Cisco WAN Automation Engine Release Notes, Release 6.3.9

First Published: 2017-03-17
Last Updated: 2017-08-03

This document describes the features, limitations, and bugs for Cisco WAN Automation Engine (Cisco WAE) Release 6.3.9.

Contents

This document includes the following sections:

Introduction

Cisco WAE is a model-driven path visibility and path computation engine that simulates, automates, and optimizes multi-vendor, multi-layer networks by leveraging time-series traffic and flow data. For more information on Cisco WAE, visit http://www.cisco.com/go/wae.

Cisco Systems, Inc.
www.cisco.com

Open Source

A list of open source software used in Cisco WAE can be found in Open Source Software Used in Cisco WAN Automation Engine.

Resolved Bugs

The following are descriptions of the resolved bugs in Cisco WAE Release 6.3.9. The bug ID links you to the Cisco Bug Search tool.

Table 1 Resolved Bugs

Bug ID	Description
CSCvb98122	Cisco WAE Collector, WAE Live, and WAE Design include a version of the LIBSSH2 protocol that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2015-1782
CSCvc98439	Interfaces that have a configured capacity greater than 1.0e+06 are not discovered as traffic engineering-enabled. Consequently, when doing a failure analysis, there are no demands that use these links.
CSCvd02128	In WAE Live, if the data point time stamps are not aligned for the capacity property, the stacked graph is shown incorrectly. (If the time stamps are aligned, the stacked graph displays correctly.)

Using the Cisco Bug Search Tool

You can use the Cisco Bug Search Tool to search for a specific bug or to search for all bugs in a release.

Step 1 Go to the Cisco Bug Search Tool.

Step 2 Enter your registered Cisco.com username and password, and then click **Log In**. The Bug Search page opens.

Note If you do not have a Cisco.com username and password, you can register for them.

Step 3 Use any of these options to search for bugs, and then press Enter (Return) to initiate the search:

- To search for a specific bug, enter the bug ID in the Search For field.
- To search for bugs based on specific criteria, enter search criteria in the Search For field, such as a problem description or a feature.
- To search for bugs based on products, enter or select the product from the Product list. For example, if you enter “WAE,” you have several options from which to choose.
- To search for bugs based on releases, in the Releases list select whether to search for bugs affecting a specific release, bugs that were fixed in a specific release, or both. Then enter one or more release numbers.

Step 4 When the search results are displayed, use the filter tools to narrow the results. You can filter the bugs by status, severity, modified date, and so on.

To export the results to a spreadsheet, click **Export Results to Excel**.

Known Limitations

This section describes the limitations and restrictions for Cisco WAE.

WAE Design

macOS Sierra 10.12 implements an additional security measure for applications that are not distributed through the App Store, which includes WAE Design.

By default, WAE Design is in a quarantine state as shown by the following command on a terminal:

```
xattr Mate.app
```

The command returns the following for a quarantined application:

```
com.apple.quarantine
```

As a workaround, remove WAE Design from quarantine by entering:

```
xattr -r -d com.apple.quarantine Mate.app
```

Then, you can run WAE Design 6.3.x on macOS Sierra 10.12.

WAE Collector and WAE Network Interface (NI)

- Due to vendor MIB limitations, Collector cannot represent QoS traffic on interfaces that have more than one VLAN configured. If a network contains such interfaces, their queue traffic statistics are omitted from the collection. The total traffic on these interfaces is still measured. As a result, per class-of-service demands estimated through Demand Deduction are less accurate. Estimates of traffic totals over all classes of services, however, are not affected.
- Due to lack of MIB support, SR tunnel type is not collected for Cisco IOS XR routers through SNMP.
- Collection of interface egress shaping rate for Alcatel-Lucent devices does not support LAG interfaces.
- Shared Risk Link Groups (SRLGs) are not supported in Alcatel-Lucent Service Aware Manager (SAM) collection.

WAE NI

- The interval for continuous LSP discovery in WAE NI cannot be less than 60 seconds.
- LSP's ActualPathHop cannot be resolved when using continuous collection. As a workaround, use interval-based collection.

Collector

- OSPFv3 and IPv6 IS-IS databases cannot be collected. The workaround is to use a manual snapshot.

- SNMPv3 is not an available option when configuring default credentials.
- `snmp_find_interfaces`
  - Does not support association of a GRE tunnel with the physical interface it uses to reach the tunnel destination since the IP-Tunnel MIB lacks this information.
  - Does not update LAG port status if LAGs are discovered running both `parse_configs` and `snmp_find_interfaces`. The workaround is to run only `snmp_find_interfaces`.
- Juniper routers: Signaled standby LSP path option is not available from the standard MPLS-TE MIB for Juniper routers. Only the active path option name is collected.
- Cisco IOS XR routers
  - IGP topology collected through `parse_igp` and `login_find_igp_db`

    – IS-IS link-state database with TE extensions contains incorrect interface “admin-weights” (TE metric) on Intel-based routers.

    – IPv6 IS-IS link-state database does not contain IPv6 interface addresses or parallel interfaces. This information is only available when Cisco IOS XR supports IS-IS IPv6 TE extensions. The `snmp_find_interfaces` tool collects this information.
  - MAC Accounting is not supported.
  - `snmp_find_rsvp` does not set the Standby value in the <LSPPaths> table for signaled backup paths or collect named affinities configured with affinity-maps.
- BGP peers
  - `find_bgp` does not build BGP pseudo-nodes among internal ASNs.
  - `find_bgp` does not collect BGP peers under PE-CE VRFs.
- `parse_configs`
  - Does not accurately detect the bandwidth of some Juniper ‘ge’ interfaces that have a capacity of 10 Gbps.
  - Collects POS bundles, but has limitations due to unavailability of the port OperStatus property.
- TE Extended Admin Groups (EAGs), also known as extended affinities, are not supported.
- Port circuits are not built for LAG/bundle members whose nodes are not within the same IGP instance as the AS.
- There is no support for building port circuits for LAG members that are not within the same IGP (inter-AS circuits)
- It is not possible to distinguish between physically connected and unconnected LAG ports that are down for LAG port matching.
- `snmp_find_ospf_db` cannot be used when routers have a large number of links that cannot fit into a single PDU.
- `find_bgpls` does not support multi-area OSPF or multi-level IS-IS, non-TE-enabled interfaces, and pseudo-nodes. The workaround is to use SNMP- or login-based discovery.
- `get_inventory` does not collect Juniper multi-chassis router hardware inventory.
- Segment routing
  - SR protected adjacency SIDs are not supported.
  - Concurrent RSVP-TE and SR-TE paths are not supported on the same LSP.

SAM-OSS Integration with Snapshots

- `sam_getplan` does not populate the <NodeTraffic> table. This table is derived and populated when `sam_getplan` and SNMP tools are used together.
- `sam_getplan` does not populate the NetIntActivePath column in the <LSPs> table.
- If `sam_getplan` and SNMP tools are used together in the snapshot process for multi-vendor network collection, then Alcatel-Lucent traffic measurements cannot be aligned with those collected from other router platforms.

Cisco Open SDN Controller (OSC)

During detailed PCEP tunnel creation or when modifying PCEP tunnels, affinity values are misinterpreted if multiple affinities are specified. This limits you to specifying one affinity for IncludeAffinity, IncludeAnyAffinity, and ExcludeAffinity, and each of these values must be a number within [0,31].

NSO Controller

- LSP affinities are deployed, while interfaces affinities require separate provisioning.
- LSPs that exist in the network by another controller cannot be updated.
- Deployment of each RSVP-TE named-path or SR-TE segment-list is limited to a single LSP.
- Cisco IOS XR: WAE client specifies the XR LSP signaled-name, while NSO service and device use tunnel-id. The workaround is to deploy all Cisco IOS XR LSPs using the tunnel-id and to make sure that existing LSPs are not redeployed.
- NEDs (NSO console)
  - For Cisco IOS XR, there is no option to give the IP address of the LSP directly; you can only specify a loopback address. There is no option to give tunnel affinity values directly; you can only specify an affinity-map name.
  - For Junos, there is no inter-domain keyword, which is used only when an inter-area LSP is created.

WAE System

Installation and Startup

- The WAE NI server and the WAE Core server cannot reside on the same device or on the same VM. Note that the *Cisco WAE Server Installation Guide* assumes that they are on the same device. If needed, contact your support representative for further installation details.
- If the OS is using an old CA certificate to verify the integrity of the EPEL repository, you might see this error from the OS vendor:

  ```
  Error: Cannot retrieve metalink for repository: epel. Please verify its path and try again.
  ```

  - One workaround is to perform an offline installation. For instructions, refer to the “Offline Installation” chapter in the *Cisco WAE Server Installation Guide*.
  - Another workaround is to change https to http.

Note This is not a secure solution. For information on how to resolve OS security issues, contact your OS vendor.

1. In the `/etc/yum.repos.d/epel.repo` file, change the first instance of https to http.

   ```
   sudo vim /etc/yum.repos.d/epel.repo
   ```

   Change `https` to `http` in the following line:

   ```
   mirrorlist=[https://mirrors.fedoraproject.org/metalink-repo=epel-6&arch=$basearch]
   ```

2. Execute yum to clean up makecache.

   ```
   sudo yum clean all && yum makecache
   ```

3. Rerun the installer. For detailed installation instructions, see the *Cisco WAE Server Installation Guide*.

   ```
   sudo bash wae-k9-<version>.bin
   ```

- The `$CARIDEN_HOME` directory is not automatically added to `$PATH` (only `$CARIDEN_HOME/bin` is). If not in `$CARIDEN_HOME/bin`, to start the WAE Design GUI from the command line, you must specify its full path.

  ```
  /opt/cariden/software/mate/current/mate
  ```

Web Server

The `embedded_web_server` tool is deprecated. The recommendation is to use the `wae-web-server` service, which is constantly monitored to be brought up automatically.

By default, this web service starts upon installation completion. Therefore, if you stop the web server using the `embedded_web_server` tool (`embedded_web_server -action stop`), the web server does not stop. The workaround is the following:

```
service wae-svcs-mon stop
embedded_web_server -action stop
```

WAE Statistics UI

The WAE Statistics page does not appear in some web browsers if you do not have the correct SSL certificates. To work around this, install the correct SSL certificates (see the "Installing an SSL Web Certificate" section in the *Cisco WAE System Administration Guide*) or do the following:

1. Click the WAE Statistics link. The URL format is https://<*server_IP*>:8443; for example, https://192.0.2.14:8443.
2. Copy the URL of the page to another browser window.
3. In the new browser, change the URL port from 8443 to 8843; for example, https://192.0.2.14:8843.
4. Follow the browser messages to accept the connection and add it as an exception.

Web User Management

Both the System UI and the WAE Design Archive UI have local user management capabilities. If both are used to configure users, WAE uses the most recently updated information. The recommendation is to use only the System UI to manage local users.

License Check Failures on Newer Linux Distributions

Some newer Linux distributions have started using a new way (via `biosdevname`) of naming hardware devices, including the network interfaces. This causes some software that depends on the traditional naming (for example, `eth0`, `eth1`) to fail on license checks, including MATE.

The workaround is to append `biosdevname=0` to the kernel line of the grub configuration file and reboot. (Syntax varies among distributions.)

After reboot, you should be able to use ifconfig to verify that the NICs are named `eth0` (or `eth1`, ...) instead of the `biosdevname` names (such as `p34p1`).

Java Memory

Certain tools (such as `sam_getplan` and `parse_configs`) may require more memory to start than what is available. The symptom is an error message similar to the following:

```
Error occurred during initialization of VM.
Could not reserve enough space for object heap.
Error: Could not create the Java Virtual Machine.
Error: A fatal exception has occurred. Program will exit.
```

The workaround is to set the maximum memory to a low enough value in the `CARIDEN_JAVA_OPTIONS` variable before calling the tool. An example setting is as follows:

```
set CARIDEN_JAVA_OPTIONS=-Xmx1000m
```

Use of App Engine APIs to Deploy SR and RSVP Non-PCEP LSPs

Although you can use App Engine APIs to deploy SR and RSVP non-PCEP LSPs in WAE 6.3.9, we recommend that you use WAE Design to deploy these types of LSPs through NSO.

App Engine APIs are fully supported in WAE 6.4.x.

Accessibility Features

All product documents are accessible except for images, graphics, and some charts. If you would like to receive the product documentation in audio format, braille, or large print, contact accessibility@cisco.com.

Related Documentation

For related documentation, see the *Cisco WAE 6.3 Documentation Roadmap*.