Qualys Cloud Agent Linux 6.0 (x64)

June 2023

We're excited to tell you about new features, improvements, platform coverage changes, and fixes in this Cloud Agent release. These updates are specific to the agent binary. Platform updates for new features and fixes of management, syncing, tagging, and reporting capabilities of Cloud Agents are documented in the Cloud Platform and Cloud Suite release notes.

New Features

- Added support for Endpoint Detection and Response (EDR) and Endpoint Protection (EPP). The following table lists the supported operating systems:

Operating System	Qualys EDR	Qualys EPP
Amazon Linux 2	✓	✓
CentOS Linux 6	✓	⊘
CentOS Linux 7	✓	✓
Debian 9, 10, and 11	✓	✓
Oracle Enterprise Linux (OEL) 6	✓	⊘
Oracle Enterprise Linux (OEL) 7 and 9	✓	✓
SUSE Linux Enterprise Server (SLES) 12 and 15	✓	✓
Red Hat Enterprise Linux (RHEL) 6	✓	⊘
Red Hat Enterprise Linux (RHEL) 7, 8, and 9	✓	✓
Ubuntu 16, 18, 20 and 22	✓	✓

  Qualys EDR must be enabled for the selected agent host for support on the Qualys Endpoint Protection (EPP).

  Required application version: Endpoint Detection and Response (EDR) 2.5.0

- Host quarantine feature using EDR: The asset quarantine feature can restrict network communication with a specific host in case of any malicious event. You can quarantine an asset from the Endpoint Detection and Response (EDR) application.

  When an asset is quarantined, the asset will be isolated from the network and communicates only with the Qualys Cloud Agent. However, you can configure the applications that the quarantined asset can access.

  Once the asset is in a healthy state, you can release the asset from the quarantined state using the EDR application.

  Required application version: Endpoint Detection and Response (EDR) 2.5.0

- Troubleshooting options in the Cloud Agent application interface: Earlier, the administrator user needed to access the asset and perform multiple steps for performing common troubleshooting actions, such as restarting the agent service.

  With this feature, you can perform common troubleshooting actions easily using the Cloud Agent application interface.

Copyright 2023 by Qualys, Inc. All Rights Reserved.

- Enable or disable the trace log level
- Restart agent service

Note: These options are available only to the Administrator user.

Required application version: Qualys Cloud Platform 3.15.1.0

- Proxy support: Added support for HTTPS- TLS proxy to establish an encrypted connection to the proxy. You can configure the agent to use the proxy in one of the following ways:
  - /etc/sysconfig/qualys-cloud-agent– applies to Cloud Agent for Linux (.rpm)
  - /etc/default/qualys-cloud-agent– applies to Cloud Agent for Linux (.deb)
  - /etc/environment–- applies to Cloud Agent for Linux (.rpm) and Linux (.deb)

Enhancements

- Patch Management
  - Introduced new status messages to indicate the agent health status for Patch Management for the following scenarios:
    - The agent has received the patch.
    - The job is pending as another patch job is in progress.
  - Added job timeout reason message to display the timeout reason in the Patch Management application.

Required application version: Patch Management 2.2.0.0

Behavior Changes

There are no behavior changes in this release.

Platform Coverage Support (Operating Systems)

There is no new platform coverage added in this release.

Fixed Defects

The following reported and notable issues have been fixed in this release.

ID	Description
CRM-99218	Fixed an issue, where the cloud agent scan did not detect CID 7646 for a host, while the scan run using a scanner detected CID 7646 for the same host.
CRM-103327	Fixed an issue, where the hostname was not getting updated in the Cloud Agent application for the Linux agent installed on SUSE Linux Enterprise Server (SLES) platform.
CRM-101243 CRM-102050	Fixed an issue where the filecontentcheck in the UDC scan does not check the symlink file. Now, the filecontentcheck in UDC scan checks for the original and symlink files.
LXAG-13519	Fixed an issue where a lag was observed in patch scan result indexing due to duplicate messages. Now, the Agent has a unique Datetime, conetxtID, and StatusCode for each status in Patch Agent Health Status (AHS)table.

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Known Limitations and Workarounds

- On SUSE Linux Enterprise Server (SLES) version 12 platform without a service pack, FIM events are getting dropped.

Known issues for Host quarantine feature using EDR

- iptables is deprecated from RHEL 9. However, it is available in the Linux package repository. You can install the iptables package using the `yum install iptables` command. iptables rules persist after the system reboot. However, it might take time for the system to reboot, agent loading, and re-applying the quarantine policy.
- If the agent is running with a non-root user, set the value to `usesudo=1`. This setting is mandatory to execute the iptables commands.
- As part of the quarantine process, if you switch a group, the iptables rules will be based on the earlier gid of the Qualys process. However, you can change to the same group with which the agent was configured using the command utility.
- After the host is quarantined, only a particular effective gid-owner will have access to the internet and any other user or group will be unable to access the internet. Many processes can have the same effective gid.
- Two processes that are members of the same group, and the same gid will have the same group access permissions. This allows network connectivity.
- The instanceid and MetaData check fail after the host is in quarantine state. This failure is due to port number 80 being used for communication. Communication is allowed only on port 443.
- Agent will not communicate if configured proxy is an ipv6. If an agent is configured with ipv6 proxy, do not perform Quarantine Host action as it will result in an undefined behavior.
- Qualys group process is currently available for quarantined agents in VM/PC and EDR applications.

Copyright 2023 by Qualys, Inc. All Rights Reserved.