



ブート整合性の可視性

- [ブート整合性の可視性について \(1 ページ\)](#)
- [ソフトウェアイメージとハードウェアの確認 \(1 ページ\)](#)
- [プラットフォーム ID とソフトウェア整合性の確認 \(2 ページ\)](#)
- [ブート整合性の可視性に関する追加情報 \(6 ページ\)](#)
- [ブート整合性の可視性の機能履歴 \(6 ページ\)](#)

ブート整合性の可視性について

ブート整合性の可視性によって、シスコのプラットフォーム ID とソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォーム ID は、プラットフォームの製造元でインストールされた ID を提供します。ソフトウェアの整合性ではブート整合性の測定値が明らかになり、それを使用してプラットフォームが信頼できるコードを起動しているかどうかを評価できます。

ブートプロセス中に、ソフトウェアはブートローダーアクティビティの各ステージのチェックサムレコードを作成します。

このレコードを取得して、シスコ認定レコードと比較し、ソフトウェアイメージが正規かどうかを確認できます。チェックサム値が一致していない場合は、シスコによって認定されていない、または未承認パーティによって改ざんされているソフトウェアイメージを実行している可能性があります。

ソフトウェアイメージとハードウェアの確認

このタスクでは、スイッチの起動時に作成されたチェックサムレコードを取得する方法について説明します。特権 EXEC モードで次のコマンドを入力します。



- (注) 次のコマンドを実行した後で、メッセージ **% Please Try After Few Seconds** が CLI に表示されることがあります。これは CLI の障害を示すものではありませんが、必要な出力を取得するために必要な基盤となるインフラストラクチャの設定を示します。数分間待機して、コマンドを再度試すことをお勧めします。

メッセージ **% Error retrieving SUDI certificate** および **% Error retrieving integrity data** は、実際の CLI 障害を示します。

手順

	コマンドまたはアクション	目的
ステップ 1	show platform sudi certificate [sign [nonce nonce]] 例： Device# show platform sudi certificate sign nonce 123	特定の SUDI のチェックサム レコードを表示します。 <ul style="list-style-type: none"> • (オプション) sign : 署名を示します • (オプション) nonce : ナンス値を入力します
ステップ 2	show platform integrity [sign [nonce nonce]] 例： Device# show platform integrity sign nonce 123	ブート段階のチェックサム レコードを表示します。 <ul style="list-style-type: none"> • (オプション) sign : 署名を示します • (オプション) nonce : ナンス値を入力します

プラットフォーム ID とソフトウェア整合性の確認

プラットフォーム ID の確認

次に、PEM 形式でセキュアな固有デバイス識別子 (SUDI) チェーンを表示する例を示します。SUDI にエンコードされるのは、個々のデバイスの製品 ID とシリアル番号であり、何千ものデバイスからなるネットワーク上でデバイスを一意に識別できます。最初の証明書は Cisco Root CA 2048 で、2 番目はシスコの下位 CA (ACT2 SUDI CA) です。どちらの証明書も、<https://www.cisco.com/security/pki/> で公開されているものと一致しているかを確認できます。3 番目は SUDI 証明書です。

```
Device# show platform sudi certificate sign nonce 123
-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KctU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDEsJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
```

```

Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQDExJDaXNjbyBSb290IENBIDIwNDgwgEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwgEIAoIBAQCwmrmp68Kd6f1cba0ZmKUEIhH
xmJVhEAYv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmAHBKeN8hf570YQXJ
FcjPFto1YmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUL4F1pyXOWWqCZe+36ufijXWlLvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6ke01a06g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYUCUTOG/rksc35LgLfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFbi71R803UXHOjgxxkLtv5M0hmEVRBW7hmW
Yqpao2TB9k5UM8Z3/sUcuVdJcr18JOagxEu5sv4dEX+5wW4q+ffY0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJdTsd9i7rp77rMKSSh0T8lasz
Bvt9YaretIpsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGeOcaEblfJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQkOXuPL1hS27PKSb3TkL4Eq1ZKR4OCXPdJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

```

```

MIIEPDCCAySgAwIBAgIKYQlufQAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAyD
VQKKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQDExJDaXNjbyBSb290IENBIDIwNDgW
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQKKEwVDAxNj
bzEVMBMGALUEAxMMQUNUMiBTURJiENBmIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBGgKCAQEA0m513THIXA9tN/hs5qR/6UZRpdd+9aE2JbFknjht6gfHKd477AkS
5XAtUs5oxDYvt/zEbs1Zq3+LR6qrqKQVu6JYvH05UYLBqCj38s76Nlk53905Wzp
9pRcmRCPUx+a6tHF/qRuOiJ4mdedYz03qPCpxzprWJDPclM4iYKHuMqMqmgm+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXDgJ130veF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sX1XtEoJSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdvQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GALUdDgQWBBRI2PHxwDvW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAGwBQn
88gVHm6aAgkWrSugiWBF2nsqvjBDBGNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZW50cm9udG9zaW50cm9udG9zaW50cm9udG9zaW50cm9udG9z
BQcBAQREMEIwQAYIKwYBBQUHMAKGNh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNmMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEBAQKv
AQwAMEMwQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY21zY28uY29tL3N1Y3VyXAR5
L3BraS9wb2xpy21lcY9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAgh1qclr9tx4hzWgDERm371yeuEmqcIffi9b9+GbMSJbi
ZHc/Cc101Ju0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Ik1t8nNbcKY
/4dwlEx+7amATUQ04QggIE67wVlPu6bgAE3Ja/nRS3xKYSnj8H5TehimbSv6TEci
i5jUhOWryAK4dVo8hcJkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djfKn
hyl47d7cZR4DY4LlUfM2PlAs8YyjzoNpK/urSRI14wdI1plRlnH7KND15618yfvP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----

```

```

MIIDezCCAmOgAwIBAgIEAc+JiTANBgkqhkiG9w0BAQsFADANMQ4wDAYDVQKKEwVDA
xNjbyzEVMBMGALUEAxMMQUNUMiBTURJiENBmB4XDTE3MDgxoTEwNDMzOVoxDTI3
MDgxOTEwNDMzOVowZzEmMCQGA1UEBRMduE1EokM5MzAwLTI0VVggU046RkNKMjEz
NEwwMEMxZjAMBGNVBAoTBUNpc2NvMRgwFgYDVQQLLEw9BQ1QTMiBMAxR1IFNVREkx
EzARBGNVBAmtckM5MzAwLTI0VVggwGgEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQDdav5txv4THsqxwWC7AxzHm5Mz28Feqk8FA3tXAv0tV8RXtY4Z9I9XgRzw
Yw8chkn8LuDMcmGmk8DP+ct++vAF4nkVeIeBeOHnx2RuC9rcR8tuKjCimamDk0M
JHk12w/9+TbdKdNBEy6Sueh1RPVbuSkloQLQcOYW7CsYC5tI1GkKkfk1nGEK3ni3
ztIpsi7QHyp6k59yccnbzXSdwoBrtpIIEk/iHwFRQdlMUunnfIshI7yPneo7V0
NnPC08wk+CA+8XeXk/fnDeGAswKRK1tW9jDP/sY1YubBJNJ4ToqqG6W/hbNvu3Y
Nys24osSvnn5Bp7on3Rf7eHq9hNjAgMBAAGjbjBzBtMA4GALUdDwEB/wQEAWIF4DAM
BgNVHRMBAf8EAjAAAME0GALUdEQRGMEsgQyJKwYBBAEJFQIDoDUTM0NoaXBjRd1V
WUPPVkVZNEZRT0xSbkpwSUUxaGNpQXhNQ0F4Tnpvd05Eb3hNeUfiY1FjPTANBgkq
hkiG9w0BAQsFAAOCAQEASXX+iZLMvHQIR1/s1Pobm0kP/bYeHsgDTRQPRHbCM1HH
ROfjJDaJMHcspB17XtclKNNFowYUEkjoePyHjpxxhekGIqgD6Xt4rW6v/058Haw6
QbAhJFGZriVxFOBvW20VQ4ezyaGoqA+0I2GzQD/zggUY6zsVwKMe6inoEgXcYap
5GqF4weEoty9u+OKqr3ppWU475lXnNm/h+WHbNtunL6r7wZfe5dFQIXR5Qp5gRa
svpSsCoKm6PwiUhw25CvtZ9NTg0tu5t5D7aVcxLeR8XbAlpjfgxw/RtSsjNse3+
ZkOgJUESqlxwzxcGULY+vDINyRQ/sP6y7cT+niT00A==
-----END CERTIFICATE-----

```

Signature version: 1

Signature:

```
-----BEGIN RSA SIGNATURE-----
```

オプションの RSA 2048 署名は、3つの証明書、署名のバージョンおよびユーザーにより提供されるナンスに対するものです。

```
RSA PKCS#1v1.5 Sign {<Nonce (UINT64)> || <Signature Version (UINT32)> || <Cisco Root CA
  2048 cert (DER)> ||
<Cisco subordinate CA (DER)> || <SUDI certificate (DER)> }
```

シスコの管理ソリューションには、上記の出力を解釈する機能が装備されています。しかし、OpenSSL コマンドを使用した簡単なスクリプトを使用してプラットフォームの ID を表示して署名を確認することもでき、それによってシスコの一意的デバイス ID を確保できます。

```
[linux-host:~]openssl x509 -in sudicert.pem -subject -noout
subject= /serialNumber=PID:C9300-24P SN:FDO1946BG05/O=Cisco/OU=ACT-2 Lite SUDI/CN=C9300-24P
```

ソフトウェア整合性の確認

次に、ブート段階のチェックサムレコードを表示する例を示します。ハッシュ測定値は、連続してブートされたソフトウェアの3つの段階それぞれについて表示されます。これらのハッシュをシスコが提供する基準値と比較できます。出力に署名するオプションを使用すると、出力は正規であり改ざんされていないことを保証する機能が検証ツールに付与されます。リプレイ攻撃から保護するために、ナンスを提供できます。



(注) ブート整合性ハッシュはMD5ハッシュではありません。バンドルファイルに対して **verify/md5 cat9k_iosxe.16.10.01.SPA.bin** コマンドを実行すると、ハッシュは一致しません。

次に、インストールモードでの **show platform integrity sign nonce 123** コマンドの出力例を示します。この出力には、インストールされている各パッケージファイルの測定値が含まれます。

```
Device# show platform integrity sign nonce 123
Platform: C9300-24P
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F82826514658055C39932B95F53512341BF20F3CC7D4083C980450EA6CD84608EE636B5B15D13414203CED35603F01974B8676C6AC6F9DC45E25CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0
cat9k-espsbase.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEF43
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
```

```

E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:

```

次に、バンドルモードでの **show platform integrity sign nonce 123** コマンドの出力例を示します。この出力には、バンドルファイルとインストールされている各パッケージの測定値が含まれます。

```

Device# show platform integrity sign nonce 123
Platform: C9300-24P
Boot 0 Version: MA0081R06.1307262016
Boot 0 Hash: A99EF9F31CE3F3F8533055407F1C88C62176E667E4E1DA0649EAA7A1282F205E0A
Boot Loader Version: System Bootstrap, Version 16.8.0.3, RELEASE SOFTWARE (P)
Boot Loader Hash:
F82826514658055C3993AB95F53512341BF20F3CC7D4083C980450EA6CD84608EE638B5E15D13414203CED35603F01974B8676C6AC6F9C4525CD1039E686C40A
OS Version: 16.10.01
OS Hashes:
cat9k_iosxe.16.10.01.SPA.bin :
F4CAD08EE1EF841C3A2E3ED8540829F08F3CBA9336F38E45669D4D8B15AD15E365B922AC8B4D00D5B63E2806D6A1EDAB7839DD9DC8D7E366A49ED648C113440
cat9k-cc_srdriver.16.10.01.SPA.pkg :
D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0
cat9k-espbases.16.10.01.SPA.pkg :
3EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEF3
cat9k-guestshell.16.10.01.SPA.pkg :
B0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03E
cat9k-rpbase.16.10.01.SPA.pkg :
4057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C6
cat9k-rpboot.16.10.01.SPA.pkg :
AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057
cat9k-sipbase.16.10.01.SPA.pkg :
9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A
cat9k-sipspa.16.10.01.SPA.pkg :
E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673
cat9k-srdriver.16.10.01.SPA.pkg :
4FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E211
cat9k-webui.16.10.01.SPA.pkg :
CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7
cat9k-wlc.16.10.01.SPA.pkg :
AA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCAAA7ED0AE935CB0BD84E0D0D155C1DEFB03EB0C64057AD6A9673E2114FA7CCCA
PCR0: 9745B571B66D79F0936F4D292B5672B50F50FD1E56E74248D48A33582E992574
PCR8: 1CC295C233DA41BD3530A6F09C21991E8406BFFC88249D7778CA4BB0B9E71EB7
Signature version: 1
Signature:

```

ブート整合性の可視性に関する追加情報

関連資料

関連項目	マニュアルタイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	<i>Command Reference (Catalyst 9300 Series Switches)</i>

ブート整合性の可視性の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Fuji 16.8.1a	ブート整合性の可視性	ブート整合性の可視性によって、シスコのプラットフォームIDとソフトウェアの整合性情報が可視化され、実用可能になります。プラットフォームIDは、プラットフォームの製造元でインストールされたIDを提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。