:

subnet<space> <qualys gateway entries>

### Sample Distribution of Qualys gateways per Subnet.

10.74.40 https\_proxy="**https://ldn1lx0126**.corp.ad.tullib.com:8080;https://ldn1lx0129.corp.ad.tullib.com:8080;https://ldn1lx0130.corp.ad.tullib.com:8080;https://ldn1lx0132.corp.ad.tullib.com:8080;https://ldn1lx0126.corp.ad.tullib.com:8080"

10.46.2 https\_proxy="**https://ldn1lx0127**.corp.ad.tullib.com:8080;https://ldn1lx0128.corp.ad.tullib.com:8080;https://ldn1lx0129.corp.ad.tullib.com:8080;https://ldn1lx0130.corp.ad.tullib.com:8080;https://ldn1lx0132.corp.ad.tullib.com:8080"

10.72.40 https\_proxy="**https://ldn1lx0128**.corp.ad.tullib.com:8080;https://ldn1lx0129.corp.ad.tullib.com:8080;https://ldn1lx0130.corp.ad.tullib.com:8080;https://ldn1lx0132.corp.ad.tullib.com:8080;https://ldn1lx0126.corp.ad.tullib.com:8080"

10.44.53 https\_proxy="**https://ldn1lx0129**.corp.ad.tullib.com:8080;https://ldn1lx0130.corp.ad.tullib.com:8080;https://ldn1lx0132.corp.ad.tullib.com:8080;https://ldn1lx0126.corp.ad.tullib.com:8080;https://ldn1lx0127.corp.ad.tullib.com:8080"

10.44.61 https\_proxy="**https://ldn1lx0130**.corp.ad.tullib.com:8080;https://ldn1lx0126.corp.ad.tullib.com:8080;https://ldn1lx0127.corp.ad.tullib.com:8080;https://ldn1lx0128.corp.ad.tullib.com:8080;https://ldn1lx0129.corp.ad.tullib.com:8080"

10.44.171 https\_proxy="**https://ldn2lx0126**.corp.ad.tullib.com:8080;https://ldn2lx0127.corp.ad.tullib.com:8080;https://ldn2lx0128.corp.ad.tullib.com:8080;https://ldn2lx0129.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080"

10.1.237 https\_proxy="**https://ldn2lx0127**.corp.ad.tullib.com:8080;https://ldn2lx0128.corp.ad.tullib.com:8080;https://ldn2lx0128.corp.ad.tullib.com:8080;https://ldn2lx0129.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080"

10.101.40 https\_proxy="**https://ldn2lx0128**.corp.ad.tullib.com:8080;https://ldn2lx0129.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080;https://ldn2lx0125.corp.ad.tullib.com:8080;https://ldn2lx0126.corp.ad.tullib.com:8080"

10.46.136 https\_proxy="**https://ldn2lx0129**.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080;https://ldn2lx0125.corp.ad.tullib.com:8080;https://ldn2lx0126.corp.ad.tullib.com:8080;https://ldn2lx0127.corp.ad.tullib.com:8080"

10.46.130 https\_proxy="**https://ldn2lx0130**.corp.ad.tullib.com:8080;https://ldn2lx0126.corp.ad.tullib.com:8080;https://ldn2lx0127.corp.ad.tullib.com:8080;https://ldn2lx0128.corp.ad.tullib.com:8080;https://ldn2lx0129.corp.ad.tullib.com:8080"

10.80.32 https\_proxy="**https://ldn1lx0132**.corp.ad.tullib.com:8080;https://ldn1lx0126.corp.ad.tullib.com:8080;https://ldn1lx0127.corp.ad.tullib.com:8080;https://ldn1lx0128.corp.ad.tullib.com:8080;https://ldn1lx0129.corp.ad.tullib.com:8080"

10.200.32 https\_proxy="**https://sng1lx0012**.corp.ad.tullib.com:8080;https://sng2lx0012.corp.ad.tullib.com:8080"

10.202.39 https\_proxy="**https://sng2lx0012**.corp.ad.tullib.com:8080;https://sng1lx0012.corp.ad.tullib.com:8080"

10.1.10 https\_proxy="**https://njc1lx0001**.corp.ad.tullib.com:8080;https://njc2lx0001.corp.ad.tullib.com:8080"

10.10.52 https\_proxy="**https://njc2lx0001**.corp.ad.tullib.com:8080;https://njc1lx0001.corp.ad.tullib.com:8080"

### Qualys Cloud Agent Certificate Configuration

As default Qualys Cloud Agent were using port 1080, but in TPCIAP Qualys Cloud Agent deployment were using port 8080 as connectivity into Qualys Gateways which requires certificate to be downloaded and put it on the Qualys Cloud Agent configuration. To download the certificate use the following URL below.

|  |  |
| --- | --- |
| **Hostname of QGS** | **Nexus Path for respective Certificate (.pem) for each QGS** |
| njc1lx0001 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - njc1lx0001/njc1lx0001 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20njc1lx0001/njc1lx0001%20-%20Appliance-Certificate.pem) |
| njc2lx0001 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - njc2lx0001/njc2lx0001 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20njc2lx0001/njc2lx0001%20-%20Appliance-Certificate.pem) |
| sng1lx0012 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - sng1lx0012/sng1lx0012 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20sng1lx0012/sng1lx0012%20-%20Appliance-Certificate.pem) |
| sng2lx0012 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - sng2lx0012/sng2lx0012 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20sng2lx0012/sng2lx0012%20-%20Appliance-Certificate.pem) |
| ldn1lx0126 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0126/ldn1lx0126 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0126/ldn1lx0126%20-%20Appliance-Certificate.pem) |
| ldn1lx0127 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0127/ldn1lx0127 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0127/ldn1lx0127%20-%20Appliance-Certificate.pem) |
| ldn1lx0128 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0128/ldn1lx0128 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0128/ldn1lx0128%20-%20Appliance-Certificate.pem) |
| ldn1lx0129 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0129/ldn1lx0129 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0129/ldn1lx0129%20-%20Appliance-Certificate.pem) |
| ldn1lx0130 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0130/ldn1lx0130 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0130/ldn1lx0130%20-%20Appliance-Certificate.pem) |
| ldn2lx0125 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0125/ldn2lx0125 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0125/ldn2lx0125%20-%20Appliance-Certificate.pem) |
| ldn2lx0126 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0126/ldn2lx0126 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0126/ldn2lx0126%20-%20Appliance-Certificate.pem) |
| ldn2lx0127 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0127/ldn2lx0127 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0127/ldn2lx0127%20-%20Appliance-Certificate.pem) |
| ldn2lx0128 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0128/ldn2lx0128 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0128/ldn2lx0128%20-%20Appliance-Certificate.pem) |
| ldn2lx0129 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0129/ldn2lx0129 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0129/ldn2lx0129%20-%20Appliance-Certificate.pem) |
| ldn2lx0130 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn2lx0130/ldn2lx0130 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn2lx0130/ldn2lx0130%20-%20Appliance-Certificate.pem) |
| ldn1lx0132 | [http://nexus.tpicapcloud.com/repository/secure\_binaries/qualys/QGS - ldn1lx0132/ldn1lx0132 - Appliance-Certificate.pem](http://nexus.tpicapcloud.com/repository/secure_binaries/qualys/QGS%20-%20ldn1lx0132/ldn1lx0132%20-%20Appliance-Certificate.pem) |

All certificates has been put together into one file we called **“Appliance-Certificate.pem”** and put under ldnpinfuxm03:/etc/ansible/roles/common-tools-realm/files/Appliance-Certificate.pem and being populated to newly build Linux servers during installation process as well as existing Linux servers.

Fine below the configuration file, and the destination path under **/etc/qualys/cloud-agent/qagent.conf** that defined the certificate file of Qualys gateway and propagated to all Linux Servers.

Certificates location path: "**/etc/qualys/cloud-agent/cert/Appliance-Certificate.pem**"

Certificate declaration configuration file: **/etc/qualys/cloud-agent/qagent.conf**

#---bof---

{

"certs": [

{

"os": "Ubuntu",

"cafile": "/etc/ssl/certs/ca-certificates.crt"

},

{

"os": "Centos",

"cafile": "**/etc/qualys/cloud-agent/cert/Appliance-Certificate.pem**"

},

{

"os": "Suse",

"cafile": **"/etc/qualys/cloud-agent/cert/Appliance-Certificate.pem**"

},

{

"os": "OSX",

"cafile": ""

},

{

"os": "AIX",

"cafile": "/var/ssl/certs/ca-bundle.crt"

}

]

}

#---eof---

Sample log output that certificate were successfully configured on an agent.

Qualys Cloud Agent Log: **/var/log/qualys/qualys-cloud-agent.log**

…..  
2020-06-18 05:48:50.563 [qualys-cloud-agent][22011]:[Information]:[140583102097216]:Connection timeout: 60 seconds, Request timeout: 600 seconds

2020-06-18 05:48:50.563 [qualys-cloud-agent][22011]:[Information]:[140583102097216]:**Cert OS: Centos, CA path:/etc/qualys/cloud-agent/cert/Appliance-Certificate.pem**

2020-06-18 05:48:50.563 [qualys-cloud-agent][22011]:[Debug]:[140583102097216]:Webservice uri: https://qagpublic.qg1.apps.qualys.eu/CloudAgent/

2020-06-18 05:48:50.563 [qualys-cloud-agent][22011]:[Debug]:[140583102097216]:**Using Proxy: ldn2lx0129.corp.ad.tullib.com:8080**

2020-06-18 05:48:50.607 [qualys-cloud-agent][22011]:[Information]:[140583102097216]:Finished curl request

…..

## Qualys Cloud Agent ActivationID and CustomerID

In TPICAP Qualys Cloud Agent activationID keys for Linux were using only 3 and it defined per region only.

APAC:

ActivationId=c5c79f46-237a-430b-bfd9-96cbf7895d77

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

AMER:

ActivationId=4cbf2459-cb83-4d1a-8364-a4415508bd68

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

EMEA

ActivationId=0bfc6401-4fa2-4175-9cc2-fb8070f75e9a

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

ActivationID and CustomerID were being save under **/etc/qualys/cloud-agent/qualys-cloud-agent.conf** file.

## Method 1: Linux Qualys Cloud Agent deployment - Manual

The Qualys Cloud Agent manual deployment can be done using customized script called **agentinstall.sh** under any Unix Jumphost reside at **/root/qualys/agentinstall.sh.**

[root@ldnpinfuxm01 qualys]# **cat agentinstall.sh**

#---bof---

#!/bin/bash

# Configuring qualys cloud agent

# Add qualys account automatically if not found

# Check if server is accessible via ssh as root or if server is pingable

# Exit if password prompt found during ssh (quickie exit to move to the next server)

# Filter if server or IP resolvable

# Auto Qualys gateway assignment based on subnet

host=$@

for i in $host

do

#echo Checking if $i is pingable

hostchk=`ping -c1 $i`

if [[ $? -eq 0 ]]

then

hostssh=`ssh -o StrictHostKeyChecking=no -o BatchMode=yes -q $i date`

if [[ $? -eq 0 ]]

then

# Checking check if qualys-cloud-agent package already installed

qualysrpmcheck=`ssh -q $i 'rpm -qa |grep qualys | wc -l' `

chkval=$qualysrpmcheck

if [[ $chkval -eq 0 ]]

then

echo "Qualys cloud agent package not found. Installing it on $i"

scp -p qualys-cloud-agent.x86\_64.rpm $i:/var/tmp

ssh -q $i 'rpm -ivh /var/tmp/qualys-cloud-agent.x86\_64.rpm'

scp -p Appliance-Certificate.pem $i:/etc/qualys/cloud-agent/cert

scp -p qagent.config $i:/etc/qualys/cloud-agent

echo $i: `host $i |awk '{print $4}'`

subnet=`host $i | awk '{print $4}' | cut -d . -f 1-3`

subnetfile=subnetgwdist

cat $subnetfile | egrep "$subnet"

cat $subnetfile | egrep "$subnet" | cut -d " " -f 2- > qualys-cloud-agent

echo

echo Server: $i is using the following gateways below

cat qualys-cloud-agent

scp -p qualys-cloud-agent $i:/etc/sysconfig

ssh -q $i '/usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=0bfc6401-4fa2-4175-9cc2-fb8070f75e9a CustomerId=b546b3c9-3885-53eb-e040-18ac09046184 User=svcqca LogLevel=5 UseSudo=1 SudoUser=svcqca UserGroup=svcqca'

ssh -q $i 'chown -R svcqca:svcqca /etc/qualys /etc/sysconfig/qualys-cloud-agent'

ssh -q $i 'service qualys-cloud-agent restart'

ssh -q $i 'rm /var/tmp/qualys-cloud-agent.x86\_64.rpm'

else

echo $i `ssh -q $i 'rpm -qa | grep qualys'`

ssh -q $i 'ps -ef |grep qualys-cloud-agent'

fi

else

echo $i host is not accessible via ssh or passwordless ssh as root not allowed

fi

else

echo $i host not pingable

fi

done

#---eof---

### Running the **agentinstall.sh** script

1. Login as root on any of the Unix Jumphost,

Unix Jumphost : APAC - sngpinfuxm01, AMER - usprvrepo01d and EMEA - ldnpinfuxm01

1. As root, **cd /root/qualys**
2. Run, **“./agentinstall.sh <server name/s>**

**Example:**

[root@ldnpinfuxm01 qualys]# **./agentinstall.sh ldn2lx0131**

Qualys cloud agent package not found. Installing it on ldn2lx0131

\_\_\_\_\_ \_\_\_ \_\_\_ \_\_\_ \_ \_\_\_

|\_ \_| \_ \ |\_ \_/ \_\_| /\_\ | \_ \

| | | \_/ | | (\_\_ / \_ \| \_/

|\_| |\_| |\_\_\_\\_\_\_/\_/ \\_\\_|

WARNING!

This system including all related equipment, network devices and internet access (the "System") is restricted to authorised use only. By using the System, you agree that you are authorised to do so. if you are not authorised to use the System, you must discontinue any use of the System immediately. Unauthorized use, or misuse, of the System is a violation of applicable laws, regulations and policies and may subject you to criminal prosecution.

Use of the system, and all information (including personal information) placed or sent over the System, is subject to monitoring, recording and investigation, and may be used for any purpose. Your use of the System, authorised or unauthorised, constitutes your consent to such.

qualys-cloud-agent.x86\_64.rpm 100% 5780KB 5.6MB/s 00:00

warning: **/var/tmp/qualys-cloud-agent.x86\_64.rpm**: Header V4 DSA/SHA1 Signature, key ID a663d36e: NOKEY

Preparing... ########################################

Updating / installing...

qualys-cloud-agent-2.6.0-88 ########################################

Created symlink from /etc/systemd/system/multi-user.target.wants/qualys-cloud-agent.service to /usr/lib/systemd/system/qualys-cloud-agent.service.

\_\_\_\_\_ \_\_\_ \_\_\_ \_\_\_ \_ \_\_\_

|\_ \_| \_ \ |\_ \_/ \_\_| /\_\ | \_ \

| | | \_/ | | (\_\_ / \_ \| \_/

|\_| |\_| |\_\_\_\\_\_\_/\_/ \\_\\_|

WARNING!

This system including all related equipment, network devices and internet access (the "System") is restricted to authorised use only. By using the System, you agree that you are authorised to do so. if you are not authorised to use the System, you must discontinue any use of the System immediately. Unauthorized use, or misuse, of the System is a violation of applicable laws, regulations and policies and may subject you to criminal prosecution.

Use of the system, and all information (including personal information) placed or sent over the System, is subject to monitoring, recording and investigation, and may be used for any purpose. Your use of the System, authorised or unauthorised, constitutes your consent to such.

**Appliance-Certificate.pem** 100% 25KB 25.3KB/s 00:00

\_\_\_\_\_ \_\_\_ \_\_\_ \_\_\_ \_ \_\_\_

|\_ \_| \_ \ |\_ \_/ \_\_| /\_\ | \_ \

| | | \_/ | | (\_\_ / \_ \| \_/

|\_| |\_| |\_\_\_\\_\_\_/\_/ \\_\\_|

WARNING!

This system including all related equipment, network devices and internet access (the "System") is restricted to authorised use only. By using the System, you agree that you are authorised to do so. if you are not authorised to use the System, you must discontinue any use of the System immediately. Unauthorized use, or misuse, of the System is a violation of applicable laws, regulations and policies and may subject you to criminal prosecution.

Use of the system, and all information (including personal information) placed or sent over the System, is subject to monitoring, recording and investigation, and may be used for any purpose. Your use of the System, authorised or unauthorised, constitutes your consent to such.

**qagent.config** 100% 454 0.4KB/s 00:00

ldn2lx0131: 10.91.68.116

**10.91.68** **https\_proxy="https://ldn2lx0129.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080;https://ldn2lx0125.corp.ad.tullib.com:8080;https://ldn2lx0126.corp.ad.tullib.com:8080;https://ldn2lx0127.corp.ad.tullib.com:8080**"

Server: ldn2lx0131 is using the following gateways below

https\_proxy="https://ldn2lx0129.corp.ad.tullib.com:8080;https://ldn2lx0130.corp.ad.tullib.com:8080;https://ldn2lx0125.corp.ad.tullib.com:8080;https://ldn2lx0126.corp.ad.tullib.com:8080;https://ldn2lx0127.corp.ad.tullib.com:8080"

\_\_\_\_\_ \_\_\_ \_\_\_ \_\_\_ \_ \_\_\_

|\_ \_| \_ \ |\_ \_/ \_\_| /\_\ | \_ \

| | | \_/ | | (\_\_ / \_ \| \_/

|\_| |\_| |\_\_\_\\_\_\_/\_/ \\_\\_|

WARNING!

This system including all related equipment, network devices and internet access (the "System") is restricted to authorised use only. By using the System, you agree that you are authorised to do so. if you are not authorised to use the System, you must discontinue any use of the System immediately. Unauthorized use, or misuse, of the System is a violation of applicable laws, regulations and policies and may subject you to criminal prosecution.

Use of the system, and all information (including personal information) placed or sent over the System, is subject to monitoring, recording and investigation, and may be used for any purpose. Your use of the System, authorised or unauthorised, constitutes your consent to such.

**qualys-cloud-agent** 100% 229 0.2KB/s 00:00

Setting necessary permission for user: svcqca

Setting necessary permission for user: svcqca

Setting necessary permission for group: svcqca

hostid search path: /etc

Redirecting to /bin/systemctl restart qualys-cloud-agent.service

## Method 2: Linux Qualys Cloud Agent deployment –Automation (Ansible)

For any new RHEL server 7.6 and above we use our Satellite server to build new Linux servers. For Qualys Cloud Agent deployment for newly build server/s, we added an entries into ldnpinfuxm03:/etc/ansible/roles/common-tools-realm/tasks/main.yml.  
  
  
7.1 Qualys Cloud Angent Ansible Role Entries:

Ansible role URL: **ldnpinfuxm03:/etc/ansible/roles/common-tools-realm/tasks/main.yml**

#---Ansible role entries----

---

# tasks file for qualys\_cloud\_agent

#

#Qualys for rsyslog - AG / CA - 310320

- name: Create svcqca Group

group:

name: svcqca

gid: 2708

- name: Create svcqca User

user:

name: svcqca

uid: 2708

group: svcqca

comment: "Qualys Cloud Agent Service Account"

home: "/home/svcqca"

shell: /bin/bash

password: "$6$lNK6g1B7$Miw5TpHbjPxW2lOhxAitfb22saRUH0W9dMuubcmLUzg2isiN5agVCL8MjSJrmMd5PEoPkknyZzGiWQbGKJUep/"

- name: Add Qualys SSH-Key

authorized\_key:

user: svcqca

state: present

key: "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCrOOi3cMubz5DTl85EIho6zJDNjBBcp6H1CXmYfgiXKr/XhqgyCOgCPJof7ikvleikm2UE5J7KiIRyvN0LvPDXe3dz1xGEm/sy7lLGyMQUFF0GnTDsFVeEYx6703U/m0kUgRquBP1UCD6KWnplVzHA+chBK9xLrojxteanbZ8jTW3I07HzzvT9ygiNkHF2IPW9f5vWeqkDqhMcNGjh1UDIPFajTd1W73BKr5R4uk3AetCO0PbcYVF5fjVkGEDyw9/m1ZjUQK/T7Bhv1mkGgz7dsAQnT5h74T22EblNvALL8fe/8QoSgKRD3GosRN5JtNvyJ6xiK7O5Ux6azK2tmtQf"

- name: Copy Qualy Cloud Agent package to server

copy:

src: qualys-cloud-agent.x86\_64.rpm

dest: /var/tmp/qualys-cloud-agent.x86\_64.rpm

- name: Install Qualys Cloud Agent from Common Tools

yum:

name: /var/tmp/qualys-cloud-agent.x86\_64.rpm

state: present

- name: Copy Qualys Gateway Certificates to /etc/qualys/cloud-agent/cert/Appliance-Certificate.pem

copy:

src: Appliance-Certificate.pem

dest: /etc/qualys/cloud-agent/cert/Appliance-Certificate.pem

force: yes

- name: Change ownership to qualys cloud agent service account

file:

path: "{{ item }}"

state: directory

recurse: yes

owner: svcqca

group: svcqca

with\_items:

- /etc/qualys

- /usr/local/qualys

- name: Copy subnets details files to /var/tmp

copy:

src: subnetgwdist

dest: /var/tmp/subnetgwdist

force: yes

- name: Copy qualysgw.sh script to /var/tmp

copy:

src: qualysgw.sh

dest: /var/tmp/qualysgw.sh

force: yes

- name: Settings Qualys Cloud Agent Gateway Config

shell: /bin/bash /var/tmp/qualysgw.sh

ignore\_errors: yes

- name: Distribute config for EMEA

command: /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=0bfc6401-4fa2-4175-9cc2-fb8070f75e9a CustomerId=b546b3c9-3885-53eb-e040-18ac09046184 User=svcqca LogLevel=3 UseSudo=1 SudoUser=svcqca UserGroup=svcqca

when: OU\_Location | regex\_search('EMEA')

- name: Distribute config for APAC

command: /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=c5c79f46-237a-430b-bfd9-96cbf7895d77 CustomerId=b546b3c9-3885-53eb-e040-18ac09046184 User=svcqca LogLevel=3 UseSudo=1 SudoUser=svcqca UserGroup=svcqca

when: OU\_Location | regex\_search('APAC')

- name: Distribute config for AMER

command: /usr/local/qualys/cloud-agent/bin/qualys-cloud-agent.sh ActivationId=4cbf2459-cb83-4d1a-8364-a4415508bd68 CustomerId=b546b3c9-3885-53eb-e040-18ac09046184 User=svcqca LogLevel=3 UseSudo=1 SudoUser=svcqca UserGroup=svcqca

when: OU\_Location | regex\_search('AMER')

--------end of entries------

### How does it work and what does the Ansible Role do in Qualys Agent Deployment?

Basically we create new server profile at the Satellite server for every new RHEL server.

Basic steps in Building new server  
1. Login as -a account at <https://ldnpinfuxm03.eur.ad.tullib.com/>

2. Click on Host -> Create Host -> Provide the new server profile details, this include (IP address and etc.)

3. At Ansible Roles -> Locate the “**common-tools-realm**”, then click the + sign to add.  
4. Hit Submit to start building the new server.

5. Once Completed we handover to the user for verification test.

Here is a sample of the server build logs related to Qualys Cloud Agent Deployment via Server Build Automation.

260:

TASK [qualys-tools : Create svcqca Group] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 261:

ok: [ldn2lx0131.corp.ad.tullib.com]

 262:

 263:

TASK [qualys-tools : Create svcqca User] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 264:

ok: [ldn2lx0131.corp.ad.tullib.com]

 265:

 266:

TASK [qualys-tools : Add Qualys SSH-Key] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 267:

ok: [ldn2lx0131.corp.ad.tullib.com]

 268:

 269:

TASK [qualys-tools : Copy Qualy Cloud Agent package to server] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 270:

changed: [ldn2lx0131.corp.ad.tullib.com]

 271:

 272:

TASK [qualys-tools : Install Qualys Cloud Agent from Common Tools] \*\*\*\*\*\*\*\*\*\*\*\*\*

 273:

changed: [ldn2lx0131.corp.ad.tullib.com]

 274:

 275:

TASK [qualys-tools : Copy Qualys Gateway Certificates to /etc/qualys/cloud-agent/cert/Appliance-Certificate.pem] \*\*\*

 276:

changed: [ldn2lx0131.corp.ad.tullib.com]

 277:

 278:

TASK [qualys-tools : Change ownership to qualys cloud agent service account] \*\*\*

 279:

changed: [ldn2lx0131.corp.ad.tullib.com] => (item=/etc/qualys)

 280:

changed: [ldn2lx0131.corp.ad.tullib.com] => (item=/usr/local/qualys)

 281:

 282:

TASK [qualys-tools : Copy subnets details files to /var/tmp] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 283:

changed: [ldn2lx0131.corp.ad.tullib.com]

 284:

 285:

TASK [qualys-tools : Copy qualysgw.sh script to /var/tmp] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 286:

changed: [ldn2lx0131.corp.ad.tullib.com]

 287:

 288:

TASK [qualys-tools : Settings Qualys Cloud Agent Gateway Config] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 289:

changed: [ldn2lx0131.corp.ad.tullib.com]

 290:

 291:

TASK [qualys-tools : Distribute config for EMEA] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 292:

changed: [ldn2lx0131.corp.ad.tullib.com]

 293:

 294:

TASK [qualys-tools : Distribute config for APAC] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 295:

skipping: [ldn2lx0131.corp.ad.tullib.com]

 296:

 297:

TASK [qualys-tools : Distribute config for AMER] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 298:

skipping: [ldn2lx0131.corp.ad.tullib.com]

 299:

 300:

TASK [qualys-tools : Qualys Agent Re-Start Service] \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 301:

changed: [ldn2lx0131.corp.ad.tullib.com]

 319:

PLAY RECAP \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

 320:

ldn2lx0131.corp.ad.tullib.com : ok=17 changed=10 unreachable=0 failed=0 skipped=4 rescued=0 ignored=0

 321:

 322:

Exit status: 0

## Qualys Cloud Agent Logs

Qualys Cloud Agent logs can be located at /var/log/qualys/qualys-cloud-agent.log, as default it is set to LogLevel=3 and archive file will be maximum 5 log rotate with 10mb size each. Qualys Log configuration can be found at /etc/qualys/cloud-agent/qagent-log.conf

### /etc/qualys/cloud-agent/qagent-log.conf file content

logging.channels.c1.class: ConsoleChannel

logging.channels.c1.formatter: f1

logging.channels.c2.class: SyslogChannel

logging.channels.c2.facility: 24

logging.channels.c2.formatter: f2

logging.channels.c2.name: qualys-cloud-agent

logging.channels.c2.options: 1

logging.channels.c3.archive: number

logging.channels.c3.class: FileChannel

logging.channels.c3.formatter: f1

logging.channels.c3.path: **/var/log/qualys/qualys-cloud-agent.log**

logging.channels.c3.purgeCount: **5**

logging.channels.c3.rotation: **10M**

logging.channels.splitter.channels: c2,c3

logging.channels.splitter.class: SplitterChannel

logging.formatters.f1.class: PatternFormatter

logging.formatters.f1.pattern: %Y-%m-%d %H:%M:%S.%i [%s][%P]:[%p]:%t

logging.formatters.f1.times: local

logging.formatters.f2.class: PatternFormatter

logging.formatters.f2.pattern: [%P]:[%p]:%t

logging.formatters.f2.times: local

logging.loggers.l1.channel: c3

logging.loggers.l1.level: debug

logging.loggers.l1.name: qualys-cloud-agent

logging.loggers.l2.level: debug

logging.loggers.l2.name: qualys-cloud-agent.provision

logging.loggers.l3.channel: splitter

logging.loggers.l3.level: information

logging.loggers.l3.name: qualys-cloud-agent.uninstall

logging.loggers.l4.level: debug

logging.loggers.l4.name: qualys-cloud-agent.scan

logging.loggers.root.channel: c3

logging.loggers.root.level: information

## Qualys Cloud Agent Main Configuration file

The Qualys Cloud Agent is reside at /etc/qualys/cloud-agent/qualys-cloud-agent.conf, there were 3 configuration files used by the agents which is based on regions..

### APAC: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content

#Config File

#LogLevel: Higher value means more verbose. 0=fatal, 1=error, 2=warning, 3=info, 4=debug, 5=tracing

#CmdMaxTimeOut: TimeOut in seconds. Any command execution that exceeds this time will be killed.

#ProcessPriority: To set process priority(nice value).

#RequestTimeOut: Http request timeout in seconds.

#CmdStdOutSize: Command std output size in KB. Any command output size exceeds this time will be truncated.

SudoCommand=sudo

LogFileDir=/var/log/qualys/

CmdMaxTimeOut=1800

ProcessPriority=0

RequestTimeOut=600

UseAuditDispatcher=1

CmdStdOutSize=1024

LuaScriptTimeOut=3600

ActivationId=c5c79f46-237a-430b-bfd9-96cbf7895d77

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

LogLevel=5

UseSudo=1

SudoUser=svcqca

UserGroup=svcqca

### AMER: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content

#Config File

#LogLevel: Higher value means more verbose. 0=fatal, 1=error, 2=warning, 3=info, 4=debug, 5=tracing

#CmdMaxTimeOut: TimeOut in seconds. Any command execution that exceeds this time will be killed.

#ProcessPriority: To set process priority(nice value).

#RequestTimeOut: Http request timeout in seconds.

#CmdStdOutSize: Command std output size in KB. Any command output size exceeds this time will be truncated.

SudoCommand=sudo

LogFileDir=/var/log/qualys/

CmdMaxTimeOut=1800

ProcessPriority=0

RequestTimeOut=600

UseAuditDispatcher=1

CmdStdOutSize=1024

LuaScriptTimeOut=3600

ActivationId=4cbf2459-cb83-4d1a-8364-a4415508bd68

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

LogLevel=3

UseSudo=1

SudoUser=svcqca

UserGroup=svcqca

### EMEA: /etc/qualys/cloud-agent/qualys-cloud-agent.conf File Content

#Config File

#LogLevel: Higher value means more verbose. 0=fatal, 1=error, 2=warning, 3=info, 4=debug, 5=tracing

#CmdMaxTimeOut: TimeOut in seconds. Any command execution that exceeds this time will be killed.

#ProcessPriority: To set process priority(nice value).

#RequestTimeOut: Http request timeout in seconds.

#CmdStdOutSize: Command std output size in KB. Any command output size exceeds this time will be truncated.

SudoCommand=sudo

LogFileDir=/var/log/qualys/

CmdMaxTimeOut=1800

ProcessPriority=0

RequestTimeOut=600

UseAuditDispatcher=1

CmdStdOutSize=1024

LuaScriptTimeOut=3600

ActivationId=0bfc6401-4fa2-4175-9cc2-fb8070f75e9a

CustomerId=b546b3c9-3885-53eb-e040-18ac09046184

LogLevel=3

UseSudo=1

SudoUser=svcqca

UserGroup=svcqca

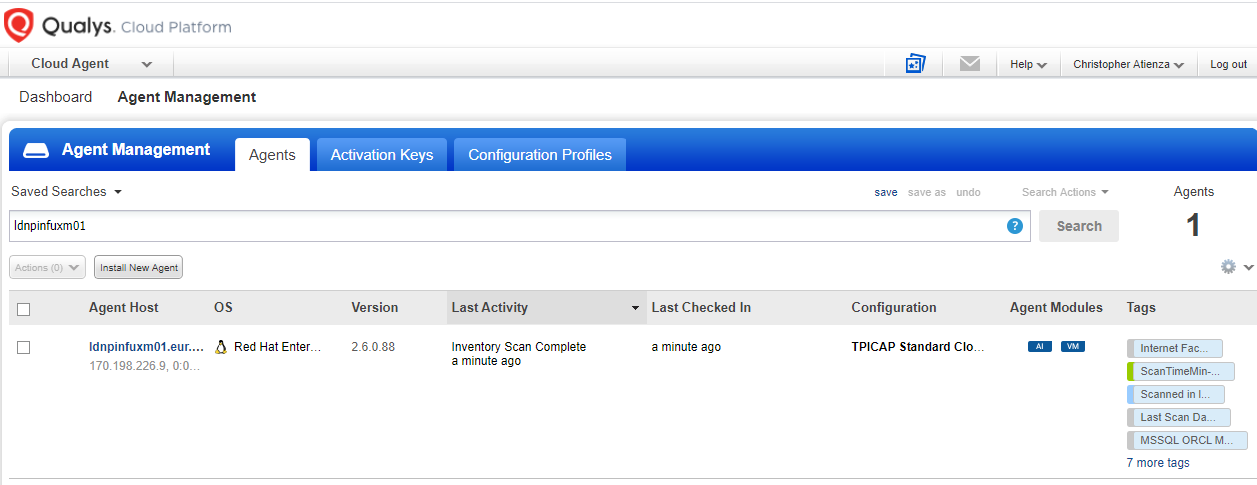
## Qualys Cloud Agent connectivity verification

To validate that the Qualys cloud agent were able to connect into its Qualys Gateways we use a customized script we called **/root/qualys/chkagent.sh** which can be found to all Linux Jumphost under /root/qualys directory.  
  
The string we need to look at in /var/log/qualys/qualys-cloud-agent.log should be “Validation check passed for the Config”, once we get this at the log the agent were successfully configured and agent will be visible at <https://qualysguard.qualys.eu/portal-front/module/ca/#tab=ca-agents.datalist-agents>.

Usage: **/root/qualys/chkagent.sh <servername/s>**

Sample:  
  
root@ldnpinfuxm01 qualys]# **/root/qualys/chkagent.sh ldnpinfuxm01**

ldnpinfuxm01; ldnpinfuxm01.eur.ad.tullib.com 170.198.226.9 ; /var/log/qualys/qualys-cloud-agent.log.4:2020-05-22 13:34:22.864 [qualys-cloud-agent][1051]:[Information]:[139746311657280]:Validation check passed for the Config: 4a30907c-5618-4e3c-9027-9cbdc8619c27

**Qualys Cloud Agent Portal:**  


## Start and Stopping the Qualys Cloud Agent services,

### To stop the Qualys Cloud Agent Service

service qualys-cloud-agent stop

or

systemctl stop qualys-cloud-agent

### To start the Qualys Cloud Agent Service

service qualys-cloud-agent start

or

systemctl start qualys-cloud-agent