Software Integrity Assurance

This chapter describes Runtime Integrity Assurance feature.

This chapter includes the following sections:

Finding Feature Information

Your software release might not support all the features documented in this module. For the latest caveats and feature information, see the Bug Search Tool at https://tools.cisco.com/bugsearch/ and the release notes for your 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 "New and Changed Information"chapter or the Feature History table in this chapter.

Overview of Runtime Integrity Assurance

The Runtime Integrity Assurance feature provides assurance about the authenticity of the Cisco NX-OS system and its components. This feature ensures that the system is not exposed to any tampered code by measuring the Cisco NX-OS system and its components. Use CLI and NX-API to access the measurement of the Cisco NX-OS components on the Cisco Nexus switch. You can verify the authenticity of the Cisco NX-OS components by comparing the measurements against Known Good Values (KGVs) that are available on Cisco Connection Online (CCO) for the corresponding Cisco NX-OS release.

Note Ensure that both the switch and the controller support the Runtime Integrity Assurance feature. You should also verify whether the Cisco DCNM release being used by you supports this feature.

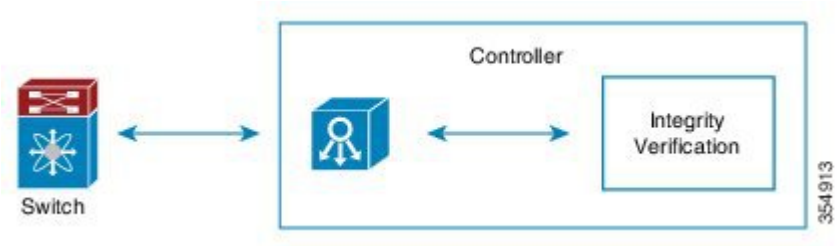
Runtime Integrity Assurance feature is enabled by default and cannot be disabled. However, verification at the controller is optional. In this case, you can access the measurements by using the CLI and compare the measurements against KGVs manually.

How Runtime Integrity Assurance Works

The security features in Cisco NX-OS provides resilience against attacks. From Cisco NX-OS Release 8.0 (1), the system security monitoring functionality provides status for the following security features:

Runtime integrity assurance involves two entities, namely, a switch and a controller. An integrity verification functionality is also embedded within the controller. This integrity verification entity within the controller analyzes the integrity data received from a switch.

Figure 1: Runtime Integrity Assurance on Cisco Nexus 7000 Series Switch



On a switch, measurement of the running software is performed. This is carried out when a file is loaded for execution. The measurements are available through the CLI and NX-API.

You can schedule verification at recurring intervals on the controller. Additionally, the controller collects the measurements from a switch and compare them against the KGVs. For more information, see the *Cisco DCNM Fundamentals Guide*.

Manual Verification of Files

Runtime integrity assurance through the controller is preferred for verification of files. However, you can also verify files manually by using the CLI.

To manually verify files, log in to CCO and download the KGVs. You can manually compare the hashes, which have been dumped through CLI, with the KGVs.

To display runtime integrity information, use one of the following commands:

- **show software integrity total** - Displays the number of measurements available in runtime integrity hash digests.
- **show software integrity** *index* - Displays hash digest entries by specifying the starting index value.

Note NX-API also supports the **show software integrity** command. Therefore, you can write scripts to verify the hash values received from the switch and the KGVs downloaded from CCO.

Displaying Information About Runtime Integrity Assurance

The following example shows how to display the number of measurements available in hash digests:

```
switch# show software integrity total
1092
```

The following example shows how to display the hash digest entries:

```
switch# show software integrity index 0
index pcr template-hash template-name al
gorithm:filedata-hash filena
me-hint
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
reference: 1481115089
1 10 1d8d532d463c9f8c205d0df7787669a85f93e260 ima-ng sh
a1:0000000000000000000000000000000000000000 boot_a
ggregate
2 10 1cb9d1e2795a75857f70d6a23cb77e4843467617 ima-ng sh
a256:850c63f1b32f19b2dcde9fa199a83da920c9e377e1e2dc52a6c7fdd045a21475 /etc/r
c.d/rcS.d/S98admin-login
3 10 95929573f5252fa80ad4bfb3b6dd644c5617d359 ima-ng sh
a256:1c684d45641dd23e1b2a763006030b9be46d8309581876c7a34feee1c87e037c /bin/b
ash
```

Additional References for Software Integrity Assurance

This section includes additional information related to Software Integrity Assurance feature.

Related Documents

Related Topic	Document Title
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Security Command Reference*

Feature History for Software Integrity Assurance

This table lists the release history for this feature.

Table 1: Feature History for Software Integrity Assurance

Feature Name	Release	Feature Information
Runtime Integrity Assurance	8.0(1)	This feature was introduced. The following command was introduced: • **show software integrity total**