Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSes) on a device, you must ensure that the following conditions are met:

- You must assign a DS to the device. Refer to the “Diagnostic Signature Downloading” section for more information on how to assign DSes to devices.

- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Information About Diagnostic Signatures

Diagnostic Signatures Overview

Diagnostic signatures (DS) for the call-home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DSes provides the ability to define more types of events and trigger types to perform the required actions than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify its integrity, reliability, and security.

The structure of a DS file can be one of the following formats:

- Metadata-based simple signature that specifies event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI . The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats mentioned above.

The following basic information is contained in a DS file:

- ID (unique string): unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription): unique description of the DS file that can be used in lists for selection.
- Description: long description about the signature.
- Revision: version number, which increments when the DS content is updated.
- Event & Action: defines the event to be detected and the action to be performed after the event happens.

Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download.

Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Workflow

The Diagnostic Signature feature is enabled by default on the Cisco software. The following is the workflow for using diagnostic signatures:

1. Find the DS(es) you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
2. The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded.
4. The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.
5. The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature Events and Actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed

after the event happens, such as collecting **show** command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature Event Detection

Event detection in DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and call-home are the supported event types, where "immediate" indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two or more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an evnt occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS file that are used to customize the files.

DS actions are categorized into the following five types:

- call-home
- command
- emailto
- script
- message

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses "diagnostic-signature" as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

DS action type message defines action to generate message to notify or remind user certain important information. The message could be broadcasted to all TTY lines or generated as a syslog entry.

Diagnostic Signature Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment***variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring Call Home Service for Diagnostic Signatures

Configure the call home service feature to set attributes such as the contact email address where notifications regarding diagnostic signature (DS) downloads are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and we recommend using it. If used, you only need to change the destination transport-method to the http setting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **service call-home**
4. **call-home**
5. **contact-email-addr** *email-address*
6. **mail-server** {*ipv4-addr* | *ipv6-addr* | *name*} **priority** *number*
7. **profile** *profile-name*
8. **destination transport-method** {**email** | **http**}
9. **destination address** {**email** *address* | **http** *url*}
10. **subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}]
11. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**service call-home** **Example:** `Device(config)# service call-home`	Enables Call-Home service on a device.
Step 4	**call-home** **Example:** `Device(config)# call-home`	Enters Call-Home configuration mode for the configuration of Call-Home settings.
Step 5	**contact-email-addr** *email-address* **Example:** `Device(cfg-call-home)# contact-email-addr userid@example.com`	Assigns an email address to be used for Call-Home customer contact.
Step 6	**mail-server** {*ipv4-addr* | *ipv6-addr* | *name*} **priority** *number* **Example:** `Device(cfg-call-home)# mail-server 10.1.1.1 priority 4`	Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call-Home.

	Command or Action	Purpose
Step 7	**profile** *profile-name* **Example:** `Device(cfg-call-home)# profile user1`	Configures a destination profile for Call-Home and enters Call-Home profile configuration mode.
Step 8	**destination transport-method** {**email** | **http**} **Example:** `Device(cfg-call-home-profile)# destination transport-method http`	Specifies a transport method for a destination profile in the Call-Home.
Step 9	**destination address** {**email** *address* | **http** *url*} **Example:** `Device(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Configures the address type and location to which Call-Home messages are sent. **Note** To configure diagnostic signature, you must use the http option.
Step 10	**subscribe-to-alert-group inventory** [**periodic** {**daily** *hh:mm* | **monthly** *day hh:mm* | **weekly** *day hh:mm*}] **Example:** `Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30`	Configures a destination profile to receive messages for the Inventory alert group for Call-Home. • This command is used only for the periodic downloading of DS files.
Step 11	**exit** **Example:** `Device(cfg-call-home-profile)# exit`	Exits Call-Home profile configuration mode and returns to Call-Home configuration mode.

What to Do Next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configuring Diagnostic Signatures

Before You Begin

Configure the Call Home Service feature to set attributes for the Call Home profile as described in the "Configuring Call Home Service for Diagnostic Signatures" section. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

SUMMARY STEPS

1. **call-home**
2. **diagnostic-signature**
3. **profile** *ds-profile-name*
4. **environment ds_** *env-varname ds-env-varvalue*
5. **end**
6. **call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*}
7. **show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **postrequisite** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home** **Example:** `Device(config)# call-home`	Enters call-home configuration mode for the configuration of Call Home settings.
Step 2	**diagnostic-signature** **Example:** `Device(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 3	**profile** *ds-profile-name* **Example:** `Device(cfg-call-home-diag-sign)# profile user1`	Specifies the destination profile on a device that DS uses.
Step 4	**environment ds_** *env-varname ds-env-varvalue* **Example:** `Device(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.
Step 5	**end** **Example:** `Device(cfg-call-home-diag-sign)# end`	Exits call-home diagnostic signature mode and returns to privileged EXEC mode.
Step 6	**call-home diagnostic-signature** {{**deinstall** | **download**} {*ds-id* | **all**} | **install** *ds-id*} **Example:** `Device# call-home diagnostic-signature download 6030`	Downloads, installs, and uninstalls diagnostic signature files on a device.
Step 7	**show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **postrequisite** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [**download**]]	Displays the call-home diagnostic signature information.

	Command or Action	Purpose
	Example: `Device# show call-home diagnostic-signature actions`	

Configuration Examples for Diagnostic Signatures

Examples: Configuring Diagnostic Signatures

The following example shows how to enable the periodic downloading request for diagnostic signature (DS) files. This configuration will send download requests to the service call-home server daily at 2:30 p.m. to check for updated DS files. The transport method is set to HTTP.

```
Device> enable
Device# configure terminal
Device(config)# service call-home
Device(config)# call-home
Device(cfg-call-home)# contact-email-addr userid@example.com
Device(cfg-call-home)# mail-server 10.1.1.1 priority 4
Device(cfg-call-home)# profile user-1
Device(cfg-call-home-profile)# destination transport-method http
Device(cfg-call-home-profile)# destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 14:30
Device(cfg-call-home-profile)# exit
Device(cfg-call-home)# diagnostic-signature
Device(cfg-call-home-diag-sign)# profile user1
Device(cfg-call-home-diag-sign)# environment ds_env1 envarval
Device(cfg-call-home-diag-sign)# end
```

The following is sample output from the **show call-home diagnostic-signature** command for the configuration displayed above:

```
Device# show call-home diagnostic-signature

Current diagnostic-signature settings:
Diagnostic-signature: enabled
Profile: user1 (status: ACTIVE)
Environment variable:
ds_env1: abc
Downloaded DSes:
DS ID    DS Name                         Revision Status     Last Update (GMT+00:00)
-------- ------------------------------- -------- ---------- -------------------
6015     CronInterval                    1.0      registered 2013-01-16 04:49:52
6030     ActCH                           1.0      registered 2013-01-16 06:10:22
6032     MultiEvents                     1.0      registered 2013-01-16 06:10:37
6033     PureTCL                         1.0      registered 2013-01-16 06:11:48
```

Additional References for Diagnostic Signatures

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
Debug commands	Cisco IOS Debug Command Reference - Commands A through D Cisco IOS Debug Command Reference - Commands E through H Cisco IOS Debug Command Reference - Commands I through L Cisco IOS Debug Command Reference - Commands M through R Cisco IOS Debug Command Reference - Commands S through Z
High Availability commands	Cisco IOS High Availability Command Reference

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for Configuring Diagnostic Signatures

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to . An account on Cisco.com is not required.

Table 1: Feature Information for Configuring Diagnostic Signatures

Feature Name	Releases	Feature Information
Diagnostic Signatures		The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks. The following commands were introduced or modified: **active** (diagnostic signature), **call-home diagnostic-signature**, **clear call-home diagnostic-signature statistics**, **debug call-home diagnostic-signature**, **diagnostic-signature**, **environment** (diagnostic signature), **profile** (diagnostic signature), and **show call-home diagnostic-signature**.